

## ВИСНОВОК

**про наукову новизну, теоретичне та практичне значення результатів дисертації Землянко Георгія Андрійовича на тему «Методи та засоби для забезпечення кібербезпеки системи багатофункційних флотів безпілотних апаратів в умовах комбінованих кібератак», поданої на здобуття наукового ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека**

На засіданні кафедри комп'ютерних систем, мереж і кібербезпеки за участі: голови засідання – заступника зав. каф. 503, канд. техн. наук, проф. Фурманов К. К., канд. техн. наук, доц. Бабешко Є. В., канд. техн. наук, доц. Дужий В. І., ст. викладача Дужа В. В., ст. викладача Єгорова Є. В., ст. викладача Желтухін О. В., канд. техн. наук, доц. Ілляшенко О. О., асистента Карпенко А. С., канд. техн. наук, доц. Колісник М. О., канд. техн. наук, доц. Куланов В. О., д-р техн. наук, проф. Морозова О. І., канд. техн. наук, проф. Орехов О. О., д-р техн. наук, доц. Певнев В. Я., канд. техн. наук, доц. Перепеліцин А. Є., канд. техн. наук, доц. Піскачов О. І., канд. техн. наук, доц. Тецький А. Г., канд. техн. наук, доц. Узун Д. Д., д-р техн. наук, проф. Фесенко Г. В., д-р техн. наук, проф., зав. кафедри Харченко В. С., ст. викладача Холодна З. Б., канд. техн. наук, доц. Шостак А. В., д-р техн. наук, проф. Скляр В. В., д-р техн. наук, проф. Брежнев Є. В., канд. техн. наук, доц. Ключніков І. М., аспіранта Землянко Г. А., аспіранта Вдовіченко О. О., д-р техн. наук, проф. Горбенко А. В., аспіранта Лейченко К. О., аспіранта Нарожний В. В., аспіранта Кулягін А. І. відбулася публічна презентація дисертаційної роботи Землянко Георгія Андрійовича на тему «Методи та засоби для забезпечення кібербезпеки системи багатофункційних флотів безпілотних апаратів в умовах комбінованих кібератак».

На підставі обговорення змісту презентації дисертаційної роботи ухвалено висновок про наукову новизну, теоретичне та практичне значення результатів дисертації (результати голосування – одноголосно).

**1. Актуальність теми дослідження.** З впровадженням безпілотних апаратів у різноманітні сфери, включаючи аерокосмічну та промислову, зростає ймовірність їх вразливості до кібератак, які можуть мати серйозні наслідки для безпеки та ефективності їх роботи. Враховуючи велику кількість функцій, які виконують безпілотні апарати, від охорони даних до управління пристроями на місці, а також їх потенційний вплив на критичні системи, важливо розробити та впровадити ефективні методи та засоби для захисту їх від кіберзагроз. Забезпечення кібербезпеки безпілотних апаратів передбачає розробку комплексної стратегії, яка включатиме в себе виявлення, аналіз та відповідь на кіберзагрози, захист від несанкціонованого доступу та збереження конфіденційності даних. Оскільки безпілотні апарати можуть бути використані у широкому спектрі сфер, включаючи військову, комерційну та цивільну, важливою стає розробка адаптивних та розширених методів кіберзахисту, які враховуватимуть специфіку їх функціонування та потенційні загрози.

Отже, дослідження методів та засобів для забезпечення кібербезпеки системи багатофункційних флотів безпілотних апаратів в умовах комбінованих кібератак є актуальним та важливим завданням, що вимагає уваги та подальших досліджень у сучасному інформаційному суспільстві.

**2. Зв'язок роботи з науковими програмами, планами, темами.** Отримані автором результати дисертації виконано на кафедрі комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ» при виконанні держбюджетної науково-дослідницької роботи ДР № 0121U112172 впродовж 2021 -2023 рр., ДР № 0121U113842 впродовж 2021 -2023 рр., ДР № 0117U05349 впродовж 2018-2020 рр., ДР № 0118U003822 впродовж 2018-2020 рр., а також у міжнародному проєкті ЄС ERASMUS+ "Internet of Things: Emerging Curriculum for Industry and Human Applications (ALIOT, №573818-EPP-1-2016-1-UK-EPPKA2-SBHE-JP), 2016-2020 рр.

### **3. Наукова новизна отриманих результатів.**

1) Вперше запропоновано моделі кіберфізичної системи багатофункційних флотів безпілотних апаратів як об'єкта оцінювання кібербезпеки, які, на відміну від відомих, описують концептуальну схему, що об'єднує комплекс мобільних підсистем, а саме безпілотних літальних, наземних і безкіпажних апаратів та інформаційну інфраструктуру, надають теоретико-множинне представлення програмно-апаратних компонентів на різних рівнях ієрархії, порушників, загроз, вразливостей і атак та їх онтологічних зв'язків, і забезпечують повноту аналізу такої системи в умовах зовнішніх впливів, а також надають можливості формування множини контрзаходів для захисту фізичних і кіберактивів.

2) Удосконалено метод (ІМЕСА) аналізу кіберзагроз, наслідків та критичності атак на активи кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів шляхом деталізованого опису впливу на різні властивості безпеки (конфіденційність, цілісність, доступність, спостережність) і різні підсистеми, а також розроблення моделей і послідовностей комбінованих послідовно-паралельних кібератак різними порушниками і засобами, що надає змогу підвищити достовірність оцінювання кібербезпеки та обґрунтувати стратегії захисту та вибір контрзаходів для забезпечення прийняттого ризику.

3) Удосконалено метод вибору контрзаходів для забезпечення кібербезпеки кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів завдяки формуванню множини контрзаходів з врахуванням впливу на різні складові кібербезпеки, в умовах одиничних та комбінованих кібератак, з використанням процедур спрямованого пошуку варіантів покриття, що забезпечує прийнятний ризик при мінімальних витратах або мінімальний ризик при обмежених витратах.

### **4. Теоретичне та практичне значення результатів роботи.**

Автором дисертаційної роботи:

1. Розроблено алгоритми та програмні засоби для проведення розширеного ІМЕСА аналізу кібербезпеки кіберфізичної системи багатофункційних флотів безпілотних апаратів;

2. Розроблено структуру та елементи інформаційної технології для підтримки прийняття рішень щодо ризик-орієнтованого оцінювання та вибору контрзаходів для забезпечення безпеки відповідно до вимог.

Достовірність отриманих наукових і практичних результатів, підтверджуються результатами оцінювання ризиків успішних атак з використанням якісних і кількісних показників на підставі аналізу матриць критичності без і після запровадження відповідних контрзаходів, прикладами оцінювання показників кібербезпеки та вибору контрзаходів з використанням розроблених методів і алгоритмів при одиничних і комбінованих атаках і результатами практичного основних наукових положень, запропонованих програмних засобів та елементів інформаційної технології в навчальному процесі, наукових проектах.

Отримані наукові результати, можуть бути використані у науково-дослідних та проектних організаціях, ІТ-компаніях, університетах – при викладанні відповідних дисциплін, та інших організаціях, які спеціалізуються в галузі безпечних інформаційних технологій, зокрема, для побудови та забезпечення кібербезпеки та резильєнтності національної критичної ІТ-інфраструктури та захисту інформаційних активів стратегічних галузей промисловості.

### **5. Апробація/використання результатів дисертації.**

Результати досліджень автора обговорювались на наступних конференціях:

- "International Workshop on Intelligent Information Technologies & Systems of Information Security" (м. Хмельницький, 2021 р.);
- "Integrated Computer Technologies in Mechanical Engineering" (м. Харків, 2020, 2021, 2023);
- "International Workshop on Reliability Engineering and Computational Intelligence 2020 (RECI 2020)" (City Zilina, Slovakia, 2020);
- Матеріали III НТК "Інформаційна, функціональна та кібербезпека" (СКІФіК-2023)" (Харків, Україна, 2023 р.).

Розроблені автором наукові положення впроваджені у:

- у навчальному процесі кафедри комп'ютерних систем, мереж і кібербезпеки ХАІ (лекціях та практичних заняттях з навчальних дисциплін «Надійність та функціональна безпека ІКС», «Програмування систем IoT», «Захист інформації в ІКС», «Комплексні системи захисту інформації») для бакалаврів, магістрів і аспірантів, що навчаються за спеціальністю 125 – Кібербезпека;

- при виконанні держбюджетної науково-дослідницької роботи ДР № 0121U112172 впродовж 2021 -2023 рр., ДР № 0121U113842 впродовж 2021 -2023 рр., ДР № 0117U05349 впродовж 2018-2020 рр., ДР № 0118U003822 впродовж 2018-2020 рр.

- у міжнародному проекті ЄС ERASMUS+ “Internet of Things: Emerging Curriculum for Industry and Human Applications (ALIOT, №573818-EPP-1-2016-1-UK-EPPKA2-SVHE-JP), 2016-2020 pp.

- при обґрунтуванні вимог та аналізі кібербезпеки комп'ютерних мереж і мобільних систем (компанія CD-Link).

### **6. Дотримання принципів академічної доброчесності**

Дисертація Землянко Георгія є оригінальною роботою, виконана здобувачем самостійно й доброчесно, текст рукопису дисертаційної роботи не містить ознак академічного шахрайства. Роботу передано експерту для проведення науково-технічної експертизи щодо збігів із Інтернет-джерелами, про що буде надано відповідний звіт.

**7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.**

Основні результати дисертації опубліковано 13 наукових публікацій, у тому числі:

- 2 статті опубліковано у наукових фахових виданнях, включених до переліку спеціалізованих видань України;
- 3 статті опубліковані у наукових фахових виданнях, індексовані в базі даних Scopus;
- 2 колективні монографії;
- 6 публікацій у матеріалах національних та міжнародних конференцій, у т.ч. у працях конференції, індексованої у базі даних Scopus.

