

РЕЦЕНЗІЯ

Ключнікова Ігоря Миколайовича
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 обумовлена зростанням ролі безпілотних авіаційних комплексів у виконанні критично важливих завдань та необхідністю забезпечення їх кібербезпеки в умовах невизначеності кіберзагроз. Складність архітектури таких комплексів, залежність від каналів керування, навігації та обміну даними, а також наявність апаратно-програмних вразливостей зумовлюють потребу в розробленні та удосконаленні методів виявлення, аналізу й оцінювання можливих режимів вторгнень.

У роботі акцентовано увагу на тому, що оцінювання кібербезпеки таких комплексів ускладнюється невизначеністю щодо переліку кіберзагроз, вразливостей та способів їх експлуатації. За цих умов формального виявлення вразливостей недостатньо, оскільки їхній реальний вплив на операційну діяльність комплексу потребує додаткової перевірки.

З огляду на це доцільним є розроблення методів, що поєднують оцінювання режимів вторгнень з їх експериментальною перевіркою шляхом тестування на проникнення. Такий підхід сприяє підвищенню повноти й достовірності оцінювання кібербезпеки, уточненню критичності виявлених режимів вторгнень та обґрунтуванню вибору 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:

- 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;

- 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;

- 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 виконані здобувачем на кафедрі Кібербезпеки та інтелектуальних інформаційних технологій (503) Національного аерокосмічного університету «Харківський авіаційний інститут» в рамках НДР: «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 наукових результатів дисертаційної роботи забезпечується коректним використанням методів системного, функціонального, ризик-орієнтованого та ймовірного аналізу, а також застосуванням процедур тестування на проникнення. Обґрунтованість отриманих результатів підтверджується формалізацією режимів вторгнень, їх експериментальною перевіркою на симуляційній платформі та практичним впровадженням розроблених методів і засобів.

Таким чином, поставлене в дисертаційній роботі наукове завдання розроблення методів і засобів комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів виконано у повному обсязі, а здобувачем продемонстровано високий рівень проведення наукових досліджень.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності. Дисертаційна робота Абакумова А. І. за змістом повністю відповідає Стандарту вищої освіти зі спеціальності 125 Кібербезпека та напрямкам досліджень відповідно до освітньої програми Кібербезпека.

Дисертаційна робота є завершеною науковою працею, яка містить результати особистого внеску здобувача у науковий напрям забезпечення кібербезпеки безпілотних авіаційних комплексів.

За результатом аналізу Звіту подібності за результатами перевірки дисертаційної роботи на текстові збіги, можна зробити висновок, що дисертаційна робота Абакумова Артема Ігоровича є результатом самостійних досліджень здобувача та не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. На використані ідеї, результати і тексти інших авторів в роботі наведені належні посилання на відповідне джерело.

Мова та стиль викладення результатів. Дисертаційна робота виконана українською мовою з використанням наукового стилю. Виклад матеріалу є послідовним і логічно пов'язаним із завданнями дослідження: від аналізу предметної області та методів оцінювання кібербезпеки безпілотних авіаційних комплексів до розроблення власних та удосконалення існуючих методів, розроблення програмних засобів і їх апробації.

Автор коректно використовує спеціалізовану термінологію, дотримується точності формулювань і послідовності аргументації. Подання теоретичних положень

доповнено формалізаціями, моделями, таблицями та результатами експериментальної перевірки, що забезпечує зрозумілість матеріалу для фахівців відповідної галузі.

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

У вступі обґрунтовано тему дисертації, визначено об’єкт, предмет, мету і завдання дослідження, наведено методи дослідження, наведені отримані результати та їх наукова новизна та практичне значення.

Перший розділ присвячено розгляду безпілотних авіаційних комплексів як об’єкта вторгнень, їх архітектури, вразливостей та вектори кібератак. Також виконано аналіз методів оцінювання кібербезпеки, формалізовано показники повноти й достовірності оцінювання режимів вторгнень та обґрунтовано завдання і методіку дослідження.

У другому розділі проведено оцінювання методів аналізу кібербезпеки безпілотних авіаційних комплексів та розроблено функціональну IDEF0-модель комбінованого методу та їх порівняння. Запропоновано модель, що охоплює взаємопов’язані етапи аналізу системи, оцінювання вразливостей, апіорного й апостеріорного ІМЕСА-аналізу, моделювання режимів вторгнень та марковського моделювання.

Третій розділ містить розроблений метод кількісного оцінювання кібербезпеки та готовності безпілотних авіаційних комплексів на основі марковських моделей з урахуванням параметрів тестування на проникнення. Також, у розділі представлено удосконалення ризик-орієнтованого методу ІМЕСА-аналізу шляхом поєднання апіорного й апостеріорного оцінювання з процедурами тестування на проникнення.

У четвертому розділі представлено експериментальні дослідження з апробації розроблених методів і засобів на запропонованій симуляційній платформі. Виконано ІМЕСА-аналіз режимів вторгнень, побудовано дерево вторгнень, розраховано показники повноти й достовірності оцінювання, сформовано перелік контрзаходів. Отримані результати підтверджують їх практичну значущість, також наведено дані щодо їх впровадження.

Висновки містять узагальнення основні результати дисертаційної роботи, їх значення для забезпечення кібербезпеки безпілотних авіаційних комплексів та напрями подальших досліджень.

Оформлення дисертаційної роботи відповідає вимогам, визначеним в наказі Міністерства освіти і науки України від 12 січня 2017 р. № 40 “Про затвердження вимог до оформлення дисертації”.

Оприлюднення результатів дисертаційної роботи. Наукові результати дисертації представлені у 9 наукових публікаціях здобувача, серед яких: 4 статті у наукових виданнях, включених до переліку наукових фахових видань України (на дату опублікування), з яких 2 статті – у виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus і віднесених до першого — третього квартилів (Q1–Q3) відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports; 1 розділ у колективній монографії; 3 публікації у матеріалах міжнародних наукових конференцій та 1 публікація у матеріалах наукової конференції

України. Окрім того, результати дисертаційної роботи апробовано на 7 наукових фахових конференціях і семінарах.

Наукові публікації здобувача пов'язані з темою дисертації та повністю відображають основні результати дослідження. У працях, виконаних у співавторстві, здобувачем зроблено вагомий особистий внесок, який полягає у розробленні моделей і методів, експериментальній перевірці запропонованих рішень, а також аналізі й узагальненні результатів, отриманих у ході досліджень.

За результатами розгляду публікації та результатів апробації можна зробити висновок, що основні наукові результати, представлені в дисертаційній роботі, апробовано та висвітлено у наукових публікаціях здобувача належним чином.

Недоліки та зауваження до дисертаційної роботи:

– 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;

– у четвертому розділі представлено програмний засіб, апробований на послідовному сценарії режиму вторгнення, що охоплює Wi-Fi-деауθενфікацію 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;

– 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.

Наведені зауваження не зменшують цінність, наукову новизну та практичну значимість отриманих результатів та 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, є закінченим науковим дослідженням, яке за сукупністю теоретичних та практичних результатів розв’язує наукове завдання, що має істотне значення для галузі інформаційних технологій. Дисертаційна робота 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, а її автор – Абакумов Артем Ігорович, заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Рецензент:

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

Ігор КЛЮШНІКОВ