КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.825
УДК 004.056.5:004.738.5:004.7

Складанний Павло Миколайович
к.т.н., доцент, завідувач кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Гулак Геннадій Миколайович
д.т.н., професор, професор кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-9131-9233
hulak@kubg.edu.ua

Корнієць Віктор Анатолійович
аспірант
Інститут проблем математичних машин і систем НАН України, Київ, Україна
ORCID ID: 0000-0002-4967-8395
viktorkorniets@gmail.com

КОАЛІЦІЙНИЙ ПІДХІД ДО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ІНФОРМАЦІЙНИХ СИСТЕМ ЩО ЗАСТОСОВУЮТЬ ХМАРНІ ТЕХНОЛОГІЇ

Анотація. Забезпечення кібербезпеки в умовах використання хмарних технологій потребує ефективної взаємодії між організаціями, що спільно експлуатують інформаційні системи в об'єднаній інфраструктурі. Особливо це актуально для структур із власною вертикаллю управління та відомчими вимогами до захисту інформації. У таких умовах ключову роль відіграє коаліційний підхід до управління кібербезпекою, який дозволяє узгоджувати дії різних учасників для досягнення спільної мети — захисту інформаційних ресурсів у хмарному середовищі. Дослідження показують, що координація зусиль підвищує ефективність захисту, зменшує ризики витоків та сприяє гарантоздатності систем. Особливе значення цей підхід має для мереж ситуаційних центрів, які діють у сфері національної безпеки. У роботі розглянуто використання рольової моделі доступу (RBAC), метод одноразових логінів і запропоновано організаційно-технічну модель управління доступом у коаліційній системі кібербезпеки на базі хмарних технологій. В роботі використано методи системного аналізу, моделювання архітектури інформаційних систем, формалізації ролей доступу на основі еталонної моделі RBAC (Role-Based Access Control), а також методи коаліційного управління для узгодження політик кібербезпеки між організаціями. Крім того, застосовано підхід до автентифікації з використанням одноразових логінів для підвищення безпеки керування доступом у хмарному середовищі. У результаті дослідження розглянуто проблеми побудови захищеної інформаційно-комунікаційної системи на базі хмарних технологій із використанням сервісів центрів обробки даних. Особливістю такої системи є участь кількох організацій з власними нормативами захисту інформації, що потребує коаліційного підходу до управління кібербезпекою. На основі аналізу визначено сутність цього підходу як узгодженої взаємодії між учасниками для підвищення ефективності захисту даних і якості сервісів. У межах роботи запропоновано модель організаційно-технічного забезпечення гарантоздатності та кібербезпеки, онтологічну модель управління доступом за методологією RBAC, а також метод використання одноразових логінів для автентифікації. Запропоновані рішення спрямовані на зміцнення кіберстійкості систем, що використовують хмарні сервіси. У роботі запропоновані модель організаційно-технічного забезпечення гарантоздатності та кібербезпеки на основі коаліційного підходу до забезпечення захисту, онтологічна модель убезпечення бізнес процесів згідно методології RBAC, а також метод

застосування одноразових логінів в системі управління доступом. Зазначені моделі та метод спрямовані на підвищення рівня безпеки інформаційно-комунікаційних систем що використовують хмарні сервіси. Подальші дослідження планується зосередити на аспектах програмного моделювання запропонованих рішень.

Ключові слова: гарантоздатність; кібербезпека; загроза; захист інформації; мережа зв'язку.

ВСТУП

Діюче законодавство України (https://zakon.rada.gov.ua/laws/show/80/94-вр#Text, 1994) у цілому досить детально регламентує питання взаємодії суб'єктів у сфері захисту інформації, а також визначає їхню відповідальність за виконання завдань з кіберзахисту в межах централізованих інформаційно-комунікаційних систем, що мають одного власника або адміністратора безпеки. Такий підхід є логічним для внутрішньої інфраструктури підприємств, установ чи органів державної влади, де вся відповідальність за побудову, підтримку і захист ІКС зосереджується в рамках єдиного управлінського контуру. Однак з розвитком міжвідомчої цифрової взаємодії, потреби у спільному використанні ІТ-інфраструктури зростають, що породжує ситуації, в яких функціональні компоненти однієї інформаційної системи належать різним незалежним організаціям. Такі системи можна класифікувати як спільні або коаліційні інформаційно-комунікаційні системи (collaborative systems), і вони потребують зовсім іншого підходу до управління безпекою — з урахуванням автономності кожного учасника та необхідності узгоджених дій у сфері кіберзахисту.

Типовим прикладом такої ситуації є мережі ситуаційних центрів, що функціонують у сфері національної безпеки та оборони (Гречанінов, 2021). Вони об'єднують низку техніко-інформаційних комплексів, створених при різних органах державного управління, силових структурах або спеціалізованих установах. Хоча загальне функціонування таких мереж координується головним ситуаційним центром, кожен учасник залишається незалежною організаційною одиницею з власною вертикаллю управління, ІТ-інфраструктурою та нормативними документами щодо захисту інформації, у тому числі технічного та криптографічного. Відтак виникає необхідність побудови єдиної, скоординованої, але гнучкої системи управління кібербезпекою, яка дозволяла б дотримуватися інтересів кожного учасника і водночас забезпечувала захист усієї коаліційної ІКС.

Ще одним важливим аспектом є використання в таких системах центрів обробки даних (ЦОД), що базуються на хмарних технологіях (ХТ) (Гречанінов, Оксанич, & Лопушанський, 2022). Завдяки своїм перевагам — зокрема, оперативному розгортанню сервісів, відсутності необхідності значних капітальних витрат, а також гнучкій масштабованості — ХТ стали домінуючим підходом до організації зберігання та обробки даних у сучасних ІКС. Це особливо зручно для ситуаційних центрів, які працюють із великими обсягами оперативної інформації та повинні швидко адаптувати обчислювальні потужності до поточних задач.

Водночас, застосування хмарних рішень в умовах багатовідомчої взаємодії створює нові виклики для кібербезпеки. Головним «вузьким місцем» є організація захисту інформації, що зберігається й обробляється у спільному хмарному середовищі, доступ до якого мають користувачі з різних організацій. Навіть за умов дотримання базових принципів безпеки з боку хмарного провайдера, зберігається високий ризик витоку інформації, компрометації доступу або ненавмисного порушення цілісності даних. Постає

питання: як забезпечити узгоджену політику доступу до даних і сервісів у середовищі, де кожен суб'єкт має власну систему ролей, відповідальності та повноважень.

У цьому контексті коаліційний підхід до управління кібербезпекою виступає як концептуальна основа побудови ефективної системи захисту. Його суть полягає у формуванні спільної політики безпеки, яка враховує різнорівневу відповідальність учасників, але водночас забезпечує уніфіковані правила доступу, управління інцидентами, реагування на загрози та гарантування цілісності спільної IT-інфраструктури. Застосування моделей управління доступом, таких як RBAC (Role-Based Access Control), дозволяє структурувати повноваження користувачів, визначити політики доступу відповідно до функціональних ролей і централізовано або децентралізовано керувати ними з урахуванням специфіки кожного учасника.

Таким чином, запровадження коаліційного підходу в умовах хмарних технологій є не лише актуальним, а й критично необхідним кроком до побудови стійких, масштабованих та безпечних інформаційно-комунікаційних систем у міжвідомчих і багаторівневих структурах.

Метою статті є системний аналіз визначених проблемних аспектів застосування моделі RBAC для управління гарантоздатністю та кібербезпекою інформаційних систем що застосовують хмарні технології та формування пропозицій щодо її покращення.

Огляд літератури. Системне дослідження що виконане в (Смірнова, 2024) дає актуальний всебічний огляд сучасних публікацій, які присвячені організаційно-технічним аспектам забезпечення кібербезпеки хмарних технологій, та акцентує увагу на реалізації заходів з безпеки трьох моделей хмарних сервісів: інфраструктура як послуга (IaaS), платформа як послуга (PaaS) та програмне забезпечення як послуга (SaaS) в яких фігурують тільки два основних гравці: хмарний провайдер та абонент хмарних послуг.

Зокрема, у дослідженні з урахуванням різних характеристик платформ IaaS, PaaS і SaaS надані рекомендації щодо проектування контролю доступу та узагальнені правила політики безпеки для кожної хмарної системи. При цьому рольова модель RBAC та аспекти її застосування не розглядаються.

