УДК 004.382.7

DOI: 10.31673/2412-9070.2023.052022

В. М. ДАНИЛЬЧЕНКО, ст. викладач,
Державний університет інформаційно-комунікаційних технологій, Київ

ДОСЛІДЖЕННЯ МОБІЛЬНОЇ ОНЛАЙН-СИСТЕМИ БЛОКУВАННЯ МІКРОКОМП'ЮТЕРА НА ОСНОВІ ТЕХНОЛОГІЇ NFC

На сучасному етапі енергетична промисловість стрімко розвивається, потужність мереж розширюється, а ступінь автоматизації постійно зростає. Також підвищуються вимоги до процесів перемикання, перевірки та усунення несправностей електричного обладнання. Розширення потужності мереж і автоматизація зумовлюють використання складніших систем та обладнання, посилюючи вимоги до знань, навичок операторів мережі, а також до використовуваних ними інструментів та технологій. У статті розглянуто технологію NFC (Near Field Communication) — нове покоління п'ятиступеневої системи онлайн-мікрокомп'ютера на базі платформи Qt для смартфонів Android із використанням NFC. Ця конструкція здатна вирішити проблему, коли оператор не може спілкуватися та обмінюватися даними в реальному часі на місці події, використовуючи традиційну онлайн-мікрокомп'ютерну п'ятиступеневу систему під час операцій перемикання. Традиційна онлайн-мікрокомп'ютерна п'ятиступенева система ускладнює спілкування та обмін даними операторів мережі в реальному часі на місці події. Це може створити проблеми, якщо операторові потрібна інформація або допомога під час виконання операцій перемикання. Мобільна онлайн-мікрокомп'ютерна система блокування для запобігання неправильній роботі поліпшить інформаційну систему та інтелект традиційної мікрокомп'ютерної системи з п'ятьма рівнями захисту та удосконалить функціональність використання на місці.

Ключові слова: мікрокомп'ютер; NFC; мережа; п'ятиступенева система безпеки; мобільна система.

Вступ

Комп'ютерний ключ широко застосовується в системі блокування від неправильного спрацьовування. За цими правилами, оператор спочатку має попередньо переглянути весь процес операції перемикання на хості захисту від пропусків, а потім створити квиток операції. Якщо помилка виправлення виникає під час репетиції, операційний квиток не буде згенеровано. Потрібно передати та підказати вміст помилки та запропонувати кроки, які мають бути змінені [4]. Після завершення репетиції квиток операції імпортується в ключ комп'ютера-адаптера, а оператор може перенести ключ комп'ютера на місце для здійснення фактичного перемикання операції. На кожному етапі роботи перемикача спочатку потрібно виконати завдання розблокування за допомогою комп'ютерного ключа і відкрити замок, відповідний силовому обладнанню, щоб продовжити роботу електроживлення обладнання. Якщо замок, який відкривається комп'ютерним ключем, не відповідає обладнанню, яке має спрацювати, замок примусово блокується, і водночас ключ від комп'ютера видає тривогу, в такий спосіб уникаючи настання аварії [3].

Під час зміни режиму роботи та керування електромережею попередження помилок системи широко застосовується в енергосистемі і перебуває в стані постійного оновлення. Нині безпроводову базову станцію може бути встановлено на всій території, як у приміщенні, так і за його межами. Крім того, розроблено п'ятизахисну систему на базі безпроводової мережі для поліпшення керування енергетичним обладнанням [1]. Комунікаційні та керувальні функції ЕОМ використовуються разом із функцією судження мікроконтролера для реалізації системи запобігання помилкам [2]. Система онлайн-контролю блокування розвиває режим центру керування мережею, централізованого контролю та єдиного керування. Вона також реалізує централізовану п'ятирівневу систему [3]. У фактичному процесі використання поточної мікрокомп'ютерної технології з п'ятьма стійками всі дані мають рівномірно контролюватися в межах головної станції. Функції попереднього перегляду операцій, бібліотеки квитків керування та запити, налаштування бази логічних правил та інші аспекти також мають бути реалізовані на головній станції.

Аналіз дослідження. Залежність станції є сильною, що ускладнює дистанційне використання технології п'яти захистів та обмежує можливість розширення функціонала системи на мобільних пристроях. Смартфони зараз активно використовуються в мережному бізнесі та керуванні, ставши новою формою розвитку та застосування електромереж.

