УДК 004.523
DOI: 10.31673/2409-7292.2019.043439

Л.П. Крючкова, В.О. Пшоннік, М.О. Вовк

АКУСТИЧНИЙ МЕТОД АВТОРИЗАЦІЇ В СИСТЕМАХ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Розглянуто акустичний метод авторизації в системах контролю та управління доступом. Розроблено блок-схеми алгоритмів роботи контроллера та мобільного додатку. Обґрунтовано доцільність застосування акустичного методу авторизації в сучасних СКУД.

Ключові слова: система контролю та управління доступом, авторизація, акустичний метод авторизації, блок-схема алгоритму.

Вступ

Система контролю та управління доступом (СКУД) – це програмно-апаратне рішення для організації доступу персоналу до об’єктів або приміщень на території підприємства [1,2].

Всі режими доступу, що використовуються при автоматизованому контролі, можна розбити на три групи:

- без обмеження доступу;
- доступ по праву доступу;
- заборона доступу.

Режими вільного проходу застосовуються для приміщень, доступ у які повинен бути постійно або тимчасово відкритий для всього персоналу або при аварійних ситуаціях.

Режими заборони доступу можуть застосовуватися у тому випадку, якщо необхідно запобігти доступу до всіх чи деяких приміщень (зон) на тимчасовій або постійній основі всім, крім обмеженого числа спеціально уповноважених осіб. Заборона доступу може бути плановою або екстреною, при виникненні особливих ситуацій.

Режими доступу згідно з присвоєними правами є основними в системах контролю доступу.

Спосіб надання конкретній особі прав доступу істотно впливає на надійність контролю доступу в цілому. Тому найбільш доцільно надати таку можливість тільки одному співробітнику – *Адміністратору* СКУД, який діє на основі прийнятих в організації адміністративних процедур. При цьому має бути виключена можливість зміни наданих прав іншими особами, в тому числі власниками. Стосовно автоматизованих систем це вимагає обмеження доступу до використовуваних технічних засобів.

Нажаль, комерційні організації, а тим більше самі виробники систем контролю і управління доступом не надають статистичних даних про проникнення сторонніх на об'єкти і викликані ними втрати. Але такі проникнення і втрати є, причому, досить істотні.

СКУД дозволяють здійснювати:

- обмеження доступу співробітників і відвідувачів об'єкта в приміщення, що охороняються;
- часовий контроль переміщень співробітників і відвідувачів по території об'єкта;
- контроль дій охорони під час чергування;
- табельний облік робочого часу кожного співробітника;
- фіксацію часу приходу і залишення об’єкта відвідувачами;
- часовий та персональний контроль відкриття внутрішніх приміщень (коли і ким відкриті);
- спільну роботу з системами охоронно-пожежної сигналізації та відеоконтролю (при спрацьовуванні сповіщувачів блокуються, або навпаки, наприклад, при пожежі, розблоковуються двері приміщення, що охороняється, або включається відеокамера);
- реєстрацію та видачу інформації про спроби несанкціонованого проникнення в приміщення.

Інформаційну структуру циклу управління в СКУД подано на рис.1. При цьому задачами оператора ідентифікації являються: визначення апаратного “імені людини”, її місцезнаходження, суттєвих індивідуальних ознак та фіксація часу ідентифікації (рис. 2) [3].

