

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U003733

Особливі позначки: відкрита

Дата реєстрації: 27-12-2024

Статус: Захищена

Реквізити наказу МОН / наказу закладу:



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Гулак Євген Геннадійович

2. Yevhen H. Hulak

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0003-4984-686X

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерні науки

Дата захисту: 19-02-2025

Спеціальність за освітою: Інженер телекомунікацій

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 26.204.01

Повне найменування юридичної особи: Інститут проблем математичних машин і систем Національної академії наук України

Код за ЄДРПОУ: 05417503

Місцезнаходження: проспект Академіка Глушкова, буд. 42, Київ, 03680, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

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

Повне найменування юридичної особи: Інститут проблем математичних машин і систем Національної академії наук України

Код за ЄДРПОУ: 05417503

Місцезнаходження: проспект Академіка Глушкова, буд. 42, Київ, 03680, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56.01

Тема дисертації:

1. Моделі та методи забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору
2. Models and methods of guaranteeing capability and cyber security of information and communication systems of the energy sector

Реферат:

1. Дисертація присвячена вирішенню актуального наукового завдання, сутність якого полягає в розробці моделей та методів забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору для підвищення спроможностей Об'єднаних Енергетичних Систем України (ОЕС-У) протистояти кризовим ситуаціям. Енергетика є високотехнологічною галуззю народного господарства, вона потребує для вирішення завдань управління відповідними електроенергетичними комплексами застосування новітніх інформаційних технологій, що спроможні у реальному часі забезпечувати збирання, передачу, обробку та відображення технологічної інформації для її аналізу персоналом й прийняття на її основі необхідних управлінських рішень. Зазначене, зокрема, стосується систем управління технологічними

процесами, диспетчерського управління електротехнічними підприємствами, контролю якості електричної енергії, обліку електричної енергії тощо. Складним інформаційним та управляючим системам енергетичного сектору притаманні існування складних, іноді суперечливих зв'язків та взаємних впливів, наявність значної кількості різнорідних компонентів, які для досягнення певної мети об'єднані в єдину систему, наявність багатьох власників та розпорядників у різних підсистемах, що призводить до неузгодженості заходів з захисту та контролю безпеки. Зазначені фактори, безперечно, ускладнюють впровадження єдиних підходів до реалізації комплексу організаційно-технічних заходів та засобів захисту, виникає низка науково-технічних проблем, які стосуються: – узгодження порядку та умов корпоративного захисту інформаційно-технологічної системи, яка складається з підсистем різних власників (розпорядників); – встановлення принципів побудови та вимог з безпеки до шлюзу взаємодії між інформаційно-технологічними підсистемами, щодо яких визначені різні вимоги з безпеки тощо. Отже, актуальним постає наукове завдання, щодо забезпечення необхідного рівня гарантоздатності та кібербезпеки складної критичної інформаційної інфраструктури енергетичного сектору шляхом побудови корпоративного сегменту кіберзахисту та кіберстійкості, а також реалізації підсистеми криптографічного захисту, що забезпечуватиме підвищений рівень конфіденційності, цілісності та імітостійкості під час взаємодії між різними підсистемами. Метою дисертаційного дослідження є підвищення гарантоздатності та кібербезпеки інформаційних систем енергетичного сектору завдяки поєднанню корпоративного захисту складної критичної інформаційної інфраструктури на основі розробки відповідних моделей і методів забезпечення кіберзахисту та кіберстійкості з використанням вдосконаленої архітектури та децентралізованого підходу до розмежування доступу в мережі центру кібербезпеки, а також криптографічних рішень для безпечного інформаційного обміну між підсистемами енергетичного сектору. У відповідності до сформованої мети для вирішення зазначеної науково-прикладної проблеми забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору для підвищення кіберстійкості ОЕС-У в роботі були отримані такі наукові результати: 1. Вперше на основі формування класів еквівалентності запропоновано методику декомпозиції складних систем, що підлягають кіберзахисту, яка враховує можливість інформаційного обміну між підсистемами з різними вимогами до захисту інформації з обмеженим доступом. 2. Вдосконалено модель побудови корпоративного центру кібербезпеки енергетичного сектору на основі сервіс-орієнтованої архітектури з визначеною бізнес-логікою та відповідним набором функцій, що забезпечуватиме динамічне оброблення кіберінцидентів у реальному часі. Вдосконалена модель відповідає сучасним викликам безпеці та враховує специфіку завдань і функцій ОЕС-У. 3. Вдосконалено модель побудови децентралізованої системи розмежування доступу в мережі центру кібербезпеки на основі оригінальної методики розподілу секрету. Запропонована модель припускає її масштабування та мінімізує ризик несанкціонованого доступу до інформаційних ресурсів. 4. Подальшого розвитку набула модель побудови підсистеми криптографічного захисту інформації, що забезпечуватиме можливість двоконтурного шифрування для розмежування доступу в децентралізованій системі розмежування доступу до інформаційних ресурсів, розроблені та обґрунтовані рекомендації щодо підвищення безпеки криптографічного захисту інформації коротких службових повідомлень. 5. Подальшого розвитку набула методика оцінки та раціонального визначення характеристик захисту криптографічної підсистеми.

