ВІДГУК

офіційного опонента,
доктора технічних наук, професора, завідувача кафедри прикладної математики та обчислювальної техніки Національної металургійної академії України,
Швачича Геннадія Григоровича

на дисертаційну роботу Давидова В'ячеслава Вадимовича "**Моделі та методи підвищення безпеки байт-код орієнтованого програмного забезпечення в умовах кібератак**", яка подана на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Актуальність теми дисертації.

Існуючі тенденції загального використання комп'ютерних та комп'ютеризованих засобів обумовлюють високий рівень вимог щодо розроблюваного програмного забезпечення. При цьому вимоги до безпеки програмного забезпечення є ще більш високими у зв'язку із збільшенням випадків кібератак. Особливо жорсткі вимоги безпеки висуваються до байт-код орієнтованого програмного забезпечення комп'ютерних систем критичного застосування, де ступінь ризику надзвичайна висока. Однак, як показують події останніх років, нехтування питаннями безпеки програмних засобів в процесі розробки призводить лише до збільшення кількості успішно проведених кібератак та до економічних, фінансових, іміджевих та інших втрат підприємств і держави в цілому.

Одним із основних завдань науковців у цьому напрямі є удосконалення існуючих моделей та методів захисту інформації. Дане завдання широко розглядається в роботах багатьох науковців. Однак відомі роботи більшою мірою мають криптографічну спрямованість і не мають на меті підвищення безпеки на етапах життєвого циклу розробки програмного забезпечення. Крім того, у більшості досліджень не враховується динаміка можливих змін та

приховування програмного коду. Все вищезазначене свідчить про актуальність теми дисертаційної роботи.

Дисертаційна робота Давидова В'ячеслава Вадимовича присвячена вирішенню наукової проблеми підвищення безпеки байт-код орієнтованого програмного коду в умовах кібератак на основі синтезу підсистеми забезпечення конфіденційності та автентичності програмних продуктів.

Дисертаційна робота виконана у межах пріоритетних наукових напрямів, які охоплюють актуальні проблеми, відповідно до рішення Ради президентів академій наук України від 30 січня 2019 року «Про Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019-2023 роки», «Інформатика» за темами: «Розроблення і удосконалення методів верифікації та тестування баз знань», «Розроблення математичних методів та систем моделювання об'єктів та процесів». Дисертаційну роботу виконано в межах зареєстрованих науково-дослідних робіт Національного технічного університету «Харківський політехнічний інститут»: «Дослідження методів управління та захисту даних в комп'ютеризованих інформаційно-вимірювальних та розподілених системах» (ДР №0119U002603) та «Створення завдань по мові програмування "С", тестування методологічної концепції, адаптації програми для інтеграції у систему вищої освіти України» (ДР №0119U103871) в яких автор є співвиконавцем окремих етапів.

Основний зміст роботи.

У *вступі* обґрунтовано актуальність дисертації, визначено мету, об'єкт та предмет дослідження. Сформульовано проблему дисертаційного дослідження, наукові завдання, наведено основні наукові та практичні результати. Відзначено особистий внесок здобувача, апробацію результатів дисертаційної роботи на конференціях, наведено відомості про публікації та структуру роботи.

У *першому розділі дисертаційної роботи* було досліджено модель забезпечення безпеки програмного забезпечення. Аргументовано доказано необхідність розвитку даної моделі шляхом адаптації існуючих вимог до безпеки

програмних засобів протягом усього життєвого циклу розробки програмного забезпечення. Досліджено характеристики якості програмного забезпечення та сформовано універсальний показник безпеки програмних засобів. Вказано на необхідність підвищення безпеки саме *Standalone* типу застосунків. Також доведено вразливість системного рівня *Standalone* застосунків.

У *другому розділі дисертаційної роботи* проведено дослідження алгоритмів перевірки логіко-смислової подібності стандартних послідовних схем програм, заснованих на пошуку найбільш схожих смислових траєкторій програми. Наведено основні поняття, пов'язані з графом спільних обчислень програм. Отримав подальший розвиток метод перевірки логіко-смислової подібності програм складної логічної структури, що відрізняється від відомих розпаралелюванням процесів, що обчислюються при порівнянні подібних елементів програмного коду, а також формуванням та використанням графу спільних обчислень в процесі пошуку подібних елементів коду. Це дозволило розпаралелити дані процеси та досягти поліноміальної складності процесу верифікації, що в свою чергу зменшило час перевірки коду на логіко-смислову подібність для визначення впливу розробленого методу обфускації коду на його коректність.

