

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0226U000662

Державний реєстраційний номер: 0124U000980

Особливі позначки: відкрита

Дата реєстрації: 14-01-2026

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток

Початок етапу: 01.2024

Закінчення етапу: 12.2025

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, м. Хмельницький, Хмельницький р-н., Хмельницька обл., 29016, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380975546925, 380382728076

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Міністерство освіти і науки України

Код за ЄДРПОУ: 38621185

Місцезнаходження: проспект Берестейський, буд. 10, м. Київ, 01135, Україна

Форма власності:

Сфера управління: Кабінет Міністрів України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380444813221

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 34 - договір (замовлення) з центральним органом виконавчої влади, академією наук (головними розпорядниками бюджетних коштів на проведення НДДКР)

Напрямок фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 2201040

Фактичний обсяг фінансування (тис. грн.): 1600.000

VII. Відомості про ДіР

Назва роботи українською:

Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток

Назва роботи англійською:

System for detecting malware and computer attacks in corporate networks using false attack objects and traps

Реферат українською:

Об'єкт дослідження – процес забезпечення безпеки, відмовостійкості, живучості та захисту інформації комп'ютерних систем корпоративних мереж шляхом розроблення системи виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток. Мета роботи – вирішення актуальної науково-прикладної проблеми підвищення рівня безпеки, відмовостійкості, живучості та захисту інформації комп'ютерних систем корпоративних мереж шляхом розроблення системи виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток. Для досягнення мети проекту необхідно розв'язати наступні завдання. Методи дослідження – теорії множин і теорії графів, методи класифікації, теорії комп'ютерних мереж, компоненти штучного інтелекту, теорії випадкових процесів та моделювання. В проекті виконано побудову нової частково централізованої розподіленої системи виявлення worm-вірусів, проведено з нею експериментальні дослідження щодо встановлення ефективності функціонування, стійкості, деградації, достовірності виявлення worm-вірусів та впроваджено її у виробництво. Формалізовано предметну галузь, розроблено математичний апарат, методи та розроблено частково централізовану розподілену систему, що дозволяють підвищити рівень безпеки, відмовостійкості, живучості та захисту інформації комп'ютерних систем корпоративних мереж. Розроблювана система може бути використана як для комерційних організацій, так і для державних установ, військових формувань та правоохоронних органів завдяки тому, що вона спрямована на забезпечення національної безпеки України в частині покращення стану її кібербезпеки в умовах кібервійни з агресором, а також на етапі повоєнної відбудови міст, критична інфраструктура яких використовувати концепцію розумного та безпечного міста.

Реферат англійською:

The object of research is the process of ensuring the security, fault tolerance, survivability and information protection of computer systems of corporate networks by developing a system for detecting malicious programs and computer attacks in corporate networks using false attack objects and traps. The purpose of the work is to solve the current scientific and applied problem of increasing the level of security, fault tolerance, survivability and information protection of computer systems of corporate networks by developing a system for detecting malicious programs and computer attacks in corporate networks using false attack objects and traps. To achieve the goal of the project, the following tasks must be solved. Research methods are set theory and graph theory, classification methods, computer network theory, artificial intelligence components, stochastic process theory and modeling. The project built a new partially centralized distributed worm detection system, conducted experimental studies with it to establish the effectiveness of functioning, stability, degradation, reliability of worm detection, and implemented it in production. The subject area was formalized, mathematical apparatus and methods were developed, and a partially centralized distributed system was developed that allow increasing the level of security, fault tolerance, survivability, and information protection of computer systems in corporate networks. The developed system can be used both for commercial organizations and for state institutions, military formations and law enforcement agencies due to the fact that it is aimed at ensuring the national security of Ukraine in terms of improving its cybersecurity in the context of a cyber war with an aggressor, as well as at the stage of post-war reconstruction of cities whose critical infrastructure uses the concept of a smart and safe city.

Індекс УДК:004.7, 681.5; 681.51; 681.52, 004.9: 004.05: 004.89: 004.056.57: 004.492

Коди тематичних рубрик: 50.37.23, 50.41.27

Керівники роботи

Власне Прізвище Ім'я По-батькові: Савенко Олег Станіславович

Науковий ступінь: д. т. н.

Вчене звання: професор

Ідентифікатор ORCID ID:

Додаткова інформація:

VIII. Наукова (науково-технічна) продукція (НТП)

Назва НТП українською: Система виявлення зловмисного програмного забезпечення та прогнозування рівня якості програмного забезпечення

Назва НТП англійською: Malware detection system and software quality level prediction

НТП, яку передбачалося створити: Створено

Причини, через які НТП не було створено:

Отримані результати: Програмні продукти, програмно-технологічна документація

Галузь застосування: 72.19

Реєстраційний номер картки технології:

Опис НТП: Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток, як системи для заплутування зловмисників при проведенні ними атак та використанні ЗПЗ, а також розроблення нових методів та засобів забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення, які підвищують ефективність виявлення в корпоративних мережах. Система забезпечує підвищену ефективність виявлення ЗПЗ та комп'ютерних атак у корпоративних мережах за рахунок використання хибних об'єктів атак та пасток, дворівневої моделі протидії, параметричного контролю модулів ПЗ та онтологічної верифікації. Рівень рішення перевищує вітчизняні та більшість зарубіжних аналогів за комплексністю захисту та живучістю систем. Впровадження системи знижує витрати на запобігання кібератакам та витрати на відновлення після атак, підвищує ефективність мережевої інфраструктури. Вартість реалізації виправдана економією на витратах персоналу та збереженні даних, що робить продукт привабливим для корпоративного ринку. Система не потребує додаткових енергоресурсів чи токсичних матеріалів, зменшує ризики відновлення інфраструктури після атак, що позитивно впливає на екологічне навантаження та електроспоживання ІТ-інфраструктури. Проект створює принципово нову ІТ-продукцію для підвищення кібербезпеки корпоративних мереж, сприяє заміщенню імпорту, підвищенню продуктивності праці та ефективності роботи персоналу. Забезпечує нові інформаційно-комунікаційні послуги та підвищує надійність роботи критичних корпоративних систем.

Соціально-економічна спрямованість НТП: Створення принципово нової продукції (матеріалів, технологій тощо) для забезпечення експортного потенціалу та заміщенню імпорту, Підвищення автоматизації виробничих процесів, Інше (Створення принципово нової ІТ-продукції для підвищення кібербезпеки корпоративних мереж, сприяє заміщенню імпорту, підвищенню продуктивності праці та ефективності роботи персоналу. Забезпечує нові інформаційно-комунікаційні послуги та підвищує надійність роботи критичних корпоративних систем.)

Вплив НТП на довкілля: не має

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 02.2024

Закінчення етапу: 10.2024

Споживачі продукції: комерційні організації, державні установи, правоохоронні органи

Перспективні ринки: корпоративний та державний сектор

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

Охоронні документи на ОПІВ

комп'ютерні програми: 1. Свідоцтво про реєстрацію авторського права на твір №134190 Україна. Комп'ютерна програма «Програмне забезпечення організації розподіленої системи виконання програмного коду в ізольованих середовищах» / Реґіда П. Г., Савенко О. С., Нічепорук А. О., Дрозд А. І. 2025. URL: <https://sis.nipo.gov.ua/uk/search/detail/1853743/> 2. Свідоцтво про реєстрацію авторського права на твір №136704. Комп'ютерна програма «Програмне забезпечення автоматизованого порівняння об'єктів операційних середовищ комп'ютерних систем (АПООСКС)» / Ю. В. Стецюк, Б. О. Савенко. Дата реєстрації 09.06.2025. URL: <https://sis.nipo.gov.ua/uk/search/detail/1868611/>

