

# Облікова картка ДіР



## I. Загальні відомості

**Державний обліковий номер:** 0226U000365

**Державний реєстраційний номер:** 0121U107693

**Особливі позначки:** відкрита

**Дата реєстрації:** 08-01-2026

## II. Етап виконання ДіР

**Номер етапу:** 4

**Назва етапу:** Розробка технології розпізнавання загроз ТРІКС ЄІП. Розробка технології аналізу загроз ТРІКС ЄІП.

**Початок етапу:** 01.2024

**Закінчення етапу:** 12.2024

**Вид звітнього документа:** Проміжний звіт

## III. Відомості про виконавця ДіР

**Повне найменування юридичної особи (або ПІБ фізичної особи):** Інститут проблем реєстрації інформації Національної академії наук України

**Код за ЄДРПОУ:** 03771755

**Місцезнаходження:** вул. М. Шпака, буд. 2, м. Київ, Київська обл., 03113, Україна

**Форма власності:**

**Сфера управління:** Національна академія наук України

**Ідентифікатор ROR:** Не застосовується

**Розмір організації:**

**Телефон:** 380444563318

## IV. Відомості про співвиконавців ДіР

## V. Відомості про замовника ДіР

**Повне найменування юридичної особи (або ПІБ фізичної особи):** Національна академія наук України

**Код за ЄДРПОУ:** 00019270

**Місцезнаходження:** вул. Володимирська, буд. 54, м. Київ, Київська обл., 01030, Україна

**Форма власності:**

**Сфера управління:** Кабінет міністрів

**Ідентифікатор ROR:** Не застосовується

**Розмір організації:**

**Телефон:** 380442350981, 380442262341, (044) 239-66-72

## 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:** 2.1 - фундаментальні дослідження

### Джерела фінансування

7713 - кошти держбюджету

**Код програмної класифікації видатків і кредитування (КПКВК):** 6541030

|                                                           |
|-----------------------------------------------------------|
| <b>Фактичний обсяг фінансування (тис. грн.):</b> 1467.201 |
|-----------------------------------------------------------|

## **VII. Відомості про ДіР**

### **Назва роботи українською:**

Розробка технології забезпечення живучості територіально-розподілених інформаційних комп'ютерних систем у єдиному інформаційному просторі (шифр: ТРІКС-2021)

### **Назва роботи англійською:**

Development of technology to ensure the survivability of territorially distributed information computer systems in a single information space (code: TDICS-2021)

### **Реферат українською:**

Розглянуто технологію розпізнавання загроз ТРІКС ЄІП як сукупність методів, інструментів і процесів, спрямованих на виявлення потенційних загроз, що включає такі основні процеси: збір даних про стан ТРІКС ЄІП та її елементів; виявлення та розпізнавання загроз; автоматичне або ручне прийняття заходів після виявлення загрози, таких як блокування, сповіщення або усунення уразливостей. Розглянуто методи сигнатурного, аномального і гібридного розпізнавання загроз, методи на основі: машинного навчання, інформації про загрози, аналізу уразливостей; аналізу контенту. Виконано порівняльний аналіз розглянутих методів, наведено інструменти для їх реалізації. Розроблено покрокові блок-схеми застосування кожного із методів, наведено приклади їх практичного використання. Розроблено та описано алгоритм розпізнавання загроз ТРІКС ЄІП. Наведено моделі розпізнавання загроз. Розглянуто технологію аналізу загроз ТРІКС ЄІП, як сукупність методів, інструментів і процесів, що включає такі основні етапи: отримання даних про загрози від технології розпізнавання загроз; оцінка та прогнозування ризиків: використання моделей аналізу ризиків для визначення ймовірності реалізації загроз і оцінки їхнього впливу на систему; моделювання реалізації загрози (небажаного впливу): створення сценаріїв атак для оцінки можливих шляхів реалізації загроз; формалізація аналітичного висновку про загрозу для ТРІКС ЄІП. Розглянуто методи аналізу загроз ТРІКС ЄІП: моделювання загроз, аналізу ризику для оцінки та визначення ймовірності реалізації загроз і їх потенційних наслідків, аналізу поведінки, аналізу на основі розвідки загроз, статистичного аналізу. Наведено інструменти для їх реалізації. Розроблено та описано алгоритм аналізу загроз ТРІКС ЄІП. Наведено моделі, які використовуються для аналізу загроз ТРІКС ЄІП. Наведено загальні принципи застосування технології забезпечення живучості для виявлення, розпізнавання та аналізу загроз ТРІКС ЄІП.