2. The dissertation is devoted to the solution of an actual scientific task, the essence of which is the development of models and methods for ensuring the guarantee capability and cyber security of information and communication systems of the energy sector in order to increase the capabilities of the United Energy Systems of Ukraine (UES-U) to withstand crisis situations. Energy is a high-tech branch of the national economy, it requires the use of the latest information technologies capable of providing real-time collection, transmission, processing and display of technological information for its analysis by personnel and making the necessary management decisions based on it in order to solve the tasks of managing the relevant electric power complexes. This applies, in particular, to systems for managing technological processes, dispatching control of electrical engineering enterprises, quality control of electrical energy, accounting for electrical energy, etc. Complex information and management systems of the energy sector are characterized by the existence of complex, sometimes

contradictory relationships and mutual influences, the presence of a significant number of heterogeneous components that are combined into a single system to achieve a certain goal, the presence of many owners and managers in different subsystems, which leads to inconsistencies in security protection and control measures. These factors undoubtedly complicate the implementation of unified approaches to the implementation of a complex of organizational and technical means and protection measures, a number of scientific and technical problems arise, which concern: – coordination of the order and conditions of corporate protection of the information technology system, which consists of subsystems of different owners (administrators); – establishment of construction principles and security requirements for the gateway of interaction between information technology subsystems, for which various security requirements are defined, etc. Therefore, the scientific task of ensuring the necessary level of cyber security and guarantee capability of the complex critical information infrastructure of the energy sector by building a corporate segment of cyber protection and cyber resilience, as well as implementing a cryptographic protection subsystem, which will ensure an increased level of confidentiality and impersonation resistance during interaction between different subsystems, becomes urgent. The aim of the dissertation research is to increase the cyber security and guarantee capacity of information systems of the energy sector thanks to the combination of corporate protection of complex critical information infrastructure based on the development of appropriate models and methods for ensuring cyber protection and cyber resilience using an improved architecture and a decentralized approach to delimiting access in the network of the cyber security center and new cryptographic solutions for secure information exchange between subsystems of energy sector systems. In accordance with the formed goal to solve the specified scientific and applied problem of ensuring the guaranteeability and cyber security of information and communication systems of the energy sector to increase the cyber resilience of UES-U, the following scientific results were obtained in the work: 1. For the first time, based on the formation of equivalence classes, a method of decomposition of complex systems subject to cyber protection is proposed, which takes into account the possibility of information exchange between subsystems with different requirements for protecting information with limited access. 2. The model of building a corporate cyber security center of the energy sector based on a service-oriented architecture with a defined business logic and a corresponding set of functions that will ensure dynamic processing of cyber incidents in real time has been improved. The improved model meets modern security challenges and takes into account the specific tasks and functions of the UES-U. 3. The model of building a decentralized system of delimiting access in the network of the cyber security center based on the original method of secret distribution has been improved. The proposed model assumes its scaling and minimizes the risk of unauthorized access to information resources. 4. The model of building a subsystem of cryptographic protection of information gained further development, which will provide the possibility of double-circuit encryption for delimiting access in a decentralized system of delimiting access to information resources, developed and substantiated recommendations to increase the security of cryptographic protection of information of short service messages. 5. The method of evaluation and rational determination of the characteristics of the protection of the cryptographic subsystem acquired further development.