У *третьому розділі дисертаційної роботи* синтезовано комплекс алгоритмів обфускації і деобфускації програмних модулів, який відрізняється від відомих урахуванням варіативності типів даних. Це дозволило описати дані процеси на верхньому стратегічному рівні формалізації. В рамках дослідження була розроблена уніфікована *GERT*-модель процесу обфускації програмних модулів. Дана модель відрізняється від відомих реалізацією парадигми використання математичного апарату гамма-розподілу в якості ключового на всіх етапах моделювання процесу обфускації. Такий підхід дозволив досягти уніфікації моделі в умовах модифікації *GERT*-мережі. 4. При цьому розроблено методи обфускації строкових літералів та імен ідентифікаторів, доцільність використання яких підтверджено експериментом, в якому наведено, що час, який витрачається на деобфускацію з використанням розроблених засобів обфускації,

до п'яти разів більше. Проаналізовано основні метрики оцінки якості коду та запропоновано теоретичні вдосконалення на основі практичного досвіду аналізу необфускованого коду. Запропоновані вдосконалення засновані на наступних показниках, які будуть відрізнятися в декомпільованому обфускованому і необфускованому вихідних кодах: кількісні показники частоти виникнення операторів мови, такі як оператори циклу, безумовні переходи і мітки; частоті використання ідентифікаторів, таких як змінні, константи, функції. Розроблено спосіб отримання метрик для багатопроектного рішення, що дозволяє отримати зведений файл для можливості подальшої обробки.

У *четвертому розділі дисертаційної роботи* розроблено модель безпечного переходу та кодування ліцензійних ідентифікаторів на основі математичного апарату *GERT*-мереж з парадигмою Гама-розподілу, що дозволило підвищити точність результатів моделювання. Дана логіка впроваджується в залежності від ідентифікаційного або серійного номера ПЗ. Розроблено методологію масштабування розробленої математичної моделі. Показана доцільність використання кожного типу масштабування з урахуванням критичності часу виконання здійснення перевірки безпеки програмного забезпечення на основі ліцензійних ідентифікаторів. Так, при вертикальному масштабуванні, у зв'язку з використанням паралельного процесу обробка даних, час обробки даних практично не змінилося.

У *п'ятому розділі дисертаційної роботи* розроблено модулі програмного комплексу, які демонструють можливість створення цифрового ідентифікатора - ліцензійного ключа з урахуванням індивідуальних даних кінцевого користувача, що запобігає можливості тиражування ліцензійного ключа зловмисниками. Розроблено узагальнену структуру процесу формування цифрового ідентифікатора ПЗ. Відмінною особливістю запропонованої структури є використання формальних даних про комп'ютерні системи, на які ліцензійне ПЗ встановлюється в процесі формування ліцензійного цифрового ідентифікатора. Запропоновано алгоритм функціонування системи і генерації ліцензійного ключа, адаптованого до вхідних даних і можливих умов верифікації ПЗ

Розроблено структурно-функціональну модель формування цифрового ідентифікатора програмного забезпечення для захисту її авторських прав. Відмінною особливістю даної моделі є використанням індивідуальних даних комп'ютерної системи кінцевого користувача для однозначної ідентифікації приналежності. Також, модель враховує можливість вбудовування довільного (заданого розробниками) коду в тіло ліцензійного ключа, який буде виконуватися при верифікації. Дані маніпуляції призвели до ускладнення аналізу та зламу ліцензійної складової програмного забезпечення.

У *шостому розділі дисертаційної роботи* розроблено імітаційну модель системи підвищення безпеки байт-код орієнтованого програмного забезпечення в умовах використання кібератак. Ця модель дозволила провести порівняльні дослідження та отримати кількісні значення показника ефективності розроблених моделей та методів. Наведено рекомендації з практичного використання розроблених методів та засобів підвищення безпеки байт-код орієнтованого програмного забезпечення в умовах використання кібератак.

Висновки по роботі сформульовані достатньо чітко та стисло узагальнюють основні досягнуті результати досліджень та їх практичну реалізацію.

Список використаних джерел охоплює достатню кількість праць зарубіжних та вітчизняних авторів в даній предметній галузі. Опрацьований перелік джерел свідчить про глибокий аналіз сучасного стану досліджуваної проблеми та здобутки в цій сфері.

Наукова новизна дисертаційної роботи.

– Отримав подальший розвиток метод перевірки логіко-смислової подібності програм складної логічної структури, що відрізняється від відомих розпаралелюванням процесів, які обчислюються при порівнянні подібних елементів програмного коду, а також формуванням та використанням графу спільних обчислень в процесі пошуку подібних елементів коду. Це дозволило знизити складність процесу верифікації.

