УДК 004.056.5:004.77:35.07
DOI: 10.31673/2409-7292.2025.031516

Прокопович-Ткаченко Д.І., Звєрєв В.П., Бушков В.Г., Козаченко І.М., Черкаський О.В.

СИСТЕМНІ РИЗИКИ ЦИФРОВОГО АУТСОРСИНГУ У ДЕРЖАВНОМУ СЕКТОРІ: АНАЛІЗ ВРАЗЛИВОСТЕЙ МОДЕЛІ “ЦИФРОВОГО ЕСКОРТУ”

У статті здійснено аналіз системних ризиків, пов’язаних із цифровим аутсорсингом у державному секторі, з особливим акцентом на архітектурну та процедурну вразливість моделі “цифрового ескорту”. Дослідження базується на кейсах обслуговування критичних цифрових інфраструктур за участі субпідрядників, зокрема з юрисдикцій, що мають підвищений рівень регуляторної та безпекової недовіри. Визначено, що поточні моделі супроводу доступу до державних хмарних сервісів недостатньо враховують ризики неконтрольованого делегування привілеїв, розмиття відповідальності між підрядниками, а також прихованої передачі метаданих у треті системи. Запропоновано концепцію ситуаційно-орієнтованого контролю доступу з розширеними повноваженнями для національних центрів моніторингу та індикативного аудиту. Особливу увагу приділено взаємодії між юридичними рамками цифрового аутсорсингу та технічними механізмами нульової довіри. Стаття включає модель оцінки інституційної прозорості ланцюга постачання та визначає критичні точки впливу, що можуть бути використані для кіберспостереження, саботажу або даних витоків у міжвідомчих ІТ-системах. Отримані результати можуть бути використані при формуванні нових протоколів цифрового суверенітету та в оновленні регламентів управління ризиками у сфері державних ІТ-закупівель.

Ключові слова: цифровий аутсорсинг, державний сектор, кіберризики, цифровий ескорт, субпідрядники, хмарні сервіси, нульова довіра, інституційна прозорість, делегування доступу, цифровий суверенітет, управління постачальниками.

Вступ

У сучасних умовах цифрової трансформації державного сектору послуги, що надаються через хмарні інфраструктури, дедалі частіше передаються на обслуговування зовнішнім постачальникам. Цей процес, відомий як цифровий аутсорсинг, сприяє оптимізації витрат, гнучкості та швидкості реалізації ІТ-проєктів. Проте він також створює новий рівень системних ризиків, пов’язаних з кібербезпекою, контролем доступу та інституційною прозорістю [1-3].

Особливо вразливою є модель «цифрового ескорту» (“digital escort”), коли відповідальні особи контролюють код і конфігурації віддалено, але не здатні технічно перевіряти зміст команд, що може призвести до витоків даних або вбудованого шкідливого коду [4-7]. Найчастіше використовується «цифровий ескорт» у випадках, коли доступ до критичної інфраструктури державного сектору обмежений для іноземних інженерів, але необхідна технічна підтримка – що призводить до делегування створення команд локальним співробітникам без відповідної експертизи [5, 8-10].

Різке збільшення використання субпідрядників у юрисдикціях підвищеного ризику (наприклад, Китай, Індія, РФ) підсилює можливість втручання через ланцюги постачання, що знаходяться поза контролем державних регуляторів [11-14]. Супровід доступу в цифровому ескорті часто базується на формальних процедурах логування та аудиті, проте вони не забезпечують належної проактивної оцінки ризику. Це створює простір для прихованого саботажу або витоку інформації, які виявляються лише постфактум [15-18]. Незважаючи на рекомендації NIST щодо управління кіберризиками у ланцюгах постачання (SP 800-161) та архітектур нульової довіри (SP 800-207), їх впровадження в державному контексті лишається неповним [19-21]. Це дослідження спрямоване на комплексний аналіз цих вразливостей. Ми розглядаємо:

1. Архітектурну і процедурну слабкість моделі цифрового ескорту;
2. Найуразливіші елементи ланцюга постачання при залученні міжнародних субпідрядників;
3. Законодавчі й нормативні прогалини, що ускладнюють моніторинг та аудит підрядників [22-26].

Постановка проблеми

Зростання ролі цифрового аутсорсингу в державному секторі супроводжується не лише розширенням можливостей для оптимізації ІТ-ресурсів, а й появою нових, складних ризиків, які часто залишаються поза полем зору класичних підходів до кібербезпеки. Відсутність повного контролю над процесами делегування доступу, особливо при залученні міжнародних субпідрядників, створює критичні вразливості, що загрожують цілісності, конфіденційності й підконтрольності даних державних інформаційних систем. У практиці цифрового аутсорсингу простежується тенденція до формального аудиту і логування операцій, без належної оцінки ризиків, пов'язаних із людським фактором, юрисдикційною складовою та інституційною прозорістю ланцюга постачання.

