Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U000718

Особливі позначки: відкрита

Дата реєстрації: 31-03-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Дрозд Андрій Ігорович

2. Andriy I. Drozd

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: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерна інженерія

Дата захисту:

Спеціальність за освітою: Інженерія програмного забезпечення

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): PhD 12563

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

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

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.39, 50.41.17, 20.56.01

Тема дисертації:

1. Методи та системи виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів

2. Methods and systems for detecting computer attacks in corporate networks based on population algorithms

Реферат:

1. У роботі подано результати дослідження, спрямованого на підвищення ефективності протидії зловмисним діям у корпоративних мережах шляхом удосконалення архітектури та методів функціонування обманних систем з приманками і пастками (ОСПП). Запропоновано оновлену архітектуру таких систем, у якій синтезовано популяційні алгоритми, зокрема алгоритм молі й полум'я, що забезпечує оптимізацію формування послідовностей кроків у процесі реалізації комп'ютерних атак і дій зловмисного програмного забезпечення. Завдяки цьому досягається уникнення повного перебору можливих варіантів, прискорення збіжності рішень під час динамічних змін у середовищі корпоративної мережі та врахування потенційної здатності зловмисників здійснювати двоцільові атаки. Здійснено аналіз архітектури сучасних обманних систем, методів їх організації функціонування, методів виявлення комп'ютерних атак та типів популяційних алгоритмів, які можуть бути синтезовані в архітектурі ОСПП. В роботі представлено архітектуру ОСПП, в якій синтезовано алгоритм молі і полум'я для покращення їх функціонування під час атак, моделі двоцільових

комп'ютерних атак, метод синтезу алгоритму дискретної оптимізації молі й полум'я в архітектурі ОСПП метод організації функціонування ОСПП в корпоративних мережах, метод виявлення атак відмова в обслуговуванні у мережах на основі статистичних показників а також розроблено відповідну обманну систему, здійснено постановку експериментів та проведені дослідження із розробленою системою. Об'єктом дослідження є процес організації ОСПП для виявлення КА та ЗПЗ в корпоративних мережах. Предметом дослідження є методи організації обманних систем з приманками і пастками для виявлення комп'ютерних атак та зловмисного програмного забезпечення в корпоративних мережах. Метою дисертаційного дослідження є покращення протидії комп'ютерним атакам та зловмисному програмному забезпеченню в корпоративних мережах шляхом оптимізації кроків обманних систем з приманками і пастками за рахунок синтезу популяційних алгоритмів в центрах прийняття рішень. Наукова новизна отриманих результатів полягає в наступному: удосконалено архітектуру обманних систем з приманками і пастками, в якій на відміну від відомих варіантів архітектури, здійснено синтез популяційних алгоритмів, зокрема алгоритму молі і полум'я, для оптимізації формування послідовності наступних кроків при здійсненні КА та дій ЗПЗ, уникнення повного перебору варіантів, швидкої збіжності обраних кроків при триваючих впливах та зміни послідовності кроків з врахуванням поточних змін в оточуючому середовищі корпоративних мереж, а також врахування потенційної спроможності зловмисників до здійснення двоцільових КА; розроблено новий метод синтезу алгоритму дискретної оптимізації молі й полум'я в архітектурі обманних систем з приманками і пастками, який, на відміну від відомих, характеризується формуванням дискретного простору пошуку з координатним поданням об'єктів, синтезом спірального сліду на основі секторного оцінювання потенційних кроків і кутових характеристик, урахуванням часу як параметра зміни кроків та динамічним переміщенням молі й полум'я для уникнення передчасної збіжності до локальних оптимумів, що дало змогу розробляти обманні системи, які забезпечують довготривале й адаптивне функціонування у процесі протидії зловмисникам у корпоративних мережах за рахунок зміни кроків для опрацювання подій; розроблено новий метод організації функціонування обманних систем з приманками і пастками в корпоративних мережах, в якому на відміну від відомих, в архітектурі обманних систем синтезовано популяційні алгоритми, зокрема алгоритм молі і полум'я, для здійснення ними вибору наступних кроків для уникнення реалізації зловмисниками двоцільових атак що дає змогу уникати повного перебору варіантів з можливих кроків, швидкої збіжності обраних кроків при триваючих впливах та зміну послідовності кроків з врахуванням поточних змін в оточуючому середовищі корпоративних мереж та ускладнює дії за рахунок прийняття рішень на основі популяційних алгоритмів з можливістю самостійно блокувати або активувати сервери чи комп'ютерні станції, приманки чи пастки під час встановлення потенційно зловмисних впливів в корпоративних мережах; розроблено новий метод виявлення атак відмови в обслуговуванні у мережах на основі статистичних показників, який на відміну від відомих, базується на обчисленні статистичних ознак мережного IP-трафіку при розбитті потоку пакетів на часові вікна, і встановлює динамічні зміни трафіку на рівні всього аналізованого періоду, що дозволяє підвищити достовірність виявлення атак відмова в обслуговуванні. Практичне значення отриманих результатів. Розроблено обманну систему з приманками і пастками для виявлення КА та ЗПЗ в корпоративних мережах, особливістю якої є прийняття в ній рішень щодо наступних кроків та їх коригування з використанням алгоритму дискретної оптимізації молі і полум'я, а також імплементацією в її компонентах методу виявлення комп'ютерних атак на основі аналізу їх статичних показників.

