

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U000908

Особливі позначки: відкрита

Дата реєстрації: 13-02-2024

Статус: Запланована

Реквізити наказу МОН / наказу закладу:



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Кушнерьов Олександр Сергійович

2. Oleksandr Kushnerov

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0001-8253-5698

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 051

Назва наукової спеціальності: Економіка

Галузь / галузі знань: соціальні та поведінкові науки

Освітньо-наукова програма зі спеціальності: Економіка

Дата захисту: 06-03-2024

Спеціальність за освітою: 051 Економіка

Місце роботи здобувача: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Римського-Корсакова, буд. 2, Суми, Сумський р-н., 40007, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): 4234

Повне найменування юридичної особи: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Римського-Корсакова, буд. 2, Суми, Сумський р-н., 40007, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Римського-Корсакова, буд. 2, Суми, Сумський р-н., 40007, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 06.51.25, 06.61.33, 06.01.30

Тема дисертації:

1. Детермінанти поширення та локалізації кіберзагроз в умовах цифровізації національної економіки
2. Determinants of the spread and localization of cyber threats in terms of the national economy digitalization

Реферат:

1. У дисертації наведено теоретичне узагальнення й запропоновано нове вирішення науково-прикладного завдання розвитку науково-методичних засад ідентифікації та локалізації кіберзагроз в умовах цифровізації національної економіки. Динамічний аналіз кількості наукових публікацій з питань протидії кібершахрайствам та посилення рівня кібербезпеки, реалізований за допомогою інструментарію VOSviewer v.1.6.10 та Scopus Citation Overview tool засвідчив, що середньорічний темп зростання опублікованих наукових статей з цієї проблематики складає 20%. У 2022 році опубліковано 690 наукових публікацій з досліджуваної тематики, що на 88,5% більше порівняно з 2018 роком. Науковці з США, Великобританії та Індії є найбільш активними у дослідженні питання кібербезпеки та кіберзахисту. Результати бібліометричного аналізу засвідчили наявність чотирьох кластерів. За результатами контекстуально-часового аналізу з питань кібершахрайств встановлено, що протягом 2019-2020 років основна увага почала приділятися технологіям та засобам забезпечення кібербезпеки, а починаючи з 2021 року науковий інтерес був зміщений на дослідження кіберфізичних систем, використання технологій штучного інтелекту для протидії кібератакам, вивчення ролі

кіберзахисту при впровадженні інтернету речей. У роботі обґрунтовано трактувати кіберзагрозу як дію наявних та/або потенційно можливих дестабілізуючих факторів й умов навмисного або випадкового порушення безпеки функціонування громадянина, економічних суб'єктів та держави у кіберпросторі. У роботі проведено змістове розмежування таких понять як «кіберзагроза», «кіберінцидент», «кібератака», «кіберзлочин». Розширено перелік об'єктів кібербезпеки за рахунок інформаційно-комунікаційних засобів фізичних осіб, які використовуються ними для реалізації суспільно та життєвоважливих потреб під час використання кіберпростору. На основі результатів ретроспективного аналізу тенденцій поширення кіберзагроз визначено ключові драйвери стрімкого нарощення загроз та ризиків у кіберпросторі. Упродовж 2005-2020 років найбільша кількість кібератак (41,8% від загального обсягу) була ініційована злочинцями з Китаю, при цьому 40% з них були направлені на об'єкти критичної інфраструктури у сфері публічного управління та 36% – на об'єкти приватного сектору. Найбільш розповсюдженою формою кібератаки у світі є різні види фішингу, що передбачає викрадення важливої інформації за допомогою електронних листів із застосуванням соціальної інженерії та обману. Щодо України, то у 2022 році офіційно зареєстровано 415 кіберінцидентів, що в 2,8 рази більше порівняно з 2021 роком. Розроблена методологія для типологізації країн за рівнем участі їх резидентів у здійсненні фінансових кібернетичних шахрайствах, яка передбачає врахування широкого кола індикаторів, що характеризують різні види злочинності та активність кримінальних угруповувань в країні, а також стану корупції, активності на даркнет-ринку, рівня кіберзлочинності та накладення на країну міжнародних санкцій. За результатами використання кластерного аналізу та побудови дерев класифікації обґрунтовано доцільність виокремлення двох груп країн. Для віднесення країни до першої групи необхідними та достатніми є наступні умови: значення змінної «ризик корупції та хабарів» має приймати значення більше 56,500 одиниць, значення змінної «загальний дохід, який отримано на даркнет-ринку» – менше 5,4100 одиниць, значення змінної «міжнародні санкції, які накладені на країну» – менше 0,05 одиниць, значення змінної інтегрального рівня активності кримінальних угруповувань, яке приймає значення менше 0,504 одиниць, значення змінної інтегрального рівня характеристики різних видів злочинності – не більше 0,590 одиниць. За протилежних умов вищезазначених індикаторів країни віднесено до другої групи. Удосконалено методи обґрунтування факторів поширення кіберзагроз в національній економіці за допомогою системного поєднання сигмоїдної моделі, методів машинного навчання SVM та групового врахування аргументів Івахненка. На основі аналізу п'ятнадцяти індикаторів, що характеризують різні види кібершахрайств, розроблено узагальнений індекс кіберзагроз для економічних суб'єктів. За результатами емпіричного дослідження встановлено, що основними драйверами зростання кібершахрайства є частка населення, що користується онлайн банкінгом, рівень навичок в Інтернеті та інтенсивність онлайн діяльності.

