DOI: https://doi.org/10.36910/6775-2524-0560-2025-60-11
УДК: 004.056.5, 004.773, 004.85
Гриненко Олександр Валерійович, здобувач, дослідник
https://orcid.org/0009-0008-7062-1108
Кальченко Вадим Володимирович, ст. викладач
https://orcid.org/0000-0001-6492-3806
Ободяк Віктор Корнелійович, к.т.н., доцент
https://orcid.org/0000-0002-8539-1252
Пугач Ігор Олександрович, асистент
https://orcid.org/0009-0002-9644-9357
Савченко Тарас Русланович, здобувач, дослідник
http://orcid.org/0000-0002-9557-073X
Сумський державний університет, м. Суми, Україна

АДАПТИВНЕ ПСЕВДОВИПАДКОВЕ ПЕРЕЛАШТУВАННЯ РОБОЧОЇ ЧАСТОТИ З ІНФОРМАЦІЙНО-ЕКСТРЕМАЛЬНИМ КЕРУВАННЯМ ДЛЯ ЗАХИЩЕНИХ БЕЗПІЛОТНИХ МЕРЕЖ

Гриненко О. В., Кальченко В. В., Ободяк В. К., Пугач І. О., Савченко Т. Р. Адаптивне псевдовипадкове перелаштування робочої частоти з інформаційно-екстремальним керуванням для захищених безпілотних мереж. У статті досліджується проблема вразливості каналів зв'язку безпілотного літального апарату (БПЛА) в умовах активного застосування засобів радіоелектронної боротьби (РЕБ). Сучасні безпілотні системи дедалі частіше стають об'єктами цілеспрямованих атак, що включають перехоплення та модифікацію трафіку, глушіння керуючих сигналів, підміну даних або запуск деструктивних кібератак на канали зв'язку. З метою забезпечення надійності, безпеки та безперервності зв'язку між БПЛА та наземною станцією управління, авторами запропоновано багаторівневу адаптивну архітектуру захисту, що включає кілька взаємодоповнюючих компонентів: адаптивне псевдовипадкове перестрибування частот (FHSS), програмно-визначувані мережі (SDN/NFV), вбудовані IDS/IPS-системи виявлення атак та апаратні модулі довіри. Застосування логістичного відображення та нормалізованого інформаційного критерію інформаційно-екстремального навчання дозволяє динамічно керувати FHSS-послідовностями з урахуванням стану каналу та рівня загроз. SDN-контролер, використовуючи гнучке керування мережею, виконує моніторинг каналів, виявляє ознаки атак або нестабільності та в режимі реального часу переналаштовує маршрути передачі даних. Результати проведених експериментальних досліджень підтверджують ефективність запропонованого рішення – затримка обробки сигналу становила лише 8–12 мс, що є прийнятним для критичних задач керування, а коливання показника успішної доставки пакетів (PDR) під час адаптивної зміни каналів не перевищували 5 %, що свідчить про стабільність та відновлюваність системи навіть під час активного радіоелектронного впливу. Поєднання інформаційно-екстремального управління, адаптивного FHSS та гнучкої архітектури SDN/NFV створює ефективну систему протидії РЕБ і кіберзагрозам. Запропонований підхід не лише підвищує живучість та доступність каналів зв'язку, але й сприяє збереженню точності моделей машинного навчання (ML) розпізнавання, які працюють на борту БПЛА, що є критично важливим для виконання бойових або розвідувальних завдань у ворожому середовищі.
Ключові слова: FHSS; SDN/NFV; Zero-Trust; IDS/IPS; БПЛА; стійкість до глушіння; інформаційно-екстремальне навчання.

Hrynenko O. V., Kalchenko V. V., Obodyak V. K., Pugach I. O., Savchenko T. R. Adaptive pseudo-random reconfiguration of the operating frequency with information-extreme control for protected unmanned networks. The article explores the issue of the vulnerability of unmanned aerial vehicle (UAV) communication channels under conditions of active use of electronic warfare (EW) systems. Modern unmanned systems are increasingly becoming targets of deliberate attacks, including traffic interception and modification, jamming of control signals, data spoofing, or launching destructive cyberattacks on communication channels. To ensure the reliability, security, and continuity of communication between the UAV and the ground control station, the authors propose a multi-level adaptive protection architecture that includes several complementary components: adaptive pseudo-random frequency hopping (FHSS), software-defined networks (SDN/NFV), embedded IDS/IPS attack detection systems, and hardware trust modules. The use of logistic mapping and a normalized information criterion of information-extreme learning allows for dynamic control of FHSS sequences, taking into account the channel state and threat level. The SDN controller, through flexible network management, monitors the channels, detects signs of attacks or instability, and reconfigures data transmission routes in real time. The results of experimental studies confirm the effectiveness of the proposed solution — signal processing delay was only 8–12 ms, which is acceptable for critical control tasks, and fluctuations in the packet delivery ratio (PDR) during adaptive channel switching did not exceed 5%, indicating the system's stability and resilience even under active electronic interference. The combination of information-extreme control, adaptive FHSS, and flexible SDN/NFV architecture creates an effective system for countering EW and cyber threats. The proposed approach not only increases the survivability and availability of communication channels but also helps preserve the accuracy of machine learning (ML) recognition models operating onboard the UAV, which is critically important for carrying out combat or reconnaissance missions in hostile environments.
Keywords: FHSS; SDN/NFV; Zero-Trust; IDS/IPS; UAV communications; jamming resilience; information-extreme learning.

Постановка наукової проблеми. Сучасні автономні безпілотні літальні апарати (БПЛА) усе частіше використовуються для розпізнавання наземних об'єктів із застосуванням алгоритмів машинного навчання, проте критичною слабкістю таких систем залишається вразливість їх мережних каналів до глушіння, перехоплення та кібернападів, що може призвести до втрати зв'язку з оператором або компрометації переданих даних. Існуючі підходи до захисту, зокрема класичні віртуальні приватні мережі (VPN) та статичне псевдовипадкове перелаштування робочої частоти (Frequency-Hopping Spread Spectrum, FHSS), не забезпечують достатньої адаптивності в умовах мінливого радіочастотного середовища та цілеспрямованих атак.

Запропоноване рішення полягає у створенні багаторівневої мережевої інфраструктури, яка поєднує програмно-визначувані мережі (SDN/NFV) зі стратегіями ZeroTrust і адаптивним FHSS, керованим інформаційно-екстремальним модулем машинного навчання. Такий підхід дозволяє в реальному часі моніторити якість каналів, динамічно переналаштовувати маршрутизацію та політики безпеки згідно з інформаційним критерієм , а також локалізувати та нейтралізувати спроби глушіння й перехоплення за допомогою вбудованих систем виявлення та запобігання вторгнень (IDS/IPS) і апаратних модулів захисту.

Метою роботи є розробка та апробація такої адаптивної мережевої архітектури для БПЛА, здатної забезпечити водночас високу точність класифікації наземних об'єктів і стійкість до кіберзагроз.

Аналіз останніх досліджень і публікацій. Класичні схеми псевдовипадкового перестрибування робочої частоти (FHSS) у безпілотних мережах традиційно забезпечують стійкість до вузькосмугових перешкод і ускладнюють перехоплення сигналу. На практиці, найбільш вразливими місцями FHSS є процес синхронізації сигналів та чутливість до радіочастотного середовища. Саме тому в сучасній літературі посилюється акцент на адаптивні варіанти FHSS, де вибір підканалів керується якістю лінії зв'язку та поведінковими індикаторами мережі за допомогою використання апаратних чи алгоритмічних засобів підвищення непередбачуваності послідовностей [1]. Також часто можна побачити дослідження, які спрямовані на роботу з оптимальними сімействами частотних послідовностей з низькою кореляцією, «no-hit/low-hit-zone» та «wide-gap» властивостями, що знижують взаємні завади і підсилюють характеристики захисту від радіоелектронної протидії (РЕП) у квазі-синхронних режимах доступу . Показовими є нещодавні конструкції LHZ-FHS з оцінкою, що узгоджується з межами Peng–Fan–Lee [2], а також широкі «wide-gap» набори з поліпшеними межами Лемпеля–Ґрінберґера [3], що безпосередньо підвищують завадостійкість FH-систем у складних спектральних умовах.

Через зростання попиту на засоби РЕП, нові підходи поєднують адаптивне FHSS із ігровими моделями вибору частоти носія та методами підсиленого навчання, які дозволяють у реальному часі протидіяти кібератакам [4]. Запропоновані способи симуляції сценаріїв для радіочастотних мереж та середовища прийняття рішень демонструють, що сліпе або статичне перестрибування між частотами має фіксовану межу толерантності до радіоелектронної протидії. Однак системи, які були навчені в динамічному середовищі, здатні адаптуватися до не статичного спектра й тактики супротивника. Наприклад стратегії для подолання обмежень, які накладаються засоби РЕП, у бездротових і радіолокаційних системах [5] підтверджують переваги RL-підходів, порівняно з традиційними методами, особливо за умов складного багатоджерельного впливу.

Також, згідно останніх тенденцій досліджень захисту радіозв'язку, все більшої популярності набувають методи Zero-Trust з мікросегментацією для безпілотних і периферійних сценаріїв. Їх основний принцип: «Never trust, always verify» забезпечується через контекстну автентифікацію, авторизацію чи дрібнозернисту ізоляцію сервісів. Таким чином, адаптивні алгоритми Zero-Trust для 5G/IoT дозволяють зменшити затримки та накладні витрати, одночасно масштабуючи контроль доступу [6]. При цьому, для збільшення продуктивності та надійності сучасних систем зв'язку, апаратні модулі безпеки (TPM/Secure Element) поєднуються з бортовими системами. Такі комбінації використовуються для захисту ключів, сертифікатів і журналів подій із можливістю аудиту, а також для виявлення радіочастотних та мережевих аномалій у реальному часі [7].

Окремий пласт сучасних публікацій присвячений практичним викликам «безпілотної війни» в конфліктах останніх років, де БПЛА змушені масово протистояти РЕП. Можна стверджувати про еволюцію контрзаходів — від швидкого частотного перестрибування з елементами штучного інтелекту до дешевших альтернатив CRPA-антен. Ця тенденція підтверджує прикладне значення адаптивного FHSS для збереження стійкого командно-телеметричного каналу у реальних бойових умовах [8].

Отже, сучасний стан досліджень дозволяє зробити висновок, що ізольовані рішення - класичне FHSS з фіксованим зерном, статичні правила Zero-Trust або окремі IDS/IPS-агенти - не забезпечують необхідної адаптивності в мінливому RF-середовищі з інтелектуальним супротивником.

Мета дослідження. Розробка системи кіберзахисту БПЛА на основі адаптивних, інформаційно-керованих модулів FHSS, SDN/NFV, мікросегментацією Zero-Trust та апаратною довірою в поєднанні з адаптивністю ML модуля та динамічного керування мережею.

Основна частина. Для забезпечення надійного зв'язку та протидії кіберзагрозам у системах БПЛА необхідно враховувати:

- Конфіденційність – шифрування всіх каналів управління й передачі даних.
- Цілісність – захист від модифікації команд і телеметрії в польоті.
- Доступність – стійкість до DoS/DDoS–атак і радіоперешкод.
- Аутентифікація й авторизація – перевірка достовірності як бортових модулів, так і наземних станцій.

Для апаратної частини системи використовуються захищені модулі (TPM або Secure Element), які надійно зберігають криптографічні ключі та сертифікати, необхідні для встановлення довірених з'єднань. На борту кожного БПЛА функціонують агенти IDS/IPS, які в режимі реального часу аналізують радіочастотний трафік і мережеву активність, своєчасно виявляючи спроби несанкціонованого доступу або аномалії в передаванні даних. Водночас усі події та інциденти мережевого рівня фіксуються у захищених журналах із хешованим ланцюжком записів, що забезпечує можливість їх подальшого аудиту та розслідування.

Окрім цього у концепції Zero-Trust Networking жоден компонент мережі не вважається безпечним за замовчуванням, тому кожен запит має проходити сувору перевірку автентичності та авторизації перед наданням доступу до ресурсів. Для подальшої ізоляції критичних сервісів застосовується підхід micro-segmentation, який розділяє мережевий простір на незалежні сегменти відповідно до функціональних зон, зокрема управління польотом, передачі відео й телеметрії та обміну з аналітичним центром. Така архітектура дозволяє локалізувати будь-який інцидент у межах одного сегмента та значно зменшити зону ураження в разі кібератаки.

Узагальнюючи, впровадження програмно-визначуваних мереж із віртуалізованими функціями безпеки забезпечує оперативне переналаштування потоків і захист від нових загроз, тоді як Zero-Trust із micro-segmentation дозволяє локалізувати атаки та мінімізувати їх вплив. Додаткове використання апаратних модулів безпеки, бортових IDS/IPS і захищеного логування гарантує цілісність критичних даних [9] і можливість ретельного аудиту інцидентів, що разом створює багаторівневу стійку мережну інфраструктуру для БПЛА.

Проектування захищеної мережної інфраструктури з інформаційноекстремальним керуванням складається з чотирьох взаємопов'язаних підсистем у межах єдиного симуляційного середовища:

Модуль адаптивного FHSS реалізовано як 16-бітний лінійний регістр зворотного зв'язку (LFSR), зерно якого формується комбінацією виходу хаотичної карти (логістичний відображувач з параметром r=3.9) та нормалізованого значення інформаційного критерію . Це дозволяє згенерувати псевдовипадкову послідовність переходів між двадцятьма підканалами по 2 МГц у діапазоні 2,4 ГГц із інтервалом 20 мс.

Модуль інформаційноекстремального керування (IEControl) накопичує статистику успішних класифікацій від модуля ML і, після кожного пакета в 100 переданих кадрів, обчислює критерій на основі варіації показників класифікації. Це значення передається назад у генератор LFSR для наступного циклу FHSS.

