УДК 004.056.5

В.М. Білоус[1]
О.О. Кметюк[1]
О.В. Кириченко[2]

ПІДВИЩЕННЯ ЗАХИСТУ ВІД НСД УДОСКОНАЛЕННЯМ СИСТЕМИ МОНІТОРИНГУ УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ ШИФРУВАННЯ ДАНИХ ТА РЕЗЕРВНОГО КАНАЛУ

[1]Вінницький Національний технічний університет
[2]Вінницький інститут конструювання одягу і підприємництва

Анотація

Робота присвячена вдосконаленню системи контролю та управління доступом (СКУД) для підвищення захищеності від несанкціонованого доступу. Враховуючи зростання кіберзагроз, у роботі запропоновано комплексний підхід до забезпечення безпеки на основі використання резервного каналу зв'язку GSM та шифрування даних алгоритмом AES.

Проведено аналіз можливостей вдосконалення системи шляхом запровадження автоматичного перемикання на резервний канал зв'язку при збої основного, що забезпечує безперервність роботи. Алгоритм шифрування AES обрано для забезпечення конфіденційності та цілісності інформації, а також для відповідності сучасним стандартам безпеки.

Підсумкові результати демонструють, що така система здатна забезпечити високу стійкість до загроз, безперервність доступу та легку адаптивність до нових вимог.

Ключові слова: система контролю та управління доступом (СКУД), резервний канал зв'язку, захист від несанкціонованого доступу, GSM, шифрування AES.

Abstract

The work is devoted to the improvement of the access control and management system (ACMS) to increase protection against unauthorized access. Taking into account the growth of cyber threats, the work proposes a comprehensive approach to ensuring security based on the use of a backup GSM communication channel and data encryption with the AES algorithm.

An analysis of the possibilities of improving the system by introducing automatic switching to a backup communication channel in case of failure of the main one, which ensures continuity of work, was carried out. The AES encryption algorithm is chosen to ensure the confidentiality and integrity of information, as well as to meet modern security standards.

The final results demonstrate that such a system is able to provide high resistance to threats, continuity of access and easy adaptability to new requirements.

Keywords: Physical Access Control System (PACS), redundant communication channel, tamper protection, GSM, AES encryption.

Вступ

В умовах стрімкого зростання складності та масштабів кіберзагроз питання захисту інформації від несанкціонованого доступу (НСД) і безперервності роботи систем набуває все більшої актуальності. Сучасні виклики, такі як блокування основних каналів зв'язку чи перехоплення даних, потребують рішень, які не лише реагують на загрози, але й передбачають їх, забезпечуючи проактивний захист. Підприємства та організації, які працюють із конфіденційними даними, потребують ефективних рішень для забезпечення безпеки, тому вдосконалення систем контролю та управління доступом є ключовим елементом у побудові надійної інформаційної інфраструктури.

Результати дослідження

Пропонується підвищення захищеності системи контролю і управління доступом (СКУД) від несанкціонованого доступу [1] за рахунок вдосконалення безпеки через використання резервного каналу зв'язку, який здатний автоматично активуватися в разі блокування основного та шифрування даних, щоб забезпечити конфіденційність та цілісність інформації.

Основні вимоги до резервного каналу:

- забезпечення безперебійного зв’язку при збоях основного каналу;
- максимальна швидкість автоматичного перемикання на резервний канал у випадку блокування або відмови основного каналу;
- шифрування даних сучасним криптографічним алгоритмом без суттєвого впливу на швидкодію системи.

При виборі технологій для резервного каналу зв'язку серед доступних варіантів пропонуються Ethernet та GSM, кожен із яких має свої переваги та недоліки залежно від умов використання. Ethernet забезпечує стабільність зв’язку в середовищах із електромагнітними перешкодами, тоді як GSM забезпечує більшу мобільність і гнучкість, що є перевагою у віддалених місцях або в умовах, де прокладання кабелів обмежене.

Серед існуючих алгоритмів шифрування обирається AES як найбільш оптимальний варіант [2]. Це симетричний алгоритм, що забезпечує високу швидкодію та підтримку в багатьох сучасних апаратних платформах, дозволяючи системі функціонувати ефективно навіть за високих вимог до безпеки.

Вибір GSM для резервного зв’язку та AES для шифрування даних пропонується як найбільш доцільне рішення для покращення захисту від несанкціонованого доступу. Поєднання GSM та AES створює ефективний та стійкий підхід до забезпечення безпеки системи контролю доступу, що здатне забезпечити безперервну роботу системи навіть у випадку збоїв основного каналу, зберігаючи високу конфіденційність і доступність даних у будь-яких умовах. GSM забезпечує резервний канал для підтримання стабільного зв’язку, а AES гарантує надійне шифрування даних з високою швидкістю обробки, що є критичним для захисту інформації (рис. 1).

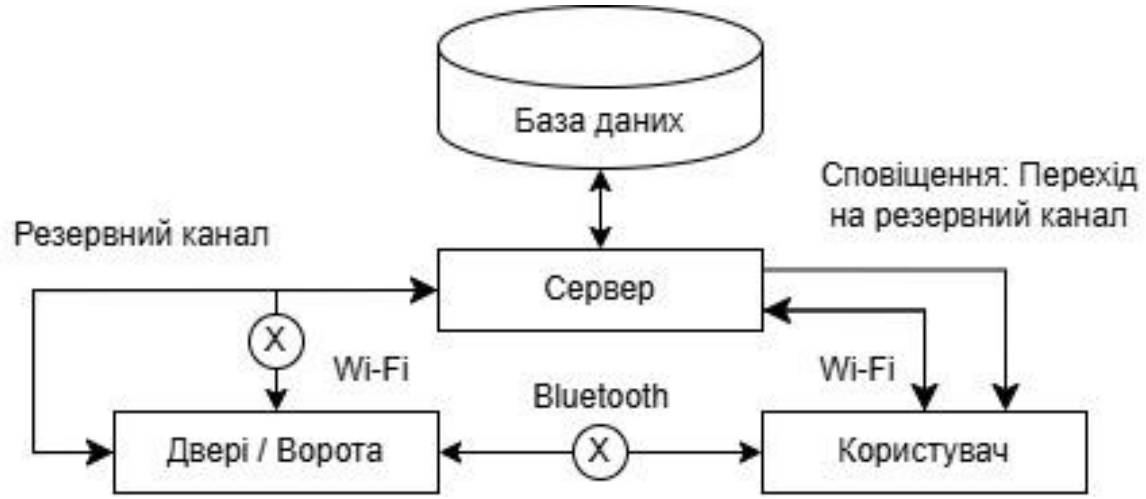

Рис. 1. Принцип роботи вдосконаленої СКУД при атаці на основні канали зв’язку

При виборі конкретних елементів для реалізації апаратної частини системи резервного каналу зв’язку обрано GSM-модем Quectel EC25 [3] завдяки його можливості працювати у різних мережевих діапазонах та функцією автоматичного перемикання між мережами, що значно підсилить стійкість системи контролю доступу до зовнішніх і внутрішніх загроз, забезпечать надійність і стабільність зв’язку у ситуаціях, коли основний канал зв’язку недоступний.

Переваги обраного GSM-модему:

- підтримка різних стандартів мобільного зв’язку, включно з GSM, WCDMA та LTE, що дозволяє забезпечити стійкий зв’язок у різних умовах;
- автоматичне перемикання між мережами, яке є важливим для безперебійного функціонування системи;
- висока швидкість передачі даних, що дозволяє підтримувати ефективну комунікацію;
- низьке енергоспоживання, що дозволяє працювати в режимі очікування протягом тривалого часу;
- можливість використання додаткового джерела живлення, яке забезпечить роботу системи у випадку збоїв у постачанні енергії.

Алгоритм роботи вдосконаленої СКУД з резервним каналом передбачає кілька важливих етапів:

1. Виявлення блокування основного каналу – постійний моніторинг для фіксації зниження пропускної здатності чи втрати зв’язку.

2. Перехід на резервний канал – автоматичне перемикання на резервний канал у разі виявлення проблем з основним.

3. Ініціація сповіщень – інформування адміністраторів про інцидент та перехід на резервний канал.

4. Збереження журналу подій – ведення запису всіх інцидентів для подальшого аналізу.

5. Відновлення основного зв’язку – повернення до основного каналу після стабілізації ситуації.

Таким чином, описані рішення формують надійну основу для розробки сучасної СКУД, здатної забезпечити захищеність даних і безперервність доступу навіть у разі атак чи технічних збоїв.

Моніторинг і реагування на збої включає механізми автоматичного виявлення відмов і швидкого перемикання на резервний канал GSM, що забезпечує безперервність роботи розробленої системи у разі атак або технічних проблем. Система сповіщення миттєво інформує адміністратора про інцидент, надаючи йому можливість оперативно реагувати та усувати проблеми.

Резервне джерело живлення додатково підвищує надійність системи, забезпечуючи її автономну роботу у випадку відключення електроенергії. Це гарантує, що система контролю доступу залишатиметься функціональною і захищатиме об’єкт навіть при критичних обставинах.

Таким чином, розроблена система контролю доступу з резервним GSM-каналом і алгоритмом шифрування AES є комплексним рішенням, що забезпечує надійність і стійкість до виникаючих кіберзагроз. Система здатна виявляти блокування основного каналу, швидко відновлювати зв'язок через резервний канал, а також забезпечувати конфіденційність та цілісність даних завдяки AES-шифруванню, що створює основу для стабільної та ефективної роботи.

Розглянемо більш детально ці важливі аспекти:

1. Масштабованість і адаптивність системи – обрані компоненти дозволяють легко провести адаптацію системи до нових вимог, таких як розширення мережевих можливостей чи оновлення програмного забезпечення для покращення захисту.

2. Стійкість до атак та забезпечення конфіденційності даних – алгоритм шифрування AES ефективно захищає дані від перехоплення і несанкціонованого доступу, а використання GSM як резервного каналу дозволяє системі зберігати функціональність навіть під час атак на основний канал зв’язку.

3. Система моніторингу та аналітики – постійне ведення журналу подій і запис усіх інцидентів забезпечують повний аудит і аналіз потенційних загроз. Це дозволяє оптимізувати налаштування системи та виявляти нові можливості для її вдосконалення, зокрема, за рахунок вивчення патернів атак.

4. Інтеграція з іншими безпековими системами – розроблена система може бути інтегрована з іншими системами для формування комплексної інфраструктури безпеки, що дозволяє забезпечити ще більший рівень захищеності та обмін даними між підсистемами.

Таким чином, запропонована система контролю та управління доступом є не тільки ефективною і захищеною, але й забезпечує гнучкість, адаптивність та стійкість до постійно змінюваних загроз. Резервний канал GSM у поєднанні з AES-шифруванням створює надійний бар’єр для несанкціонованого доступу, дозволяючи системі ефективно функціонувати у широкому спектрі умов і з мінімальними ризиками.

Розроблена система СКУД відповідає найвищим вимогам захисту і готова до впровадження у реальні умови, де постійно зростають кіберзагрози та вимоги до конфіденційності інформації. Такий підхід підтримує принципи сучасної інформаційної безпеки тріади CIA, включаючи гнучкість і масштабованість системи, що робить її актуальною для використання на різних об’єктах – від комерційних офісів до критичних об’єктів інфраструктури.

Система, побудована на основі резервного GSM-каналу та AES-шифрування, забезпечує не тільки захист від поточних кіберзагроз, але й становить стратегічну інвестицію в майбутнє підприємства. Це рішення здатне підтримувати високу продуктивність і стійкість системи у разі збоїв та забезпечує масштабованість для відповідності зростаючим вимогам бізнесу.

Комплексна інтеграція описаних технологій створює основу для ефективного та безпечного управління доступом, здатна забезпечити довгострокову стабільність і захист критичних даних підприємства, що відповідає сучасним стандартам у сфері інформаційної безпеки.

Висновки

Запропоноване рішення щодо вдосконалення системи контролю та управління доступом може бути шаблонним прикладом для організацій, які прагнуть досягти високого рівня захищеності інформації та безперебійної роботи системи, навіть у найскладних умовах.

Основні переваги запропонованої системи:

1. Система забезпечує ефективне управління ризиками кібербезпеки і відповідність загальновизнаним стандартам безпеки, таким як ISO 27001 та GDPR завдяки резервному каналу зв'язку та шифруванню AES, що надає захист інформації від перехоплення, атак на канали зв'язку, а також від збоїв у роботі основного каналу.

2. Швидке відновлення зв'язку та реагування на збої завдяки автоматичному перемиканню на резервний канал при проблемах із основним каналом забезпечує безперервність роботи СКУД. Система здатна миттєво реагувати на інциденти, інформуючи адміністраторів та відповідальних осіб для швидкого вжиття необхідних заходів.

3. Надійний облік та аналіз подій забезпечується фіксацією подій, що дозволяє вивчати поведінку системи та аналізувати потенційні загрози. Це допомагає не тільки у вдосконаленні поточної системи, але й у розробці кращих практик для майбутніх рішень.

4. Потенціал інтеграції та масштабування забезпечується запропонованою архітектурою системи, яка передбачає можливість взаємодії з іншими системами безпеки (наприклад, відеоспостереженням, системами протипожежної сигналізації та сповіщення), що створює основу для побудови комплексної безпекової інфраструктури. Система може бути легко масштабована з урахуванням потреб компанії або розширення її функціональності.

Розроблене рішення відповідає сучасним стандартам інформаційної безпеки, забезпечуючи комплексний підхід до захисту інформації та управління доступом. Це рішення не тільки актуальне для сучасних умов, але й закладає основу для безпечного та гнучкого розвитку системи в майбутньому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: навч. посіб. Київ: Видавництво НА СБ України, 2020. 256 с.

2. Основи криптографічного захисту інформації : електронний навчальний посібник комбінованого (локального та мережного) використання [Електронний ресурс] / Яремчук Ю. Є., Салієва О. В., Бондаренко І. О. – Вінниця : ВНТУ, 2024. – 139 с.

3. Quectel EC25 Series. [Електронний ресурс]. – Режим доступу: https://www.quectel.com/product/lte-ec25-series/ (дата звернення 29.12.2024). – Quectel EC25 Series

Білоус Віталій Михайлович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, місто Вінниця, e-mail: vitalii.bilous@vntu.edu.ua

Кметюк Олександр Олександрович – магістр кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, місто Вінниця, e-mail: kmetyuk.sasha@gmail.com

Кириченко Олександр Вікторович – директор Фахового коледжу, Вінницький інститут конструювання одягу і підприємництва, місто Вінниця, e-mail: olkirichenko@gmail.com

Bilous Vitaliy M. – Assistant Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: vitalii.bilous@vntu.edu.ua

Kmetiuk Oleksandr O. – Master of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: kmetyuk.sasha@gmail.com

Kyrychenko Oleksandr V. – Director of the Vocational College, Vinnytsia Institute of Clothing Design Entrepreneurship, Vinnytsia, olkirichenko@gmail.com