В (Gouglidis, & Mavridis, 2012) для управління доступом в сучасних системах спільної роботи (collaborative systems) сотень акторів (дієвих осіб, користувачів) деякої віртуальної організації вперше запропонована модель domRBAC — модифікована версія RBAC. В дослідженні показано, що для успішної співпраці необхідно виконати перелік життєво важливих вимог, а саме: співпраця між доменами, щоб забезпечити безпечне середовище під час співпраці, можливість накладати обмеження на використання ресурсів і керувати політиками безпеки простим і ефективним способом. Питання початкового налаштування моделі з урахуванням бізнес процесів віртуальної організації в роботі не розглядаються.

В (Esna-Ashari et al., 2011) проаналізовано статичне та динамічне розділення специфікацій обмежень обов'язків у моделі RBAC та визначено їхню вразливість. Також запропоновані необхідні покращення для забезпечення їхньої безпеки для врахування в новій версії стандарту. Аспекти налаштування моделі з урахуванням бізнес процесів організації в роботі також не розглядаються.

МЕТОДИ ДОСЛІДЖЕННЯ

В роботі використано методи системного аналізу, моделювання архітектури інформаційних систем, формалізації ролей доступу на основі еталонної моделі RBAC (Role-Based Access Control), а також методи коаліційного управління для узгодження

політик кібербезпеки між організаціями. Крім того, застосовано підхід до автентифікації з використанням одноразових логінів для підвищення безпеки керування доступом у хмарному середовищі.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Ефективну методологію управління доступом до ресурсів інформаційних систем запропоновано у стандарті ANSI INCITS 359-2012 що визначає моделі та методи, які побудовані на основі ролей користувачів (Role Based Access Control, RBAC) (https://csrc.nist.gov/projects/role-based-access-control/rbac-library). Стандарт описує еталонну модель RBAC (рис. 1) та її системні й адміністративні функціональні специфікації.

Згадана модель включає наступні основні елементи, які разом утворюють основу для керування доступом.

Користувачі (Users), що можуть бути фізичними особами або системами, яким надається доступ до ресурсів інформаційно-комунікаційної системи. Кожен користувач може бути пов’язаний з однією або декількома сутностями — ролями, що визначають права його доступу.

*Ролі (*Roles), кожна з яких асоційована з певним набором прав доступу користувачів, яким визначено таку роль. Вихідними даними для формування ролей є завдання або частина роботи (Assignment) організації, що доручена користувачу у рамках виконання схвалених його функціональних обов’язків.

Дозволи (Permissions), які є схваленими потребами виконання конкретних дій з ресурсом, наприклад, читання, запис або видалення даних.

Сесії (Sessions), кожна з яких є конкретним процесом взаємодії користувача з інформаційно-комунікаційною системою, під час якого користувач може активувати одну або кілька ролей для виконання завдань.

Ієрархії ролей (Role Hierarchies): структура, що встановлює відношення типу «батько-дочка», коли ролі вищого рівня успадковують дозволи від ролей нижчого рівня. Ця структура допомагає спростити керування, дозволяючи організовувати ролі у відносинах.

Зв’язування ролей та користувачів — це механізм, який дозволяє призначати користувачам ролі, які можуть бути постійними або тимчасовими.

Зв’язування дозволів та ролей — це визначає, які дозволи пов’язані з кожною роллю. Це дозволяє керувати доступом на основі ролей, а не окремих користувачів.

Зазначені елементи разом забезпечують гнучку та ефективну модель управління доступом, дозволяючи організаціям контролювати, хто має доступ до яких ресурсів та дій у системі.

Системна і адміністративна функціональні специфікації RBAC визначають функції, що поділяються на три категорії: адміністративні операції, які надають можливість створювати, видаляти та підтримувати елементи та зв’язки моделі, адміністративні перевірки, які надають можливість виконувати операції запитів до елементів і зв’язків RBAC, і, нарешті, функціонал системного рівня, якій визначає функції для створення сеансів користувачів, включаючи активацію/дезактивацію ролей, виконання обмежень на активацію ролі та формування рішення про доступ.

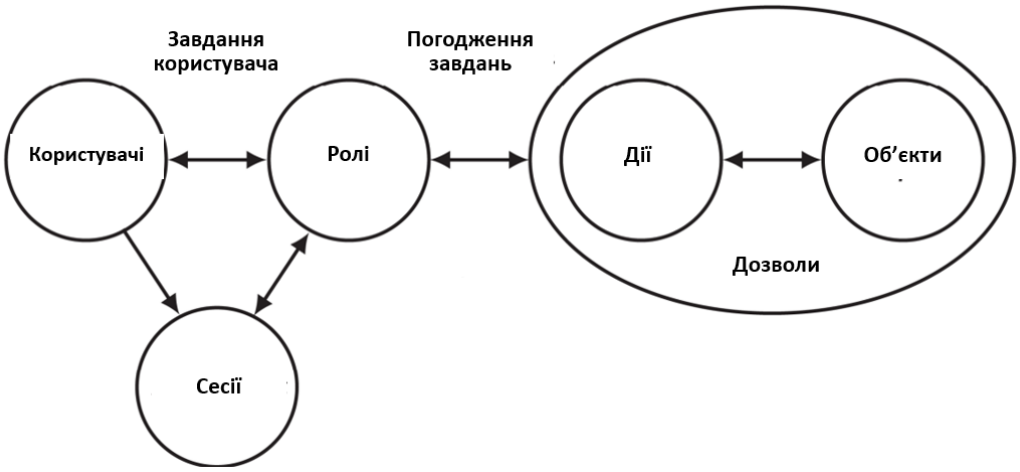

Рис. 1. Модель Role Based Access Control [4]

Модель RBAC підвищує ефективність керування дозволами користувачів у великих системах і гарантує, що адміністратори безпеки можуть застосовувати принципи безпеки найменших привілеїв і поділу обов'язків/привілеїв [6], оскільки вони мають чітке уявлення про рівень доступу, який має даний користувач відповідно до ролей, які йому призначені.

Модель RBAC також спрощує вирішення проблеми визначення користувачам правильних прав доступу до системи.

Оскільки користувачам призначаються ролі (рис. 1), яким відповідають певні множини дозволів (Permissions), які, у свою чергу, корелюються з деякими сукупностями операцій в інформаційно-комунікаційній системі, адміністратору потрібно лише перевірити, чи призначено користувачам правильні ролі, щоб переконатися, що вони мають правильні права доступу (припускаючи, що ролі та дозволи створено правильно). Подібним чином зміна рівня доступу, наданого ролі відповідно до змін в організаційній політиці або структурі, в RBAC є тривіальною, оскільки потрібно буде змінити лише призначення дозволу ролі, щоб вплинути на права доступу кожного користувача, якому призначено роль.

Водночас, до недоліків зазначеної моделі можливо віднести наступне. Початкове налаштування моделі може бути складним та трудомістким, оскільки вимагає глибокого розуміння організаційних ролей та пов'язаних з ними дозволів.

В разі великої кількості користувачів управління ролями може бути складним, особливо коли ролі перетинаються або коли для виконання різних функцій потрібно багато конкретних ролей.

Створення занадто великої кількості різних ролей може призвести до плутанини та труднощів в ефективному управлінні дозволами. Неякісне опрацювання переліку завдань що відповідають певним ролям може призвести до надмірного надання дозволів користувачам, що може мати наслідком неприпустиме підвищення рівня ризиків для кібербезпеки. Підсумовуючи викладене, слід зробити висновок що хоча модель RBAC пропонує значні переваги з точки зору ефективності управління, вона може створювати певні проблеми. Розв'язанню відповідних проблем саме присвячене поточне дослідження.

Виходячи з наведеного неформального означення об'єкту захисту як інформаційно-комунікаційної системи (надалі – мережа), функціональні елементи якої, належать декільком незалежним організаціям, та яка користується хмарними сервісами, можливо уточнити склад коаліції суб'єктів інформаційних відносин.

Під коаліцією тут розуміється об’єднання деякої кількості організацій, які для спільного вирішення певних завдань, зокрема, формування управлінських рішень формують та використовують спеціальний інформаційний ресурс, щодо якого висуваються підвищені вимоги в частині забезпечення його конфіденційності, цілісності та доступності протягом заздалегідь визначеного часу.

