Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U000699

Особливі позначки: відкрита

Дата реєстрації: 28-02-2025

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Запорожченко Михайло Михайлович
2. Mykhailo Zaporozhchenko

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0003-0182-9497

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: 36680 Кібербезпека (125 Кібербезпека)

Дата захисту: 02-04-2025

Спеціальність за освітою: Кібербезпека

Місце роботи здобувача: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 7856

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, 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: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56, 20.56.03

Тема дисертації:

1. Методи прогнозування соціоінженерних атак на корпоративні інформаційні системи на основі профілю захищеності користувача

2. Methods of predicting social engineering attacks on corporate information systems based on the user’s security profile

Реферат:

1. Запорожченко М.М. Методи прогнозування соціоінженерних атак на корпоративні інформаційні системи на основі профілю захищеності користувача. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека. – Державний університет інформаційно-комунікаційних технологій, МОН України, Київ, 2025. Соціоінженерні атаки залишаються однією з критичних загроз для організацій через експлуатацію людського фактору як ключової вразливості. Аналіз сучасних підходів до виявлення та прогнозування соціоінженерних атак виявив їхню фрагментарність, адже більшість моделей зосереджені лише на окремих аспектах захисту (технічному, організаційному) або показниках користувачів (демографічних, психологічних, поведінкових), без урахування

взаємозв'язків та впливу зовнішніх умов. Така обмеженість може призводити до ненадійних прогнозів і недостатньої ефективності протидії атакам. Крім того, сучасні методи часто потребують значних ресурсів і великих обсягів даних, що ускладнює їхнє впровадження в організаціях із обмеженими можливостями. З огляду на це виникає нагальна потреба у вирішенні актуального наукового завдання, сутність якого полягає в розробці інтегративного методу прогнозування соціоінженерних атак на корпоративні інформаційні системи, який ґрунтується на комплексній моделі профілю захищеності користувача. Метою дослідження є підвищення рівня захищеності корпоративних інформаційних систем від соціоінженерних атак на основі прогнозування вразливості шляхом створення профілю захищеності користувача. В процесі досягнення зазначеної мети та вирішення наукового завдання у роботі одержано основні наукові результати: вперше розроблено комплексну модель профілю захищеності користувача як основу для інтегративного методу прогнозування соціоінженерних атак на корпоративні інформаційні системи, яка базується на мультиплікативній згортці результатів дослідження психологічного, організаційного, технічного факторів та фактору інформаційного впливу відносно конкретного користувача і дає можливість визначення потенційної вразливості користувачів організації до соціоінженерних атак; удосконалено метод оцінки компонентів профілю захищеності користувача, який відрізняється від базового підходу, заснованого на методі аналізу ієрархій, використанням динамічно змінюваного набору показників, що забезпечує комплексну та адаптивну оцінку впливу факторів профілю захищеності на рівень вразливості користувача з урахуванням зміни його індивідуальних характеристик та специфіки організаційного середовища; удосконалено метод виявлення найбільш ймовірних траєкторій соціоінженерних атак, який відрізняється від відомих підходів застосуванням графової моделі взаємодії користувачів корпоративної інформаційної системи з урахуванням типів і інтенсивності їх комунікаційних зв'язків, що забезпечує можливість ідентифікації найбільш уразливих користувачів і визначення критичних траєкторій багатоетапних соціоінженерних атак для оцінювання ризиків компрометації корпоративної інформаційної системи. Практичне значення одержаних результатів полягає в тому, що розроблений метод прогнозування соціоінженерних атак на корпоративні інформаційні системи надає можливість оцінювати ймовірність компрометації користувачів, виявляти найуразливіші категорії та впроваджувати цільові заходи захисту, що підвищує рівень захищеності корпоративних інформаційних систем. На базі методу запропоновано критерії для оцінки психологічного, організаційного, технічного факторів та фактору інформаційного впливу, які можуть бути використані фахівцями з кібербезпеки для розробки адаптивних стратегій протидії соціоінженерним загрозам. За результатами впровадження рекомендованих заходів покращено значення захисту від одноетапних соціоінженерних атак у межах від 10.3% до 42.8% для різних категорій користувачів, а загальне зниження ймовірності компрометації внаслідок багатоетапних атак становить у середньому 21% (від 19% до 24.3%). Ключові слова: соціоінженерна атака, інформаційна система, прогнозування атак, оцінка вразливості користувача, графова модель, інформаційний вплив, математична модель, зловмисник, багатоетапна атака, траєкторія атаки, кібербезпека, кіберпростір, прийняття рішень, соціальні мережі.