2. The dissertation provides a theoretical generalization and offers a new solution to the scientific and applied task of developing the scientific and methodological foundations of identification and localization of cyber threats in terms of digitalization of the national economy. A dynamic analysis of the number of scientific publications on countering cyber fraud and strengthening the level of cyber security, implemented using the VOSviewer v.1.6.10 toolkit and the Scopus Citation Overview tool, showed that the average annual growth rate of published scientific articles on this issue is 20%. In 2022, 690 scientific publications on the subject under study were published, which is 88.5% more than in 2018. Scientists from the USA, Great Britain and India are the most active in researching the issue of cyber security and cyber defence. The results of the bibliometric analysis proved the existence of four clusters. According to the results of a contextual and temporal analysis of cyber fraud issues, it was established that during 2019-2020, the main attention began to be paid to technologies and means of ensuring cyber security. Starting from 2021, scientific interest was shifted to the study of cyber-physical systems, the use of artificial intelligence technologies to counter cyber-attacks, as well as the study the role of cyber protection in the implementation of the Internet of Things. It is justified in the study to interpret the cyber threat as the effect of existing and/or potentially possible destabilizing factors and conditions of intentional or accidental violation of the security of the functioning of the citizen, economic entities, and the state in cyberspace. A meaningful distinction of such concepts as “cyber threat”, “cyber incident”, “cyber-attack”, “cybercrime” is made. The list of

cyber security objects has been expanded due to the information and communication means of individuals, which are used by them to realize socially and vitally important needs when using cyberspace. Based on the results of a retrospective analysis of the trends in the spread of cyber threats, the key drivers of the rapid increase in threats and risks in cyberspace have been identified. During 2005-2020, the largest number of cyberattacks (41.8% of the total volume) was initiated by criminals from China, while 40% of them were directed to objects of critical infrastructure in the field of public administration, and 36% to objects of the private sector. The most widespread form of cyberattack in the world is various types of phishing, which involves the theft of important information with the help of e-mails using social engineering and deception. As for Ukraine, 415 cyber incidents were officially registered in 2022, which is 2.8 times more than in 2021. A methodology has been developed for the typology of countries according to the level of participation of their residents in financial cyber fraud, taking into account a wide range of indicators characterizing various types of crime and the activity of criminal groups in the country, as well as the state of corruption, activity on the dark net market, the level of cybercrime and the imposition to the country of international sanctions. Based on the results of the use of cluster analysis and the construction of classification trees, the expediency of separating two groups of countries is substantiated. The following conditions are necessary and sufficient to assign a country to the first group: the value of the variable "risk of corruption and bribes" should be greater than 56,500 units, the value of the variable "total income received on the dark net market" should be less than 5,4100 units, the value of the variable "international sanctions imposed on the country" should be less than 0,05 units, the value of the variable of the integral level of the criminal groups activity, which takes a value of less than 0.504 units, the value of the variable of the integral level of the characteristics of various types of crime should be no more than 0.590 units. Under the opposite conditions of the above-mentioned indicators, the country is assigned to the second group. Methodological principles for analyzing factors in the rapid spread of cyber threats in the national economy have been improved. This involves combining the sigmoid model with SVM machine learning and Ivakhnenko's group considerations. A comprehensive cyber threats index for economic entities was created using fifteen indicators for various fraud types. Empirical research on the accelerated growth of cyber fraud in the national economy identified key drivers: the percentage of the population using online banking, Internet skill levels, and online activity intensity.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Фундаментальні наукові дослідження з найбільш важливих проблем розвитку науково-технічного, соціально-економічного, суспільно-політичного, людського потенціалу для забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держави

Стратегічний пріоритетний напрям інноваційної діяльності: Не застосовується

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Доценко Т. В., Кушнерьов О. С. Використання гравітаційного моделювання при оцінюванні ризику використання банків з метою легалізації доходів, отриманих злочинним шляхом. Теорія та практика забезпечення розвитку кіберпростору України : монографія / за ред. О .В. Кузьменко, Г. М. Яровенко. Київ: Інтерсервіс, 2020. С. 110-131
- Доценко Т. В., Кушнерьов О. С. Моделювання інтегрального індексу загрози національної економіки за допомогою метода Кернела. Теорія та практика забезпечення розвитку кіберпростору України: монографія / за ред. О .В. Кузьменко, Г. М. Яровенко. Київ: Інтерсервіс, 2020. С. 157-172
- Золковер А. О., Кузьменко О. В., Кушнерьов О. С., Койбічук В. В. Бібліометричний аналіз досліджень кіберзлочинності в умовах цифровізації фінансового сектору економіки держави. Вісник Хмельницького національного університету. 2019. № 6, Том 2. С. 253-259.

- Бойко А. О., Миненко С. В., Кушнерьов О. С., Хмелик О.С. Створення управлінських інформаційних систем виявлення фінансових операцій, що підлягають під ознаки внутрішнього фінансового моніторингу. Вісник Сумського державного університету. Серія Економіка. 2017. № 4. С. 58-66.
- Боженко В.В., Кушнерьов О.С., Кільдей А.Д. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. Економічний форум. 2021. № 4. С. 116-121.
- Кузьменко О. В., Доценко Т. В., Кушнерьов О. С. Удосконалення системи фінансового моніторингу: автоматизація процесу верифікації клієнтів банку. Науковий погляд: економіка та управління. 2021. № 2. С. 88-95.
- Леонов С. В., Кузьменко О. В., Койбічук В. В., Кушнерьов О. С. Розроблення моделі бізнес-процесу автоматизованого моніторингу фінансових операцій банком для протидії легалізації кримінальних доходів. Вісник Сумського державного університету. Серія Економіка. 2021. № 1. С. 9-16.
- Леонов С. В., Кузьменко О. В., Кушнерьов О. С., Люльов О. В., Квілінський О. С. Теоретичні основи формування інформаційної бази дослідження ризику використання фінансових установ України з метою легалізації кримінальних доходів. Вісник Сумського державного університету. Серія Економіка. 2020. С. 104-113.
- Кузьменко О. В., Доценко Т. В., Кушнерьов О. С. Оцінювання ризику використання банків з метою легалізації кримінальних доходів на основі гравітаційного моделювання. Проблеми і перспективи економіки та управління. 2020. № 1 (21). С. 205-219.
- Кушнерьов О. С. Тенденції шахрайських операцій на банківському ринку та можливості протидії. Інноваційна економіка. 2019. № 3-4. С. 180-188.
- Kuzmenko O.V., Kubálek J., Bozhenko V.V., Kushneryov O.S., Vida I. An approach to managing innovation to protect financial sector against cybercrime *Podjęcie do zarządzania innowacjami w celu ochrony sektora finansowego przed cyberprzestępczością*. Polish Journal of Management Studies. 2021. № 24. С. 276-291.
- Kuzmenko O., Krukhmal O., Koibichuk V., Hrytsenko K., Kushneryov O., Hordiienko V., Pasemko G., Taran O., Smihunova O. Survival Analysis Methods for Assessing the Anti-Money Laundering System Effectiveness. WSEAS Transactions on Business and Economics. 2023. 20. P. 1185-1206.

