Облікова картка ДіР

I. Загальні відомості

Державний обліковий номер: 0223U000961

Державний реєстраційний номер: 0122U200863

Особливі позначки: відкрита

Дата реєстрації: 22-01-2023

II. Етап виконання ДіР

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

III. Відомості про виконавця ДіР

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

Код за ЄДРПОУ: 33680120

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

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380352475051

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Комунальне підприємство "Тернопільський інформаційно-аналітичний центр" Тернопільської обласної ради

Код за ЄДРПОУ: 44218492

Місцезнаходження: вул. Михайла Грушевського, буд. 8, м. Тернопіль, Тернопільський р-н., Тернопільська обл., 46021, Україна

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380673640909

VI. Джерела, напрями та обсяги фінансування ДіР

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

Напрям фінансування: 2.7 - інше

Джерела фінансування

7722 - кошти підприємств, установ, організацій України

Фактичний обсяг фінансування (тис. грн.): 30.000

VII. Відомості про ДіР

Назва роботи українською:

Розробка алгоритмів розвідки кіберзагроз на базі платформи з відкритим кодом

Назва роботи англійською:

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

Реферат українською:

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 англійською:

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: 50.39.31

Керівники роботи

Власне Прізвище Ім'я По-батькові: Яцків Василь Васильович

Науковий ступінь: д. т. н.

Вчене звання: проф.

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Алгоритми розвідки кіберзагроз на базі платформи з відкритим кодом

Назва НТП англійською: Cyber threat intelligence algorithms based on an open source platform

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методичні документи

Галузь застосування: M 72 Наукові дослідження та розробки

Реєстраційний номер картки технології:

Опис НТП: 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

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 09.2022

Закінчення етапу: 12.2022

Споживачі продукції: Підприємства, установи та організації

Перспективні ринки: Україна

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обгрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. 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.

X. Заключні відомості

Керівник юридичної особи Крисоватий Андрій Ігорович
д. е. н., 08.00.08

Перелік осіб-виконавців

Ігнатєв Ігор Васильович

Кулина Сергій Васильович

Яцків Василь Васильович
(д. т. н., 05.13.05)

Відповідальний за підготовку облікових документів Москаль Ю.В.

Телефон +38 (035) 251-75-52

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