SDN/NFVконтролер за допомогою Python фреймворку SimPy аналізуємо якість кожного підканалу (вимірений коефіцієнт втрат через процес глушіння) і динамічно коригуємо набір «здорових» каналів. При виявленні нестабільних або заглушених підканалів контролер оновлює віртуальні маршрути, що дозволяє оперативно ізолювати недієздатні сегменти спектра.

Модуль ML-імітації спрощено моделює процес класифікації наземних об'єктів у трьох категоріях («людина», «транспорт», «фон») із базовою точністю 95 % за умов відсутності радіоперешкод. Для кожного прийнятого пакета від модуля FHSS він повертає скориговану точність залежно від втрат, яку використовує IEControl для обчислення .

Запропонована архітектура дозволяє у реальному часі відстежувати якість каналів, оперативно формувати псевдовипадкові послідовності перескакування частот і динамічно

виконувати переналаштовування мережевої інфраструктури. Завдяки цьому прототип демонструє стійкість до радіоглушіння та забезпечує стабільний зв'язок навіть у складних умовах змінного RFсередовища, що підтверджує ефективність обраного підходу реалізації.

Як основний метод машинного навчання було обрано інформаційно-екстремальний алгоритм [10], [11], який дозволяє уніфікувати правила прийняття рішень шляхом перенесення їх у бінарний простір Хеммінга. Передбачається, що таким чином система зможе краще розпізнавати найменш виражені ознаки або ті, що знаходяться на перетині кількох класів розпізнавання з мінімальним вхідним математичним описом об'єкта. Основна ідея інформаційно-екстремального алгоритму полягає в пошуку глобального максимуму інформаційного критерію, усередненого по алфавіту класів розпізнавання, в робочій (допустимій) області визначення його функції:

$$\delta_K^* = \arg\{\max_{G_\delta}\{\max_{G_E \cap \{k\}} \bar{E}^{(k)}\}\} \quad (1)$$

де δ_K^* – оптимальний параметр поля допуску керування; G_δ – допустимий діапазон значень параметра δ поля допуску керування; $\{k\}$ – впорядкований за часом набір кроків машинного навчання; G_E – допустима область визначення інформаційної критеріальної функції.

При такій реалізації вхідними даними для алгоритму машинного навчання є масив $\left\{y_{m,i}^{(j)}\right\}$ з системою нормалізованих полів допуску $\{\delta_{H,i}\}$ на ознаках розпізнавання, яка визначає діапазон значень системи допуску керування.

Як критерій оптимізації параметрів машинного навчання систем підтримки прийняття рішень (СППР) було використано модифіковану інформаційну міру Кульбака у вигляді:

$$E_m^{(k)} = \frac{1}{n} log_2 \left\{ \frac{2n+10^{-r}-\left[K_1^{(k)}+K_2^{(k)}\right]}{\left[K_1^{(k)}+K_2^{(k)}\right]+10^{-r}} \right\} \left| n - \left(K_2^{(k)} - K_3^{(k)}\right) \right| \quad (2)$$

Нормалізована модифікація критерію (2) має вигляд (3):

$$E_m^{(k)} = \frac{E_{K_m}^{(k)}}{E_{K_{max}}^{(k)}}, \quad (3)$$

де $K_1^{(k)}$ – кількість подій, у яких вектори ознак класу розпізнавання $X_{h,s,m}^o$ помилково не призначені йому; $K_2^{(k)}$ – кількість подій, у яких вектори ознак сусіднього класу розпізнавання помилково призначені класу розпізнавання X_m^o; n_{min} – мінімальний розмір репрезентативної навчальної вибірки; 10^{-r} – достатньо мале число, яке вводиться, щоб уникнути ділення на нуль.

На основі отриманих оптимальних геометричних параметрів контейнерів класу розпізнавання можна побудувати правила прийняття рішень:

$$\left(\forall X_m^o \in \Re^{|M|}\right)\left(\forall x^{(j)} \in \Re^{|M|}\right) \begin{bmatrix} if(\mu_m > 0)(\mu_m = \max\{\mu_m\}) then x^{(j)} \\ \in X_m^o else x^{(j)} \notin X_m^o \end{bmatrix} \quad (4)$$

де $x^{(j)}$ – розпізнаний вектор, а μ_m – функція належності вектора $x^{(j)}$ для контейнера класу розпізнавання X_m^o.

У виразі (4) функція належності для гіперсферичного контейнера класу розпізнавання визначається формулою (5):

$$\mu_m = 1 - \frac{d(x_m^* \oplus x^{(j)})}{d_m^*} \quad (5)$$

де x_m^* та d_m^* – оптимальні параметри машинного навчання: усереднена бінарна реалізація та радіус гіперсферичного контейнера відповідно.