Зазначений термін обраний на основі його сутності, а саме: на відміну від деяких інших типів об’єднань, кожен із учасників коаліції зберігає самостійність у питаннях, що не пов’язані із метою коаліції. В нашому випадку метою існування коаліції є виконання визначених завдань шляхом задоволення спеціальних інформаційних потреб.

Коаліція включає декілька її учасників, що найменш один з яких, вочевидь, повинен виконувати цільову функцію координації спільних інформаційних дій всіх учасників (Гречанінов, 2021), включаючи заходи зі забезпечення належної якості створюваних та збережених ресурсів. Зокрема, учасник коаліції що виконує функцію координації щодо систем, у яких обробляються державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом, має сприяти виконанню завдань, які визначені в (Esna-Ashari et al., 2011).

Неодмінним учасником коаліції має бути провайдер хмарних сервісів, якщо з його допомогою створюється сховище спеціальної інформації, оскільки цей елемент системи також повинен відповідати загальній політиці безпеки.

Таким чином, коаліційний підхід до забезпечення гарантоздатності інформаційно-комунікаційної системи (якості її сервісів) та її кібербезпеки повинен передбачати максимальну співпрацю між різними зацікавленими сторонами — учасниками коаліції, включаючи державні установи, компанії приватного сектору, некомерційні організації та інші відповідні суб’єкти. Цей підхід повинен ґрунтуватися на розумінні того, що жодна окрема організація не може виключно власними силами ефективно вирішувати складні проблеми забезпечення кібербезпеки та реагувати на її виклики.

Загалом, коаліційний підхід має підвищувати ефективність зусиль із забезпечення якості сервісів та кібербезпеки шляхом використання сильних сторін і можливостей різних зацікавлених сторін, які працюють над досягненням спільних цілей. Ключовими аспектами коаліційного підходу мають бути наступні.

1. Спільна відповідальність, яка означає, що кожен учасник коаліції визнає власну роль у створенні безпечнішого та надійнішого комунікаційного середовища та зобов’язується неухильно вживати конкретних організаційно-технічних заходів щодо забезпечення якості сервісів та кібербезпеки.
2. Обмін інформацією за участю координатора між учасниками коаліції допомагає покращити ситуаційну обізнаність і дозволяє швидше реагувати на нові загрози, усувати уразливості, впроваджувати кращі практики та технологічні досягнення.
3. Розробка єдиних або узгоджених часткових політик безпеки учасників коаліції сприяє усуненню або компенсації невідповідності галузевих профілів безпеки (базових профілів безпеки) (https://zakon.rada.gov.ua/laws/show/80/94-вр#Text, 1994).
4. Стандартизація процедур, протоколів для покращення сервісів та кібербезпеки всіх учасників допомагає забезпечити взаємодію та узгодженість між різними системами та платформами.
5. Раціональний розподіл ресурсів для реалізації більших проектів або ініціатив, які можуть виходити за межі можливостей окремих організацій,

може підвищувати ефективність рішень та інновацій, призводити до синергетичного ефекту.

6. Спільні тренінги та навчання учасників коаліції сприятимуть вдосконаленню навичок і знань персоналу, залученого реалізації сервісів та забезпечення кібербезпеки.
7. Узгоджені дії в рамках реагування на інциденти кібербезпеки або порушення якості сервісів сприятимуть зменшенню потенційних збитків, підвищенню оперативності ліквідації наслідків реалізації загроз, раціональному управлінню ресурсами та комунікаціями.

З урахуванням наведеного модель опрацювання безпекових завдань між учасниками коаліції (на рівні організацій) може мати наступний вигляд (табл. 1).

Таблиця 1

Учасники коаліційного захисту мережі створюють та реалізують

<table>
<tr><th>Провайдер хмарних сервісів</th><th>Користувач-координатор</th><th>Звичайний користувач</th></tr>
<tr><td colspan="2">Політика ідентифікації та автентифікації 1</td><td>Політика ідентифікації та автентифікації 2</td></tr>
<tr><td>Політика розмежування доступу 1</td><td colspan="2">Політика розмежування доступу 2</td></tr>
<tr><td colspan="2">Політика управління ключами шифрування 1</td><td>Єдина політика управління ключами шифрування 2</td></tr>
<tr><td colspan="2">Політика використання засобів шифрування 1</td><td>Єдина політика використання засобів шифрування 2</td></tr>
<tr><td colspan="3">Єдина політика антивірусного захисту</td></tr>
<tr><td>Узгоджена (в частині сервісів для коаліції) політика реєстрації подій</td><td colspan="2">Єдина політика реєстрації подій</td></tr>
<tr><td>Узгоджена (в частині сервісів для коаліції) політика відновлення</td><td colspan="2">Узгоджена політика відновлення та реагування на інциденти кібербезпеки або порушення якості сервісів</td></tr>
<tr><td rowspan="2">Політика безпеки серверів 1</td><td colspan="2">Узгоджена політика безпеки серверів 2</td></tr>
<tr><td colspan="2">Узгоджена політика безпека кінцевих точок</td></tr>
<tr><td>Політика</td><td>Політика DLP 2</td><td>Політика DLP 3</td></tr>
<tr><td colspan="3">Узгоджена політика застосування SIEM та комунікацій з питань безпеки</td></tr>
<tr><td>Політика захисту від</td><td colspan="2">Політика захисту від DDoS 2</td></tr>
</table>

З наведеної таблиці можливо з’ясувати, що в запропонованій моделі коаліційної безпеки роль користувач — координатор (КК) додатково до інших функцій реалізує завдання «екранування» мережі, оскільки використовується:

- окремі процедури «зовнішньої» ідентифікації/автентифікації з провайдером хмарних сервісів (ПХС) та «внутрішньої» ідентифікації/автентифікації з іншими користувачами (ІК);
- передача даних через незахищене середовище здійснюється з використанням процедур шифрування різних для ділянок ПХС — КК та КК — ІК, що регулюються відповідними частковими політиками управління ключами шифрування та політикою використання засобів криптографічного захисту інформації (https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf, 2015).

З метою дотримання вимог гарантоздатності та кібербезпеки до провайдера хмарних сервісів висуваються вимоги узгодження (в частині сервісів для коаліції) політики реєстрації подій в системі та політики відновлення попереднього стану після реалізації кіберінцидентів. Аналогічна за суттю вимога висувається щодо політики застосування SIEM та обміну інформацією про загрози.

Інші особливості запропонованої моделі розподілу безпекових завдань є логічною відповіддю на визначені вище концептуальні характеристики коаліційного підходу до забезпечення безпеки. Зважаючи на те, що учасниками визначеної мережі є організації (підприємства), а фактичними користувачами мережі є їх персонал, уявляється доцільним з'ясувати особливості реалізації механізму управління доступом до її інформаційних ресурсів.

Модель управління доступом на основі методології RBAC. Однією з проблемних складових практичного впровадження методології RBAC (Role-Based Access Control) у хмаро орієнтованих коаліційних інформаційних системах є визначення початкового набору завдань, дій та дозволів користувачів, а також раціональне формування ролей в умовах великої кількості суб'єктів доступу. Особливо це ускладнюється в багатовідомчих системах, де кожна організація-учасник має власну структуру бізнес-процесів, політику безпеки та рівень IT-зрілості. У такому середовищі ефективне управління доступом неможливе без уніфікації підходів до аналізу, класифікації та моделювання діяльності учасників спільної інформаційної системи.

З метою адаптації RBAC до умов коаліційного функціонування пропонується формувати систему дозволів та ролей на основі структурного опису бізнес-процесів, які реалізуються учасниками ІКС. У даному контексті користувачі об'єднуються в межах системи як суб'єкти певного підприємства чи мережі, що прагне досягти спільної мети — наприклад, забезпечення національної безпеки, інформаційної стійкості чи моніторингу критичних подій. Для цього визначаються упорядковані сукупності взаємозалежних завдань — бізнес-процеси, які класифікуються за чотирма основними типами: операційні, допоміжні, управлінські та стратегічні (Weske, 2024).

Ключові бізнес-процеси є основою для визначення критичних завдань і мають прямий вплив на досягнення цілей та ефективне функціонування коаліційної інформаційної системи. Вони ідентифікуються шляхом оцінки впливу на успіх та стійкість ІКС в умовах динамічного середовища, що характерне для хмарних технологій (Borek et al., 2014, Stoiljković Ranđelović et al, 2018).