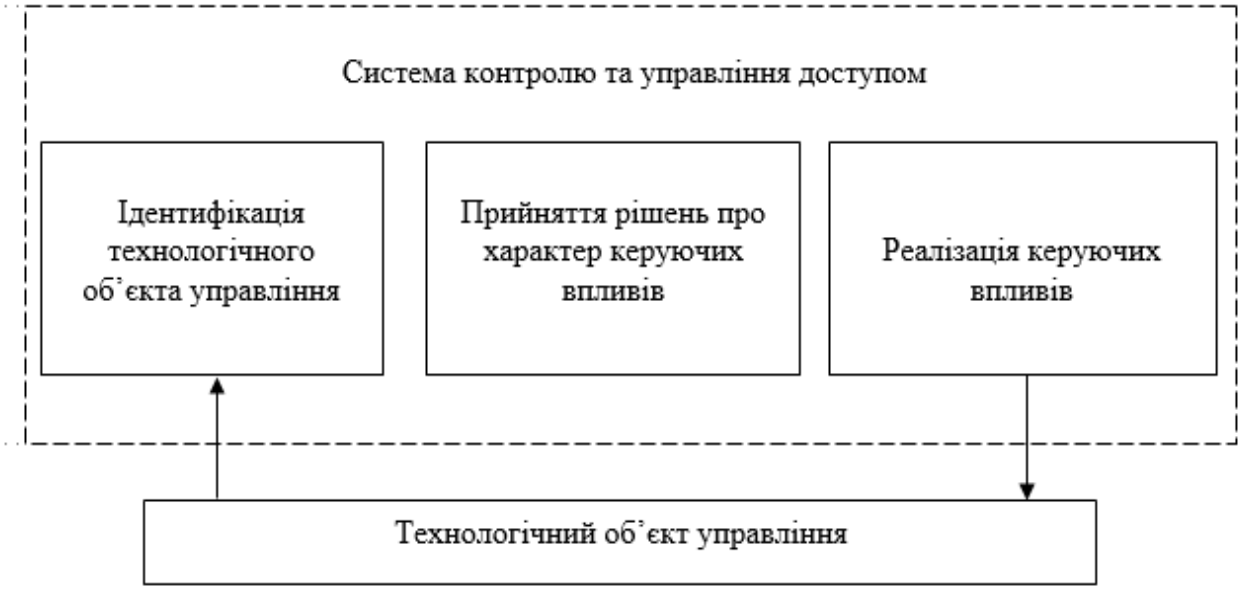

Рис. 1. Інформаційна структура циклу управління в СКУД

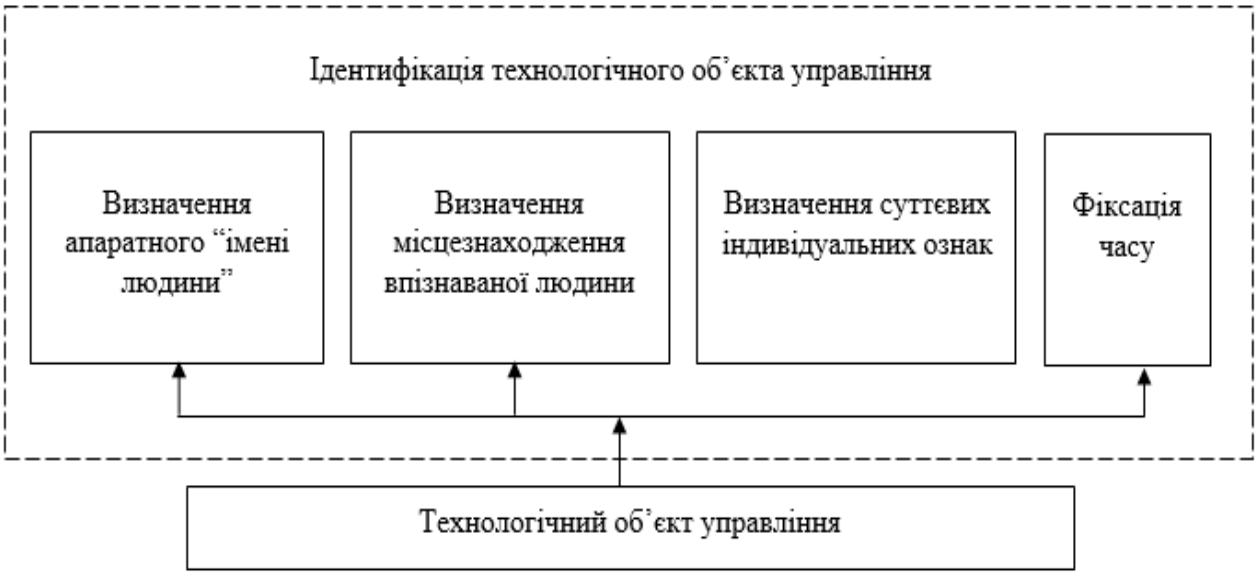

Рис. 2. Задачі оператора ідентифікації в СКУД

Способи ідентифікації користувачів СКУД можна розділити на дві групи. Першу з них утворюють способи, засновані на застосуванні зовнішніх по відношенню до користувача ідентифікаторів – електронних ключів, що містять унікальний код, який розпізнається СКУД і яким в її базі даних поставлені у відповідність персональні дані користувача. Другу групу утворюють способи ідентифікації, засновані на використанні біометричних характеристик самого користувача.

