ВІЙСЬКОВА АКАДЕМІЯ ЗБРОЙНИХ СИЛ АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ "ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ДП "ПІВДЕННИЙ ДЕРЖАВНИЙ ПРОЕКТНО-КОНСТРУКТОРСЬКИЙ ТА НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ АВІАЦІЙНОЇ ПРОМИСЛОВОСТІ"

УНІВЕРСИТЕТ МІСТА ЖИЛІНА

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей одинадцятої міжнародної науково-технічної конференції

8 – 9 квітня 2021 року

Том 2: секції 3 – 5

Баку – Харків – Київ – Жиліна – 2021

УДК 004/681.3

У збірнику подано тези доповідей одинадцятої міжнародної науково-технічної конференції “Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління”. Розглянуті питання за такими напрямами: теоретичні та прикладні аспекти систем прийняття рішень, оптимізації та управління системами і процесами; комп’ютерні методи і засоби інформаційно-комунікаційних технологій та управління; методи швидкої та достовірної обробки даних в комп’ютерних системах та мережах; безпека функціонування комп’ютерних систем та мереж, інформаційні технології у цивільній безпеці.

Затверджено до друку на розширеному засіданні вченої ради ДП «Харківський НДІ технології машинобудування», протокол № 3 від 24 березня 2021 року.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

СЕКЦІЯ 3

МЕТОДИ ШВИДКОЇ ТА ДОСТОВІРНОЇ ОБРОБКИ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Керівник секції: д.т.н., проф. В. А. Краснобаєв, ХНУ, Харків
Секретар секції: к.т.н., доц. І. І. Слюсар, ПДАА, Полтава

"TRUTH" SOFTWARE FOR MILITARY RECONNAISSANCE DATA DEVELOPMENT

Mammadov V.M.
Ministry of Defence of the Azerbaijan Republic, Baku
Bayramov A.A., Sabziev E.N.
Azerbaijan National Academy of Sciences Control Systems Institute, Baku

During development of obtained reconnaissance, data it should be consider a reliability of the source, data reliability, uncertainty, truthfulness, importance, and accuracy [1, 2]. With aim of automation of the reconnaissance data processing, the calculation algorithm and the "TRUTH" program have been developed and presented in given paper. The program has been prepared on PASCAL algorithmical language in Dephi package. This program solves 5 reconnaissance tasks in automatic mode.

1. Determination of a reliability of the reconnaissance source and the level of competence. Input parameters are: the sum of service durations of the reconnaissance source, established by low the common service years, the number of successful implemented reconnaissance tasks of source, the total tasks for source.

2. Determination of an uncertainty of the reconnaissance information. Input parameters are: an information uncertainty of source data, an information uncertainty of the expert comment.

3. Determination of a truthfulness of the data. Input parameters are: an information uncertainty of data, a level of the data reliability.

4. Determination of an importance of the reconnaissance. Input parameters are: a day of obtained information, a day of the report (a current day).

5. Assessment of a accuracy of the reconnaissance information. Input parameters are: a reliability of the information source, a truthfulness of the reconnaissance information.

The offered program provides an improvement of the effectiveness to use of the reconnaissant power and tools.

References

1. Bayramov A.A., Mammadov V.M. Conclusion algorithm based on the reconnaissance data processing results. *Advanced İnformation Systems*. Kharkov. 2020, vol. 4, №2. pp. 5-7.

2. Bayramov A.A., Mammadov V.M. Calculation method for determining information criteria in reconnaissance data processing. *Journal of Defense Resources Management*. Vol. 11, issue 1(20). 2020. pp.49-54.

ЛЮДИНО-МАШИННЕ ТЕХНОЛОГІЧНЕ ПРОГНОЗУВАННЯ

Слюсар В.І., Купчин А.В.
Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ, Україна

В роботі наведені основні аспекти проведення технологічного форсайту із використанням як експертних оцінок, так і штучного інтелекту.

Метою доповіді є висвітлення нового методу прийняття рішення у технологічному форсайті на основі нечіткої логіки, на вхід якої подаються оцінки за певними критеріями від системи штучного інтелекту та експертів.

Технологічний форсайт зазвичай проводиться на основі думок експертів та їх суб'єктивних оцінок [1]. Така методика є застарілою та не дозволяє проводити якісний форсайт, результати якого завжди мають певну похибку, що залежить від великої кількості впливаючих факторів.

Запропонований авторами метод форсайту базується на застосуванні системи нечіткого висновку. Вхідними змінними визначені оцінки за найбільш вагомими критеріями відбору проривних (критичних) технологій, а саме: масштаб застосування, перспективність, науково-технічний потенціал, економічна доцільність, ефективність та часовий горизонт.

Всебічна цифровізація дає можливість отримати об'єктивні оцінки за певними критеріями з Інтернету. Наприклад, перспективність технологій може бути оцінена в результаті моніторингу відкритих джерел на основі певного алгоритму та системи оцінок. Людина не в змозі опрацювати такі масиви даних, тому в цьому випадку доцільно застосування системи штучного інтелекту. В той же час за іншим критерієм, наприклад «масштаб застосування», доцільно використати досвід експертів, які більш якісно можуть оцінити повноту впровадження технології у готові продукти та їх серійне виробництво. Таким чином, оцінювання за всіма критеріями можна комбінувати між людиною та машиною. Запропонований метод поєднує у собі швидкість та об'єктивність штучного інтелекту з досвідом найбільш фахових спеціалістів. Для України такий підхід є досить новим, проте, людино-машинні системи вже є звичайною практикою для країн НАТО [2].

Побудова на цій основі нейронної мережі для повної автономізації процесу прийняття рішення є перспективою подальших досліджень.

Список літератури

1. Romanowski M., Nadolny K. Technological Foresight – characterisation of research methods used in prospective analysis. *Journal of Mechanical and Energy Engineering*. 2018. № 2. С. 101-108. DOI: 10.30464/jmee.2018.2.2.101.

2. Slyusar V.I. Artificial intelligence as the basis of future control networks. // Coordination problems of military technical and devensive industrial policy in Ukraine. Weapons and military equipment development perspectives/ VII International Scientific and Practical Conference. Abstracts of reports. - October 8–10, 2019. Kyiv. Pp. 76-77. – DOI: 10.13140/RG.2.2.30247.50087.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

Дегтярьова Л.М., Слюсарь І.І.
Полтавська державна аграрна академія, м. Полтава, Україна
Курчанов В.М.
Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут, Полтава, Україна

З розвитком інформаційних технологій, кіберзагрози стають більш складними та цілеспрямованими і потребують адекватних рішень щодо захисту IT-інфраструктури [1]. Зважаючи на зростання кількості інформації, що зберігається, використання гібридних хмарних варіантів інфраструктури стає нормою. Але контролювати та підтримувати в безпеці розподілений характер середовища стає складніше, і захищеність даних і цілісність безпеки корпоративної мережі стали основним завданням для системних адміністраторів. Як наслідок, використання класичних засобів і заходів захисту не завжди протидіють відповідним загрозам. **Метою доповіді** є формування підходу щодо забезпечення контролю над виникаючими потенційними ризиками шляхом додавання до інструментарію брандмауера додаткового функціоналу на основі штучного інтелекту (ШІ) [2].

В доповіді наводяться варіант реалізації технології «sandbox», з можливістю інтелектуального аналізу поведінки програм без використання безпосередньо мережного середовища підприємства (організації) на основі тимчасової безпечної ізоляції та подальшого вивчення потенційної загрози для хмарного середовища. Спираючись на надійні джерела і перелік найбільш актуальних загроз, брандмауер, забезпечений засобами ШІ, можна оптимізувати для посилення можливостей блокування шкідливих програм і перевірки всіх URL, які можуть бути використані працівниками підприємства (організації) і є потенційними носіями шкідливих програмами і ботнетів. В цілому, брандмауер на основі може адаптуватися до обставин і вчитися на вразливості.

Таким чином, ШІ здатен впоратись з відомими і невідомими кіберзагрозами, гарантувати ефективну роботу мережі, додаючи рівень самонавчання до процесу управління брандмауером та моніторингу процесу мережевих з'єднань.

Список літератури

1. Слюсарь І.І., Слюсар В.І., Дегтярьова Л.М., Курчанов В.М. Інструментарій віддаленого доступу до ресурсів інформаційних управляючих систем. Проблеми інформатизації: тези доп. 8-ої міжнародної науково-технічної конференції (Черкаси – Харків – Баку – Бельсько-Бяла, 26-27 лис. 2020 р.). Черкаси, 2020. Т. 3. С. 43.

2. Курпьюн Т. Защита сетей малого и среднего бизнеса с помощью искусственного интеллекта. URL: https://www.anti-malware.ru/analytics/Technology_ Analysis/artificial-intelligence-part-in-network-security.

КІЛЬКІСНА ОЦІНКА ВТОРИННИХ ДЕФЕКТІВ ПРОГРАМНИХ ЗАСОБІВ НА ОСНОВІ АПРОКСИМАЦІЇ ТРЕНДА ДЕФЕКТІВ ПОЛІНОМОМ ДРУГОГО СТЕПЕНЯ

Руденко О.А.
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна
Руденко З.М.
Полтавський коледж нафти і газу Національного університету «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

Однією з найсуттєвіших проблем при оцінюванні надійності програмних засобів є оцінка кількості вторинних дефектів.

Метою доповіді є аналіз одержання коефіцієнтів многочлена другого степеня, що описує скориговану лінію апроксимації трендів дефектів.

Одним з напрямків досліджень кількісної оцінки вторинних дефектів є порівняння тренда дефектів зі зміщеною лінією апроксимації [1]. В [2] показано алгоритм оцінювання кількості вторинних дефектів, в якому використовується скоригована лінія експоненціальної апроксимації тренда дефектів.

На основі аналізу функцій ризику моделей оцінки надійності програмних засобів зроблено висновок щодо необхідності використання поліноміальної другого степеня апроксимації тренда дефектів. Одержані коефіцієнти рівняння зміщеної лінії апроксимації $n = a_1 t^2 + b_1 t + c_1$.

$$a_1 = a\left(1 - \sigma / \left(a t_1^2 + b t_1 + c\right)\right); \quad (1)$$

$$b_1 = \sigma\left(a / \left(a t_1^2 + b t_1 + c\right) - 1 / \left(t_k - t_1\right)\right); \quad (2)$$

$$c_1 = c + \sigma\left(a t_1 t_k / \left(a t_1^2 + b t_1 + c\right) - t_1 / \left(t_k - t_1\right) - 1\right), \quad (3)$$

де a, b, c – коефіцієнти рівняння лінії апроксимації, t_1, t_k – час, що відповідає кінцю першого і останнього інтервалу часу відповідно; σ – середнє квадратичне відхилення числа виявлених дефектів.

Список літератури

1. Rudenko O., Odarushchenko E., Rudenko Z., Rudenko M., "The Secondary Software Faults Number Evaluation Based on Correction of the Experimental Data Exponential Line Approximation", Conference Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies DESSERT'2018, Kyiv, 2018, pp. 401-405.

2. Руденко О.А. Знаходження параметрів скоригованої лінії експоненціальної апроксимації експериментальних даних виявлених дефектів при оцінюванні кількості вторинних дефектів програмних засобів / О.А. Руденко, З.М. Руденко, Г.В. Головко, О.Б. Одарущенко // Системи управління, навігації та зв'язку. – Полтава : ПолтНТУ, 2018. – Вип. 6 (52). – С. 74-78.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА З ВИКОРИСТАННЯМ УНІФІКОВАНИХ КОМУНІКАЦІЙ

Слюсарь І.І., Городянин А.В., Пілюгін В.А.
Полтавська державна аграрна академія, м. Полтава, Україна
Курчанов В.М.
Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут, Полтава, Україна

Як відомо, одним з елементів сучасних корпоративних інформаційних систем (КІС), в тому числі, закладу вищої освіти (ЗВО), являється система управління взаємовідносинами з клієнтами (Customer Relationship Management, CRM).

Метою доповіді є аналіз особливостей застосування уніфікованих комунікацій (Unified Communications, UC) в інтересах забезпечення повноцінного функціонування CRM.

В доповіді запропонований варіант використання IP-АТС 3CX в якості інструментарію для впровадження UC [1]. При створенні корпоративної мережі VoIP ЗВО, яка може використовуватись в навчальному процесі, основна увага приділялась диверсифікації комунікацій [2]. Для цього організовувались транки з зовнішніми VoIP-провайдерами, наприклад: Sipnet. Він має вихід на стаціонарні телефонні мережі та системи національних операторів мобільного зв'язку, а також безкоштовну підтримку внутрішніх абонентів, що є досить привабливим для навчального процесу. Також, до IP-АТС 3CX було підключено кілька різнопланових за функціоналом VoIP- і GSM-шлюзів, що дозволило реалізувати комунікації не тільки з Укртелекомом, але і кількома відомчими АТС. При цьому, для визначення особливостей підключення віддалених абонентів використовувався прикордонний контролер сесій (Session Border Controller, SBC) на мікрокомп'ютери Raspberry PI. В інтересах мінімізації витрат інтеграція CRM і UC організовувалась на базі Bitrix24. Такий підхід обґрунтований наявністю готових програмних рішень у вигляді API. Таким чином, спільне використання IP-АТС 3CX і Bitrix24 дозволяє здійснювати всю номенклатуру сучасного спектру операцій з клієнтами в рамках використання CRM. Подальші дослідження спрямовані на реалізацію функції Call Tracking.