Таким чином, на етапі класифікації об'єктів, згідно з правилами прийняття рішень (5), визначається, чи належить об'єкт до одного з класів, заданих алфавітом X_m^o.

Отже, загальна функціональна категоріальна модель інформаційно-екстремальної системи машинного навчання матиме вигляд, наведений на рис.1 [12,13].

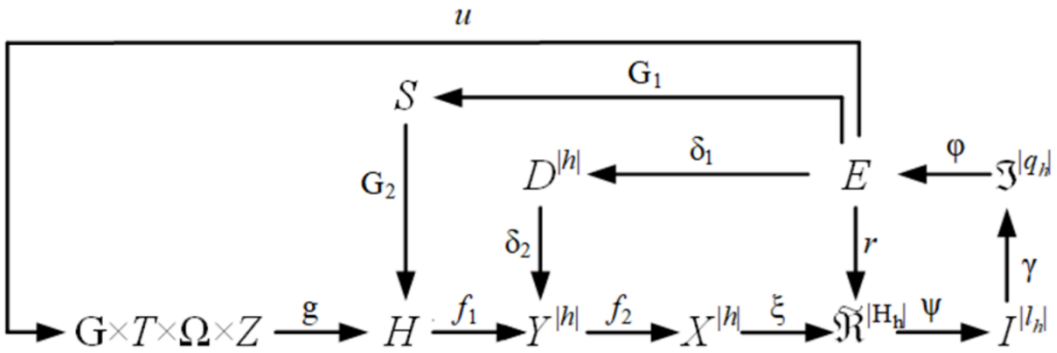

Рис. 1. Категорійна модель інформаційно-екстремального машинного навчання

На рис. 1 декартовий добуток T× G × Ω × Z задає джерело інформації. Терм-множина (E) значень інформаційних критеріїв є спільною для всіх контурів оптимізації параметрів машинного навчання. Оператор r: $E \to \Re^{|H_h|}$ відновлюється для кожної страти декурсивного дерева відновлює в радіальному базисі простору ознак Геммінга, в процесі інформаційно-екстремального машинного навчання в загальному випадку нечітке покриття класів розпізнавання, яке шляхом реалізації оператора ς покриває розподіл двійкових реалізацій навчальної матриці ($X^{|h|}$) в $\Re^{|H_h|}$. Далі оператор $: X_h \to I^{|I_h|}$ перевіряє основну статистичну гіпотезу ($\gamma_1 : x_{h,n}^{j} \in X_{h,m}^{o}$). Оператор γ обчислює набір характеристик точності ($I^{|q_h|}$), де $q_h = l_h$. На кожному кроці машинного навчання оператор φ обчислює інформаційний критерій оптимізації, який є функцією характеристик точності. Цикл оптимізації допусків керування замикається через множину $D^{|h|}$, елементами якої є значення допусків керування для діагностичних ознак. Оператор u_H регулює процес машинного навчання.

Для перевірки ефективності розробленої системи було змодельовано три експериментальні сценарії з різними стратегіями FHSS та глушінням. Для кожного з них використовувалося 1 000 пакетів, а результати збиралися протягом 10 повторних прогонів для статистичної достовірності. Зміна каналів відбувалася з інтервалом 20 мс, а інформаційноекстремальне оновлення зерна LFSR і SDN здійснювалося після кожних 100 пакетів на основі обчисленого критерію та виходу логістичної карти (r=3.9).

Таблиця 1. Результати апробації системи

Сценарій	**Тип FHSS**	**Зерно генератора**	**Спектр сигналу**	**Кількість пакетів**	**Кількість прогонів**
S_0	відсутнє	-	вузькосмуговий і широкосмуговий	1000	10
S_1	класичне FHSS	фіксоване			
S_2	адаптивне IE-FHSS	оновлюване за E_m			

Метрики оцінювання включали співвідношення доставлених до відправлених пакетів (PDR), середню точність класифікації наземних об'єктів та частку часу успішного глушіння (Jamming Success Rate). Такий підхід дозволяє уніфіковано порівняти стійкість і продуктивність кожної з трьох стратегій у реалістичних умовах радіочастотного середовища та цілеспрямованих атак.

Таким чином, експериментальні дані підтвердили суттєву перевагу адаптивного IEFHSS порівняно з класичними підходами. У таблиці приведено середні значення та стандартні відхилення трьох ключових метрик: рівень доставки пакетів (PDR), точність класифікації наземних об'єктів і частку часу успішного глушіння (JSR).

