Рішення
разової спеціалізованої вченої ради
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії **Абакумов Артем Ігорович**, 1991 року народження, громадянин України, освіта вища: у 2014 році закінчив Національний технічний університет «Харківський політехнічний інститут» і отримав повну вищу освіту за спеціальністю «Інформаційні вимірювальні системи» та здобув кваліфікацію інженера-електрика. Виконав акредитовану освітньо-наукову програму «Кібербезпека».

Разова спеціалізована вчена рада утворена наказом ректора Національного аерокосмічного університету «Харківський авіаційний інститут» Міністерства освіти і науки України, м. Харків, від «22» квітня 2026 року № 187 у складі (без змін):

голови разової спеціалізованої вченої ради – Лукіна Володимира Васильовича, доктора технічних наук, професора, завідувача кафедри інформаційно-комунікаційних технологій ім. О. О. Зеленського Національного аерокосмічного університету «Харківський авіаційний інститут»;

рецензентів – Фесенка Германа Вікторовича, доктора технічних наук, професора, професора кафедри кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут»;

Клюшнікова Ігоря Миколайовича, доктора технічних наук, старшого наукового співробітника, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут»;

офіційних опонентів – Яцківа Василя Васильовича, доктора технічних наук, професора, завідувача кафедри кібербезпеки Західноукраїнського національного університету;

Каштальян Антоніни Сергіївни, доктора технічних наук, доцента, професора кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету

на засіданні «22» червня 2026 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології Абакумову Артему Ігоровичу на підставі публічного захисту дисертації «Методи та засоби комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів» за спеціальністю 125 Кібербезпека.

Дисертацію виконано в Національному аерокосмічному університеті «Харківський авіаційний інститут» Міністерства освіти і науки України, м. Харків.

Науковий керівник: Харченко Вячеслав Сергійович, член-кореспондент НАН України, доктор технічних наук, професор, завідувач кафедри кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут».

Дисертацію подано у вигляді спеціально підготовленого рукопису, у якому відображено нові науково обгрунтовані результати проведених здобувачем досліджень, що виконують конкретне наукове завдання і мають вагоме значення для галузі знань 12 Інформаційні технології. Дисертація виконана державною мовою і відповідає встановленим МОН вимогам щодо оформлення дисертації. Обсяг основного тексту є достатнім для розкриття теми в межах галузі 12 Інформаційні технології за спеціальністю 125 Кібербезпека. Таким чином, у дисертації дотримано вимоги п. 6 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу

вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами).

Здобувач має 9 наукових праць за темою дисертації, з яких 4 статті опубліковано в наукових фахових виданнях України, зокрема 2 – у виданнях, внесених до міжнародної наукометричної бази даних Scopus, 4 – у матеріалах національних та міжнародних наукових конференцій, 1 – розділ у колективній монографії.

Наукові праці, у яких висвітлено основні наукові результати дисертації:

1. Абакумов А. І., Харченко В. С. 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.

2. 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.

3. 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.

4. 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). P. 282–298. DOI: 10.32620/reks.2026.1.18.

У дискусії взяли участь (голова, рецензенти, офіційні опоненти, інші присутні) та висловили зауваження:

Рецензент Фесенко Герман Вікторович:

1. У переліку використаних джерел дисертаційної роботи частка україномовних наукових публікацій є порівняно незначною, а праці інших українських дослідників у дотичних напрямах представлені обмежено. З огляду на активний розвиток вітчизняних досліджень у сфері кібербезпеки кіберфізичних і безпілотних систем, доцільним було б ширше врахувати відповідні наукові результати, що посилило б позиціювання роботи в національному науковому контексті.

2. Під час формалізації марковських моделей автором прийнято припущення, що кібератаки можуть відбуватися лише у стані S1 (виконання місії). Таке спрощення є зрозумілим з погляду побудови моделі, однак воно обмежує її застосовність до сценаріїв, у яких компрометація компонентів безпілотного авіаційного комплексу може відбуватися на етапі підготовки місії, у стані готовності або після завершення польоту. Зокрема, це може стосуватися модифікації прошивки, компрометації бортових комп'ютерів, станції наземного керування або кібератак через ланцюг постачання.

3. Дослідження зосереджено виключно на оцінці кібербезпеки одиничного безпілотного авіаційного комплексу, тоді як сучасні тенденції передбачають і їх застосування у складі гетерогенних безпілотних систем, а саме у координованій взаємодії з іншими безпілотними авіаційними комплексами та наземними роботизованими засобами. Запропонований комбінований метод і розроблені марковські моделі не враховують специфіки кіберзахисту подібних архітектур.

Рецензент Клюшніков Ігор Миколайович:

1. У роботі основну увагу приділено превентивному аналізу вразливостей та обґрунтуванню контрзаходів, спрямованих на зниження ймовірності успішної експлуатації вразливостей безпілотних авіаційних комплексів. Водночас показники резильєнтності безпілотного авіаційного комплексу, тобто здатності системи зберігати функціональність у разі часткової компрометації або продовжувати місію у режимі деградованих можливостей, у формальному апараті дослідження не вводяться. Як свідчить досвід бойового застосування, повне запобігання компрометації не завжди можливе, тож кількісне оцінювання сценаріїв продовження місії після успішної атаки на окремі компоненти безпілотного авіаційного комплексу становить важливий аспект оцінки його кібербезпеки.

2. У четвертому розділі представлено програмний засіб, апробований на послідовному сценарії режиму вторгнення, що охоплює Wi-Fi-деавтентифікацію та подальшу атаку за словником. Водночас подальші етапи розвитку атаки не автоматизовано, що дещо обмежує демонстрацію можливостей запропонованого програмного засобу для відтворення складніших сценаріїв вторгнень.

