Голові спеціалізованої вченої ради
Д 73.052.04 Черкаського державного технологічного університету
18000, м. Черкаси, бул. Шевченка, 460.

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, доцента Бабенко Віри Григорівни на дисертаційну роботу Давидова Вячеслава Вадимовича "Моделі та методи підвищення безпеки байт-код орієнтованого програмного забезпечення в умовах кібератак" на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Актуальність теми дисертації.

Розвиток інформатизації у суспільстві останніх років висунув на одне з перших місць проблему захисту величезної кількості інформації, що формується, оброблюється і передається в комп'ютерних системах, а також підвищення рівня безпеки програмного забезпечення щодо різних дестабілізуючих факторів. Комп'ютерні технології суттєво розширило можливості як легальних користувачів програмного забезпечення, так і зловмисників щодо використання методів і засобів несанкціонованого доступу до програмних продуктів. Окремо це питання стосується байт-код орієнтованого програмного забезпечення, яке має ряд специфічних особливостей розробки та використання у сучасних комп'ютерних системах.

Тому дисертаційна робота Давидова Вячеслава Вадимовича що присвячена вирішенню наукової проблеми підвищення безпеки байт-код орієнтованого програмного коду в умовах кібератак на основі синтезу підсистеми забезпечення конфіденційності та автентичності програмних продуктів. є актуальною.

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 у 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.

Перший розділ присвячено дослідженню моделі забезпечення безпеки програмного забезпечення. Аргументовано доведено необхідність розвитку даної моделі шляхом адаптації існуючих вимог до безпеки програмних засобів протягом усього життєвого циклу розробки програмного забезпечення. Досліджено характеристики якості програмного забезпечення. Доведено, що для забезпечення захищеності програмних продуктів необхідно підвищити якість таких послуг безпеки як: цілісність, автентифікація, конфіденційність, управління доступом. Сформовано універсальний показник безпеки програмних засобів, що відрізняється від відомих зменшенням фактору суб’єктивності вагових коефіцієнтів показника. Зазначено актуальність науково-практичної проблеми підвищення безпеки байт-код орієнтованого програмного коду в умовах кібератак на основі синтезу підсистеми забезпечення конфіденційності та автентичності програмних продуктів.

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 здійснено синтез комплексу алгоритмів обфускації і деобфускації програмних модулів, який відрізняється від відомих урахуванням варіативності типів даних. Це дозволило описати дані процеси на верхньому стратегічному рівні формалізації. Розроблено уніфіковану математичну модель процесу обфускації програмних модулів на базі методу графічної оцінки. В межах моделі розроблено алгоритми обфускації лексем, обфускації строкових виразів, обфускації імен ідентифікаторів та обфускації логічних виразів. Розроблено GERT-модель процесу обфускації програмних модулів, а також досліджено уніфіковану GERT-модель зі зміненою кількістю вузлів та при цьому проведено оцінку якості обфускації програмних модулів. Синтезовано апарат оцінки якості обфускації програмних модулів на основі показників якості програмного продукту та розроблено алгоритм отримання метрик якості коду програмного продукту.

Четвертий розділ дисертаційної роботи присвячено розробці моделі безпечного переходу і 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. 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 змінюється.

У п’ятому розділі 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. Сформований ліцензійний ключ є програмним кодом, що виконується на стороні кінцевого користувача. Розроблено узагальнену структуру процесу формування цифрового ідентифікатора програмного забезпечення. 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.

У шостому розділі 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. Проведена оцінка ефективності розроблених моделей та методів підвищення безпеки програмного забезпечення показала, що їх використання в дисертаційної роботі дозволить збільшити час зламу програмного забезпечення до 1,4 разів. Отримані результати дисертаційної роботи дозволили обґрунтувати рекомендації з практичного використання розроблених методів та засобів підвищення безпеки байт-код орієнтованого програмного забезпечення в умовах використання кібератак.

Наукова новизна дисертаційної роботи.

– 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 знизити складність процесу верифікації.

– Вперше розроблена GERT-модель процесу обфускації програмних модулів на основі реалізації парадигми використання математичного апарату гамма-розподілу у якості ключового на всіх етапах моделювання процесу обфускації, що дозволило уніфікувати моделі в умовах модифікації GERT-мережі.

– Вдосконалено метод обфускації програмних модулів, що відрізняється від відомих урахуванням варіативності типів лексем та ідентифікаторів та дозволяє 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 і 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 продукту 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 кібератак.

