УДК 004.056.5

І. О. Храмова
Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

Про деякі ризики безпеки в розподілених інформаційних системах з єдиним інформаційним простором

Розглянуто виклики безпеки, що виникають у територіально розподілених інформаційних комп'ютерних системах (ТРІКС), які функціонують у межах єдиного інформаційного простору (ЄІП). Проаналізовано ризики, пов'язані з появою централізованих точок ураження, семантичною неоднозначністю розподілення елементів управління безпекою, порушенням політик доступу, а також проблеми, пов'язані з виявленням інцидентів та відновленням системи. Окрему увагу приділено аналізу обмежень CAP-теореми в контексті живучості ТРІКС з ЄІП.

Ключові слова: *територіально-розподілена інформаційна комп'ютерна система, єдиний інформаційний простір, безпека, живучість, CAP-теорема, узгодженість, доступність, логічне виведення.*

Вступ

Забезпечення живучості розподілених систем є критичним завданням для комп'ютерної інфраструктури. Єдиний інформаційний простір (ЄІП), як логічно та семантично узгоджене середовище, в якому всі компоненти територіально розподіленої інформаційної комп'ютерної системи (ТРІКС) мають доступ до спільних даних, метаданих, політик і сервісів, повинен забезпечувати цілісність інформаційного обміну, уніфікацію форматів, синхронізацію станів даних і централізоване управління доступом [1]. У контексті живучості ТРІКС саме ЄІП виконує роль, так би мовити, «інформаційного каркасу», що покликаний зберігати функціональність системи навіть за часткових відмов. Проте, деякі особливості подібного архітектурного рішення варто враховувати.

ТРІКС з ЄІП, забезпечуючи логічно узгоджене середовище для обміну даними, створює цим додаткові виклики безпеки. Хоча ЄІП є каркасом, що підтримує функціональність системи, але такі властивості як централізація, семантична неоднозначність і складність синхронізації даних у розподіленому середовищі утворюють ризики, які варті особливої уваги, серед яких:

— централізовані точки ураження (наприклад, реєстри, тимчасові ключі автентифікації, тощо);

— атаки типу впровадження хибних даних у спільний простір, атаки через спільні механізми авторизації, розподілені атаки відмови в доступі;

— семантична неоднозначність і втрата узгодженості політик доступу;

— фрагментарне виявлення інцидентів через асинхронність;

— ризики при відновленні, як то: розбіжності станів, втрата трансакційної цілісності.

ТРІКС з ЄІП, підтримуючи живучість системи, змушена балансувати між узгодженістю, доступністю та стійкістю до розділення мережі. Згідно доведеній CAP-теоремі [2], всі три властивості водночас жодна розподілена система забезпечити не може, а це також створює певні виклики під час вибору тих чи інших заходів підтримки живучого стану системи та її критичних компонентів.

Централізовані точки ураження

У територіально-розподілених інформаційних комп'ютерних системах, що функціонують у межах ЄІП, створюються вузли доступу до даних, які є критичними для сталого функціонування: реєстри, конфігурації, тимчасові ключі автентифікації (токени). Ці, створені ЄІП вузли, відіграють роль спільних точок взаємодії між доменами. За своєю природою, вони є централізованими та високо привілейованими, що робить їх потенційно вразливими до цілеспрямованих атак, які здатні порушити живучість ТРІКС з ЄІП.

Серед найбільш небезпечних типів атак, які можуть бути спрямовані на критичні компоненти ЄІП, слід виокремити наступні.

Впровадження хибних даних у спільний простір (Data poisoning) — атака полягає у внесенні неправдивих, маніпулятивних або шкідливих даних до спільного інформаційного ресурсу, що використовується автоматизованими системами прийняття рішень або для завдань реплікації.

Наприклад, у рамках тестування розподілених систем на основі онтологій, було виявлено, що внесення хибних конфігурацій до спільного реєстру призводило до некоректної маршрутизації запитів і втрати узгодженості між доменами [3].

До можливих наслідків атак цього типу відносяться:

— хибні висновки автоматизованого модуля прийняття рішень;

— порушення логіки узгодженості;

— втрата довіри до істинності джерел;

— каскадне поширення помилкових даних.

Атаки через спільні механізми авторизації (Privilege escalation) — зловмисник використовує спільні механізми автентифікації або авторизації (наприклад, токени, ACL, RBAC), щоб отримати доступ до ресурсів, які йому не належать, або підвищити свої привілеї. Про подібну атаку повідомлялось у [4], де в одному з експериментальних середовищ було продемонстровано, що компрометація токена доступу до модуля логічного виведення (reasoning-модуля) дозволила змінити логіку узгодженості між доменами, що призвело до втрати глобальної узгодженості.

До можливих наслідків такої атаки для ТРІКС з ЄІП відносяться:

— несанкціонований доступ до критичних даних;

— порушення політик довіри;

— імовірність модифікації правил логічного виведення або конфігурацій;

— втрата цілісності ЄІП.