Методологія виявлення бізнес-процесів для побудови коаліційної моделі доступу в RBAC включає кілька етапів, тісно пов'язаних із формуванням онтологічної моделі убезпечення бізнес-процесів (рис. 2). По-перше, слід чітко визначити стратегічні та операційні цілі, яких прагнуть досягти учасники ІКС. По-друге, потрібно зібрати та систематизувати інформацію про існуючі процеси — це досягається через анкетування, інтерв'ю, спостереження, аналіз документації, нормативів та внутрішніх регламентів.

Наступним етапом є моделювання виявлених процесів із використанням візуальних нотацій, таких як BPMN (Business Process Model and Notation) або IDEF0, що дозволяє відобразити взаємозв'язки між діями, ресурсами та виконавцями. На основі створених моделей проводиться аналіз потреб в інформаційному забезпеченні, визначаються критичні точки доступу до інформаційних об'єктів та узгоджуються дії, які потребують дозволів з боку системи управління доступом.

Результатом аналізу є формування таблиці ролей і відповідних дозволів, яка у подальшому використовується для призначення користувачів до ролей відповідно до їх функціональних обов'язків. Ефективним інструментом є використання матриці потреб у ресурсах, що структурно подібна до матриці RACI (Responsible, Accountable, Consulted, Informed) (Matthews, 2024), де кожна дія (операція) у бізнес-процесі співвідноситься з виконавцями, рівнем їх відповідальності та ступенем доступу до інформаційних ресурсів.

У контексті коаліційного підходу, така модель дозволяє:

- забезпечити прозоре розмежування повноважень між представниками різних організацій;
- впровадити гнучку, але контрольовану політику доступу;
- адаптувати рольову модель до змін у структурі спільної ІКС без необхідності повної ревізії політики безпеки;
- мінімізувати ризики надмірного надання дозволів і порушення принципу мінімальних привілеїв, що критично важливо у хмарному середовищі з динамічним масштабуванням ресурсів.

Таким чином, використання методології RBAC у поєднанні з формалізованим описом бізнес-процесів та матричним поданням повноважень є одним із базових інструментів реалізації ефективного управління доступом у коаліційних інформаційних системах, що застосовують хмарні технології. Такий підхід дозволяє забезпечити узгодженість політик доступу між незалежними організаційними структурами. Він підвищує рівень контрольованості дій користувачів у спільному хмарному середовищі та знижує ймовірність несанкціонованого доступу (Virginia et al., 2011, Saltzer et al., 1975). Можливість гнучкого призначення ролей відповідно до актуальних бізнес-процесів сприяє оперативному реагуванню на зміни в структурі ІКС. У результаті досягається баланс між безпекою, функціональністю та масштабованістю коаліційної системи.

Зокрема, якщо для реалізації цілей створення мережі потрібно реалізувати множину операційних дій $\mathcal{D} = \{d_1, d_2, \dots, d_n\}$, для виконання яких потрібен доступ до інформаційних активів $\mathcal{A} = \{a_1, a_2, \dots, a_m\}$, тоді матрицю розміру $m \cdot n$

$$X = \|x_{ij}\|_{m \cdot n} \quad (1)$$

будемо називати матрицею початкових потреб для бізнес проєкту, якщо $x_{ij} = 0$ коли актив a_i не використовується для виконання операції d_j та $x_{ij} = 1$ в іншому випадку.

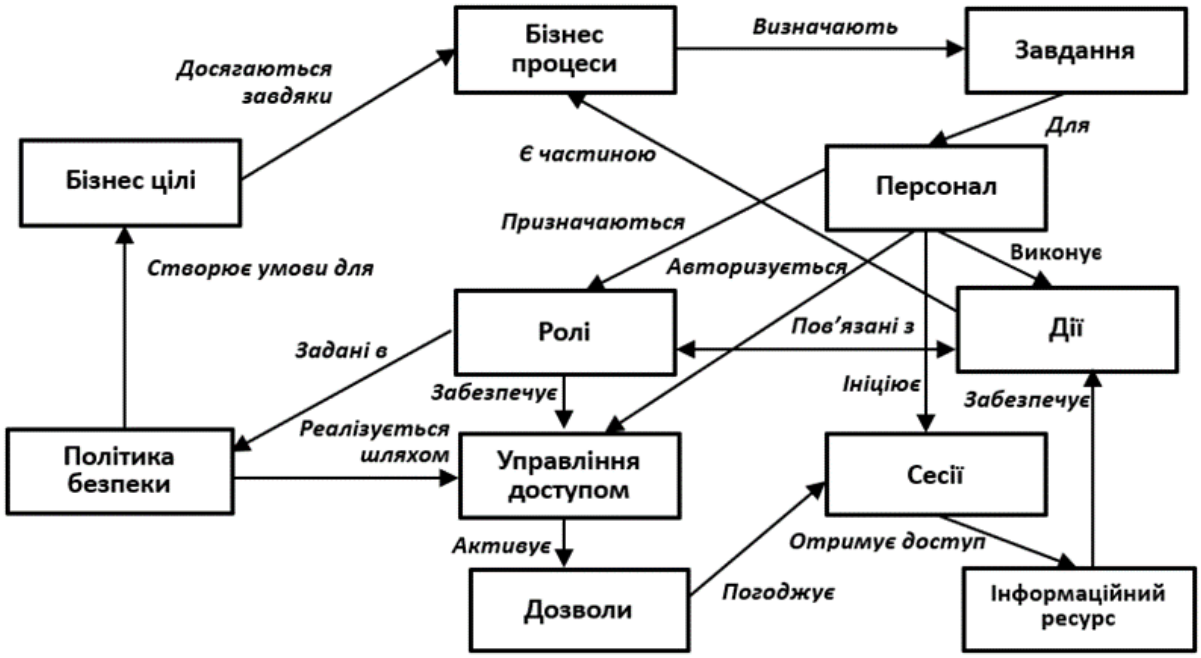

Рис. 2. Онтологічна модель убезпечення бізнес процесів згідно методології RBAC

Наступним кроком в рамках реалізації моделі RBAC на основі матриці початкових потреб $\boldsymbol{X}$ та пропозицій учасників коаліції щодо необхідної кількості спеціалізацій виконавців має бути сформований перелік ролів користувачів інформаційних активів:

$$\widetilde{\boldsymbol{\mathcal{R}}} = \{\boldsymbol{R_1}, \boldsymbol{R_2}, \dots, \boldsymbol{R_k}, \dots, \boldsymbol{R_S}\}, \quad (2)$$

де $\boldsymbol{R_k} = < \widehat{\boldsymbol{\mathcal{D}}}_{\boldsymbol{k}}, \widehat{\boldsymbol{\mathcal{A}}}_{\boldsymbol{k}} >, \widehat{\boldsymbol{\mathcal{D}}}_{\boldsymbol{k}} = \{\boldsymbol{d_{j1}}, \boldsymbol{d_{j2}}, \dots, \boldsymbol{d_{jp}}\}, \widehat{\boldsymbol{\mathcal{A}}}_{\boldsymbol{k}} = \{\boldsymbol{a_{i1}} \boldsymbol{a_{i2}}, \dots, \boldsymbol{a_{iq}}\}\ \boldsymbol{k} = \overline{\boldsymbol{1,S}}$, $\boldsymbol{p > 1}$, $\boldsymbol{q > 1}$ — кортеж, що характеризує певну роль, $\boldsymbol{2 \leq S}$ — кількість різних ролів.

При цьому дія $\boldsymbol{d_j} \in$ вважається припустимою для ролі $\boldsymbol{R_k}$, а доступ до певного активу погодженим, якщо $\boldsymbol{d_j} \in \widehat{\boldsymbol{\mathcal{D}}}_{\boldsymbol{k}}$ та існує $\boldsymbol{a_i} \in \widehat{\boldsymbol{\mathcal{A}}}_{\boldsymbol{k}}$ такий, що $\boldsymbol{x_{ij} = 1}$.

В процесі визначення переліку ролей (2) необхідно раціонально розв'язати протиріччя між реалізацією функціонального призначення мережі та забезпеченням її безпеки, оскільки, з одного боку, розширення доступу до інформаційних активів сприяє підвищенню ефективності бізнес процесів, з іншого може призвести до підвищення ризику реалізації загроз їхньої безпеці.