IX. Бібліографічний опис

- 1 Izonin I. Quality and Security of Critical Infrastructure Systems / I. Izonin, T. Hovorushchenko, Sh. K. Shandilya // Big Data and Cognitive Computing. – 2024. – Vol. 8, No. 1. – Paper 10. – Режим доступу: <https://doi.org/10.3390/bdcc8010010>
- 2 Hovorushchenko T. Advancements in AI-Based Information Technologies: Solutions for Quality and Security / T. Hovorushchenko, I. Izonin, H. Kutucu // Systems. – 2024. – Vol. 12, No. 2. – Paper 58. – Режим доступу: <https://doi.org/10.3390/systems12020058>.
- 3 Method for Determining the Security Level of Software / T. Hovorushchenko, Yu. Voichur, D. Medzaty, A. Boyarchuk, A. Hnatchuk // CEUR Workshop Proceedings. – 2024. – Vol. 3675. – P. 72–85. – Режим доступу: <https://ceur-ws.org/Vol-3675/paper6.pdf>.
- 4 Multi-computer malware detection systems with metamorphic functionality / A. Kashtalian, S. Lysenko, O. Savenko, A. Nicheporuk, T. Sochor, V. Avsiyevych // Radioelectronic and Computer Systems. – 2024. – No. 1. – P. 152–175. – Режим доступу: <https://doi.org/10.32620/reks.2024.1.13>.
- 5 A trust model that ensures the correctness of computing in grid computing system / P. Rehida, O. Savenko, A. Sachenko, A. Drozd, P. Vizhevski // CEUR Workshop Proceedings. – 2024. – Vol. 3675. – P. 388–401. – Режим доступу: <https://ceur-ws.org/Vol-3675/>.
- 6 A graph-based vulnerability detection method / Y. Sierhieiev, V. Paiuk, A. Sachenko, A. Nicheporuk, A. Kwiecien // CEUR Workshop Proceedings. – 2024. – Vol. 3675. – P. 388–401. – Режим доступу: <https://ceur-ws.org/Vol-3675/>.
- 7 Detection and prediction of the vulnerabilities in software systems based on behavioral analysis with machine learning / Y. Sierhieiev, V. Paiuk, A. Nicheporuk, A. Kwiecien, O. Huralnyk // CEUR Workshop Proceedings. – 2024. – Vol. 3736. – P. 239–254. – Режим доступу: <https://ceur-ws.org/Vol-3736/>.
- 8 Obfuscation technologies of high-level source code using artificial intelligence / I. Golovko, O. Savenko, P. Vizhevski, O. Klein, A.-B. M. Salem // CEUR Workshop Proceedings. – 2024. – Vol. 3736. – P. 324–338. – Режим доступу: <https://ceur-ws.org/Vol-3736/>.