Список літератури

1. Городянин А.В., Слюсарь І.І. Інструментарій для впровадження уніфікованих комунікацій. Матеріали XVII щорічного міждисциплінарного семінару «Студентські роботи за науковою тематикою кафедри інформаційних систем та технологій» (Полтава, 26 лис. 2020 р.). Полтава: ПДАУ, 2020 р. С. 9-11.

2. Городянин А.В., Слюсарь І.І. Організація віддаленого доступу в корпоративних інформаційних системах // Матеріали щорічної студентської наукової конференції Полтавської державної аграрної академії (Полтава, 17 лис. 2020 р.). Полтава: ПП «АСТРАЯ», 2020. С. 15-17.

ПРІОРИТЕТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АГРАРНОМУ СЕКТОРІ

Слюсарь І.І., Уткін Ю.В., Копішинська О.П., Дегтярьова Л.М.
Полтавська державна аграрна академія
Полтава, Україна
Слюсар В.І.
Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ, Україна

Метою доповіді є формування пріоритетних напрямів використання штучного інтелекту (ШІ) [1] в аграрному секторі. Вони ґрунтуються на вже існуючих прототипах та/або аналогах, що використовуються для реалізації концепції «Індустрія 4.0», інтелектуальних систем та технологій, в тому числі на основі IoT і Big Data. **В доповіді** зазначені напрями умовно розділені за рівнями, що пов’язані з існуючими підходами до класифікації інформаційних систем. Перший рівень пов'язаний з прогнозуванням [2]: урожайності за визначеними культурами в рослинництві; ціни на визначену продукцію; ціни на землю з урахуванням агрохімічного паспорту; ціни на паливо, а також створення систем підтримки прийняття рішення. Другий рівень пов'язаний з плануванням: оптимальних графіків, маршрутів використання техніки, логістичних операцій, складської логістики, карт сівозмін, а також з ідентифікацію проблемних ділянок полів, ґрунтів, водних об’єктів. Застосування на цьому рівні може використовуватись для скорочення витрат і підвищення ефективності розведення продукції тваринництва. Ці моделі використовуються для оптимізації годівлі, підтримки чистоти і здоров'я тварин, а також допомоги фірмам (компаніям) в прийнятті максимально ефективних рішень при господарських операціях. За аналогією, застосування для скорочення витрат і підвищення ефективності продукції рослинництва, наприклад, підрахунок сходів і біологічної урожайності. Третій рівень забезпечує керування: розумною фермою, теплицею або іншим замкнутим технологічним процесом; безпілотними, безекіпажними платформами (системами); системами збору продукції; складської логістики. Четвертий рівень реалізує оперативний контроль: якості виконання посівних робіт, обробки ґрунту, якості роботи сільськогосподарської техніки, а також контроль використання ресурсів і класифікацію культур.

Список літератури

1. Slyusar V.I. Artificial intelligence as the basis of future control networks. //Coordination problems of military technical and devensive industrial policy in Ukraine. Weapons and military equipment development perspectives/ VII International Scientific and Practical Conference. Abstracts of reports. – October 8-10, 2019. Kyiv. Pp. 76-77.

2. Дослідження та аналітика. URL: https://drone.ua/poslugi-dlya-silskogo-gospodarstva/doslidzhennya-i-analitika/?lang=uk.

ROUTING TABLES UPDATE ALGORITHM IN SEMANTIC INFORMATION CENTRIC NETWORKING

Patsei N.V., Jaber G., Navrotsky Y.Y.
Belarussian State Technological University, Minsk, Belarus

In [1] was presented the system of naming and addressing object and message routing in Semantic Information Centric Networking (SICN). Data/content caching plays an important role in this SICN project.

The goal of report is consideration the algorithm for updating information in routing tables. Routers hold three tables where the three address dimensions' combined in them: Semantic-ID (connects semantic address to publisher ID address), Geo-ID (connects publisher ID address and geographical), Geo-Semantic (matches semantic address to geographical). Each table includes two parts. The first part, which is the address part (publisher ID, geographical and semantic addresses) that names the data and are learnt or defined from publisher advertisement. The second part of each table, which is the orientation part (TTL and Interface) that directs the data toward the subscriber. The interface are the input output ports, which connects network nodes. Hops number shows the cost to reach data in terms of number of hops. If a subscriber sends Interest Request Message (IRM) and it reaches the router, the router will search its tables for an entry match. There are three cases:

Case 1: If there is no positive match between IRM and any addressing table in the router, the router will broadcast the IRM to the network from all its interfaces in a spanning tree technique to avoid loops. The Content Reply Message (CRM) will allow updating all the routing tables across the requested paths towards the subscriber who sent the IRM for the first time. Thus, when there are no previous records in the tables, it will be created with a default TTL.

Case2: If positive naming matches occurs between IRM and routing table and the router already caches the content, TTL will be updated in the routing table. Then the Address Reply Message (ARM) will be send to the subscriber with the three addresses dimensions without the content to allow the subscriber to choose.

Case3: If positive naming matches occurs between IRM and routing table but the content is not cached locally in the router, the router will forward the message toward the nearest publisher which could be a relay cache or the original publisher. The latest will send the reply message with its three addressing dimensions.

In all cases, the interfaces in the tables will be learnt from the interface that passed the reply message.

References

1. Jaber G, Patsei N., Rahal F., Abboud A. Naming and Routing Scheme for Data Content Objects in Information-Centric Network // 2020 Open Conference of Electrical, Electronic and Information Sciences (eStream): Proceedings of the Conference: April 30, 2020, Vilnius, Lithuania. IEEE-2020. P.93-97. DOI: 10.1109/eStream50540.2020.9108879.

ОПТИМІЗАЦІЯ РОЗПОДІЛУ ПОТУЖНОСТЕЙ ІНФОРМАЦІЙНИХ КАНАЛІВ НА ОСНОВІ АЛГОРИТМУ ОРЛІНА

Івохін Є.В., Аджубей Л.Т.
Київський національний університет імені Тараса Шевченка, Україна
Гавриленко В.В., Сілантьєва Ю.О.
Національний транспортний університет, Київ, Україна

Розв'язування практичних задач транспортного типу, що відносяться до класу цілочисельних оптимізаційних задач, представляє особливий інтерес. Це пов'язано з тим, що на основі багатоіндексних транспортних моделей розроблено та запропоновано ряд методів для вирішення проблем розподілу та планування інформаційних потоків. При цьому, одним з перспективних підходів для вирішення таких задач є потокові методи [1].

Метою доповіді є побудова математичної моделі процесу розподілу обмежених потужностей каналів передачі даних між різними вузлами мережі Інтернет, що дозволить розв'язати задачу ефективного збільшення сумарної пропускної здатності каналів зв'язку користувачів шляхом зміни потужності комунікаційних серверів з урахуванням побажань абонентів та можливостей технічних засобів комутації. Для проведення обчислювального експерименту сформульовано постановку та розв'язано задачу оптимізації пропускної здатності мережевих каналів зв'язку в схемі «провайдер – комунікаційний сервер - користувач» [2] за наявності обмежень на обсяги споживання.

В доповіді наводяться результати застосування алгоритму оптимального розподілу потужностей каналів передачі даних на основі потокового алгоритму Орліна [3], який дозволяє звести задачу транспортного типу до потокової задачі, пропонуючи ефективну обчислювальну схему. Отримано результати пропускних спроможностей каналів реальної комп'ютерної мережі при перспективному збільшенні потужностей з'єднань, які представлені інтервалами допустимих змін. Проведено аналіз розв'язків, отриманих для різних потужностей комунікаційних серверів, зроблені висновки про оптимальний вибір рішення для забезпечення потреб користувачів. Отримані результати показують, що запропонований алгоритм є ефективним методом вирішення задачі розподілу, що знайшло повне підтвердження в результаті проведення практичних кроків реорганізації серверного парку реальної установи.

Список літератури

1. Прилуцкий М.Х., Афраймович Л.Г. Распределение ресурсов в иерархических системах транспортного типа. Новые подходы в исследованиях информационно-телекоммуникационных систем и технологий. Нижний Новгород, 2007. 80 с.

2. Pentico D.W. Assignment problems: A golden anniversary survey. *European Journal of Operational Research*. 2007. V.176. P.774-793.

3. Orlin J.B. A Faster strongly polynomial minimum cost flow algorithm. *European Journal of Operational Research*. 1993. V. 41. N2. P.338-350.

ОПТИМІЗАЦІЯ МІЖПЛАНЕТНИХ ТРАЄКТОРІЙ КОСМІЧНИХ АПАРАТІВ З КОМБІНУВАННЯМ ВЕЛИКОЇ ТА МАЛОЇ ТЯГИ

Харитонова Л.В., Щербаков А.С., Кабиш Н.О.
Національний транспортний університет, Київ, Україна

Метою доповіді є аналіз проблеми розробки перспективних космічних апаратів, здатних забезпечити доставку великих вантажів з низької навколоземної орбіти на геостаціонарну, а також – на орбіти супутників планет Сонячної системи і Місяця – однієї з найбільш важливих задач сучасної космонавики [1]. Ефективне виконання міжпланетних експедицій вимагає впровадження новітніх типів рушійних систем та проведення відповідних досліджень оптимальних перельотів космічних апаратів (КА) з такими рушійними системами.

В доповіді розглядається задача про максимізацію корисного навантаження при виконанні перельоту Земля-Марс за заданий час. Для опису руху КА застосовується метод сфер впливу [2].

Загальна задача розглядається як задача сукупної оптимізації програм керування, параметрів граничних умов та масових параметрів підсистем великої та малої тяги і є задачею оптимального керування для динамічної системи, рух якої відбувається у трьох фазових просторах. Внаслідок застосування аналітичного розв'язку задачі оптимізації руху на геліоцентричній ділянці, отриманого за допомогою модифікованого методу транспортуючої траєкторії А.А. Суханова [3], кількість фазових просторів вдається зменшити до двох – пов'язаних із виконанням планетоцентричних маневрів. Дослідження оптимального керування проведено за допомогою принципу максимуму Понтрягіна. Задача оптимального керування для динамічної системи зі зміною фазового простору [4] зведена до модифікованої задачі для динамічної системи з об'єднаним фазовим простором. Побудовані програми оптимального керування, виведені умови трансверсальності та умови стрибка.

Список література

1. Howe S. Recent Activities at the CSNR for Developing Nuclear Thermal Rockets // 61st International Astronautical Congress, Prague, Czech Republic, September 27-October 1, 2010. Proceedings, Paper IAC-10-C4.7 –C3.5.2.

2. Kharytonov O.M., Kiforenko B.M. Finite-thrust optimization of interplanetary transfers of space vehicle with bimodal nuclear thermal propulsion // Acta Astronautica, 69 (2011), pp. 223-233.

3. Суханов А.А., де А. Прадо А.Ф.Б. Модификация метода транспортирующей траектории // Космич. исследования. 2004, Т. 42, №1. С. 107-112.

4. Асланян А.А. Принцип максимума для разрывных динамических систем // Теория функций, функциональный анализ и их приложения: Респ. междувед. науч. сб. / Харьковский государственный университет им. А.М. Горького. – Вып. 37. – Х.: Вища школа. Изд-во при Харьк. ун-те, 1982. С. 132-137.

ОПТИМІЗАЦІЯ І МОДЕЛЮВАННЯ ПРОЦЕСУ ПРОКАТКИ СТАЛІ НА ПЛАСТИЛІНОВИХ МОДЕЛЯХ

Харитонова Л.В.
Національний транспортний університет, Київ, Україна
Сердітов О.Т., Ключников Ю.В., Артюх М.Ю.
Національний технічний університет України
«КПІ імені Ігоря Сікорського», Київ, Україна

Вивченню процесу деформування пластиліну для моделювання прокатки присвячений ряд робіт [1-4]. В них головна увага приділена розгляду пошуку шляхів отримання подібності механізму опору деформування пластиліну і сталі в залежності від величини деформацій, швидкості деформації і температури сталі і пластиліну. Отримані залежності не дозволяють провести моделювання і оптимізацію подібності формо змінення сталі і пластиліну.

Метою доповіді є пошук оптимальних показників, що впливають на подібність формозміни сталі і пластиліну при моделюванні прокатки.

В роботі приведені результати експерименту, у якому оптимізована кількісна міра відповідності формо змінення пластиліну і сталі. В якості характеристики формо змінення обрана величина розширення при прокатуванні в гладеньких циліндричних валках. При моделюванні і оптимізації процесів обробки металів тиском необхідно враховувати те, що пластилін більш чутливий до зміни стану контактних поверхонь деформуючого інструменту. Показано, що значна величина розширення пластиліну не дозволяє отримати кількісні залежності для процесів прокатки, пов'язаних з послідовним деформуванням всіх бічних сторін розкату, наприклад прокатки металу на блюмінгах, слябінгах і заготівельних станах. Розкид властивостей пластиліну різних партій або заводів-виробників пояснюється коливаннями властивостей сировини, порушеннями технології приготування матеріалу і тому не може бути повністю врахований аналітично. Разом з тим, вплив коливань складу пластиліну на його формозміни невеликий [4].

Список література

1. Сугамото Т. Исследование пластилина применительно к температурным характеристикам стали. Тэтцу-то-хагане, 1977, Т. 63, вып. 1, С. 208.

2. Грановский Ю.В. Планирование эксперимента при поиске оптимальных условий. М.: Наука, 1970. 283 с.

3. Журавлев Д.Ф. Моделирование процессов получения деформированных заготовок. Журнал. Проблемы и перспективы студенческой науки, Новокузнецк, 2019, №1 (5), С. 29-32.

