Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0821U100719

Особливі позначки: відкрита

Дата реєстрації: 05-05-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Сорокін Денис Володимирович

2. Sorokin Denys V.

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 22-04-2021

Спеціальність за освітою: 0924 Телекомунікації Інформаційні мережі зв'язку

Місце роботи здобувача: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, м. Київ, 03680, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 26.861.004

Повне найменування юридичної особи: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, м. Київ, 03680, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

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

Повне найменування юридичної особи: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, м. Київ, 03680, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.39

Тема дисертації:

1. МЕТОДИКА СТВОРЕННЯ ЗАХИЩЕНИХ СПЕЦІАЛІЗОВАНИХ МЕРЕЖ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ НАДАННЯ ПРОМИСЛОВИХ СЕРВІСІВ

2. A methodology for creating protected specialized networks, aimed at increasing the efficiency of industrial services provision

Реферат/анотація:

1. Дисертаційна робота присвячена вирішенню актуального наукового завдання, сутність якого полягає в розробці методики створення захищених спеціалізованих мереж з метою підвищення ефективності надання промислових сервісів. Промислові об'єкти важкої та металургійної промисловості постійно накопичують значні обсяги конфіденційної інформації про своїх співробітників, клієнтів, виробництва продукції, наукові дослідження, розробки та фінансові результати. Поряд з тим, постають і нові виклики до доступу, обробки та зберігання такої інформації на підприємствах. Отримання фінансових результатів, конфіденційної інформації до рук конкурентів, або кіберзлочинців, можуть завдати підприємствам незворотних фінансових та репутаційних збитків. Основними засобами протидії загрозам інформаційної та кібербезпеки, залишаються комплекс засобів адміністративно розпорядчих дій та впровадження систем захисту інфраструктури від зовнішнього несанкціонованого доступу та незаконного заволодіння конфіденційними

даними. Проводячи в дослідженні аналіз кібератак за останні п’ять років, більшість атак припало на критичну інфраструктуру, енергетичних, транспортних, логістичних підприємств. Відправною точкою у дослідженні є аналіз працюючих промислових сервісів, та вивчення можливостей сучасних технологій для створення універсальної спеціалізованої інформаційно-промислової мережі, що зможе забезпечити потреби бізнесу та промисловості на рівні доступності мережі та безпеки несанкціонованого доступу. Значний вплив інформаційної сфери на суспільний прогрес зумовлює необхідність посилення уваги до розгортання та впровадження приватних промислових мереж, з метою підвищення ефективності функціонування спеціалізованих інформаційно-промислових мереж, які можуть бути використані в вугільній та металургійній промисловості. Відповідно до сьогоденних суспільних викликів, та можливих ризиків, які мають місце в приватних мережах, в дисертаційному дослідженні розглянуто альтернативні підходи та методики розгортання, побудови приватних промислових мереж. Розробка такої методики дозволить створювати гнучку систему, яка вирішуватиме потреби бізнесу, пов'язаного з автоматизацією промислового виробництва та інформаційної безпеки. Моделі побудови інфраструктури спрямовані на забезпечення основних промислових сервісів для підприємств вугільної, гірничої та важкої промисловості. В результаті аналізу моделей діючих промислових мереж, виявляються значні недоліки, що обумовлені середовищем поширення сигналів. Саме тому постає потреба в розробці універсальної методики створення спеціалізованих захищених мереж, що підвищить ефективність надання промислових сервісів на базі теоретичних та практичних рішень, що використовують електромагнітне випромінення в особливих умовах. За результатами математичних розрахунків випливає, що поширення радіохвиль в особливих умовах значно відрізняється від поширення радіохвиль на поверхні землі. Поширення радіохвиль в тунелі, в шахті, можна відобразити в променевій теорії, що є більш прийнятною, оскільки довжина хвилі стає дуже малою в порівнянні з поперечним діаметром тунелю. Внаслідок великої кількості ліній відбитих сигналів, поширення радіохвиль відбуватиметься з багатопроменевими характеристиками, з релеєвським або райсовським завмиранням. Відразу за перешкодою виникнуть дифракційні втрати за рахунок затінення. Основною причиною є коефіцієнт ослаблення радіосигналу при поширенні в тунелях, який зокрема, залежить від неоднорідності, змін в напрямку тунелю, перешкод, а також електричних властивостей гірських порід. Аналіз методики розрахунків показав, що потужність сигналу буде змінюватися. Сигнал може розповсюджуватись по прямій, відбиватися, або заломлюватися. Якість прийому буде залежати від декількох факторів: умови прийому, частотних зрушень, часових затримок та типу модуляції. На прийом сигналу можуть впливати небажані сигнали від інших джерел, що можуть використовувати ті ж самі частоти, що і корисний сигнал. Результати дослідження показали, що при плануванні спеціалізованої мережі радіодоступу необхідно враховувати додаткові показники загасання сигналів для організації надійних каналів зв’язку в особливих умовах поширення електромагнітних хвиль. Теоретичне експериментальне дослідження поширення електромагнітного поля в різних діапазонах частот в гірських породах, показало можливість передачі сигналів на відстані, що перевищують 200 м, в "чистій" гірничій виробці і понад 1 км з використанням направлених антен. За результатами математичної оцінки поширення радіохвиль, запропоновано два сценарії розгортання захищеної приватної промислової мережі в шахті. Для виконання вимог доступності мережі, при виникненні інциденту в підземній частині шахти, запропоновано методику резервування частини системи RAN, та резервування географічно рознесеної підсистеми Core (EPC).

