ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації *Абакумова Артема Ігоровича* на тему «Методи та засоби комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів», представлену на здобуття ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека

На засіданні кафедри кібербезпеки та інтелектуальних інформаційних технологій за участі:

Харченка Вячеслава Сергійовича, чл.-кор. НАН України, д.т.н., професора, завідувача кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Фесенка Германа Вікторовича, д.т.н., професора, професора кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Брежнєва Євгена Віталійовича, д.т.н., професора кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Пєвнєва Володимира Яковлевича, д.т.н., доцента, професора кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Клюшнікова Ігоря Миколайовича, д.т.н., ст. наук. співр., доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Перепелицина Артема Євгеновича, к.т.н., доцента, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Колісник Марини Олександрівни, к.т.н., доцента, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Піскачова Олександра Івановича, к.т.н., ст. наук. співр., доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Бабешка Євгена Васильовича, к.т.н., доцента, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Дужого В'ячеслава Ігоровича, к.т.н., доцента, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Тецького Артема Григоровича, к.т.н., доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Куланова Віталія Олександровича, к.т.н., доцента, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Землянка Георгія Андрійовича, д.ф., доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Вдовіченка Олександра Олександровича, д.ф., доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Дужої Вікторії Вікторівни, ст. викладача кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Холодної Зої Борисівни, ст. викладача кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;

Желтухіна Олександра Васильовича, ст. викладача кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;
Годунова Олександра Сергійовича, ст. викладача кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;
Демури Руслана Івановича, аспіранта кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;
Семенця Олександра Юрійовича, аспіранта кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;
Остапенка Леоніда Юрійовича, аспіранта кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;
Неретіна Олексія Сергійовича, аспіранта кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;
Канарського Євгенія Олександровича, аспіранта кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;
Щеглова Владислава Романовича, аспіранта кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;
Скоробогатька Станіслава Віталійовича, аспіранта кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;
Юдіна Олеся Вікторовича, аспіранта кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;
Косаревського Богдана Валерійовича, аспіранта кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»;
Стряпуніна Антона Олександровича, аспіранта кафедри кібербезпеки та інтелектуальних інформаційних технологій «ХАІ»,

а також запрошених:
Соколової Євгенії Віталіївни, к.т.н., доцента, доцента кафедри інженерії програмного забезпечення «ХАІ»;
Федоренка Миколи Івановича, к.т.н, асистента кафедри прикладної лінгвістики «ХАІ»;
Заславського Володимира Анатолійовича, д.т.н., професора, професора кафедри математичної інформатики Київського національного університету імені Тараса Шевченка;
Волочія Богдана Юрійовича, д.т.н., професора, професора кафедри програмно-апаратних систем інфокомунікацій Національного університету «Львівська політехніка»;
Каштальян Антоніни Сергіївни, д.т.н, доцента, професора кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету;
Яцківа Василя Васильовича, д.т.н, професора, завідувача кафедри кібербезпеки Західноукраїнського національного університету;
Коваля Василя Сергійовича, к.т.н, доцента кафедри інформаційно-обчислювальних систем та управління Західноукраїнського національного університету;

Бикового Павла Євгеновича, к.т.н, доцента кафедри інформаційно-обчислювальних систем та управління Західноукраїнського національного університету,

відбулася публічна презентація дисертаційної роботи *Абакумова Артема Ігоровича* на тему «**Методи та засоби комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів**».

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

1. Актуальність теми дослідження

Актуальність теми дослідження зумовлена стрімким розширенням сфер застосування безпілотних авіаційних комплексів, які еволюціонували від засобів точкової розвідки до багатофункціональних платформ, що виконують завдання спостереження, ударного ураження, логістичного забезпечення та захисту військ у чутливих операційних середовищах, де компрометація системи керування або розкриття місцезнаходження оператора безпосередньо загрожує виконанню місії та безпеці особового складу. Масштабне залучення комерційних моделей безпілотних авіаційних комплексів в умовах збройних конфліктів додатково загострює проблему, адже такі апарати можуть містити вразливості в механізмах телеметрії та ідентифікації, а їх прошивки, модифіковані з тактичною метою маскування, можуть вносити нові вразливості. Водночас засоби радіоелектронної боротьби, що діють на фізичному та протокольному рівнях (глушіння, GPS-спуфінг, перехоплення каналу керування), є одним з основних чинників втрат безпілотних повітряних суден на лініях бойового зіткнення, а рівень цих втрат унеможливлює покладання виключно на реактивні підходи до кіберзахисту. Існуючі методи оцінювання захищеності безпілотних авіаційних комплексів переважно спираються або на аналітичні процедури експертного оцінювання критичності загроз, або на ізольоване тестування на проникнення, і не забезпечують комплексного врахування як невизначеності щодо вразливостей нульового дня, так і результатів їх емпіричної верифікації, що знижує повноту й достовірність оцінювання та обґрунтованість вибору контрзаходів. Це обумовлює необхідність розроблення комбінованих методів, здатних поєднати аналіз режимів вторгнень з процедурами тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів.

2. Зв'язок роботи з науковими програмами, планами, темами

Отримані автором результати дисертації виконано на кафедрі кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «ХАІ» в рамках виконання держбюджетних науково-дослідницьких робіт: «Наукові засади і методи забезпечення гарантоздатності флотів БПЛА інтелектуальних систем моніторингу

потенційно небезпечних і військових об'єктів» (№ Д/Р 0121U112172, 2021-2023 рр.); «Методи, програмно-апаратні засоби та технології забезпечення гарантоздатності інтелектуальних систем індустріального інтернету речей» (№ Д/Р 0122U001065, 2022-2023 рр.); «Методи, засоби та технології моделювання, розроблення, розгортання та забезпечення гарантоздатності мобільних інтелектуальних систем для об'єктів критичної інфраструктури» (№ Д/Р 0124U003250, 2024-теперішній час).

3. Наукова новизна отриманих результатів

У дисертації вперше одержані такі нові наукові результати:

1. Вперше запропоновано комбінований метод аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів, який на відміну від відомих, базується на визначенні сумісності, послідовності проведення та виборів варіантів аналітичних та експериментальних процедур аналізу вразливостей та вторгнень, що надає змогу підвищити повноту і достовірність оцінювання.
2. Удосконалено метод оцінювання кібербезпеки безпілотних авіаційних комплексів в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень, який базується на застосування марковських моделей, що забезпечує можливість отримання кількісних показників готовності залежно від тривалості та періодичності тестування на проникнення.
3. Удосконалено ризик-орієнтований метод аналізу режимів вторгнень та їх наслідків шляхом визначення кінцевих ризиків за результатами апостеріорного аналізу з використанням процедур тестування на проникнення, що дозволяє підвищити обґрунтованість вибору контрзаходів.

4. Теоретичне та практичне значення результатів роботи

Теоретичне значення результатів роботи полягає у розвитку підходів до забезпечення кібербезпеки безпілотних авіаційних комплексів шляхом поєднання аналітичного апарату аналізу режимів вторгнень та їх наслідків з емпіричними процедурами тестування на проникнення, що дозволяє комплексно враховувати як невизначеність щодо вразливостей компонентів безпілотних авіаційних комплексів, так і результати їх верифікації в умовах активних кіберзагроз. Розроблені марковські моделі операційної діяльності безпілотних авіаційних комплексів розвивають математичний апарат кількісного оцінювання кіберстійкості, забезпечуючи отримання показників готовності залежно від тривалості та періодичності тестування. Отримані моделі та методи формують основу для подальших досліджень у галузі аналізу режимів вторгнень та тестування на проникнення кіберфізичних систем, зокрема флотів безпілотних платформ.

Практичне значення полягає у можливості застосування розроблених методів і засобів для оцінювання кібербезпеки безпілотних авіаційних комплексів на етапах проєктування, адаптації та передексплуатаційного аудиту, зокрема при залученні комерційних моделей безпілотних авіаційних комплексів до виконання чутливих місій. На базі запропонованого комбінованого методу розроблено алгоритми та елементи технології, які забезпечують обґрунтований

вибір контрзаходів за встановленими критеріями та дозволяє знизити ризики перехоплення каналу керування, витоку службових даних і розкриття місцезнаходження оператора.

Отримані наукові результати можуть бути використані у підрозділах, відповідальних за забезпечення кібербезпеки безпілотних авіаційних комплексів, у службах технічного супроводу безпілотних комплексів, у навчальних програмах підготовки фахівців з кібербезпеки безпілотних систем, науково-дослідних проєктах, а також адаптовано для застосування до інших кіберфізичних систем.

5. Апробація/використання результатів дисертації

Основні результати роботи представлені на конференціях:

1. «Критичні комп'ютерні технології та системи (КриКТехС-2022/6/171)» (м. Харків, Україна, 2022 р.);

2. "Dependable System, Services and Technologies Conference (DESSERT'2022)" (Athens, Greece, 2022);

3. II НТК «Інформаційна, функціональна та кібербезпека (СКІФіК-2022)» (м. Харків, Україна, 2022 р.);

4. "International Conference on Computational Linguistics and Intelligent Systems (COLINS-2023)" (Kharkiv, Ukraine 2023);

5. "Polish Conference on Artificial Intelligence (PP-RAI'2023)" (Lodz, Poland, 2023);

6. Молодіжний науково-технічний семінар «Гарантоздатні Інформаційні Технології» (ГІТ) (м. Харків, Україна, 2023, 2025);

7. "Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)" (Naples, Italy, 2025).

Результати дисертаційного дослідження впроваджено:

– у навчальному процесі кафедри кібербезпеки та інтелектуальних інформаційних технологій у вигляді лекційного матеріалу та лабораторних занять у навчальній дисципліні «Штучний інтелект і бази знань», зокрема, під час розгляду підходів до аналізу вразливостей, виявлення режимів вторгнень, ризик-орієнтованого оцінювання кіберзахищеності та вибору контрзаходів для кіберфізичних систем і систем штучного інтелекту, а також при виконанні кваліфікаційних робіт бакалаврів і магістрів кафедри за спеціальністю «Кібербезпека та захист інформації»;

– при виконанні науково-дослідницьких робіт «Наукові засади і методи забезпечення гарантоздатності флотів БПЛА інтелектуальних систем моніторингу потенційно небезпечних і військових об'єктів» (№ Д/Р 0121U112172, 2021-2023 рр.), «Методи, програмно-апаратні засоби та технології забезпечення гарантоздатності інтелектуальних систем індустріального інтернету речей» (№ Д/Р 0122U001065, 2022-2023 рр.);

«Методи, засоби та технології моделювання, розроблення, розгортання та забезпечення гарантоздатності мобільних інтелектуальних систем для об'єктів критичної інфраструктури» (№ Д/Р 0124U003250, 2024-теперішній час);

– при розробленні, тестуванні та супроводження програмного продукту WebSpellChecker SDK, призначеного для перевірки правопису, граматики, стилю та інтелектуального опрацювання тексту (компанія ТОВ «ВЕБСПЕЛЧЕКЕР»).

6. Дотримання принципів академічної доброчесності

Дисертація А.І. Абакумова 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 з Internet-джерелами, про що буде надано відповідний звіт.

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

За результатами досліджень опубліковано 9 наукових праць, у тому числі:

– 2 статті у фахових виданнях України категорії «А», проіндексовані в базі Scopus;

– 2 статті у наукових фахових виданнях України категорії «Б» за спеціальністю;

– 1 розділ в колективній монографії;

– 2 публікації у матеріалах міжнародних конференцій з індексацією у Scopus;

– 1 публікація у матеріалах міжнародної конференції;

– 1 публікація у матеріалах національної конференції.

Статті в фахових виданнях України категорії «А», проіндексовані в базі Scopus:

1. Abakumov A., Kharchenko V., Popov P. Proactive unmanned aerial system cybersecurity analysis: combining a priori – a posteriori IMECA and penetration testing methods. *Radioelectronic and Computer Systems*. 2026. No. 1(117).

У статті розроблено метод проактивного аналізу кібербезпеки безпілотних авіаційних комплексів, який поєднує ризик-орієнтоване оцінювання режимів вторгнення з застосуванням IMECA з їх емпіричною валідацією через процедури тестування на проникнення. Запропоновано блок-схему, яка формалізує процес виявлення вразливостей та потенційних режимів вторгнення та мінімізує невизначеність при оцінці ризиків. Експериментальну перевірку методу виконано на SITL платформі, що дозволило підтвердити попередньо виявлені режими вторгнення та ідентифікувати 35 додаткових. Побудовано апріорні та апостеріорні таблиці IMECA і матриці критичності, сформовано перелік контрзаходів, потенційне впровадження яких усуває всі неприйнятні ризики, знижуючи ризик більшості режимів вторгнення до контрольованої зони.