2. The paper presents the results of a study aimed at increasing the effectiveness of countering malicious actions in corporate networks by improving the architecture and methods of functioning of deceptive systems with decoys and traps (OSPP). An updated architecture of such systems is proposed, in which population algorithms are synthesized, in particular the moth and flame algorithm, which optimizes the formation of sequences of steps in the process of implementing computer attacks and malware actions. This avoids a complete enumeration of possible options, accelerates the convergence of solutions during dynamic changes in the corporate network environment, and takes into account the potential ability of attackers to carry out dual-purpose attacks. The analysis of the architecture of modern deceptive systems, methods of their organization of functioning, methods

for detecting computer attacks and types of population algorithms that can be synthesized in the OSPP architecture is carried out. The paper presents the architecture of the OSPP, in which the algorithm of moths and flames is synthesized to improve their functioning during attacks, models of two-purpose computer attacks, the method of synthesis of the algorithm of discrete optimization of moths and flames in the OSPP architecture, the method of organizing the functioning of the OSPP in corporate networks, the method of detecting denial-of-service attacks in networks based on statistical indicators, as well as the appropriate deceptive system was developed, experiments were set up and studies were carried out with the developed system. The object of the study is the process of organizing OSPP for the detection of spacecraft and runways in corporate networks. The purpose of the dissertation research is to improve counteraction to computer attacks and malware in corporate networks by optimizing the steps of deceptive systems with decoys and traps through the synthesis of population algorithms in decision-making centers. The scientific novelty of the results obtained is as follows: the architecture of deception systems with decoys and traps has been improved, in which, in contrast to the known variants of architecture, the synthesis of population algorithms, in particular the moth and flame algorithms, has been carried out to optimize the formation of the sequence of subsequent steps in the implementation of spacecraft and actions of the malware, to avoid a complete enumeration of options, rapid convergence of selected steps with ongoing impacts and changes in the sequence steps taking into account current changes in the environment of corporate networks, as well as taking into account the potential capability of intruders to carry out dual-purpose spacecraft; A new method for the synthesis of the algorithm for discrete optimization of moths and flames in the architecture of deceptive systems with decoys and traps has been developed, which, in contrast to the known ones, is characterized by the formation of a discrete search space with a coordinate representation of objects, the synthesis of a spiral trace based on sectoral estimation of potential steps and angular characteristics, taking into account time as a parameter of step change, and the dynamic movement of moths and flames to avoid premature convergence to local optimums, which made it possible to develop deceptive systems that ensure long-term and adaptive functioning in the process of countering intruders in corporate networks by changing steps for processing events; A new method of organizing the functioning of deceptive systems with decoys and traps in corporate networks has been developed, in which, in contrast to the well-known ones, population algorithms, in particular the moth and flame algorithm, are synthesized in the architecture of deceptive systems, in order for them to choose the next steps to avoid the implementation of two-purpose attacks by attackers, which makes it possible toavoid a complete enumeration of options from possible steps, rapid convergence of selected steps with ongoing impacts and change in the sequence of steps taking into account current changes in the environment of corporate networks and complicates actions due to decision-making based on population algorithms with the ability to independently block or activate servers or computer stations, decoys or traps when establishing potentially malicious influences in corporate networks. Practical significance of the results obtained. A deceptive system with decoys and traps for detecting spacecraft and runways in corporate networks has been developed, the peculiarity of which is decision-making on the next steps and their adjustment using the algorithm of discrete optimization of moths and flames, as well as the implementation of the method of detecting computer attacks in its components based on the analysis of their static indicators.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Савенко О.С., Дрозд А.І., Медзатий Д.М. Концептуальна архітектура обманних систем з приманками і пастками на основі популяційних алгоритмів. Вимірювальна та обчислювальна техніка в технологічних