4. Романцев Б.А. Чан Ба Хюси. Исследование процессов винтовой прокатки в четырехвалковой клети методом моделирования. Металлург, №7, 2018. С. 21-29.

РОЗВИТОК СУЧАСНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Котетунов В.Ю.
Національний транспортний університет, Київ, Україна

В сучасному світі більш відома і популярна операційна система Windows 10. Але сьогодні існує велика кількість альтернативних операційних систем з аналогічним інтерфейсом і більшою стабільністю в роботі.

Метою доповіді є розгляд існуючих альтернативних операційній системі Windows 10, які мають аналогічний інтерфейс і забезпечують більшу стабільність в роботі.

В доповіді наводяться основні переваги операційних систем і переваги над Windows 10.

Головним конкурентом операційній систем Windows 10 знаходиться остання версія Linux Mint. Основиною перевагою є те що операційна система є повністю безкоштовною і має хорошу технічну підтримку. плюси: швидкий запуск, взаємодіє навіть з найпростішим залізом, зрозумій інтерфейс [1, 2].

Наступною альтернативою є Ubuntu універсальна розробка на движку Debian GNU і Linux. Основними перевагами є: забезпечує легку і просту роботу, постійна підтримка користувачів, безпеку високого рівня, безкоштовне програмне забезпечення, операційна система безкоштовна.

MacOS продукт іменитої американської компанії Apple. Плюси:просте управління, надійність і безпека, швидка і стабільна в роботі. Основним мінусом є те що працює тільки з певними видами процесорів.

Chrome OS продукт компанії Google. Головною відмінністю цієї ОС вважається гібридне ядро. Основні плюси: ключове місце відводиться браузеру Chrome, системні вимоги низькі, вбудована програма захисту активно справляється з усіма загрозами, надсилаючи безпечні системні модулі, простота у використанні, за допомогою Google Play. Основним мінусом:підключення до мережі Інтернет.

FreeBSD операційна система, яка раніше використовувалась тільки на серверах, проте на поточний день вона адаптована і для використання звичайних комп'ютерах. Основними плюсами є: хороша оптимізація і продуктивне споживання ресурсів.

В доповіді розкриті основні переваги операційних системи і переваги над Windows 10. Наведені основні альтернативи операційній системі Windows 10.

Список літератури

1. Батаев, А.В. Операционные системы и среды: Учебник / А.В. Батаев, Н.Ю. Налютин, С.В. Синицын и др. – М.: Academia, 2018. 271 с.

2. Дроздов, С.Н. Операционные системы: Учебное пособие / С.Н. Дроздов. – Рн/Д: Феникс, 2018. 480 с.

МОДЕЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ВИМОГ ДО ДИСЦИПЛІНИ «ЗАХИСТ УКРАЇНИ» ПРИ ЗАСТОСУВАННІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Воронянський В.С., Вшивцев О.С.
Полтавський коледж нафти і газу Національного університету «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

Важливою умовою успішності занять з дисципліни «Захист України» є висока організованість та відповідальність здобувачів [1]. На заняттях стосунки між ними і викладачем, а також студентів між собою підтримуються на зразок стосунків між військовослужбовцями, викладач відіграє роль командира підрозділу і повинен власним прикладом демонструвати високий рівень дисципліни та організованості. Розклад пар, посилання на відеоконференції та інші необхідні дані повинні бути доступними для студентів (можуть бути розміщеними на сайті закладу освіти, платформах дистанційного навчання, в групах соціальних мереж, тощо). Високі вимоги до організованості та дисципліни під час занять вимагають своєчасного оповіщення про заплановані розкладом пари, про зміни в розкладі, тощо.

В умовах адаптивного карантину, проведення дистанційного навчання з предмету «Захист України» передбачає використання інформаційно-комунікаційних технологій. Поширеною практикою є використання засобів відеоконференцзв'язку Zoom, Google Meet, Microsoft Teams [2], інформаційних середовищ Moodle, Google Classroom, групових засобів сповіщення через електронну пошту, соціальні мережі, групові месенджери.

Метою доповіді є побудова моделей та дослідження типових ситуацій, що вимагають оповіщення групи студентів. **В доповіді** наводяться результати оцінки резервів часу результативного оповіщення груп здобувачів. Застарілим, але донині використовуваним способом є оповіщення студента по телефону (максимальний час сповіщення до 5 годин). У багатьох навчальних закладах розгорнуті системи корпоративної пошти, які використовуються для групового розсилання електронних листів, таке оповіщення для студентських груп має середню ефективність (до 30 хв.).

Найпоширенішим на даний час ефективним способом сповіщення є групова розсилка повідомлень через популярні месенджери (Viber, Telegram, WhatsApp, Facebook), що вимагає попереднього створення та адміністрування груп, при цьому витрати часу мінімальні (час набору повідомлення та його перегляду усіма учасниками групи, до 10 хвилин).

Список літератури

1. Використання інформаційно-комунікативних технологій на уроках предмету «Захист Вітчизни». URL: https://urok.osvita.ua/materials/edu_technology/7509/

2. Дистанційне навчання: виклики, результати та перспективи. Порадник. З досвіду роботи освітян міста Києва: навч.-метод. посіб. / Упоряд.: Воротникова І. П,. Чайковська Н. В. Київ. ун-т ім. Б. Грінченка, 2020. 456 с.

АНАЛІЗ МОЖЛИВОСТЕЙ ТЕКСТОВИХ ПРОЦЕСОРІВ

Воронянський В.С., Коновалов А.І.
Полтавський коледж нафти і газу Національного університету
«Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

Ефективне використання можливостей сучасних інформаційних технологій здобувачами повинно бути підкріплене відповідною звітною документацією, яка розробляється та модифікується за допомогою програмних додатків – текстових процесорів. **Метою доповіді** є дослідження можливостей популярних текстових процесорів та їх аналогів, що мають модель вільного доступу. **В доповіді** наводяться результати порівняння додатків Microsoft Word [1], Libre Office [2], Open Office [3], Text Maker [4], Google Docs [5].

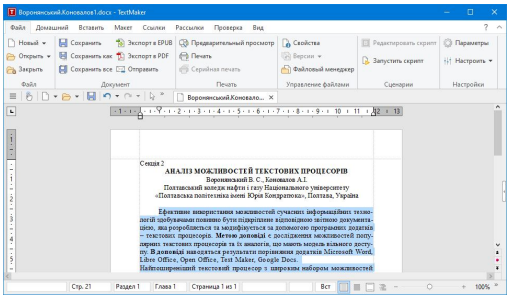

Рис.1. Інтерфейс текстового процесора Text Maker

Найпоширеніший текстовий процесор з широким набором можливостей та зручним інтерфейсом це, безумовно, Microsoft Word. На даний час використовують як десктопну, так і хмарну версію [1] цього додатка з гнучкою системою підписки. Проте додаток Word залишається платним і не має можливості портативної інсталяції (важливо для десктопної версії). З іншого боку, додаток Google Docs має лише хмарну версію, що не дозволяє використовувати його на ПК без підключення до мережі Інтернет. Для додатків Libre Office, Open Office, Text Maker наявні портативні версії, які не вимагають інсталяції. Це досить привабливі додатки для навчальних варіантів використання, оскільки вони мають безкоштовні варіанти ліцензій та інтерфейс, що копіює/повторює стрічки та кнопки Word.

Список літератури

1. Microsoft Word – програмне забезпечення для роботи з текстом. URL: https://www.microsoft.com/uk-ua/microsoft-365/word.
2. The Document Foundation. URL: https://www.documentfoundation.org
3. The Free and Open Productivity Suite. URL: https://www.openoffice.org
4. FreeOffice TextMaker. URL: https://www.freeoffice.com/en/freeoffice-textmaker
5. Google Документи. Матеріал з Вікіпедії. URL: https://uk.wikipedia.org/wiki/Google_Документи.

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ТРАНСПОРТНИХ СИСТЕМАХ

Комісаренко О.С., Баранов Г.Л.
Національний транспортний університет, Київ, Україна
Зайцев Є.О.
Інститут електродинаміки НАН України, Київ, Україна
Черницька І.О.
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

Інформаційні технології мають значний вплив на розвиток будь-якої сфери людської діяльності. Такого впливу найбільше зазнають області в яких є необхідним автоматизація процесів прийняття рішень. У цьому разі не виключенням є і транспортна галузь, в якій надзвичайно розвинуто використання сучасних інформаційних технологій для управління, прогнозування, моделювання властивостей матеріалів для транспортної галузі та тощо. Тому, **метою доповіді** є розгляд застосування сучасних інформаційних технологій для підвищення якості процесів створення перспективних матеріалів для транспортної галузі та реалізації автоматизації управління процесами взаємодії складових транспортних систем реалізованих на базі інформаційних технологгій. **В доповіді** наводяться результати аналізу стану методів моделювання та засобів автоматизації ергатичного управління процесами комунікаційної взаємодії складових ІТ. Перспективи сталого розвитку інтелектуальних транспортних систем (ITS) поки ще формують умови гетерогенної інтеграції у світову транспортну мережу з трансконтинентальними сполученнями всіх провідних держав, включаючи потенціал України. Великомасштабна інтеграція у майбутнє передбачає принципи синергетики для подолання негативних тенденцій на початку XXI століття.

Список літератури

1. Komisarenko O., Baranov G. Development of infological modeling methods in social communication problems for creation perspective completed materials // New stages of development of modern science in Ukraine and EU countries. – Riga,"Baltija Publ.", 2019. P. 37-57.

2. Комісаренко О.С., Баранов Г.Л., Чака О.Г. Інфологічне моделювання технологій створення матеріалів для футорологічних конструкцій та систем // Метрологія та прилади. Харків. 2018. №6 (74). С. 53-58.

THE QUEUING THEORY AS A TOOL OF THE DYNAMIC ANALYSIS OF THE STATE DEFENSE FORCES GROUP LOGISTICS SUPPORT SYSTEM

Makogon H., Korda M., Vasyliev O.
Military Institute of Tank Troops of National Technical University, Kharkiv

The development of logistics forces and the entry of capabilities to ensure the actions of troops (forces) in conducting interspecies, interdepartmental joint

operations is one of the priorities for the development of the state defense forces [1, 2]. The **goal** of the study is the finding out a logistics support model that allows to obtain quantitative estimates of the required number of weapons ensured a given level of combat readiness and support the serviceability of troops, as well as optimal management of procurement, repair and modernization of weapons over time. The **report** deals with the logistics support of the state defense forces group presented as a queuing model, the parameters of which are determined by statistical data from the troops. Based on the obtained solution of the corresponding of differential equations system, an analysis of the logistics support system of the state defense forces group for a certain period of time can be made [3, 4]. The dynamic analysis of the logistics support system will form the basis of the recommendation for the implementation of promising guidelines of equipping state defense forces weapons and military equipment and optimizing the management of the system according to the certain criteria [5].

References

1. Romanenko, Y. O. (2016), "Reforming the Armed Forces of Ukraine according to NATO standards", [Online], *Publichne uryaduvannya*, vol. №3 (4) available at: https://cyberleninka.ru/article/n/reformirovanie-vooruzhennyh-sil-ukrainy-po-standartam-nato.

2. Simchi-Levi, D., Chen, X., and Bramel, J. (2004), The Logic of Logistics: Theory, Algorithms, and Applications for Logistics and Supply Chain Management. New York: Springer, USA.

3.Buravlev, A.I. and Pyankov, A.A. (2010), "Troops technical support model", *Elektronnyy nauchnyy zhurnal "Vooruzheniye i ekonomika",* vol. 1(10), pp.4-10.

4. Buravlev, A.I. and Pyankov, A.A (2011) "Troops technical support management model", *Elektronnyy* nauchnyy zhurnal "Vooruzheniye i ekonomika", vol. №4(6), pp.29-34.

5. Taha, Hamdy, A. (2005) *Vvedeniye v issledovaniye operatsiy* [Operations Research An Introduction], Translated by Min'ko, A., Vil'yams, Moscow, RU.

АНАЛІЗ МОЖЛИВОСТІ ВИКОРИСТАННЯ АКУМУЛЯТОРНИХ БАТАРЕЙ, ЩО НЕ ОБСЛУГОВУЮТЬСЯ, НА ЗРАЗКАХ БРОНЕТАНКОВОГО ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

Андрєєв В.О., Чорнобай В.М.
Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна

В даний час в якості джерел живлення у вітчизняній військовій колісній та гусеничній техніці в основному використовуються акумуляторні свинцево-кислотні стартерні батареї типу 12СТ-85Р та 6СТЕН-140М, які за своїм технологічним виконанням відносяться до класу таких, що обслуговуються. У той же час поява в галузі виробництва акумуляторних батарей (АБ) новітніх технологій дозволяє значно підвищити ресурс АБ та розширити можливість їх застосування [1]. Гелевий електроліт (GEL) дозволяє досягти повної герметичності батареї, оскільки газоутворення відбувається всередині системи пор в масі геля. В батареях, виготовлені за AGM- технологією,

міститься адсорбований електроліт. У даній роботі приведено обґрунтування використання на зразках бронетанкового озброєння та військової техніки новітніх АБ на основі дослідження їх конструктивних, електричних, експлуатаційних параметрів та енергетичних можливостей.

Шляхом статистичної обробки даних у середовищі MATLAB отримані графіки залежності "стартерних" режимів розряду АБ 12СТ-85Р, 6СТЭН-140М та XTREME 670901105, їх саморозряду у часі та сумарної ємності встановлених в машині АБ при різних значеннях навколишнього середовища [2]. Показано, що AGM- батареї мають нижчий внутрішній опір в порівнянні з АБ інших типів, здатні видавати більш високі струми за короткий час. Дослідження енергетичні можливостей АБ різних пипів дозволили зробити висновок про переваги гелевих та AGM батарей перед свинцево-кислотними при збереженні на однаковому рівні масо-габаритных характеристик.

