УДК 621.391

В. С. Бєлов

АНАЛІЗ ВРАЗЛИВОСТЕЙ В КАНАЛАХ ЗАХИЩЕНОГО ЦИФРОВОГО ЗВ'ЯЗКУ

***Анотація**. Проведено визначення основних характеристик формування сигналу модуляції в каналах захищеного цифрового зв'язку на прикладі системи MOTOTRBO, визначення особливостей передачі неспотвореної мовної та службової інформації в захищеному вигляді на основі стандартних алгоритмів, які застосовуються в цифровому тракті, виявлення потенційних вразливостей та запропоновано методику зменшення вразливості системи зв'язку.*

***Ключові слова:** модуляція, цифровий зв'язок, цифровий тракт, MOTOTRBO, вразливості.*

***Abstract.** This paper provides a definition of the main characteristics of modulation signal formation in secure digital communication channels using the MOTOTRBO system as an example, identifies the features of transmitting undistorted voice and service information in a secure form based on standard algorithms used in the digital chain, identifies potential vulnerabilities, and proposes a method for reducing the vulnerability of the communication system.*

***Keywords:** modulation, digital communication, digital signal chain, MOTOTRBO, vulnerabilities.*

Актуальність проблеми.

Формування сигналу модуляції в каналах захищеного цифрового зв'язку, зокрема при професійному застосуванні в пристроях MOTOTRBO, відбувається на основі цифрового тракту, важливою задачею якого є передача неспотвореної мовної та службової інформації в захищеному вигляді.

Реалізація такої передачі здійснюється на основі стандартних алгоритмів, які застосовуються в цифровому тракті, зокрема через спеціальний алгоритм стискання на основі вокодеру AMBE+2, криптографічний захист аудіо інформації, який здійснюється шифруванням AES-256 або ARC4, додаванням сервісних даних таких як ID, Color Code та подальшого формування радіочастотного сигналу у модуляторі.

Мета роботи.

Визначити вразливості системи зв'язку в каналах захищеного цифрового зв'язку на прикладі системи MOTOTRBO та на основі отриманих даних запропоновати методику зменшення вразливості даної системи.

Основна частина.

Наразі використання ARC4 Enhanced Encryption (ADP у радіостанціях Motorola) з довжиною ключа 40 біт (10 шістнадцяткових символів) не забезпечує задовільного захисту мовної інформації в каналах захищеного цифрового зв'язку, та зламується брутфорсом (перебором) за лічені хвилини/години, маючи 2^{40} комбінацій. Більш захищеним є AES-256 (Advanced Encryption) з довжиною ключа 256 біт (64 шістнадцяткові символи), маючи 2^{256} кількість комбінацій та не чутливим для зламу брутфорсом.

Проте, в протоколі DMR шифрування AES-256 захищає виключно корисне навантаження (payload) - тобто безпосередньо зміст розмови (мовної інформації) або передані текстові дані TMS (Text Messaging Service).

Незахищеними лишаються сервісні дані, зокрема усі службові заголовки та ідентифікатори передаються в ефір у відкритому (незашифрованому) вигляді, оскільки вони необхідні ретрансляторам та іншим радіостанціям для базової маршрутизації та обробки сигналу.

Основні сервісні дані та ідентифікатори:

- Radio ID (ідентифікатор радіостанції), який є унікальним цифровим номером (від 1 до 16776415) який завжди видно в етері під час натискання кнопки PTT (передачі).
- Talkgroup ID (TGID / ідентифікатор розмовної групи): номер групи, до якої адресовано виклик. Сторонній спостерігач завжди бачить, на яку саме групу йде передача.

- Колор код (Color Code) – цифровий код в діапазоні від 0 до 15, що використовується для розділення радіомереж, які працюють на одній частоті.

Службові дані таймслотів та кадрів (Frame Metadata):

- Номер таймслоту (Slot 1 / Slot 2): інформація про те, в якому логічному каналі (TDMA) відбувається передача.
- Тип послуги (Service Type): інформація, яка вказує приймачу, що саме передається (голосовий виклик Group Call, приватний виклик Private Call, екстрений виклик Emergency Call чи передача даних/TMS).
- Службові прапорці заголовків (Full LC / Link Control): інформаційні елементи, які керують встановленням та завершенням виклику.

Метадані шифрування. Перед початком передачі пакетів приймальній стороні надсилаються відкриті параметри криптозахисту, зокрема:

- Key ID (ідентифікатор ключа): номер індексу, що вказує приймачу, який саме з кількох збережених у пам'яті ключів AES-256 слід застосувати для розшифрування.
- Algorithm ID (ідентифікатор алгоритму) прапорець, що вказує, який тип шифрування використовується (наприклад, AES-256, ARC4 або Basic)
- Вектор ініціалізації (IV — Initialization Vector): псевдовипадкове число, яке змінюється з кожним суперкадром і яке необхідне для правильної роботи алгоритму AES у режимі зчеплення блоків/лічильника для синхронізації криптографічного процесу.

Результат аналізу.

Таким чином сторонній спостерігач в радіоканалі може безперешкодно здійснити аналіз параметрів мережі, захищеної шифруванням AES-256, а саме:

- дізнатися архітектуру радіомережі, зокрема скільки в ній груп та які їх номери Talkgroup ID.
- скласти повний список радіостанцій, які виходять на зв'язок через Radio ID.
- бачити, хто саме (абонент з Radio ID 1) викликає кого (абонент з Radio ID 2) або в яку групу відбувається виклик чи передача трафіку.
- фіксувати точний час, тривалість та інтенсивність переговорів конкретних кореспондентів.