- 9 Method of random dynamic control transfer between network nodes for a partially centralized OS security system / Y. Stetsyuk, M. Stetsyuk, B. Savenko, A. Kwiecien, L. Kopania // CEUR Workshop Proceedings. – 2025. – Vol. 3963. – P. 264–283. – Режим доступу: <https://ceur-ws.org/Vol-3963/paper22.pdf>.
- 10 Method and rules for determining the next centralization option in multicomputer system architecture / A. Kashtalian, S. Lysenko, T. Kysil, A. Sachenko, O. Savenko, B. Savenko // International Journal of Computing. – 2025. – Vol. 24, No. 1. – P. 35–51. – Режим доступу: <https://doi.org/10.47839/ijc.24.1.3875>.
- 11 Evaluation criteria of centralization options in the architecture of multicomputer systems with traps and baits / A. Kashtalian, S. Lysenko, A. Sachenko, B. Savenko, O. Savenko, A. Nicheporuk // Radioelectronic and Computer Systems. – 2025. – No. 1. – P. 264–297. – Режим доступу: <https://doi.org/10.32620/reks.2025.1.18>.
- 12 Anomaly-based detection of DDoS attacks in encrypted network traffic using autoencoder neural networks / Danchuk S., Nicheporuk A., Yashyna O., Sochor T. // CEUR Workshop Proceedings. – 2025. – Vol. 4013. – P. 165–173. – Режим доступу: <https://ceur-ws.org/Vol-4013/paper13.pdf>.
- 13 Detecting software implants using system decoys / Denysiuk D., Savenko O., Lysenko S., Savenko B., Nicheporuk A. // CEUR Workshop Proceedings. – 2024. – Vol. 3899. – P. 277–287. – Режим доступу: <https://ceur-ws.org/Vol-3899/paper25.pdf>.
- 14 Savenko O. Detection of buffer overflow vulnerabilities in system software based on a graph and transformer model / O. Savenko, P. Gaj, Y. Sierhieiev // Proceedings of the International Workshop on Applied Intelligent Security Systems in Law Enforcement (AISSLE-2025). – Vinnytsia, Ukraine, 30–31 Oct. 2025. – P. 292–305. – Режим доступу: <https://ceur-ws.org/Vol-4126/paper17.pdf>.
- 15 Modern strategies for data leak detection and prevention in corporate networks / Sachenko A., Vizhevskiy P., Savenko O., Ostroverkhov V., Maslyyak B. // Proceedings of the MoDaST-2025 Doctoral Consortium. – Lviv, Ukraine, 15 June 2025. – P. 275–292. – Режим доступу: <https://ceur-ws.org/Vol-4005/paper19.pdf>.
- 16 A model for probabilistic monitoring and proactive restart of real-time operating systems under intensive state changes in cyber-physical systems / Kozelskyi O., Drozd A., Savenko B., Gaj P. // CEUR Workshop Proceedings. – 2025. – Vol. 4013. – P. 198–210. – Режим доступу: <https://ceur-ws.org/Vol-4013/paper16.pdf>.
- 17 Optimization of centralization of network OS security resources based on dynamic transfer of control between network nodes / Sachenko A., Sochor T., Savenko B., Stetsyuk Yu., Stetsyuk V. // Proceedings of the International Workshop on Applied Intelligent Security Systems in Law Enforcement (AISSLE-2025). – Vinnytsia, Ukraine, 30–31 Oct. 2025. – P. 48–61. – Режим доступу: <https://ceur-ws.org/Vol-4126/paper5.pdf>.
- 18 Hovorushchenko T. Universalization of the method of predicting quality level of software based on the requirements / T. Hovorushchenko, Yu. Voichur, D. Medzatyi // Proceedings of the 14th IEEE International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024). – Athens, Greece, 11–13 Oct. 2024.
- 19 Improvement of effectiveness for static application security testing for detection of SQL injection vulnerabilities / Sierhieiev Y., Paiuk V., Savenko O., Drozd A. // Proceedings of the 14th IEEE International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024). – Athens, Greece, 2024. – P. 1–6. – Режим доступу: <https://doi.org/10.1109/DESSERT65323.2024.11122171>.
- 20 Prokofiev I., Savenko O. Method of statistical analysis of software code based on complex parameters // Proceedings of the 14th IEEE International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024). – Athens, Greece, 2024. – P. 1–7. – Режим доступу: <https://doi.org/10.1109/DESSERT65323.2024.11122184>.
- 21 Obfuscation process with machine learning module / Golovko I., Savenko O., Vizhevskiy P., Sachenko A. // Proceedings of the 14th IEEE International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024). – Athens, Greece, 2024. – P. 1–7. – Режим доступу: <https://doi.org/10.1109/DESSERT65323.2024.11122185>