– Вперше розроблена *GERT*-модель процесу обфускації програмних модулів, що реалізує парадигми використання математичного апарату гамма-

розподілу у якості ключового на всіх етапах моделювання процесу обфускації. Це дозволило досягти уніфікації моделі в умовах модифікації *GERT*-мережі.

– Вдосконалено метод обфускації програмних модулів, що відрізняється від відомих урахуванням варіативності типів лексем та ідентифікаторів. Це дозволило підвищити показник безпеки програмного забезпечення.

– Вперше розроблено критерій оцінки якості обфускації програмного забезпечення шляхом синтезу лінійної композиції часткових критеріїв метрик якості коду, що дозволило кількісно оцінити ступінь обфускованості програмних продуктів.

– Вперше розроблено модель безпечного переходу та кодування ліцензійних ідентифікаторів на основі математичного апарату *GERT*-мереж з парадигмою гамма-розподілу, що дозволило підвищити точність результатів моделювання.

– Вдосконалено метод формування цифрового ідентифікатора програмного забезпечення для захисту його авторських прав шляхом введення та вдосконалення модулів менеджерів ліцензій, контроля цілісності та ідентифікації. Відмінною особливістю даного методу є використання індивідуальних даних комп'ютерної системи кінцевого користувача для однозначної ідентифікації приналежності, що дозволило підвищити безпеку байт-код орієнтованих програмних застосунків в умовах кібератак.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їх достовірність.

Обґрунтованість та достовірність наукових положень, висновків і рекомендацій дисертації забезпечується аргументованими результатами досліджень та співставленням з результатами математичного моделювання.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати дають змогу підвищити безпеку байт-код орієнтованих програмних додатків, що в свою чергу дозволяє забезпечити достатній рівень захищеності програмного забезпечення в умовах кібер-атак.

Результати дисертації впроваджені та використовуються у діяльності

підприємств «Line Up», «Нікс Солюшенс ЛТД», Державного підприємства «Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості», Державного підприємства «Харківський науково-дослідний інститут технологій машинобудування», а також використано у навчальному процесі Національного технічного університету «Харківський політехнічний інститут».

Практичне значення отриманих результатів підтверджено відповідними актами впровадження.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на таких наукових конференціях та семінарах: XXIII Міжнародна науково-практична конференція «Інформаційні технології, наука, техніка, технологія, здоров'я» (Харків, 2015); XV Міжнародний науковий семінар «Сучасні проблеми інформатики в управлінні, економіці, освіті та подоланні наслідків Чорнобильської катастрофи» (Шацьк, 2016); 26th National Scientific Symposium with International Participation «Metrology and Metrology assurance» (Sozopol, Bulgaria, 2016); 7th World Congress «Aviation in the XXI-st Century» (Київ, 2016); VII Міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Полтава, 2017); V Міжнародна науково-технічна конференція «Проблеми інформатизації» (Полтава, 2017); 28th International Scientific Symposium «Metrology and Metrology Assurance (MMA)» (Sozopol, Bulgaria, 2018); VI Міжнародна науково-технічна конференція «Проблеми інформатизації» (Черкаси, 2018); Всеукраїнська науково-практична конференція «Актуальні питання протидії кіберзлочинності та торгівлі людьми» (Харків, 2018); 10th International Conference on Dependable Systems, Services and Technologies (DESSERT) (Leeds, UK, 2019); 29th International Scientific Symposium «Metrology and Metrology Assurance (MMA)» (Sozopol, Bulgaria, 2019); Sun SITE Central Europe (CEUR) Workshop Proceedings (Kyiv, 2019); VIII Міжнародна науково-технічна конференція «Проблеми інформатизації»

(Черкаси, 2020); XX Міжнародна науково-практична конференція «Інформаційні технології і безпека» (Київ, 2020); XI Міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Харків, 2021), Fifth International Scientific and Technical Conference «Computer and Information Systems and Technologies» (Kharkiv, 2021).

Публікації. Основні положення дисертації опубліковано в 36 наукових працях, у тому числі: 18 наукових статей (з них 1 входить до бази даних Scopus (другий квартіль); 1 – опубліковано у закордонному рецензованому виданні; 16 – у вітчизняних фахових наукових журналах), 16 тез доповідей (з них 3 входять до бази даних Scopus), а також 2 монографії (з них – 1 одноосібна).