Список літератури

1. Перспективы использования аккумуляторных батарей в военной гусеничной и колесной технике / А. И. Бондарь [и др.] // Интегрированные технологии и энергосбережение. – 2013. – № 3. – С. 7-14.

2. Lynch, S. Dynamical Systems with Applications using MATLAB / Stephen Lynch. – Springer International Publishing, 2014. – 514 p.

МОДЕЛЮВАННЯ КАБЕЛЬ-ТРОСА В ЗАВДАННІ БУКСИРУВАННЯ КОЛІСНО-ГУСЕНІЧНИХ МАШИН МЕТОДОМ ЗОСЕРЕДЖЕНИХ ПАРАМЕТРІВ

Ісаков О.В., Омельчук О.В., Лисенко В.О.
Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна

Створення тренажерів маневрування та управління рухом колісно-гусеничних машин (КГМ), а так само створення дослідно-налагоджувальних стендів систем автоматичного керування рухом машини, вимагає наявності математичних моделей. Однією з важливих математичних моделей, необхідних для таких тренажерів і стендів є модель тросів або кабель-тросів, що зв'язують машину з буксиром. Математична модель зв'язку (роса або кабель-троса) описується рівнянням в приватних похідних, що робить цю задачу складнішою. Реалізація таких моделей обмежена кінцевою продуктивністю програмного та апаратного забезпечення, що використовуються в тренажерах і стендах [1, 2]. У **доповіді** розглянуто задачу розробки математичної моделі кабель-троса в завданні буксирування БМП-2 для використання в тренажерах і стендах. Авторами пропонується розглядати трос як складний нелінійний об'єкт та прийняти припущення, що трос і будь-який його сегмент підкоряється закону Гука. Крім того, можна знехтувати розподіленими по довжині троса крутними моментами, які виникають при дії на трос сили розтягування. Ці припущення дозволяють спростити рівняння і використовувати метод зосереджених

параметрів [3]. Для розв'язання задачі використовуються силові граничні умови. В обраному методі моделювання постановка граничних умов зводиться до завдання закону руху першому і останньому N+1 –му вузлу, на які умовно розбитий трос. Запропонована математична модель руху забезпечує моделювання всіх основних режимів буксирування КГМ в реальному режимі часу в складі стендів систем автоматичного керування рухом машини. За перспективний напрямок дослідження розглядається використання синтетикних волокон, що забезпечить зменшення їх ваги тросів.

Список літератури

1. W.Raman-Nair, R. E. Baddour, Three-dimensional coupled dynamics of a buoy and multiple mooring lines: formulation and algorithm, Oxford University Press, 2002.

2. Юдин, Ю. И. Расчет усилий, действующих на объекты буксировки со стороны буксирной связи / Ю. И. Юдин, С. В. Пашенцев, В. В. Каян // Вестник Мурманского государственного технического университета. - 2013. - Т. 16, № 1. - С. 193-196

3. Соловейчик Ю.Г., Рояк М.Э. и др. Метод конечных элементов для решения скалярных и векторных задач. Новосибирск: Изд-во НГТУ, 2007. 896 с.

АЛГОРИТМ ВЕКТОРИЗАЦІЇ РАСТРОВИХ ЗОБРАЖЕНЬ ДЛЯ СТВОРЕННЯ ІНФОГРАФІКИ ОСВІТНЬОГО ПРОЦЕСУ

Базелюк В.М., Святий І.Р.
Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна

З кожним роком зростає потреба в знаходженні ефективних засобів навчання, які допоможуть підвищити представлення навчального матеріалу, зацікавити курсантів (студентів), підвищити їх мотивацію до вивчення предмета, стимулювати розумову діяльність і розвивати творчий потенціал. Так, методично потужним засобом навчання можна вважати інфографіку, оскільки плакати формують уміння самостійно працювати з джерелами інформації, дають змогу курсанту можливість знайти правильну відповідь, поглибити знання. Актуальність дослідження обумовлена необхідністю поєднання графічних об'єктів, різних за своєю природою.

Доповідь присвячена процесам автоматизації обробки растрових зображень з метою перетворення їх у векторний формат. Авторами наведено короткий опис завдання векторизації. Виділяються наступні етапи роботи алгоритму: завантаження і ініціалізація; підрахунок використовуваних унікальних квітів і формування таблиці кольорів; виділення контурів областей на растрі; виділення крайніх точок областей на растрі; формування масивів з точок, хаотично розташованих на зображенні (по при знаку приналежності точок з однаковим кольором масиву точок цього кольору); формування векторної моделі (на основі контурів всіх областей, отриманих при використанні алгоритму обходу контуру); растеризація векторної моделі (зорова перевірка на відповідність векторної моделі растрової) [1, 2].

Алгоритм векторизації представлений в загальній рекомендаційної формі. Це пояснюється тим, що розглянута задача виявляється завжди дуже специфічною при її вирішенні. Запропоновано загальну конструкція завдань, вирішення яких необхідне в більшості випадків попередньої обробки матеріалів при створенні інфографіки для освітнього процесу

Список літератури

1. Скворцов А.В. Применение триангуляции для решения задач вычислительной геометрии / А.В. Скворцов, Ю.Л. Костюк // Геоинформатика. Теория и практика. Вып. 1. – Томск: Изд-во Том. гос. ун-та, 1998. – С. 22–47.

2. Сташевский С.Ю. Алгоритм векторизации растровых изображений в общем виде / Автоматизированные системы обработки информации, управления и проектирования // Доклад Томского государственного университета систем управления и радиоэлектроники. Томск – 2004. □ 7 с.

ВІЗУАЛІЗАЦІЯ РЕЗУЛЬТАТІВ КОНТРОЛЮ РІВНЯ ГАЛЬМІВНОЇ РІДИНИ В ГОЛОВНИХ ЦИЛІНДРАХ ГАЛЬМІВНОЇ СИСТЕМИ ЗРАЗКІВ КОЛІСНОЇ ТА ГУСЕНИЧНОЇ ТЕХНІКИ

Калінін І.В., Балаш Я.В.
Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна

Точний контроль рівня гальмівної рідини в головних циліндрах гальмівної системи є невід'ємною складового в системі щоденного технічного обслуговування зразків колісної та гусеничної техніки [1,2].

Доповідь присвячено дослідженню можливості автоматизації та постійного контролю рівня гальмівної рідини в головних циліндрах гальмівної системи машини без доступу до них. На прикладі БТР-80 для перевірки рівня гальмівної рідини в головних циліндрах гальмівної системи машини авторами пропонується застосовувати ємнісний датчик, який безперервно і дистанційно відображає інформацію про кількість гальмівної рідини на панелі приладів машини. Кнопка вмикання і рідкокристалічний кольоровий дисплей на панелі приладів. Передбачається, що інформація про зміну ємності з вимірювача направляється в мікропроцесор, який остаточно обробляє інформацію від датчика, при необхідності формує сигнал для аналогового виходу і забезпечує підтримку протоколу зв'язку через цифровий інтерфейс. Крім того, датчик електрично з'єднують з рідкокристалічним кольоровим дисплеєм рівня, при цьому загоряється синя нижня смуга показує необхідність доливання гальмівної рідини.

Автоматизація контролю рівня гальмівної рідини в головних циліндрах гальмівної системи БТР-80 з візуалізацією результатів дозволить підвищити точність його проведення, скоротити час і трудовитрати щоденного технічного обслуговування та увеличить ресурс роботи механізмів гальмівної системи машини.

Список літератури

1. Пархоменко А.В., Гумелёв В.Ю., Пестов О.В. Боевые и специальные машины. Технические описания и инструкции по эксплуатации // Электронная база данных / Часть 1.1. Бронетранспортер БТР-80 // Портал научно-практических публикаций [Электронный ресурс]. URL: http://portalnp.ru/2014/06/1938
2. Гумелёв В.Ю., Пархоменко А.В., Постников А.А., Андрющенко А.А. Краткие сведения о порядке проведения и операциях контрольного осмотра бронетранспортера БТР-80 // Современная техника и технологии. 2016. № 5.

РОЗРАХУНОК ВИТРАТ ЕКСПЛУАТАЦІЙНОГО РЕСУРСУ КОЛІСНИХ ГУСЕНІЧНИХ МАШИН ЗАСОБАМИ КОРЕЛЯЦІЙНОГО АНАЛІЗУ

Ковальов І.О., Пасько Б.В.
Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна

Сучасні колісні гусеничні машини являють собою складні системи, є сукупністю сумісно діючих елементів – вузлів, механізмів, з'єднань та агрегатів, які забезпечують виконання ним завдань за призначенням. Справність і готовність машини до використання за призначенням забезпечуються її технікними станом. З урахуванням індивідуальних властивостей конкретної машини, умов її експлуатації, характеру графіка навантаження та інших факторів темп зносу як окремих вузлів так і підсистем машини може значно відрізнятися від показників, визначених для машини-аналога [1, 2]. **Метою доповіді** є розробка пропозиції уніфікації методики розрахунків витрати експлуатаційного ресурсу колісних гусеничних машин та шляхи її технічної реалізації. В доповіді наводяться результати аналізу міжремонтного ресурсу танка Т-64Б та окремих вузлів, механізмів, з'єднань та агрегатів машини, на основі якого визначено простір ознак для розрахунку витрат експлуатаційного ресурсу колісних гусеничних машин в залежності від умов виконання ними завдань за призначенням. Авторами запропонована методика побудови рівняння регресії, що описує залежність експлуатаційного ресурсу машини від значень витрат експлуатаційного ресурсу її окремих складальних одиниць та систем. У доповіді запропоновані конструктивні рішення щодо більш ретельного визначення витрат експлуатаційного ресурсу двигуна машини [3].

Список літератури

1. Волох Олександр Петрович. Методика обґрунтування раціональних значень параметрів технічного обслуговування машин інженерного озброєння при їх використанні за призначенням : дис... канд. техн. наук: 20.02.14 / Військовий інженерний ін-т Подільського ДАТУ. Кам'янець-Подільський, 2007. 182 с.
2. Демиденко Е.З. Линейная и нелинейная регрессия. – М.: Финансы и статистика, 1981. – 302 с.
3. Раскин Л. Г. Анализ сложных систем и элементы теории оптимального управления. – Москва: Сов. радио, 1976. –344 с.

ОПТИМАЛЬНЕ ПОЗИЦІОНУВАННЯ СИЛ І ЗАСОБІВ ЛОГІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ТА ЇХ РАЦІОНАЛЬНЕ РОЗМІЩЕННЯ ВІДНОСНО ПІДРОЗДІЛІВ СИЛ ОБОРОНИ ДЕРЖАВИ В ЗАЛЕЖНОСТІ ВІД ЗМІНИ ТАКТИЧНОЇ ОБСТАНОВКИ ЯК ЗАДАЧА ЛІНІЙНОГО ПРОГРАМУВАННЯ

Ковальов І.О., Яжло Р.С., Баканов К.Л., Заверуха Г.В., Василенко Д.В.
Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна

Розробка нових математичних моделей надасть змогу забезпечити комплексний аналіз основних сил і засобів логістичного забезпечення (ЛЗ) та підвищити ефективність планування оснащення підрозділів сил оборони держави (СОД) засобами матеріально-технічного забезпечення (МТЗ) в залежності від зміни тактичної обстановки [1.2].

У доповіді надане формулювання оптимального позиціонування сил і засобів ЛЗ та їх раціональне розміщення відносно військових підрозділів в залежності від зміни тактичної обстановки як задача лінійного програмування. Для розв'язання цієї задачі запропонований формалізований аналіз позиціонування сил і засобів ЛЗ військових підрозділів СОД при виконанні ними завдань за призначенням [3,4].

На основі дослідження математичної моделі зроблені пропозиції щодо пошуку оптимальних управлінських рішень в залежності від зміни тактичної обстановки. В подальшому пропонується розглянути можливість візуалізації інформації у графічному режимі. Наприклад, доцільно інтерактивне відображення районів розташування підрозділів МТЗ, місця збірного пункту пошкоджених машин, шляхи маневру, підвозу та евакуації пошкоджених зразків озброєння та техніки, тощо.

Список літератури

1. Романенко Євген Олександрович. Реформирование вооруженных сил Украины по стандартам НАТО // Публічне урядування. □ 2016. □ №3 (4). □ Режим доступу: https://cyberleninka.ru/article/n/reformirovanie-vooruzhennyh-sil-ukrainy-po-standartam-nato

2. Simchi-Levi D. The Logic of Logistics: Theory, Algorithms, and Applications for Logistics and Supply Chain Management / D. Simchi-Levi, X. Chen, J. Bramel. – [2nd ed.]. – New York : Springer, 2004. – 375 p.

3. Акулич И.Л. Математическое программирование в примерах и задачах: Учебное пособие для студентов экономических специальностей. □М.: Высш. шк., 1986. □319 с.

4. Хемди А. Таха. Введение в исследование операций. □ М: Издательский дом «Вильямс», 2005. □912 с.