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: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Гулак Г. М., Скітер І. С., Гулак Є. Г. (2021) Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об'єктів ядерної енергетики. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка". 2021. Т. 4, № 12. 172–186
- Деренговський В.В., Кафтанатіна О.А., Кордюков П.Л., Меньшенін Є.А., Гулак Є.Г. (2021) Розробка математичної моделі впливу радіаційно небезпечних об'єктів на довкілля при пожежі. Математичні машини і системи. 2021. №4. С. 99–111
- Гулак Г., Жданова Ю., Складанний П., Гулак Є., Корнієць В. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145-158
- Гулак Є. Г. (2024) Методика раціонального синтезу підсистеми криптографічного захисту інформації в мережах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка» 4(24), 282-297
- A. Morozov, A. Hrebennyk, E. Trunova, I. Skiter, and E. Hulak. Design of Industry Centers of Cyber Security of Facilities of Critical Infrastructure. Workshop on Cybersecurity Providing in Information and Telecommunication Systems CPITS-II-2021: October 26, 2021, Kyiv, Ukraine, vol. 3187, pp. 27-37. ISSN: 1613-0073
- H. Hulak, V. Grechaninov, E. Hulak, P. Skladannyi, V. Sokolov Decentralized Access Demarcation System Construction in Situational Center Network. Cybersecurity Providing in Information and telecommunication Systems (CPITS-II-2021): October 26, 2021, Kyiv, Ukraine, vol. 3188, pp. 197-206. ISSN: 1613-0073
- Hulak, H., Skladannyi, P., Sokolov, Sokolov V., Hulak, E., Korniiets V., Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System, 2nd International Conference on Conflict Management in Global Information Networks: November 2022, Kyiv, Ukraine: Vol. 3530, pp. 102-111, ISSN: 1613-0073

Наукова (науково-технічна) продукція: методи, теорії, гіпотези; програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0122U201115, 0121U000107

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Складанний Павло Миколайович
2. Pavlo M. Skladannyi

Кваліфікація: к. т. н., доцент, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-7775-6039

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Гнатюк Сергій Олександрович
2. Serhii Gnatyuk

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: 0000-0003-4992-0564

Додаткова інформація:

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович
2. Oleksii Smirnov

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0001-9543-874X

Додаткова інформація:

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, буд. 8, Кропивницький, Кропивницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Немкова Олена Анатоліївна

2. Olena Nyemkova

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: 0000-0003-0690-2657

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Оксанич Ірина Миколаївна

2. Iryna M. Oksanich

Кваліфікація: к. т. н., с.н.с., 05.13.06

Ідентифікатор ORCID ID: 0000-0002-1208-3427

Додаткова інформація:

Повне найменування юридичної особи: Інститут проблем математичних машин і систем
Національної академії наук України

Код за ЄДРПОУ: 05417503

Місцезнаходження: проспект Академіка Глушкова, буд. 42, Київ, 03680, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

VIII. Заключні відомості

**Власне Прізвище Ім'я По-батькові
голови ради**

Литвинов Валерій Андроникович

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

Литвинов Валерій Андроникович

**Відповідальний за підготовку
облікових документів**

Каревіна Наталія Павлівна

Реєстратор

УкрІНТЕІ

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



Юрченко Тетяна Анатоліївна