2. The thesis is dedicated to the solution of an urgent scientific task, its essence being the development of a methodology for creating protected specialized networks, aimed at increasing the efficiency of industrial services provision. Industrial facilities of the heavy and metallurgical industries constantly accumulate huge volumes of sensitive data about their employees, customers, production, scientific research, solutions and financial outcomes. Obtaining financial results, sensitive data by rivals or cyber criminals may cause enterprises’ irreversible financial and reputational losses. The main means of counteracting information and cyber security threats are a complex of administrative disposals and introduction of infrastructure protection from external unauthorized access and illegal sensitive data takeover. As a result of analyzing cyber attacks for the last five years, most attacks have accounted for the crucial infrastructure, energy, transport, logistics enterprises. The starting point of the research

is the analysis of the functioning industrial services and studying advanced technologies opportunities to create a unified specialized information and industrial network, able to satisfy the business and industry needs at the level of the network accessibility and unauthorized access security. A considerable impact of the information sphere on the social progress specifies the necessity of closer attention to expand and introduce private industrial networks for the purpose of increasing the efficiency of functioning of specialized information and industrial networks that may be used in the coal and metallurgical industries. Development of such a methodology will make it possible to create a flexible system, meeting needs of the business, related to industrial production automation and information security. Due to the system of network elements authenticity, access to the IoT platform will be restricted, making it possible to minimize risks of hackers' attack isothermic methods via a smart-gadget. While considering model systems of constructing and administering industrial networks infrastructure, four separate levels are defined that are combined into a unified information and communication industrial infrastructure. The analysis of the functioning models of industrial networks has resulted in detecting considerable failures, caused by the signal propagation environment. That is why there emerges the need to develop a universal methodology of creating specialized protected systems, improving the efficiency of providing industrial services, based on theoretical and practical solutions, using electromagnetic emission under special conditions. To develop such a methodology, special environment is analyzed and mathematical schemes of electromagnetic emission spread in mines are calculated. The mathematical calculations result in the conclusion that radio waves spread under special conditions is radically different from radio waves spread on the Earth surface. As a result, radio waves spread will occur with multi-ray characteristics, with relay or Rician fading. Following the interference, diffraction losses occur due to shading. In modern mines a considerable level of electrical and magnetic interference is caused by the functioning electrical equipment in underground mining workings. To tackle the issue of electrical and magnetic interference impact, it is necessary to conduct separate research with a proper list of the used equipment. The calculations analysis has proven that a signal power will differ depending on the antenna height and location. The signal can spread in a line pattern, be echoed or be deflected. The reception quality will depend on several factors. In a similar way the signal reception can be influenced by unwanted signals from other sources that can use the same or neighboring frequencies. The research outcomes have shown that while planning a specialized radio access network it is necessary to take into account additional indices of signal fading for the purpose of organizing reliable communication channels under the special conditions of electrical and magnetic waves spread. The theoretical experimental research of electrical and magnetic field spread in various frequency ranges in rocks has shown the possibility of distant transmission of signals, exceeding 200 m, in "clear" underground mining workings and more than 1 km with the beam antenna application. Based on the outcomes of mathematical assessment of radio waves spread, two scenarios of developing a protected private industrial network in a mine have been suggested. To meet the network accessibility demands, in case of an incident in the underground mine part, the methodology of reserving a RAN system part, as well as reserving a far-flung Core (EPC) subsystem.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Гайдур Галина Іванівна

2. Haidur Halyna I.

Кваліфікація: д. т. н., 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Юдін Олександр Костянтинович

2. Yudin Oleksandr K.

Кваліфікація: д. т. н., 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Радівілова Тамара Анатоліївна

2. Radivilova Tamara A.

Кваліфікація: к. т. н., 01.05.02

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Довженко Надія Михайлівна
2. Dovzhenko Nadiia M

Кваліфікація: к. т. н., 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Лаптєв Олександр Анатолійович
2. Laptiev Oleksandr Anatoliiovych

Кваліфікація: д. т. н., 05.13.21, 20.02.14

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Савченко Віталій Анатолійович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Савченко Віталій Анатолійович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.