Розподілена атака відмови в обслуговуванні (DDoS) — атака спрямовується на перевантаження компонентів, що обслуговують ЄІП (наприклад, вузлів реплікації, автоматизованих модулів прийняття рішень, модулів інтеграції), з метою зробити їх недоступними для легітимних запитів. Щоб уникнути розподіленої відмови в обслуговуванні, бажано запобігти їй, а після того, якщо вона вже сталася, вжити відповідних заходів для боротьби з нею. Наприклад, у дослідженні [5] було запропоновано подібну модель захисту від DDoS-атак, засновану на семантичному аналізі запитів.

Наслідками розподіленої DDoS- атаки можуть бути:

— втрата доступності критичних для ЄІП сервісів;

— затримка або зупинка реплікації даних;

— неможливість досягнення узгодженості даних;

— активація аварійних режимів зупинки.

Отже, захист централізованих точок доступу до даних, які стосуються організації ЄІП і можуть стати мішенню для атак різного типу, є критичним, оскільки вони мають підвищену ймовірність втрати узгодженості, доступності та довіри до ТРІКС у цілому.

Взаємозалежність політик доступу

Узгодженість політик доступу між доменами у ЄІП є не лише технічною, а й семантичною вимогою. Вона забезпечує стабільність довірчої моделі, що визначає рівень довіри між різними об'єктами (користувачами, системами, процесами) в комп'ютерній мережі або системі, а також надає контрольоване делегування повноважень і захист від ескалації привілеїв.

У публікаціях [6, 7] описано декілька прикладів, де динамічна зміна ролі вузла в розподілених системах призводила до неконтрольованого доступу між доменами та порушення політик узгодженості. Найбільш релевантні приклади стосуються багатодоменних середовищ із рольовою авторизацією (RBAC), де відсутність семантичної синхронізації між доменами створює вразливість до ескалації привілеїв. Розглянемо ці ризики у контексті деградації живучості ТРІКС з ЄІП.

Неузгоджена зміна ролі вузла. Коли вузол змінює свою роль (наприклад, secondary на primary) без узгодження з глобальними політиками доступу чи консенсусними правилами, система втрачає узгодженість у розподілі функцій, що може призвести до каскадних відмов. Очікуваними наслідками, які впливають на живучість системи, в цьому випадку можуть бути:

— порушення кворуму та консенсусу вузлів;

— конфлікти даних і дублювання функцій;

— зниження довіри до системи, оскільки немає гарантії правильного розподілу ролей вузлів.

Втрата узгодженості політик доступу. Коли ACL/RBAC політики на різних вузлах перестають збігатися (наприклад, різні правила для одних і тих самих користувачів), відбувається порушення єдиної моделі довіри в ЄІП, і система стає вразливою до атак і внутрішніх конфліктів. Наслідками в цьому випадку будуть:

— неконтрольований доступ до ресурсів;

— компрометація безпеки та довіри;

— неможливість централізованого управління правами.

Відсутність семантичної синхронізації. Суть полягає в розходженні загальної онтології і семантичних моделей вузлів і втраті єдиної логіки узгодженості даних. Система перестає бути семантично єдиною, що руйнує основу ЄІП як «каркасу узгодженості». Внаслідок цього з'являються:

— різні інтерпретації одних і тих самих даних;

— помилки модулів логічного виведення рішення (reasoning-модулів), що ґрунтуються на неузгоджених онтологіях;

— неможливість коректної реконструкції чи оркестрування.

Усі ці прояви неузгодженості політик доступу та управління ведуть до деградації живучості ТРІКС з ЄІП.

Комбінація моделі семантичної синхронізації політик доступу та універсальної довірчої моделі має базуватисяь на багатодоменній онтології довіри з узгоджувальною логікою винесення рішень про надання доступу. Це дозволяє забезпечити узгодженість, масштабованість і живучість системи навіть при зміні ролей вузлів чи конфлікті політик.

Підкріплена онтологією модель семантичної синхронізації політик доступу реалізується через такі компоненти:

— онтологію політик доступу, що описує ролі, ресурси, правила доступу, контексти і обмеження безпеки;

— семантичні правила, які визначають, коли політики вважаються узгодженими між доменами;

— модуль логічного виведення: використовується для винайдення конфліктів і надання пропозицій синхронізації;

— сценарії синхронізації через автоматичне оновлення ACL/RBAC політик на вузлах при зміні ролей або конфігурацій;

— логування змін політик для аналізу інцидентів.

Вузли ТРІКС періодично обмінюються онтологіями та логічно виведеними висновками для підтримки узгодженості.

Універсальна довірча модель для ТРІКС з ЄІП дозволить:

— визначати рівень довіри до вузла або користувача перед наданням доступу;

— виявляти конфлікти довіри між доменами;

— делегувати права лише в разі семантичної узгодженості.

Модель реалізується через такі компоненти:

1) онтологію довіри (Trust-Ontology): визначає типи довіри (технічну, організаційну, семантичну), рівні довіри, джерела;

2) модель довіри, яка враховує такі фактори як роль вузла, історію взаємодій, тип ресурсу;

3) логічне виведення (reasoning) рішень узгодження між доменами через відповідні модулі з підтвердженням узгодження;

4) механізм делегування, який дозволяє передавати права доступу між доменами лише при семантичній узгодженості;

5) інтеграцію онтології довіри з онтологією політик доступу через спільні класи та властивості.

UML-діаграма взаємодії моделі семантичної синхронізації політик доступу і універсальної довірчої моделі для виявлення конфлікту довіри до користувача та вузла у ТРІКС з ЄІП наведена на Рис. 1.

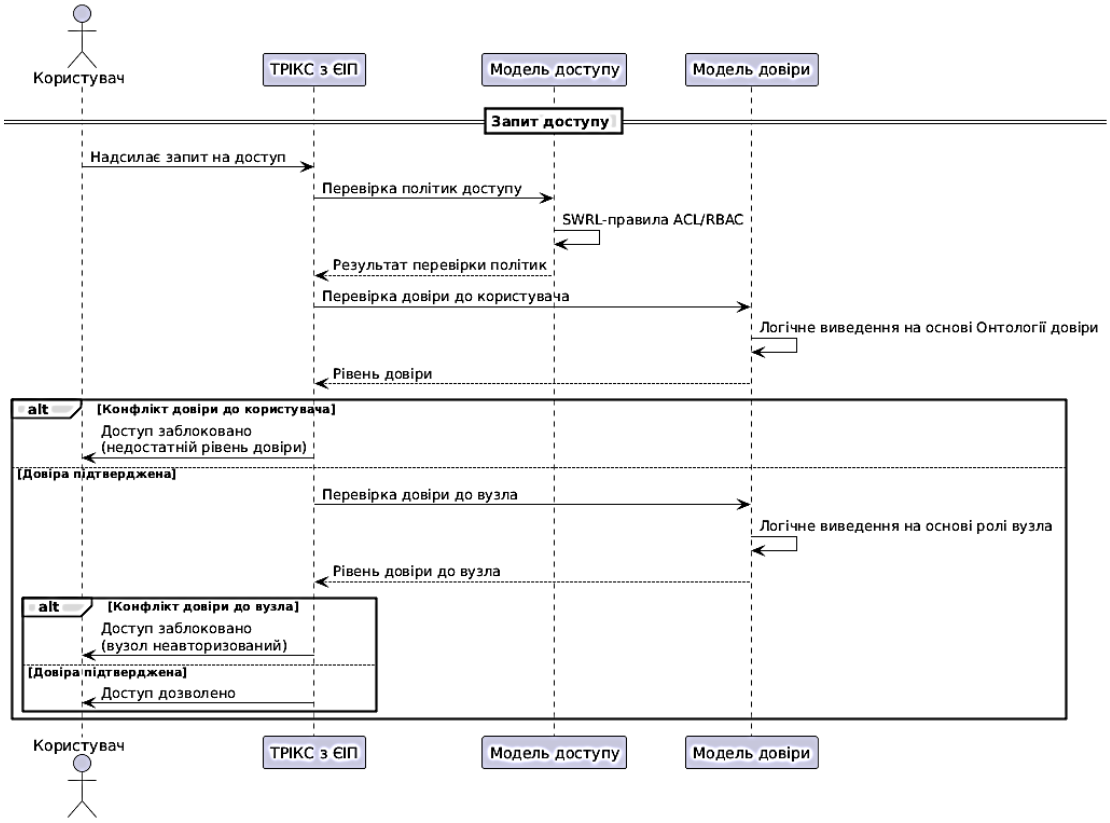

Рис. 1. UML-діаграма взаємодії моделі семантичної синхронізації політик доступу та універсальної довірчої моделі у середовищі ТРІКС з ЄІП

Ускладнення виявлення інцидентів

Через розподілену природу середовища формування ЄІП інциденти безпеки мають тенденцію до фрагментарного прояву, тобто їхні наслідки можуть бути локалізованими, частково прихованими або семантично неузгодженими з глобальним станом системи. Це зумовлено асинхронною природою взаємодії вузлів, автономністю доменів і відсутністю централізованого механізму семантичної кореляції подій.

Зокрема, атака на один вузол — наприклад, шляхом маніпуляції токенами, внесення хибних даних або тимчасового блокування reasoning-модулів може не викликати негайної реакції в інших доменах, але спричинити каскадні ефекти, які проявляться із затримкою або в іншій формі.

Без всебічного моніторингу, що охоплює не лише технічні логи подій (журнали), а й семантичні шаблони модулів логічного виведення, такі інциденти можуть залишатися невиявленими, що створює ризик порушення узгодженості, довіри та живучості системи [8–10].

Уникнути невиявлених інцидентів дозволив би такий підхід, який би поєднав семантично узгоджені записи про події з різних вузлів, що можуть мати різні

формати, із онтологією інцидентів, яка утримує комбінації подій, що можуть свідчити про атаку або порушення, та певною моделлю довіри до вузлів, яка дозволяє ігнорувати хибні сигнали з ненадійних вузлів.

Семантична кореляція подій із використанням онтологій інцидентів і релевантних правил логічного виведення дозволяє виявляти інциденти навіть при фрагментованих або неочевидних сигналах у багатодоменному середовищі ТРІКС з ЄІП.

