

## БЕЗПЕКА ТЕХНОЛОГІЇ RFID

Волобуєва Д. М.

Національний аерокосмічний університет ім. М. Е. Жуковського  
«ХАІ»

Науковий керівник Землянко Г. А.

**Актуальність.** В останні роки RFID технології набирають популярність серед великих компаній в сфері торгівлі, транспорту, контролю доступу. Також у різних медичних системах починають активно впроваджувати дану технологію. RFID використовують для маркування лікарських препаратів та аналізів. Одночасно з цим, з'являється багато проблем з виходом з ладу цієї технології [1].

**Метою** роботи є дослідження безпеки сучасних RFID-міток.

**Основні положення.** На даний час, RFID-мітки використовують у більшості випадків для відстеження переміщення об'єктів, для контролю у системах інвентарного обліку, для захисту від крадіжок тощо.

Радіочастотна ідентифікація (Radio Frequency Identification) – це технологія, яка дозволяє ідентифікувати різноманітні об'єкти [2]. Система радіочастотної ідентифікації RFID включає в себе RFID-мітку, яка складається з мікрочіпа, де зберігається інформація, та антени, за допомогою якої передає та отримує дані. RFID-зчитувачі, необхідні для розпізнання та отримання відомостей, які переносяться у базу даних [3].

Протоколи, за якими найчастіше використовуються RFID-мітки в Україні – це ISO 14443(A), ISO 15693, ISO 18000. Перші два протоколи мають проблеми з колізією, а у останнього проблеми з зчитуванням міток.

На даний час у продажу мають різноманітні зчитувачі та записуючі прилади. RFID-мітки працюють на різноманітних частотах: 134,2 кГц (LF), 13,56 МГц (HF), 860-960 МГц (UHF) [4]. Мітки бувають активними та пасивними. Пасивна мітка працює без джерела живлення, отримуючи живлення лише за допомогою сигналу сканеру. Недолік активної мітки – для неї потрібен сканер великої потужності, вбудоване або зовнішнє живлення. Перевагами RFID-міток перед штрих-кодом є многократне змінення інформації, швидкість занесення даних та розмір [5].

В процесі роботи було розглянуто протокол EM4100 працюючий на частоті 125 кГц. У пасивній мітці як тільки зростає напруга до рівня спрацьовування, RFID-ключ передає 64 біта даних. Перевірка цілісності даних здійснюється мікроконтролером за допомогою обчислення бітів

контролю парності для кожної «строки» і «стовбця» та порівняння з отриманими даними від RFID-ключа [4, 5].

Для захисту від функційних загроз RFID-міток потрібно використовувати спеціальні захисні чохла, які блокують RFID-сигнали. Для запобігання копіювання RFID-міток можливо використання криптографії. Для більш складних пристроїв можливо використати автентифікацію методом «запит-відповідь», тобто сканер подає запит мітці, яка у свою чергу відповідає секретним цифровим ключем. Ключ можна отримати завдяки симетричній або асиметричній криптографії.

**Висновки.** Розглянута технологія RFID потребує доопрацювання, в зв'язку с тим, що вона не є досить безпечною в плані збереженості даних, які розташовані на мітці, також потребується переробка протоколів або створення нового. Але дана технологія може замінити штрих-коди, так як може перезаписуватись та бути скритна. Мітки вміщують набагато більше інформації в меншому розмірі, та можуть бути зчитані з більшої відстані. Через це вони можуть бути використані також для логістики.

#### Список літератури

1. V. Borodavka, M. Tsuranov, Biometrics: analysis and multi-criterion selection. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. (дата звернення: 20.11.2021);
2. Технологія RFID – що це? *Go RFID*. URL: <https://go-rfid.ru/novosti-i-statii/novosti-tehnologiy/chto-takoe-tehnologiya-rfid> (дата звернення: 02.10.2021);
3. Де застосовується RFID?  
*IDS*. URL: [https://ids.by/index.php?option=com\\_content&view=article&id=14%3A%20primenyatsya-rfid-&catid=4%3A%20rfidinfo&Itemid=10](https://ids.by/index.php?option=com_content&view=article&id=14%3A%20primenyatsya-rfid-&catid=4%3A%20rfidinfo&Itemid=10)  
(дата звернення: 12.10.2021);
4. Радіочастотна ідентифікація (RFID): принцип роботи та застосування *.Elektrik Info*. URL: <http://elektrik.info/device/1247-radiochastotnaya-identifikaciya-rfid.html> (дата звернення: 14.10.2021);
5. Атаки на RFID. *Хабр*. URL: <https://habr.com/ru/post/148663/> (дата звернення: 24.10.2021).

#### Відомості про авторів

Волобуєва Дар'я Михайлівна, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-970-74-72, [d.volobueva@student.csn.khai.edu](mailto:d.volobueva@student.csn.khai.edu)

Земляноко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, [g.zemlyanko@csn.khai.edu](mailto:g.zemlyanko@csn.khai.edu)