

М. Б. Тарасюк,
І. М. Колесникова

АКТУАЛЬНІ ПИТАННЯ КІБЕРЗАХИСТУ ПРОГРАМНО-ВИЗНАЧУВАНИХ РАДІОСИСТЕМ (SDR)

Анотація. У роботі досліджено проблематику кіберзахисту програмно-визначуваних радіосистем (SDR), які активно застосовуються у сучасних військових системах зв'язку. Проаналізовано основні вразливості SDR, визначено потенційні кіберзагрози, а також запропоновано підходи до підвищення рівня їх захищеності. Особливу увагу приділено захисту програмного забезпечення, автентифікації радіовузлів та забезпеченню цілісності систем.

Ключові слова: зв'язок, радіосистеми, захист, кіберзагрози.

Abstract. The paper examines the issues of cyber protection of software-defined radio systems (SDR), which are actively used in modern military communication systems. The main vulnerabilities of SDR are analyzed, potential cyber threats are identified, and approaches to increasing their security level are proposed. Special attention is paid to software protection, authentication of radio nodes and ensuring the integrity of systems.

Keywords: communication, radio systems, protection, cyber threats.

Сучасні військові системи зв'язку характеризуються високою динамічністю, адаптивністю та вимогами до швидкої перебудови параметрів передачі даних. Одним із ключових технологічних рішень, що забезпечує такі властивості, є програмно-визначувані радіосистеми (Software-Defined Radio, SDR), у яких значна частина функцій традиційного радіо реалізується програмно.

Разом із перевагами SDR виникають нові ризики кібербезпеки, оскільки програмна складова стає потенційною точкою атаки. У військових умовах це може призвести до порушення зв'язку, витоку інформації або навіть повного виведення системи з ладу. Тому забезпечення кіберзахисту SDR є актуальним завданням у сфері безпеки військових телекомунікацій.

SDR-системи базуються на використанні універсального апаратного забезпечення та програмного керування радіочастотними параметрами. Це дозволяє змінювати частоти, модуляції та протоколи без заміни обладнання.

До ключових переваг SDR належать:

- гнучкість і адаптивність;
- можливість швидкого оновлення функціоналу;
- інтеграція з мережевими технологіями.

Водночас така архітектура створює нові поверхні атаки, пов'язані з програмним забезпеченням, мережевими інтерфейсами та каналами управління.

Аналіз показує, що SDR є вразливими до широкого спектра кібернетичних атак:

- Компрометація програмного забезпечення – впровадження шкідливого коду у прошивки або прикладні модулі;
- Несанкціонований доступ – отримання контролю над радіосистемою через мережеві інтерфейси;
- Атаки на радіосигнал – підміна, перехоплення або модифікація сигналів;
- Атаки типу «відмова в обслуговуванні» (DoS) – перевантаження системи або блокування каналів зв'язку;
- Порушення цілісності конфігурації – зміна параметрів роботи радіосистеми.

Особливу небезпеку становлять комбіновані атаки, що поєднують кібернетичний вплив із радіоелектронною боротьбою.

Для забезпечення захисту SDR необхідно застосовувати комплексний підхід, що включає такі заходи:

- Захищене завантаження (Secure Boot) – забезпечує запуск лише довіреного програмного забезпечення;
- Криптографічний захист – шифрування даних та цифрові підписи для перевірки цілісності;
- Автентифікація та авторизація – контроль доступу до радіосистеми;
- Моніторинг та виявлення аномалій – аналіз поведінки системи для виявлення атак;
- Оновлення програмного забезпечення – регулярне усунення вразливостей.

Крім того, доцільним є використання ізоляції критичних компонентів та сегментації мережі для обмеження розповсюдження атак.

У військових системах зв'язку реалізація кіберзахисту SDR ускладнюється рядом факторів:

- обмежені ресурси обчислювальної техніки;
- необхідність автономної роботи;
- вплив радіоелектронної боротьби;
- вимоги до високої надійності та безперервності зв'язку.

У таких умовах важливо забезпечити баланс між рівнем захисту та продуктивністю системи. Перспективним є використання адаптивних механізмів захисту, які змінюють свою конфігурацію залежно від рівня загроз.

Подальший розвиток кіберзахисту SDR пов'язаний із:

- інтеграцією технологій штучного інтелекту для виявлення атак;
- розробкою захищених протоколів управління радіомережами;
- використанням апаратних засобів захисту (Trusted Platform Module);
- створенням самовідновлюваних систем зв'язку.

Програмно-визначувані радіосистеми є важливим елементом сучасних військових систем зв'язку, проте їх програмна природа створює нові кіберзагрози. Ефективний кіберзахист SDR потребує комплексного підходу, що включає технічні, програмні та організаційні заходи.

Застосування сучасних методів захисту дозволяє підвищити стійкість SDR до кібернетичних атак та забезпечити надійне функціонування військових систем зв'язку в умовах сучасних загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Mitola J. Software Radio Architecture: Object-Oriented Approaches to Wireless Systems Engineering. Wiley, 2000.
2. Reed J. H. Software Radio: A Modern Approach to Radio Engineering. Prentice Hall, 2002.
3. Shi Y., Tague P. Secure Software-Defined Radio: A Survey of Security Threats and Countermeasures. IEEE Communications Surveys & Tutorials, 2018.
4. Clancy T. C., Goergen N. Security in Cognitive Radio Networks: Threats and Mitigation. IEEE Conference Publications, 2013.
5. Khan F., Jan M. A. Security Challenges in Software Defined Radio Systems. Journal of Communications, 2021.
6. Sutton P. D., Nolan K. E., Doyle L. E. Cyclostationary Signatures in Practical Cognitive Radio Applications. IEEE Journal, 2008.

Тарасюк Микола Борисович – студент кафедри військової підготовки, Вінницький національний технічний університет, м. Вінниця, e-mail: tarasyuk.m12@gmail.com

Колесникова Інна Миколаївна – викладач кафедри військової підготовки Вінницького національного технічного університету, м. Вінниця, e-mail: i.kolesnykova@donnu.edu.ua

Tarasiuk Mykola Borysovych – student of the Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: tarasyuk.m12@gmail.com

Kolesnykova Inna Mykolaivna – lecturer at the Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: i.kolesnykova@donnu.edu.ua