

ВІДГУК
офіційного опонента Каштальян Антоніни Сергіївни
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 об'єктивною необхідністю забезпечення кібербезпеки безпілотних авіаційних комплексів. У сучасних умовах ведення бойових дій такі комплекси, зокрема їх адаптовані комерційні моделі, виконують критично важливі завдання розвідки та корегування вогню. При цьому вони функціонують у середовищі постійного впливу широкого спектра загроз – від фізичного придушення сигналів до GPS-спуфінгу та цілеспрямованого перехоплення каналів керування.

Автор звертає увагу на існування суперечності між зростаючими масштабами втрат безпілотних апаратів через вразливості телеметрії та ідентифікації і недостатньою ефективністю виключно реактивних засобів захисту. Наявні штатні механізми за певних умов здатні розкривати критичні службові дані та місцезнаходження оператора, що зумовлює гостру потребу в проактивному виявленні та оцінюванні вразливостей та можливих режимів вторгнень ще до безпосереднього бойового застосування комплексу.

У зв'язку з цим інтегрування різнотипних методів аналізу вторгнень з процедурами активного тестування на проникнення в єдиний методичний цикл є своєчасним рішенням, здатним забезпечити необхідну повноту та достовірність оцінювання критичності режимів вторгнень. Отже, розроблення методів та засобів комбінованого аналізу вторгнень для забезпечення кібербезпеки безпілотних авіаційних комплексів і подальшого впровадження дієвих контрзаходів є надзвичайно актуальним і важливим науково-прикладним завданням.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Проведений аналіз дисертаційної роботи дозволяє зробити висновок про належний рівень обґрунтованості отриманих результатів. Автор застосував комплексний підхід, успішно поєднавши апарат теорії множин, теорії марковських процесів та ризик-орієнтованого аналізу режимів вторгнень і їхніх наслідків (IMECA) з процедурами практичного тестування на проникнення. Сформульоване в роботі наукове завдання вирішено у повному обсязі, що свідчить про високий рівень володіння здобувачем сучасними методами наукових досліджень.

Наукова новизна результатів дисертаційного дослідження полягає в такому:

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.

Достовірність результатів та їх практична значущість підтверджуються ймовірнісним моделюванням, апробацією запропонованого комбінованого методу на симуляційній платформі, а також впровадженням отриманих рішень у навчальний процес Національного аерокосмічного університету «Харківський авіаційний інститут», науково-дослідні роботи та проєктно-розробницьку діяльність ТОВ «ВЕБСПЕЛЧЕКЕР».

У роботі розв'язано актуальне науково-прикладне завдання розроблення методів та засобів аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів. Отримані результати дослідження є новими, обґрунтованими та підтвердженими експериментально.

Отже, в дисертаційній роботі поставлене наукове завдання виконано повністю, здобувач повною 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 повністю відповідає вимогам наукового стилю.

Логіка викладення матеріалу є чіткою та послідовною: дослідження розгортається від ґрунтового аналізу предметної області до розроблення моделей і методів та їх подальшої практичної апробації. Така структура забезпечує цілісність та обґрунтованість отриманих результатів.

Матеріал викладено у доступній формі для фахівців галузі, при цьому складні теоретичні положення супроводжуються необхідними поясненнями та зберігають

доступність для сприйняття. Стиль викладення характеризується професійністю, точністю формулювань і аргументованістю.

Автор коректно використовує спеціалізовану термінологію та понятійний апарат у сфері кібербезпеки.

Структура роботи.

Дисертація складається з вступу, чотирьох розділів, висновків, списку літератури та додатків. Загальний обсяг дисертації 187 сторінок.

У вступі обґрунтовано вибір теми дисертаційного дослідження, сформульовано об'єкт, предмет, мету і завдання дослідження, наведено методи дослідження, а також відображено наукову новизну і практичне значення результатів.