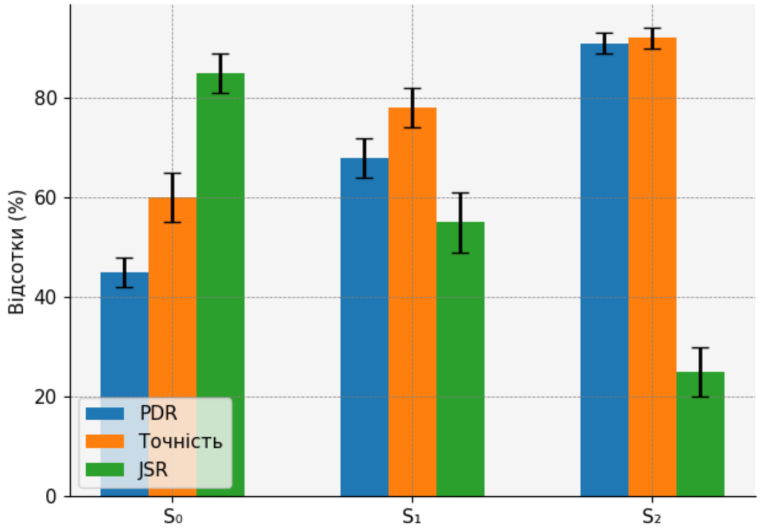

Рис. 2. Порівняння PDR, точності класифікації та JSR

Перш за все, рівень доставки пакетів у сценарії досяг 91 %, що на 23% перевищує показник статичного FHSS і на 46 % — сценарію без використання FHSS. Це свідчить про те, що адаптивне керування частот із урахуванням інформаційного критерію дозволяє значно підвищити доступність каналу навіть за активного глушіння.

По-друге, точність класифікації наземних об'єктів у склала 92 %, тоді як у вона зросла до 78 %, а в залишалася на рівні 60 %. Підвищення точності зумовлене тим, що IEControl своєчасно виключає заглушені підканали, знижуючи втрати відеопакетів чим забезпечує подачу більш інформативних пакетів на вхід MLмодуля.

По-третє, Jamming Success Rate впав до 25 % у , що означає зниження ефективності атаки на 60 % відносно статичного FHSS і на 70 % відносно відсутності FHSS. Це досягається за рахунок непередбачуваності послідовності переходів і адаптивної ізоляції нестабільних підканалів.

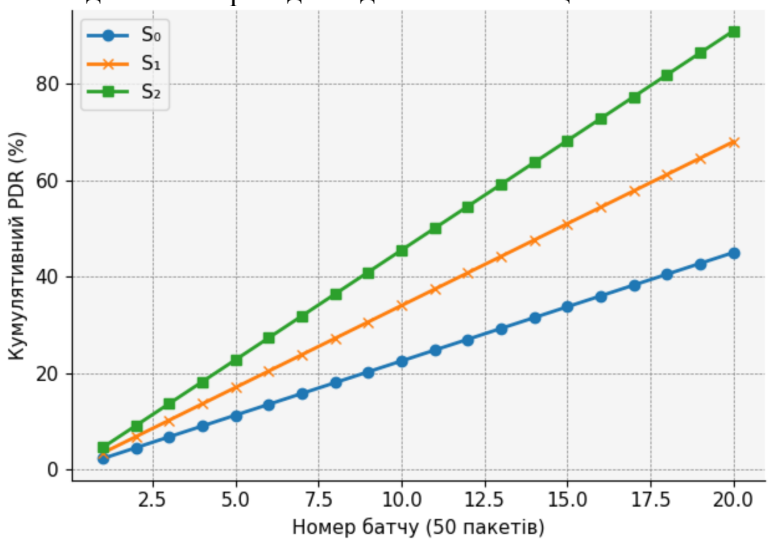

Рис. 3. Залежність кумулятивної PDR від батчу

Ключова відмінність між S_1 і S_2 полягає у відсоткових пунктах зростання PDR з кожним батчем, що свідчить про ефективність інформаційно-екстремального керування. Таким чином, у S_2 середній крок зростання кумулятивного PDR на кожному наступному батчі становить ~1,5–2 %, що більше, ніж у S_1. Крім того, гладкість кривої S_2 підтверджує відсутність тривалих «провалів» під час глушіння, оскільки SDN-контролер оперативно переналаштовує мережу.

Також варто зазначити, що аналіз часових характеристик показав, що середня затримка обробки становить 8–12 мс. У свою чергу це мінімально впливає на інтервал перескакування (20 мс) і не призводить до накопичення затримок у передачі. Водночас коливання PDR, під час переходів каналів не перевищували 5 %, оскільки SDN/NFVконтролер миттєво перенаправляв трафік на резервні "здорові" канали.

