

РЕЦЕНЗІЯ

Фесенка Германа Вікторовича
на дисертаційну роботу
Абакумова Артема Ігоровича
на тему «Методи та засоби комбінованого аналізу вторгнень і тестування на проникнення
для забезпечення кібербезпеки безпілотних авіаційних комплексів»,
подану на здобуття ступеня доктора філософії
у галузі знань 12 Інформаційні технології
за спеціальністю 125 Кібербезпека

Актуальність теми дисертації.

Актуальність дисертаційної роботи визначається необхідністю розвитку методів і засобів оцінювання кібербезпеки безпілотних авіаційних комплексів як складних кіберфізичних систем, що застосовуються у завданнях моніторингу інфраструктури, спостереження, логістичного забезпечення, реагування на надзвичайні ситуації, а також у військових операціях. Такі комплекси поєднують бортові, наземні та комунікаційні складові, а їх функціонування залежить від захищеності каналів керування, навігації, телеметрії та передавання даних. У зв'язку з цим порушення конфіденційності, цілісності або доступності окремих компонентів може безпосередньо впливати на виконання польотного завдання, збереження апарата та безпеку оператора.

У дисертаційній роботі обґрунтовано, що аналіз кібербезпеки безпілотних авіаційних комплексів має виконуватися з урахуванням невизначеності кіберзагроз, вразливостей і можливих режимів вторгнень. Особливу складність становить те, що наявність вразливості не завжди дає змогу однозначно оцінити її наслідки без експериментальної перевірки, а виключно реактивні засоби кіберзахисту не забезпечують достатнього рівня попереднього виявлення та оцінювання критичних режимів вторгнень. Це зумовлює потребу в систематизації вразливостей і кібератак, формалізованому оцінюванні критичності їх наслідків та визначенні впливу таких режимів на кібербезпеку і готовність безпілотних авіаційних комплексів до виконання місій.

З огляду на зазначене, доцільним є поєднання аналітичних процедур аналізу вторгнень із процедурами експериментального тестування на проникнення. Такий підхід дозволяє підвищити повноту і достовірність оцінювання кібербезпеки безпілотних авіаційних комплексів, уточнювати критичність режимів вторгнень за результатами експериментальної верифікації та обґрунтовувати вибір контрзаходів. Отже, розроблення методів і засобів комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів є актуальним науково-прикладним завданням.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

1. Вперше запропоновано комбінований метод аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів, який, на відміну від відомих, базується на визначенні сумісності, послідовності проведення та виборі варіантів аналітичних та експериментальних процедур аналізу вразливостей та вторгнень, що надає змогу підвищити повноту і достовірність оцінювання кібербезпеки.

2. Удосконалено метод оцінювання кібербезпеки та готовності безпілотних авіаційних комплексів в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень, який базується на застосуванні 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.

Наукові дослідження були виконані здобувачем на кафедрі кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут» в рамках таких науково-дослідних 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 індустриального 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 р. – дотепер) під керівництвом завідувача кафедри кібербезпеки та інтелектуальних інформаційних технологій, доктора технічних наук, професора Харченка Вячеслава Сергійовича.

Достовірність отриманих наукових результатів підтверджується застосуванням комплексу взаємопов'язаних методів дослідження, зокрема системного аналізу, функціонального моделювання, ризик-орієнтованого аналізу, експертного оцінювання, тестування на проникнення та ймовірнісного моделювання. Обґрунтованість запропонованих рішень забезпечується формалізацією процесів аналізу режимів вторгнень, використанням аналітичних та експериментальних процедур оцінювання, апробацією комбінованого методу на симуляційній платформі, а також підтвердженням практичної значущості результатів їх впровадженням у навчальний процес, науково-дослідні роботи та проектно-розробницьку діяльність.

Отже, поставлене в дисертаційній роботі наукове завдання розроблення методів і засобів комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів виконано повністю, а здобувач достатньою мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Абакумова А. І. повністю відповідає Стандарту вищої освіти зі спеціальності 125 Кібербезпека та напрямкам досліджень відповідно до освітньої програми «Кібербезпека».

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення кібербезпеки безпілотних авіаційних комплексів.

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові збіги, можна зробити висновок, що дисертаційна робота Абакумова Артема Ігоровича є результатом самостійних досліджень здобувача і не містить елементів

фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Мова та стиль викладення результатів.

Дисертаційна робота виконана українською мовою та загалом відповідає вимогам наукового стилю. Логіка викладення матеріалу є послідовною: від аналізу предметної області та методів оцінювання кібербезпеки безпілотних авіаційних комплексів до розроблення комбінованого методу, моделей, програмних засобів і практичної апробації результатів. Така структура забезпечує цілісність дослідження та обґрунтованість отриманих наукових результатів.