Зазначимо, що виходячи з принципу мінімізації привілеїв та повноважень кількість погоджених припустимих дій $\boldsymbol{d_j} \in \widehat{\boldsymbol{\mathcal{D}}}_{\boldsymbol{k}}$ в кожній ролі $\boldsymbol{R_k}$ можна оцінити за допомогою критерію, що будується на основі відомої задача про укладання рюкзака (Корбут, & Фінкельштейн, 1969). Потреба розв'язку задачі про рюкзак виникає у процесі прийняття рішень багатьох сферах, наприклад, таких як пошук раціонального способу подрібнення с

и У випадку пропонованої процедури раціонального визначення ролі $\boldsymbol{R_k}$ формальний р пис критерію її формування в термінах задачі про укладання рюкзака [16] буде мати н наступний вигляд.

в Будемо вважати, кожна дія з множини операційних дій $\boldsymbol{d_j} \in \boldsymbol{\mathcal{D}} = \{\boldsymbol{d_1}, \boldsymbol{d_2}, \dots, \boldsymbol{d_n}\}$ має Н евну цінність $\boldsymbol{c_j} \in [\boldsymbol{0}, \boldsymbol{1}]$ для реалізації ключових бізнес процесів. Також будемо в важати, що доступ до активу $\boldsymbol{a_i} \in \boldsymbol{\mathcal{A}}$ може мати наслідком реалізацію загрози для И конфіденційності, цілісності та/або доступності цього активу з ваговим параметром $\boldsymbol{w_i}$. Параметри $\boldsymbol{c_j}$ та $\boldsymbol{w_i}$ визначаються експертним шляхом (Гнатієнко, 2008).

(Кожна координата $\boldsymbol{x_{ij}}$ вектору-рядку $\overline{\boldsymbol{X}}_{\boldsymbol{i}} = (\boldsymbol{x_{i1}}, \boldsymbol{x_{i2}}, \dots, \boldsymbol{x_{in}})$ матриці $\boldsymbol{X}$ (1) пов'язує Н конкретну дію $\boldsymbol{d_j} \in \boldsymbol{\mathcal{D}}$ з інформаційним активом $\boldsymbol{a_i} \in \boldsymbol{\mathcal{A}}$. Вектор $\overline{\boldsymbol{X}}_{\boldsymbol{i}}$ будемо вважати а придатним для застосування в якості умовного центроїду для формування множини з припустимих дій для певної ролі $\boldsymbol{R_k}$ якщо він максимізує значення виразу:
et al., 2004).

$$\boldsymbol{C} = \sum_{\boldsymbol{j=1}}^{\boldsymbol{n}} \mathrm{c}_{\boldsymbol{j}} \cdot \boldsymbol{x_{ij}} \text{ за умов } \sum_{\boldsymbol{j=1}}^{\boldsymbol{n}} \boldsymbol{w_i} \cdot \boldsymbol{z_{ij}} \leq \boldsymbol{R} \quad (3)$$

де $\boldsymbol{R}$ заздалегідь встановлений граничний рівень ризику настання кіберінциденту у разі погодження деякої дії з певним інформаційним активом.

Якщо вектор $\overline{\boldsymbol{X}}^*$ придатний для застосування у якості умовного центроїду, а $\boldsymbol{\delta}$ — граничне значення відстані $\boldsymbol{\Delta}$ по Ґемінгу для двійкових векторів, при цьому

$$\boldsymbol{\Delta}(\overline{\boldsymbol{X}}^*, \overline{\boldsymbol{X}}_{\boldsymbol{i}}) \leq \boldsymbol{\delta}, \boldsymbol{i} = \boldsymbol{i_1}, \boldsymbol{i_2}, \dots, \quad (4)$$

тоді множина векторів-рядків $\{\overline{\boldsymbol{X}}^*, \overline{\boldsymbol{X}}_{\boldsymbol{i}}, \boldsymbol{i} = \boldsymbol{i_1}, \boldsymbol{i_2}, \dots\}$ матриці $\boldsymbol{X}$ породжує множину припустимих дій $\widehat{\boldsymbol{\mathcal{D}}}_{\boldsymbol{1}} = \{\boldsymbol{d_{j1}}, \boldsymbol{d_{j2}}, \dots : \exists\, \boldsymbol{x_{ij} = 1}, \boldsymbol{i} = \boldsymbol{i_1}, \boldsymbol{i_2}, \dots\}$.

На наступному кроці у якості центроїду за виключенням вже обраних згідно умові (4) векторів-рядків матриці $\boldsymbol{X}$ для визначення нового центроїду обирається вектор-рядок що відповідає умові (3) та повторюється процедура формування наступної множини припустимих дій $\widehat{\boldsymbol{\mathcal{D}}}_{\boldsymbol{2}}$.

На кожному наступному кроці приймається рішення щодо доцільності визначення нового центроїду з числа залишкових векторів-рядків або визнання їх такими що належать до вже створених множин припустимих дій.

Кінцевим кроком процедури визначення множин припустимих дій $\{\widehat{\boldsymbol{\mathcal{D}}}_{\boldsymbol{k}}, \boldsymbol{k} = \boldsymbol{1}, \boldsymbol{S}\}$ має бути їх аналіз на прикмет відповідності принципам обраної політики безпеки.

Метод застосування одноразових логінів в системі управління доступом. Одним із ключових механізмів забезпечення кібербезпеки в інформаційних системах, що функціонують на основі хмарних технологій і підтримують коаліційну взаємодію між кількома організаціями, є ефективне управління доступом до інформаційних ресурсів. Зокрема, йдеться про системи, в яких учасники мають різні рівні довіри, власні нормативні обмеження та потребують узгодженої, але розподіленої політики безпеки. Забезпечення конфіденційності, цілісності та доступності інформації в таких умовах залежить насамперед від стійкості системи розмежування прав доступу та її здатності протидіяти спробам несанкціонованого входу до спільних ресурсів.

У традиційних комп'ютерних системах механізм розмежування доступу базується на трьох взаємопов'язаних процедурах: ідентифікації, автентифікації та авторизації. Ідентифікація передбачає подання користувачем унікального ідентифікатора, наприклад, логіна або електронної пошти. Автентифікація — це перевірка приналежності цього ідентифікатора до користувача на основі секретного знання або даних (наприклад, пароля, біометричних параметрів). Авторизація визначає, чи має користувач необхідні повноваження для доступу до запитаного ресурсу. Найбільш поширеною формою автентифікації залишається парольний доступ, при якому для кожного користувача формується пара «логін–пароль», що дозволяє виконати перевірку під час входу до системи.

Попри поширеність, така модель має ряд вразливостей. По-перше, доступність імені користувача (username) підвищує ризик реалізації атак соціальної інженерії. По-друге, складність так званого «сильного паролю» ускладнює його запам'ятовування, що змушує користувачів записувати паролі у небезпечних місцях, зберігати їх у смартфонах, соціальних мережах чи браузерах, підвищуючи ризик їх витоку. По-третє, при використанні одного і того ж паролю в кількох системах компрометація в одній із них може спричинити компрометацію й інших, що особливо небезпечно в умовах спільного доступу до хмарних сервісів у коаліційній ІКС.

З метою мінімізації зазначених ризиків у роботі запропоновано застосовувати метод одноразових логінів (One-Time Login). Його суть полягає у тому, що під час кожного сеансу автентифікації замість статичного логіна генерується унікальний ідентифікатор, який є дійсним лише один раз або протягом короткого проміжку часу. Генерація одноразового логіна здійснюється на авторизованому пристрої користувача, зокрема на сучасному смартфоні, який попередньо зареєстровано в системі. Таким чином, навіть у разі перехоплення цього логіна сторонні особи не зможуть використати його повторно.

Запропонований метод має кілька суттєвих переваг. По-перше, він забезпечує високий рівень захисту від фішингових атак, оскільки навіть за умови розкриття логіна зловмиснику він втрачає чинність після першого використання. По-друге, відсутність постійного ідентифікатора унеможливлює підбір облікових даних та знижує ризик атак перебору. По-третє, цей метод може бути легко інтегрований у багатофакторну автентифікацію, де одноразовий логін виступає одним із факторів поряд із паролем, токеном або біометричними даними. Окрім того, одноразові логіни можуть генеруватись у залежності від контексту — часу доби, геолокації, рівня довіри до мережі або пристрою — що дозволяє адаптувати політику доступу під поточну ситуацію.

ISSN 2663 - 4023

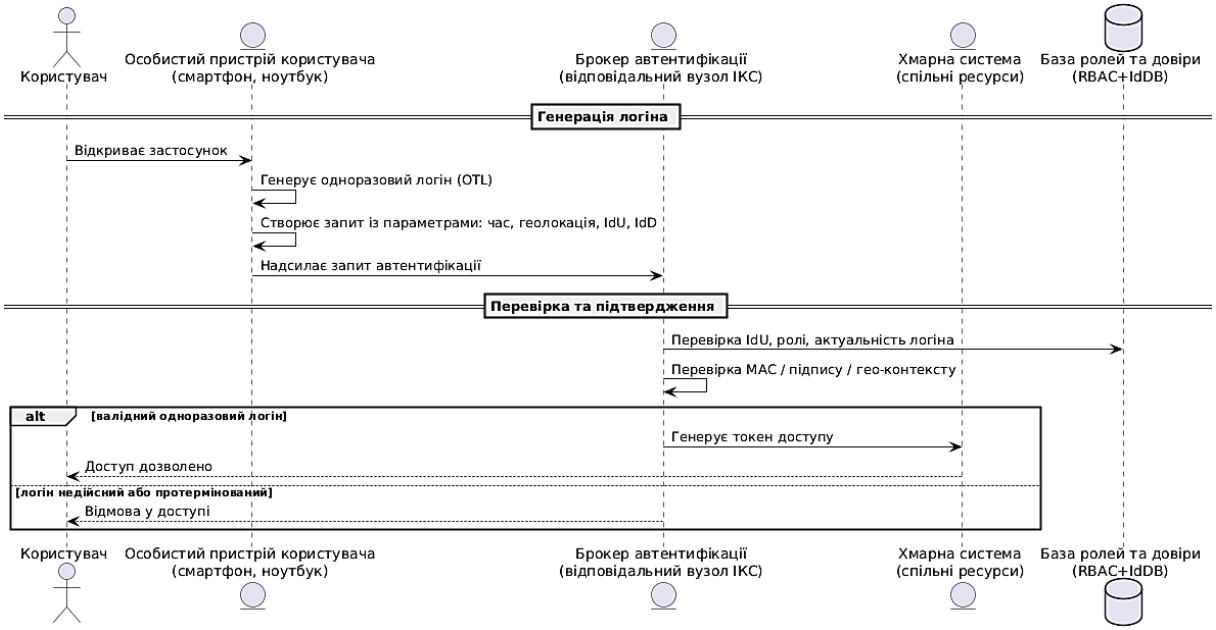

Рис. 3. Архітектура автентифікації з використанням одноразових логінів у коаліційній хмарній інформаційній системі

Рис. 3 ілюструє процес автентифікації користувача в коаліційній інформаційній системі, що використовує хмарні технології та включає кілька організацій з різним рівнем довіри. Користувач ініціює доступ до ресурсів за допомогою особистого пристрою, на якому генерується одноразовий логін (OTL), що містить унікальні ідентифікатори, часову мітку та контекстні параметри. Цей запит надсилається на вузол автентифікації (брокер), який перевіряє легітимність даних через базу ролей і довіри (RBAC). У разі підтвердження запит перенаправляється до хмарної системи, яка надає або блокує доступ до спільних ресурсів. Такий підхід дозволяє гнучко керувати доступом у багатоструктурних коаліційних середовищах із збереженням високого рівня безпеки.

Застосування одноразових логінів є особливо доцільним у коаліційних системах, де доступ до спільної хмарної інфраструктури здійснюється користувачами з різних організацій. Метод дозволяє розмежовувати зони відповідальності за обробку автентифікаційних даних, делегувати частину функцій перевірки довіреним вузлам або брокерам доступу, а також зберігати гнучкість при масштабуванні системи без порушення загальної політики безпеки. У перспективі розвиток цього методу може передбачати використання криптографічного підпису одноразового логіна, інтеграцію з блокчейн-реєстрами автентифікації, а також застосування біометричних або поведінкових характеристик для додаткової верифікації користувача (Гулак, 2023).

Таким чином, впровадження методу одноразових логінів у системи управління доступом у хмарних коаліційних середовищах дозволяє суттєво підвищити рівень безпеки, мінімізувати ризики компрометації облікових даних та адаптувати механізми доступу до сучасних загроз у динамічному, розподіленому інформаційному середовищі.

Для опису посиленого запиту користувача застосовуються такі умовні позначення:

$\boldsymbol{Ta}$ — бітовий вектор, що відповідає часу (з точністю до секунд) і даті здійснення процедури;

$\boldsymbol{IdU}$ — бітовий вектор унікального (реєстраційного) номера користувача;

$\boldsymbol{IdD}$ — бітовий вектор серійного номера особистого пристрою (девайса) користувача, який застосовується у якості інструмента отримання доступу в системі;

ISSN 2663 - 4023

$\boldsymbol{Km}$ — бітовий ключ (секретний параметр) формування коду автентифікації блоку даних $\boldsymbol{M}$ — MAC (message authentication code) — $\boldsymbol{mac(M, Km)}$, який обчислюється за допомогою безпечного алгоритму блокового шифрування $\boldsymbol{E(M, Km)}$ та цього ключу [18];

$\boldsymbol{Ke}$ — бітовий вектор — відкритий ключ системи (сервера) що забезпечує зашифрування за допомого асиметричного алгоритму паролю користувача $\boldsymbol{Pw}$.

За допомогою програмного застосунку на особистому девайсі користувача обчислюються наступні значення:

$$\widetilde{Pw} = E_A(Pw, K_e) \quad (5)$$

$$Lg = Ta \parallel IdD \parallel IdU \parallel \widetilde{Pw}, \quad (6)$$

$$Log = Lg \parallel mac(Lg, Km), \quad (7)$$

де ‖ — операція конкатенації — об’єднання бітових векторів.

З рівнянь (5–7) зрозуміло що дані до процедур ідентифікації та автентифікації включають інформацію:

- про час її створення, що спрямоване на протидіяю повтору запиту;
- ідентифікаційні дані персонального пристрою, за допомогою якого формується запит, що забезпечує підвищення безпеки застосування;
- MAC, що забезпечує контроль спроб підмінити окремі параметри запиту;
- зашифрований за допомогою відкритого ключу сервера пароль користувача, що підвищує його безпеку підчас передавання через потенційно небезпечне середовище.

Продовжуючи розгляд методу застосування одноразових логінів у системі управління доступом у контексті коаліційного підходу до забезпечення кібербезпеки інформаційних систем, що використовують хмарні технології, слід підкреслити важливість адаптації цього методу до умов багатовідомчої взаємодії та спільного використання інфраструктури з різнорівневим контролем доступу.

Запропонована схема формування посиленого запиту користувача враховує ключові вимоги до безпечного функціонування у розподіленому середовищі, де одночасно працюють користувачі з різних організацій, які мають автономні IT-сегменти, але спільно використовують ресурси коаліційної хмарної ІКС. Врахування параметра часу (Ta) дозволяє системі відслідковувати актуальність запиту та протидіяти атакам повторного відтворення (replay attacks), які є особливо небезпечними в хмарному середовищі. Включення ідентифікаторів пристрою (IdD) та користувача (IdU) забезпечує подвійне зв’язування запиту до конкретної особи та її персонального пристрою, підвищуючи рівень персоналізації автентифікації та ускладнюючи спроби несанкціонованого доступу з підроблених пристроїв.

Використання криптографічного механізму MAC з ключем Km гарантує цілісність даних запиту, оскільки навіть мінімальні зміни в бітовій структурі запиту Lg призведуть до невідповідності контрольної суми mac(Lg, Km). Це особливо важливо в коаліційних системах, де автентифікація може проводитись через посередницькі шлюзи або брокери доступу, що потребують впевненої перевірки автентичності запиту без можливості його модифікації. Зашифрований за відкритим ключем Ke пароль користувача (Pw) дозволяє безпечно передавати чутливу інформацію через незахищені канали зв’язку, що є типовим для міжорганізаційної взаємодії через хмарну інфраструктуру.

У межах коаліційної моделі управління кібербезпекою така архітектура аутентифікації дозволяє створити єдиний уніфікований механізм автентифікації з динамічною генерацією запитів, які є унікальними для кожної сесії доступу. Це дозволяє гармонізувати безпекові політики різних учасників системи без необхідності зберігання

спільних облікових даних на стороні хмарного провайдера або у центральному сховищі облікових записів. Крім того, такий підхід відкриває можливість делегування функцій автентифікації довіреним вузлам (наприклад, відомчим шлюзам безпеки), що дозволяє гнучко масштабувати систему доступу при збереженні контрольованої зони відповідальності кожного суб'єкта.

З практичної точки зору, запропонований метод може бути інтегрований у загальну архітектуру управління ідентичністю (Identity Management) коаліційної ІКС, підтримуючи концепцію «єдиного входу» (Single Sign-On) у поєднанні з багатофакторною автентифікацією. Це дозволить мінімізувати кількість запитів на автентифікацію до спільних сервісів, зменшити навантаження на інфраструктуру авторизації та забезпечити прозору взаємодію користувачів з різних організацій.

Узагальнюючи, метод одноразових логінів із застосуванням криптографічних та контекстно-залежних параметрів у системі управління доступом є ефективним рішенням у сфері кібербезпеки для коаліційних інформаційних систем, що функціонують у хмарному середовищі. Він дозволяє досягти високого рівня захищеності, адаптивності та довіри між учасниками системи, а також забезпечити узгоджене застосування політик безпеки у складних міжвідомчих структурах.

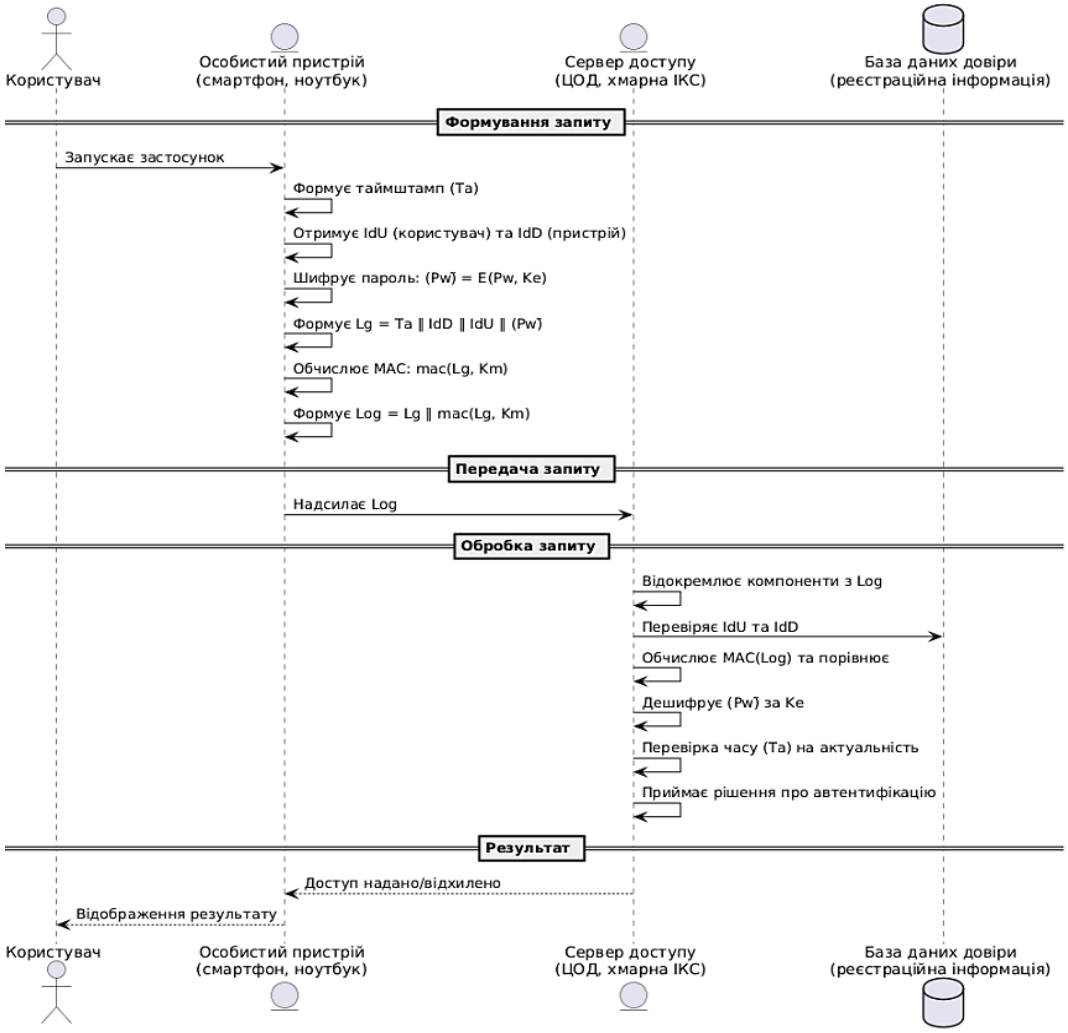

Рис. 4. Процес формування та обробки посиленого запиту користувача в системі автентифікації з використанням одноразових логінів у коаліційній хмарній ІКС

Рис. 4 ілюструє логіку взаємодії між користувачем, його особистим пристроєм (смартфоном або ноутбуком), сервером доступу (що функціонує в межах хмарної інфраструктури) та базою даних довіри, яка містить зареєстровану інформацію про користувачів і пристрої. Послідовність операцій починається з ініціації автентифікації користувачем через застосунок, що встановлений на його пристрої. Пристрій формує часову мітку (Ta), отримує ідентифікатори користувача (IdU) та пристрою (IdD), а також шифрує пароль користувача за допомогою відкритого ключа сервера (Ke), утворюючи значення (Pw̃). Далі виконується об'єднання даних у блок Lg, до якого обчислюється контрольна сума mac(Lg, Km) для перевірки цілісності, після чого формується фінальний запит Log. Після надсилання запиту до сервера доступу, останній розділяє прийнятий пакет на окремі компоненти, виконує перевірку справжності MAC-коду, актуальності часового параметра та достовірності зашифрованого паролю. У разі успішного проходження перевірок система ухвалює рішення про надання або відмову в доступі, інформуючи про це користувача. Цей процес є адаптивним до коаліційної моделі, в якій автентифікація здійснюється з урахуванням багаторівневої відповідальності, контексту доступу та динамічного середовища хмарної інформаційної системи.

ВИСНОВКИ

У результаті дослідження обґрунтовано доцільність використання коаліційного підходу до управління кібербезпекою інформаційних систем, що інтегрують хмарні технології. Запропонована модель організаційно-технічного забезпечення гарантоздатності дозволяє формалізовано координувати дії різних учасників системи захисту на основі динамічного об'єднання ресурсів, ролей та відповідальностей. Розроблена онтологічна модель убезпечення бізнес-процесів із урахуванням концепції розподіленого доступу за RBAC забезпечує структуровану і прозору реалізацію принципів мінімальних повноважень та контролю доступу.

Окрему увагу приділено методам ідентифікації та аутентифікації користувачів у хмарному середовищі. Метод одноразових логінів дозволяє підвищити стійкість системи до атак типу «перехоплення облікових даних» та зменшити ризики несанкціонованого доступу до критичних ресурсів. Усі розроблені компоненти системи працюють у синергії, формуючи багаторівневий механізм захисту, адаптований до динамічних загроз у хмарному середовищі.

Подальші дослідження доцільно спрямувати на створення повнофункціонального прототипу програмної реалізації системи, розробку сценаріїв реагування на інциденти безпеки в умовах коаліційної взаємодії, а також на оцінку ефективності та масштабованості запропонованих моделей в умовах реальних хмарних IT-інфраструктур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. On the Protection of Information in Information and Telecommunication Systems, Law of Ukraine No. 80/94-VR (1994) (Ukraine). https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
2. Grechaninov, V. F. (2021). Some issues of improving the network of situational centers in the security and defense sector. *Mathematical Machines and Systems, 3.*
3. Grechaninov, V. F., Oksanych, I. M., & Lopushanskyi, A. V. (2022). The use of cloud technologies to solve the integration of information in multilevel control systems. *Control Systems and Computers, 4*, 24–34. https://doi.org/10.15407/csc.2022.03.04.024

4. INCITS 359-2012. Information Technology – Role-Based Access Control. https://csrc.nist.gov/projects/role-based-access-control/rbac-library
5. Virginia, N. L. Franqueira et al. (2011). RBAC in Practice. *International Journal of Chronic Obstructive Pulmonary Disease*. https://www.researchgate.net/publication/254860593
6. Saltzer, J., & Schroeder, M. (1975). *The Protection of Information in Computer Systems.* Symposium on Operating Systems Principles.
7. Smirnova, T. et al. (2024). Research of cybersecurity technologies for cloud services: IAAS, PAAS and SAAS. *Cybersecurity: Education, Science, Technique, 4(24),* 6–27. https://doi.org/10.28925/2663-4023.2024.24.627
8. Gouglidis, A., Mavridis, I. (2012). domRBAC: An access control model for modern collaborative systems. *Computers & Security, 31(4),* 540–556.
9. Esna-Ashari, M. et al. (2011). Reliability of separation of duty in ANSI standard role-based access control. *Scientia Iranica D, 18(6),* 1416–1424.
10. On approval of the Rules for ensuring information protection in information, electronic communication and information-telecommunication systems, Resolution of the Cabinet of Ministers of Ukraine, No. 373 (2006) (Ukraine). https://zakon.rada.gov.ua/laws/show/373-2006-п#Text
11. *Information technology – Security techniques – Information security management systems – Requirements* (DSTU ISO/IEC 27001:2015). https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf
12. Weske, M. (2024). *Business Process Management: Concepts, Languages, Architectures. Fourth Edition*. Springer-Verlag.
13. Borek, A. et al. (2014). *Total Information Risk Management: Maximizing the Value of Data and Information Assets.* Elsevier. https://doi.org/10.1016/C2012-0-00446-2.
14. Stoiljković Ranđelović, A. et al. (2018). Identification and analysis of key business process management factors. *Economic Themes, 56(1),* 57–78. https://doi.org/10.2478/ethemes-2018-0004
15. Matthews, B. (2024). What Is a RACI Matrix? Definition, Examples, Uses. URL: https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/#:~:text=The%20four%20components%20of%20a,to%20be%20updated%20on%20progress
16. Korbut, O. A., & Finkelshtein, Yu.Yu. (1969). *Discrete Programming.* Kyiv: Nauka.
17. Kellerer, H., Pferschy, U., & Pisinger, D. (2004). *Knapsack Problems.* Berlin: Springer.
18. Hnatiienko, H. M., & Snytjuk, V. Ye. (2008). *Expert Technologies for Decision Making.* Kyiv: Maclaut LLC.
19. Hulak, H. M. et al. (2023). *Information and Cybersecurity of the Enterprise*. Lviv: Publisher Marchenko T.V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Pavlo Skladannyi
PhD, Associate Professor, Head of the Department of Information and Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID:0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Hennadii Hulak
Doctor of Sience, Professor, Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-9131-9233
h.hulak@kubg.edu.ua

Viktor Korniets
PhD Student
Institute of Mathematical Machines and Systems Problems of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0002-4967-8395
viktorkorniets@gmail.com

COALITION-BASED APPROACH TO CYBERSECURITY MANAGEMENT OF INFORMATION SYSTEMS EMPLOYING CLOUD TECHNOLOGIES

Abstract. Ensuring cybersecurity in the context of cloud technologies requires effective cooperation between organizations that jointly operate information systems within a shared infrastructure. This is especially relevant for structures with hierarchical management systems and departmental information protection requirements. In such settings, a coalition-based approach to cybersecurity management plays a key role by aligning the actions of various participants to achieve a common goal—protecting information assets in cloud environments. Research shows that coordinated efforts enhance the effectiveness of protection, reduce data leakage risks, and contribute to system dependability. This approach is particularly critical for networks of situational centers operating in the national security domain. This study explores the use of the Role-Based Access Control (RBAC) model, the method of one-time logins, and proposes an organizational and technical model for access management in coalition-based cybersecurity systems built on cloud technologies. This work applies methods of systems analysis, architectural modeling of information systems, formalization of access roles based on the RBAC (Role-Based Access Control) reference model, and coalition management methods for coordinating cybersecurity policies across organizations. Additionally, an authentication approach using one-time login credentials is implemented to enhance access control security in cloud environments. The study addresses the challenges of building a secure information and communication system based on cloud technologies utilizing data center services. A specific feature of such systems is the involvement of multiple organizations with individual information protection regulations, necessitating a coalition-based approach to cybersecurity management. Based on a detailed analysis, the essence of this approach is defined as the coordinated interaction of stakeholders aimed at enhancing data protection effectiveness and service quality. The paper proposes a model for organizational and technical assurance of dependability and cybersecurity, an ontological access management model based on the RBAC methodology, and a method of using one-time login credentials for authentication. The proposed solutions aim to strengthen the cyber resilience of systems utilizing cloud services. Further research will focus on software implementation of the suggested approaches. This study presents a model for organizational and technical assurance of dependability and cybersecurity based on a coalition-based protection strategy; an ontological model for securing business processes according to the RBAC methodology; and a method for applying one-time login credentials in access control systems. These models and methods are aimed at enhancing the security level of information and communication systems that utilize cloud services. Future research will concentrate on the software modeling aspects of the proposed solutions.

Keywords: dependability; cybersecurity; threat; information protection; communication network.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. On the Protection of Information in Information and Telecommunication Systems, Law of Ukraine No. 80/94-VR (1994) (Ukraine). https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
2. Grechaninov, V. F. (2021). Some issues of improving the network of situational centers in the security and defense sector. *Mathematical Machines and Systems, 3.*
3. Grechaninov, V. F., Oksanych, I. M., & Lopushanskyi, A. V. (2022). The use of cloud technologies to solve the integration of information in multilevel control systems. *Control Systems and Computers, 4*, 24–34. https://doi.org/10.15407/csc.2022.03.04.024
4. INCITS 359-2012. Information Technology – Role-Based Access Control. https://csrc.nist.gov/projects/role-based-access-control/rbac-library
5. Virginia, N. L. Franqueira et al. (2011). RBAC in Practice. *International Journal of Chronic Obstructive Pulmonary Disease*. https://www.researchgate.net/publication/254860593
6. Saltzer, J., & Schroeder, M. (1975). *The Protection of Information in Computer Systems.* Symposium on Operating Systems Principles.
7. Smirnova, T. et al. (2024). Research of cybersecurity technologies for cloud services: IAAS, PAAS and SAAS. *Cybersecurity: Education, Science, Technique, 4(24),* 6–27. https://doi.org/10.28925/2663-4023.2024.24.627
8. Gouglidis, A., Mavridis, I. (2012). domRBAC: An access control model for modern collaborative systems. *Computers & Security, 31(4),* 540–556.
9. Esna-Ashari, M. et al. (2011). Reliability of separation of duty in ANSI standard role-based access control. *Scientia Iranica D, 18(6),* 1416–1424.
10. On approval of the Rules for ensuring information protection in information, electronic communication and information-telecommunication systems, Resolution of the Cabinet of Ministers of Ukraine, No. 373 (2006) (Ukraine). https://zakon.rada.gov.ua/laws/show/373-2006-п#Text
11. *Information technology – Security techniques – Information security management systems – Requirements* (DSTU ISO/IEC 27001:2015). https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf
12. Weske, M. (2024). *Business Process Management: Concepts, Languages, Architectures. Fourth Edition*. Springer-Verlag.
13. Borek, A. et al. (2014). *Total Information Risk Management: Maximizing the Value of Data and Information Assets.* Elsevier. https://doi.org/10.1016/C2012-0-00446-2.
14. Stoiljković Ranđelović, A. et al. (2018). Identification and analysis of key business process management factors. *Economic Themes, 56(1),* 57–78. https://doi.org/10.2478/ethemes-2018-0004
15. Matthews, B. (2024). What Is a RACI Matrix? Definition, Examples, Uses. URL: https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/#:~:text=The%20four%20components%20of%20a,to%20be%20updated%20on%20progress
16. Korbut, O. A., & Finkelshtein, Yu.Yu. (1969). *Discrete Programming.* Kyiv: Nauka.
17. Kellerer, H., Pferschy, U., & Pisinger, D. (2004). *Knapsack Problems.* Berlin: Springer.
18. Hnatiienko, H. M., & Snytjuk, V. Ye. (2008). *Expert Technologies for Decision Making.* Kyiv: Maclaut LLC.
19. Hulak, H. M. et al. (2023). *Information and Cybersecurity of the Enterprise.* Lviv: Publisher Marchenko T.V.