- 22 Detection system of software implants using decoys / Denysiuk D., Savenko B., Kashtalian A., Savenko O., Lysenko S. // Proceedings of the 14th IEEE International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024). – Athens, Greece, 2024. – P. 1–6. – Режим доступу: <https://doi.org/10.1109/DESSERT65323.2024.11122205>.
- 23 A model of an intelligent agent for classifying malicious software using fuzzy logic / Chaikovskiy M., Chaikovska I., Savenko O., Sachenko A. // Proceedings of the 14th IEEE International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024). – Athens, Greece, 2024. – P. 1–7. – Режим доступу: <https://doi.org/10.1109/DESSERT65323.2024.11122159>
- 24 Method for distributed detection malicious activity based on analysis of execution behavior / Rehida P., Savenko O., Kashtalian A., Sachenko A. // Proceedings of the 14th IEEE International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024). – Athens, Greece, 2024. – P. 1–8. – Режим доступу: <https://doi.org/10.1109/DESSERT65323.2024.11122133>.
- 25 The impact of data processing on random forest model performance for network attacks / Prodeus M., Nicheporuk A., Martiniyuk D., Luhyn O., Grodskiy S. // Proceedings of the 14th IEEE International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024). – Athens, Greece, 11–13 Oct. 2024. – Режим доступу: <https://doi.org/10.1109/DESSERT65323.2024.11122135>.
- 26 Danchuk S. Graphs-based method for detecting cyber threats in real-time systems / S. Danchuk, A. Nicheporuk, I. Martyniuk // Proceedings of the 14th IEEE International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024). – Athens, Greece, 11–13 Oct. 2024. – Режим доступу: <https://doi.org/10.1109/DESSERT65323.2024.11122027>.
- 27 Lysenko S., Savenko O., Bokhonko O., Gaj P. Social engineering attacks models // Proceedings of the 14th IEEE International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024). – Athens, Greece, 2024. – P. 1–9. – Режим доступу: <https://doi.org/10.1109/DESSERT65323.2024.11122124>.
- 28 Савенко Б. О. Метод виявлення worm-вірусів згідно багатокласової класифікації // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2024. – № 1 (331). – С. 18–28. – Режим доступу: <https://doi.org/10.31891/2307-5732-2024-331-2>.
- 29 Савенко О. С. Метод нечіткої класифікації зловмисного програмного забезпечення з використанням інтелектуального агента / О. С. Савенко, М. О. Чайковський // Information Technology: Computer Science, Software Engineering and Cyber Security. – 2024. – № 3. – С. 140–148. – Режим доступу: <https://doi.org/10.32782/IT/2024-3-15>.
- 30 Чайковський М. О. Комплексний підхід до виявлення та аналізу поліморфного зловмисного програмного забезпечення // Measuring and Computing Devices in Technological Processes. – 2024. – № 2. – С. 42–50. – Режим доступу: <https://doi.org/10.31891/2219-9365-2024-78-5>.
- 31 Чайковський М. О. Модель мультиагентної системи для виявлення поліморфних вірусів // Herald of Khmelnytskyi National University. Technical Sciences. – 2024. – № 347(1). – С. 543–547. – Режим доступу: <https://doi.org/10.31891/2307-5732-2025-347-74>.
- 32 Рєгіда П. Г. Метод виявлення зловмисної активності в інфікованих програмах / П. Г. Рєгіда, О. С. Савенко // Information Technology: Computer Science, Software Engineering and Cyber Security. – 2024. – № 1. – С. 178–186. – Режим доступу: <https://doi.org/10.32782/IT/2024-4-21>.
- 33 Концепція застосування розподілених систем для аналізу поліморфних вірусів / Рєгіда П. Г., Бармак О. В., Каштальян А. С., Манзюк Е. А. // Вісник Хмельницького національного університету. Технічні науки. – 2024. – Т. 331. – № 1. – С. 38–43. – Режим доступу: <https://doi.org/10.31891/2307-5732-2024-331-4>.
- 34 Забезпечення безпеки в системах автоматизації будівель / Мельник В., Лигун О., Возний К., Гуральник О., Мартинюк Д. // Measuring and Computing Devices in Technological Processes. – 2024. – № 2. – С. 266–276. –

Режим доступу: <https://doi.org/10.31891/2219-9365-2024-78-31>.

35 Метод виявлення метаморфних вірусів розподіленими системами на основі порівняння еквівалентних функціональних блоків / Нічепорук А. О., Бармак О. В., Манзюк Е. А., Продеус М. С. // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. – 2024. – Т. 35 (74). – № 1. – С. 260–265. – Режим доступу: <https://doi.org/10.32782/2663-5941/2024.1.1/39>.

36 Nicheporuk A. Model of process for ensuring fault tolerance in internet of things networks / A. Nicheporuk, O. Dariychuk, S. Danchuk // Computer Systems and Information Technologies. – 2024. – No. 2. – P. 14–20. – Available at: <https://doi.org/10.31891/csit-2024-2-2>.

37 Метод виявлення кібератак на канали зв'язку інформаційних систем / Нічепорук А. О., Данчук С. В., Іванченко О. В., Посонський С. В., Андреев В. О. // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2024. – № 345, № 6(2). – С. 165–171. – Режим доступу: <https://doi.org/10.31891/2307-5732-2024-345-6-25>.

38 Вплив попередньої обробки даних на продуктивність моделі Random Forest у виявленні мережових атак / Продеус М. С., Нічепорук А. О., Іванченко О. В., Литвінчук І. В. // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2024. – № 4. – С. 415–419. – Режим доступу: <https://doi.org/10.31891/2219-9365-2024-80-51>.