2. Abakumov A., Kharchenko V., Ponochovnyi Y. UAV cyber resilience assessment method: combining IMECA, penetration testing and state-space Markov modelling. *International Journal of Computing*. 2025. Vol. 24. No. 4. P. 790–801. DOI: 10.47839/ijc.24.4.4346.

У статті розроблено комбінований метод оцінювання кіберстійкості безпілотних авіаційних комплексів, що інтегрує аналітичні процедури IMECA та тестування на проникнення з марковським моделюванням у просторі станів, формалізованим в нотації IDEF0. Проведено аналіз чутливості побудованої моделі, який виявив, що швидкість реагування системи є найбільш критичним фактором кіберстійкості. Встановлено, що зростання часу відновлення після інциденту спричиняє зниження коефіцієнта готовності на 31,2% та майже подвоює ризик компрометації, тоді як підвищення ймовірності успішного відновлення забезпечує зростання ймовірності виконання місії на 83,6%. Спростовано гіпотезу щодо ефективності частого тестування на проникнення: зміна інтервалу перевірок має незначний вплив на готовність системи, тоді як надмірна тривалість процедур знижує її на 51,0%, що вказує на доцільність зосередження зусиль на швидкості та автоматизації тестування, а не на його частоті.

Статті в наукових виданнях України категорії «Б», затверджених як фахові за спеціальністю 125:

1. Abakumov A., Kharchenko V. Combined method of UAV cyber assets security assessment by use of procedures IMECA and penetration testing. *Автоматизовані системи управління та прилади автоматики*. 2025. № 187. С. 200–219. DOI: 10.30837/0135-1710.2025.187.200.

У статті виявлено розрив між теоретичними методами оцінювання ризиків і практичними інструментами тестування на проникнення кіберактивів безпілотних літальних апаратів та розроблено комбінований метод аналізу. Запропонована IDEF0-модель охоплює чотири етапи: збір інформації та оцінювання вразливостей, реплікацію режимів вторгнення, IMECA-аналіз і вибір контрзаходів. Розгорнуто та апробовано тестове середовище на базі симуляційної платформи, що надає змогу відтворювати 80% пріоритетних режимів вторгнення, чим підтверджено практичну застосовність запропонованого методу.

2. Абакумов А., Харченко В. Тестування на проникнення систем інтернету речей: кіберзагрози, методи та етапи. *Електронне моделювання*. 2022. Т. 44, № 4. С. 79–104. DOI: 10.15407/emodel.44.04.079.

У статті проведено аналіз особливостей систем інтернету речей як об'єктів тестування на проникнення, визначено їх загрози та вразливості за результатами систематизації джерел за п'ятьма напрямами. Оцінено наслідки атак із застосуванням методу IMECA, проаналізовано контрзаходи та їх ефективність щодо зменшення наслідків атак. Деталізовано етапи проведення тестування на проникнення систем інтернету речей та сформульовано рекомендації щодо подальших досліджень.

8. Висновок наукового керівника

Виконання індивідуального навчального плану, індивідуального плану наукової роботи, досягнення результатів навчання за відповідною науково-освітньою програмою та написання дисертації Абакумовим Артемом Ігоровичем вважаю успішним. Дисертаційна робота є результатом самостійного дослідження, завершеною науковою працею, яка містить наукову новизну. Вона виконана на високому науковому рівні та відповідає всім установленим вимогам до дисертацій на здобуття наукового ступеня доктора філософії, й може бути рекомендована до захисту, а її автор Абакумов Артем Ігорович – до присудження наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Отже, вважаємо, що дисертаційна робота Абакумова Артема Ігоровича на тему «Методи та засоби комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів», представлена на здобуття ступеня доктора філософії, відповідає вимогам Порядку присудження наукового ступеня доктора філософії (Постанова Кабінету Міністрів України від 12 січня 2022 р. №44). Відтак, вона може бути представлена до захисту в разовій спеціалізованій раді для присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Головуючий на засіданні
доктор технічних наук, старший науковий співробітник,
доцент кафедри кібербезпеки та
інтелектуальних інформаційних технологій
Національного аерокосмічного університету
«Харківський авіаційний інститут» Ігор КЛЮШНІКОВ

03.04.2026 р.