УДК 621.396.21, 623.76

В. Є. Перлов

ЗАПРОВАДЖЕННЯ МЕХАНІЗМУ ОБМЕЖЕННЯ ВИКОРИСТАННЯ МОБІЛЬНОГО ЗВ'ЯЗКУ ВОРОЖИМИ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

Анотація. *Розглянуто концепцію використання інфраструктури мобільного зв'язку України для протидії ворожим безпілотним літальним апаратам, які можуть застосовувати мережі мобільних операторів для дистанційного керування та передачі розвідувальної інформації. Запропоновано механізм автоматизованого виявлення абонентських пристроїв за ознаками високошвидкісного переміщення на основі аналізу їх переходів між базовими станціями та тимчасового обмеження мобільного інтернет-зв'язку в період повітряної тривоги. Розглянуто можливість застосування порогового значення швидкості 180 км/год, технічні особливості реалізації та перспективи інтеграції запропонованого підходу в систему протидії безпілотним авіаційним комплексам.*

Ключові слова: *безпілотні літальні апарати, мобільний зв'язок, LTE, базові станції, протидія БПЛА, телекомунікаційна інфраструктура.*

Abstract. *The concept of utilizing Ukraine's mobile communication infrastructure to counter hostile unmanned aerial vehicles (UAVs) is examined. Such UAVs may exploit mobile operators' networks for remote control and transmission of reconnaissance data. A mechanism is proposed for automated detection of subscriber devices based on indicators of high-speed movement, through analysis of their transitions between base stations, and for temporary restriction of mobile Internet access during air raid alerts. The feasibility of applying a threshold speed value of 180 km/h is considered, along with technical implementation features and prospects for integrating the proposed approach into a UAV counteraction system.*

Keywords: *unmanned aerial vehicles, mobile communication, LTE, base stations, UAV counteraction, telecommunication infrastructure.*

Актуальність проблеми.

Сучасні безпілотні літальні апарати (БПЛА) активно використовують різноманітні канали передачі даних для дистанційного керування польотом, навігації та передачі розвідувальної інформації. Окрім спеціалізованих радіоканалів та mesh-мереж, одним із потенційних каналів зв'язку є мережі мобільних операторів, зокрема інфраструктура 4G/LTE [1, 2]. Використання українських мобільних мереж створює додаткові можливості для ворожих БПЛА, водночас перетворюючи цивільну телекомунікаційну інфраструктуру на потенційний елемент забезпечення військових операцій противника.

У зв'язку з цим актуальним є розроблення механізмів оперативного обмеження використання мобільного інтернету пристроями, які з високою ймовірністю можуть бути складовою систем керування ворожими БПЛА.

Мета роботи.

Обґрунтування концепції автоматизованого механізму виявлення та тимчасового обмеження використання мобільного інтернет-зв'язку абонентськими пристроями, швидкість переміщення яких перевищує встановлений пороговий показник, в умовах повітряної тривоги.

Основна частина.

Однією з особливостей функціонування мереж мобільного зв'язку є можливість визначення місцеположення абонентського пристрою та відстеження його переміщення між базовими станціями [3-5]. На основі інформації про час реєстрації пристрою в різних секторах мережі та географічне розташування відповідних базових станцій оператор може отримувати оцінку швидкості його переміщення.

Запропонована концепція передбачає використання зазначеної функціональної можливості для створення автоматизованої системи протидії використанню мобільних мереж ворожими БПЛА.

Суть пропозиції полягає у впровадженні спеціального алгоритму, який активується автоматично після оголошення повітряної тривоги. У період його дії система здійснює

моніторинг швидкості переміщення абонентських пристроїв, ідентифікованих у мережі за SIM-картами або іншими мережевими ідентифікаторами.

Як початковий пороговий параметр пропонується встановити швидкість 180 км/год. Перевищення цього значення може бути підставою для автоматичного тимчасового обмеження передачі мобільного інтернет-трафіку відповідним пристроєм.

Таким чином, пропонується реалізувати такий алгоритм функціонування:

1. **Активація системи.** Після оголошення повітряної тривоги оператори мобільного зв'язку автоматично переводять мережу в режим посиленого моніторингу мобільності абонентських пристроїв.
2. **Визначення швидкості переміщення.** На основі даних про переміщення пристрою між базовими станціями здійснюється оцінювання його швидкості.
3. **Порівняння з пороговим значенням.** Якщо розрахункова швидкість перевищує встановлений показник 180 км/год, пристрій потрапляє до категорії потенційно підозрілих.
4. **Обмеження зв'язку.** Для відповідного пристрою тимчасово обмежується передача даних через мобільну мережу, що унеможливлює або суттєво ускладнює використання цього каналу для дистанційного керування БПЛА та передачі розвідувальної інформації.
5. **Відновлення послуг.** Після завершення повітряної тривоги або припинення ознак аномального переміщення обмеження автоматично знімаються.

Важливою умовою реалізації запропонованого механізму є збереження можливості здійснення екстрених викликів та отримання критично важливих повідомлень населенням. Також необхідно передбачити винятки для легального високошвидкісного транспорту та інших пристроїв, функціонування яких потребує безперервного зв'язку.

Водночас запропонований механізм потребує врахування технічних обмежень. Точність оцінювання швидкості за переміщенням між базовими станціями залежить від щільності їх розташування, конфігурації мережі та особливостей радіопокриття. Тому порогове значення не повинно бути єдиним критерієм блокування: доцільно використовувати додаткову перевірку достовірності оцінки швидкості та механізми запобігання хибним спрацюванням.