Отже, отримані результати демонструють, що синергетичне поєднання інформаційно-екстримального керування, адаптивного FHSS і програмновизначуваних мереж забезпечує одночасно високу надійність зв'язку, стійкість до глушіння та збереження якості MLрозпізнавання, підтверджуючи ефективність запропонованого підходу.

Висновки. Проведене дослідження продемонструвало, що інтеграція інформаційно-екстримального керування із адаптивним FHSS та SDN/NFV створює ефективну, багаторівневу систему захисту каналів зв'язку автономних БПЛА. У порівнянні з сценаріями без FHSS та класичним FHSS із фіксованим зерном прототип досяг 91 % показника PDR, зберіг точність класифікації на рівні 92 % та знизив ефективність глушіння до 25 %. Ці результати підтверджують, що поєднання інформаційного критерію як основи для генерації псевдовипадкових послідовностей перескакування частот забезпечує стійкість до цілеспрямованих атак і мінімізує втрати пакетів у складних RF-умовах.

Водночас слід врахувати, що моделювання виконувалося з використанням фреймворку SimPy для спрощених моделей втрат та класифікації. Фактичний вплив затримок SDNконтролера, неточностей синхронізації FHSS і реального шуму у фізичному середовищі може дещо відрізнятися від отриманих симуляційних даних. Крім того, генерація на основі варіації класифікаційних результатів поки що не враховує потенційних похибок алгоритмів розпізнавання у разі складних умов освітлення й структури наземних об'єктів.

У наступних дослідженнях планується реалізувати прототип на апаратній платформі з програмно-визначеними радіомодемами (SDR), наприклад, Universal Software Radio Peripheral (USRP) та перевірити роботу IEFHSS у польових випробуваннях із реальними джемерами. Корисним доповненням стане адаптація ML-модуля для роботи з вбудованим GPUмодулем дрона, та оцінка впливу обчислювальної затримки на продуктивність системи. Також доцільно вивчити використання динамічних протоколів мережевого розшарування (Network Slicing у 5G) для подальшої ізоляції трафіку та забезпечення гарантованих SLA для різних типів даних (управління, телеметрія, відеопотік).

На етапі масштабування алгоритму корисним буде дослідження взаємодії кількох БПЛА в мережі, коли кожен вузол виконує локальне IEкерування, але координує перескакування через розподілений SDNконтролер. Таким чином, подальші зусилля спрямовані на перехід від симуляції до реальних випробувань, розширення можливостей машинного навчання та глибокий аналіз кіберстійкості у складних мережевих сценаріях.

Список бібліографічного опису:

1. L. Zhou and H. Wu, "New Families of Frequency-Hopping Sequence Sets with a Low-Hit-Zone," Entropy, vol. 26, no. 11, p. 948, Nov. 2024, doi: 10.3390/e26110948.
2. X. Tian, H. Han, X. Niu, and X. Liu, "Construction of Optimal Frequency Hopping Sequence Set with Low-Hit-Zone," Entropy, vol. 25, no. 7, p. 1044, July 2023, doi: 10.3390/e25071044.
3. T. Wang, X. Niu, Y. Wang, J. Zhou, and L. Xiong, "Construction of Two Kinds of Optimal Wide-Gap Frequency-Hopping Sequence Sets," IEICE Trans. Fundamentals, vol. E106.A, no. 12, pp. 1484–1492, Dec. 2023, doi: 10.1587/transfun.2023SDP0008.
4. L. Cheng et al., "Adaptive Spectrum Anti-Jamming in UAV-Enabled Air-to-Ground Networks: A Bimatrix Stackelberg Game Approach," Electronics, vol. 12, no. 20, p. 4344, Jan. 2023, doi: 10.3390/electronics12204344.
5. F. Zhang, Y. Niu, Q. Zhou, and Q. Chen, "Intelligent anti-jamming decision algorithm for wireless communication under limited channel state information conditions," Sci Rep, vol. 15, no. 1, p. 6271, Feb. 2025, doi: 10.1038/s41598-025-90201-1.
6. M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, "Verify and trust: A multidimensional survey of zero-trust security in the age of IoT," Internet of Things, vol. 27, p. 101227, Oct. 2024, doi: 10.1016/j.iot.2024.101227.
7. "A survey on emerging SDN and NFV security mechanisms for IoT systems | Request PDF," ResearchGate, doi: 10.1109/COMST.2018.2862350.
8. J. Ling, "The Invisible Russia-Ukraine Battlefield," Wired. Accessed: Aug. 13, 2025. [Online]. Available: https://www.wired.com/story/electronic-warfare-russia-ukraine/
9. V. V. Avramenko and V. M. Demianenko, "OPERATIVE RECOGNITION OF STANDARD SIGNAL TYPES," Radio Electronics, Computer Science, Control, no. 2, pp. 75–83, 2020, doi: 10.15588/1607-3274-2020-2-8.
10. Dovbysh, A., Shelehov, I., Pylypenko, S., & Berest, O. (2019). Estimation of Informativeness of Recognition Signs at Extreme Information Machine Learning of Knowledge Control System. In COLINS (pp. 143-152). URL: https://ceur-ws.org/Vol-2362/paper13.pdf
11. Naumenko, V. Piatachenko, M. Myronenko, and T. Savchenko, "Information-Extreme Machine Learning of an On-board Ground Object Recognition System with a Choice of a Base Recognition Class".
12. Naumenko, M. Myronenko, and T. Savchenko, "Information-extreme machine training of on-board recognition system with optimization of RGB-component digital images," Radioelectronic and Computer Systems, no. 4, pp. 59–70, Nov. 2021, doi: 10.32620/reks.2021.4.05.

