Облікова картка НДДКР

Державний обліковий номер: 0223U000986

Державний реєстраційний номер: 0119U100090

Відкрита

Дата реєстрації: 23-01-2023

1. Етапи виконання

Номер етапу: 1

Назва етапу: Методологічні основи забезпечення кібербезпеки України

Початок етапу: 12-2018

Закінчення етапу: 12-2022

Вид звітного документа: Остаточний звіт

2. Виконавець

Назва організації: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код ЄДРПОУ/ІПН: 34979237

Підпорядкованість: Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Адреса: вул. Верхньоключова, буд. 4, корпус 27, м. Київ, 03056, Україна

Телефон: 380442049151

E-mail: iszzi@iszzi.kpi.ua

WWW: http://iszzi.kpi.ua

3. Власник результатів НДДКР (продукції)

Назва організації: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код ЄДРПОУ/ІПН: 34979237

Адреса: вул. Верхньоключова, буд. 4, корпус 27, м. Київ, 03056, Україна

Підпорядкованість: Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Телефон: 380442049151

E-mail: iszzi@iszzi.kpi.ua

WWW: http://iszzi.kpi.ua

4. Джерела та напрями фінансування

Підстава для проведення робіт: 43 - власна ініціатива (якщо робота виконується з власної ініціативи за кошти виконавця НДР або безкоштовно)

КПКВК:

Напрям фінансування: 2.7 - інше (Безоплатно)

Джерела фінансування

Джерело фінансування: 7706 - безплатно (договір про науково-технічне співробітництво, тощо)

Фактичний обсяг фінансування за звітний етап: 0.000 тис. грн.

5. Науково-технічна робота

Назва роботи (укр)

Методологічні основи забезпечення кібербезпеки України

Назва роботи (англ)

Methodological basis of Ukraine cybersecurity

Реферат (укр)

Створено методологічні основи забезпечення кібербезпеки України. Для цього удосконалено моделі виявлення аномалій та кібернетичних атак. Запропоновано та виокремлено регресійні моделі, методи виявлення аномалій. Створено методику виявлення аномальної мережевої активності користувачів. Запропоновано моделі, методи перетворення, приховування інформації, виявлення змін у шифрованому мережевому трафіку. Розроблено моделі, методи виявлення джерел інформаційного впливу на суспільство та аналізу великих обсягів даних з питань кібербезпеки із соціальних медіа. На їх основі створено комплекс інструментальних засобів контент-моніторингу. Для оцінювання цілісності об'єктів кіберзахисту запропоновано метод Q-аналізу. Побудовано концептуальну модель кіберпростору та кібербезпеки. Запропоновано модель, метод формалізування діяльності управління ризиком кібербезпеки. Створено функційну модель реверс-інжинірингу шкідливого програмного забезпечення. На основі теорії марківських процесів запропоновано методи описання сценаріїв кібератак. Розроблено правило-орієнтований метод виявлення кіберінцидентів SIEM-системою. Створено її архітектуру та функційну модель, а також методику їх раціонального вибору. Запропоновано підходи до підвищення обізнаності користувачів стосовно реагування на кіберінциденти. Побудовано модель інформаційних процесів циклу поведінки корпоративної системи кіберзахисту. На основі біометричних характеристик користувача запропоновано моделі, методи, методики захисту комп'ютерних даних від несанкціонованого доступу. Створено модель, метод аналізування функцій систем управління інформаційною безпекою. Розроблено підсистему моніторингу комплексної системи захисту інформації. Отримані результати орієнтовані на використання у освітньому процесі закладами вищої освіти.

Реферат (англ)

Methodological foundations for ensuring the cybersecurity of Ukraine have been developed. For this purpose, models for detecting anomalies and cybernetic attacks have been improved. Regression models and anomaly detection methods are proposed and highlighted. A technique for detecting anomalous network activity of users has been developed. Models, methods of conversion, information hiding, and detection of changes in encrypted network traffic are proposed. Development has been made on models and methods of identifying sources of informational influence on society and analyzing large volumes of data on cyber security issues from social media. Based on them, a set of content monitoring tools was created. The Q-analysis method is proposed for assessing the integrity of cyber protection objects. A conceptual model of cyberspace and cybersecurity has been built. A model, a method of formalizing cybersecurity risk management activities is proposed. A functional model of reverse engineering of harmful software has been created. Based on the theory of Markov processes, methods for describing cyberattack scenarios are proposed. The SIEM system has developed a rule-oriented method of detecting cyber incidents. Its architecture and functional model, as well as the methodology of their rational selection, have been created. New ways to increase user awareness of responding to cyber incidents are proposed. A model of the information processes of the behavior cycle of the corporate cybersecurity system has been built. Based on the user's biometric characteristics, models, methods, and techniques for protecting computer data from unauthorized access are proposed. A model, a method of analyzing the functions of information security management systems has been created. A monitoring subsystem of the complex information protection system has been developed. The obtained results are intended for use in the educational process by institutions of higher education.

Індекс УДК: 004.7, 004[056.5+413.4]

Коди тематичних рубрик НТІ: 50.37.23

6. Науково-технічна продукція (НТП)

НТП 1

Назва продукції (укр): Методологічні основи забезпечення кібербезпеки України

Назва продукції (англ): Methodological basis of Ukraine cybersecurity

Очікувані результати: Методологічні основи

Галузь застосування: Інформаційні технології - Кібербезпека

Опис продукції (укр): Створено методологічні основи забезпечення кібербезпеки України на основі розроблення моделей, методів, методик виявлення (запобігання) вторгнень у комп'ютерні системи та мережі; стеганографічного захисту інформації; аналізування соціальних мереж; оцінювання ризиків кібербезпеки; виявлення, аналізування та реагування на кіберінциденти; захисту комп'ютерних систем і мереж.

Соціально-економічна спрямованість НТП: Створення принципово нової продукції (матеріалів, технологій тощо) для забезпечення експортного потенціалу та заміщенню імпорту

Стадія завершеності НТП: Звіт по НДДКР

Впровадження НТП: Не впроваджено

Строки впровадження:

Виробник продукції: ІСЗЗІ КПІ ім. Ігоря Сікорського

Споживачі продукції:

Перспективні ринки:

Права інтелектуальної власності: За договорами

Форми та умови передачі продукції: Навчання персоналу, Спільні НДДКР

7. Бібліографічний опис

Додонов О. Г., Ланде Д. В., Нестеренко О. В., Березін Б. О., Підхід до прогнозування дієвості державного управління з використанням технологій OSINT, Інформаційні технології та безпека : матеріали міжнародної науково-практичної конференції (Київ, 28 листопада 2019 р.). Київ, 2019, С. 230–233.

Dodonov A., Lande D., Tsyganok V., Andriichuk O., Kadenko S., Graivoronskaya A. Information Operations Recognition. From Nonlinear Analysis to Decision-Making. Saarbrücken : Lambert Academic Publishing, 2019. 292 p.

Horniichuk I., Yevetskyi V., Kubrak V. Applying mobile devices in biometric user authentication systems. Information technology and security. 2019. Vol. 7, Iss. 1. P. 14–24. DOI: https://doi.org/10.20535/2411-1031.2019.7.1.184213.

Горнійчук І. В., Євецький В. Л. Комп'ютерна програма для автентифікації користувачів засобами системи автентифікації користувачів за їх рукописним підписом "MarMurAuth Authentication Module". Свідоцтво про реєстрацію авторського права на твір № 84552; заявл. 09.11.2018; зареєстр. 18.01.2019.

Горнійчук І. В., Євецький В. Л. Комп'ютерна програма реєстрації користувачів для автентифікації засобами системи автентифікації користувачів за їх рукописним підписом "MarMurAuth Registration Module". Свідоцтво про реєстрацію авторського права на твір № 84553; заявл. 09.11.2018; зареєстр. 18.01.2019.