2. Zaporozhchenko M.M. Methods of predicting social engineering attacks on corporate information systems based on the user's security profile. – Qualifying scientific work on manuscript rights. Dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 125 "Cybersecurity". – State University of Information and Communication Technologies, MES of Ukraine, Kyiv, 2024. Social engineering attacks remain one of the critical threats to organizations due to the exploitation of the human factor as a key vulnerability. An analysis of current approaches to detecting and predicting social engineering attacks has revealed their fragmentation, as most models focus only on certain aspects of protection (technical, organizational) or user indicators (demographic, psychological, behavioral), without taking into account the interconnections and influence of external conditions. This limitation can lead to unreliable forecasts and insufficient effectiveness in countering attacks. In addition, modern methods often require significant resources and large amounts of data, which makes it difficult to implement them in organizations with limited capabilities. Thus, there is an urgent need to solve an ongoing scientific task, the purpose of which is to develop an integrative method for predicting social engineering attacks on corporate information systems based on a comprehensive model of the user's security profile. The purpose of

the study is to increase the level of security of corporate information systems against social engineering attacks based on vulnerability prediction by creating a user security profile. In the process of achieving this purpose and solving the scientific task, the main scientific results were obtained: for the first time, a comprehensive user security profile model has been developed as a basis for an integrative method for predicting social engineering attacks on corporate information systems, based on the multiplicative convolution of the results of the study of psychological, organizational, technical factors and the factor of information influence in the context of a particular user, which makes it possible to determine the potential vulnerability of users of the organization to social engineering attacks; the method for assessing the components of the user's security profile has been improved, which differs from the basic approach based on the hierarchy analysis method by using a dynamically changing set of indicators, which provides a comprehensive and adaptive assessment of the impact of security profile factors on the level of user vulnerability, taking into account changes in their individual characteristics and the specifics of the organizational environment; the method for identifying the most likely trajectories of social engineering attacks has been improved, which differs from the known approaches by using a graph model of interaction between users of a corporate information system, taking into account the types and intensity of their communication links, which makes it possible to identify the most vulnerable users and determine the critical trajectories of multi-stage social engineering attacks to assess the risks of compromising a corporate information system. The practical significance of the results obtained is that the developed method for predicting social engineering attacks on corporate information systems makes it possible to assess the probability of user compromise, identify the most vulnerable categories and implement targeted countermeasures, which increases the level of corporate information systems security. Based on the method, criteria for assessing the psychological, organizational, technical, and information influence factors are proposed, which can be used by cybersecurity specialists to develop adaptive strategies to counter social engineering threats. As a result of the implementation of the recommended countermeasures, the level of protection against one-stage social engineering attacks has improved in the range from 10.3% to 42.8% for different categories of users, and the overall reduction in the likelihood of compromise due to multi-stage attacks is an average of 21% (from 19% to 24.3%). Keywords: social engineering attack, information system, attack prediction, user vulnerability assessment, graph model, information influence, mathematical model, threat actor, multi-stage attack, attack trajectory, cybersecurity, cyberspace, decision making, social networks.

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:

- Якименко Ю.М., Рабчун Д.І., Запорожченко М.М. Місце соціальної інженерії в проблемі витоку даних та організаційні аспекти захисту корпоративного середовища від фішингових атак з використанням електронної пошти. Кібербезпека: освіта, наука, техніка. 2021. № 1 (13). С. 6-15. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/278/238
- Запорожченко М.М., Дзюба Т.М. Життєвий цикл та різновиди соціоінженерних атак. Зв'язок. 2021. № 4 (152). С. 17-20. URL: http://con.dut.edu.ua/index.php/communication/article/view/2544/2448
- Muzhanova T., Yakymenko Y., Zaporozhchenko M., Tyshchenko V. International vendor-neutral certification for information security professionals. Кібербезпека: освіта, наука, техніка. 2022. № 4 (16). С. 129-141. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/369/306
- Запорожченко М.М. Місце OSINT в життєвому циклі кібератаки. Телекомунікаційні та інформаційні технології. 2023. № 1. С. 53-60. URL:

https://tit.dut.edu.ua/index.php/telecommunication/article/view/2455

- Якименко Ю.М., Рабчун Д.І., Мужанова Т.М., Запорожченко М.М., Щавінський Ю.В. Технічний аудит захищеності інформаційно-телекомунікаційних систем підприємства. Кібербезпека: освіта, наука, техніка. 2023. № 4 (20). С. 45-61. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/466
- Shchavinsky Y. V., Muzhanova T. M., Yakymenko Y. M., Zaporozhchenko M. M. Application of artificial intelligence for improving situational training of cybersecurity specialists. Information Technologies and Learning Tools. 2023. Vol. 97, № 5. P. 215-226. (Web of Science). URL: https://journal.iitta.gov.ua/index.php/itlt/article/view/5424
- Lehominova S. V., Shchavinsky Y. V., Muzhanova T. M., Rabchun D. I., Zaporozhchenko M. M. Application of sentiment analysis to prevent cyberattacks on objects of critical information infrastructure. International Journal of Computing. 2023. Vol. 22, № 4. P. 534-540. (Scopus). URL: https://computingonline.net/computing/article/view/3362
- Легомінова С.В., Щавінський Ю.В., Рабчун Д.І., Запорожченко М.М., Будзинський О.В. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації. Кібербезпека: освіта, наука, техніка. 2024. № 1 (25). С. 294-303. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/630
- Запорожченко М.М. Моделювання профілю захищеності користувача для визначення його потенційної вразливості до соціоінженерних атак. Телекомунікаційні та інформаційні технології. 2024. № 4. С. 129-135. URL: https://tit.dut.edu.ua/index.php/telecommunication/article/view/2570
- Запорожченко М.М. Метод оцінки ймовірності реалізації траєкторій соціоінженерної атаки в корпоративних інформаційних системах. Наукові записки Державного університету інформаційно-комунікаційних технологій. 2024. № 2. С. 236-242. URL: https://journals.dut.edu.ua/index.php/sciencenotes/article/view/3109
- Lehominova S. V., Zaporozhchenko M. M., Shchavinsky Y. V., Muzhanova T. M., Tyshchenko V. S., Yushchenko M. O. Methodology for determining means of monitoring information security by the method of expert assessment. International Journal of Computing. 2024. Vol. 23, № 4. P. 681-691. (Scopus). URL: https://computingonline.net/files/journals/1/archieve/IJC_2024_23_4_17.pdf

Наукова (науково-технічна) продукція: методи, теорії, гіпотези

Соціально-економічна спрямованість: підвищення рівня інформаційної безпеки корпоративних інформаційних систем

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0123U100743, 0120U105132, 0118U100058

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Легомінова Світлана Володимирівна

2. Svitlana V. Lehominova

Кваліфікація: д. е. н., професор, 08.00.04

Ідентифікатор ORCID ID: 0000-0002-4433-5123

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, 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. Молодецька Катерина Валеріївна
2. Kateryna V. Molodetska

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0001-9864-2463

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Києво-Могилянська академія"

Код за ЄДРПОУ: 16459396

Місцезнаходження: вул. Г. Сковороди, буд. 2, Київ, 04070, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Складанний Павло Миколайович
2. Pavlo M. Skladannyi

Кваліфікація: к. т. н., доцент, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-7775-6039

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Туровський Олександр Леонідович
2. OLEKSANDR TUROVSKYI

Кваліфікація: д. т. н., професор, 05.12.13

Ідентифікатор ORCID ID: 0000-0002-4961-0876

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Гайдур Галина Іванівна
2. HALYNA HAIDUR

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

Ідентифікатор ORCID ID: 0000-0003-0591-3290

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

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

Запорожченко Михайло Михайлович

Реєстратор

УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна