які фактори впливають на дальність їх виявлення та якими методами може бути забезпечений їх контроль. У сучасних умовах ці питання набувають особливого значення у зв'язку із широким використанням бездротових технологій, IoT-пристроїв та програмно-визначених радіосистем.

Таким чином, розвиток технологій штучного інтелекту не зменшує актуальності фізичного та радіотехнічного компонентів підготовки фахівців з кібербезпеки, а навпаки – підвищує їх значення. Автоматизація окремих програмних задач призводить до того, що конкурентною перевагою майбутніх спеціалістів стають саме глибокі фундаментальні знання у сфері фізичних процесів передавання інформації, технічного захисту інформації та роботи зі спеціалізованими вимірювальними комплексами.

У сучасних умовах ефективна підготовка фахівців з кібербезпеки потребує поєднання програмно-аналітичних компетентностей із глибоким розумінням фізичних процесів передавання інформації, практичними навичками аналізу сигналів та роботи зі спеціалізованою вимірювальною апаратурою.

1. Горлинський, В. Освітні пріоритети підготовки фахівців з кібербезпеки в умовах воєнного стану в державі / Віктор Горлинський, Борис Горлинський // Information Technology and Security. – 2024. – Vol. 12, Iss. 2 (23). – Pp. 268-282. – Bibliogr.: 36 ref.
2. Лаптєв О. А., Марченко В. В. Застосування завад для захисту інформації від витоку радіоканалом // Сучасний захист інформації. 2025. № 1 (61). С. 89–97.
3. ПІДХІД ДО ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ РАДІОКЕРОВАНИХ МОДЕЛЕЙ ЗА ЇХ РАДІОСИГНАЛОМ / В. О. МАРТОВИЦЬКИЙ та ін. Вісник Херсонського національного технічного університету. 2025. Т. 2, № 2(93). С. 228–237. URL: https://doi.org/10.35546/kntu2078-4481.2025.2.2.27 (дата звернення: 16.04.2026).

Забезпечення стійкості бездротового каналу зв'язку для дистанційного керування мобільною платформою

УДК 004.056.5

Софія Яворівська[1], Марина Деркач[2], Тарас Лобур[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]avorivskasofia@gmail.com, [2]m_derkach@tntu.edu.ua, [3]lobur_t@tntu.edu.ua

У сучасних умовах стрімкого розвитку Інтернету речей (IoT) питання безпечного дистанційного керування пристроями набуває критичного значення [1]. Бездротові канали зв'язку, що використовуються для передачі команд, часто стають об'єктами кіберзагроз, таких як перехоплення сигналу або зловмисна модифікація даних. Для забезпечення надійної роботи подібних систем необхідно поєднувати апаратну стійкість із комплексним управлінням ризиками інформаційної безпеки.

Для реалізації такого підходу було розроблено систему дистанційного керування мобільною платформою. Головним вузлом системи виступає мікроконтролер ESP32-S2-WROVER, який забезпечує отримання, обробку

команд керування та відповідає за мережеву взаємодію через Wi-Fi. Апаратна частина включає підсистему стабілізації напруги на базі AMS1117-3.3 для живлення логічної частини та драйвер двигунів L298N для силового блоку. Використання драйвера обумовлене необхідністю комутації значних струмів для двигунів M1 та M2, якими ESP32 керує через сигнали IN1-IN4 та EnA/EnB. На рисунку 1 представлена принципова електрична схема системи дистанційного керування мобільною платформою на базі мікроконтролера ESP32-S2-WROVER, розроблена у середовищі KiCad.

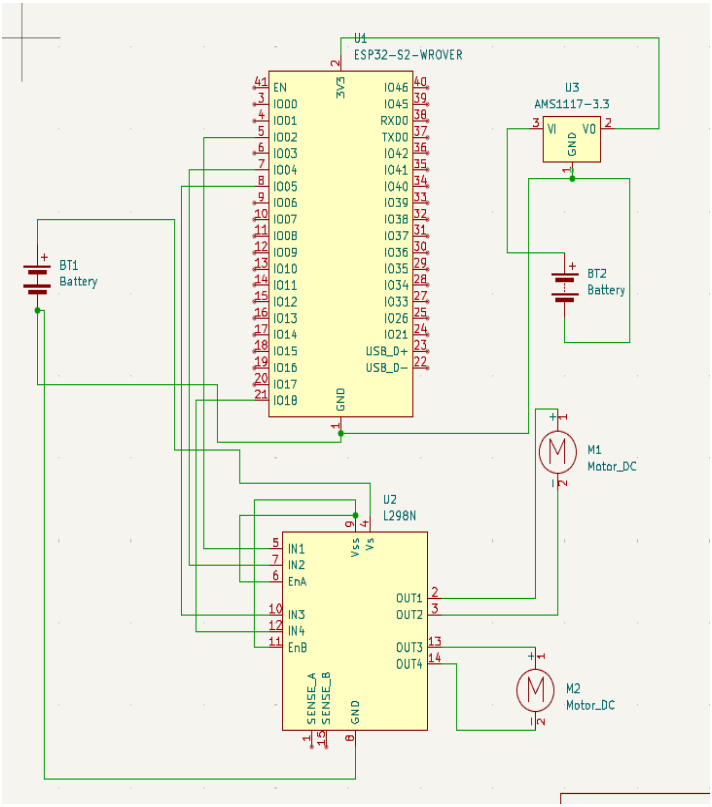

Рис. 1. Принципова електрична схема системи дистанційного керування мобільною платформою

Детальна архітектура взаємозв'язків між мікроконтролером, підсистему живлення та силовими компонентами системи представлена на принциповій схемі. Живлення драйверу двигунів від окремої батареї BT1, що відповідає тільки за мотори, адже їм потрібно більше енергії, та логічної частини від окремої батареї BT2 із загальною точкою заземлення GND дозволяє мінімізувати перешкоди в бездротовому каналі зв'язку.

Проєктування апаратної частини дозволило забезпечити фізичну надійність системи дистанційного керування мобільною платформою, проте робота у відкритому бездротовому середовищі вимагає додаткового рівня захисту на рівні передачі даних.

На основі аналізу розробленої архітектури було встановлено, що відсутність криптографічного захисту та використання відкритих мережевих портів створює умови для реалізації низки кіберзагроз, таких як несанкціоноване перехоплення трафіку (sniffing) або атаки типу DoS, що можуть призвести до повної втрати контролю над мобільною платформою.

Оцінка ризиків дозволила обрати стратегію їх зниження шляхом практичного впровадження механізмів захисту відповідно до стандарту ISO/IEC 27001/2022 [2], який надає систематизований підхід до управління інформаційною безпекою. Ці механізми включають:

- мережевий контроль доступу через фільтрацію MAC-адрес, фактично забороняючи підключення до мережі неавторизованим пристроями, і надаючи його лише заздалегідь внесеним MAC-адресам до списку дозволених;
- обов'язкове використання криптографічних засобів для захисту трафіку, а саме впровадження автентифікації команд, що передбачає механізм перевірки цифрового підпису кожної команди керування, це в свою чергу дозволяє системі ідентифікувати достовірність джерела;
- закриття всіх непотрібних мережевих портів на Wi-Fi-модулі ESP32, аби мінімізувати потенційні точки входу для атак.

Водночас для систематизації виявлених вразливостей було впроваджено ведення журналів логування спроб підключення до Wi-Fi та команд, які надсилаються для керування мобільною платформою, що дозволяє здійснювати моніторинг активності користувачів в мережі та вчасно ідентифікувати аномальні спроби доступу.

У результаті реалізовано захищену систему дистанційного керування мобільною платформою на базі мікроконтролера ESP32-S2-WROVER. Практичне дослідження, що включало серію тестувань, зокрема спроба підключення неавторизованого пристрою, перехоплення трафіку без шифрування, імітація повторної атаки (replay attack) та DoS-навантаження, підтвердило надійність обраних механізмів захисту у забезпеченні стійкості бездротового каналу зв'язку. Фактично несанкціоновані дії не мали успіху, а система дистанційного керування стабільно блокувала підозрілі запити.

1. Malyuta Y., Derkach M., Lobur T. (2025) Modelling Fog Computing Network Architecture for Secure IoT Data Processing. Security of Infocommunication Systems and Internet of Things, vol 3, no 2.
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.