

*В. Бадігон, студент бакалаврату  
М. Українець, викладач  
Державний університет «Житомирська політехніка»*

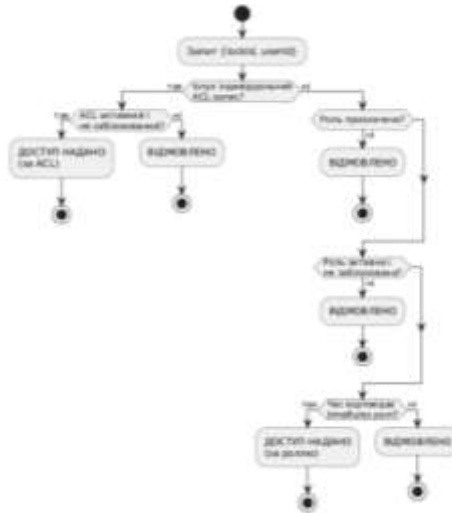
## **ГІБРИДНА МОДЕЛЬ АВТОРИЗАЦІЇ З ТЕМПОРАЛЬНИМИ ОБМЕЖЕННЯМИ ДЛЯ ХМАРНИХ ПЛАТФОРМ КЕРУВАННЯ СМАРТ- ЗАМКАМИ**

Сучасні системи фізичного контролю доступу реалізуються як розподілені Internet of Things (IoT)-платформи з централізованою авторизацією, проте класичні моделі Role-Based Access Control (RBAC) і Access Control List (ACL) не завжди відповідають вимогам динамічного середовища Інтернету речей [3].

RBAC є природною моделлю для офісного середовища з організаційними ролями, проте не підтримує часових обмежень і не дозволяє виражати індивідуальні дозволи поза межами групової політики. ACL забезпечує гранульований контроль на рівні ресурсу, проте не масштабується — адміністративні витрати зростають пропорційно добутку кількості користувачів і ресурсів [3].

Концепція часових обмежень у контролі доступу закладена в роботах Бертіно [1] і отримала подальший розвиток у моделі Temporal Role-Based Access Control (TRBAC) [2]. В IoT-контексті темпоральні обмеження набувають особливого значення: доступ технічного персоналу або тимчасових відвідувачів має бути чинним виключно протягом визначеного часового вікна. Дослідження підтверджують, що інтеграція часових обмежень у моделі авторизації суттєво підвищує безпеку та гнучкість IoT-систем без надмірного ускладнення архітектури [5]. Таким чином, жодна з розглянутих моделей окремо не забезпечує одночасно адміністративної простоти, темпоральної гнучкості та можливості гранульованих винятків. Метою цього дослідження є розробка гібридної моделі авторизації, яка поєднує переваги RBAC, темпоральних обмежень і механізму індивідуальних ACL-записів, усуваючи таким чином обмеження кожного з підходів окремо.

Пропонується гібридна модель авторизації для хмарних платформ керування смарт-замками, що поєднує RBAC із темпоральними обмеженнями на рівні ролі та механізм пріоритетних індивідуальних ACL-записів для виняткових випадків. Кожна роль містить структуру timeRules — композицію незалежних часових правил із визначеними днями тижня й часовим діапазоном, що дозволяє виражати складні розклади доступу без ускладнення схеми бази даних. Запит на авторизацію у форматі {lockId, userId} обробляється за дворівневим алгоритмом: (1) перевірка наявності індивідуального ACL-запису — якщо існує, він застосовується з найвищим пріоритетом; (2) у протилежному випадку — перевірка ролі користувача та відповідного темпорального правила з урахуванням блокувань і терміну дії. Для мінімізації затримки перевірки рекомендується кешування записів із синхронною інвалідацією при кожній зміні політики [4]. Модель має відомі обмеження: складніший аудит порівняно з чистою RBAC та ризик деградації до ACL при надмірному використанні індивідуальних винятків.



**Рис. 1** Діаграма діяльності алгоритму авторизації

У результаті дослідження запропоновано гібридну модель авторизації, що поєднує адміністративну простоту RBAC, виразність темпоральних обмежень і гнучкість гранульованого контролю через механізм індивідуальних винятків. Дворівнева ієрархія пріоритетів забезпечує баланс між керованістю системи та точністю налаштування доступу, що робить її обґрунтованим архітектурним рішенням для хмарних IoT-платформ фізичного контролю доступу в офісному середовищі. Подальше дослідження передбачає формальну верифікацію запропонованої моделі та оцінку її продуктивності в умовах реального навантаження.

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bertino E., Bettini C., Ferrari E., Samarati P. An access control model supporting periodicity constraints and temporal reasoning // ACM Transactions on Database Systems. – 1998. – Vol. 23, No. 3. – С. 231–285.
  2. Joshi J., Bertino E., Latif U., Ghafoor A. A generalized temporal role-based access control model // IEEE Transactions on Knowledge and Data Engineering. – 2005. – Vol. 17, No. 1. – С. 4–23.
  3. Ferrante A. et al. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions // Sensors. – 2023. – Vol. 23, No. 4. – 1805.
  4. Carlson J. Redis in Action. – Manning Publications, 2013.
- Krakallah M. W., Nait-Bahloul S. Hybrid Access Control Model for IoT Environments: Formalization and Verification Using Timed Automata // SN Computer Science. – 2025.