В публікації пропонується акустичний метод авторизації для систем автоматичного контролю та управління доступом персоналу до приміщень на території об'єкта.

Акустичний метод авторизації

При розробці методу було прийнято рішення розподілити різні етапи авторизації в СКУД між трьома несучими частотами.

Розподіл несучих частот:

- Частоту 19500 герц використати для передачі інформації від контролерів системи до телефонів, що її використовують задля інформування їх про вільні місця (тайм слоти) в ефірі.
- Частоту 19000 герц використати для передачі інформації від контроллерів системи до телефонів, що її використовують при встановленні сеансу зв'язку, а також для передачі інформації для телефону, коли сеанс встановлений.
- Частоту 18500 герц використати для передачі інформації від телефонів, що її використовують при встановленні сеансу зв'язку, до контроллерів системи, а також для передачі інформації для контроллерів системи, коли сеанс встановлений.

Для ускладнення обробки та аналізу інформації, отриманої в спробах перехоплення сигналів при нормальному режимі роботи пристроїв, було прийнято рішення використати асиметричне кодування інформації з урахуванням моменту самого кодування перед її відправкою акустичним каналом. Це дає змогу обмінюватись повідомленнями у ненадійному каналі передавання інформації з впевненістю в стійкості до можливого перехоплення та аналізу інформації в прийнятний для зловмисника час [4].

Система контролю та управління доступом містить:

- Сервер.
- Шлюз мобільного додатку.
- Контроллер.

Функції сервера:

- Зберігання повної бази даних користувачів системи контролю та управління доступом, а також інформації, які контроллери можуть дозволяти прохід через конкретний пропускний пункт по відношенню до кожного користувача.
- Управління контроллерами.

Функції шлюзу мобільного додатку:

- Забезпечення обміну даними між сервером контролю користувачів та контроллерів з додатками, встановленими на мобільних телефонах користувачів.

Функції контроллера:

- Дискретизація прийнятих сигналів на несучій частоті прийому.
- Відновлення дискретних сигналів перед відправкою на несучій частоті передачі.
- Зберігання локальної бази користувачів, яким дозволений прохід через конкретний пропускний пункт.
- Контроль за станом пункту проходу.

При прийнятті на роботу нового співробітника необхідно:

- Зареєструвати нового користувача в системі та встановити йому права доступу.
- Встановити додаток на його мобільний телефон.

Блок-схеми алгоритмів роботи контроллера та мобільного додатку подано відповідно на рис. 3 і рис. 4.

Рішення задачі надійності авторизації користувачів системи забезпечується за рахунок використання алгоритму асиметричного кодування з урахуванням точного часу.

Рішення задачі контролю місцезнаходження користувачів в рамках території використання системи забезпечується за рахунок завчасної авторизації телефонів в системі (рис. 3 та рис.4). Додатково це дає можливість відслідковувати спроби проходу через слабо контрольовані прохідні пункти (наприклад, двері для доступу в контрольоване приміщення) кожного користувача в групі осіб, навіть якщо лише однин з них підтвердив необхідність відкриття дверей.