Горнійчук І. В., Євецький В. Л. Комп'ютерна програма реєстрації та автентифікації засобами системи автентифікації користувачів за їх рукописним підписом "MarMurAuth Android Module". Свідоцтво про реєстрацію авторського права на твір № 84551; заявл. 09.11.2018; зареєстр. 18.01.2019.

Горнійчук І. В., Євецький В. Л., Безух.Б. Ю. Комп'ютерна програма реєстрації користувачів для автентифікації засобами

системи автентифікації користувачів за їх точковим почерком – PointWriteAuth. Свідоцтво про реєстрацію авторського права на твір № 95966; заявл. 30.01.2020; зареєстр. 11.02.2020.

Горнійчук І. В., Євецький В. Л., Наконечна Г. В. Мобільний застосунок користувачів для автентифікації засобами системи автентифікації користувачів за їх рукописним підписом – Signature Statistic. Свідоцтво про реєстрацію авторського права на твір № 102321; заявл. 26.01.2021; зареєстр. 04.02.2021.

Горнійчук І. В., Євецький В. Л., Наконечна Г. В. Комп'ютерна програма для аналізу біометричних характеристик рукописного підпису користувачів "Signature Statistics Analyzer". Свідоцтво про реєстрацію авторського права на твір № 112042; заявл. 09.02.2022; зареєстр. 22.02.2022.

Yevetskyi V., Horniichuk I. Analysis of stability of the user's keyboard handwriting characteristics in the biometric authentication systems. Information technology and security. 2018. Vol. 6, Iss. 2. P. 19–28. DOI: https://doi.org/ 10.20535/2411-1031.2018.6.2.153487.

Yevetskyi V., Horniichuk I. Selection of handwritten signature dynamic indicators for user authentication. Information Technology and Security. 2020. Vol. 8, Iss. 1. P. 19–30. DOI: https://doi.org/10.20535/2411-1031.2020.8.1.217994.

Yevetskyi V., Horniichuk I., Nakonechna H. Influence of destabilizing factors on the stability of user's handwritten signature indicators. Information Technology and Security. 2020. Vol. 8, Iss. 2. P. 144–152. DOI: https://doi.org/ 10.20535/2411-1031.2020.8.2.222592.

Кисельов П. А., Ланде Д. В. Розробка програмних засобів аналізу та прогнозування інформаційних операцій. Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем : матеріали науково-практичної конференції курсантів (студентів), аспірантів, докторантів та молодих вчених (Київ, 21–22 травня 2019 р.). Київ, 2019. С. 180.

Ланде Д. В., Кальян Н. А., Матіїшин О. Т., Система агрегації соціальних медіа з питань кібербезпеки. Теоретичні і прикладні проблеми фізики, математики та інформатики : матеріали XVII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (Київ, 26–27 квітня 2019 р.). Київ, 2019. С. 10–11.

Lande D., Shnurko-Tabakova E. OSINT as a part of cyber defense system. Theoretical and Applied Cybersecurity. 2019. No. 1. P. 103–108. DOI: http://dx.doi.org/ 10.20535/tacs.2664-29132019.1.169091.

Ланде Д. В., Субач І. Ю., Бояринова Ю. Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. 298 с.

Ланде Д. В., Субач І. Ю., Соболєв А. М. Комп'ютерна програма контент-моніторингу соціальних мереж з питань кібербезпеки "Кіберагрегатор" ("Кіберагрегатор"). Свідоцтво про реєстрацію авторського права на твір. № 91831; зареєстр. 31.07.2019.

Ланде Д. В., Субач І. Ю., Соболєв А. М. Комп'ютерна програма контент-моніторингу соціальних мереж з питань кібербезпеки "Кіберагрегатор" ("Кіберагрегатор"). Свідоцтво про реєстрацію авторського права на твір. № 91831; зареєстр. 31.07.2019.

Mokhor V., Tsurkan V., Pokrovska V. Analysis of cyber exercises approaches. Information Technologies and Security. Aachen, Germany, 2021. Vol. 2859. P. 61–70. URL: http://ceur-ws.org/Vol-2859/paper6.pdf. DOI: https://doi.org/10.5281/zenodo.6946082.

