Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0821U100429

Особливі позначки: відкрита

Дата реєстрації: 18-03-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Киричок Роман Васильович
2. Kyrychok Roman Vasylovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 15-03-2021

Спеціальність за освітою: Безпека інформаційних і комунікаційних систем

Місце роботи здобувача: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, м. Київ, Київська обл., 03680, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 26.861.007

Повне найменування юридичної особи: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, м. Київ, Київська обл., 03680, 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: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, м. Київ, Київська обл., 03680, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Повне найменування юридичної особи: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, м. Київ, Київська обл., 03680, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.23.25, 50.01.77

Тема дисертації:

1. Метод автоматичного активного аналізу захищеності корпоративних мереж на основі інтелектуальної валідації вразливостей.

2. The method of automatic active security analysis of corporate networks based on intelligent vulnerability validation.

Реферат:

1. Киричок Р.В. Метод автоматичного активного аналізу захищеності корпоративних мереж на основі інтелектуальної валідації вразливостей. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека». – Державний університет телекомунікацій, МОН України, Київ, 2021. Дисертаційна робота присвячена вирішенню актуального наукового завдання, сутність якого полягає в розвитку методу автоматичного активного аналізу захищеності корпоративних мереж на основі оцінювання якості механізму валідації вразливостей функціонуючих інформаційних систем. Для досягнення мети підвищення результативності автоматичного активного аналізу захищеності корпоративних мереж завдяки інтелектуалізації процесу валідації вразливостей програмних та апаратних платформ на основі фаззі технології було вирішено наступні задачі: 1. Вперше запропоновано математичну модель аналізу кількісних характеристик процесу валідації вразливостей, що ґрунтується на поліномах Бернштейна, які дозволяють описати динаміку даного процесу. Використання даної моделі дозволяє отримувати аналітичні залежності для кількості успішно валідованих та невалідованих вразливостей, а також для кількості випадків валідації вразливостей, що призвели до критичних помилок за час раціонального циклу валідації виявлених вразливостей під час активного аналізу захищеності корпоративної мережі. 2. Вперше розроблено методику аналізу якості роботи механізму валідації виявлених вразливостей корпоративної мережі, яка базується на інтегральних рівняннях, що враховують кількісні характеристики досліджуваного механізму валідації вразливостей в певний момент часу. Дана методика дозволяє будувати закони розподілу показників якості процесу валідації вразливостей та кількісно оцінювати якість роботи механізму валідації виявлених вразливостей, що в свою чергу дозволяє в режимі реального часу відслідковувати та контролювати хід валідації виявлених вразливостей під час активного аналізу захищеності. 3. Вперше розроблено метод побудови нечіткої бази знань для прийняття рішень при валідації вразливостей програмних та апаратних платформ під час активного аналізу захищеності цільової корпоративної мережі, що базується на використанні нечіткої логіки, яка дає можливість забезпечити отримання достовірної інформації про якість механізму валідації вразливостей непрямим шляхом. Побудована база знань дозволяє формувати вирішальні правила прийняття рішень щодо реалізації тієї чи іншої атакуючої дії, що в свою чергу дозволяє розробляти експертні системи для автоматизації процесу прийняття рішень при валідації виявлених вразливостей цільових інформаційних систем та мереж. 4. Отримав подальший розвиток метод автоматичного активного аналізу захищеності корпоративних мереж, який на основі синтезу запропонованих моделі, методики та методу дозволяє, на відміну від існуючих, абстрагуватися від умов динамічної зміни середовища, тобто постійного розвитку інформаційних технологій, що призводить до зростання кількості вразливостей та відповідних векторів атак, а також зростання готових до використання експлойтів вразливостей та їх доступності, і враховувати лише параметри якості самого процесу валідації вразливостей. Розроблений та доведений до практичної реалізації метод автоматичного активного аналізу захищеності корпоративних мереж на основі інтелектуальної валідації вразливостей, завдяки оперативному контролю та корегуванню ходу валідації виявлених вразливостей дозволяє підвищити, згідно з єдиним інтегральним показником, якість валідації вразливостей до 20 разів, що в свою чергу свідчить про підвищення загальної результативності автоматичного активного аналізу захищеності корпоративних мереж. Дисертація виконувалась в Державному університеті телекомунікацій. Результати наукових досліджень були використані на кафедрі інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації під час виконання науково-дослідної роботи на тему «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах кібернетичних атак» (№ 0114V00391, ДУТ, м. Київ). Також результати наукових досліджень прийняті до впровадження в діяльність НДУ «ІНСТИТУТ КІБЕРБЕЗПЕКИ» (акт від 18.02.20); в ТОВ «ЄВРОТЕЛЕКОМ» (акт від 02.03.20). Ключові слова: корпоративна мережа, активний аналіз захищеності, цільова система, валідація вразливостей, експлойт, якість механізму.