процесах. Measuring and computing devices in technological processes. 2025. №84(4). С. 127-151.
- Дрозд А. Метод виявлення комп'ютерних атак типу відмови в обслуговуванні на основі статистичних показників мережного трафіку. Information Technology: Computer Science, Software Engineering and Cyber Security. 2025. № 4, С. 79–89.
- Савенко О.С., Дрозд А.І., Коробчинський М.В. Метод синтезу популяційних алгоритмів в архітектурі обманних систем з приманками і пастками. Вимірювальна та обчислювальна техніка в технологічних процесах. Measuring and computing devices in technological processes. 2025. №82(2). С. 459–474.
- RAMSKYI I., DROZD A., LYHUN O., PONOCHOVNA O. SYSTEM FOR CYBERSECURITY EVALUATION OF CORPORATE NETWORKS. Computer Systems and Information Technologies. 2025. № 2. С. 123–131.
- Дрозд А.І. Метод організації функціонування обманних систем з приманками і пастками в корпоративних мережах. Вісник Хмельницького національного університету. Технічні науки. 2025. № 359 (6.2). С. 445–457.
- Savenko O., Rusyn B., Lysenko S., Ciszewski T., Savenko B., Drozd A., Nicheporuk A., Sachenko A. Synthesis of a Moth and Flame Algorithm for Incorporation into the Architecture of Deceptive Systems with Baits and Traps. Applied Sciences. 2026. 16(5). 2415.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0124U000980 0126U002082

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Коробчинський Максим Володимирович
2. Maksum V. Korobchunskii

Кваліфікація: д.т.н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Воєнно-дипломатична академія імені Євгенія Березняка

Код за ЄДРПОУ: 14303342

Місцезнаходження: вул. Юрія Іллєнка, Київ, 04050, Україна

Форма власності: Державна

Сфера управління: Міністерство оборони України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Савенко Олег Станіславович
2. Oleg S. Savenko

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Якименко Ігор Зіновійович
2. Igor Z. Yakymenko

Кваліфікація: к. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Західноукраїнський національний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: вул. Львівська, Тернопіль, Тернопільський р-н., 46009, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Мулеса Оксана Юріївна
2. Oksana Y. Mulesa

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Державний вищий навчальний заклад "Ужгородський національний університет"

Код за ЄДРПОУ: 02070832

Місцезнаходження: вул. Підгірна, Ужгород, Ужгородський р-н., 88000, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Кльоц Юрій Павлович

2. Yurii P. Klots

Кваліфікація: к.т.н., доц., 05.13.13

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація: 2007р, ДК №041583

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Кисіль Тетяна Миколаївна

2. Tetiana M. Kysil

Кваліфікація: к. ф.-м. н., доц., 01.01.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Говорущенко Тетяна Олександрівна

Власне Прізвище Ім'я По-батькові головуючого на засіданні Говорущенко Тетяна Олександрівна

Відповідальний за підготовку облікових документів Синюк Олег Миколайович

Реєстратор Юрченко Тетяна Анатоліївна

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна