КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.743
УДК 004.005(49)

Капелюшна Тетяна Вікторівна
д.е.н, доцент, професор кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0001-7490-6751
e-skr@ukr.net

Мужанова Тетяна Михайлівна
к.держ.упр., доцент, доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0002-7435-0287
muzanovat@gmail.com

Берестяна Тетяна Володимирівна
старший викладач кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0007-1455-234X
berestianatv@gmail.com

Голобородько Сергій Олександрович
ст. викладач кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0006-9892-3031
s.holoborodko@duikt.edu.ua

Примаченко Діана Володимирівна
асистент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0003-2386-7440
primachenkodiana08@gmail.com

МЕХАНІЗМ УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ НА ПІДПРИЄМСТВІ

Анотація. У статті розглянуто питання щодо захисту інформаційних ресурсів підприємства шляхом управління доступом до них. Проаналізовано основні моделі управління доступом, серед яких: рольова модель управління доступом (Role-Based Access Control); модель доступу на основі набору атрибутів ABAC (Attribute-Based Access Control); модель контролю доступу на основі ідентичності (Identity and Access Management, IAM); модель обов'язкового контролю доступу (Mandatory Access Control); модель дискреційного або вибіркового контролю доступу (Discretionary Access Control); гібридні моделі управління доступом (поєднання різних підходів до управління доступом, що дозволяє організаціям створювати більш гнучкі та ефективні стратегії контролю доступу до інформаційних ресурсів); Identity-Based Access Control (IBAC); модель керування доступом на основі цілей (PACF); модель Next Generation Access Control (NGAC) і Blockchain-Based Access Control, що інтегрують сучасні технології, такі як блокчейн і розподілені системи. Представлено переваги та недоліки розглянутих моделей управління доступом до інформаційних ресурсів на підприємстві. Розглянуто Закон України «Про захист персональних даних», а саме його частину, що стосується гарантування збереження приватності інформації. Відмічено, що в ЗУ про «Основи законодавства України про охорону здоров'я» прописано правила поводження працівників медзакладів із інформацією пацієнтів, що обумовлює потребу визначення цілей збору даних клієнтів та доступу до них. Запропоновано механізм управління доступом до інформаційних ресурсів підприємства (сфери охорони здоров'я) з визначеними цілями, інструментами та технологіями управління доступом, розподілом ролей та політиками доступу, рекомендованим регуляторним полем.

© Т.В. Капелюшна, Т.М. Мужанова, Т.В. Берестяна, С.О. Голобородько, Д.В. Примаченко, 2025

Ключові слова: безпека; управління доступом; управління безпекою підприємств; механізм управління інформаційною безпекою підприємства.

ВСТУП

Комунікація є важливою складовою життя суспільства, функціонування підприємств, особливо за теперішніх невизначених умов, коли переважна більшість працівників виконують роботу дистанційно. Кількість інформації та інформаційні потоки збільшуються через активне спілкування, обмін даними. Процес комунікації забезпечується наявністю засобів інформаційної взаємодії, інформаційної інфраструктури та інформаційних ресурсів, потреба у захисті яких зростає з причин активної діджиталізації процесів, оцифрування послуг.

Інструменти управління доступом є невід'ємною частиною інформаційних систем, включають такі технології, як: багатофакторна автентифікація, що посилює рівень захисту, забезпечуючи додаткову впевненість у тому, що доступ отримує саме уповноважена особа. Управління доступом потребує постійного удосконалення через нові виклики, серед яких перехід на хмарні технології, оскільки дані більше не зберігаються у локальних мережах, а розподілені у хмарному середовищі. Окрім того, управління доступом є інструментом для запобігання внутрішнім загрозам, адже значна частина інцидентів інформаційної безпеки виникає через дії співробітників організацій — як навмисні, так і ненавмисні. Ефективна система доступу дозволяє обмежувати можливості працівників у полі їх функціональних обов'язків, запобігаючи доступу до інформації, яка не стосується їхньої діяльності. Наявність вищезгаданих викликів обумовлює потребу в удосконаленні управління доступом до інформаційних ресурсів й забезпеченні їх постійного захисту.

Постановка проблеми. Управління доступом не може залишатися статичним, оскільки потребує удосконалення відповідно до нових викликів і загроз. Важливо в управлінні доступом враховувати швидке впровадження новітніх технологій, таких як хмарні обчислення, Інтернет речей (IoT), штучний інтелект, за допомогою яких розширюється можливість обробки даних, що одночасно продукує нові загрози безпеки даних. Наразі дані зберігаються не лише в локальних мережах, але й у розподілених середовищах, тим самим ускладнюючи їх захист. Управління доступом в таких умовах дозволяє гарантувати контрольованість безпеки інформації незалежно від того, де вона фізично розташована.

Управління доступом має базуватися на принципах, які забезпечують його ефективність та адаптивність до сучасних викликів. Одним із таких принципів є принцип мінімізації привілеїв, суть якого полягає в тому, що кожному користувачеві чи системі надається лише той рівень доступу, який необхідний для виконання його функцій в організації, що допомагає зменшити ймовірність помилок чи зловмисних дій. Поділ обов'язків не менш важливий принцип, спрямований на розподіл критичних завдань між різними особами або системами, щоб уникнути концентрації повноважень у руках однієї особи. Упередження загроз безпеці інформаційних ресурсів підприємства — основна задача управлінця з кібербезпеки та захисту інформації, досягнення якої можливе за підбору конкретної, прийнятної у відповідності до специфіки його діяльності й функціонування, моделі управління. Побудова механізму управління доступом до інформаційних ресурсів підприємства сприятиме посиленню інформаційної безпеки підприємства.

Аналіз останніх досліджень та публікацій. Інформаційні ресурси являють собою сукупність накопичених знань, ідей та інструкцій щодо їх реалізації, зафіксованих у формі, що забезпечує можливість їх багаторазового відтворення та використання. До таких ресурсів належать наукові праці, книги, статті, патенти, дисертації, документація з науково-дослідної та дослідно-конструкторської діяльності, технічні переклади, а також інформація про передові виробничі технології. Відмінною особливістю інформаційних ресурсів є їх здатність до експоненційного зростання: чим активніше вони використовуються, тим швидше поповнюється їх обсяг, що відрізняє їх від традиційних ресурсів.

Як зазначає Арістова І.В., інформаційні ресурси поєднуються із інформаційно-комунікаційною інфраструктурою, що є основою для ефективного управління, обміну та захисту інформації (територіально розподілені державні та корпоративні комп'ютерні мережі, телекомунікаційні системи, сучасні інформаційні, комп'ютерні та телекомунікаційні технології), а також з науково-виробничим потенціалом у сфері електронних комунікацій (організаційні структури та кадрові ресурси, що забезпечують функціонування й розвиток національної інформаційної інфраструктури, ринок інформаційних технологій та засобів зв'язку, система масової інформації, а також нормативно-правове забезпечення в сфері інформаційних відносин) [1]. Їх координація та розвиток сприяє створенню безпечного та ефективного інформаційного середовища.

Мороз В.М. вважає, що під інформаційним ресурсом слід розуміти системну єдність впорядкованої у межах певного носія (сховища, місця розташування тощо) інформації (знань) з середовищем її формування, накопичення та розвитку, а також засобами та технологіями її зберігання, використання та передачі [2].

Задля забезпечення контролю доступу щодо того, ким і в який спосіб отримується доступ до інформаційних ресурсів варто належну увагу приділяти управлінню доступом, із включенням широкого спектру механізмів, технологій і процесів, які спрямовані на збереження конфіденційності, цілісності та доступності інформації. Суть управління доступом полягає в тому, щоб створити механізм розмежування прав користувачів відповідно до їхніх ролей, обов'язків і завдань, які вони виконують. Це дозволяє мінімізувати ризики, пов'язані з несанкціонованим доступом до даних, неправомірним використанням ресурсів чи випадковим порушенням безпеки. Л. Байс вважає, що успішне управління доступом залежить від вибору моделі, яка найкраще відповідає потребам організації [3], системи управління доступом яких, на думку А. Ахмада, ґрунтуються на моделях, які визначають логіку та правила доступу до інформаційних ресурсів відповідно до ролі користувача у системі [4].

Таким чином, управління доступом виступає ключовим інструментом для забезпечення надійного функціонування систем у межах прийнятних рівнів ризику й потребує побудови єдиного механізму його забезпечення.

Мета статті. Сформувати механізм управління доступом до інформаційних ресурсів підприємства задля забезпечення безпеки його функціонування та захисту інформації.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Н. Вайнер визначив, що інформація залишається осередком кібернетики — міждисциплінарної науки, що вивчає принципи управління, зв'язку та регуляції в складних системах, незалежно від їхньої фізичної природи (біологічних, технічних,

соціальних тощо) [5]. За ЗУ «Про інформацію», інформація — будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [6]. Інформація є ресурсом, а інформаційні ресурси є частиною факторів виробництва, що викликає інтерес до забезпечення їх безпеки на рівні із матеріальними ресурсами.

Як було зазначено вище, успішність управління доступом залежить від вибору моделі, моделі управління доступом — це концептуальні підходи, які визначають правила і механізми контролю доступу користувачів до інформаційних ресурсів у межах організації чи системи. Вибір моделі є основоположним для забезпечення безпеки, адже кожна модель має свої особливості, переваги, обмеження та сфери застосування. У сучасних інформаційних системах існує кілька базових моделей управління доступом, кожна з яких розроблена для вирішення конкретних завдань і відповідає заявленим потребам організації [7]. Залежно від особливостей бізнес-процесів, масштабу компанії та характеру інформаційних активів, використовуються різні типи систем управління доступом, основні із них представлено на рис. 1.

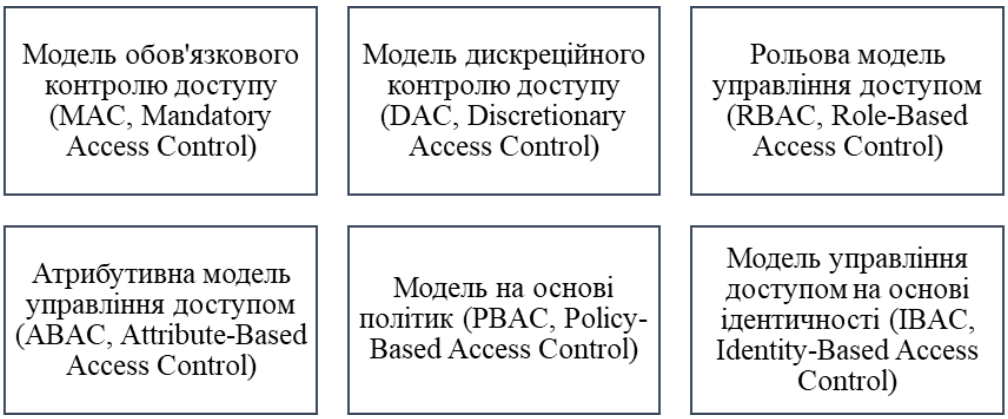

Рис. 1. Поширені моделі управління доступом

Рольова модель управління доступом (RBAC, Role-Based Access Control) базується на наданні прав доступу користувачам на основі їхніх ролей у організації, що дозволяє централізовано керувати доступом до систем, додатків і даних, забезпечує зручність адміністрування і високий рівень безпеки. Основним принципом RBAC є те, що кожен користувач отримує доступ до ресурсів залежно від ролі, яка визначається як набір дозволів або привілеїв, які відповідають певним обов’язкам і функціям співробітника («адміністратор», «менеджер», «співробітник», «гість») [8].

Модель RBAC дозволяє централізовано контролювати доступ до інформаційних ресурсів і забезпечує чітке розмежування прав доступу, що мінімізує ймовірність виникнення помилок при призначенні прав доступу, оскільки зміни в доступах до систем можна зробити в межах ролі, а не для кожного користувача окремо (якщо співробітник змінює свою роль з «менеджера» на «співробітника», всі його доступи до ресурсів, що відповідають цій ролі, автоматично знижуються без необхідності вручну коригувати права доступу).

RBAC має низку переваг, серед яких: забезпечення високої безпеки та зручності в управлінні доступом, що є критичним для великих організацій у разі кількості користувачів більше за тисячу осіб; модель є легкою для впровадження і підтримки, особливо в організаціях із визначеними і усталеними ролями [9]. Проте, як і будь-яка система, RBAC має й недоліки: обмежена гнучкість, оскільки система базується на

фіксованих ролях і наборі прав доступу (проблема у випадках, коли доступ до ресурсів залежить від динамічних факторів або умов — місцезнаходження користувача, тип пристрою, час доби або інші специфічні умови); складність створення набору ролей, що враховували особливості та нюанси доступу для кожного співробітника; зростання кількості ролей, що спричиняє складність управління; проблеми в адаптації до змін у бізнес-структурі у разі швидкого коригування ролі та привілеїв; зловживання правами доступу; складність інтеграції RBAC у разі використання організацією зовнішніх сервісів, хмарних платформ.

Тож, рольова модель управління доступом (RBAC) є відмінним вибором для багатьох організацій, які мають чітко визначену структуру ролей і обов'язків. Вона забезпечує високий рівень безпеки завдяки чітким ієрархічним структурам прав доступу, що значно спрощує процес адміністрування. Водночас дана модель потребує пильного нагляду при її впровадженні, оскільки необхідно ретельно продумати структуру ролей і відповідних прав доступу, щоб забезпечити максимально ефективний контроль доступу при мінімізації можливих ризиків [10].

У моделі ABAC (Attribute-Based Access Control, ABAC) доступ до інформаційних ресурсів надається або обмежується на основі набору атрибутів. Атрибути можуть бути різними: від ідентифікаційних даних користувача (наприклад, його посади, відділу або рівня доступу) до атрибутів, що стосуються ресурсів (наприклад, конфіденційності або типу файлу), а також до атрибутів можуть бути віднесені умови, в яких здійснюється доступ (час доби, географічне місцезнаходження або тип пристрою, з якого здійснюється підключення) [11].

ABAC дозволяє організаціям створювати більш детальні політики доступу, що враховують конкретні умови доступу. У випадку, якщо хоча б одна з умов змінюється (наприклад, користувач намагається отримати доступ з мобільного пристрою або поза робочим часом), доступ буде автоматично заблокований.

Атрибути, які використовуються в ABAC:

- атрибути користувача (персональні дані (наприклад, ім'я, посада, відділ, рівень доступу, досвід роботи); динамічні атрибути (місцезнаходження, час доступу або тип пристрою));
- атрибути ресурсів (характеристики файлів, документів, систем або додатків, такі як їх конфіденційність, тип або статус);
- умовні атрибути (географічне розташування користувача або тип мережі, через яку здійснюється доступ) [12].

Така модель дозволяє також значно підвищити рівень безпеки, оскільки обмежує доступ не лише на основі ролі користувача, але й з урахуванням інших змінних умов. Це робить модель більш захищеною від зловмисних атак, таких як фішинг або несанкціонований доступ через вкрадені облікові дані, оскільки для доступу до ресурсів повинні бути виконані не тільки основні вимоги, а й додаткові умови.

Одним із основних недоліків моделі є складність реалізації та управління політиками доступу через велику кількість атрибутів і умов, що мають бути враховані при визначенні доступу, адміністрування таких систем може бути складним і вимагати значних ресурсів.

Іншою складністю є потреба у високому рівні автоматизації та підтримки політик, оскільки навіть невеликі зміни в атрибутах можуть вимагати коригувань у численних політиках доступу. Це створює додаткові труднощі для великих організацій, де кількість атрибутів і правил може бути великою. Крім того, для того, щоб ABAC працював

ефективно, всі використовувані системи повинні бути інтегровані та підтримувати необхідні атрибути, що потребує великих інвестицій в інфраструктуру [13].

Контроль доступу на основі ідентичності (Identity and Access Management, IAM) забезпечує управління ідентифікацією користувачів та їх доступом до різних інформаційних ресурсів в організації. Система IAM не тільки дозволяє ефективно керувати правами доступу, але й гарантує безпеку шляхом автентифікації та авторизації користувачів, а також забезпечує дотримання політик безпеки. IAM складається з набору процесів, політик та технологій, що дозволяють організаціям контролювати, хто може отримати доступ до їхніх ресурсів, а також визначати, який рівень доступу користувач може мати.

У своїй основі IAM допомагає організаціям вирішувати важливі питання, пов’язані з ідентифікацією користувачів, управлінням їх правами доступу та веденням обліку використання ресурсів [15].

Серед головних переваг системи IAM є централізоване управління доступом до всіх корпоративних ресурсів. В організаціях з великою кількістю користувачів та різноманітними системами доступу централізоване управління дозволяє знижувати витрати на адміністрування, полегшує підтримку політик безпеки і допомагає забезпечити відповідність вимогам законодавства, таким як GDPR, HIPAA або PCI-DSS. Крім того, автоматизація процесів управління доступом дозволяє зменшити людські помилки, що виникають в процесі ручного управління доступами.