### **Реферат англійською:**

The TDICS SIS threat recognition technology is considered as a set of methods, tools and processes aimed at identifying potential threats, which includes the following main processes: collecting data on the status of TDICS SIS and its elements; detecting and recognizing threats; automatically or manually taking measures after detecting a threat, such as blocking, notifying or eliminating vulnerabilities. Methods of signature, anomalous and hybrid threat recognition are considered, methods based on: machine learning, threat information, vulnerability analysis; content analysis. A comparative analysis of the considered methods is performed, tools for their implementation are provided. Step-by-step flowcharts of the application of each of the methods are developed, examples of their practical use are provided. The TDICS SIS threat recognition algorithm is developed and described. Threat recognition models are presented. The TDICS SIS threat analysis technology is considered as a set of methods, tools and processes, which includes the following main stages: obtaining threat data from threat recognition technology; risk assessment and forecasting: using risk analysis models to determine the probability of threat implementation and assessing their impact on the system; modeling the threat implementation (undesirable impact): creating attack scenarios to assess possible ways of threat implementation; formalizing an analytical conclusion about the threat for TDICS SIS. The TDICS SIS threat analysis methods are considered. Tools for their implementation are presented. The TDICS SIS threat analysis algorithm is developed and described. Models used for TDICS SIS threat analysis are presented. General principles for applying survivability technology to detect,

recognize and analyze TDICS SIS threats are presented.

**Індекс УДК:** 025.4.03; 002.53:004.65, 004.5

**Коди тематичних рубрик:** 20.23.21

**Керівники роботи**

**Власне Прізвище Ім'я По-батькові:** Додонов Олександр Георгійович

**Науковий ступінь:** д.т.н.

**Вчене звання:** професор

**Ідентифікатор ORCID ID:**

**Додаткова інформація:**

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

**Назва НТП українською:** Опис технологій розпізнавання та аналізу загроз територіально-розподілених інформаційних комп'ютерних систем у єдиному інформаційному просторі.

**Назва НТП англійською:** Description of technologies for recognizing and analyzing threats to geographically distributed information computer systems in a single information space.

**НТП, яку передбачалося створити:** Створено

**Причини, через які НТП не було створено:**

**Отримані результати:** Методи, теорії, гіпотези

**Галузь застосування:** Інформаційна структура критичних інфраструктур

**Реєстраційний номер картки технології:**

**Опис НТП:** Розроблені технології дозволяють виявляти та блокувати загрози ТРІКС ЄІП на ранніх стадіях, виявляти уразливості та слабкі місця в захисті, перш ніж вони будуть використані зловмисниками; дають змогу активно захищатися від атак, покращувати безпеку, приймати обґрунтовані рішення та мінімізувати потенційні збитки.

**Соціально-економічна спрямованість НТП:** Інше (Створення технології, що забезпечить здатність комп'ютерних систем адаптуватися до нових умов функціонування та протистояти негативним впливам, спрямованим на погіршення їх спроможності виконувати цільову функцію в умовах деградації ресурсів)

**Вплив НТП на довкілля:** Не впливає

**Впровадження НТП:** Не впроваджено

**Практична реалізація НТП**

**Початок етапу:**

**Закінчення етапу:**

**Споживачі продукції:**

**Перспективні ринки:**

**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:**

## IX. Бібліографічний опис

1. Додонов О.Г., Кузьмичов А. І. Кількісне оцінювання функціональної стійкості мережевих структур за параметричною чутливістю оптимізаційної моделі // Реєстрація, зберігання і обробка даних, 2024, Т. 26, № 1.

