Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0823U100479

Особливі позначки: відкрита

Дата реєстрації: 11-07-2023

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Вейлінь Цао ...

2. Weilin Cao

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 123

Назва наукової спеціальності: Комп'ютерна інженерія

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 06-07-2023

Спеціальність за освітою: Комп'ютерна інженерія

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 64.050.097

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, м. Харків, Харківський р-н., Харківська обл., 61002, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, м. Харків, Харківський р-н., Харківська обл., 61002, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23, 50.41.25

Тема дисертації:

1. Метод підвищення безпеки програмного забезпечення на основі технологій тестування на проникнення

2. The software security improving method based on the penetration testing technology

Реферат:

1. Дисертація на здобуття наукового ступеня доктора філософії зі спеціальності 123 «Комп'ютерна інженерія». – Національний технічнийуніверситет «Харківський політехнічний інститут». – Харків, 2023. Предмет дослідження – метод підвищення безпеки програмного забезпечення. Об'єкт дослідження – процес забезпечення безпеки програмного забезпечення. Дисертаційна робота присвячена вирішенню актуальної науково-технічної задачі розробки методу підвищення безпеки програмного забезпечення (ПЗ) з урахуванням можливостей синтезу технологій автоматизованого тестування безпеки ПЗ та глибокого машинного навчання. Дослідження життєвого циклу програмного забезпечення та процесів тестування, що супроводжують цей цикл, виконано за допомогою теорії графів(GERT modeling). Розробка і дослідження методу автоматизованого тестування безпеки проводилися з використанням методу глибокого навчання з підкріпленням. Удосконалення методу оцінки ефективності розробленого методу здійснювалося з

використанням методу динаміки середніх величин. Оцінка достовірності теоретичних і практичних результатів проводилася з використанням положень теорії ймовірностей і математичної статистики. Наукова новизна отриманих результатів обумовлена теоретичним узагальненням і новим вирішенням важливої науково-технічної проблеми, що полягає в розробці методу підвищення безпеки програмного забезпечення на основі технологій тестування на проникнення. Отримано такі наукові результати: – вперше був розроблений метод автоматизованого тестування вторгнень з використанням пошукової системи Shodan, платформи аналізу мережевої безпеки MulVal та даних вразливостей програмного забезпечення CVE для введення та побудови реалістичних сценаріїв атаки та перевірки для глибокого навчання за допомогою технології підкріплення. Це дозволило згенерувати дерево атак для різних навчальних процедур, оптимізувати відповідні сценарії автоматичного тестування безпеки програмного забезпечення, і таким чином підвищити ефективність процесу безпеки програмного забезпечення; – удосконалена математична модель процесу тестування на проникнення в комп'ютерні системи, відмінна від відомих можливостей тестування захищеності спеціалізованих інформаційних платформ комп'ютерних систем, що дозволило оцінити ймовірність тестування часу на проникнення в заданий інтервал; – математична модель процесу тестування на проникнення в комп'ютерні системи отримала подальший розвиток. Відмінною особливістю цієї моделі є використання розподілу Ерланга в якості основного при математичній формалізації процесів переходу від стану до стану. Це дозволило, з одного боку, уніфікувати математичну модель і представити процес тестування на більш високому рівні ієрархії тестування, з іншого – спростити його. Практична значимість отриманих результатів полягає в адаптації процесу тестування програмного забезпечення до підвищених вимог безпеки і можливостей тестування засобів автоматизації, з використанням технологій глибокого навчання з підкріпленням. Практичне значення отриманих результатів полягає в наступному: – комплекс математичних моделей процесу тестування на проникнення в комп'ютерних системах з використанням мережевого підходу моделювання GERT спростив схему тестування на проникнення в 1,7 рази з урахуванням можливих змін процедур (включаючи додавання нових процедур і послуг) для оцінки імовірнісно-часових характеристик і можливостей його масштабування при збільшенні обсягу і складності розв'язуваних задач; – синтез основних компонентів методу автоматичного тестування на проникнення дозволив підвищити ефективність процесу безпеки програмного забезпечення (знизити відносні пошкодження на всіх етапах життєвого циклу програмного забезпечення до 6 разів). Результати дисертації впроваджені та використовуються в діяльності Компанії "Line Up", Науково-дослідного центру судової експертизи з питань інтелектуальної власності, а також використовується в навчальному процесі Національного технічного університету «Харківський політехнічний інститут»". У вступі обґрунтовується актуальність теми дисертації, формулюються основна мета і завдання роботи, викладається наукова новизна і практична цінність отриманих результатів. Перший розділ присвячено аналізу та порівняльним дослідженням методів тестування на проникнення програмного забезпечення. У другому розділі описаний процес тестування на проникнення складних математичних моделей.У третьому розділі розроблено метод автоматизованого тестування на проникнення з використанням технології глибокого машинного навчання. Четвертий розділ присвячено дослідженню ефективності методупідвищення безпеки програмного забезпечення та обґрунтуванню практичних рекомендацій щодо його використання. Ключові слова: програмне забезпечення, автоматизоване тестування, тестування безпеки, глибоке машинне навчання, нечітка модель GERT, кіберзагроза, вразливість програмного забезпечення, невідповідність безпеки програмного забезпечення.

