1. Denniss W., Bradley J. RFC 8628: OAuth 2.0 Device Authorization Grant. IETF, 2019. URL: https://datatracker.ietf.org/doc/html/rfc8628.
2. Jones M., Bradley J., Sakimura N. RFC 7519: JSON Web Token (JWT). IETF, 2015. DOI: 10.17487/RFC7519.
3. Voloshchuk A. & Osukhivska H. Adaptive multi-protocol communication for energy systems. Scientific Journal of the Ternopil National Technical University. 2025. Vol. 119, No. 3. P. 97-106.

Ампліфікація інтегрованої системи управління інформаційною безпекою

УДК 004(056.53+413.4)::001.51

Володимир Мохор[1], Олександр Бакалинський[1], Ярослав Дорогий[2], Василь Цуркан[1,3]

[1]ІПМЕ ім. Г.Є. Пухова НАН України, v.mokhor@gmail.com, baov@meta.ua

[2]ДонНТУ, yaroslav.dorohyi@donntu.edu.ua
[3]КПІ ім. Ігоря Сікорського, v.v.tsurkan@gmail.com

Діяльність будь-якої організації орієнтована на задоволення потреб і очікувань зацікавлених сторін [1]. Серед них виокремлюється зберігання властивостей інформації. Насамперед конфіденційності (приватності), цілісності та доступності [2]. Таке виділення пов'язується з тим, що інформація є цінністю для організацій і тлумачиться як актив. До того ж з використанням продуктів, послуг на основі штучного інтелекту [3]. Це спонукає до забезпечення їх відповідального розроблення, упровадження, використання та, як наслідок, призводить до виникнення емерджентних ризиків. Тож ампліфікування інтегрованої системи управління інформаційною безпекою є актуальним.

Розробляння інтегрованої системи управління інформаційною безпекою на прикладі сфери енергетики було запропоновано в [2]. Її складники визначено з урахуванням внутрішніх і зовнішніх обставин діяльності організацій. З огляду на це інтегровано системи управління інформаційною безпекою, кібербезпекою і приватністю. Завдяки отриманому рішенню можливе забезпечення непорушності властивостей конфіденційності, приватності, цілісності, доступності інформаційних активів. У даному випадку базовим складним виокремлено систему управління інформаційною безпекою. Попри це, впровадженістю продуктів, послуг на основі штучного інтелекту зумовлено необхідність гарантування належності обробляння відповідних емерджентних ризиків. Зокрема, протидіяння негативним проявам, наприклад [3], змінювання способів розроблення, упровадження, використання і поведінки. Тому системою управління штучним інтелектом [3] пропонується розширити запропоноване в [2] інтегроване рішення [1].

Отже, ампліфікація інтегрованої системи управління інформаційною безпекою дозволить забезпечити застосовність продуктів, послуг на основі штучного інтелекту відповідно до потреб і очікувань зацікавлених сторін. І, як

наслідок, гарантувати належне обробляння неприйнятних емерджентних ризиків.

1. International Organization for Standardization. Integrated management systems. A practical guide. 2026 URL: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100435_preview.pdf (accessed on: 26.04.2026).
2. Мохор В. В., Цуркан В. В. Інтегрована система управління інформаційною безпекою об'єктів критичної інфраструктури сфери енергетики. *Кібербезпека енергетики* : матеріали науково-практичної конференції (Київ, 27 травня 2022 р.). Київ : ІПМЕ ім. Г.Є. Пухова НАН України, 2022. С. 123–125.
3. ISO/IEC 42001:2023. Information technology. Artificial intelligence. Management system. [From 2023-12-18]. URL: https://www.iso.org/standard/ 42001 (accessed on: 26.04.2026).

Синтез сигналів управління складної форми для захищеного каналу зв'язку БПЛА

УДК 004.056: 621.39

Назарій Когут[1], Орест Синявський[2]

Національний університет "Львівська політехніка",
[1]nazarii.m.kohut@lpnu.ua, [2]orest.y.syniavskyi@lpnu.ua

Вступ. Сучасний етап розвитку безпілотних літальних апаратів (БПЛА) характеризується їх масовим застосуванням у військових та цивільних сферах. Головною умовою успішного виконання місій БПЛА є надійне та безперервне функціонування каналів управління та телеметрії. Проте радіоканали БПЛА є вразливими до навмисних завад (РЕБ), перехоплення даних та підміни сигналів управління (GPS/сигнального супфінгу). Традиційні методи захисту, такі як криптографічне шифрування, не захищають фізичний рівень зв'язку від придушення шумовими або прицільними завадами. Тому розробка методів синтезу сигналів управління складної форми, які мають високу прихованість та завадозахищеність, є актуальним науково-технічним завданням.

Аналіз останніх досліджень і публікацій. Питанням побудови завадостійких систем зв'язку присвячено роботи багатьох вітчизняних та закордонних вчених. Найчастіше для захисту каналів БПЛА використовують технології розширення спектра: псевдовипадкове переналаштування робочої частоти (ППРЧ) та прямого розширення спектра послідовністю (ПРСП) [1– 3].

Проте за умов застосування інтелектуального радіоелектронного придушення (Smart Jamming), традиційні закони формування сигналів стають прогнозованими для завадових систем противника. Потребують вдосконалення математичні моделі синтезу сигналів, які б адаптивно змінювали свою структуру у реальному часі.

Мета роботи. Підвищення завадозахищеності та імітостійкості каналу зв'язку БПЛА шляхом синтезу фазоманіпульованих та частотно-маніпульованих сигналів складної форми на основі нелінійних динамічних систем.