39 Ефективність і вдосконалення SAST у контексті SQL Injection вразливостей / Сергеев Є. О., Каштальян А. С., Ковальчук В. В., Савенко О. С., Іванченко О. В. // Information Technology: Computer Science, Software Engineering and Cyber Security. – 2024. – № 3. – С. 149–158. – Режим доступу: <https://doi.org/10.32782/IT/2024-3-16>.

40 Продеус М.С. Система моніторингу, виявлення, реагування та захисту інформації на основі Honeypot-файлів / М.С. Продеус, А.О. Нічепорук, А.С. Каштальян // Central Ukrainian Scientific Bulletin. Technical Sciences. – 2025. – Issue 11(42), Part I. – С. 56–67. – URL: [https://mapiea.kntu.kr.ua/pdf/11\(42\)_I/8.pdf](https://mapiea.kntu.kr.ua/pdf/11(42)_I/8.pdf)

41 Стецюк Ю. Модель централізованої системи безпеки операційних систем з механізмом маркування конфіденційної інформації / Ю. Стецюк, О. Савенко // Information Technology: Computer Science, Software Engineering and Cyber Security. – 2025. – № 2. – С. 143–155. – DOI: <https://doi.org/10.32782/IT/2025-2-15>

42 Стецюк Ю. Модель централізованої системи безпеки операційних систем стійких до витоків конфіденційної інформації / Ю. Стецюк, О. Савенко // Вісник Хмельницького національного університету. Серія «Технічні науки». – 2025. – № 353(3.2). – С. 409–419. – DOI: <https://doi.org/10.31891/2307-5732-2025-353-57>

43 Забезпечення якості, безпеки та захисту комп'ютерних систем корпоративних мереж : монографія / О.С. Савенко, Т.О. Говорущенко, С.М. Лисенко та ін. // – Хмельницький: ХНУ, 2025. – 327 с.

44 Проміжне програмне забезпечення частково централізованих розподілених систем виявлення зловмисного програмного забезпечення в комп'ютерних мережах: авторське право на твір №124480 : комп'ютерна програма / Б. Савенко, В. Севостьянов, О. Матюкін. – дата реєстрації 07.03.2024 ; опубл. 31.05.2024, Бюл. № 81. – URL: <https://sis.nipo.gov.ua/uk/search/detail/1802406/>

45 Проміжне програмне забезпечення мультикомп'ютерних систем спеціалізованого призначення (AMJS) : авторське право на твір №124518 : комп'ютерна програма / А.С. Каштальян, В. Р. Авсієвич, А. О. Нічепорук, О. С. Савенко. – дата реєстрації 11.03.2024 ; опубл. 31.05.2024, Бюл. № 81. – URL: <https://sis.nipo.gov.ua/uk/search/detail/1802407/>

46 Програмне забезпечення організації розподіленої системи виконання програмного коду в ізольованих середовищах : авторське право на твір №134190 : комп'ютерна програма / П. Г. Рєгіда, О. С. Савенко, А. О. Нічепорук, А. І. Дрозд. – дата реєстрації 10.03.2025 ; опубл. 30.04.2025, Бюл. № 88. – URL: <https://sis.nipo.gov.ua/uk/search/detail/1853743/>

47 Програмне забезпечення автоматизованого порівняння об'єктів операційних середовищ комп'ютерних систем (АПООСКС) : авторське праве на твір №136704 : комп'ютерна програма / Ю. В. Стецюк, Б. О. Савенко. – дата реєстрації 09.06.2025 ; опубл. 31.07.2025, Бюл. № 91. – URL: <https://sis.nipo.gov.ua/uk/search/detail/1868611/>

Х. Заключні відомості

Керівник юридичної особи

Синюк Олег Миколайович
д. т. н., 05.05.10

Перелік осіб-виконавців

Говорущенко Тетяна Олександрівна
(д. т. н., професор, 05.13.06)

Лисенко Сергій Миколайович
(д.т.н., професор, 05.13.06)

Нічепорук Андрій Олександрович
(к. т. н., доц., 05.13.06)

Павлова Ольга Олександрівна
(д.філософ, доц., 122)

Регіда Павло Геннадійович
(д.філософ)

Відповідальний за підготовку облікових документів

Шмурікова Олена Павлівна

Телефон

+380687706043

Реєстратор

Юрченко Тетяна Анатоліївна

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Тетяна Анатоліївна