АНОТАЦІЯ

Сорокін Д.В. Методика створення захищених спеціалізованих мереж для підвищення ефективності надання промислових сервісів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека». – Державний університет телекомунікацій, МОН України, Київ, 2021.

Дисертаційна робота присвячена вирішенню актуального наукового завдання, сутність якого полягає в розробці методики створення захищених спеціалізованих мереж з метою підвищення ефективності надання промислових сервісів.

В умовах розвитку та впровадження сучасних інформаційних технологій в життєдіяльність сьогоднішнього суспільства, а саме в органи державної влади, фінансові інститути, корпорації та в приватний сектор економіки – де пріоритетного значення набуває розвиток та діджиталізація важкої промисловості.

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.

З точки зору бізнесу, розвиток інформаційної безпеки підприємства повинен бути збалансований щодо витрат економічної моделі вкладених інвестицій. Це дозволяє оптимально вирішувати задачі інформаційної безпеки, а саме: конфіденційності, цілісності та доступності.

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 (BlackEnergy, TeleBots, CryptoLocker, GreyEnergy, Industroyer, Petya та NotPetya, BadRabbit, Buhtrap, WannaCry, TeslaCrypt, Nyetya), 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.

На базі цих підходів, пропонується розгорнути гнучку систему радіодоступу, що працюватиме в особливих радіоумовах, та скоординує роботу структурних підсистем підприємств (M2M пристроїв, Smart-датчиків). Замість автономних підсистемних мереж телеметрії та мережі виконавчих пристроїв, на передній план виходить рішення, що підтримують міжмашинний зв'язок, здатний відстежувати і стандартизувати дії агентів по всьому ланцюгу взаємодій бізнес-процесу підприємства. Мережева взаємодія M2M пристроїв дозволить знизити похідні операційні витрати і підвищити гнучкість підприємств.

Розробка такої методики дозволить створювати гнучку систему, яка вирішуватиме потреби бізнесу, пов'язаного з автоматизацією промислового виробництва та інформаційної безпеки.

Завдяки системі аутентифікації мережевих елементів, доступ до платформи IoT буде обмежений, це дозволить мінімізувати ризики ізотермічних методів атак хакерів на smart-пристрої.

При розгляді модельних систем побудови та управління інфраструктури промислових мереж, відокремлюють чотири окремих рівня, які об'єднуються між собою в єдину інфокомунікаційну промислову інфраструктуру: рівень підприємства; рівень виробництва; рівень машинної взаємодії; рівень телеметрії та датчиків. Такі моделі побудови інфраструктури спрямовані на забезпечення основних промислових сервісів для підприємств вугільної, гірничої та важкої промисловості, які потребують сервісів, що забезпечать: облік рухомої техніки і матеріальних засобів (використання сучасних ERP-систем); управління безпілотними апаратами та машинами (взаємодія M2M пристроями); сервіс оперативного групового зв'язку (Voice/Video/PtT); сервіс телеметрії (взаємодія smart-датчиків); сервіс передачі геолокації співробітників і техніки (GPS-tracking/ Tiger-tracking); сервіс безпеки доступу та сигналізації (система моніторингу та безпека периметру / відео-нагляду); сервіс сигналізації та аварійного оповіщення (оповіщення про небезпеку / звукова та світлова сирена); сервіс конференц-зв’язку (селекторний зв'язок, відеоконференція); сервіс передачі даних.

Для розробки методики аналізуються мережі, що побудовані на основі відкритих мереж, які засновані на міжнародних стандартах і адаптовані до вимог на всіх рівнях автоматизації, які забезпечують простоту і оптимальність вибору обладнання. Аналізується можливості та вимоги мереж: промислового Ethernet, як мережа, яка працює за принципом доступу до середовища, заснованого на механізмі виявлення конфліктів (колізій); Modbus, як мережа, що взаємодіє з M2M пристроями; мережа CAN, як мережа контролерів, що забезпечує роботу

виконавчих пристроїв; AS-I, як мережева підсистема, що забезпечує роботу промислово-інформаційних завдань.