Висновки.

Враховуючи те, що структура цифрового тракту та радіоінтерфейсу (Air Interface) стандарту DMR є стандартизованою, і не може бути зміненою через особливості синхронізації, передачі службової інформації та розміру кадру, необхідно застосувати методи, які не матимуть кількісного впливу на обсяг даних, що передається. Зокрема через інтеграцію алгоритму захисту в квадратурний модулятор, де існує можливість обробки потоку даних перед безпосередньою передачею до радіоінтерфейсу.

Список використаних джерел:

1. Кичак, В. М. Реалізація універсального цифрового демодулятора на основі швидкодіючих перетворювачів [Текст] / В. М. Кичак, В. С. Бєлов, А. С. Бєлов // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2012. – No2. – С. 152-156.

2. Бєлов, В. С. Визначення бітових спотворень в каналах з прямою корекцією помилок [Текст] / В. М. Кичак, В. С. Бєлов, А. С. Бєлов // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2012. – No1. – С. 121-125.

3. ETSI TS 102 361-1 V2.5.1 (2017-10). Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 1: DMR Air Interface protocol. Technical Specification. Sophia Antipolis : ETSI, 2017. 164 p. URL: etsi.org (дата звернення: 09.11.2026).

4. ETSI TS 102 361-2 V2.4.1 (2017-10). Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 2: DMR Voice and generic services and facilities. Technical Specification. Sophia Antipolis : ETSI, 2017. 106 p. URL: etsi.org (дата звернення: 09.11.2026).

5. Бєлов В.С. Аналіз спектру в діапазоні НВЧ на основі квадратурної обробки елементарних складових / В.С. Бєлов, А.С. Бєлов // Міжнародний науково-технічний журнал

«Вимірювальна та обчислювальна техніка в технологічних процесах» – Хмельницький – 2014 – №1 – с. 83-87.

6. Aumasson J.-P. Serious Cryptography: A Practical Introduction to Modern Encryption. *No Starch Press*, 2017. 312 p. URL: https://nostarch.com/serious-cryptography-2nd-edition (дата звернення: 09.11.2026).

7. ETSI TS 102 361-4. Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 4: DMR trunking protocol. *European Telecommunications Standards Institute*, 2023. URL: https://dmrassociation.org/public-downloads/standards/ts_10236104v011201p.pdf (дата звернення: 09.11.2026).

8. Guide to Digital Call Management Capabilities. *Motorola Solutions*, 2021. URL: motorolasolutions.com (дата звернення: 09.11.2026).

9. ETSI TS 102 361-1 V2.6.1 (2023-01). Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 1: DMR Air Interface (AI) protocol. — [Електронний ресурс]. — Режим доступу: etsi.org

10. TSI TS 102 361-4 V1.11.1 (2023-01). Digital Mobile Radio (DMR) Systems; Part 4: DMR trunking protocol. — Офіційні релізи Асоціації DMR. — Режим доступу: dmrassociation.org

11. Комплексна методологія побудови DMR-архітектури на основі програмно-конфігурованих радіосистем / С. О. Галкін, І. В. Петров // Науковий журнал ЗСУ. – 2021. – № 3 (14). – С. 45–52. – Режим доступу: https://nzlubp.org.ua/index.php/journal/article/view/626 (дата звернення: 09.11.2026).

12. MOTOTRBO Systems Design Guide : Technical Manual / Motorola Solutions, Inc. – Chicago : Motorola Publishing, 2022. – 430 p.

13. Бєлов В. С. Моніторинг систем радіозв’язку // Матеріали XL науково-технічної конференції професорсько-викладацького складу, співробітників та студентів університету з участю працівників науково-дослідних організацій та інженерно-технічних працівників підприємств м. Вінниці та області : електрон. наук. вид. / Вінницький національний технічний університет. – Вінниця : ВНТУ, 2011. – URL: https://scholar.google.com/scholar?cluster=8084092101155618113&hl=en&oi=scholarr (дата звернення: 09.11.2026).

14. Полуденко О. С., Бєлов В. С. Дослідження режимів роботи та рівнів застосування DMR мереж // Матеріали XLVII науково-технічної конференції професорсько-викладацького складу, співробітників та студентів університету з участю працівників науково-дослідних організацій та інженерно-технічних працівників підприємств м. Вінниці та області [Електронний ресурс] / Вінницький національний технічний університет. – Вінниця : ВНТУ, 2018. – URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/20905/4395.pdf (дата звернення: 09.11.2026).

Бєлов Володимир Сергійович - здобувач кафедри інфокомунікаційних систем і технологій Вінницького національного технічного університету, м. Вінниця, вул. Хмельницьке шосе, буд. 95, інд. 20021, e-mail: belov@vntu.edu.ua ORCID https://orcid.org/0000-0002-2253-0024

Bielov Volodymyr - Ph.D. Candidate at the Department of Infocommunication Systems and Technologies, Vinnytsia National Technical University, Vinnytsia, Khmelnytske Shose str., Building 95, Postal Code 20021, e-mail: belov@vntu.edu.ua ORCID https://orcid.org/0000-0002-2253-0024