Мохор В., Цуркан В. Функції системи управління інформаційною безпекою. ITSEC : матеріали X міжнародної науково-технічної конференції (Київ, Шарм-ель-Шейх, 19–24 березня 2020 р.). Київ, 2020. С. 53.

Мохор В., Цуркан В., Дорогий Я., Бакалинський О. Метод концептуалізування системних досліджень систем управління інформаційною безпекою. Information Technology and Security. January – June 2020. Vol. 8, Iss. 1 (14). P. 92–101. DOI: https://doi.org/10.20535/2411-1031.2020.8.1.218012.

Рябцев В., Шарадкін Д., Клят Ю. Порівняльне дослідження алгоритмів виявлення точок змін в регресійних моделях часових рядів. Information Technology and Security. July-December 2021. Vol. 9, Iss. 2 (17). P. 137–150. DOI: https://doi.org/10.20535/2411-1031.2021.9.2.249887.

Соболєв А. М. Виявлення в глобальній мережі Інтернет інформаційних джерел, які розповсюджують недостовірну

інформацію. Реєстрація, зберігання і обробка даних. 2019. Том 21, № 3. С. 56–68.

Соболєв А. М., Ланде Д. В. Метод виявлення критичних інформаційних ресурсів в глобальній мережі Інтернет. Information Technology and Security. January–June 2019. Vol. 7. Iss. 1 (12). P. 4–13.

Соколов В. В., Шаповал О. М., Шарадкін Д. М. Ансабль алгоритмів виявлення аномалій в часових рядах та його використання до задач моніторингу стану систем в реальному часі, Збірник наукових праць ВІТІ. 2020, № 3, С. 82–93.

Subach I., Kubrak V., Mykytiuk A. Methodology of rational choice of security incident management system for building operational security center. Information Technology and Security. Aachen, Germany, 2019. Vol. 2577. P. 11–20. URL: http://ceur-ws.org/Vol-2577/paper2.pdf.

Субач І., Кубрак В., Микитюк А. Архітектура та функціональна модель перспективної проактивної інтелектуальної системи SIEM-системи для кберзахисту об'єктів критичної інфраструктури. Information Technology and Security. 2019. Vol. 7, Iss. 2. С. 208□215. DOI: https://doi.org/10.20535/2411-1031.2019.7.2.190570.

Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information Technology and Security. 2019. Vol. 7, Iss. 1. P.69–78. DOI: https://doi.org/10.20535/2411-1031.2019.7.1. 184326.

Цуркан В. В. Метод функціонального аналізування систем управління інформаційною безпекою. Кібербезпека : освіта, наука, техніка. 2020. Том 4, № 8. С. 192–201. DOI: https://doi.org/10.28925/2663-4023.2020.8.192201.

8. Звітна документація

Кількість сторінок в звіті: 360

Мова звіту: Українська

Кількість файлів у звіті: 1

9. Заключні відомості

Перелік осіб-виконавців

Євецький Віктор Леонідович (к. т. н., доц.)

Гвоздінська Валерія Олександрівна

Гиренко Ігор Миколайович (к. т. н.)

Горнійчук Іван Вікторович

Кубрак Володимир Олександрович

Куліков Василь Михайлович (к. т. н., доц.)

Ланде Дмитро Володимирович (д. т. н., професор)

Микитюк Артем Вячеславович

Пучков Олександр Олександрович (к. філос. н., професор)

Соболєв Артем Миколайович (к. т. н.)

Субач Ігор Юрійович (д. т. н., професор)

Успенський Олександр Анатолійович (к. т. н., доц.)

Цуркан Василь Васильович (к. т. н., доц.)

Шаповал Олександр Миколайович

Шарадкін Дмитро Михайлович (к. т. н., доц.)

Яковів Ігор Богданович (к. т. н., доц.)

Керівник організації:

Пучков Олександр Олександрович (к. філос. н., професор)

Керівники роботи:

Субач Ігор Юрійович (д. т. н., професор)

Керівник відділу реєстрації наукової діяльності УкрІНТЕІ

Юрченко Т.А.