2. Kyrychok R.V. The method of automatic active security analysis of corporate networks based on intelligent vulnerability validation. – Qualification scientific work on the rights of a manuscript. Dissertation for the degree of Doctor of Philosophy in specialty 125 “Cybersecurity”. – State University of Telecommunications, MES of Ukraine,

Kyiv, 2021. The dissertation is devoted to solving an urgent scientific problem, the essence of which is the development of the method of automatic active security analysis of corporate networks based on assessing the quality of the vulnerability validation mechanism of functioning information systems. To achieve the goal of increasing the effectiveness of automatic active security analysis of corporate networks by intellectualizing the process of vulnerability validation of software and hardware platforms based on fuzzy technology, the following tasks were solved: 1. For the first time, a mathematical model of analysing the quantitative characteristics of the vulnerability validation process is proposed, based on Bernstein polynomials, which allow describing the dynamics of this process. The use of this model makes it possible to obtain analytical dependencies for the number of successfully validated and invalidated vulnerabilities, as well as for the number of vulnerability validation cases that led to critical errors over the rational cycle of validation of identified vulnerabilities during the active analysis of the corporate network security. 2. For the first time, a methodology for analysing the quality of the validation mechanism for the identified vulnerabilities of the corporate network was developed, which is based on integral equations that take into account the quantitative characteristics of the investigated vulnerability validation mechanism at a certain point in time. This methodology makes it possible to build laws for the distribution of quality indicators of the vulnerability validation process and quantitatively assess the quality of the validation mechanism for the identified vulnerabilities, which in turn allows real-time monitoring and controlling the validation progress of the identified vulnerabilities during the active security analysis. 3. For the first time, it was developed the method of building a fuzzy knowledge base for making decisions when validating the vulnerabilities of software and hardware platforms during the active security analysis of the target corporate network, based on the use of fuzzy logic, which makes it possible to provide reliable information about the quality of the vulnerability validation mechanism in an indirect way. The built knowledge base allows the formation of final decision-making rules for the implementation of one or another attacking action, which in turn makes it possible to develop expert systems to automate the decision-making process when validating the identified vulnerabilities of target information systems and networks. 4. The method of automatic active security analysis, formed on the basis of the synthesis of the proposed model, methodology and method, has received further development. This method, in contrast to the existing ones, allows one to abstract from the conditions of dynamic changes in the environment, that is, the constant development of information technologies, which leads to an increase in the number of vulnerabilities and corresponding attack vectors, as well as to an increase in ready-to-use exploit vulnerabilities and their availability, and take into account only quality parameters of the vulnerability validation process itself. The method of automatic active security analysis of corporate networks based on intelligent vulnerability validation has been developed and brought to practical implementation, due to operational control and correction of the course of validation of identified vulnerabilities, it allows to increase, according to a single integral indicator, the quality of vulnerability validation to 20 times, which in turn indicates on improving the overall effectiveness of the automatic active security analysis of the corporate networks. The dissertation was carried out at the State University of Telecommunications. The results of scientific research were used at the Department of Information and cyber security of the Educational-scientific Institute of Information security in carrying out research work on the topic “Development of methods and means of increasing the survivability of information and communication systems in the conditions of the impact of cyber-attacks” (№ 0114V00391, SUT, Kyiv). Also, the results of scientific research were accepted for implementation in the activities of the Research Institution “CYBER SECURITY INSTITUTE” (act of 18.02.20); in EUROTELEKOM LLC (act of 02.03.20). Keywords: corporate network, active analysis of the security, target system, vulnerability validation, exploit, mechanism quality.

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. Гайдур Галина Іванівна
2. Haidur Halyna I.

Кваліфікація: д. т. н., 05.13.06

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. Казмірчук Світлана Володимирівна
2. Kazmirchuk Svitlana V.

Кваліфікація: д. т. н., 05.13.21

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. Лукова-Чуйко Наталія Вікторівна

2. Lukova-Chuiko Natalia Viktorivna

Кваліфікація: д. т. н., 05.13.06

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. Лаптєв Олександр Анатолійович

2. Laptiev Oleksandr Anatolievich

Кваліфікація: д. т. н., 05.13.21, 20.02.14

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. Гахов Сергій Олександрович

2. Gakhov Serhii O

Кваліфікація: к. військ. н., 20.02.12

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 Савченко Віталій Анатолійович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Савченко Віталій Анатолійович

Відповідальний за підготовку облікових документів

Реєстратор

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