Наукова (науково-технічна) продукція: методи, теорії, гіпотези

Соціально-економічна спрямованість: створення методів протидії фінансовим кіберзагрозам та кібершахрайствам у фінансових установах з метою збереження стабільності фінансово-економічної системи та власності громадян

Охоронні документи на ОПВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0121U100467, 0122U000783, 0123U101945, 0121U100473

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Бойко Антон Олександрович

2. Anton Boiko

Кваліфікація: д. е. н., професор, 08.00.03, 08.00.08

Ідентифікатор ORCID ID: 0000-0002-1784-9364

Додаткова інформація:

Повне найменування юридичної особи: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Римського-Корсакова, буд. 2, Суми, Сумський р-н., 40007, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Маргасова Вікторія Геннадіївна

2. Viktoriya Marhasova

Кваліфікація: д. е. н., професор, 08.00.03

Ідентифікатор ORCID ID: 0000-0001-8582-2158

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Чернігівська політехніка"

Код за ЄДРПОУ: 05460798

Місцезнаходження: вул. Шевченка, буд. 95, Чернігів, Чернігівський р-н., 14035, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Демчишак Назар Богданович

2. Nazar Demchyshak

Кваліфікація: д. е. н., професор, 08.00.08

Ідентифікатор ORCID ID: 0000-0001-6852-7405

Додаткова інформація:

Повне найменування юридичної особи: Львівський національний університет імені Івана Франка

Код за ЄДРПОУ: 02070987

Місцезнаходження: вул. Університетська, буд. 1, Львів, 79000, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Пахненко Олена Михайлівна
2. Olena Pakhnenko

Кваліфікація: к. е. н., доц., 08.00.08**Ідентифікатор ORCID ID:** 0000-0002-4703-4078**Додаткова інформація:****Повне найменування юридичної особи:** Сумський державний університет**Код за ЄДРПОУ:** 05408289**Місцезнаходження:** вул. Римського-Корсакова, буд. 2, Суми, Сумський р-н., 40007, Україна**Форма власності:** Державна**Сфера управління:** Міністерство освіти і науки України**Ідентифікатор ROR:****Власне Прізвище Ім'я По-батькові:**

1. Семенов Андрій Юрійович
2. Andrii Semenog

Кваліфікація: к. е. н., доц., 08.00.08**Ідентифікатор ORCID ID:** 0000-0003-3222-9574**Додаткова інформація:****Повне найменування юридичної особи:** Сумський державний університет**Код за ЄДРПОУ:** 05408289**Місцезнаходження:** вул. Римського-Корсакова, буд. 2, Суми, Сумський р-н., 40007, Україна**Форма власності:** Державна**Сфера управління:** Міністерство освіти і науки України**Ідентифікатор ROR:****VIII. Заключні відомості****Власне Прізвище Ім'я По-батькові
голови ради**

Школьник Інна Олександрівна

**Власне Прізвище Ім'я По-батькові
головуючого на засіданні**

Школьник Інна Олександрівна

**Відповідальний за підготовку
облікових документів**

Бойко Антон Олександрович

Реєстратор

УкрІНТЕІ

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



Юрченко Тетяна Анатоліївна