A HETEROGENEOUS QUEUING NETWORK AS A SIMULATION TOOLSL FOR INVESTIGATION AN UNRELIABLE WIRELESS SENSOR NETWORK MOT

Kramchaninov A.
Ivan Kozhedub Kharkiv National University of the Air Force, Kharkiv
Makogon H.
Military Institute of Tank Troops of National Technical University, Kharkiv
Ptakhina I.
Kharkiv Petro Vasylenko National Technical University of Agriculture, Kharkiv

Today, wireless sensor networks (WSN) have defined a new class of distributed communication systems, the use of which in the military sphere is appropriate for determining the location of mobile targets, the territorial spread of chemical weapons, and so on**.** The configuration of the wireless sensor network should be flexible and change depending on the current position in space and power supply capabilities. Sensory nodes usually function in an unfriendly environment. Due to the discharge of power supplies, the buffer overflow of lost packets may cause network mots to shut down. Thus, it becomes problematic to predict the behavior of the network under different operating modes and make an estimate of the number of losses, which is necessary to understand the accuracy and reliability of calculations that take place in the process of collecting data by mot sensors and countering threats and attacks [1, 2]. The report deals with the question of study the WNS characteristics, analysis of their properties and development of methods for evaluating the basic characteristics and determining ways to improve the reliability of the functioning of the nodes. It was defined the main characteristics of the sensor network mot as a Queuing network. They are: the mathematical expectation (ME) of the S_1 systems requirements number; ME of the S_2 systems requirements number; service network response time; ME of the requirements stay time in the S_1 system; ME of the requirements stay time in the S_2 system; ME of the lost packages number. The obtained results allow us to understand and study the processes occurring in wireless queuing networks and to predict network operation in a hostile environment. The ability to estimate the number of packets lost gives you an understanding of the reliability of network mots [3].

References

1. Sergiyevskiy, M. “Wireless Sensor Networks”, [Online], available at: http://www.compress.ru/Article.aspx?id=17950.

2. Karl, H and Willig, A (2005). *Protocols and Architectures for Wireless Sensor Networks*. John Wiley & Sons, Ltd., Hoboken, US.

3. Lozhkovs□kyy, A.H. (2010), *Teoriya masovoho obsluhovuvannya v telekomunikatsiyakh* [Queuing theory in telecommunications], Odes□ka natsional□na akademiya zv□yazku, Odesa, UA.

THE DEVELOPMENT OF SOFTWARE AND HARDWARE OF BATTERY-POWERED TRACKERS FOR BATTERY CARE AND BATTERY MANAGEMENT

Makogon H., Suchko R., Slavutskiy I., Kukhta A.
Military Institute of Tank Troops of National Technical University, Kharkiv

During operation the battery may have such faults as suffixation of the plates, accelerated self-discharge, short circuit, electrolyte leakage, oxidation of the pole pins, which usually lead to deterioration of its electrical characteristics.

Express-diagnosis allows to reduce these shortcomings to the minimum [1,2].

The **goal** of the study is to develop a methodology for assessing the lead-acid batteries' parameters and to provide recommendations for their long-term management and carrier.

The **report** presents the analysis of practical operation of the lead-acid batteries, determines a set of diagnostic parameters, which can be used to draw a conclusion about the technical state of a battery and change of its electric, operational and design properties.

Statistical data processing using the mathematical apparatus of correlation analysis allows to determine the causes and dependencies between the battery's parameters, and make their assessment based on the established criteria.

Generalized results presented in the form of a correlation galaxy makes it possible to build a diagnostic graph-model of battery in the form of a correlation galaxy [3].A promising direction in the development of battery operation is the development of *Battery Tracks* - software and hardware for battery maintenance (control) and its management [4]. By monitoring such generalized diagnostic parameters of the lead-acid battery as *State of Health and the State of Charge* using such a device the user obtains continuous and accurate reporting of the remaining charge, and cautions the state when a battery needs to be replaced.

References

1. Lead-acid batteries: The growing need for monitoring state-of-charge and health [On-line] // Electronic Products. Cambridge, MA – URL: https://www.electronicproducts.com/lead-acid-batteries-the-growing-need-for-monitoring-state-of-charge-and-health/

2. Aleshkin A. A. (ed.) (2013), "Method of on-line diagnostics of the available capacity of lead-acid accumulators (batteries)", *Elektrokhimicheskaya energetika,* № 1, pp.46–53.

3. Grzhibovsky A.M. (2008) [On-line],"Correlation analysis", *Ekologiya cheloveka,* № 9. URL: https://cyberleninka.ru/article/n/korrelyatsionnyy-analiz.

4. Simon Wen. Impedance TrackTM Gas Gauge for Novice, Application Report (SLUA375), [On-line]: Texas Instruments, Jan 2006: http://www.ti.com/lit/an/slua375/slua375.pdf.

DIAGNOSING DATA IN A NON-POSITIONAL NUMBER SYSTEM OF RESIDUAL CLASSES

Krasnobayev V., Koshman S., Kovalchuk D.
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

A foundation of some modern specialized informational and telecommunication systems is based on computer systems (CS) of handling of integer data, represented in non-positional notation in residue classes (SRC). In this case, one of the main ways of achieving high effectiveness of functioning of telecommunication systems while handling integer data in real-time is an improvement, firstly, such features of CS in SRC as reliability and performance of data handling. The largest effectiveness of SRC usage can be achieved in case if implemented algorithms consist of a set of such arithmetical operations as addition, multiplication, and subtraction [1, 2]. On the other hand, a necessity of providing fault-tolerant functioning of CS in SRC requires the development and deployment of methods of quick control, diagnostic, and data error correction, which are different from methods, used in regular binary positional notations (PN) [3].

The purpose of the report is the development of the method of quick diagnostic of data in SRC while entering minimal informational redundancy.

The report proposed a method allows decreasing the time of diagnostic of errors of data, represented in SRC, which increases diagnostic operability. A reduction of the quantity of bases in AS increases informativeness AS about error placement and measure. It decreases the time of AS reduction to incorrect bases. The usage of the suggested method of operative diagnostic of data increases the total effectiveness and feasibility of using non-positional code structures in SRC in computing systems. Therefore, the suggested method allows reducing the time of diagnosis of data errors in NCS, represented in SRC, which is increasing the diagnostic operability while entering minimal informational redundancy. Geometrical model of the procedure of AS informativeness increasing and specific example of usage of the suggested method of diagnostic of data in SRC confirms its practical feasibility. The most effective way of the method usage is in the computational chain, which does not allow perform all planned procedures to AS reduction to the incorrect basis, i.e. in a quite long chain of calculations of CS.

References

1. Krasnobayev V. A. and Koshman S. A. A method for operational diagnosis of data represented in a residue number system. *Cybernetics and Systems Analysis*. March 2018. – Volume 54, Issue 2, pp. 336-344. DOI: https://doi.org/10.1007/s10559-018-0035-y

2. Krasnobayev V. A., Yanko A. S. and Koshman S. A. A Method for arithmetic comparison of data represented in a residue number of system. *Cybernetics and Systems Analysis*. January 2016. Volume 52, Issue 1, pp. 145-150. DOI: https://doi.org/10.1007/s10559-016-9809-2

DEVELOPMENT OF THE ADDER STRUCTURE BY MODULO OF THE SYSTEM OF RESIDUAL CLASSES

Krasnobayev V., Koshman S., Kovalchuk D.
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

The operation of adding two numbers is one of the main operations that is implemented by a computer system (CS) both in the positional binary number system (PNS) and in the non-positional system of residual classes (SRC) [1]. The adder of two numbers is the main part of the CS arithmetic unit in the PNS. In SRC, the modular addition operation is implemented based on the use of low-bit binary adders modulo. One of the ways to implement the modular addition operation is based on the use of structures of positional binary adders [2]. This approach provides a wide range of options for implementing the structure of such adders. This allows you to make full use of the available practical experience in the design and selection of binary adder structures.

The purpose of the report is to develop an algorithm for synthesizing the structure of the adder of two residuals of numbers by an arbitrary value of the SRC module, by organizing inter-bit connections between the binary digits of the adder, the combination of which determines the structure of the adder modulo.

The paper considers the results of the synthesis of binary adders for an arbitrary SRC modulus. The adder synthesis algorithm is based on the use of existing positional adders, which are widely used in CS operating in PNS. The paper directly presents an algorithm for synthesizing an adder by an arbitrary SRC module. The algorithm is implemented by introducing and using additional interdigit connections. Rules for the introduction of these additional connections are formulated. It is shown that the use of additional links (based on the structure of a positional adder) allows you to create an adder that implements the operation of adding two remainders of numbers presented in the SRC. A set of k modulo adders is an adder of two numbers in the SRC. Specific examples of the synthesis of adders with arbitrary modules for various values of the SRC modules are given. The research results can be useful in the design of high-speed and reliable digital computing devices in the SRC, which is especially important with the existing element base using FPGA.

References

1. V. A. Krasnobayev, A. A. Kuznetsov, S. A. Koshman, and K. O. Kuznetsova. A method for implementing the operation of modulo addition of the residues of two numbers in the residue number system. *Cybernetics and Systems Analysis*. Vol. 56, No. 6, November, 2020, 1029-1038. https://doi.org/10.1007/s10559-020-00323-9.

2. Krasnobayev V. A. and Koshman S. A. Method for implementing the arithmetic operation of addition in residue number system based on the use of the principle of circular shift. *Cybernetics and Systems Analysis*. July, 2019. Volume 55, Issue 4, pp. 692-698.

IMPLEMENTATION OF SPECIALIZED COMPUTERS IN THE RESIDUE NUMBER SYSTEMS ON THE BASIS OF FPGA

Koshman S., ShalashovR.
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

Today, one of the promising platforms for the implementation of high-speed specialized computer components are Field-Programmable Gate Array (FPGA). It is known that FPGA is a chip, the logic of which is not determined by its creation, but is set by programming in specialized software packages. With the FPGA, data processing algorithms are effectively implemented in such areas as digital signal processing, control and measurement equipment, construction of specialized accelerators, cryptography, machine learning and more. Modern FPGAs are characterized by low cost, high speed, significant functionality, multiple reprogramming, low power consumption and so on [1].

The purpose of the report there is a formation and research of architecture of specialized spreadsheets in the residue number systems (RNS), which are built on the basis of FPGA.

The report presents the results of research on the using of non-positional number system in residual classes during the formation of specialized computers. The paper shows that the using of RNS allows to accelerate the execution of arithmetic operations such as addition, subtraction and multiplication, and increase the productivity of information processing in real time [2]. The architecture of the computer in the RNS is a set of computing tracts that works in parallel and independently of each other. This feature of RNS is based on the next properties: independence, equality and low-digit residues. It is due to the property of low-digit residues in RNS are developed tabular methods for implementing arithmetic operations [3]. Thus the tabular structures are quite effectively realized on the basis of FPGA, thanks to the internal organization of logical elements. The results of the research showed that the feasibility of implementing RNS in the construction of high-performance computers that can be used as arithmetic extenders in the construction of computer systems [4].

References

1. Грушвицкий Р.И., Мурсаев А.Х., Угрюмов Е.П. Проектирование систем на микросхемах программированной логики. СПб.: БХВ-Петербург, 2002. – 608 с.

2. Акушский И. Я., Юдицкий Д. И. Машинная арифметики в остаточных классах. Москва: Радио и связь, 1968. 444 с.

3. Koshman S. A., Barsov V. I., Krasnobayev V. A., Yaskova K. V., Derenko N. S. Method of bit-by-bit tabular realization of arithmetic operations in the system of residual classes. *Радіоелектронні і комп'ютерні системи.* 2009. № 5 (39). С. 44-48.

4. Koshman S., Krasnobayev V., Kuznetsov A., Rassomakhin S., Zamula A., Kavun S. Effective Data Processing in Coding, Digital Signals and Cryptography: monograph. ASC Academic Publishing, 2018, 352 p

РОЗРОБКА СИСТЕМИ ДЛЯ ПРОВЕДЕННЯ ЗМАГАНЬ З ПРОГРАМУВАННЯ НА БАЗІ МІКРОСЕРВІСІВ ТА КОНТЕЙНЕРИЗАЦІЇ

Малєєва О.В., Палагно А.Д.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

З розвитком програмного забезпечення і Інтернету взагалі, все більше і більше рутинна праця заміщається скриптами, або іншим програмним забезпеченням, що сприяє створенню нових програмних продуктів. Адже, скрипти не можуть покрити абсолютно усі можливі варіанти використання додатку. Тому і виникла необхідність автоматизувати, надати гнучкості та зробити результат виконання скриптів зрозумілим для користувачів, які можуть навіть не замислюватися, що і як працює.

Такими користувачами можуть бути, як люди не знайомі з мовами програмування, так і досвідчені розробники програмного забезпечення. Наприклад, викладач хоче автоматизувати перевірку лабораторних робіт, або проведення змагань з програмування, або розробник хоче автоматизувати процес збірки модулів у мікросервісному проекті [1].

Існує безліч сервісів, що допомагають з автоматизацією, але їх дуже важко доповнювати. Іншими словами, необхідно витратити багато часу, щоб кастоматизувати поточний продукт.

Для вирішення вказаних проблем розроблено інструмент, який дозволяє будувати додаток або код у спеціально виділеному середовищі, враховуючи особливості додатку, або у випадку коду, - мову програмування [2]. Протестовано використання даної системи у змаганнях з програмування.

Проведено аналіз швидкості виконання додатків або коду, зроблено порівняння з можливими частковими аналогами. Отримані дані свідчать, що швидкість та автономність системи дозволяє її використовувати у різних умовах та середовищах. В зв'язку з цим чинності набувають можливість масштабування системи для використання її у розподілених системах із значною кількістю користувачів, що є однієї із головних переваг.

Список літератури

1. Newman, S. Building Microservices [Текст] / S. Newman. – New York: O`Riley, 2017.

2. Kleppmann, M. Designing Data-Intensive Application [Текст] / M. Kleppmann. – New York: O`Riley, 2015.

РОЗРОБКА MIDDLEWARE ДЛЯ МІГРАЦІЇ ДОДАТКІВ МІЖ СИСТЕМАМИ УПРАВЛІННЯ БАЗ ДАНИХ

Момот М.О., Губарєв Є.С.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Необхідність внесення змін у базу даних, з якою працює додаток, існувала вже давно, але зараз вона набуває піку своєї актуальності. Наразі умови на ринку СКБД змінюються дуже швидко. Щоб продавати користувачам найякісніший та найдешевший сервіс, треба швидко реагувати на ці зміни – використовувати найбільш актуальну для поточних задач, швидку, надійну та дешеву СКБД. У більшості випадків процес рефакторингу [1] та міграції здійснюється вручну. При цьому залучається велика команда розробників та спеціалістів з БД, які обробляють код вручну до того моменту, поки повністю не відновлять весь функціонал та не усунуть усі помилки, пов'язані зі зміною типу БД. Цей процес займає багато часу та потребує багато коштів. Також під час цього процесу має місце людський фактор та пов'язані з цим залишкові помилки. Існує декілька сервісів, які реалізують функціонал міграції коду додатків. Проте ці сервіси у своїй більшості налаштовані на міграцію до хмарних середовищ великих компаній. Також вони підтримують обмежений функціонал з міграції.

Метою доповіді є дослідження можливості автоматизованої міграції коду додатків на різних мовах програмування між різними СКБД.

В доповіді наводяться результати аналізу існуючих програм або сервісів з міграції додатків між СКБД. Виявлені їх основні переваги і недоліки. Як платформу конвертації обрано AWS Database Migration Service. На основі проведеного аналізу було сформовано основні вимоги до програми, яка створюється, розроблено основні алгоритми роботи програми для міграції, сплановано архітектуру та структуру програми, яка розробляється. На першому етапі програма забезпечує міграцію коду з СКБД Oracle до PostgreSQL [2], реалізована підтримка таких мов програмування для міграції як Java, Groovy та C. Створена післяміграційна підтримка для виправлення помилок. Middleware має два варіанти інтерфейсу:

1) інтерфейс користувача з компонентами для взаємодії, створений з використанням технології JavaFX;

2) взаємодія з додатком за допомогою консольних команд (CLI), який прискорює швидкість взаємодії та підтримує скрипти (списки команд).

Список літератури

1. Эмблер С. В. Рефакторинг баз данных: эволюционное проектирование [Текст] / С. Эмблер, П. Садаладж ; пер. с англ. К. А. Птицына. – М. : Вильямс, 2007. – 672 с

2. Shameel Ahmed. Migrating your SQL Server Workloads to PostgreSQL [Text]. Independently Published, 2020. – 104 p.

ЕФЕКТИВНІСТЬ СТИСНЕННЯ ЗОБРАЖЕНЬ В ЗАЛЕЖНОСТІ ВІД ПОПЕРЕДНЬОЇ ОБРОБКИ

Щербакова Ю.А., Скіцка М.В.
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Зберігання і передача інформації завжди потребують максимальної ефективності. З цією метою застосовується стиснення даних, що в залежності від процесу поділяють на стиск з втратами якості і стиснення без втрат. За умов застосування попередньої обробки у графічних редакторах цей процес можна удосконалити. Було проведено дослідження впливу обробки фотографій у графічних редакторах Adobe Photoshop і GIMP на якість та коефіцієнт стиснення зображень за використанням алгоритмів JPEG та JPEG 2000.

Ефективність стиску зазвичай вимірюється, використовуючи метрики, такі як піковий сигнал / шум (PSNR), коефіцієнт корисної середньої квадрату (RMSE) та інші [1, 2]. В рамках роботи було розроблено програмний продукт, який стискає зображення та вимірює метрики. Проаналізовано можливість отримання максимально зменшеного розміру зображення, в тому числі за допомогою різних метрик перевірено втрати якості при стисканні. Отримано коефіцієнти стиску зображення та метрики втрат якості при використанні різних методів попередньої обробки (зміна контрастності, насиченості, яскравості, вібрації, то що) [3]. Дослідження проводилось на цифрових зображеннях різної якості.

За результатами проведених експериментів було розроблено рекомендації що до комплексного використання Adobe Photoshop або GIMP та JPEG (JPEG 2000). Враховуючи отримані результати можна обрати той, чи інший метод обробки, який відповідає потребам – покращує коефіцієнт стисненого зображення чи робить майже непомітними втрати якості. Порівняння JPEG та JPEG2000 [4] довело, що на побутовому рівні JPEG є більш зручним, бо якість при компресії близько 20 разів суттєвої різниці не має, а обробка файлів JPEG 2000 складніша та вимагає додаткової обчислювальної потужності. Але JPEG 2000 є необхідним на професійному рівні за потреб отримання високоякісних результатів по якості та ступеню стиснення.

Список літератури

1. Миано, Дж. Форматы и алгоритмы сжатия изображений в действии. М. : Издательство Триумф, 2003.-336 с.

2. Методы сжатия данных: Сжатие изображений. Режим доступа : http://www.compression.ru/book/part2/part2__3.htm

3. Нечепоренко О. В., Миценко С. А. Системный анализ и оценка методов сжатия данных для баз данных лазерных технологических комплексов. – Вісник Хмельницького національного університету, №1, 2014. С. 94-99.

4. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии. – М. : Триумф, 2003.

MULTISPECTRAL IMAGES PROCESSING USING SYSTEMS ON CHIPS

Podorozhniak A., Kvochka M.
National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine

Nowadays, thanks to the rapid development of aerospace research programs, the use of multispectral images has become widespread and has found practical application in many areas, such as weather forecasting, environmental monitoring (monitoring state of water, soils, forests, etc.) and even military activities. In the vast majority of cases, the analysis of multispectral images by visual method is almost impossible, so the data obtained from observations must be classified using various algorithms and methods of machine learning [1, 2]. The training of an artificial intelligence model regardless the chosen methods usually requires significant power consumption, hardware costs and computing power, but the actual use of the resulting model can be considered on more budget computers, even such as systems on chips [3].

The purpose of the report is to research and develop a model of a system for multispectral images processing using an integrated circuit also known as a system on chip (SoC). The developed model has practical application in the field of burned areas monitoring and detection [4].

The report presents the results of the study of technical and economic feasibility of using systems on chips in the multispectral image processing field, as well as a general analysis and comparison of the proposed system architecture with other common analogues. Aspects such as energy efficiency of using different types of systems, the possibility of autonomous operation, as well as the integration of data analysis systems with global networks are compared. Analysis results of investigated problem show that due to the fact that modern systems on the chip are available to the end user and provide opportunities such as data multiprocessing and connection of peripherals, they are suitable for deployment of functional models of multispectral data processing.

References

1. Schowengerdt R. A. Remote sensing: Models and methods for image processing, Academic Press, 3rd ed., 2007, 560 p.

2. Yaloveha V., Hlavcheva D., Podorozhniak A. Usage of convolutional neural network for multispectral image processing applied to the problem of detecting fire hazardous forest areas. *Advanced Information Systems*. 2019. Vol. 3, № 1, pp. 116–120. DOI: https://doi.org/10.20998/2522-9052.2019.1.19

3. Myrgard M. R. Acceleration of deep convolutional neural networks on multiprocessor system-on-chip. Master's thesis. Uppsala University, Uppsala, 2019, 48 p. URL: http://uu.diva-portal.org/smash/get/diva2:1326323/FULLTEXT01.pdf.

4. Moore P., Hardesty J., Kelleher S., Maginnis S. and Myers R. Forests and wildfires: fixing the future by avoiding the past, XII World Forestry Congress, Quebec, Canada, 2003. URL: http://www.fao.org/3/xii/0829-b3.htm.

ДОСЛІДЖЕННЯ МЕТОДІВ ОБРОБКИ ЗОБРАЖЕНЬ

Рундін Я.В., Бульба С.С.
Національний технічний університет «ХПІ», Харків, Україна

Збільшення обчислювальної потужності комп'ютерних систем призвело до можливості покращення якості зображення інформації що відображається на екранах. Сучасний користувач вже не уявляє свою роботу з цифровими технологіями без графічного інтерфейсу. А отже виникає необхідність в використанні та розробці методів роботи, що дають змогу отримати ефективні результати обробки зображень [1, 2].

Метою доповіді є огляд існуючих методів обробки зображень. В доповіді розглядаються сучасні методи обробки зображень. Сьогодні існують різні ін.-струменти та методи обробки зображень в комп'ютерних системах. Існує велика кількість напрямків обробки зображень, до них відносяться: локально-адаптивна обробка зображень; фільтрація зображень; розширення меж зображень; реконструкція розмитих зображень; зміна межі зображень; оптимізація палітри зображень; кодування і стиснення зображень; покращення зображень з викривленими характеристиками яскравості; підвищення візуальної якості зображень; виявлення обличь на основі кольору. Кожен з розглянутих методів має як негативні так і позитивні сторони, а отже необхідно чітко розуміти для яких цілей та в яких сферах буде використовуватися обраний метод.

Список літератури

1. Shumeiko A. Discrete trigonometric transform and its usage in digital image processing / A.Shumeiko, V.Smorodskyi // EIQJ .— 2017 .— №4(6) .— C.21-26..

2. Gerald C. Holst Electro-Optical Imaging Sytems Perfomance. - Winter Park, Florida USA, SPIE Optical Engineering Press, 2001 – 445 p.

ПЕРЕВАГИ ТА НЕДОЛІКИ НЕРЕЛЯЦІЙНИХ БАЗ ДАНИХ

Сатаров Р.Б., Баленко О.І.
Національний технічний університет «ХПІ», Харків, Україна

Збільшення різноманітності створених програмних продуктів та систем призводить до необхідності різних способів зберігання даних та інструментів взаємодії з ними. Основним інструментом для цього є реляційні бази даних на основі SQL, але їх можливостей було недостатньо для необхідних задач. Тому були створені NoSQL-бази даних, які використовують інші підходи до вирішення проблем [1-3]. NoSQL - база даних, яка забезпечує механізм зберігання та видобування даних відмінний від підходу таблиць-відношень в реляційних базах даних. **Метою дослідження** є розгляд різниці між реляційними та нереляційними базами даних. Аналіз позитивних та негативних факторів використання NoSQL-баз даних. До позитивних факторів відносяться: можливість збереження великих об'ємів неструктурованої інформації; NoSQL-бази краще піддаються масштабуванню; не вимагають великого обсягу підготовчих дій, що потрібен для реляцій-

них баз; власні мови запитів сучасних NoSQL сховищ набагато більше підходять для виконання простих маніпуляцій з базою даних; висока продуктивність при виконанні простих запитів. Негативними факторами використання нереляційних баз даних є: додаток сильно прив'язується до конкретної СУБД. Мова SQL універсальна для всіх реляційних сховищ, і тому в разі зміни СУБД не доведеться переписувати весь код; процес створення реляційного сховища включає в себе етап проектування моделі даних. На цій стадії можна оцінити вузькі місця обраної стратегії і спроектувати дійсно надійну і зручну систему. NoSQL рішення не вимагають визначати схему бази даних перед початком роботи, тому в процесі розробки можна наштовхнутися на непередбачені труднощі, які можуть привести до відмови від даного NoSQL рішення.

Список літератури

1. Сильные и слабые стороны NoSQL [Електронний ресурс] - Режим доступу: https://habr.com/ru/sandbox/113232/
2. SQL против NoSQL на примере MySQL и MongoDB [Електронний ресурс] - Режим доступу: https://tproger.ru/translations/sql-vs-nosql/
3. ОГЛЯД НЕРЕЛЯЦІЙНИХ БАЗ ДАНИХ [Електронний ресурс] / Шаров С. В., Петровський В. В. - Режим доступу: https://rb.gy/hdpecq

ВИДІЛЕННЯ ОБ'ЄКТІВ НА ЗОБРАЖЕННЯХ МІКРОБІОЛОГІЧНИХ ДОСЛІДЖЕНЬ МЕТОДАМИ ВИДІЛЕННЯ КОНТУРІВ

Янковський О.А., Чиркіна О.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Одним із завдань комп'ютерної обробки зображень є відокремлення об'єктів інтересу. У багатьох випадках ця процедура пов'язана з побудовою контуру об'єкта. Незважаючи на те, що в літературі досить гарно розглянуті базові алгоритми виділення контурів об'єктів [1, 2], задача виділення контуру, об'єкта, його меж, вимагає особливого підходу для кожного конкретного випадку. Для кожного прикладу необхідно підібрати відповідний алгоритм видалення фону на зображенні, виділити його межі, в деяких випадках доводиться усувати розриви на межах об'єктів, викликаних, наприклад, поганою якістю знімка. Це важливо для вивчення таких параметрів об'єкта інтересу як його колір, форма, орієнтація і т.п. **Метою доповіді** є аналіз найбільш поширених алгоритмів виділення контурів об'єктів і застосування їх до знімків, отриманих за допомогою електронного мікроскопа. У Доповіді наведені зображення і приклади результатів застосування до них розглянутих алгоритмів, а також алгоритмів виділення меж об'єктів, побудови кістяка об'єкта. Отримані результати можуть використовуватися, наприклад для методів імунної гістохімії при пошуку і оцінки кількості різних речовини, об'єктів з патологією в різних тканинах організму. Також розглянуті приклади побудови границь об'єктів на знімках, отриманих за допомогою аерофотозйомки, що важливо для розпізнавання обїєктів, їх аналізу. Обробка зображень виконувалася за допомогою програмного пакету MATLAB.

Список літератури

1. Р. Гонсалес, Р. Вудс. Цифровая обработка изображений. СПб.: Питер, 2005. 1071 с.
2. В.Т. Фисенко, Т.Ю. Фисенко. Компьютерная обработка и распознавание изображений: учебное пособие. –СПб.: СПбГУ ИТМО, 2008. -192 с.
3. П.И. Рудаков, И.В, Сафонов. Обработка сигналов и изображений. MATLAB 5x. М.: ДИАЛОГ-МИФИ, 2000. – 416 с.

МОДЕЛІ ТРАКТУ ОБРОБКИ СИГНАЛІВ

Білокурова А.О., Філіппенко О.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Мета роботи – побудова моделі тракту обробки сигналів псевдодоплерівського пеленгатора задля дослідження реакції на сигнали з різними характеристиками. Для оцінки адекватності було здійснено моделювання функціонування системи за допомогою пакету Matlab/Simulink. З метою спрощення моделі та зменшення часу моделювання були здійснені певні припущення - здійснене моделювання тільки принципу обробки сигналу, що підлягає аналізу. З моделі виключені гетеродини, перетворювачі частоти та фільтри проміжної частоти. Мета моделювання полягає в аналізі виду реконструйованого сигналу, який дає можливість визначити фазове зміщення у вхідному сигналі в залежності від руху вібраторів антенної решітки, що комутується, та аналізі залежності формі цього сигналу від співвідношення сигналу до шуму, що надходить з антени. Для здійснення моделювання сигналів, що надходять з антен решітки було використано блоки затримки Transport Delay, які імітують зсув фронту хвилі, що надходить. Співвідношення затримок визначає кут хвилі, що надходить до решітки. Для плавного руху віртуальної антени треба послідовно змінювати амплітуди сигналів з попарно сусідніх антен, що надходять до суматора. Після формування сигналу від антени з електронним обертанням, він подається на модуль фазового розрізнення, де відбувається виділення сигналу, який несе інформацію про фазовий зсув вхідних сигналів антен. В результаті після проходження виділеного сигналу через фільтр нижніх частот залишається сигнал, що несе інформацію про напрямок приходу сигналу від джерела радіовипромінювання. Для оцінки залежності точності функціонування системи від типу вхідного сигналу було здійснено оцінку характеру змінення вихідного сигналу каналу обробки сигналів при різних рівнях вхідного сигналу та від чистого гармонічного сигналу до шумового сигналу на вході моделі.

Список літератури

1. N. Cianos, .Low-Cost, High-Performance DF and Intercept Systems., Proc. of 1993WESCON Conference, pp. 372-376, September 1993.
2 David Adamy, “EW 101 A First Course in Electronic Warfare” Artech House Boston London.

МЕТОДИ АНАЛІЗУ МЕДИЧНИХ ЗОБРАЖЕНЬ

Іващенко Г.С., Гомелєв А.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Своєчасна медична діагностика є невід'ємною умовою попередження розвитку патологій, які в подальшому можуть призвести до тяжких захворювань. Серед засобів діагностики найбільшого поширення набув аналіз медичних зображень. У теперішній час отримані медичні зображення передаються кваліфікованим лікарям для виявлення певних відхилень від норми. Нажаль, деякі патології не піддаються діагностиці, поки хворий не набуде стадії, коли відхилення чітко видно на знімку, а окрім цього, має місце проблема людського фактору, тобто, ефективність аналізу залежить від кваліфікації лікаря, його уваги, що може бути порушена емоційним станом та втомою, умовами освітлення в кімнаті тощо. Тому автоматизація або засоби підтримки рішень в аналізі медичних зображень є актуальною проблемою, для вирішення якої доцільним є використання засобів штучного інтелекту.

Метою роботи є дослідження методів аналізу зображень та побудова моделей машинного навчання, які дозволять розпізнавати на медичних відображеннях випадки відхилення від нормального, здорового стану організму та виконувати класифікацію знайдених відхилень.

Для забезпечення автоматизації аналізу розглянута програмна платформа ML.NET, що надає доступ до бібліотеки OpenCV та платформи TensorFlow. Для вирішення завдання розпізнавання об'єктів на медичному зображенні використані штучні нейронні мережі ResNet-50 [1], ResNet-101, Inception-v3 [2] та MobileNetV2 [3], використання якої дозволяє зменшити час та ресурсоємкість обробки, що має особливе значення у випадку розміщення мережі у хмарі.

Наведені результати порівняльного аналізу використання методів класифікації медичних зображень. Отримані дані показують переваги використання архітектури ResNet-50 у поєднанні з попередньою обробкою даних, яка полягає у бінаризації, сегментації та фільтрації зображення.

Список літератури

1. ResNet (34, 50, 101): «остаточные» CNN для классификации изображений [Електронний ресурс] // NeuroHive – Режим доступу до ресурсу: www/ URL: https://neurohive.io/ru/vidy-nejrosetej/resnet-34-50-101/ – 29.01.2019 р. – Загол. з екрану.

2. Szegedy C., Vanhoucke V., Ioffe S., Shlens J., Wojna Z. Rethinking the Inception Architecture for Computer Vision. *IEEE Conference on Computer Vision and Pattern Recognition.* 2016. С. 2818-2826. DOI: https://doi.org/10.1109/CVPR.2016.308.

3. Sandler M., Howard A., Zhu M., Zhmoginov A., Chen L-C. MobileNetV2: Inverted Residuals and Linear Bottlenecks. *IEEE Conference on Computer Vision and Pattern Recognition*. 2018. С. 4510-4520. DOI: https://doi.org/10.1109/CVPR.2018.00474.

РОЗРОБКА СТРУКТУРИ ДОДАТКУ РОЗПІЗНАВАННЯ СИМВОЛІВ

Філімончук Т.В., Павленко Б.С.
Харківський Національний Університет Радіоелектроніки, Харків, Україна

Технології розпізнавання символів [1] почали використовувати в минулому столітті, і зараз активно використовуються для аналізу, обробки та отримання інформації. Сьогодні такі системи успішно використовуються в конкретних додатках, де висока швидкість має велике значення, через величезну кількості запитів, наприклад в областях сортування пошти та читання чеків. Тому подальший розвиток та дослідження даної технології є важливою науковою задачею [2]. Головним принципом автоматичного розпізнавання образів є навчання машини класам шаблонів, які можуть виникнути (визначити зовнішній вигляд) та її коректному опрацьовуванню для отримання необхідних результатів. Із задачею розпізнавання образів пов'язана необхідність використання моделей або датасетів для створення тестових програми. Ефективність роботи програми в реальному середовищі багато в чому залежить від розміру датасету, в зв'язку з чим, завдяки сучасним технологіям, розробляються більш точні методи, які засновано на нейронних мережах або оптимальних статичних класифікаторах. Такі методи дозволять технології оптичного розпізнавання символів піднятися на новий рівень.

Метою доповіді є розробка структури програмного забезпечення, яке дозволяє розпізнавати символи на растровому зображенні, враховуючи особливість їх написання та порівняння їх з датасетом. Також наведено модель оптичного розпізнавання символів, що використовує метод порівняння символів з шаблонами із дата сету, приклади та результати практичного використання технології оптичного розпізнавання символів, демонструється принцип роботи програми, її сильні та слабкі сторони, наведено опис стандартних компонентів OCR, таких як оптичне сканування, сегментація локації, препроцессінг або попередня обробка, вилучення особливостей та розпізнавання після обробки. Наведені приклади демонструють роботу розробленого програмного забезпечення та використання методів обробки растрового зображення у зв'язці з датасетом.

Список літератури

1. Иванов В.Г., Ломоносов Ю.В., Любарский М.Г. Классификация символов в алгоритмах сжатия изображения текста и системы оптического распознавания. *Вестник НТУ «ХПИ»*, 2012, №62 (968). – с. 83–90.

2. Филимончук Т.В., Волк М.А., Казмина Д.Р., Ольшанская Т.И., Рисухин М.В. Модифицированная информационная технология распределения заданий на ресурсы для систем облачных вычислений. *Сучасний стан наукових досліджень та технологій в промисловості. 2019*, №1(7). С. 121-128.

МЕТОД ПІДВИЩЕННЯ ЯКОСТІ ПЕРЕДАЧІ ІНФОРМАЦІЇ В БЕЗПРОВІДНІЙ МЕРЕЖІ

Лазуренко Б.О., Корольов А.О.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

Актуальність сучасних безпровідних мереж обумовлена постійно зростаючими вимогами до швидкості передачі інформації та якості зв'язку. Тому **метою доповіді** є підвищення безпеки, пропускної здатності та завадостійкості персональних та локальних мереж з низьким рівнем енергоспоживання в умовах дії природних та штучних завад.

Основним показником якості каналу зв'язку в безпровідній мережі є співвідношення сигнал/завада на вході кореляційного приймача. Запропоновано підвищувати рівень завадостійкості та прихованості інформаційного сигналу шляхом подвійної нелінійної обробки його спектру [1] і оптимізації маршруту передачі інформації. Розширення спектру інформаційного сигналу у передавачі здійснюють шляхом множення його на розширюючу еталонну функцію та передачу його по каналу з завадами до приймача. Обробку прийнятого сигналу здійснюють шляхом додаткового множення прийнятого сигналу на еталонну функцію, за результатами якого здійснюється стиск інформаційного сигналу до спектру переданого із одночасним розширенням спектру завад. Подальша цифрова фільтрація дозволяє відокремити спектр сигналу від шуму, а кореляційна обробка дозволяє відновити та накопичувати прийняті сигнали, що кодують інформаційний біт, підвищуючи співвідношення сигнал/шум на вході детектора приймача [2]. Також розроблено метод, який вирішує задачу підвищення швидкості передачі інформації у безпровідній мережі шляхом оптимізації маршруту передачі. При цьому додатково вводять коефіцієнт незайнятості кожного з каналів мережі, складають таблицю коефіцієнтів незайнятості каналів між усіма користувачами мережі, співвідносять таблицю коефіцієнтів незайнятості каналів із таблицею якості каналу зв'язку та визначають оптимальні сегменти маршруту на основі порівняння відповідних даних обох таблиць за їх максимальними значеннями.

Список літератури

1. Slepian D. Some comment on the Detection of Gaussian Signals in Gaussian Noise //JRE Transactions on Information Theory, 1952. - № 2.

2. Серков О.А., Панченко С. В., Трубчанінова К.А., Горюшкіна А.Є., Лазуренко Б.О. Спосіб прийому цифрових двійкових сигналів в умовах шуму. Патент України на корисну модель № 145319 U МПК H04B 1/06, Опубл. 25.11.20, Бюл. № 22, заявка № u 2020 04847 подана 29.07.2020.

АНАЛІЗ ЗАСОБІВ КЛАСТЕРИЗАЦІЇ ДАНИХ

Кузьменко О.В., Черних О.П.
Національний технічний університет
«Харківський політехнічний інститут», Харків, Україна

На сьогодні зростання обсягів даних з різними властивостями приводить до необхідності аналізу швидкодіючих і надійних засобів кластеризації.

Рішення завдання кластеризації принципово неоднозначно за декількома причинами: досить немає однозначно найкращого критерію якості кластеризації та число кластерів, як правило, невідомо заздалегідь і встановлюється відповідно до деякого суб'єктивного критерію. Важко забезпечити чітку категоризацію методів кластеризації, оскільки вони можуть перекриватися, так що метод може мати функції з декількох категорій. Методи кластеризації можна розділити на два основних типа: ієрархічна і секційна кластеризації.

У загальному вигляді кластерний аналіз включає наступні етапи: відбір вибірки об'єктів для кластеризації; визначення безлічі змінних, за якими будуть оцінюватися об'єкти у вибірці; обчислення значень міри схожості між об'єктами; застосування методу кластерного аналізу для створення груп схожих об'єктів (кластерів); представлення результатів аналізу. Визначено, що загальна схема кластеризації одна, але існує багато реалізацій цієї схеми.

Однією з цілей кластеризації є виявлення внутрішніх зв'язків між даними шляхом визначення кластерної структури. Розбиття спостережень на групи схожих об'єктів дозволяє спростити подальшу обробку даних і прийняття рішень, застосовуючи до кожного кластеру свій метод аналізу. Після отримання та аналізу результатів можливе корегування обраного методу кластеризації до отримання оптимального результату.

Для визначення оптимального числа кластерів в роботі були розглянуті алгоритм пов'язаних компонентів і алгоритм пошарової кластеризації. За допомогою пошарової кластеризації були обрані пов'язані компоненти на різних рівнях і задана потрібна глибина одержуваних кластерів, що, в свою чергу, прискорило роботу кластерів.

Однак, при загальному використанні будь-якого алгоритму важливо розуміти його достоїнства і недоліки та обов’язково враховувати природу даних, з якими він краще працює.

Список літератури

1. Олдендерфер М.С., Блэшфилд Р.К. Кластерный анализ / Факторный, дискриминантный и кластерный анализ. — М.: Финансы и статистика, 1989 – 215 с.

2. Шлезингер М. Десять лекций по статистическому и структурному распознаванию. // Шлезингер М., Главач В. − Киев: Наукова думка, 2004. − 343 с.

МОДЕЛЬ РОЗПОДІЛУ ОБЧИСЛЮВАЛЬНИХ РЕСУРСІВ В КЛАСТЕРНИХ СИСТЕМАХ

Філімончук Т.В., Булавков Б.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Поява нових інформаційних технологій, таких як хмарні обчислення та кластерні системи, зумовило розвиток технологій розв'язання задач великої обчислювальної складності. До найбільш перспективних напрямків, які використовуються на даний час, можна віднести технології паралельних розподілених обчислень, тому розподіл обчислювальних ресурсів в кластерних системах є актуальною задачею.