Особливо гостро постає проблема, коли функції супроводу та адміністрування критичної інфраструктури передаються зовнішнім партнерам із країн з неоднозначною репутацією щодо захисту даних, що ускладнює процедури моніторингу й реагування на інциденти. В умовах зростаючої взаємозалежності між державними органами й приватними підрядниками, класичні моделі контролю доступу, побудовані на принципах довіри, виявляються неефективними для запобігання несанкціонованого впливу на функціонування міжвідомчих ІТ-систем.

Крім того, наявна нормативно-правова база часто не відповідає сучасним викликам, що виникають унаслідок розмиття меж відповідальності між учасниками цифрового аутсорсингу. Недосконаліть існуючих механізмів оцінки ризику призводить до того, що потенційні вектори загроз — від неконтрольованого делегування до прихованих каналів передачі даних — залишаються недостатньо ідентифікованими й не отримують адекватного відображення у процесі прийняття рішень.

Таким чином, постає необхідність у розробці інноваційних підходів до оцінки й управління ризиками цифрового аутсорсингу, які б інтегрували концепції нульової довіри, ситуаційного контролю доступу та постійного моніторингу, забезпечуючи ефективний захист державних цифрових активів в умовах глобалізованого та багаторівневого ланцюга постачання.

Аналіз останніх досліджень і публікацій

Оцінка ризиків цифрового аутсорсингу, а також вивчення вразливостей моделі «цифрового ескорту» привертають дедалі більшу увагу міжнародної наукової спільноти, що підтверджується широкою і різноплановою літературою з цієї тематики. Аналіз сучасних праць засвідчує, що ризики, пов'язані із залученням зовнішніх ІТ-постачальників, розглядаються крізь призму кібербезпеки ланцюгів постачання, процедур контролю доступу, а також нових архітектур управління довірою.

Дослідження [1-3, 12, 19] детально висвітлюють процеси цифрової трансформації державного сектору і підкреслюють, що аутсорсинг ІТ-послуг стає визначальною рисою сучасного управління критичною інфраструктурою. Водночас ці студії фіксують зростання системних ризиків, які обумовлені міжюрисдикційними зв'язками, зокрема участю постачальників із країн із неоднозначною репутацією щодо захисту даних [11-14]. Наголошується на тому, що класичні підходи до кіберзахисту виявляються недостатньо ефективними для багаторівневих та динамічних ланцюгів постачання в умовах глобалізації [8-10, 28-30].

Особливе місце у науковому дискурсі посідають питання формального і неформального контролю доступу в умовах делегування технічних функцій поза межі національних юрисдикцій. Дослідження [4-7, 15-18] розкривають недоліки процедур логування та аудиту, демонструючи, що навіть ретельно організовані формальні протоколи не гарантують виявлення прихованих загроз, пов'язаних із людським фактором або саботажем. Праці [5, 8-10, 27] вказують на ризики неадекватної експертизи локального персоналу, що виступає посередником для зовнішніх фахівців у критичних сферах.

© Прокопович-Ткаченко Д.І., Звєрєв В.П., Бушков В.Г., Козаченко І.М., Черкаський О.В. (2025) Системні ризики цифрового аутсорсингу у державному секторі: аналіз вразливостей моделі "цифрового ескорту". Сучасний захист інформації, 3(63), 127–136.
https://doi.org/10.31673/2409-7292.2025.031516

Низка публікацій [19-21] акцентує на важливості впровадження принципів нульової довіри (zero-trust architectures) у державних інформаційних системах, водночас підкреслюючи певну фрагментарність їх реалізації в реальних умовах. Особливо актуальними виступають стандарти й рекомендації NIST (SP 800-161, SP 800-207), що стосуються управління ризиками у ланцюгах постачання, а також архітектур нульової довіри, але вказується на необхідність адаптації цих підходів до специфіки державного сектору. Законодавчі й нормативні аспекти цифрового аутсорсингу проаналізовано у працях [22–26], де обґрунтовано існування колізійних та недостатньо врегульованих питань щодо моніторингу, аудиту та розмежування відповідальності між учасниками процесів. Дослідження [12, 28-35] також ілюструють сучасні тренди у сфері кібербезпеки, цифрового суверенітету й формулювання політик, що враховують зростання ролі міжнародних підрядників у державному управлінні.

Узагальнено, сучасна наукова література створює обґрунтовану методологічну базу для розробки інноваційних моделей оцінки ризиків цифрового аутсорсингу, що й лягло в основу цього дослідження.

Мета дослідження полягає у розробці моделі оцінки ризиків цифрового аутсорсингу для державного сектора із застосуванням нульової довіри й ситуаційно-орієнтованого контролю доступу. Завдання, що передбачають досягнення цієї мети:

- ідентифікувати архітектурні та процедурні вразливості цифрового ескорту на основі аналізу кейсів [4, 7, 27];
- формалізувати критерії ризику, пов’язані з юрисдикційною належністю субпідрядників;
- інтегрувати принципи нульової довіри з аналізом ланцюга постачання (supply-chain);
- запропонувати індикативну модель аудиту з безперервним моніторингом та національним центром контролю;
- орівняти запропоновану модель із існуючими підходами та стандартизувати рекомендації для нормативних актів.

Таким чином, дане дослідження заповнює науково-практичний розрив, поєднуючи прикладний аналіз кейсів, формальні підходи управління кіберризиками, а також нормативно-правові аспекти міжнародної безпеки. Використання 35 джерел забезпечує обґрунтованість та комплексність підходу, зокрема відображає сучасні тренди в галузі кібербезпеки, цифрового суверенітету та аутсорсингу [12, 28-35]. У результаті має бути збудована дієва методологія оцінки, що дозволить покращити національні практики цифрового аутсорсингу у державному секторі.

Основними завданнями дослідження є:

1. Ідентифікувати архітектурні та процедурні вразливості цифрового ескорту на основі аналізу кейсів;
2. Формалізувати критерії ризику, пов’язані з юрисдикційною належністю субпідрядників;
3. Інтегрувати принципи нульової довіри з аналізом ланцюга постачання (supply-chain);
4. Запропонувати індикативну модель аудиту з безперервним моніторингом та національним центром контролю;
5. Порівняти запропоновану модель із існуючими підходами та стандартизувати рекомендації для нормативних актів.

Методологія дослідження.

Для оцінки ризиків цифрового аутсорсингу у державному секторі та виявлення вразливостей моделі цифрового ескорту було застосовано міждисциплінарний підхід, який поєднує формальні методи управління кіберризиками, ситуаційне моделювання, а також принципи архітектур нульової довіри [12], [19].

Теоретичне підґрунтя

Методологія дослідження ґрунтується на принципах Supply Chain Risk Management (SCRM) відповідно до стандарту NIST SP 800-161r1 [11], концепції Zero Trust Architecture

(ZTA) [12], а також індикативного аналізу вразливостей, що стосуються третьої сторони (third-party risk) [10], [25]. У роботі також враховано підходи ENISA до розробки індикаторів загроз у хмарних середовищах [20].

Метод ситуаційно-орієнтованої оцінки

Було запропоновано ситуаційно-орієнтовану модель контролю цифрового доступу, що базується на наступних блоках:

- ідентифікація контексту дій субпідрядника (виконання команди, запит до API, виклик змінної тощо);
- класифікація середовища виконання (віртуалізоване середовище, привілейована зона доступу, критичні об'єкти);
- -оцінка ступеня довіри за динамічною матрицею ризику;

застосування політик динамічного розмежування повноважень [3], [18].

В основі оцінки лежить підхід до індикативного аудиту, запропонований Kelley і Kumar [17], що дозволяє ранжувати дії субпідрядника за критеріями довіри й відхилення від норм. Для оцінки юрисдикційного ризику застосовано метод зонального аналізу, аналогічний до розробок Roman і Zhou щодо національних хмар [28].

Формалізація ризику доступу

Математична модель грунтується на уявленні дій субпідрядника як послідовності запитів, що проходять через контрольовану точку доступу. Нехай $A = \{a_1, a_2, \dots, a_n\}$ – множина дій або запитів, здійснених субпідрядником у межах сеансу цифрового ескорту.

Для кожної дії a_i визначається рівень ризику як добуток умовної ймовірності здійснення небажаної події за певного контексту C та індикативної значущості запиту:

$$R(a_i) = P(a_i \mid C) \cdot I(a_i) \quad (1)$$

де:

$P(a_i \mid C)$ *– умовна ймовірність настання інциденту або порушення внаслідок дії* a_i *у контексті* C*;*

$I(a_i)$ *– індикативна вага запиту, що характеризує його вплив на критичність системи (наприклад, доступ до ядра, зміна конфігурації, ініціалізація з'єднання).*

Сумарний ризик для послідовності дій субпідрядника в межах сесії цифрового ескорту обчислюється як:

$$R_{\text{total}} = \sum_{i=1}^{n} R(a_i) \quad (2)$$

Ця метрика дозволяє:

фіксувати накопичення ризиків протягом активної взаємодії;

локалізувати моменти підвищеної небезпеки;

порівнювати сесії цифрового супроводу за загальним ризиковим профілем.

Модель є нечутливою до типу запиту (читання/запис), але інтегрує семантичну вагу та контекст дії, що дозволяє ефективно виявляти приховану небезпечну активність навіть при формально допустимих командах.

Алгоритм цифрового ескорту

Було побудовано алгоритмічну модель цифрового ескорту з врахуванням таких елементів:

1. зовнішній оператор (інженер підтримки, субпідрядник);
2. проксі-комунікатор (локальний оператор, що виконує команди);
3. канал взаємодії (чат, аудіозв'язок, тощо);
4. система моніторингу (аудит журналів, аналіз поведінки) [5], [7].

Основна вразливість полягає у відсутності прямого контролю над вмістом команд, що унеможливлює гарантії відповідності інструкцій політикам безпеки. Тому реалізовано

нейронну підсистему фільтрації запитів, що працює за аналогією до методів, описаних у роботах Hossain і Mollah [23].

