Секція 2

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БПЛА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ: СИСТЕМАТИЗАЦІЯ АТАК, КОНТРЗАХОДІВ ТА МОДЕЛЕЙ ОЦІНЮВАННЯ

Веприцька О.Ю.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: Харченко В.С.

Актуальність. У зв'язку зі стрімким зростанням ринку безпілотних літальних апаратів (БПЛА), який, за прогнозами, досягне 50,4 мільярда доларів США до 2032 року [1], забезпечення їх кібербезпеки стає необхідністю. Інтеграція штучного інтелекту (ШІ) в БПЛА значно підвищує їх автономність, функціональність та здатність адаптуватися до змін у середовищі, але водночас створює нові вразливості до кібератак. Важливість цих викликів зростає в умовах російсько-української війни, де БПЛА стали базою для окремого виду ЗСУ.

Метою роботи є аналіз загроз, атак та втручань, а також обґрунтування вибору контрзаходів для підвищення рівня кібербезпеки систем БПЛА з урахуванням їхніх вразливостей і використання ШІ для посилення атак і засобів захисту. Підхід дослідження ґрунтується на:

– застосуванні методології Security Informed Safety [2] та техніки IMECA для систем БПЛА з урахуванням особливостей використання ШІ;

– використанні моделі якості ШІ для обґрунтування вимог до ШІ в БПЛА [3] як засобів виконання функцій та захисту кіберактивів.

Основні положення. В рамках проведеної роботи:

– визначено основні перешкоди для впровадження ШІ в системи БПЛА, з огляду на ризики безпеки, технічні обмеження та їх кібербезпеку;

– запропоновано класифікацію контрзаходів з урахуванням аспекту ШІ;

– проаналізовано контрзаходи на регуляторному та технічному рівнях, а також оцінено їхній вплив на загальні ризики кібербезпеки та безпеки;

– наведено приклад створення моделей якості, ризик орієнтована (IMECA), логіко-ймовірнісна (дерева атак) та стохастична (марковська модель) для оцінки ШІ-систем на борту та засобів захисту БПЛА, що використовуються для задачі розмінування.

Висновки. Основний внесок цього дослідження полягає в класифікації загроз та засобів захисту з урахуванням аспекту ШІ та прикладі

впровадження стандартизації компонентів ШІ в БПЛА залежно від визначених функцій [4]. Запропонована систематизація включає регуляторні методи, орієнтовані переважно на легалізацію використання, стандартизацію та контроль якості БПЛА і ШІ, а також відповідні програмно-технічні засоби реалізації цих методів. Запропонований підхід може бути поширений на аналіз безпеки критичних систем, що працюють в агресивному інформаційному та фізичному середовищі, і забезпечення проактивного захисту від атак, посилених засобами ШІ.

Список літератури

1. Global Unmanned Aerial Vehicle Market 2024-2033. *Custom Market Insights*. URL – https://www.custommarketinsights.com/report/unmanned-aerial-vehicle-market (дата звернення: 02.11.2024).
2. Illiashenko O, Babeshko I., Kharchenko V., Fesenko H., Di Giandomenico F. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection / Entropy. 2023. Volume 25(8). Page 1123. DOI: https://doi.org/10.3390/e25081123.
3. Kharchenko V., Fesenko H., Illiashenko O. Quality Models for Artificial Intelligence Systems: Characteristic-Based Approach, Development and Application. Sensors. 2022. Volume 22(13). Page 4865. DOI: https://doi.org/10.3390/s22134865.
4. Veprytska O., Kharchenko V. Analysis of AI powered attacks and protection of UAV assets: quality model-based assessing cybersecurity of mobile system for demining. International Workshop on Intelligent Information Technologies & Systems of Information Security. 2024. URL: https://ceur-ws.org/Vol-3675/paper26.pdf (дата звернення: 02.11.2024).

Відомості про авторів

Веприцька Олена Юріївна, аспірантка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.veprytska@csn.khai.edu
Харченко Вячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, v.kharchenko@csn.khai.edu