Для мінімізації ризику помилкового обмеження зв'язку для звичайних користувачів доцільно передбачити альтернативний механізм підтвердження особи абонента. Зокрема, у мобільних застосунках операторів зв'язку може бути реалізована функція відновлення доступу до мобільного інтернету шляхом проходження ідентифікації через державний застосунок «Дія». Після успішного підтвердження особи система зможе тимчасово зняти обмеження передачі мобільних даних для відповідної SIM-картки або абонентського пристрою.

Додатковим запобіжником має стати обов'язкова дія, яку може виконати лише людина в реальному часі. Наприклад, це може бути підтвердження запиту в застосунку «Дія» з використанням біометричної перевірки або іншого механізму підтвердження присутності користувача. Такий підхід ускладнить автоматизоване відновлення доступу до мережі пристроями, які використовуються для керування безпілотними літальними апаратами, та водночас дасть змогу легітимним абонентам оперативно відновити користування мобільним інтернетом.

Важливо, щоб механізм ідентифікації не передбачав автоматичного розкриття персональних даних абонента мобільному оператору понад обсяг, необхідний для підтвердження особи та відновлення послуги. Передавання підтвердження між «Дією» та оператором має здійснюватися через захищений механізм взаємодії, із дотриманням вимог законодавства про захист персональних даних.

Таким чином, поєднання автоматизованого виявлення підозрілої активності, тимчасового обмеження мобільного інтернету та можливості відновлення доступу після підтвердження особи людиною може зробити запропонований механізм більш вибірковим і зменшити його вплив на звичайних користувачів.

Очікувані результати та перспективи впровадження.

Запровадження запропонованого механізму дозволить використовувати наявну телекомунікаційну інфраструктуру України як додатковий інструмент протидії ворожим БПЛА. Його потенційна перевага полягає у відсутності необхідності створення окремої системи радіоелектронного впливу, оскільки основні функції моніторингу та обмеження можуть реалізовуватися на рівні програмного забезпечення мобільних операторів.

Практична реалізація потребуватиме координації між мобільними операторами, військовими структурами та державними органами, відповідальними за кібербезпеку й телекомунікації.

Варто також зазначити, що такий механізм не є універсальним засобом протидії БПЛА, оскільки не впливає на автономні системи навігації, спеціалізовані радіоканали та mesh-мережі. Однак він може усунути або суттєво обмежити один із доступних противнику каналів передачі даних.

Висновки

Запропоновано концепцію використання технологічних можливостей мобільних операторів для автоматизованого виявлення та тимчасового обмеження мобільного інтернет-зв'язку пристроїв, які демонструють ознаки високошвидкісного переміщення під час повітряної тривоги.

Реалізація такого підходу дозволить сформувати додатковий рівень захисту національної телекомунікаційної інфраструктури та зменшити можливості використання цивільних мобільних мереж для забезпечення функціонування ворожих безпілотних авіаційних комплексів.

Перспективним напрямом подальших досліджень є розроблення математичної моделі оцінювання швидкості абонентських пристроїв за даними мобільної мережі, визначення оптимальних порогових параметрів та експериментальна перевірка ефективності запропонованого механізму.

Список використаних джерел:

1. Enea. Riders on the Cellular Storm: Mobile Connected Unmanned Aerial Vehicles in Conflict

: White Paper. 2026. URL: https://www.enea.com/insights/riders-on-the-cellular-storm-mobile-connected-unmanned-aerial-vehicles-in-conflict/

2. Zulkifley M. A., Behjati M., Nordin R., Zakaria M. S. Mobile Network Performance and Technical Feasibility of LTE-Powered Unmanned Aerial Vehicle. Sensors. 2021. Vol. 21, No. 8. Article 2848. DOI: https://doi.org/10.3390/s21082848.

3. Lin X., Yajnanarayana V., Muruganathan S. D., Gao S., Asplund H., Määttänen H.-L., Bergström M., Euler S., Wang Y.-P. E. The Sky Is Not the Limit: LTE for Unmanned Aerial Vehicles. IEEE Communications Magazine. 2018. Vol. 56, No. 4. P. 204–210. DOI: https://doi.org/10.1109/MCOM.2018.1700643.

4. Shayea I., Dushi P., Banafaa M., Rashid R. A., Ali S., Sarijari M. A., Daradkeh Y. I., Mohamad

H. Handover Management for Drones in Future Mobile Networks—A Survey. Sensors. 2022. Vol. 22, No. 17. Article 6424. DOI: https://doi.org/10.3390/s22176424.

5. Chowdhury M. M. U., Sinha P., Mahler K., Güvenç İ. Mobility State Detection of Cellular-Connected UAVs Based on Handover Count Statistics. IEEE Open Journal of Vehicular Technology. 2023. Vol. 4. P. 490–504. DOI: https://doi.org/10.1109/OJVT.2023.3296138.

Перлов Віктор Євгенійович *– кандидат технічних наук, доцент кафедри технологій та автоматизації машинобудування Вінницького національного технічного університету, м. Вінниця, вул. Хмельницьке шосе, буд. 95, інд. 20021, e-mail: perlov@vntu.edu.ua ORCID https://orcid.org/0009-0005-0011-5515*

Perlov Viktor *– Candidate of Technical Sciences, Associate Professor at the Department of Technologies and Automation of Mechanical Engineering, Vinnytsia National Technical University, Vinnytsia, Khmelnytske Shose str., Building 95, Postal Code 20021, e-mail: perlov@vntu.edu.ua, ORCID https://orcid.org/0009-0005-0011-5515*