Обов’язковий контроль доступу (Mandatory Access Control, MAC) активно використовується в системах, де важливий високий рівень безпеки, таких як урядові структури, військові організації та інші структури, які працюють з конфіденційною інформацією. Відмінною рисою MAC є те, що доступ до ресурсів в системі визначається не користувачем, а адміністраторами системи за допомогою встановлених політик безпеки. У цьому випадку користувачі не можуть самостійно змінювати рівень доступу або приймати рішення щодо того, хто і що може бачити, редагувати або використовувати. Усі ці рішення приймаються з урахуванням заздалегідь визначених політик, які зазвичай встановлюються на рівні системи і є обов’язковими для виконання.

Основною концепцією MAC є те, що кожен об’єкт системи (файл, програма, процес, пристрій тощо) має певний рівень безпеки, а користувачі мають доступ лише до тих об'єктів, рівень безпеки яких відповідає рівню доступу, що їм надано. Система має строгі правила доступу, які гарантують, що інформація не буде передаватися між об’єктами з різними рівнями безпеки. Наприклад, дані з високим рівнем конфіденційності (такі як державні секрети) не можуть бути доступні користувачам з низьким рівнем дозволу [16]. Кожен об’єкт і кожен користувач у такій системі мають свою мітку безпеки. Мітки безпеки можуть включати: рівень секретності (секретно, конфіденційно, для службового користування), а також інші атрибути, такі як категорії даних (для досліджень, фінансів, для загального користування тощо). Користувач, у свою чергу, має мітку доступу, яка визначає його рівень дозволу для доступу до різних об’єктів. Зазвичай, користувачі мають різні рівні доступу до різних типів інформації, інколи можуть мати доступ лише до неконфіденційних даних, або до всіх даних за певними умовами. Особливість MAC полягає у політиках, встановлених адміністраторами системи, а не на рішеннях окремих користувачів, тобто користувачі не можуть самостійно змінювати доступ до даних або визначати, хто має право доступу. Замість цього система має централізовану модель управління, де права доступу визначаються на основі політик безпеки, а доступ до ресурсів надається або обмежується залежно від відповідності між міткою користувача та міткою об’єкта. Використовується

політика «не нижче» (no read up, write down, або «CLEARANCE»), яка передбачає, що користувач може зчитувати інформацію лише на своєму рівні та не нижче, а писати або змінювати інформацію можна лише на рівні, що нижче рівня доступу користувача, або ж політика «не вище» (no write up, read down), що обмежує користувачів від запису або зміни даних на рівні, який вище за їхній рівень доступу.

Контроль доступу дискреційний або вибірковий (Discretionary Access Control, DAC) передбачає можливість самостійного визначення хто з інших користувачів може отримати доступ до файлів, програм, баз даних, що дозволяє забезпечити велику гнучкість у використанні ресурсів та управлінні доступом, оскільки власники об'єктів можуть передавати права доступу іншим користувачам без необхідності залучати адміністратора системи. У той же час, система DAC надає певний рівень контролю доступу, але вимагає від користувачів обережності, оскільки зловживання правами доступу або недбалий підхід до управління доступами може призвести до порушень безпеки.

Основна перевага DAC полягає в його простоті та гнучкості. Користувачі можуть швидко налаштувати доступ до ресурсів без необхідності залучати системних адміністраторів або створювати складні правила доступу, тобто є дієвою у невеликих організаціях або в командних проєктах, де співробітники часто обмінюються інформацією та ресурсами, DAC дозволяє швидко делегувати доступ. Основний ризик при використанні моделі — можливість надання доступу користувачами до чутливих даних неавторизованим особам.

Існують також інші стратегії та моделі управління доступом, які можуть бути застосовані разом з DAC для досягнення більшого рівня безпеки. Наприклад, рольовий контроль доступу (RBAC) або контроль доступу на основі атрибутів (ABAC) можуть бути використані для додаткової ієрархії та централізованого управління доступом. В таких випадках DAC може використовуватися в поєднанні з іншими методами для досягнення збалансованого підходу до управління правами доступу.

Гібридні моделі управління доступом являють собою поєднання різних підходів до управління доступом, що дозволяє організаціям створювати більш гнучкі та ефективні стратегії контролю доступу до інформаційних ресурсів. Такі моделі комбінують сильні сторони кількох основних систем управління доступом, таких як рольовий контроль доступу (RBAC), контроль доступу на основі атрибутів (ABAC), контроль доступу на основі матриці (MAC) та дискреційний контроль доступу (DAC), щоб задовольнити специфічні потреби та вимоги безпеки в різних ситуаціях. Використання гібридних моделей дозволяє адаптувати механізми доступу до конкретних умов організації, враховуючи як вимоги безпеки, так і потребу в гнучкості, швидкості й ефективності.

Перевагою гібридних моделей є їх здатність забезпечити баланс між централізованим контролем та гнучкістю, що дозволяє організаціям ефективно реагувати на ці зміни, поєднуючи різні моделі контролю доступу та створюючи більш динамічні та адаптивні політики доступу.

Однак, для ефективної роботи з гібридними моделями, організаціям потрібно мати добре розроблену інфраструктуру безпеки, включаючи автоматизовані інструменти для моніторингу, аналізу та аудиту доступу, а також чітко визначені політики безпеки, що дозволяють мінімізувати можливі помилки та недоліки в управлінні доступом.

Identity-Based Access Control (IBAC) використовує матрицю доступу, якою задаються права доступу, такі як: читання, запис або виконання, де рядки представляють користувачів, а стовпці — об'єкти. На основі IBAC розроблені дві похідні моделі: списки

контролю доступу (ACLs), які фокусуються на правах доступу об'єкта та списки можливостей (Capabilities), що зосереджені на правах суб'єкта.