Відповідність автореферату дисертації. Зміст автореферату є ідентичним до змісту дисертації й повною мірою відображає основні завдання, наукову новизну, практичне значення, висвітлює всі отримані результати, висновки та запропоновані рекомендації.

Зауваження по роботі.

Позитивно оцінюючи представлену дисертацію як результат наукового дослідження важливої проблеми, слід висловити ряд міркувань і зауважень, які мають бути розглянуті при захисті та зможуть допомогти автору в його подальшій науковій роботі. Зокрема:

1. У першому розділі дисертаційної роботи автор актуалізує завдання підвищення безпеки ПЗ з одночасним дотриманням вимог до основних показників його якості. На жаль, у своїх подальших дослідженнях дисертант нехтує цими показниками, або розкриває їх сутність не в повному обсязі. Було б доцільним використання показників якості програмного забезпечення як обмеження при моделюванні та вирішенні оптимізаційних завдань.

2. За аналізом досліджень дисертанта, які наведені в третьому, четвертому та п'ятому розділах, можна зробити висновки про наявність невизначеності при формуванні вхідних даних. Але, на жаль, математичний апарат, що використано в дисертаційні роботі не передбачає врахування цього фактору.

3. У третьому розділі отримання метрик якості коду виконується за допомогою бібліотеки *Rolsyn*, яка орієнтова для *C#* додатків. Це накладає обмеження на її використання (наприклад, для *Java* додатків). Доцільно було б розширити спектр досліджуваних бібліотек.

4. На рис. 5.1 дисертаційної роботи при зображенні розташування компонентів системи формування цифрового ідентифікатора програмного забезпечення автору доречно було б зробити окремі уточнення або розмежування, зокрема персонального комп'ютера кінцевого користувача.

5. Зміст поданого дослідження був би більш збалансованим, а висновки більш обґрунтованими за умови повного аналізу інформації щодо характеристики програмних засобів для яких проводились дослідження та оцінка якості обфускації.

6. Подекуди можна зустріти лінгвістичні неточності, коли автор, вживає деякі стійкі вирази у формі, властивій не українській мові. Наприклад, «з леми 4 слідує» замість «з леми 4 випливає» (с. 9 автореферата), «представляється громіздким вираженням» замість «вираз має деяку громіздкість» (с. 114 дисертації), «теорема швидше стверджує» замість «теорема скоріш стверджує» або «теорема більшою мірою стверджує» (с. 61, 167 дисертації), «швидше за все» замість «скоріш за все» (с. 167, 207 дисертації), тощо.

7. Звертає на себе увагу схильність дисертанта до надмірного вживання довгих складнопідрядних речень (с. 51 дисертації, де речення подано на 7 рядках), що, втім, не заважає розумінню змісту роботи і може вважатися певною особливістю авторського стилю.

Відзначені зауваження не ставлять під сумнів основні наукові та практичні результати, і суттєво не впливають на загальну позитивну оцінку дисертаційної роботи.

Завершуючи відгук, слід сказати, що висловлені зауваження не змінюють позитивної оцінки поданої наукової роботи. В цілому, дисертація відрізняється оригінальністю, високим науковим рівнем і новизною, строгим логічним обґрунтуванням, має важливе наукове і практичне значення. Висновки і

положення дисертації аргументовані й достовірні. Публікації автора повно відображають зміст дисертації та підтверджують достатньо високий рівень проведеного дослідження. Зміст роботи, об'єкт і предмет дослідження, основні положення і результати відповідають спеціальності, з якої дисертація подана до захисту.

Висновок.

Дисертаційна робота Давидова Вячеслава Вадимовича представляє собою завершене актуальне наукове дослідження. В роботі отримано нові науково-обґрунтовані результати, які дозволяють розвинути методи та моделі підвищення безпеки байт-орієнтованого програмного забезпечення в умовах кібератак.

Вважаю, що докторська дисертація Давидова В'ячеслава Вадимовича за актуальністю теми, ступенем обґрунтованості наукових положень, рівнем апробації та публікацій, науковою новизною та практичною цінністю отриманих результатів відповідає вимогам, що висуваються до докторських дисертацій згідно п. 9, 10, 12 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567, а сам автор заслуговує на присудження йому наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент,
завідувач кафедри прикладної математики
та обчислювальної техніки
Національної металургійної академії України,
доктор технических наук, професор

Геннадій ШВАЧИЧ

26 серпня 2021

Підпис Г. Швачича

засвідчую

начальник відділу кадрів

В.С. Шифрін

Міністерство освіти і науки України * Національна металургійна академія України * 02070766