3. Тестування на проникнення реалізовано переважно з використанням традиційних інструментів, зокрема aircrack-ng. З огляду на сучасні тенденції розвитку кібербезпеки, доцільним було б у подальших дослідженнях розглянути можливість залучення інструментів штучного інтелекту для виявлення сценаріїв атак, адаптивного тестування на проникнення та оптимізації послідовностей експлуатації вразливостей. Це могло б підвищити адаптивність запропонованого методу до невідомих режимів вторгнень.

Офіційний опонент Яцків Василь Васильович:

1. Матриця MITRE ATT&CK згадується у функціональній моделі (підрозділ 2.2.3) як один з елементів керування, що використовується для моделювання кіберзагроз. Однак у фактичному застосуванні методу в розділі 4 структуроване зіставлення виявлених режимів вторгнень з тактиками та техніками MITRE ATT&CK не проводиться.

2. У функціональній моделі рівня А3 передбачено застосування динамічного фаззингу, однак у розділі 4 експериментальна апробація фаззингу не здійснюється.

3. У підрозділі 3.2.1 формалізовано 10-бальну ординальну шкалу оцінювання показників ймовірності (P) та тяжкості (S) з лінійною нормалізацією до інтервалу (0; 1] та трирівневою лінгвістичною класифікацією. Зокрема, у формулі (3.28) встановлюються граничні значення: «Низька» – (0; 0.3], «Середня» – (0.3; 0.7], «Висока» – (0.7; 1.0]. Натомість у розділі 4 використовуються виключно лінгвістичні позначення L/M/H без явного зазначення числових значень ймовірності та тяжкості.

Офіційний опонент Каштальян Антоніна Сергіївна:

1. У підрозділах 3.1.1-3.1.3 здобувач наводить базові значення параметрів марковських моделей (табл. 3.1, 3.2, 3.4, 3.5, 3.7 та 3.8), серед яких визначальну роль для оцінювання впливу тестування на проникнення на готовність безпілотних авіаційних комплексів відіграють періодичність (T_{PT}) та тривалість тестування (τ_{PT}). Проте супровідне обґрунтування вибору значень цих параметрів є недостатньо розгорнутим. Наведені характеристики базових значень відображають експертне судження без емпіричного підкріплення. Зокрема, відсутні посилання на опубліковані дослідження аналогічних кіберфізичних систем реального часу, у яких можуть бути представлені відповідні часові розподіли. Виконані аналізи чутливості демонструють відносний вплив параметрів на коефіцієнт готовності, однак це не знімає питання щодо обґрунтованості вибору базових значень.

2. У табл. 4.5 подано матрицю критичності, згідно з якою після впровадження рекомендованих контрзаходів усі виявлені режими вторгнень переходять до зони низького ризику, за винятком трьох режимів із залишковим середнім ризиком. Однак механізм кількісного переоцінювання показників ймовірності та тяжкості після впровадження контрзаходів у тексті не висвітлено, а формальне відображення цих змін у роботі відсутнє.

3. У підрозділі 2.1.2 виконано систематичне порівняння одинадцяти методів аналізу та оцінювання кібербезпеки за п'ятьма критеріями на методологічному рівні. Проте у розділі 4 запропонований комбінований метод не зіставляється експериментально з результатами застосування альтернативних підходів до тієї ж самої симуляційноїплатформи. Зокрема, відсутнє кількісне порівняння з ізольованим IMECA-аналізом, з класичним тестуванням на проникнення без аналітичних етапів або з іншими комбінованими підходами.

4. У підрозділі 4.1.4 на апріорному етапі IMECA-аналізу зазначено лише два режими вторгнень – Wi-Fi-деавтентифікацію та атаку за словником, обидва з яких ідентифіковано виключно за результатами активної розвідки та сканування цільової мережі. Однак у таксономії кіберзагроз, наведеній у підрозділі 1.1.2, описано суттєво ширший спектр потенційно застосовуваних до досліджуваної конфігурації можливих режимів вторгнень, які могли б бути включені до апріорної таблиці аналітично, до проведення експериментальної верифікації.

5. У підрозділі 2.2.2 декомпозиція функціональної моделі (Додаток А, рис. А.1) виявлення вразливостей реалізується двома паралельними блоками: оцінювання відомих вразливостей через зіставлення з базами вразливостей та виявлення вразливостей «нульового дня». Виходи обох блоків консолідуються та передаються на вхід апріорного IMECA. Однак у тексті відсутні формалізовані правила інтеграції цих двох категорій вразливостей, як обробляються потенційні конфлікти між аналітичними оцінками з різних джерел, та яким чином агрегуються ймовірнісні характеристики при паралельному виявленні однієї і тієї ж вразливості обома блоками.

Результати відкритого голосування:

«За» 5 членів ради,

«Проти» 0 членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує Абакумову Артему Ігоровичу ступінь доктора філософії з галузі знань 12 Інформаційні технології, за спеціальністю 125 Кібербезпека.

Відеозапис трансляції захисту дисертації додається.

Окрема думка члена разової ради не надходила.

Голова разової спеціалізованої вченої ради _____ Володимир ЛУКІН
(підпис)

Підпис голови разової спеціалізованої
вченої ради Володимира ЛУКІНА
засвідчую
Вчений секретар Національного
аерокосмічного університету «Харківський
авіаційний інститут» _____ Тетяна БОНДАРЄВА
(підпис)

М.П.