Роль клієнта мобільного телефона поступово змінюється на нову модель сучасного соціального розвитку. Ця концепція використовує смартфон із підтриманням NFC замість традиційного комп'ютерного ключа. Розроблено мобільний клієнт на основі Qt для платформи Android, що реалізує функції онлайн-мобільної п'ятизахисної системи та пасивного блокування NFC, що більш ефективно розв'язує зазначені проблеми.

Метою дослідження є розроблення системи блокування, спрямованої на більш ефективне запобігання аваріям. Цю систему буде створено через розподіл функцій між різними станціями для додаткової перевірки та автоматичного перемикання.

© В. М. Данильченко, 2023

Основна частина

Логічна структура мобільної онлайн-системи блокування від неправильної роботи ґрунтується на технології NFC. Застосування цієї конструкції на основі оригінальної онлайнової системи блокування робить процес більш гнучким завдяки використанню технології NFC. Операція перемикання стає зручною та надійною, що робить застосунок системи блокування від неправильної роботи більш різноманітним [5]. Схему модифікованої системи блокування, яка базується на традиційній онлайн-системі блокування проти неправильного спрацьовування на основі технології NFC, зображено на рис. 1.

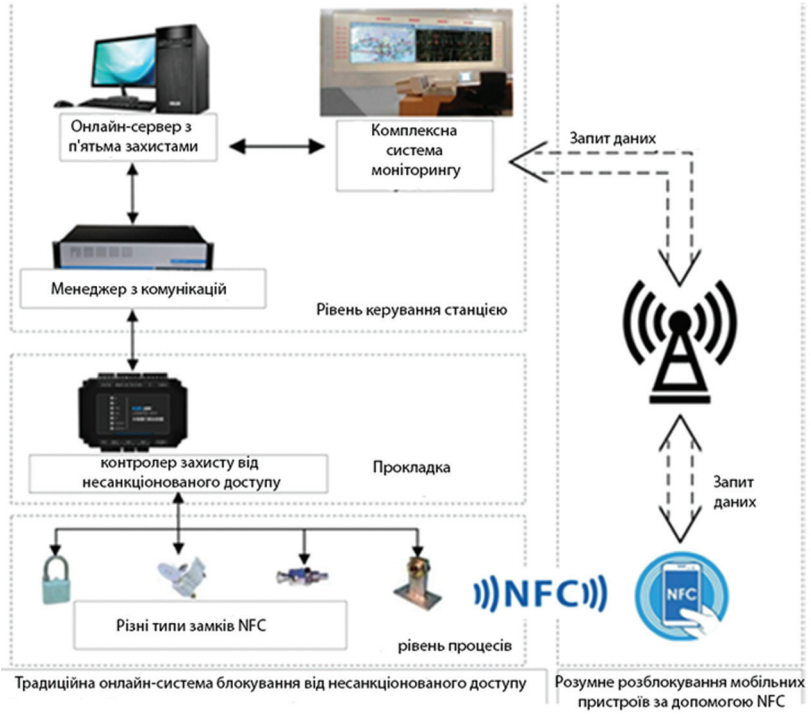

Рис. 1. Структурна схема онлайн-системи захисту від неправильного спрацьовування на основі технології NFC

Внутрішню схему замка вбудовано в схему NFC для забезпечення зв'язку між замком та мобільним телефоном, що має функцію NFC. Це дає змогу мобільному телефону з NFC замінити звичайний комп'ютерний ключ. Оператор використовує мобільний телефон із NFC для отримання квитка на операцію через управлінський центр. Щораз, коли завдання розблокування завершено, мобільний телефон із NFC має бути поблизу замка, під'єднуватися до схеми NFC замка та ідентифікувати його код. Якщо це підтверджено як цільовий замок, то мобільний клієнт повідомляє системі про результат розпізнавання. Після того, як п'ять систем захисту підтвердять коректність логіна, видається команда контролеру розблокувати захист від неправильної роботи для розблокування замка [4].

Головний пристрій постійно генерує радіочастотне поле. Коли його розміщено поблизу підпорядкованого пристрою, це поле індукує напругу на котушці підпорядкованого пристрою для його живлення. Завдяки технології модуляції навантаження підлеглий пристрій визначає швидкість передавання даних і досягає узгодженості з головним пристроєм. Внутрішню схему інтелектуального замка NFC унаочнює рис. 2. Оскільки існує багато типів розумних замків, зокрема механічних навісних, електричних, електромагнітних замків тощо, то внутрішню комунікаційну частину NFC розроблено саме для такого типу схеми.

Внутрішня частина розумного замка переважно має у своєму складі котушку антени, пасивний давач температури MAX66242 I^2C та SD5075.

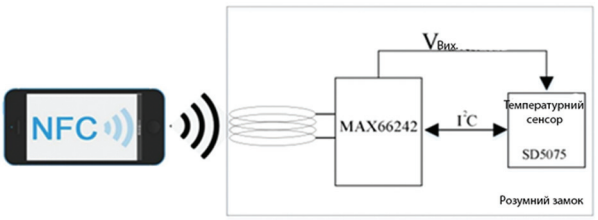

Рис. 2. Схема розумного замка

Котушка антени є носієм для передавання енергії та інформації між смартфоном і замком. Реалізовано лише оптимальну структуру радіочастотної схеми для максимального передавання радіочастотної енергії, а пасивна мікросхема є більш ефективною для здобуття енергії. Ефективність передавання радіочастотної енергії здебільшого залежить від резонансного режиму та точності резонансу схеми NFC:

$$f = \frac{1}{2\pi\sqrt{LC}}, \qquad (1)$$

$$L = \frac{1}{4\pi^2 f^2 C}, \quad (2)$$

де f — резонансна частота; L — індуктивність котушки; C — резонансний конденсатор. Резонансний конденсатор і котушка в резонансному контурі MAX66242 працюють на частоті 13,56 МГц з резонансною ємністю конденсатора 21 pF. Згідно з рівнянням індуктивність котушки становить 6,56 МГц. Беручи до уваги вплив замкового металу на резонансну частоту, індуктивність котушки тут збільшується до 6,78 МГц, а ефективність передавання енергії є оптимальною. MAX66242 — це пасивний чіп, який безпосередньо спілкується із зовнішніми смартфонами без потреби в зовнішньому джерелі живлення або з мікропроцесором. MAX66242 інтегрує механізм шифрування SHA-256 для двосторонньої безпечної автентифікації з мобільними телефонами. Отже, безпеку зв'язку гарантовано. Внутрішній ідентифікатор ROM — це унікальний 64-бітовий серійний номер, який було вбудовано в процес виробництва для забезпечення унікальності розпізнавання блокування. У MAX66242 невикористана енергія від випрямляча може бути виведена на периферійну схему через контакт V_{out}, живлення зовнішнього давача температури SD5075 і обмін даними з давачем здійснюється через інтерфейс I^2C для інформації про температуру.

Платформа *Qt* для смартфонів Android — це програмна клієнтська платформа для розгортання програм *Qt* на мобільних телефонах Android на основі мови програмування C/C++ [4]. Ця конструкція застосовує *Qt* Creator для розроблення прикладного інтерфейсу п'яти систем захисту та восьми функціональних програм у фоновому режимі, а також реалізує мобільні телефони через архітектуру C/S (клієнт – сервер). Мережний обмін даними відбувається між клієнтом та п'ятьма антисерверами. Архітектуру програмного забезпечення для п'ятизахисної системи мобільного клієнта зображено на рис. 3.

Як унаочнює рис. 3, архітектуру програмного забезпечення мобільного клієнта поділено на три рівні: рівень даних, логічний рівень і прикладний рівень. База даних є основою рівня даних, що обробляє та оновлює інформацію. Дані, що надійшли з пристроїв мережних каналів, проходять через рівень даних [3]. Система взаємодії даних інтегрує всі компоненти в одну систему. Логічний рівень відповідає за аналіз функціональних вимог та логічні операції, різноманітність функцій пристосовується під конкретні запити клієнтів. Прикладний рівень об'єднує вісім ключових п'ятифункціональних прикладних функцій, які мають розширені можливості та охоплюють усі необхідні можливості системи. Користувачі отримують операційні права для відвідування та роботи. Лише санкціоновані користувачі можуть зареєструвати та використовувати функціонал, відповідно до їхніх повноважень. Однією з основних та важливих функцій є керування квитками та виконання вправ. Це найбільш потужна функція серед п'яти систем захисту. Клієнт відповідає за перегляд, генерацію, запит, виклик та повернення квитка операції, що є базою для реального перемикання дій.

Кожен запит на операцію ретельно прокладається через п'ять ліній захисту, забезпечуючи безпеку операції перемикання. Для реалізації функції реального часу мобільного термінала клієнт взаємодіє з базою даних у режимі реального часу, щоб мати актуальний стан основного пристрою та інтелектуального замка п'ятизахистної системи. Це дає змогу оновлювати дані клієнта та надавати оператору актуальну інформацію для планування. Оператор має можливість виконувати такі функції:

- швидко викликати фонову схему підімкнення, переглядати поточний стан обладнання та планувати поточну роботу;
- визначати однозначність роботи обладнання, уникати використання одночасно кількох опера-

Рис. 3. Архітектура програмного забезпечення мобільного клієнта

ційних квитків на одному замку та енергетичному обладнанні, а також зважати на стан замка та обладнання, запобігаючи невизначеності та виникненню конфліктів;

• завдяки логіці п'ятизахисної системи оцінювати поточну операцію в реальному часі.

Процес розблокування та блокування п'ятизахисної системи мікрокомп'ютера показано на рис. 4. Подібно до інших мобільних клієнтських програм, оператор має ввести свій обліковий запис та пароль в інтерфейсі входу користувача для входу в операційну систему. Після успішного входу клієнт мобільного телефона встановлює зв'язок із п'ятьма антисерверами, синхронно відстежує дані поточного стану пристрою живлення й інтелектуального замка та оновлює дані в реальному часі. Після завершення оновлення бази даних клієнта пристрій живлення, підімкнений до основного електропроводу системи живлення, у графічному інтерфейсі клієнта відображає фактичний поточний стан, а інтерфейс клієнта інтуїтивно відображає робочий стан енергосистеми.

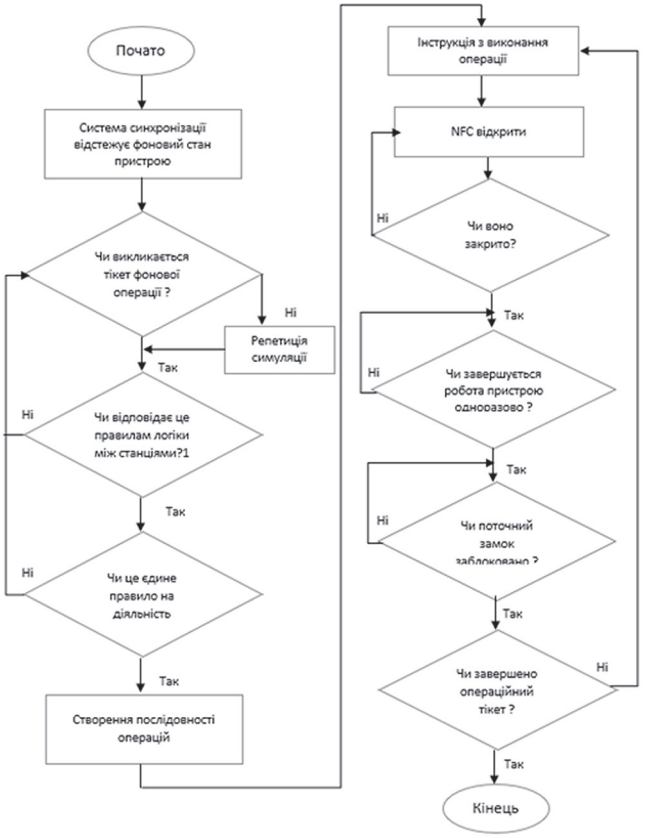

Рис. 4. Процес розблокування системи

Існують два методи виклику квитка операції комутатора [4]. Перший метод передбачає виклик заявки на операцію, яку було згенеровано та затверджено в бібліотеці заявок. Другий метод дає змогу використовувати функцію попереднього перегляду на мобільному клієнті для створення квитка операції на місці. Незалежно від того, чи генерується заявка на операцію на сервері блокування або завершується на мобільному клієнті, оператор має унікальні повноваження на керування пристроєм, до якого застосовується операція. Кожен крок, незалежно від реалізації попереднього перегляду на сайті, має бути оцінений базою правил фонової логіки. Операція, яка відповідає п'ятьом правилам антилогіки, може бути пропущена до виконання наступної операції. Якщо операція не відповідає логіці п'яти захистів, вона не може продовжувати репетицію, і з сигналом тривоги квиток операції врешті-решт не буде згенеровано.

Оператор викликає згенерований квиток операції на місці за допомогою мобільного телефона NFC і здійснює операцію перемикання відповідно до кроків розблокування, керування пристроєм, підтвердження статусу пристрою та блокування. Режим розблокування NFC передбачає, що передня частина програми NFC мобільного телефона ідентифікує ідентифікатор внутрішньої схеми NFC замка. Клієнт визначає, чи є поточний розумний замок тим, керування яким планується за допомогою ідентифікатора. Ідентифікація може передати сигнал на хост-систему для надання команди контролеру блокування для розблокування замка [3]. Під час роботи обладнання можуть виникати ситуації, коли воно не функціонує належним чином. Онлайн-система п'яти перевірок контролює стан обладнання в режимі реального часу. У разі такої ситуації виконання операційного квитка призупиняється. Після завершення роботи пристрою замок має бути знову заблокований, забезпечуючи блокування для наступного завдання. Фонова система також моніторить поточний стан замка, щоб запобігти його неправильній установці.

Висновок

Сучасні наука та технології стали основними моторами стрімкого розвитку суспільства. Цей шлях трансформував енергетичні мережі в «інтелектуальні» та «безпілотні», зумовлюючи появу більших вимог до систем блокування мікрокомп'ютерів, які забезпечують надійність роботи. У статті було запропоновано використання клієнта смартфона для збереження стабільності електромережі. Також розглянуто реалізацію клієнта мобільного телефона на платформах *Qt* і Android, розвиток восьми функцій п'ятизахисної системи мобільного термінала та застосування технології NFC для розблокування передньої частини мобільного телефона.

Список використаної літератури

*1. **Wang M. S., Guo Y. X., Wu W.** Near-field and far-field shared structure for NF Cand CNSS appli-*

cations // Iet Microwaves Antennas & Propagation. 2020. 11(15).

*2. **Wu D. Z.** Design and Application for Five Anti-wireless System on Beijing Taiyanggong Power Plant [D]. North China Electric Power University, 2019.*

*3. **Павлиш В. А., Гліненко Л. К., Шаховська Н. Б.** Основи інформаційних технологій і систем. 2018.*

*4. **Congwei Hu, Wu Chen, Shan Gao.** Data Processing For GPS Precise Point Positioning // Transactions of Nanjing University of Aeronautics & Astronautics. 2020. 22(2).*

*5. **Матвієнко М. П., Розен В. П., Закладний О. М.** Архітектура комп'ютера. 2019.*

V. Danylchenko

RESEARCH ON A MOBILE ONLINE MICROCOMPUTER LOCKING SYSTEM BASED ON NFC TECHNOLOGY

Currently, power grid sector is experiencing rapid development. The scale of the network is increasing and the degree of automation is being implemented. With these changes, the requirements for switching, testing equipment, and troubleshooting electrical equipment are increasing. A traditional tamper-proof system that uses computer keys has a number of limitations. For example, it does not provide sufficient mobility, after which the operators must be within range of the computer. In addition, this system may be vulnerable to attacks. This article proposes a new generation of five online microcomputer anti-blocking systems based on NFC (Near Field Communication) technology. This system has a number of advantages compared to the traditional system: mobility allows them to work in any place where there is access to the network, informativeness allows them to make a more informed decision, intelligence to completely prevent accidents, safety allows to prevent false activation of equipment. This project applies the smart phone client to the anti-missing lock function of the power grid, develops the mobile phone client on the Qt on Android platform, builds and perfects the eight functions of the mobile terminal five-proof system, and applies the NFC technology to unlock the mobile phone front end. The skill of the client and the mobile phone are skillfully combined to solve the problem that the data communication between the personnel and the background is difficult. A new NFC-based tamper-proof system is a promising solution that has the potential to revolutionize the power grid industry. This system has several advantages over the traditional system and can help operators make switching operations safer, more efficient and more economical.

Keywords: microcomputer; NFC; network; five-security system; mobile system.