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.

Для розробки такої методики проводиться аналіз специфічного середовища, а також розраховуються математичні схеми поширення електромагнітного випромінення в шахтах. 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. Тунель зі сторонами, які можна порівняти з довжиною хвилі, буде забезпечувати поширення сигналу за рахунок відбиття від стін, при яких більшість матеріалів демонструють високі коефіцієнти відображення. Внаслідок великої кількості ліній відбитих сигналів, поширення радіохвиль відбуватиметься з багатопроменевими характеристиками, з релеєвським або райсовським завмиранням. Також перешкоди в тунелі будуть створювати радіохвилі з частотами, значно вищими за граничну, які, переважно будуть розсіюватися під великими кутами, а отже, будуть переривати процес відображень. 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. В роботі розглянуті найпоширеніші методи визначення електричних властивостей гірських порід.

В сучасних шахтах значний рівень електромагнітних перешкод в підземних гірничих виробках створюється працюючим електричним устаткуванням. Для вирішення питання впливу рівнів електромагнітних перешкод в підземних шахтах, необхідно проводити окреме дослідження з відповідним переліком обладнання, що використовується, або може використовуватись в вугільних шахтах з особливими умовами.

Аналіз методики розрахунків показав, що потужність сигналу буде змінюватися в залежності від висоти та місця встановлення антен. Сигнал може розповсюджуватись по прямій, відбиватися, або заломлюватися. Якість прийому буде залежати від декількох факторів, таких як: умови прийому, частотних зрушень, часових затримок та типу модуляції. Аналогічним чином на прийом сигналу можуть впливати небажані сигнали від інших джерел, що можуть використовувати ті ж самі частоти, що і корисний сигнал, або сусідні частоти.

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).

Відповідно до сьогоденних суспільних викликів та можливих ризиків, які мають місце в приватних мережах, пропонується розглянути альтернативний підхід та методику розгортання промислових мереж. У відповідності отриманим

теоретичним результатам дослідження розробленої методики, запропоновано впровадження приватних промислових мереж на шахті «Ювілейна», з метою створення науково обґрунтованої спеціалізованої інформаційно-промислової мережі на базі технології LTE.

Дисертація виконувалась в Державному університеті телекомунікацій.

Результати наукових досліджень доповідались на засіданнях кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації під час виконання науково-дослідних робіт на тему «Система електронного документообігу з використанням хмарних технологій» (Державний реєстраційний №0120U10315, ДУТ, м. Київ); Науково-дослідна робота «Контроль та прогнозування перевантажень в комп'ютерних мережах» (Державний реєстраційний №0120U105655, ДУТ, м. Київ). Також результати наукових досліджень прийняті до впровадження в діяльність національного оператора фіксованого зв'язку ПрАТ «Фарлеп-Інвест» ТМ Vega Telecommunications Group (акт від 17.12.2020), телекомунікаційним інтегратором ТОВ «УКРКАМ» (акт від 23.11.2020), та телекомунікаційний оператор Королівства Саудівської Аравії, що надає послуги з інформаційних технологій та безпеки «Saudi Telecom Company SJSC».

Ключові слова: поширення радіохвиль, особливі умови, електромагнітне випромінення в шахтах, мережеві технології, архітектура мережі, промислові мережі радіодоступу, розгортання мереж з наданням сервісів промислової необхідності, резервування радіодоступу приватних промислових мереж, приватні мережі LTE, захищені мережі для мануфактурінгу, доступність мережі, кібербезпека, кіберзахист.

ANOTATION

Sorokin D.V. A methodology for creating protected specialized networks, aimed at increasing the efficiency of industrial services provision. – A qualifying scientific work as a manuscript.

The thesis in candidacy for a degree of a doctor of philosophy by specialty 125 Cyber security. – The State Telecommunications University, the Ministry of Science and Education of Ukraine, Kyiv, 2021.

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.

Under the conditions of the development and introduction of advanced information technologies into the modern society functioning, particularly, governmental agencies, financial institutions, corporations and a private economy sector, heavy industry development and digitalization are becoming a priority.

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. At the same time, new challenges in terms of access, processing and storage of information at enterprises arise. Obtaining financial results, sensitive data by rivals or cyber criminals may cause enterprises' irreversible financial and reputational losses.

From the point of view of the business, enterprise information security development must be balanced in terms of investment economic pattern losses. It makes it possible to efficiently solve information security tasks, namely, confidentiality, integrity and accessibility.

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 (BlackEnergy, TeleBots, CryptoLocker, GreyEnergy, Industroyer, Petya and NotPetya, BadRabbit, Buhtrap, WannaCry, TeslaCrypt, Nyetya), 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.

In accordance with the current social challenges and possible risks, occurring in private networks, the thesis considers alternative approaches and methods of expanding and constructing private industrial networks.

Based on the approaches, it is suggested that a flexible radio access system should be expanded, to work under special radio conditions and coordinate the work of enterprise structural subsystem (M2M devices, Smart-gauges). Instead of autonomous subsystem network of telemetry and control device networks, solutions, maintaining inter-machine connection, able to monitor and standardize agent actions all over the chain of enterprise business process cooperation, are put at the forefront. Network cooperation of M2M devices will make it possible to decrease emergent operational expenditures and to increase enterprise flexibility.

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: an enterprise level; a production level; a level of machine cooperation; a telemetry and gauges level. Such models of infrastructure construction are aimed at ensuring the main industrial services for enterprises of coal, mining and heavy industries, demanding services to ensure: accounting mobile equipment and material means (usage of up-to-date ERP-systems); managing drones and machines (M2M devices cooperation); the service of operative group communication (Voice/Video/PTT); telemetry service (cooperation of smart-gaugesв); staff and equipment GPS tracking service (GPS-tracking/ Tiger-tracking); the service of access security and alarm (monitoring and perimeter security service / video surveillance); alarm and advance warning service (danger signaling / sound and light alarm); conference communication service (selector communication, video conference); data communication service.

For the purpose of developing the methodology the research analyzes the networks, based on open networks under the international standards and adjusted to demands at all automation levels, ensuring simplicity and optimality of the equipment choice. Networks capabilities and demands are also analyzed: the industrial Ethernet, as a network, functioning according to the principle of the environment access, based on the conflict (collision) detection; Modbus, as a network, cooperating with M2M devices; CAN, as a controllers' network, ensuring executive devices functioning; AS-I, as a network subsystem, ensuring the work of industrial and informational tasks.

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. Radio waves spread in a tunnel, in a mine can be reflected in a ray path theory that is more acceptable as the wave length becomes very small in comparison with the tunnel transverse diameter. The tunnel with the sides which can be compared with the wave length will ensure signal propagation due to echoing from walls, under which conditions most materials demonstrate high echo rates. As a result of a great number of echoed signals lines, radio waves spread will occur with multi-ray characteristics, with relay or Rician fading. Tunnel interference can be also caused by radio waves of frequencies, much higher than the margin one, which will mainly spread at big angles, thus, interfering with the echoing process. Following the interference, diffraction losses occur due to shading. The main reason for it is a radio attenuation coefficient while being spread in tunnels, depending mainly on discontinuity, tunnel direction changes, interference, as well as electrical peculiarities of rocks. The work considers the most common methods of defining electrical peculiarities of rocks.

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 in underground mines, it is necessary to conduct separate research with a proper list of the used equipment, or can be used in coal mines with special conditions.

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, such as: reception conditions, frequency changes, time delays and modulation type. In a similar way the signal reception can be influenced by unwanted signals from other sources that can use the same frequencies as a useful signal uses 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.

Due to the current public challenges and potential risks, available in private networks, it is suggested that an alternative approach and a methodology of industrial networks development should be considered. In accordance with the obtained theoretical results of the developed methods research, it is suggested that private industrial networks should be introduced at the Yuvileyna mine for the purpose of creating a scientifically grounded specialized information and industrial network, based on the LTE technology.

The thesis has been completed at the State Telecommunications University.

The scientific research results have been used at the department information and cyber security of the Training-scientific institute of data protection while scientific and research works were being done dedicated to the system of electronic document

circulation with cloud technologies application (state registration №0120U10315, DUT, the city of Kyiv); the scientific and research work entitled Control and Forecasting Computer Network Overloading (state registration №0120U105655, DUT, the city of Kyiv). The research outcomes have also been accepted to be implemented into the Farlep-Invest national fixed-line telephony operator activity, Vega Telecommunications Group (report as of 17.12.2020), Telecommunication integrator LLC "UKRCAM" (report as of 23.11.2020), Telecommunication operator in the Kingdom of Saudi Arabia «Saudi Telecom Company SJSC».

KEY words: radio waves spread, special conditions, electrical and magnetic emission in mines, network technologies, network architecture, radio access industrial networks, developing networks with industrial necessity services provision, reserving radio access of private industrial networks, LTE private networks, protected networks for manufacturing, network accessibility, cyber security, cyber protection.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Публікація у наукометричній базі Scopus:

1. Sorokin D. Model and Development of Plasma Technology for the Protection of Radio-electronic Means of Laser Emission / Oleksandr Turinskyi, Maksym Iasechko, Volodymyr Larin, Dmytro Dulenko, Vladislav Kravchenko, Oleksandr Golubenko, Denys Sorokin, Oksana Zolotukhina. // International Journal of Advanced Trends in Computer Science and Engineering (IJETCSE), – 2019. ISSN 2278-3091, p. 2429-2433.

Наукові праці, статті у науково-фахових виданнях України:

2. Сорокін Д.В. Приватні мережі на базі LTE в гірничо-видобувній промисловості. / Сорокін Д.В., Бондарчук А.П., Сторчак К.П., Горба Д.Б. // Науковий журнал «Телекомунікаційні та інформаційні технології». – 2019. – № 2 (63). с.29-34.

3. Сорокін Д.В. Інфраструктура промислових мереж IoT та кіберзагрози в доступі при використанні IoT рішень / Сорокін Д.В., Бондарчук А.П., Сторчак К.П. // Науковий журнал «Телекомунікаційні та інформаційні технології». – 2019. – № 4 (65). с. 120-127.

4. Сорокін Д.В. Аналіз методів організації прав користувачів у GNU\Linux системах. / Сторчак К.П., Кравець Д.В., Тушич А.М., Сорокін Д.В. // Науковий журнал «Зв'язок». – 2020. № 4. с. 38-40.

5. Сорокін Д.В. Аналіз проблем ЕМС з метою розробки ефективної моделі проектування БЛМ на базі інформаційних систем з урахуванням електромагнітних завад / А.В. Лемешко, О.М. Ткаченко, А.О. Макаренко, О.М. Ткаленко, Д.В. Сорокін // Науковий журнал «Зв'язок». – 2020. №5. – с.16-21.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Сорокін Д.В. Частные коммерческие сети LTE для умного производства и промышленности (Private LTE & Smart Manufacturing). / Сорокін Д.В. // “ITU

Workshop for Europe and CIS Regions’’ «ICT infrastructure as a basis for digital economy»: May 14-16 2019. –Kyiv, Ukraine. p. 64-65.

7. Сорокін Д.В. Розвиток приватних і комерційних мереж IoT, а також ризики пов'язані з використанням IoT (Development of private and commercial IoT & Risks of use Internet of things). / Сорокін Д.В. // IX Міжнародна науково-технічна конференція для студентства та молоді «Світ інформації та телекомунікації»: 10 жовтня 2019 р. –Київ. с. 212-214.

8. Сорокін Д.В. Нові сфери застосування сучасних інформаційних мереж. / Сеньков О.В., Сорокін Д.В., Дібрівний О.А. // Науково-практична конференція «Проблеми комп'ютерної інженерії»: 2 грудня 2020 р. –Київ. с.73-74.