Практична цінність роботи полягає у наступному:

– розроблено метод перевірки логіко-смислової подібності програм складної логічної структури для зменшення часу процесу верифікації;

– розроблено алгоритми обфускації програмного коду для підвищення захисту коду від реверс-інжинірингу;

– розроблено критерій оцінки якості обфускації програмного коду для підвищення точності оцінки безпеки програмного забезпечення;

– розроблено алгоритми формування персоналізованого ліцензійного ключа для захисту програмного забезпечення від неліцензійного копіювання;

– розроблено алгоритми захисту ліцензійних ключів від копіювання на основі прихованих переходів та кодування ліцензійного ключа.

Практичне значення отриманих результатів підтверджено відповідними актами впровадження.

Результати дисертації впроваджені і використовуються у діяльності Компанії «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».

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 статтях (з них 1 входить до бази даних Scopus (другий квартиль); 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:

1. На стор. 41 першого розділу дисертаційної роботи зазначено, що значення коефіцієнтів k_n для досліджуваних характеристик, що використовуються у функції при побудові показника безпеки програмного забезпечення, перевагою якої є мінімізація впливу коефіцієнтів, що несуть суб'єктивний характер, обчислені експертним шляхом. Але в дисертаційній роботі не уточнено які саме методи експертної оцінки були використані, яка кількість експертів задіяна, їх компетентність та, як наслідок, яка достовірність отриманих результатів, що використовує автор для подальших розрахунків.

2. У другому розділі автор розробив метод перевірки логіко-смислової подібності програм складної логічної структури для зменшення часу процесу верифікації, але, нажаль, серед практичних рекомендацій, що відокремлені у шостому розділі, рекомендацій щодо використання цього методу не наведено. А це могло б підвищити практичну значимість дисертаційної роботи.

3. На рис. 3.9. стор.122 дисертаційної роботи автор ілюструє графіки щільності розподілу часу виконання процесу обфускації і деобфускації програмних модулів при використанні GERT-мережі, гамма-розподілу ймовірностей переходів. Хоча в дисертаційній роботі не наведено детального опису умов проведення експерименту, а саме не зазначені показники ймовірності переходів та обраних коефіцієнтів щільності ймовірності.

4. У четвертому розділі автором розроблена GERT-мережа процесу ліцензійної безпеки програмного забезпечення. При цьому здобувач у підрозділі 4.3. пропонує нарощування складності GERT-мережі. Нажаль, при вирішенні цього завдання автор нехтує звісними методами еквівалентних перетворень GERT-мережі, які б могли допомогти підвищити точність результатів моделювання.

5. У підрозділі 5.6 автор пропонує результати дослідження розробленого методу формування цифрового ідентифікатора. Зрозумілі обмеження автора

щодо умов проведення експерименту, але доцільно б було навести дані про апаратну складову експерименту та запропонувати рішення, які б розширили можливості апаратної та програмної складової при проведенні подібних досліджень.

6. На мою думку, у дисертаційній роботі існують ряд невдалих термінів та пропозицій, наприклад, підрозділ 4.1.1. закінчується невдалою фразою “Основне завдання включає розробку моделі системи безпеки програмного забезпечення на основі ліцензійних ідентифікаторів на основі побудованих алгоритмів, що використовують GERT-мережі”, або назва розділу 3. “Розробка уніфікованої математичної моделі процесу обфускації програмних модулів на базі методу графічної оцінки на аналіз” і т.і.

7. Автор у своїй дисертаційній роботі визначив, що основним завданням розроблення моделей та методів підвищення безпеки байт-код орієнтованого програмного забезпечення в умовах кібератак є удосконалення і вибір моделей, методів і засобів, що підвищують рівень конфіденційності, цілісності, непідробленості, справжності, захищеності від помилки. Хоча, я вважаю, що основним завданням доцільніше було б визначити адаптацію моделей, методів та засобів з урахуванням виявленої специфіки програмного забезпечення, методологій розробки, засобів розробки та інших факторів для забезпечення відповідного рівня безпеки програмного додатку.

8. На стор. 91 у висновках до розділу 2 автор заявляє про зменшення складності процесу верифікації при використанні графу спільних обчислень в процесі пошуку подібних елементів коду за рахунок розпаралелювання процесів обчислень. Хоча кількісних показників для порівняння одержаних результатів при застосуванні вдосконаленого методу перевірки логіко-смислової подібності програм складної логічної структури не наведено.

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

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 Вячеслава 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 наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент
доцент кафедри інформаційної безпеки
та комп'ютерної інженерії
Черкаського державного технологічного університету
доктор технічних наук, доцент В.Г. Бабенко

Підпис доктора технічних наук, доцента Бабенко В.Г. засвідчую
Учений секретар вченої ради
Черкаського державного технологічного університету І.В. Миронець