2. Dissertation for obtaining a scientific degree PHD in the speciality 123 – "Computer Engineering". – National technical university "Kharkiv polytechnic institute". – Kharkiv, 2023. The subject of research – software security enhancement method. The object of research – software security process. The dissertation work is devoted to the solution of the current scientific and technical problem of developing a method of improving the security of software, taking into account the possibilities of synthesis of technologies of automated software security testing and deep machine learning. The study of the software life cycle and testing processes accompanying this cycle was performed using graph theory (GERT modeling). The development and research of the method of automated safety

testing was carried out using the method of deep learning with reinforcement. Improvement of the method of evaluating the effectiveness of the developed method was carried out using the method of dynamics of averages. The assessment of the reliability of theoretical and practical results was carried out using the provisions of probability theory and mathematical statistics. The scientific novelty of the obtained results is due to the theoretical generalization and a new solution of an important scientific and technical problem, consisting in the development of a method for improving the security of software based on penetration testing technologies. The following scientific results have been obtained. – for the first time, a method of automated intrusion testing using the Shodan search engine, the MulVal network security analysis platform, and CVE software vulnerability data has been developed to input and build realistic attack and validation scenarios for deep learning with reinforcement technology. This allowed to generate an attack tree for various training procedures, to optimize the corresponding scenarios of automatic software security testing, and thus increase the efficiency of the software security process; – improved mathematical model of the process of testing for penetration into computer systems, different from the known capabilities of testing the security of specialized information platforms of computer systems, which allowed to estimate the probability of testing time for penetration in a given interval; – the mathematical model of the process of testing for penetration into computer systems was further developed. A distinctive feature of this model is the use of the Erlang distribution as the main one in the mathematical formalization of the processes of transition from state to state. This allowed, on the one hand, to unify the mathematical model and present the testing process at a higher level of the testing hierarchy, on the other hand, to simplify it. The practical significance of the obtained results is to adapt the software testing process to the increased security requirements and capabilities of testing automation tools, using deep learning technologies with reinforcement. The practical significance of the obtained results is as follows. – a set of mathematical models of the penetration testing process in computer systems using the GERT network modeling approach simplified the penetration testing scheme by 1.7 times, taking into account possible changes in procedures (including the addition of new procedures and services) to estimate probabilistictemporal characteristics and possibilities of its scaling at increase in volume and complexity of the solved problems; – the synthesis of the main components of the method of automatic penetration testing has increased the efficiency of the software security process (reduce the relative damage at all stages of the software life cycle to 6 times). The results of the dissertation are implemented and used in the activities of the company "Line Up", the Research Center for Forensic Examination on Intellectual Property, and are also used in the educational process of the National Technical University "Kharkiv Polytechnic Institute". The relevance of the thesis topic is justified in the introduction, the main goal and task of the work are formulated, and the scientific novelty and practical value of the obtained results are presented.The first section is devoted to the analysis and comparative studies of software penetration testing methods. In the second section, the penetration testing process mathematical models complex. In the third section, automated penetration testing method using deep machine learning technology are developed. The fourth section is devoted to the study of the efficiency of the software security improving method and substantiation of practical recommendations for its use. Key words: software, automated testing, security testing, deep machine learning, fuzzy GERT model, cyber threat, software vulnerability, software security mismatch.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Черних Олена Петрівна

2. Chernykh Olena P.

Кваліфікація: к. ф.-м. н., 01.04.07

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Коваленко Андрій Анатолійович

2. Kovalenko Andriy A.

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Трубчанінова Карина Артурівна

2. Trubchaninova Karyna A

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Кучук Ніна Георгіївна

2. Kuchuk Nina H.

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Гавриленко Світлана Юріївна

2. Gavrylenko Svitlana Y.

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Заковоротний Олександр Юрійович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Заковоротний Олександр Юрійович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.