Матеріал викладено професійно, з дотриманням точності формулювань і коректним використанням спеціалізованої термінології у сфері кібербезпеки, аналізу режимів вторгнень і тестування на проникнення. Складні теоретичні положення супроводжуються необхідними поясненнями, моделями та результатами експериментальної перевірки, що робить зміст роботи доступним для фахівців відповідної галузі.

Структура роботи.

Дисертація складається зі вступу, чотирьох розділів, висновків, переліку використаних джерел і додатків. Загальний обсяг роботи становить 187 сторінок.

У вступі обґрунтовано вибір теми дисертаційного дослідження, визначено об'єкт, предмет, мету і завдання роботи, наведено використані методи дослідження, сформульовано наукову новизну та практичне значення отриманих результатів.

У першому розділі розглянуто безпілотні авіаційні комплекси як об'єкт вторгнень, проаналізовано їх архітектуру, складові, характерні вразливості та кібератаки. На основі аналізу наявних методів оцінювання кібербезпеки безпілотних авіаційних комплексів обґрунтовано доцільність розроблення комбінованого методу аналізу вторгнень і тестування на проникнення. Також у розділі формалізовано показники повноти та достовірності оцінювання режимів вторгнень, визначено загальне й окремі завдання дослідження та обґрунтовано його методiku.

У другому розділі виконано порівняльне оцінювання методів аналізу та оцінювання кібербезпеки безпілотних авіаційних комплексів за визначеними критеріями. На цій основі розроблено функціональну IDEF0-модель комбінованого методу аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів. Модель охоплює послідовність взаємопов'язаних етапів: збирання інформації та аналізу системи, оцінювання відомих вразливостей і виявлення вразливостей «нульового дня» до апіорного ІМЕСА-аналізу, моделювання режимів вторгнень, апостеріорного ІМЕСА-аналізу та марковського моделювання у просторі станів.

У третьому розділі розроблено метод кількісного оцінювання кібербезпеки та готовності безпілотних авіаційних комплексів на основі марковських моделей з урахуванням параметрів тестування на проникнення. За результатами чисельного розв'язання систем рівнянь Чепмена-Колмогорова отримано значення коефіцієнта готовності та виконано аналіз чутливості. Крім того, у розділі представлено ризик-орієнтований метод аналізу режимів вторгнень та їх наслідків, який передбачає формалізацію показників критичності, проведення апіорного й апостеріорного ІМЕСА-аналізу та уточнення результатів через використання процедур тестування на проникнення.

У четвертому розділі наведено результати експериментальної апробації розроблених методів і засобів на спеціалізованій симуляційній платформі. Виконано апіорний та апостеріорний ІМЕСА-аналіз виявлених режимів вторгнень, побудовано дерево вторгнень, розраховано показники повноти й достовірності оцінювання, а також сформовано перелік контрзаходів. Показано, що застосування запропонованих контрзаходів сприяє зниженню кількості режимів вторгнень, які належать до зони неприйнятного ризику. Також у розділі наведено результати впровадження розроблених методів і засобів у навчальний процес, науково-дослідні роботи та проектно-розробницьку діяльність, що підтверджує практичну значущість отриманих результатів.

У висновках узагальнено основні наукові та практичні результати дисертаційної роботи, наведено положення щодо їх значення для забезпечення кібербезпеки безпілотних авіаційних комплексів і окреслено напрями подальших досліджень.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи.

Наукові результати дисертації висвітлені у 9 наукових публікаціях здобувача, серед яких: 4 статті у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України, з яких: 2 статті – у виданнях, проіндексованих у базах даних Scopus (квартили Q2 та Q3); 1 розділ у колективній монографії; 3 публікації у матеріалах міжнародних наукових конференцій та 1 публікація у матеріалах національної наукової конференції.

Також результати дисертаційної роботи апробовано на 7 наукових фахових конференціях і семінарах.

Наукові публікації здобувача відповідають темі дисертації та відображають основні положення і результати проведеного дослідження. У публікаціях, виконаних у співавторстві, особистий внесок здобувача є вагомим і полягає у розробленні моделей та методів, проведенні експериментальних досліджень, а також аналізі й узагальненні отриманих результатів.

Таким чином, основні наукові результати, представлені в дисертаційній роботі, належним чином висвітлено у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

1. У переліку використаних джерел дисертаційної роботи частка україномовних наукових публікацій є порівняно незначною, а праці інших українських дослідників у дотичних напрямках 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 посилює позиціонування 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.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів, а також не впливають на позитивну оцінку дисертаційної роботи.

Висновок про дисертаційну роботу.

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Абакумова Артема Ігоровича на тему «Методи та засоби комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має істотне значення для галузі інформаційних технологій. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п. 6–9 «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 р. № 44.

Здобувач Абакумов Артем Ігорович заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Рецензент:

доктор технічних наук, професор,
професор кафедри кібербезпеки та інтелектуальних
інформаційних технологій
Національного аерокосмічного університету
«Харківський авіаційний інститут»

Герман ФЕСЕНКО