2. Додонов О.Г., Никифоров О.В., Путятін В.Г., Додонов В.О., Куценко С.А., Германюк А.П. Територіально-розподілені інформаційні комп'ютерні системи у єдиному інформаційному просторі: базові поняття та визначення // Реєстрація, зберігання і обробка даних. 2024. Т.26. № 1. – С. 89-112.
3. Додонов О.Г., Путятін В.Г., Додонов В.О., Куценко С.А., Германюк А.П., Изварин І.В., Кравчук К.О. Технологія забезпечення живучості територіально-розподілених інформаційних комп'ютерних систем у єдиному інформаційному просторі // Реєстрація, зберігання і обробка даних. 2024. Т.26. № 1. – С.123-147.
4. Кузьмичов А.І. Кількісне оцінювання функціональної ефективності мережевих структур за аналізом чутливості оптимізаційної моделі до зовнішніх впливів. //Системні дослідження в енергетиці. 2024 2(77). – С.45-58.
5. Oleksandr Dodonov, Olena Gorbachyk, Maryna Kuznietsova. Critical Infrastructure Resilience and Cybersecurity of Information Management Systems. XXIII International Scientific and Practical Conference «Information Technologies and Security» (ITS 2023), pp. 1-10.
6. Aleksandr Dodonov, Aleksey Nikiforov, Vladimir Putyatin. Methods and Models for Building Adaptive Automated Systems of Organizational Management. XXIII International Scientific and Practical Conference «Information Technologies and Security» (ITS 2023), pp.134-145.
7. Германюк А.П. Методи та засоби протидії загрозам територіально-розподілених інформаційних комп'ютерних систем в єдиному інформаційному просторі // Реєстрація, зберігання і обробка даних. Щорічна підсумкова наукова конференція 18 вересня 2024 року: збірник / за ред. В.В.Петрова. Київ: ІПРІ НАН України, 2024. С.41-42. ISBN 977-617-8268-49-7.
8. Додонов В.О. Штучний інтелект у технології живучості систем організаційного управління // Реєстрація, зберігання і обробка даних. Щорічна підсумкова наукова конференція 18 вересня 2024 року: збірник / за ред. В.В.Петрова. Київ: ІПРІ НАН України, 2024. С.55-56. ISBN 977-617-8268-49-7.
9. Кузьмичов А. І. Застосування пост оптимального оцінювання прийнятих рішень щодо розподілу обмежених ресурсів // Реєстрація, зберігання і обробка даних. Щорічна підсумкова наукова конференція 18 вересня 2024 року: збірник / за ред. В.В.Петрова. Київ: ІПРІ НАН України, 2024. С.60-62. ISBN 977-617-8268-49-7.
10. Путятін В.Г. Метод Дельфі в задачах аналізу загроз та оцінки ризиків інформаційної безпеки територіально-розподілених інформаційних комп'ютерних систем // Реєстрація, зберігання і обробка даних. Щорічна підсумкова наукова конференція 18 вересня 2024 року: збірник / за ред. В.В.Петрова. Київ: ІПРІ НАН України, 2024. С.49-52. ISBN 977-617-8268-49-7.
11. Храмова І.О. Пом'якшення ризиків кібербезпеки корпоративних активів даних як частини критичної інфраструктури // Реєстрація, зберігання і обробка даних. Щорічна підсумкова наукова конференція 18 вересня 2024 року: збірник / за ред. В.В.Петрова. Київ: ІПРІ НАН України, 2024. С.67-69. ISBN 977-617-8268-49-7.
12. Додонов О., Горбачик О., Кузнєцова М. Способи і заходи забезпечення функціональної стійкості інформаційних систем критичних інфраструктур. // Інформаційні технології та безпека. Зб. наук. праць. – В.24. – К.: ІПРІ НАНУ, 2024. С. 3-6.
13. Додонов О., Кузьмичов А. Оптимально розподілена мережева структура розміщення і використання критичних ресурсів. // Інформаційні технології та безпека. Зб. наук. праць. – В.24. – К.: ІПРІ НАНУ, 2024. С. 118-119.
14. Храмова І. Використання каталогів даних в управлінні безпекою корпоративних інформаційних ресурсів. // Інформаційні технології та безпека. Зб. наук. праць. – В.24. – К.: ІПРІ НАНУ, 2024. С.181-184.

## **Х. Заключні відомості**

### **Керівник юридичної особи**

Петров Вячеслав Васильович

### **Перелік осіб-виконавців**

Безуглий Олексій Микитович

Бойченко Андрій Васильович

(к.т.н.)

Германюк Аліна Петрівна

(м.н.с.)

Горбачик Олена Семенівна

(к.т.н., с.н.с., 05.13.06)

Додонов Євген Олександрович

(н.с.)

Додонов Вадим Олександрович

(к. т. н., с.н.с.)

Додонов Олександр Георгійович

(д.т.н., професор, 05.13.13)

Коваль Олександр Васильович

(д. т. н., професор, 01.05.02)

Копіцена Ольга Миколаївна

Кузнецова Марина Глебівна

(к.т.н., с.н.с.)

Кузьмичов Анатолій Іванович

(к.т.н., доц., 05.13.13)

Куценко Світлана Альфредівна

(н.с)

Кірсанов Сергій Олександрович

(д. т. н.)

Путятін Володимир Григорович

(к. т. н., пров.н.с.)

Певцов Геннадій Володимирович

(д. т. н., професор)

Сенченко В'ячеслав Родіонович

(к.т.н.)

Храмова Ірина Олександрівна

(к.т.н., с.н.с., 05.13.06)

### **Відповідальний за підготовку облікових документів**

Манько Дмитро Юрійович

### **Телефон**

0730735912

### **Реєстратор**

Юрченко Тетяна Анатоліївна

**Керівник відділу УкрІНТЕІ, що є  
відповідальним за реєстрацію наукової  
діяльності**



Юрченко Тетяна Анатоліївна