Як це може виконуватись у ТРІКС з ЄІП:

— події з різних вузлів (логіни, запити, зміни політик) надходять у модуль логічного виведення на основі онтології інцидентів;

— онтологія інцидентів описує, які комбінації подій можуть свідчити про атаку або порушення;

— правила логічного виведення виводять інцидент, навіть якщо окремі події виглядають нейтральними;

— контекстна нормалізація дозволяє порівнювати події з різних доменів — наприклад, однакові запити з різними токенами;

— модуль логічного виведення формує звіт з поясненням, які події, з яких вузлів, у якому контексті призвели до виявлення інциденту;

— політика щодо виявлених інцидентів визначає, що потрібно зробити: блокувати доступ, запускати оркестрацію або делегувати права.

Логіка виведення рішення під час семантичної кореляції подій у ТРІКС з ЄІП наводиться на діаграмі

Рис. 2.

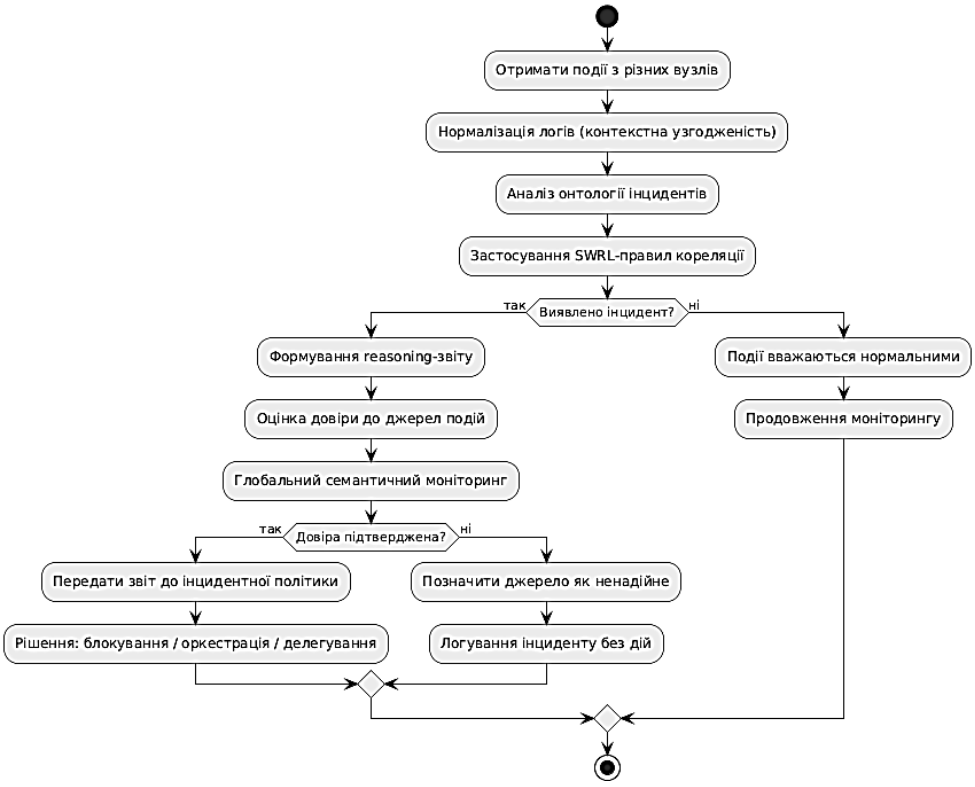

Рис. 2. Логіка виведення рішення під час семантичної кореляції подій

Ризики цілісності при відновленні

У ТРІКС, що функціонують у межах ЄІП, деякі заходи забезпечення живучості, такі як часткова реконфігурація або реструктуризація (наприклад, зміна топології, оновлення ролей вузлів або модифікація логіки узгодженості) потребує узгоджених механізмів реплікації і керування версіями даних. Їхня відсутність створює низку критичних ризиків, які можуть порушити цілісність системи як на технічному, так і на семантичному рівні.

Розбіжності у станах вузлів. Після відновлення даних вузли мають різні стани (наприклад, різні версії бази чи конфігурацій), система перестає бути єдиною, кожен вузол працює за власною логікою, відбувається порушення узгодженості ЄІП. Унаслідок цього у системі відбувається:

— втрата узгодженості між вузлами;

— неможливість коректної реплікації;

— зростання ризику каскадних відмов.

Втрата трансакційної цілісності. У тому випадку, коли транзакції не відновлюються повністю або відновлюються частково. бізнес-логіка та дані більше не гарантують цілісність і система стає непридатною для критичних процесів. Внаслідок чого відбувається:

— порушення ACID-властивостей (атомарність, узгодженість, ізоляція, довговічність);

— втрата даних або дублювання операцій;

— зниження довіри до системи.

Порушення логіки бізнес-процесів. Після відновлення даних бізнес-процеси можуть виконуються некоректно (наприклад, відбувається дублювання транзакцій, пропуск етапів, тощо). Отже, система не може виконувати свої функції відповідно до визначених політик, а це веде до деградації живучості системи і може призвести до:

— зупинки або спотворення ключових процесів;

— втрати узгодженості між підсистемами;

— зниження параметрів продуктивності та надійності.

Відсутність узгодженого механізму версіювання. Якщо немає єдиного механізму контролю версій даних і конфігурацій, система втрачає здатність до відтворюваності та контрольованого відновлення, отже, живучість знижується і виникають:

— конфлікти між різними версіями даних;

— неможливість відновити «правильну» версію;

— зростання ризику компрометації системи.

Випадок виникнення розбіжностей у станах вузлів у розподілених базах даних через відсутність узгодженого механізму версіювання, що призвів до втрати трансакційної цілісності та порушення логіки обробки запитів у фінансовому модулі системи описаний у [11]. У звіті про інциденти в хмарних розподілених системах [12], наведений випадок, коли неконтрольована реплікація спричинила розбіжності між вузлами, що обслуговували різні регіони. Це призвело до помилкових рішень у логіці бізнес-процесів, зокрема в системах управління ланцюгами постачання. Також описано масштабовану реплікацію, яка не забезпечувала узгодже-

ність даних у реальному часі, що стало причиною втрати узгодженості між мікросервісами в системі обробки замовлень [13].

Уникнути розбіжностей станів вузлів, втрати трансакційної цілісності та деградації живучості у ТРІКС ЄІП зможе узгоджене версіювання та реплікації. Такий універсальний механізм має поєднувати кілька частин.

1. Централізоване семантичне версіювання:

1) кожна зміна даних або конфігурацій отримує версію з семантичними мітками;

2) версії зберігаються у центральному реєстрі версій ЄІП, доступному всім вузлам;

3) використання онтології версіювання, яка описує типи змін (дані, політики, бізнес-логіка) та їхня взаємозалежність.

2. Узгоджена реплікація:

1) зміни поширюються між вузлами лише після підтвердження узгодження (алгоритми типу Paxos/Raft);

2) реплікація відбувається у два етапи:

— попередня синхронізація, коли вузли отримують нову версію, але не активують її;

— активація після кворуму: версія стає чинною лише після підтвердження більшістю вузлів.

3. Трансакційна узгодженість:

1) використання логів трансакцій (transaction logs) з атомарними операціями;

2) відновлення після збою відбувається шляхом відтворення трансакцій до останньої узгодженої версії (replay);

3) ACID-властивості гарантуються через двофазне підтвердження (commit) між доменами.

4. Семантична перевірка узгодженості бізнес-процесів:

1) модулі логічного виведення перевіряють, чи нова версія не суперечить онтології бізнес-процесів;

2) якщо виявлено конфлікт (наприклад, дублювання ролей або порушення політик), версія блокується до ручного або автоматизованого повторного узгодження.

Діаграма (Рис. 3) показує логіку процесу прийняття рішення після відновлення критичного вузла ТРІКС з ЄІП від запиту версії і узгодження реплікації до перевірки бізнес-логіки та прийняття рішення (відновлення, відкат до попередньої версії, повторне узгодження; тимчасове перенесення на інший (резервний) вузол).

Це дозволяє уникнути розбіжностей станів вузлів, втрати трансакційної цілісності та деградації живучості системи.

CAP-теорема і аналіз ТРІКС ЄІП у контексті забезпечення живучості

Як вже згадувалося, теорема CAP стверджує, що у розподіленій системі неможливо одночасно гарантувати такі 3 властивості, як:

1) узгодженість (Consistency, C): усі вузли бачать однаковий стан даних;

2) доступність (Availability, A): кожен запит отримує відповідь, навіть якщо деякі вузли недоступні;

— стійкість до розділення (Partition tolerance, P): система продовжує працювати навіть при втраті зв'язку між частинами.

ТРІКС з ЄІП, як територіально-розподілена система, за визначенням завжди має ризик розділення мережі (P), тому критичним під час забезпечення живучості стає вибір між узгодженістю (C) та доступністю (A). ТРІКС з ЄІП завжди змушені жертвувати або узгодженістю, або доступністю.

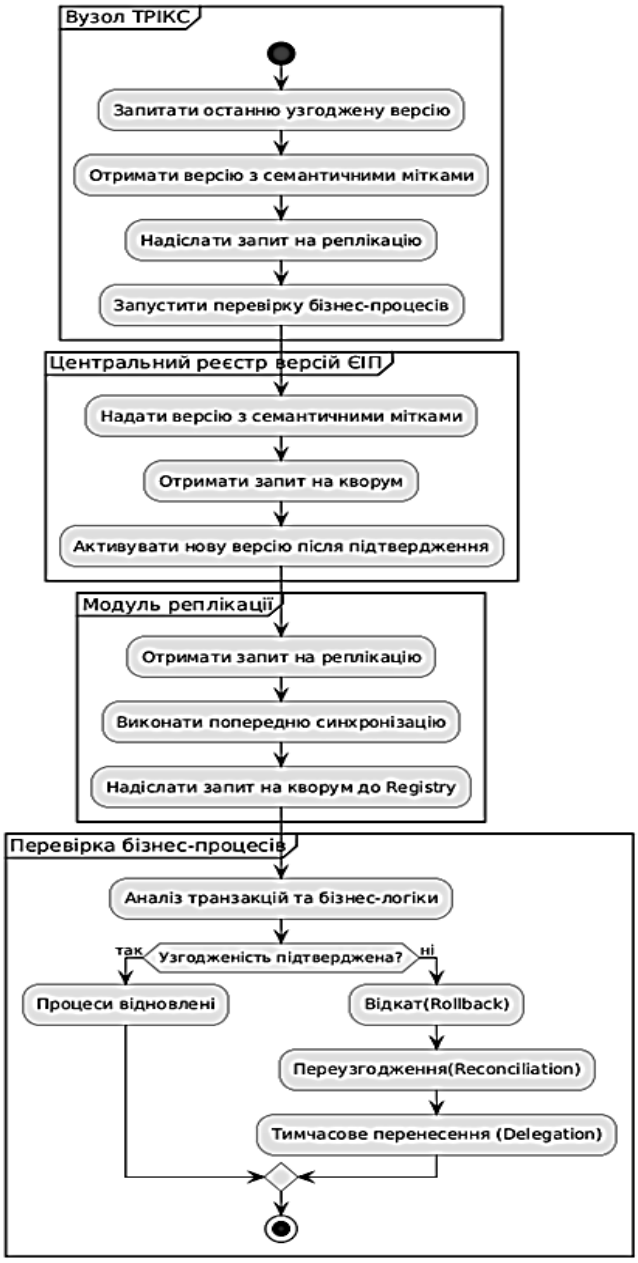

Рис. 3. Відновлення після збою у ТРІКС з ЄІП

Отже, CAP-теорема накладає невідворотні обмеження, і саме вірний вибір між CP- та AP-підходами визначатиме, як саме підтримувати живучість системи [2,

14, 15]. Коли розподілена система має обробляти мережеві розділи, що є неминучим явищем для розподіленої системи, система CP-типу приймає рішення надати пріоритет узгодженості (C) над доступністю (A) даних під час такої події. Це означає, що якщо відбувається мережевий розділ, і частина системи не може зв'язатися з рештою, для гарантії узгодженості даних на всіх вузлах, ця частина системи стане недоступною.

Система або заблокує операції, або відмовиться обробляти запити, або поверне помилку, а не ризикне надати застарілі або неправильні дані. Основний принцип тут полягає в тому, що цілісність і точність даних є надзвичайно важливими.

Системи CP часто використовують алгоритми консенсусу (такі як Paxos або Raft), щоб гарантувати, що всі затверджені записи узгоджені більшістю вузлів перед підтвердженням.

Системи CP є важливими для застосувань, де точність і цілісність даних не можуть бути порушені, навіть тимчасово. Хоча вони жертвують доступністю під час мережевих розділів, вони надають надійні гарантії цілісності даних, які необхідні для критично важливих бізнес-операцій через забезпечення:

— гарантованої узгодженості даних на всіх вузлах;

— відповідності вимогам узгодженості без необхідності обробляти остаточну узгодженість;

— передбачувану поведінку під час невдач;

— повну підтримку принципів атомарності, узгодженості, ізоляції і довговічності ACID,

Вибір AP-стратегії означає, що кожен безвідмовний вузол у розподіленій системі повертає відповідь на кожен запит. Це означає, що система завжди працездатна та реагує на запити клієнтів, навіть якщо деякі частини системи зазнають збоїв. Доступна система не обов'язково гарантує, що відповідь міститиме найактуальніші дані, але вона гарантує, що користувач отримає певну відповідь протягом розумного часу, а не через тайм-аут або повідомлення, яке сповістить про те, що система не працює. Проте, обираючи AP тип системи потрібно погодитися на компроміси:

— дані можуть бути тимчасово неузгодженими між вузлами;

— можуть знадобитися додаткові механізми для обробки конфліктуючих оновлень;

— обмежена підтримка складних об'єднань і транзакцій;

— ускладнене проєктування схем інтеграції даних;

— збільшення кількості вузлів і компонентів для моніторингу.

Аналізуючи вже розглянуті у попередніх розділах ризики деградації живучості у світлі відповідності положенням CAP-теореми можна зауважити наступне.

Розбіжності у станах вузлів підсилюють ризик: порушення умови C, деградація живучості відбувається через втрату вузлами ТРІКС єдиного стану. Трансакційна узгодженість критично важлива для міжвузлових бізнес-процесів. Її втрата веде до компрометації C та A одночасно, що руйнує довіру до системи.

Втрата трансакційної цілісності викликає порушення логіки бізнес-процесів: після відновлення даних процеси виконуються некоректно. Внаслідок цього підсилюються ризики деградації властивостей A (процеси не завершуються) та C (різні вузли бачать різні результати).

Особливістю ЄІП є те, що бізнес-логіка процесів інтегрована у політики доступу та онтології і їх порушення веде до системної нестабільності.

Відсутність узгодженого механізму версіювання веде до ризику порушення принципу C через неможливість відновити «правильну» версію. Особливістю ЄІП є те, що версіювання має бути централізованим і семантично узгодженим, а його відсутність приведе до непередбачуваних каскадних конфліктів.

Живучість ТРІКС ЄІП, або її здатність витримувати порушення та відновлюватися, обмежується CAP-теоремою, оскільки ЄІП вимагає сильної узгодженості для уникнення конфліктів у даних. При територіальному розподілі мережеві розділення посилюють ризики: система повинна обирати між блокуванням операцій (для C) або продовженням роботи з потенційно застарілими даними (для A).

У CP-режимі живучість зростає за рахунок надійності даних, але падає доступність; в AP , навпаки, система залишається живучою, але ЄІП може зазнати фрагментації [16, 17].

Комплексна стратегія вибору заходів протидії загрозам інтеграції даних у багатодоменному середовищі ТРІКС ЄІП

Рішенням порушених у попередніх розділах проблем має стати комплексна стратегія заходів протидії та інтеграція механізмів захисту в багатодоменному середовищі ТРІКС ЄІП.

Комплексна стратегія має охоплювати та поєднувати технічні, семантичні й організаційні заходи на наступних рівнях.

1. Захист даних: перевірка автентичності, семантична перевірка, reasoning-модулі.
2. Захист доступу: короткоживучі токени, синхронізація ACL/RBAC, моніторинг аномалій.
3. Захист від надмірного навантаження: балансування, семантичний аналіз запитів, резервування.
4. Моніторинг та реагування: глобальна кореляція інцидентів, автоматизоване відновлення.

Кожен рівень інтегрується у багатодоменне середовище через:

— єдину онтологію безпеки;
— семантичну синхронізацію політик;
— розподілене версіювання даних;
— модуль кореляції інцидентів;
— адаптивний механізм оркестрації ресурсів;
— багатодоменну довірчу модель.

Комплексна стратегія протидії загрозам у багатодоменному середовищі ТРІКС з ЄІП повинна базуватися на наступних принципах.

1. Семантична узгодженість усіх політик доступу та ролей вузлів.
2. Інтеграція довірчої моделі з механізмами авторизації та оркестрації.
3. CAP-орієнтоване балансування між узгодженістю, доступністю та стійкістю до розділення мережі.
4. Онтологічне моделювання для виявлення прихованих інцидентів і кореляції подій.

5. Автоматизоване логічне виведення на основі правил для прийняття рішень щодо реконфігурації, реструктуризації чи інших типів заходів підтримки живучості системи.

Підсумуємо підходи та механізми, які потрібно задіяти у комплексній стратегії для запобігання викликам безпеки інтеграції даних у ТРІКС ЄІП, згаданим у попередніх розділах:

1) захист від загроз централізованим точкам ураження має відбуватись через:

— використання розподілених реєстрів і багаторівневих механізмів автентифікації для зниження ризику атак типу Data poisoning та Privilege escalation;

— впровадження механізмів семантичної перевірки даних перед їхньою інтеграцією в ЄІП;

— застосування адаптивних анти-DDoS моделей на основі семантичного аналізу запитів;

2) узгодженість політик доступу, що досягається шляхом:

— формування онтології політик доступу, яка описує ролі, ресурси та контексти;

— використання семантичних правил узгодження для автоматичного виявлення конфліктів між доменами;

— інтеграції універсальної довірчої моделі, що враховує технічні, організаційні та семантичні рівні довіри;

3) виявлення прихованих інцидентів, яке можливе якщо:

— буде розроблено онтологію інцидентів, яка описує комбінації подій, що свідчать про атаки;

— впровадити використання модулів логічного виведення для семантичної кореляції подій навіть при їхній фрагментарності;

— виконувати контекстну нормалізацію подій для зіставлення сигналів з різних доменів;

4) забезпечення цілісності при відновленні, що досягається за рахунок:

— використання узгоджених механізмів версіювання даних і конфігурацій;

— забезпечення трансакційної цілісності через контроль ACID-властивостей у багатодоменному середовищі;

— автоматизованого відстеження змін і системних логів для аналізу інцидентів і відновлення довіри;

5) CAP-орієнтоване управління живучістю розподіленої системи у наведеній комплексній стратегії полягає у визначенні пріоритетів між узгодженістю та доступністю, які залежать від критичності сервісів, що надаються під час виникнення ризиків або інцидентів порушення безпеки. Тому необхідно під час автоматизованого прийняття рішень щодо дій з адаптації чи відновлення функціонування системи обирати для використання заходи забезпечення живучості, що узгоджуються з попередньо встановленими обмеженнями CAP-теореми.

Висновки

Особливістю ТРІКС з ЄІП є централізація ряду критичних для підтримки ЄЇП механізмів інтеграції даних і ці централізовані елементи (онтології, політики, модулі логічного виведення) утворюють додаткові ризики безпеки і вимагають семантичної узгодженості і синхронізації механізмів запобігання цим ризикам.

Необхідною умовою для підтримки живучості ТРІКС з ЄІП є міждоменна семантична синхронізація політик доступу, оскільки забезпечує не тільки узгодженість між доменами, а й захист від ескалації привілеїв.

Використання онтологічних моделей і семантичних механізмів логічного виведення на основі правил дозволить виявляти конфлікти політик доступу та підтримувати семантичну узгодженість системи.

Ефективність виявлення інцидентів у багатодоменному середовищі при їхніх фрагментарних або прихованих проявах підвищує семантичний механізм кореляції подій.

Відсутність узгодженого механізму версіювання даних і конфігурацій призводить до втрати трансакційної цілісності, порушення логіки бізнес-процесів і зниження довіри до системи.

Запропонована комплексна стратегія вибору заходів протидії у ТРІКС з ЄІП вирішує більшість з розглянутих проблем безпеки та відрізняється серед існуючих підходів певними інноваційними рішеннями, такими як інтеграція семантичних механізмів логічного виведення з контролем доступу (ACL/RBAC та універсальної довірчої моделі) для ТРІКС, що розширює стандартні моделі (MIRBAC) на ЄІП. Разом із використанням семантичного підходу стандартні моделі забезпечення живучості також посилює адаптація до комплексної стратегії CAP-теореми з пропозицією використання гібридних моделей CP/AP під час вибору заходів реагування.

1. Додонов О. Г., Путятін В. Г. та ін. Технологія забезпечення живучості ТРІКС у ЄІП. *Реєстрація, зберігання і оброб. даних*. 2024. Т. 26, № 1. С. 121-143. DOI: https://doi.org/10.35681/1560-9189.2024.26.1.308659.

2. Eric A. Brewer. 2000. Towards robust distributed systems (abstract). In Proceedings of the nineteenth annual ACM symposium on Principles of distributed computing (PODC '00). Association for Computing Machinery, New York, NY, USA, 7. https://doi.org/10.1145/343477.343502 .

3. Стрижак О. Є. Засоби онтологічної інтеграції і супроводу розподілених просторових та семантичних інформаційних ресурсів // Збірник наукових праць КНУБА. 2022. № 4. С. 12–19. URL: https://repositary.knuba.edu.ua/items/244b973f-bc4c-4885-895d-ff673b135756/full

4. Дивак В. В. Формування єдиного інформаційного середовища навчальних закладів: навч. посіб. Київ: ІІТЗН НАПН України, 2021. 112 с. URL: https://lib.iitta.gov.ua/id/eprint/712061/1/Посібник.pdf.

5. Толюпа С., Котов М. Модель захисту від розподілених атак поступового виснаження ресурсів, заснована на статистичних і семантичних підходах. *Безпека інформаційних систем і технологій*. 2024. Т. 2, № 8. С. 26–33. DOI: https://doi.org/10.17721/ISTS.2024.8.26-33.

6. Cai, Ting, and Jun-Zhan Wang. MIRBAC: A Role-Based Access Control Model for Multi-Domain Interoperability. *International Journal of Security and Its Applications*. 11.6 (2017): 1-17.

7. Zhang, X.;Jing, C.; Chen, Y.-C.; Wang, L.; Xu, L.; Fu, D. Trusted Data Access Control Based on Logistics Business Collaboration Semantics. Appl. Sci. 2024, 14, 4099. https://doi.org/10.3390/app14104099

8. Freitas S., Gharib A. GraphWeaver: Billion-Scale Cybersecurity Incident Correlation // arXiv.org. — 2024. — arXiv:2406.01842v1. — Режим доступу: https://arxiv.org/html/2406.01842v1.

9. Palko, D.; Babenko, T.; Bigdan, A.; Kiktev, N.; Hutsol, T.; Kuboń, M.; Hnatiienko, H.; Tabor, S.; Gorbovy, O.; Borusiewicz, A. Cyber Security Risk Modeling in Distributed Information Systems. *Appl. Sci.* 2023, *13*, 2393. https://doi.org/10.3390/app13042393.

10. Gnatyuk, S., Berdibayev, R., Aleksander, M., Sydorenko, V., Zhyharevych, O., Polozhentsev, A. (2024). Software System for Cybersecurity Events Correlation and Incident Management in Critical Infrastructure. In: Štarchoň, P., Fedushko, S., Gubíniová, K. (eds) Data-Centric Business and Applications.

Lecture Notes on Data Engineering and Communications Technologies, vol 213. Springer, Cham. https://doi.org/10.1007/978-3-031-62213-7_12.

11. Mahmoud H. A., Yasin H. M. Data Integrity and Consistency Challenges in Distributed Database Systems. *Engineering and Technology Journal*. 2023. Vol. 10, No. 5. C. 1–10. URL: https://everant.org/index.php/etj/article/view/1932

12. Riley L. Ensuring Data Integrity in Distributed Systems: Best Practices and Real-World Applications // Enterprise Data Shield. 2024. URL: https://www.enterprisedatashield.com/ensuring-data-integrity-distributed-systems/

13. Chloe M. Scalable Data Replication in Distributed Systems: Ensuring Data Consistency // MomentsLog. 2023. URL: https://www.momentslog.com/development/architecture/scalable-data-replication-in-distributed-systems-ensuring-data-consistency

14. CAP Theorem in System Design. URL: https://www.geeksforgeeks.org/system-design/cap-theorem-in-system-design/

15. CP Systems: Prioritizing Consistency Over Availability During. URL: https://ersantana.com/system-design/cp_systems_design

16. CAP theorem – Availability and Partition Tolerance. URL: https://stackoverflow.com/questions/12346326/cap-theorem-availability-and-partition-tolerance

17. Applying the CAP Theorem in Distributed Systems Design. URL: https://www.gocodeo.com/post/applying-the-cap-theorem-in-distributed-systems-design

Надійшла до редакції 02.02.2026