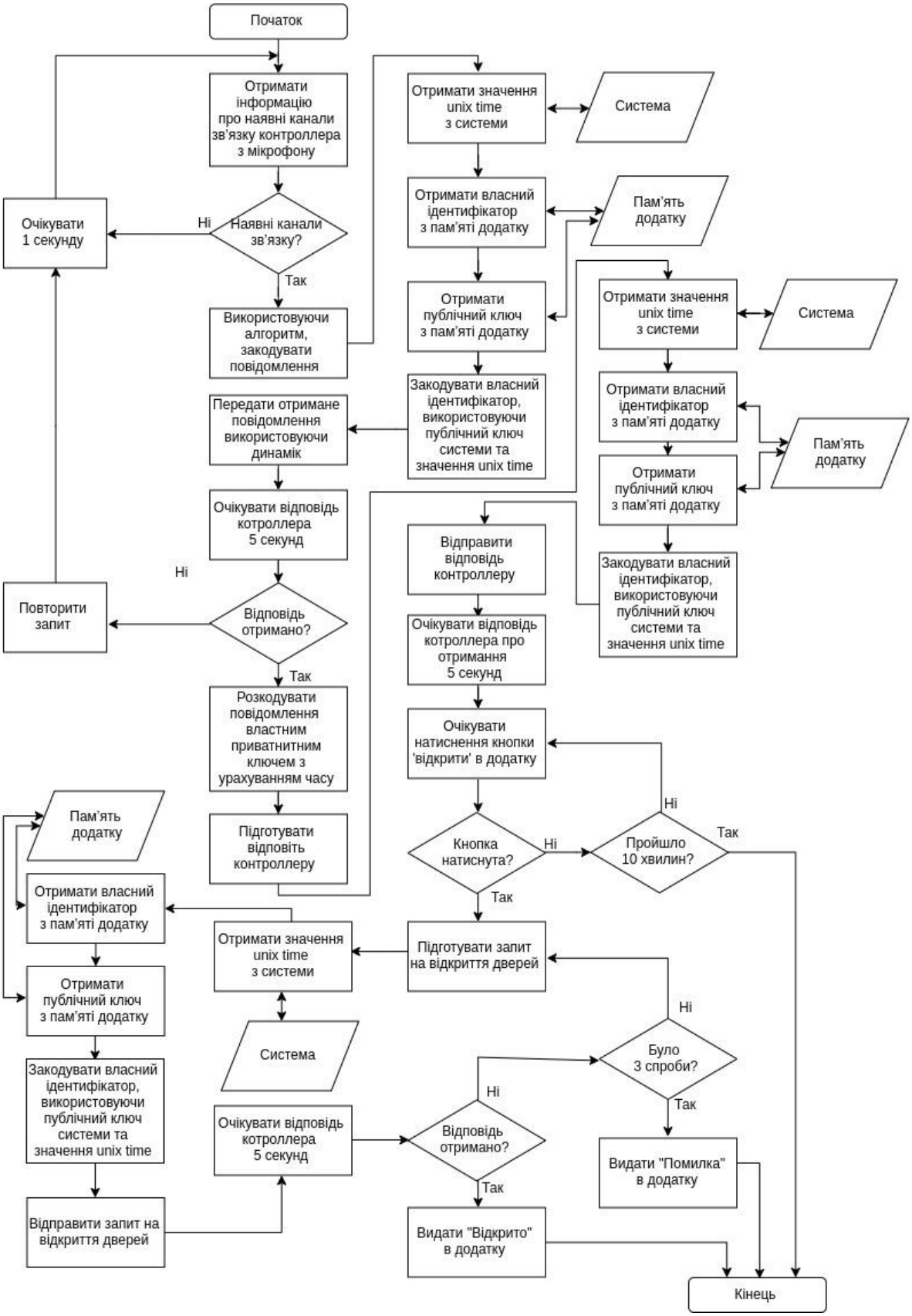

Рис. 3. Блок-схема алгоритму роботи контроллера

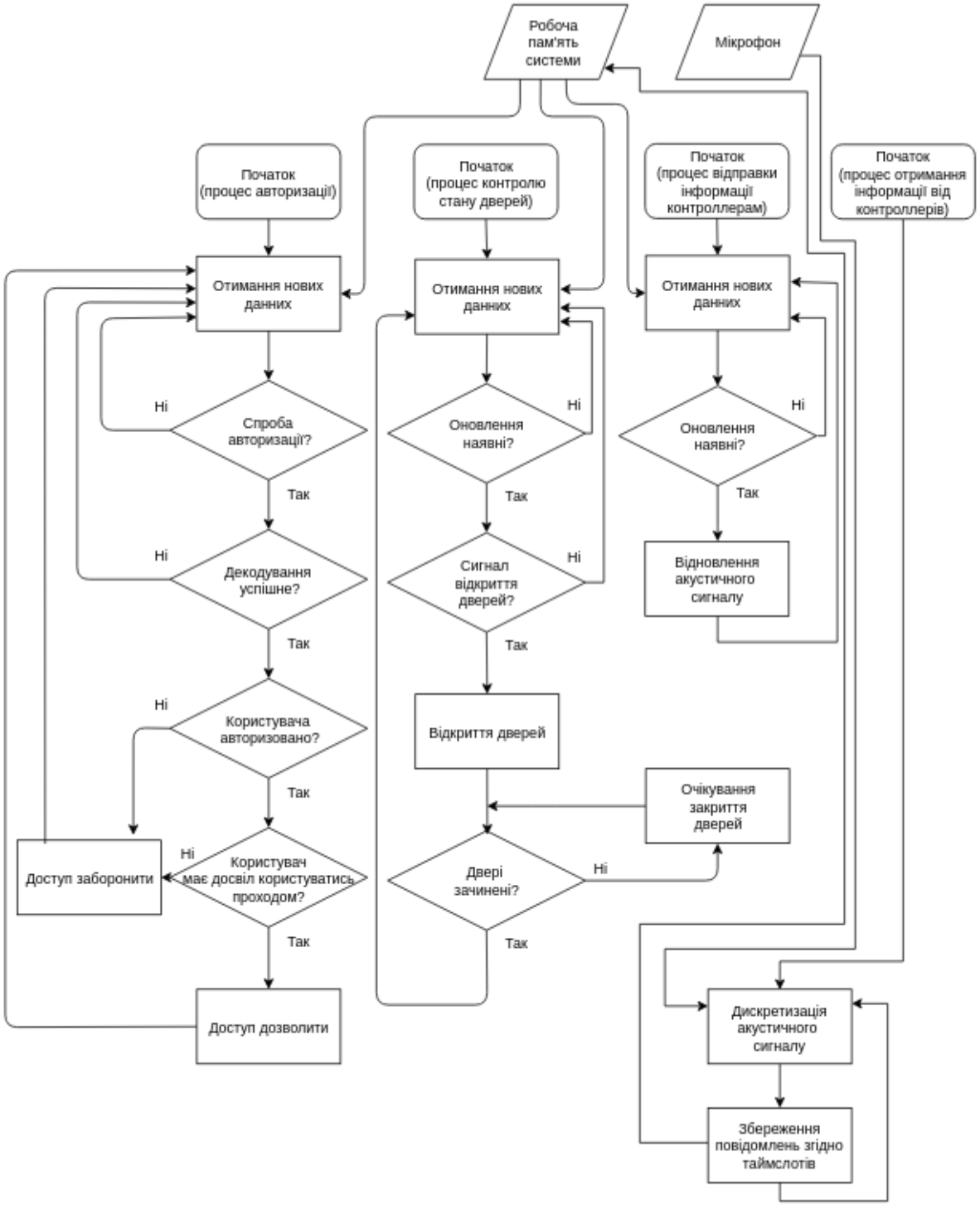

Рис. 4. Блок-схема алгоритму роботи мобільного додатку

Сервер контролює робочі параметри контроллера системи. Мобільні додатки, встановлені на телефонах користувачів, оновлюють робочі дані, необхідні для роботи системи, один раз на годину. Оновлення робочих даних мобільних додатків відбувається по каналах передачі даних телефонної мережі.

Узагальнена структурна схема системи контролю та управління доступом з використанням акустичного методу авторизації представлена на рис. 5:

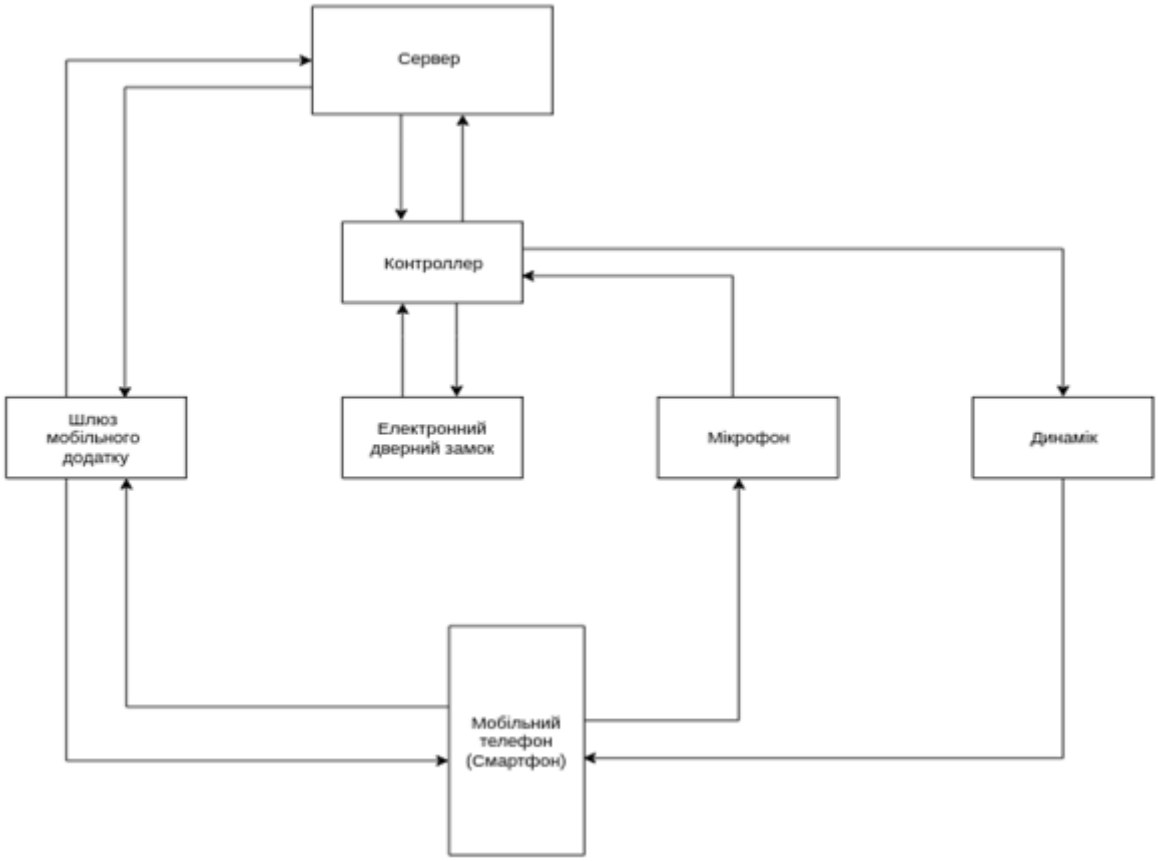

Рис. 5. Узагальнена структурна схема системи контролю та управління доступом з використанням акустичного методу авторизації

Сукупність описаних рішень надає можливість звести використання системи контролю та управління доступом до простого натискання клавіші “Відкрити” в мобільному додатку на власному телефоні, перебуваючи перед пунктом проходу, а також контролювати прохід неавторизованих користувачів, через пункти контролю доступу.

Висновки

Розглянута система контролю та управління доступом з використанням акустичного методу авторизації забезпечує надійність та захищеність авторизації користувачів, здатна оцінювати місце перебування співробітника, що користується мобільним додатком відносно наявних акустичних випромінювачів при переміщенні по території підприємства.

Перелік посилань

1. В.Л. Джхунян, В.Ф. Шаньгин. Электронная идентификация. Бесконтактные идентификаторы и смарт карты. – М.: «Издательство АСТ»: Издательство «НТ Пресс», 2004.

2. K. Finkenzeller. RFID handbook: radiofrequency identification fundamentals and applications Translated by R. Waddington J.: Wiley & Son, Ltd, 2009.

3. Крючкова Л.П. Системный поход к решению проблемы защиты информации на объектах информационной деятельности // Інформаційна безпека. Східноукраїнський національний університет ім. В. Даля №2 (6). – 2011. – С. 5 – 7.

R.A. Kleist, T.A. Chapmen et.al. RFID Labeling: Smart Labeling Concepts & Applications for the Consumer Packaged Goods Supply Chain .: Printronix, Inc., 2004.

Надійшла: 07.10.2019 Рецензент: д.т.н., доцент Гайдур Г.І.