УДК 004.056:[004.7:629.7.05]

АДАПТИВНІ МЕХАНІЗМИ ВИЯВЛЕННЯ, ПРОТИДІЇ ТА САМОВІДНОВЛЕННЯ В СІТЧАСТІЙ АРХІТЕКТУРІ КІБЕРБЕЗПЕКИ МЕРЕЖ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Семеренська В.В.
e-mail: viktoriia.semerenska@nure.ua@nure.ua
Науковий керівник – д.т.н., проф. Хаханова Г.В.
Харківський національний університет радіоелектроніки, каф. АПОТ
м. Харків, Україна

This paper investigates adaptive detection, response and self-healing mechanisms within a cybersecurity mesh architecture for multi-UAV networks. The dynamic topology and absence of a centralized security perimeter in swarm UAV systems significantly increase the attack surface and complicate traditional protection approaches. The proposed architecture integrates distributed monitoring, behavioral and anomaly-based detection, and inter-node correlation of security events. Localized response mechanisms, including node isolation, route reconfiguration and role redistribution, are applied to maintain mission continuity. The integration of adaptive detection and decentralized recovery mechanisms enhances network resilience and eliminates single points of failure. The proposed approach contributes to improving fault tolerance and cyber resilience of UAV networks operating in hostile environments.

Мережі безпілотних літальних апаратів (БПЛА) у multi-UAV конфігурації характеризуються динамічною топологією, розподіленим прийняттям рішень та відсутністю централізованого периметра безпеки. Використання відкритих радіоканалів і міжвузлової взаємодії створює передумови для атак на маршрутизацію, підміну вузлів та ін’єкцію шкідливих команд.

Централізовані моделі захисту в таких умовах є малоефективними, оскільки не враховують змінність меж довіри та автономність вузлів. Це зумовлює необхідність розподіленої архітектури кібербезпеки з адаптивними механізмами виявлення, протидії та самовідновлення.

У роботі досліджується інтеграція таких механізмів у сітчасту архітектуру кібербезпеки мереж БПЛА та їх вплив на підвищення відмовостійкості системи [1].

Архітектурна модель сітчастої кібербезпеки

Сітчаста архітектура кібербезпеки передбачає розподілене розміщення механізмів захисту без централізованого вузла контролю. Кожен БПЛА виступає автономним елементом безпеки, що реалізує функції моніторингу подій, контролю доступу та локального реагування.

Архітектура базується на динамічних доменах довіри, які формуються залежно від ролі вузла та контексту місії. Обмін метаданими безпеки між вузлами забезпечує узгоджену оцінку стану мережі без створення єдиної точки відмови.

Логічна сегментація функціональних компонентів (навігація, телеметрія, управління корисним навантаженням, міжвузлова взаємодія) обмежує можливість латерального поширення атаки. Така організація створює основу для впровадження адаптивних механізмів виявлення та координації протидії загрозам [2].

Адаптивні механізми виявлення атак

В умовах динамічної топології мереж БПЛА сигнатурні методи виявлення є недостатніми, оскільки атаки часто мають комбінований характер. У межах сітчастої архітектури запропоновано поєднання сигнатурного, поведінкового та аномалійного аналізу на рівні кожного вузла.

БПЛА здійснює локальний моніторинг параметрів мережевої взаємодії та управління, а виявлення відхилень базується на профілі нормальної поведінки з урахуванням ролі вузла. Це дає змогу ідентифікувати підміну вузлів, модифікацію маршрутів і несанкціоновані команди.

Особливістю підходу є розподілена кореляція подій через обмін індикаторами компрометації між вузлами, що дозволяє виявляти скоординовані атаки без централізованого аналізатора та скорочує час реагування [3].

Інтеграція методів машинного навчання забезпечує адаптивне оновлення моделей поведінки з урахуванням зміни умов місії, підвищуючи точність виявлення та зменшуючи кількість хибних спрацювань.

Адаптивний розподілений механізм виявлення створює основу для своєчасної локалізації загроз у мережі БПЛА.

Механізми протидії та самовідновлення мережі

Виявлення атаки в розподіленій мережі БПЛА має супроводжуватися негайним переходом до локалізованої протидії без порушення виконання місії. У запропонованій сітчастій архітектурі реагування реалізується на рівні вузла з координацією між суміжними елементами рою.

У разі виявлення ознак компрометації вузол може бути переведений у режим обмеженої довіри або ізольований від міжвузлової взаємодії. Одночасно здійснюється перебудова маршрутів передачі даних з урахуванням актуальної топології мережі. Такий підхід дозволяє мінімізувати вплив інциденту на загальну функціональність системи.

Механізм самовідновлення передбачає автоматичний перерозподіл ролей між вузлами, оновлення політик доступу та відновлення узгодженості стану мережі після локалізації загрози. За рахунок децентралізованого управління

безпекою знижується ризик каскадної деградації та зберігається цілісність виконання місії навіть у випадку часткової втрати вузлів [3].

Інтеграція механізмів адаптивного виявлення та розподіленого реагування формує основу для підвищення відмовостійкості мережі БПЛА. Відсутність єдиної точки відмови, динамічне управління довірою та здатність до перебудови топології забезпечують стійкість до складних мережевих атак і підвищують загальний рівень кіберрезильєнтності системи [4].

У роботі обґрунтовано доцільність застосування сітчастої архітектури кібербезпеки для мереж безпілотних літальних апаратів в умовах динамічної топології та відсутності централізованого периметра захисту. Запропоновано інтеграцію адаптивних механізмів виявлення атак, розподіленої кореляції подій та локалізованого реагування на рівні вузлів мережі.

Показано, що поєднання поведінкового аналізу, міжвузлового обміну індикаторами компрометації та механізмів самовідновлення забезпечує підвищення стійкості до складних мережевих атак. Реалізація ізоляції скомпрометованих вузлів, перебудови маршрутів і перерозподілу ролей дозволяє зберігати функціональність системи навіть у разі часткової деградації [2].

Таким чином, запропонований підхід підвищує відмовостійкість та кіберрезильєнтність мереж БПЛА й може бути використаний як основа для подальших досліджень у напрямі моделювання атак і цифрових двійників безпечних UAV-систем.

Список використаних джерел:

1. Zero Trust Architecture / S. Rose et al. National Institute of Standards and Technology, 2020. URL: https://doi.org/10.6028/nist.sp.800-207 (date of access: 25.02.2026).

2. A survey on security and privacy issues of UAVs / Y. Mekdad et al. *Computer Networks*. 2023. P. 109626. URL: https://doi.org/10.1016/j.comnet.2023.109626 (date of access: 25.02.2026).Gartner.

3. Condomines J.-P., Zhang R., Larrieu N. Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation. *Ad Hoc Networks*. 2019. Vol. 90. P. 101759. URL: https://doi.org/10.1016/j.adhoc.2018.09.004 (date of access: 25.02.2026).

4. Wei X., Ma J., Sun C. A Survey on Security of Unmanned Aerial Vehicle Systems: Attacks and Countermeasures. *IEEE Internet of Things Journal*. 2024. P. 1. URL: https://doi.org/10.1109/jiot.2024.3429111 (date of access: 25.02.2026).