13. Dovbysh, A., Naumenko, I., Myronenko, M., & Savchenko, T. (2020, April). Information-extreme machine learning on-board recognition system of ground objects with the adaptation of the input mathematical description. In CMIS (pp. 913-925). URL: https://ceur-ws.org/Vol-2608/paper68.pdf

References:

1. L. Zhou and H. Wu, "New Families of Frequency-Hopping Sequence Sets with a Low-Hit-Zone," Entropy, vol. 26, no. 11, p. 948, Nov. 2024, doi: 10.3390/e26110948.
2. X. Tian, H. Han, X. Niu, and X. Liu, "Construction of Optimal Frequency Hopping Sequence Set with Low-Hit-Zone," Entropy, vol. 25, no. 7, p. 1044, July 2023, doi: 10.3390/e25071044.
3. T. Wang, X. Niu, Y. Wang, J. Zhou, and L. Xiong, "Construction of Two Kinds of Optimal Wide-Gap Frequency-Hopping Sequence Sets," IEICE Trans. Fundamentals, vol. E106.A, no. 12, pp. 1484–1492, Dec. 2023, doi: 10.1587/transfun.2023SDP0008.
4. L. Cheng et al., "Adaptive Spectrum Anti-Jamming in UAV-Enabled Air-to-Ground Networks: A Bimatrix Stackelberg Game Approach," Electronics, vol. 12, no. 20, p. 4344, Jan. 2023, doi: 10.3390/electronics12204344.
5. F. Zhang, Y. Niu, Q. Zhou, and Q. Chen, "Intelligent anti-jamming decision algorithm for wireless communication under limited channel state information conditions," Sci Rep, vol. 15, no. 1, p. 6271, Feb. 2025, doi: 10.1038/s41598-025-90201-1.
6. M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, "Verify and trust: A multidimensional survey of zero-trust security in the age of IoT," Internet of Things, vol. 27, p. 101227, Oct. 2024, doi: 10.1016/j.iot.2024.101227.
7. "A survey on emerging SDN and NFV security mechanisms for IoT systems | Request PDF," ResearchGate, doi: 10.1109/COMST.2018.2862350.
8. J. Ling, "The Invisible Russia-Ukraine Battlefield," Wired. Accessed: Aug. 13, 2025. [Online]. Available: https://www.wired.com/story/electronic-warfare-russia-ukraine/
9. V. V. Avramenko and V. M. Demianenko, "OPERATIVE RECOGNITION OF STANDARD SIGNAL TYPES," Radio Electronics, Computer Science, Control, no. 2, pp. 75–83, 2020, doi: 10.15588/1607-3274-2020-2-8.
10. Dovbysh, A., Shelehov, I., Pylypenko, S., & Berest, O. (2019). Estimation of Informativeness of Recognition Signs at Extreme Information Machine Learning of Knowledge Control System. In COLINS (pp. 143-152). URL: https://ceur-ws.org/Vol-2362/paper13.pdf
11. Naumenko, V. Piatachenko, M. Myronenko, and T. Savchenko, "Information-Extreme Machine Learning of an On-board Ground Object Recognition System with a Choice of a Base Recognition Class".
12. Naumenko, M. Myronenko, and T. Savchenko, "Information-extreme machine training of on-board recognition system with optimization of RGB-component digital images," Radioelectronic and Computer Systems, no. 4, pp. 59–70, Nov. 2021, doi: 10.32620/reks.2021.4.05.
13. Dovbysh, A., Naumenko, I., Myronenko, M., & Savchenko, T. (2020, April). Information-extreme machine learning on-board recognition system of ground objects with the adaptation of the input mathematical description. In CMIS (pp. 913-925). URL: https://ceur-ws.org/Vol-2608/paper68.pdf