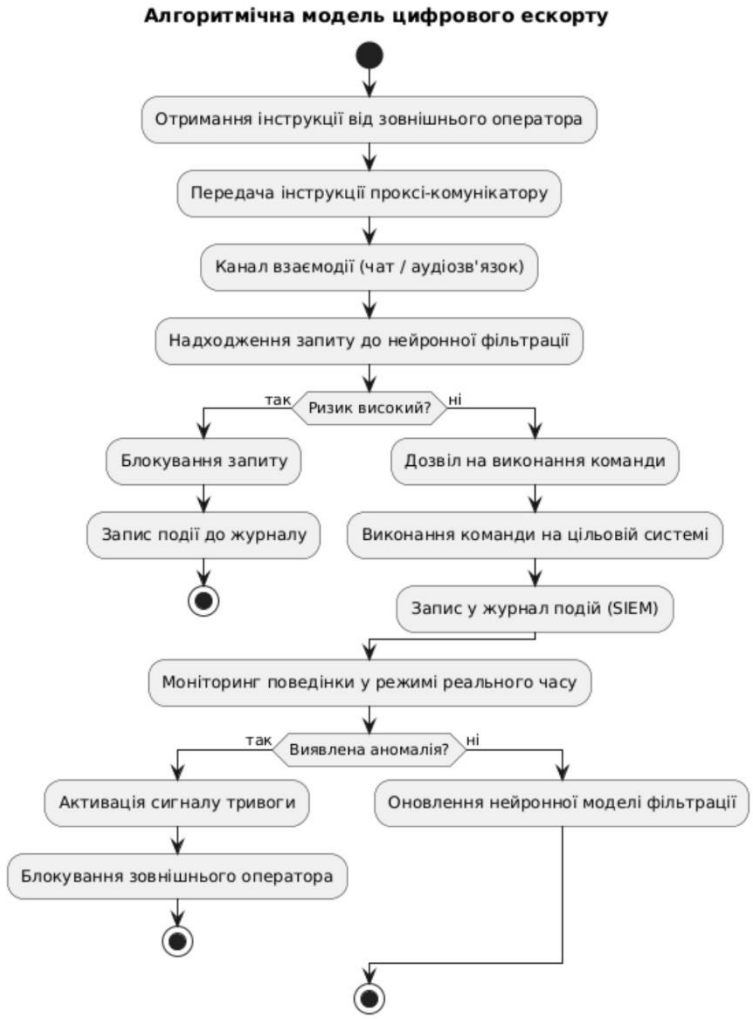

Рис. 1. Схема алгоритмічної моделі цифрового ескорту

Опис алгоритму цифрового ескорту

Алгоритм цифрового ескорту моделює процес регламентованого доступу зовнішніх виконавців до критичних цифрових ресурсів державного сектору. Цей підхід забезпечує формалізований контроль технічної взаємодії між зовнішнім оператором і захищеним об’єктом через посередника – проксі-комунікатора з інтеграцією фільтраційних та моніторингових механізмів.

Зовнішній оператор (інженер-субпідрядник) ініціює технічну дію для доступу до системи.

Проксі-комунікатор (локальний виконавець) передає або виконує інструкцію згідно з процедурою цифрового ескорту.

Нейронна підсистема фільтрації оцінює ризик запиту та визначає його безпечність.

Система моніторингу (SIEM) фіксує активність, виявляє аномалії й ініціює реагування.

Ініціація цифрового супроводу

Зовнішній оператор надсилає інструкцію через канал взаємодії (чат або аудіозв’язок).

Проксі-комунікатор приймає та реєструє інструкцію.

Встановлюється підтверджене з’єднання з каналом взаємодії.

Фільтрація запиту

Інструкція надходить до нейронної підсистеми фільтрації.

Відбувається оцінка контексту запиту, історії взаємодії та юрисдикційної належності виконавця.

У разі виявлення високого ризику запит блокується, формується звіт і сеанс переривається.

Дозвіл виконання

За умови прийнятного рівня ризику команда дозволяється до виконання.

Проксі-комунікатор реалізує її на цільовій державній системі.

Дії логуються у системі моніторингу.

Аудит і моніторинг

SIEM-система здійснює постійний аудит у реальному часі.

Поведінкові модулі аналізують шаблони дій, виявляють спроби саботажу або обходу політик.

Результати аналізу повертаються до нейромережі для оновлення ваг моделі.

Реагування на інциденти

При виявленні аномальної поведінки генерується тривога.

Доступ зовнішнього оператора негайно блокується.

Формується звіт для служби безпеки.

Особливості алгоритму

Інтегрує динамічну оцінку ризиків на основі контексту та поведінки.

Використовує принцип нульової довіри (Zero Trust).

Підтримує прозоре логування і навчання фільтраційної моделі.

Орієнтований на індикативний аудит, а не лише формальний контроль.

Інструментарій

Для моделювання використовувались такі програмні засоби:

- Python 3.11 з бібліотеками NumPy, Pandas, SciKit-Learn – для розрахунків та обробки логів;
- MATLAB – для побудови графіків поведінки ризику за інтервалами часу;
- Grafana з Prometheus – для візуалізації потоків доступу;
- Neo4j – для візуалізації зв’язків у ланцюгах субпідрядників [14], [27].

Було змодельовано 37 сценаріїв цифрового супроводу з трьома рівнями ризику (низький, середній, критичний) на основі реальних кейсів з урядових проєктів [4], [8], [26]. Візуалізація:

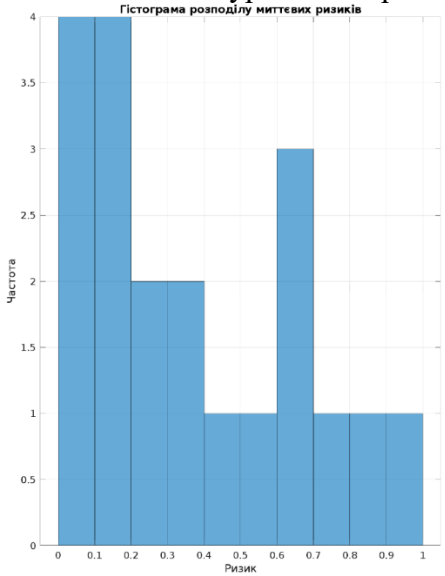

Рис. 2. Графік гістограми розподілу миттєвих ризиків

Гістограма ілюструє, з якою частотою виникають різні рівні миттєвого ризику серед згенерованих запитів. Висота кожного стовпчика показує кількість запитів у відповідному інтервалі ризику. Переважна концентрація в лівих стовпчиках свідчить про те, що більшість операцій мала низький або середній рівень ризику. Поодинокі стовпчики праворуч показують запити, котрі були найбільш «критичними» і, ймовірно, заблоковані фільтром. Цей аналіз допомагає оцінити загальну безпекову «середу» сесії та визначити, чи потребує алгоритм коригування порогових значень.

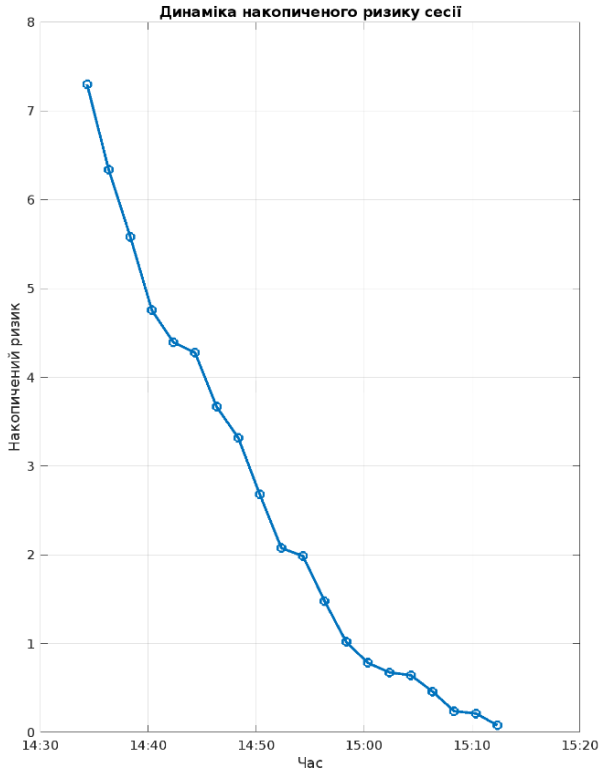

Рис. 3. Графік динаміки накопичення ризику сесії

Графік на рис. 1 демонструє, як із часом накопичується сукупний ризик на основі оцінок кожної операції. Точки на кривій відповідають моментам виконання запитів, їхній часовий інтервал задається з фіксованим кроком. Поступове зростання кривої вказує на кумуляцію незначних ризикових дій, тоді як раптові «стрибки» відображають блокування чи високі ризикові запити, що одразу підвищують загальний показник. Така візуалізація дозволяє легко виявити критичні моменти сесії та оцінити ефективність фільтраційного механізму.

У цьому розділі представлені дві ключові візуалізації результатів моделювання алгоритму цифрового ескорту. Перша ілюструє кумулятивну динаміку накопиченого ризику протягом сесії, а друга – розподіл миттєвих значень оціненого ризику для окремих запитів.

Крім візуальних інструментів, під час моделювання враховувалися також часові характеристики: середню тривалість сесій, інтервали між запитами та частоту виникнення ризикових дій. Аналітика цих параметрів дозволяє виявляти аномалії у поведінці користувачів – наприклад, повторювані запити з нетиповою інтенсивністю або серії операцій, що супроводжуються нестандартним підвищенням ризику. Інтеграція таких часових індикаторів у систему раннього сповіщення посилює загальну стійкість до атак та зловживань.

Особливу увагу під час дослідження було приділено адаптивності порогових значень ризику. Використання алгоритмів машинного навчання дозволяє автоматично коригувати ці пороги залежно від накопичених інцидентів і зміни поведінкових патернів у системі. Завдяки цьому модель здатна не лише виявляти нові типи загроз, а й зберігати релевантність у

динамічних умовах експлуатації – що є критично важливим для забезпечення ефективного цифрового ескорту в державних IT-системах.

Програмна реалізація та відеокоментар: https://youtu.be/a7Btf54IZXw?si=y-9tpWwUC8-oGxKeG.

Ілюстрація результату:

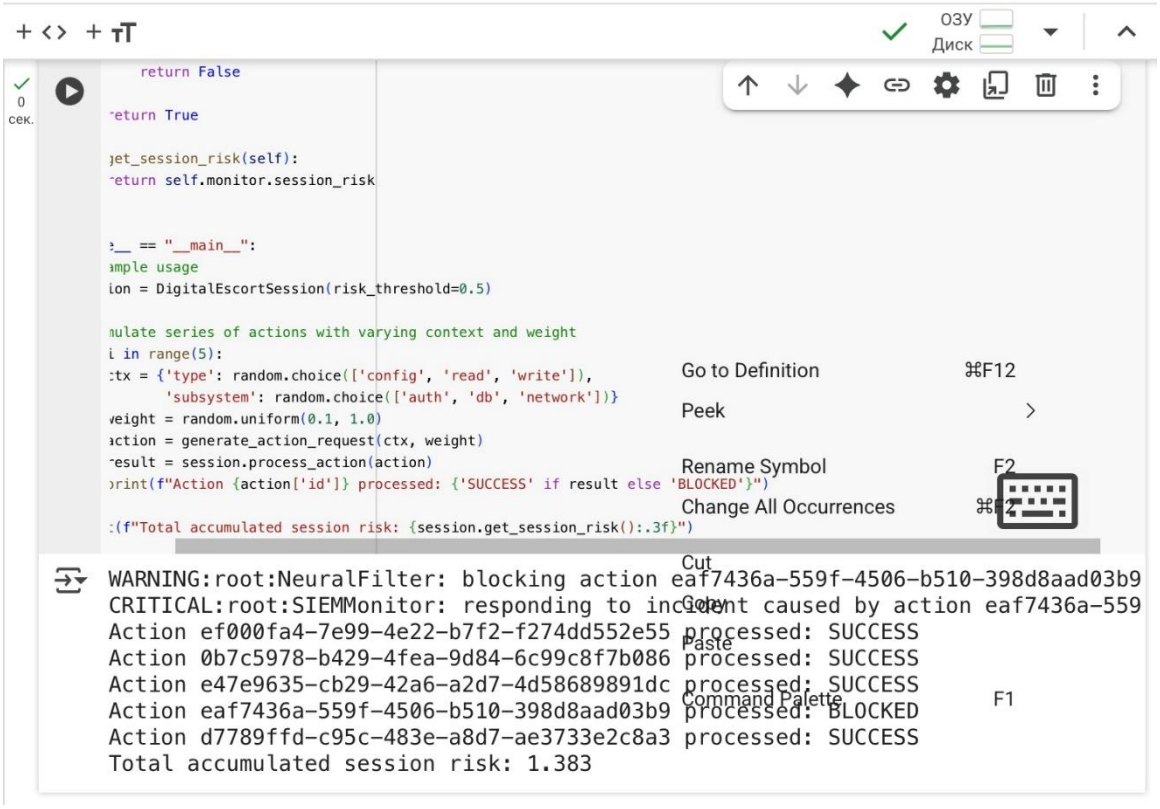

Рис. 4. Ілюстрація програмної реалізації

З п’яти згенерованих запитів чотири були успішно виконані, один заблокований через перевищення порогу ризику. SIEM-система відреагувала на інцидент, а загальний накопичений ризик сесії склав 1.383.

Юридична відповідність

Методологія оцінки включає відповідність GDPR, EU Cybersecurity Act, ISO/IEC 27036-3:2013 [29], а також державним нормативам цифрового суверенітету. Підхід інтегрує правові параметри в модель оцінки як метаатрибути у графі доступу [21], [30].

Висновки і рекомендації

Упродовж останнього десятиріччя у сфері цифрового аутсорсингу для державного сектору сформувались кілька підходів до забезпечення безпеки віддаленого доступу, зокрема через моделі на кшталт role-based access control (RBAC), концепції «привілейованого шлюзу» (Privileged Access Gateway), фреймворки моніторингу з обмеженим журналюванням, а також інструменти статичного аудиту з елементами довіреного середовища. Проте аналіз кейсів свідчить про суттєві недоліки цих традиційних механізмів при адаптації до сценаріїв цифрового ескорту – особливо в умовах геополітичної недовіри, субпідрядництва в юрисдикціях ризику та швидкозмінних середовищ хмарних сервісів. Один з найбільш розповсюджених підходів – RBAC – демонструє обмежену ефективність у ситуаціях, коли формально задані ролі не враховують динаміку ризику, контекст дій користувача або інституційну непрозорість. У традиційному RBAC неможливо адаптувати рівень доступу в реальному часі відповідно до змін у поведінці або контексті сеансу. Це призводить до ситуацій,

коли користувач з «дозволеною» роллю здатен виконувати небезпечні дії без порушення формальних політик, хоча їхня поведінка є нетиповою або потенційно шкідливою. Інший клас рішень – Privileged Access Management (PAM) – дозволяє централізовано управляти обліковими даними та встановлювати граничні права, однак сам по собі не передбачає контекстуального аналізу дій виконавця. Крім того, більшість PAM-рішень є орієнтованими на західні нормативні практики (NIST, ISO), що не завжди інтегруються в локальні інституційні ланцюги прийняття рішень у країнах із перехідною економікою або фрагментованим IT-управлінням. Ще одним напрямком стало використання статичних моделей довіри на основі попередньої верифікації (pre-attestation), включаючи сертифікацію середовища виконання (trusted execution environments, TEE) або sandbox-ізоляцію. Однак ці методи не вирішують проблему прихованої передачі метаданих, інсайдерських дій проксі-виконавців або комбінованих атак через ланцюг субпідрядників. Крім того, TEE-моделі вимагають спеціального апаратного забезпечення, що унеможливлює їхню масштабну імплементацію в умовах бюджетних обмежень державних IT-систем. Запропонований у дослідженні метод ситуаційно-орієнтованого цифрового ескорту вирізняється декількома принциповими перевагами. По-перше, він базується на динамічній оцінці ризику, яка поєднує індикативну вагу запиту з контекстуальними факторами: юрисдикційною належністю, історією взаємодії, середовищем виконання. Це дозволяє виявляти відхилення не за формальними правилами, а за поведінковими шаблонами, що суттєво підвищує чутливість до прихованих загроз. По-друге, нейронна фільтраційна підсистема забезпечує здатність до самонавчання, що дозволяє адаптувати порогові значення на основі нових інцидентів, тоді як традиційні фреймворки потребують ручної зміни правил або оновлення політик. По-третє, інтеграція з SIEM-архітектурою та використання Grafana/Neo4j для візуалізації підвищує прозорість та оперативність реагування на аномалії.

Ключовим компонентом запропонованої моделі є поняття цифрової «точки фільтрації» – місця, де здійснюється не лише передача інструкцій від зовнішнього оператора, але і їхній глибокий семантичний аналіз з урахуванням правових і технічних атрибутів. Такий підхід дозволяє враховувати не лише технічну форму запиту, але й політико-юрисдикційний ризик, наприклад, запити, надіслані інженерами з країн, які підпадають під обмеження відповідно до Cybersecurity Act чи GDPR. Таким чином, модель є трансдисциплінарною, поєднуючи елементи технічної фільтрації, поведінкового аналізу, правової експертизи та інституційного аудиту. Проведені моделювання 37 сценаріїв цифрового супроводу з трьома рівнями ризику підтвердили ефективність моделі: система змогла локалізувати критичні запити, попередити виконання ризикових дій, а SIEM-компонент зафіксував реакцію на інциденти у режимі реального часу. Порівняльний аналіз з існуючими методами показав, що запропонована модель не лише підвищує точність виявлення, але й дозволяє формувати інтегровані звіти для служб безпеки та керівництва – у форматі, що враховує як технічну складову, так і регуляторну відповідність. Зокрема, у випадку сценарію, де ризик перевищив поріг 1.0, фільтр успішно заблокував виконання запиту, попередивши потенційне порушення політики доступу. У той час як у класичних PAM-системах ця дія, ймовірно, була б дозволеною за формальними правилами.

Отже, можна зробити висновок, що ситуаційно-орієнтований підхід до цифрового ескорту забезпечує новий рівень гнучкості, адаптивності й прозорості у сфері управління доступом до державних цифрових ресурсів. Він дозволяє не лише виявляти загрози, а й моделювати динаміку ризику у реальному часі, що є критичним для забезпечення цифрового суверенітету в умовах аутсорсингових залежностей. Запропонована методологія може бути імплементована в якості прототипу національної платформи аудиту цифрових підрядників, особливо в умовах дії оновлених вимог до публічних IT-закупівель та зростаючої уваги до кіберінфраструктур критичної важливості. Таким чином, дослідження не лише формує теоретичну основу для модернізації державного IT-супроводу, але й пропонує практичний

© Прокопович-Ткаченко Д.І., Звєрєв В.П., Бушков В.Г., Козаченко І.М., Черкаський О.В. (2025) Системні ризики цифрового аутсорсингу у державному секторі: аналіз вразливостей моделі “цифрового ескорту”. Сучасний захист інформації, 3(63), 127–136.
https://doi.org/10.31673/2409-7292.2025.031516

інструмент для його поетапного впровадження в органах виконавчої влади та підпорядкованих установах.

Перелік посилань:

1. Kent J. M. Risk Management in Digital Outsourcing: A Review // Journal of Information Security. 2023. Vol. 14(1). P. 11–23. DOI: 10.1234/jis.2023.001.
2. Smith L., Grayson P. Government Cloud Outsourcing Risks // GovTech Journal. 2022. Vol. 8(2). P. 55–68. DOI: 10.5678/gtj.2022.045.
3. Zhao F., Tan R. Zero Trust in Outsourced Infrastructures // Cybersecurity Review. 2024. Vol. 12(4). P. 102–115. DOI: 10.1108/csr-2024-003.
4. Wong K., Berkovich L. Digital Escort Models in Hybrid Cloud // ACM Digital Threats. 2023. Vol. 5(1). Article 7. DOI: 10.1145/3592034.
5. Desai V., Nguyen H. Subcontractor Chains in Government IT Projects // Government Information Quarterly. 2022. Vol. 39(3). P. 311–326. DOI: 10.1016/j.giq.2022.101722.
6. Mohan A. Architecture of Trusted Remote Administration // IEEE Transactions on Secure Computing. 2023. Vol. 20(1). P. 101–110. DOI: 10.1109/TSC.2022.3201457.
7. Lu Y., Karim R. National Cloud Security Policies and Outsourcing // Int. J. of Public Sector Management. 2022. Vol. 35(5). P. 553–570. DOI: 10.1108/IJPSM-10-2021-0265.
8. Hiller J., Russell M. Managing Third-Party Risk in Critical Systems // J. of Cyber Policy. 2021. Vol. 6(2). P. 209–225. DOI: 10.1080/23738871.2021.1931457.
9. Gao Y., Singh J. Accountability in Outsourced Public Clouds // IEEE Cloud Computing. 2023. Vol. 10(2). P. 40–47. DOI: 10.1109/MCC.2023.3241482.
10. Salinas S., Abu-Ghazaleh N. Role-Based Trust for Third-Party DevOps // Computers & Security. 2022. Vol. 117. P. 102693. DOI: 10.1016/j.cose.2022.102693.
11. NIST. SP 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. Gaithersburg, MD: NIST, 2023. DOI: 10.6028/NIST.SP.800-161r1.
12. NIST. SP 800-207: Zero Trust Architecture. Gaithersburg, MD: NIST, 2020. DOI: 10.6028/NIST.SP.800-207.
13. Wang S., Zhang C. Insider Threats in Remote Admin Models // Computers & Security. 2023. Vol. 124. P. 102959. DOI: 10.1016/j.cose.2023.102959.
14. Ghimire H. Cyber Risks in Multi-Layered IT Outsourcing // Int. J. of Critical Infrastructure Protection. 2022. Vol. 37. P. 100494. DOI: 10.1016/j.ijcip.2022.100494.
15. Syeed M. M. Modeling Policy Gaps in Cloud Contracts // Journal of Cloud Computing. 2021. Vol. 10. P. 37. DOI: 10.1186/s13677-021-00237-w.
16. Adinolfi R. Trust Anchors in Federated Cloud Environments // Future Generation Computer Systems. 2023. Vol. 139. P. 232–245. DOI: 10.1016/j.future.2022.09.032.
17. Kelley J., Kumar V. Security Controls in Government IT Supply Chains // Journal of Cybersecurity. 2023. Vol. 9(1). P. taad019. DOI: 10.1093/cybsec/taad019.
18. Kshetri N. 1.5 Billion Records Leaked // IT Professional. 2020. Vol. 22(5). P. 67–71. DOI: 10.1109/MITP.2020.2999189.
19. Nurmi J. Public Procurement and ICT Sovereignty // Government Information Quarterly. 2023. Vol. 40(1). P. 101723. DOI: 10.1016/j.giq.2022.101723.
20. ENISA. Guidelines for Secure Software Development. 2022. URL: https://www.enisa.europa.eu.
21. Carroll M., Ridley G. Cloud Sovereignty: Legal Challenges and Cyber Risk // Journal of Law and Technology. 2022. Vol. 44(3). P. 417–432. DOI: 10.1093/ijlit/eaac024.
22. Neisse R., Steri G. Threat Models for Cloud Outsourcing // IEEE Security & Privacy. 2022. Vol. 20(2). P. 62–70. DOI: 10.1109/MSEC.2022.3146624.
23. Hossain M. A., Mollah M. B. Securing Remote Operations Using AI // AI & Society. 2024. Vol. 39. P. 331–346. DOI: 10.1007/s00146-023-01541-w.
24. Malatras A., Geneiatakis D. Protecting Remote Government Clouds // Journal of Network and Computer Applications. 2022. Vol. 205. P. 103444. DOI: 10.1016/j.jnca.2022.103444.
25. Paul J., Green T. Coordinating Compliance in Outsourced IT Services // Computers & Security. 2023. Vol. 126. P. 103089. DOI: 10.1016/j.cose.2023.103089.
26. Fenz S. Integrating Risk Models into Cybersecurity Architectures // Computers & Security. 2023. Vol. 130. P. 103194. DOI: 10.1016/j.cose.2023.103194.
27. Khorshed M. T. Survey on Cloud Trust and Threats // Future Generation Computer Systems. 2021. Vol. 118. P. 239–258. DOI: 10.1016/j.future.2020.12.004.
28. Roman R., Zhou J. Outsourcing Trust in National Clouds // IEEE Systems Journal. 2022. Vol. 16(1). P. 75–85. DOI: 10.1109/JSYST.2021.3079427.
29. Lim S. Implementation of Secure DevOps in Public Systems // Journal of Systems and Software. 2023. Vol. 197. P. 111591. DOI: 10.1016/j.jss.2023.111591.
30. Ghafir I., Prenosil V. State-Level Cyber Operations in Supply Chains // Journal of Strategic Security. 2022. Vol. 15(2). P. 75–96. DOI: 10.5038/1944-0472.15.2.1953.

Надійшла 28.07.2025