Облікова картка НДДКР

Державний обліковий номер: 0223U000961

Державний реєстраційний номер: 0122U200863

Відкрита

Дата реєстрації: 22-01-2023

1. Етапи виконання

Номер етапу: 1

Назва етапу: Розробка алгоритмів розвідки кіберзагроз на базі платформи з відкритим кодом

Початок етапу: 09-2022

Закінчення етапу: 12-2022

Вид звітного документа: Остаточний звіт

2. Виконавець

Назва організації: Західноукраїнський національний університет

Код ЄДРПОУ/ІПН: 33680120

Підпорядкованість: Міністерство освіти і науки України

Адреса: вул. Львівська, буд. 11, м. Тернопіль, Тернопільський р-н., Тернопільська обл., 46009, Україна

Телефон: 380352475051

E-mail: rektor@wunu.edu.ua

WWW: https://www.wunu.edu.ua/

3. Власник результатів НДДКР (продукції)

Назва організації: Західноукраїнський національний університет

Код ЄДРПОУ/ІПН: 33680120

Адреса: вул. Львівська, буд. 11, м. Тернопіль, Тернопільський р-н., Тернопільська обл., 46009, Україна

Підпорядкованість: Міністерство освіти і науки України

Телефон: 380352475051

E-mail: rektor@wunu.edu.ua

WWW: https://www.wunu.edu.ua/

4. Джерела та напрями фінансування

Підстава для проведення робіт: 52 - договір з вітчизняною організацією (органами місцевої ради, фондом, асоціацією, концерном тощо)

КПКВК:

Напрям фінансування: 2.7 - інше (господарський договір)

Джерела фінансування

Джерело фінансування: 7722 - кошти підприємств, установ, організацій України

Фактичний обсяг фінансування за звітний етап: 30.000 тис. грн.

5. Науково-технічна робота

Назва роботи (укр)

Розробка алгоритмів розвідки кіберзагроз на базі платформи з відкритим кодом

Назва роботи (англ)

Development of cyber threat intelligence algorithms based on an open source platform

Реферат (укр)

Об'єкт дослідження – процеси збору, аналізу та обміну даними про кіберзагрози. Мета роботи – підвищення ефективності алгоритмів обміну інформацією про кіберзагрози. Методи дослідження – методи розвідки кіберзагроз, методи поширення інформації про загрози, методи проектування. Узагальнений науковий результат роботи полягає в тому, що на основі бази знань про тактику та прийоми противника MITRE ATT&CK розробленого алгоритми обміну про загрози з використанням. Платформи з відкритим кодом MISP. Наукова новизна проведеного дослідження полягає у виділенні ключових компонентів оперативного аналізу загроз та Розроблений алгоритм обміну інформацією про загрози буде використано при впровадженні системи обміну інформацією на базі платформи з відкритим кодом. Прогнозні припущення щодо розвитку об'єкта дослідження – розроблення алгоритмів обміну даними про кіберзагрози з використанням технології блокчейн.

Реферат (англ)

The object of the research is the processes of collection, analysis and exchange of data on cyber threats. The purpose of the work is to improve the efficiency of algorithms for exchanging information about cyber threats. Research methods – cyber threat intelligence methods, threat information dissemination methods, design methods. The generalized scientific result of the work is that on the basis of the knowledge base about the tactics and techniques of the MITER ATT&CK enemy, algorithms for the exchange of threats with use have been developed. MISP Open Source Platforms. The scientific novelty of the conducted research consists in the selection of key components of operational analysis of threats and The developed algorithm for exchanging information about threats will be used in the implementation of an information exchange system based on an open source platform. Predictive assumptions regarding the development of the research object - the development of algorithms for exchanging data on cyber threats using blockchain technology.

Індекс УДК: 004.4; 004.4:004.7

Коди тематичних рубрик НТІ: 50.39.31

6. Науково-технічна продукція (НТП)

НТП 1

Назва продукції (укр): Алгоритми розвідки кіберзагроз на базі платформи з відкритим кодом

Назва продукції (англ): Cyber threat intelligence algorithms based on an open source platform

Очікувані результати: Методичні документи

Галузь застосування: M 72 Наукові дослідження та розробки

Опис продукції (укр): Узагальнений науковий результат роботи полягає в тому, що на основі бази знань про тактику та прийоми противника MITRE ATT&CK розробленого алгоритми обміну про загрози з використанням. Платформи з відкритим кодом MISP. Наукова новизна проведеного дослідження полягає у виділенні ключових компонентів оперативного аналізу загроз та Розроблений алгоритм обміну інформацією про загрози буде використано при впровадженні системи обміну інформацією на базі платформи з відкритим кодом. Прогнозні припущення щодо розвитку

об'єкта дослідження – розроблення алгоритмів обміну даними про кіберзагрози з використанням технології блокчейн.

Соціально-економічна спрямованість НТП: Поліпшення кібербезпеки

Стадія завершеності НТП: Звіт по НДДКР

Впровадження НТП: Впроваджено

Строки впровадження: 09.202212.2022

Виробник продукції: ЗУНУ

Споживачі продукції: Підприємства, установи та організації

Перспективні ринки: Україна

Права інтелектуальної власності: За договорами

Форми та умови передачі продукції: Спільні НДДКР

7. Бібліографічний опис

Яцків В.В. та ін. Розробка алгоритмів розвідки кіберзагроз на базі платформи з відкритим кодом : Звіт про НДР. Тернопіль, ЗУНУ, 2022. 68 с.

8. Звітна документація

Кількість сторінок в звіті: 68

Мова звіту: Українська

Кількість файлів у звіті: 1

9. Заключні відомості

Перелік осіб-виконавців

Ігнатєв Ігор Васильович

Кулина Сергій Васильович

Яцків Василь Васильович (д. т. н., проф.)

Керівник організації:

Крисоватий Андрій Ігорович (д. е. н., професор)

Керівники роботи:

Яцків Василь Васильович (д. т. н., проф.)

Керівник відділу реєстрації наукової діяльності УкрІНТЕІ

Юрченко Т.А.