Нові моделі, такі як Next Generation Access Control (NGAC) і Blockchain-Based Access Control, інтегрують сучасні технології блокчейн і розподілені системи. NGAC дозволяє комбінувати різні політики доступу, а блокчейн додає додатковий рівень захисту завдяки своїй незмінності.

Узагальнено переваги та недоліки моделей управління доступом до інформаційних ресурсів підприємства наведено у табл. 1.

Таблиця 1

Переваги та недоліки моделей управління доступом до інформаційних ресурсів підприємства

Тип моделі	Переваги	Недоліки
RBAC	Зручне управління доступом для великих організацій. Відповідність корпоративній структурі.	Складність оновлення ролей при змінах у структурі. Ризик надмірних привілеїв для певних ролей.
ABAC	Гнучкість налаштувань. Динамічне врахування умов доступу (час, місце, пристрій тощо).	Висока складність впровадження. Збільшене навантаження на систему через оцінку атрибутів.
IAM	Централізоване управління обліковими записами та правами доступу. Підтримка сучасних методів автентифікації.	Залежність від хмарних платформ для інтеграції. Можливі проблеми з масштабованістю для малих підприємств.
MAC	Високий рівень безпеки. Жорсткі політики доступу. Захист конфіденційної інформації.	Низька гнучкість. Значні витрати на адміністрування. Обмежена зручність для користувачів.
DAC	Гнучкість і простота в налаштуванні. Легке делегування доступу.	Вразливість через людський фактор. Вищий ризик несанкціонованого доступу.
Гібридні	Поєднання переваг декількох моделей. Гнучкість для адаптації до потреб організації.	Висока складність розробки та впровадження. Ризик конфліктів між компонентами різних моделей.
IBAC	Високий рівень персоналізації доступу. Простота для невеликих організацій.	Низька ефективність у великих системах. Вразливість у разі компрометації облікового запису.
NGAC	Гнучкість у налаштуванні політик. Централізоване управління та контроль доступу. Сумісність із сучасними стандартами.	Висока складність впровадження. Необхідність спеціальних знань для адміністрування.
Blockchain для управління доступом	Децентралізований контроль. Висока прозорість і надійність (невразливість до змін). Можливість роботи без посередників.	Обмежена продуктивність у масштабних системах. Значні витрати на ресурси для підтримки.
PACF	Універсальність через підтримку множинних політик. Висока автоматизація. Інтеграція з різними платформами.	Складність налаштування та підтримки. Вимоги до регулярного оновлення політик.

Враховуючи всі ці аспекти, гібридні моделі управління доступом є потужним інструментом для забезпечення безпеки та гнучкості в управлінні інформаційними ресурсами. Вони дозволяють організаціям досягти оптимального балансу між

необхідністю суворого контролю доступу та вимогою до швидкої адаптації та зручності для користувачів.

Гарантувати збереження приватності інформації потрібно для формування довіри клієнта у разі використанні компанією його даних. Згідно із ст. 5 ч. 1, 2, 4 Закону України «Про захист персональних даних», об'єктами захисту є персональні дані, які обробляються в базах персональних даних. Персональні дані, крім знеособлених персональних даних, за режимом доступу є інформацією з обмеженим доступом [17]. Закладам охорони здоров'я слід враховувати, що персональні відомості про хворих осіб та їх стан здоров'я, діагноз, методи лікування, сімейне життя тощо не підлягають розголошенню, оскільки одним з різновидів таємної інформації є лікарська таємниця, яка включає відомості про пацієнта та стан його здоров'я, діагноз захворювання, особисте життя пацієнта, в тому числі сімейне життя, методи лікування хвороби тощо. Згідно ст. 40 ЗУ від 19.11.1992 № 2801-XII «Основи законодавства України про охорону здоров'я» медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу т.і., не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків [18]. Тому медичні заклади мають чітко визначати цілі збору даних та доступу до них. Мотивами для прийняття підходу, заснованого на цілях, слугують:

1) визначення того, які дані використовуються для яких цілей (наприклад, вік та адреса електронної пошти клієнтів використовуються для маркетингового аналізу);
2) узгоджене з клієнтами використання даних варіюється в залежності від конкретної особи.

Конфіденційність даних визначається механізмом управління доступом до інформаційних ресурсів, який описує, кому можуть бути розкриті дані та, які цілі їх використання.

Контроль доступу важливий для приватної інформації у веб-сервісах. Співробітник служби безпеки повинен перевіряти запити на доступ до чутливих даних відповідно до встановлених критеріїв. Навіть коли така інформація видаляється з оприлюднених відмостей, решта даних у поєднанні з іншими джерелами інформації все одно може пов'язувати інформацію з особами, яких вона стосується. Для вирішення цього питання можна застосувати підходи на основі концепції k-анонімності як ефективний метод захисту приватної інформації. Ще одна безпечна методика захисту приватної інформації виникає в контексті інтелектуального аналізу даних. Такі методи базуються на модифікації або збуренні даних певним чином (методи, що спеціалізуються на збереженні конфіденційності, видобувають правила асоціацій, модифікуючи дані таким чином, щоб зменшити довіру до чутливих правил асоціацій).

Спільною проблемою для даних методів є якість отриманих даних; якщо дані зазнають занадто багато модифікацій, вони можуть виявитися непридатними для подальшого використання. Безпека приватної інформації не може бути легко забезпечена традиційними моделями управління доступом, оскільки ці системи зазвичай зосереджені на тому, який користувач виконує яку дію над яким об'єктом даних.

Ще однією проблемою в механізмах контролю доступу є конфлікти при створенні нових параметрів доступу. Наприклад, якщо існує кілька налаштувань контролю доступу і немає конфліктів між деякими з них; однак це може призвести до конфліктів при виконанні всіх налаштувань одночасно.

ISSN 2663 - 4023

Модель керування доступом на основі цілей (PACF) розроблена для підтримки ієрархії цілей шляхом впровадження призначених та доступних цілей і пов'язаних з ними моделей даних [19].

Основою функціонування механізму є поділ прав доступу відповідно до ролей користувачів. У контексті підприємства виділяються такі основні категорії: постачальники послуг, лікарі, вспоміжний персонал та пацієнти. Кожна роль характеризується певним рівнем доступу до інформаційних ресурсів. Постачальники послуг отримують повний доступ до налаштувань системи та інструментів моніторингу для забезпечення технічного обслуговування та підтримки. Лікарі мають можливість взаємодіяти з медичними картками пацієнтів, лабораторними результатами та діагностичними даними, тоді як вспоміжний персонал користується тимчасовими правами доступу, які визначаються поточними завданнями. Пацієнти, у свою чергу, мають обмежений доступ до власних медичних записів через спеціалізований портал.

З метою забезпечення безпеки інформаційних ресурсів у закладах охорони здоров'я пропонується використовувати механізм управління доступом до них з визначеними цілями, інструментами та технологіями управління доступом, розподілом ролей та політиками доступу, рекомендованим регуляторним полем (рис. 2).

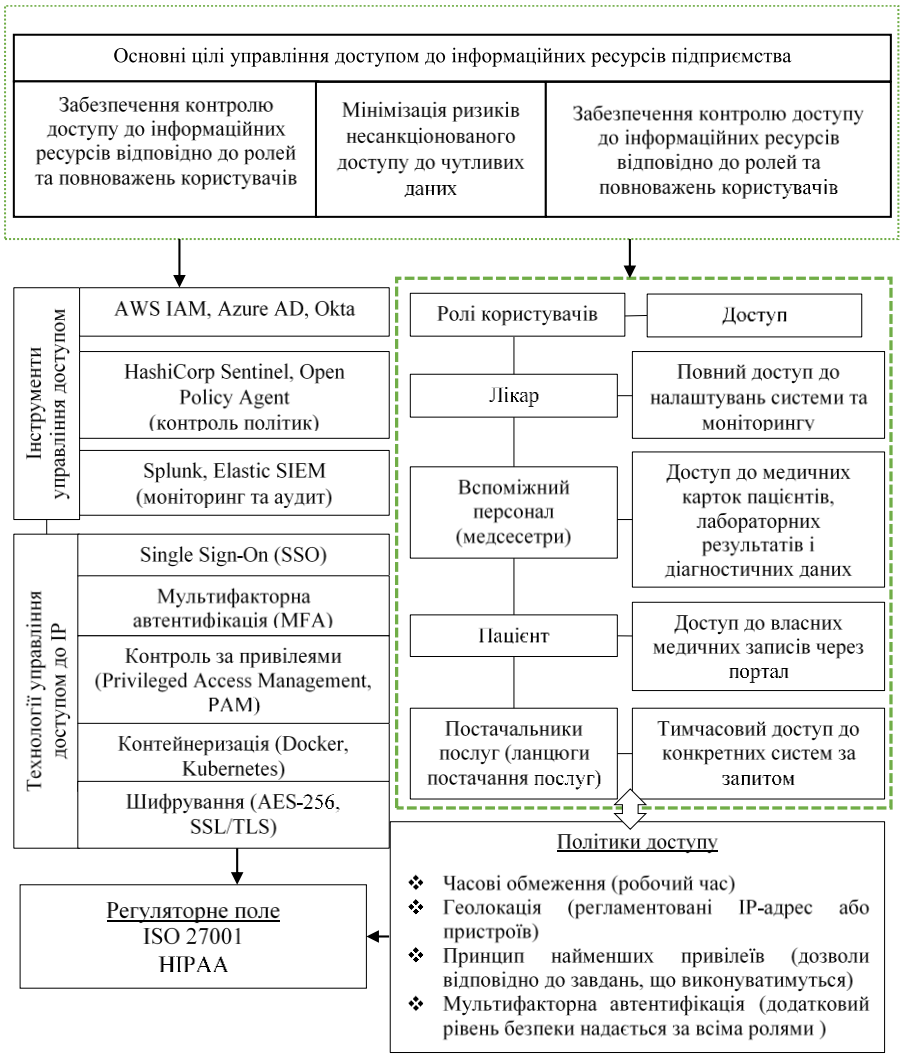

Рис. 2. Механізм управління доступом (за моделлю PACF)

Механізм передбачає використання різноманітних технологій для управління доступом, зокрема Single Sign-On (SSO) для централізованої автентифікації та зменшення складності входу в систему. Мультифакторна автентифікація (MFA) надає додатковий рівень безпеки шляхом поєднання кількох факторів перевірки: знання (пароль), володіння (мобільний пристрій) та унікальності (біометрія). Контейнеризація, базована на технологіях Docker і Kubernetes, дозволяє ізолювати окремі процеси та забезпечує безпечне середовище для виконання застосунків. Шифрування даних з використанням алгоритмів AES-256 та SSL/TLS гарантує конфіденційність інформації під час її зберігання та передачі.

Для реалізації політик доступу важливо враховувати принцип найменших привілеїв, за якого користувач отримує лише ті дозволи, які необхідні для виконання конкретних завдань. Додатковими параметрами є часові обмеження, які дозволяють доступ лише в межах робочого часу, а також геолокаційні вимоги, які обмежують підключення до системи із визначених IP-адрес або пристроїв.

Привілейований доступ контролюється через механізми управління доступом до привілейованих облікових записів (PAM), що забезпечує аудит та зниження ризиків пов’язаних з експлуатацією облікових записів з підвищеними правами. Інструменти, такі як AWS IAM, Azure AD та Okta, використовуються для централізованого управління ідентичностями користувачів, дозволяють створювати ієрархічні моделі доступу, налаштовувати політики безпеки та моніторити активність у реальному часі. Для контролю політик доступу застосовуються HashiCorp Sentinel та Open Policy Agent, які забезпечують реалізацію та дотримання правил доступу на рівні коду. Моніторинг і аудит виконуються за допомогою Splunk та Elastic SIEM, які аналізують події в системі, виявляють аномалії та надають можливості для оперативного реагування.

Інтеграція всіх компонентів механізму управління доступом здійснюється через єдину архітектуру, яка забезпечує взаємодію між компонентами. Наприклад, при вході до системи лікар спочатку проходить процес автентифікації через SSO та MFA, після чого отримує доступ лише до тих ресурсів, які визначені його роллю. Цей доступ додатково перевіряється на відповідність геолокаційним та часовим параметрам, а також політикам привілейованого управління. У разі спроби виходу за межі дозволених прав чи порушення політик система негайно повідомляє адміністратора через інструменти моніторингу, такі як Splunk, для оперативного реагування.

Використання аналітичних інструментів дозволяє виявляти підозрілі дії, наприклад, спроби доступу до даних поза межами повноважень. У таких випадках механізм автоматично блокує відповідний обліковий запис і створює запис у журналі подій для подальшого розслідування. Захист даних також включає використання контейнеризації для забезпечення ізоляції даних між різними компонентами системи. Наприклад, дані пацієнтів зберігаються у захищеному контейнері, доступ до якого можливий лише через чітко регламентовані API-виклики, що знижує ймовірність витоку даних навіть у разі компрометації однієї з частин системи.

Ефективність механізму управління доступом також залежить від регулярного перегляду та оновлення політик безпеки. Аналіз даних моніторингу дозволяє виявляти слабкі місця в архітектурі доступу та своєчасно впроваджувати необхідні зміни.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Можемо зробити висновок, що контроль доступу важливий для безпеки приватної інформації у веб-сервісах, тому співробітники служби безпеки повинні перевіряти запити на доступ до чутливих даних відповідно до встановлених критеріїв, проте адміністратори доволі часто стикаються з труднощами при налаштуванні нових параметрів доступу до конфіденційних даних, тим самим збільшуючи зусилля щодо управління в розподілених середовищах через різні вимоги до конфіденційності та постійне залучення співробітників служби безпеки. На підприємствах для забезпечення інформаційної безпеки недостатньо видалити ідентифікаційну інформацію, імена або номери соціального страхування, тож для анонімізації даних, їх захисту у відповідності із ЗУ «Про захист персональних даних» необхідно розробляти механізм управління доступом до інформаційних ресурсів підприємства, на основі моделі, яка відповідатиме вимогам законодавства щодо захисту даних, що опрацьовуються організаціями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Aristova, I. (2002*). State information policy and its implementation in the activities of the internal affairs bodies of Ukraine: organizational and legal foundations.* [diss. ... Doctor of Law: 11.00.07]
2. Moroz, V. (2020). Information resource as an object of public administration: content, principles and characteristics of the system. *Public administration: improvement and development, 1.* https://doi.org/10.32702/2307-2156-2020.1.1
3. Bays, L. R., Oliveira, R. R., Barcellos, M. P., Gaspary, L. P., & Mauro Madeira, E. R. (2015). Virtual network security: threats, countermeasures, and challenges. *Journal of Internet Services and Applications, 6(1).* https://doi.org/10.1186/s13174-014-0015-z
4. Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security, 86,* 402–418. https://doi.org/10.1016/j.cose.2019.07.001
5. Norbert, W. (2019). Cybernetics or Control and communication in the animal and the machine. MA: The MIT Press. https://doi.org/10.7551/mitpress/11810.001.0001
6. On Information, Law of Ukraine № 2657-XII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2657-12#Text
7. Swamy, A. (2022). Advance cellular networks (4G, 5G, 6G). *International journal of health sciences.* https://doi.org/10.53730/ijhs.v6ns2.7943
8. Horodyskyi, R., Vavrichen, O., & Strelbitskyi, M. (2024). Assessment of threats of information leakage through satellite communication channels. *Science and technology today, 2(30).*
9. Dudykevych, V., Mykytyn, H., Bortnik, L., & Stosyk, T. (2024), Security methodology of cyber-physical systems and the internet of things in intellectualization of infrastructure objects. *Computer systems and network, 6(1),* 44–53. https://doi.org/10.23939/csn2024.01.044
10. Lubko, D., & Miroshnychenko, M. Yu. (2024). Analysis of modern approaches and techniques in the field of information and data protection. *Bulletin of Kherson National Technical University, 1(88),* 231–236. https://doi.org/10.35546/kntu2078-4481.2024.1.32
11. Kravchuk, V. (2024). The concept of information security on the Internet. *The 8 th International scientific and practical conference "Innovative development of science, technology and education",* 757–763.
12. Vasylenko, M. (2018). Improving the cybersecurity of information and communication systems: quality in the context of improving information legislation. *Problems and judgments, 3,* 17–24.
13. Korobeinikova, T., & Yamnych, A. (2023). Information security risk assessment for personnel. *SWorldJournal, 20(01),* 43–51. https://doi.org/10.30888/2663-5712.2023-20-01-024
14. Narendra, R., Tadapaneni, Sr, & Sabri, M. (2020). Cloud computing security challenges. *SSRN Electronic Journal, 7,* 1–6.
15. Karpovych, I. M., Hladka, O. M., & Nakonechna, Y. A. (2020). Analysis of security risks of the information system at an IT-enterprise. *Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences, 5*. https://doi.org/10.32838/2663-5941/2020.5/12

16. Sopilko, I. (2021). Information security and cybersecurity: a comparative legal aspect. Scientific works of National Aviation University. Series: Law Journal "Air and Space Law", 2(59), 110–115. https://doi.org/10.18372/2307-9061.59.15603
17. About personal data protection, Law of Ukraine № 2297-VI (2010) (Ukraine). https://zakon.rada.gov.ua/laws/show/2297-17#Text
18. Fundamentals of Ukrainian legislation on healthcare, Law of Ukraine № 2801-XII (1993) (Ukraine). https://zakon.rada.gov.ua/laws/show/2801-12#Text
19. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Tetiana Kapeliushna
Doctor of Economics, Associate Professor,
Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-7490-6751
e-skr@ukr.net

Tetiana Muzhanova
PhD in Public Administration, Associate Professor,
Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-7435-0287
muzanovat@gmail.com

Tetiana Berestiana
Senior Lecture of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0007-1455-234X
berestianatv@gmail.com

Sergii Goloborodko
Senior Lecture of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0006-9892-3031
s.holoborodko@duikt.edu.ua

Diana Prymachenko
Assistant of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0003-2386-7440
primachenkodiana08@gmail.com

MECHANISM FOR MANAGING ACCESS TO INFORMATION RESOURCES AT AN ENTERPRISE

Abstract. The article discusses the issue of protecting enterprise information by controlling access to it. The main access management models are analyzed, including: Role-Based Access Control; Attribute-Based Access Control (ABAC); Identity and Access Management (IAM); Mandatory Access Control; Discretionary Access Control; Hybrid Access Management (combination of different access management approaches that allow organizations to create more flexible and effective access control strategies for information resources); Identity-Based Access Control (IBAC); Purpose-Based Access Control (PACF); Next Generation Access Control (NGAC) and Blockchain-Based Access Control, which integrate modern technologies such as blockchain and distributed systems. The advantages and disadvantages of the considered models of access management for information resources in the enterprise are presented. The Law of Ukraine "On Personal Data Protection", namely its part concerning the guarantee of preserving the privacy of information, is considered. It is noted that the Law of Ukraine on "Fundamentals of the Legislation of Ukraine on Healthcare" stipulates the rules for the treatment of patients' information by medical institution employees, which necessitates the need to determine the purposes of collecting client data and access to them. A mechanism for managing access to information resources of an enterprise (in the healthcare sector) with defined goals, tools and technologies for access management, role distribution and access policies recommended by the regulatory field is proposed.

Keywords: security; access management; enterprise security management; enterprise information security management mechanism.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Aristova, I. (2002*). State information policy and its implementation in the activities of the internal affairs bodies of Ukraine: organizational and legal foundations.* [diss. ... Doctor of Law: 11.00.07]
2. Moroz, V. (2020). Information resource as an object of public administration: content, principles and characteristics of the system. *Public administration: improvement and development, 1*. https://doi.org/10.32702/2307-2156-2020.1.1
3. Bays, L. R., Oliveira, R. R., Barcellos, M. P., Gaspary, L. P., & Mauro Madeira, E. R. (2015). Virtual network security: threats, countermeasures, and challenges. *Journal of Internet Services and Applications, 6(1)*. https://doi.org/10.1186/s13174-014-0015-z
4. Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security, 86*, 402–418. https://doi.org/10.1016/j.cose.2019.07.001
5. Norbert, W. (2019). Cybernetics or Control and communication in the animal and the machine. MA: The MIT Press. https://doi.org/10.7551/mitpress/11810.001.0001
6. On Information, Law of Ukraine № 2657-XII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2657-12#Text
7. Swamy, A. (2022). Advance cellular networks (4G, 5G, 6G). *International journal of health sciences.* https://doi.org/10.53730/ijhs.v6ns2.7943
8. Horodyskyi, R., Vavrichen, O., & Strelbitskyi, M. (2024). Assessment of threats of information leakage through satellite communication channels. *Science and technology today, 2(30).*
9. Dudykevych, V., Mykytyn, H., Bortnik, L., & Stosyk, T. (2024), Security methodology of cyber-physical systems and the internet of things in intellectualization of infrastructure objects. *Computer systems and network, 6(1)*, 44–53. https://doi.org/10.23939/csn2024.01.044
10. Lubko, D., & Miroshnychenko, M. Yu. (2024). Analysis of modern approaches and techniques in the field of information and data protection. *Bulletin of Kherson National Technical University, 1(88)*, 231–236. https://doi.org/10.35546/kntu2078-4481.2024.1.32
11. Kravchuk, V. (2024). The concept of information security on the Internet. *The 8 th International scientific and practical conference "Innovative development of science, technology and education"*, 757–763.
12. Vasylenko, M. (2018). Improving the cybersecurity of information and communication systems: quality in the context of improving information legislation. *Problems and judgments, 3*, 17–24.
13. Korobeinikova, T., & Yamnych, A. (2023). Information security risk assessment for personnel. *SWorldJournal, 20(01)*, 43–51. https://doi.org/10.30888/2663-5712.2023-20-01-024
14. Narendra, R., Tadapaneni, Sr, & Sabri, M. (2020). Cloud computing security challenges. *SSRN Electronic Journal, 7*, 1–6.
15. Karpovych, I. M., Hladka, O. M., & Nakonechna, Y. A. (2020). Analysis of security risks of the information system at an IT-enterprise. *Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences, 5*. https://doi.org/10.32838/2663-5941/2020.5/12
16. Sopilko, I. (2021). Information security and cybersecurity: a comparative legal aspect. Scientific works of National Aviation University. Series: Law Journal "Air and Space Law", 2(59), 110–115. https://doi.org/10.18372/2307-9061.59.15603
17. About personal data protection, Law of Ukraine № 2297-VI (2010) (Ukraine). https://zakon.rada.gov.ua/laws/show/2297-17#Text
18. Fundamentals of Ukrainian legislation on healthcare, Law of Ukraine № 2801-XII (1993) (Ukraine). https://zakon.rada.gov.ua/laws/show/2801-12#Text
19. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.

(cc) BY-NC-SA

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.