У першому розділі на основі систематизованої таксономії кіберзагроз безпілотних авіаційних комплексів, а також порівняльного аналізу існуючих методів забезпечення кібербезпеки безпілотних авіаційних комплексів аргументовано доцільність розроблення комбінованого методу аналізу вторгнень і тестування на проникнення. Також у цьому розділі формалізовано показники повноти і достовірності оцінювання режимів вторгнень та обґрунтовано загальне й окремі завдання дослідження, а також його методику.

У другому розділі розроблено рамкову модель порівняння методів забезпечення кібербезпеки безпілотних авіаційних комплексів на основі п'яти критеріїв, за якими виконано порівняльне оцінювання одинадцяти наявних методів. Розроблено функціональну модель комбінованого методу аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів, яка охоплює сім послідовно пов'язаних етапів від збирання інформації та аналізу системи до марковського моделювання у просторі станів. Запропонована модель забезпечує покриття всіх п'яти визначених критеріїв.

У третьому розділі запропоновано три марковські моделі операційної діяльності безпілотних авіаційних комплексів з урахуванням параметрів тестування на проникнення. На основі чисельного розв'язання систем рівнянь Чепмена-Колмогорова у середовищі MATLAB отримано базові значення коефіцієнта готовності та виконано аналіз чутливості. Також у цьому розділі представлено ризик-орієнтований метод аналізу режимів вторгнень та їхніх наслідків (ІМЕСА) шляхом формалізації показників критичності та структурованої схеми апіорного й апостеріорного оцінювання з ітеративною верифікацією через процедури тестування на проникнення.

У четвертому розділі виконано експериментальну апробацію розроблених методів та засобів на спеціалізованій симуляційній платформі. Проведено апіорне ІМЕСА-оцінювання, що сформулоало множину з двох аналітично визначених режимів вторгнень, а також апостеріорне ІМЕСА-оцінювання 37 режимів вторгнень з побудовою дерева вторгнень. Розраховано показники повноти оцінювання та обґрунтовано його достовірність, сформовано перелік контрзаходів, матриця критичності після впровадження контрзаходів відображає суттєве зниження кількості режимів, які перебувають у зоні неприйнятної ризику. Крім того, представлений у цьому розділі аналіз результатів впровадження у навчальний процес Національного аерокосмічного університету «Харківський авіаційний інститут», науково-дослідні роботи та ТОВ «ВЕБСПЕЛЧЕКЕР» підтвердив наукову новизну дослідження та його значущість для практичного застосування у сфері кібербезпеки безпілотних авіаційних комплексів.

У висновках наведено основні результати дисертаційної роботи, сформульовано практичне значення отриманих результатів, а також визначено напрями майбутніх 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 Web of Science Core Collection та/або Scopus, віднесених до першого–третього квартилів 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 національної наукової конференції.

Також результати дисертації були апробовані на 7 наукових конференціях і семінарах.

Наукові публікації автора повністю відповідають темі дисертації та підкріплюють її результати. Роботи виконані самостійно, з коректним цитуванням та дотриманням усіх вимог академічної доброчесності.

У публікаціях, виконаних у співавторстві, особистий внесок здобувача є вагомим і пов'язаний із постановкою дослідницьких завдань, розробленням моделей і методів, їх апробацією, а також аналізом та узагальненням отриманих результатів.

Таким чином, наукові результати, описані в дисертаційній роботі, повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

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 (t_{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 симуляційної

платформи. Зокрема, відсутнє кількісне порівняння з ізольованим ІМЕСА-аналізом, з класичним тестуванням на проникнення без аналітичних етапів або з іншими комбінованими підходами.

4. У підрозділі 4.1.4 на апіорному етапі ІМЕСА-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, наведений у підрозділі 1.1.2, описано суттєво ширший спектр потенційно застосовуваних до досліджуваної конфігурації можливих режимів вторгнень, які могли б бути включені до апіорної 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 консоліднуються та передаються на вхід апіорного ІМЕСА. 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.

Вважаю, що висловлені зауваження не є концептуальними, не зменшують загальної наукової новизни та практичної значимості результатів і 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.

Офіційний опонент:

професор кафедри комп'ютерної інженерії та
інформаційних систем
Хмельницького національного університету,
доктор технічних наук, доцент

Антоніна КАШТАЛЬЯН