#### Статті у наукових фахових видання, затверджених МОН України:

Assoc. Prof., Dr A. P. Plakhteyev, MSc student H. Zemlianko (KhAI). Section 31. Prototyping and rapid development of IoT systems. //Drozd A. et al. Internet of Things for Industry and Human Application //Volumes 1–3. Volume 2. Modelling and Development. – 2019.

Здобувач представив створення прототипів та швидкий розвиток систем Інтернету речей (IoT) з урахуванням їх застосування у промисловості та для людських потреб.

Землянко Г.А., Певнєв В.Я., Ніколас Бардис, Харченко В. С., Розділ 9. Розробка моделі загроз для безпілотних літальних апаратів. Методи та технології забезпечення якості та безпеки інтелектуальних систем : кол. монографія / за заг. ред. В. С. Харченка, О. І. Морозової. Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ». Київ : «Видавництво «Юстон», 2023. С. 159–177.

Здобувач розглядає розробку моделі загроз для безпілотних літальних апаратів у контексті методів та технологій забезпечення якості та безпеки інтелектуальних систем.

Zemlianko H., Kharchenko V. Cyber Security Systems of Highly Functional Uav Fleets for Monitoring Critical Infrastructure: Analysis of Disruptions, Attacks and Counterapproaches. *Elektronnoe modelirovanie*. 2024. T. 46, № 1. С. 41–54. DOI: <https://doi.org/10.15407/emodel.46.01.041>

Здобувач представив аналіз систем кібербезпеки високофункціональних флотів безпілотних літальних апаратів для моніторингу критичної інфраструктури: розгляд порушень, атак та контрзаходів.

Землянюк Г.А., Харченко В.С. ІМЕСА-аналіз кібербезпеки систем багатофункціональних флотів БПЛА при комбінованих атаках: базові моделі та вибір контрзаходів. *Measuring and computing devices in technological processes*. 2023. № 4. С. 225–233. URL: <https://doi.org/10.31891/2219-9365-2023-76-30>.

Здобувач представив аналіз кібербезпеки систем багатофункціональних флотів безпілотних літальних апаратів (БПЛА) у контексті комбінованих кібератак, включаючи розробку базових моделей та вибір ефективних контрзаходів для захисту цих систем.

#### Статті у журналах з кваліфікацією Q3:

Ensuring the Data Integrity in Infocommunication Systems / V. Pevnev та ін. *International Journal of Computing*. 2022. С. 228–233. DOI: <https://doi.org/10.47839/ijc.21.2.2591>

Здобувач розглядає питання забезпечення цілісності даних у інформаційно-комунікаційних системах та їхній вплив на ефективність функціонування таких систем, опираючись на аналіз сучасних методів та технологій.

Zemlianko H., Kharchenko V. Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique. *Radioelectronic and Computer Systems*. 2023. № 4. С. 152–170. DOI: <https://doi.org/10.32620/reks.2023.4.11>

Здобувач представив розробку концептуальної моделі та методики на основі ІМЕСА для аналізу ризиків кібербезпеки в системах багатофункціональних флотів безпілотних апаратів.

Torianyk V., Kharchenko V., Zemlianko H. IMECA based assessment of internet of drones systems cyber security considering radio frequency vulnerabilities //IntelITSIS //CEUR Workshop Proceedings. – 2021. – С. 460-470

Здобувач провів оцінку кібербезпеки систем Інтернету речей на основі ІМЕСА з урахуванням вразливостей радіочастотної смуги для безпілотних апаратів.

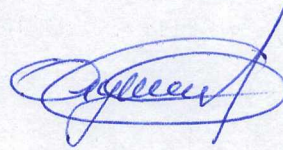
## **8. Висновок наукового керівника**

Виконання індивідуального навчального плану, індивідуального плану наукової роботи, досягнення результатів навчання за відповідною освітньо-науковою програмою та написання дисертації Землянком Георгієм Андрійовичем – вважаю успішним. Дисертаційна робота є результатом самостійного

дослідження, завершеною науковою працею, яка містить наукову новизну. Вона виконана на належному науковому рівні та відповідає встановленим вимогам до дисертацій докторів філософії, і може бути рекомендована до захисту, а її автор Землянко Георгій Андрійович, до присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Отже, вважаємо що дисертаційна робота Землянко Георгія Андрійовича «Методи та засоби для забезпечення кібербезпеки системи багатофункційних флотів безпілотних апаратів в умовах комбінованих кібератак», подана на здобуття наукового ступеня доктора філософії відповідає вимогам Порядку присудження ступеня доктора філософії (Постанова Кабінету Міністрів України від 12 січня 2022 р. № 44). Відтак, може бути представлена до захисту в разовій спеціалізованій вченій раді для присудження ступеня доктора філософії в галузі знань в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Головуючий на засіданні  
кандидат технічних наук, професор, заступник завідувача кафедри  
комп'ютерних систем, мереж і кібербезпеки  
Національного аерокосмічного університету  
ім. М. С. Жуковського «Харківський  
авіаційний інститут»



Клайд ФУРМАНОВ