Раціональним інструментом підбору оптимальних обчислювальних ресурсів є використання спеціалізованих середовищ моделювання (MicroGrid, ChicSim, OptorSim, SimGrid, GridSim), функції розподілу в яких покладено на спеціалізований засіб (планувальник). Планувальник завдяки інформації від постачальника завдань здійснює їх розподіл на підставі переліку правил та дисциплін розподілу. На даний час планувальник, як правило, реалізує одну найпростішу дисципліну розподілу [1], що ніяким чином не оптимізує використання обчислювальних ресурсів кластерних систем.

Метою доповіді є розробка моделі розподілу обчислювальних ресурсів, яка дозволить розподіляти завдання, які надходять на вхід кластерної системи, враховуючи і вимоги постачальника задач, і вимоги постачальника обчислювальних ресурсів. Модель розподілу розширена за рахунок введення до неї низки додаткових параметрів, які в свою чергу допомагають збільшити продуктивність використання обчислювальних ресурсів кластерних систем. Як правило розподіл обчислювальних ресурсів з урахуванням вимог постачальників завдань, слід здійснювати з урахуванням ряду параметрів, що в свою чергу накладає труднощі, тому що потребує розв’язання задачі багатокритеріальної оптимізації [2]. В ході дослідження проведена низка експериментів з розподілу обчислювальних ресурсів для множини дисциплін розподілу. Результати, які були отримані в ході проведення експериментів, свідчать про зменшення часу виконання деяких пулів завдань, середнього часу знаходження в черзі та проценту простою обчислювальних ресурсів кластерних систем.

Список літератури

1. Волк М.А, Филимончук Т.В., Гридель Р.Н. Методы распределения ресурсов для GRID-систем. Збірник наукових праць ХУПС. Харков: ХУПС, 2009. №1(19). с.100-104.

2. T. Filimonchuk, M.O. Volk, I.Ruban, V.Tkachov. Development of information technology of tasks distribution for grid-systems using the GRASS simulation environment. Eastern-European Journal of Enterprise Technologies. Information and controlling system. Vol.3/9 (81). 2016. P.45-53.

СПЕЦИФІКА ЧАТ-БОТІВ ЯК ПАРАДИГМА РОЗРОБКИ МОДЕЛІ ФРЕЙМОРКУ

Філімончук Т.В., Хабазня Д.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

На даний час популярність чат-ботів – це очевидний етап процесу розвитку технологій [1] за рахунок скорочення видимої інформації про ресурс. Платформи чат-ботів, які представили більшість популярних мессенджерів, створили новий простір для розвитку нових і вже існуючих проектів. Причинами для цього стало декілька факторів. По-перше, це концепція чату, яка націлена на швидку взаємодію між учасниками діалогу. По-друге, використання Rest API, що дозволяє існуючим проектам не розробляти чат-бот з нуля, а масштабувати готовий проект лише створивши в ньому API для взаємодії с мессенджером. По-третє, відсутність Front-end шару, що значно зменшує обсяг роботи та дозволяє розробити повноцінний чат-бот проект невеликою командою Back-end розробників. Специфіка взаємодії серверу бота та серверу мессенджеру не дозволяє повноцінно використовувати вже існуючі фреймворки, які орієнтовано на веб-застосунки «класичного» веб-сайту. Розробники чат-ботів починають стикатися з однотипними структурними задачами, вирішенням яких завжди займався фреймворк.

Метою доповіді є аналіз моделі фреймворку для побудови чат-ботів будь-якої складності. Модель включає в себе нові архітектурні рішення, які вирішують специфічні задачі будь-якого чат-бот за стосунку: динамічна побудова розмітки кнопок, гнучкі сценарії побудови діалогу. Крім того модель включає модулі, які завжди присутні у будь якому фреймворку, але з огляду на нову бот-перспективу. Прикладами є модуль безпеки с шифруванням тексту повідомлень, модуль локалізації та модуль адміністрування чат-боту.

Аналіз галузі диктує технології побудови Proof Of Concept моделі. Основною мовою програмування обрана мова Groovy, базована на JVM, з використанням бази даних Postgres. Для розробки тестового застосунку на базі фреймворку використана Telegram API, як найбільш функціональна та документована бібліотека, для розгортання інфраструктури – хмарна PaaS платформа Heroku [2].

Список літератури

1. Филимончук Т.В., Волк М.А., Казмина Д.Р., Ольшанская Т.И., Рисухин М.В. Модифицированная информационная технология распределения заданий на ресурсы для систем облачных вычислений. *Сучасний стан наукових досліджень та технологій в промисловості*. 2019, №1(7). С. 121-128.

2. Веллинг Л., Томсон Л. Разработка веб-приложений. Москва: Вильямс, 2010. 848 с.

СЕКЦІЯ 4
БЕЗПЕКА ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Керівник секції: д.т.н., проф. О. А. Смірнов, ЦНТУ, Кропивницький
Секретар секції: к.т.н., доц. О. В. Сєвєрінов, ХНУРЕ, Харків

МЕНЕДЖМЕНТ ВРАЗЛИВОСТЕЙ В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Поддубний В.О., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

У зв'язку з модернізацією чинного законодавства України в сфері технічного захисту інформації, системи управління інформаційною безпекою (СУІБ) набувають все більшого розповсюдження, замінюючи комплексні системи захисту інформації (КСЗІ) в існуючих інформаційно-телекомунікаційних системах. Однією з особливостей СУІБ, на відміну від КСЗІ, є більш детальна обробка ризиків. Джерелами ризиків можуть бути вразливості програмного забезпечення, що встановлено в ІТС [1]. Існуючі нормативні документи потребують розробки методик формального опису інформаційної системи [2] для оцінки ризику, пов'язаного з обробкою програмних вразливостей в ІТС. Такі методики допоможуть організаціям, що створюють СУІБ більш конкретно та однозначно оцінювати ризики та приймати рішення.

Метою доповіді є побудова системи оцінки вразливостей в ІТС та обробка ризику, що створюють дані вразливості. В доповіді наводяться основні принципи побудови системи оцінки вразливостей в ІТС, її структура, принципи впровадження та використання. Особливостями даної системи є використання декількох оцінок для ранжування критичності вразливості відносно системи, а також відносно виразності властивостей вразливості та використання формального опису [3] для моделі зв'язків компонентів та процесів в ІТС. Така система повинна інтегруватися в політику безпеки СУІБ та встановлювати чіткі формалізовані правила щодо контролю програними вразливостями в ІТС та ризиком, що пов'язаний з ними. Це зменшить людський фактор при оцінці ризиків та прийняття рішень, та забезпечить однозначність результатів.

Список літератури

1. Поддубний В.О., Сєвєрінов О.В., Пустомельник О.С. Менеджмент вразливостей як складова частина політики безпеки ІТС // Системи управління, навігації та зв'язку. – Полтава: ПНТУ. - 2020. – Вип. 4(62). – С. 55-58.
2. Гвоздьов Р.Ю., Олійников Р.В., Метод та методика формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах// Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 91 – 96.
3. Поддубний В.О., СєвєріновО.В. Менеджмент вразливостей з використанням формалізованого опису. Радіотехніка. 2020. Вип. 203. С. 72 – 77.

ВИКОРИСТАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ У КРИПТОАНАЛІЗІ БЛОЧНОГО СИМЕТРИЧНОГО ШИФРУ AES

Кохан С.А., Руженцев В.І.
Харківський національній університет радіоелектроніки, Харків, Україна

З розвитком технологій машинного навчання, з'являються нові підходи та методи криптоаналізу шифрів. За останні роки набуває популярності метод криптоаналізу який базується на використанні штучних нейронних мереж.

В процесі навчання на вхід нейронної мережі подається шифртекст, а очікуваним виходом є відкритий текст. Після навчання з достатньою кількістю пар відкритих текстів і шифртексту, які зашифровані одним і тим же ключем, нейронна мережа зможе генерувати відкритий текст із зашифрованого тексту, який не був частиною процесу навчання, якщо цей шифртекст зашифрований одні і тим же ключем. Таким чином, результатом даної атаки є функціональний алгоритм еквівалентний початковому дешифруванню за винятком відсутності ключа, використовуваного в процесі шифрування.

У роботі [1] дана атака застосовується до алгоритму блочного шифрування AES з режимами роботи ECB та CBC. В якості нейронних мереж були використані нейронна мережа прямого поширення, а також каскадна нейронна мережа прямого поширення. Дослідження проводилося з різною кількістю біт шифртекстів та відкритих текстів для навчання нейронної мережі, а саме від 2^8 до 2^{13}. При дослідженні нейронної мережі прямого поширення вдалося повністю відновити від 500 до 700 байт відкритого тексту з 2^{17} байт. Кількість біт яка використовувалась при навчанні нейронної мережі не вплинула на кінцевий результат. При використанні каскадної нейронної мережі прямого поширення вдалося повністю відновити від 800 до 5300 байт відкритого тексту з 2^{17} байт. Каскадна нейронна мережа, при навчанні якої використовувалось 2^{13} біт відкритих текстів та шифртекстів показала кращій результат.

Проведений аналіз атаки на шифр AES показав, що для успішної реалізації атаки за допомогою нейронних мереж може знадобитися менша кількість пар відкритих та закритих текстів, ніж для реалізації атаки перебором.

Наведені результати показують, що дуже важливим є вибір топології нейронної мережі, її тип, а також кількість біт яка використовується для її навчання. У зв'язку з цим наступним кроком є дослідження та використання різноманітних типів нейронних мереж для криптоаналізу сучасних шифрів. Отримані результати можуть бути використані як універсальний інструмент аналізу стійкості криптографічних алгоритмів.

Список літератури

1. Xinyi Hu and Yaqun Zhao. Research on Plaintext Restoration of AES Based on Neural Network. Hindawi Security and Communication Networks Volume 2018, Article ID 6868506, 9 pages https://doi.org/10.1155/2018/6868506

МЕТОДИКА ФОРМАЛЬНОГО ПРОЕКТУВАННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Гвоздьов Р.Ю., Сєвєрінов О.В., Караваєв В.М.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком інформаційних технологій, наданням електронних послуг в країні проектуються та вводяться в експлуатацію все більше інформаційних систем, до яких висуваються обов'язкові вимоги до захисту інформації [1]. Одним із шляхів для задоволення вимог до безпеки таких систем є побудова комплексної системи захисту інформації (далі – КСЗІ).

Нормативними документами в сфері технічного захисту інформації визначено сім ієрархічних критеріїв гарантій від Г-1 до Г-7 включно, які визначають ступінь впевненості в тому, що кожна з функціональних вимог безпеки здатна протистояти певним загрозам. НД ТЗІ 2.5-004.99 висуває вимоги до процесу проектування КСЗІ, де стиль формалізованої (частково формалізованої) специфікації є обов'язковим для отримання рівня гарантій Г-4 та вище.

На даний момент, не існує методик для формального проектування КСЗІ в інформаційно-телекомунікаційних системах (далі – ІТС).

Метою доповіді є аналіз існуючих мов формального опису системи, які в перспективі можуть використовуватися для проектування КСЗІ в ІТС та створення наукового підґрунтя для подальших досліджень в цій сфері.

Процес проектування включає в себе модель політики безпеки та проект архітектури комплексу засобів захисту. Методика формального проектування КСЗІ в ІТС повинна включати в себе формалізовану модель політики безпеки, формалізовану модель ІТС та алгоритм формування комплексу заходів захисту [2].

Формалізовані моделі політики безпеки інформації та ІТС, можуть бути використані при побудові системи оцінки вразливостей системи [3, 4].

Список літератури

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

2. Р.Ю. Гвоздьов, Р.В. Олійников, Метод та методика формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах// Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 91 – 96.

3. В.О. Поддубний, О.В. Сєвєрінов, Менеджмент вразливостей з використанням формалізованого опису// Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 72 – 77.

4. Гвоздьов Р. Методика формального проектування КСЗІ в ІТС / Р. Гвоздьов, В. Заболотний, А. Бойко // Global Cyber Security Forum : матеріали Першого міжнародного науково-практичного форуму, 14 – 16 листопада 2019 р. – Харьков : ХНУРЭ, 2019. – С. 39–40.

СУЧАСНІ МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Кліпоносова В.С., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Однією з актуальних задач розвитку інформаційних технологій на сучасному етапі є забезпечення надійного захисту інформації. Існуючі сьогодні методи захисту інформації поділяють на: апаратні, програмні, змішані; останні поєднують у собі як апаратні, так і програмні засоби. Задача захисту інформації є особливо актуальною в умовах активного розвитку систем електронної торгівлі та банківських операцій, систем дистанційного навчання та великих корпоративних мереж, де циркулює конфіденційна інформація. Важливою та ще не вирішеною проблемою захисту інформації є ефективна ідентифікація користувача, який отримує доступ до конфіденційної інформації [1]. Біометричні технології ідентифікації та автентифікації мають низку переваг перед традиційними і знаходять все більше застосування в комп'ютерних системах [2].

Біометричне підтвердження, а не проста перевірка пароля, який може бути вкрадений, перехоплений або вгаданий, є ключовим при розширенні Інтернет-торгівлі, створенні нових систем безпеки інформації в корпоративних мережах та системах дистанційного навчання та тестування.

Метою доповіді є аналіз існуючих методів біометричної ідентифікації та автентифікації, обґрунтований вибір методів для подальшого дослідження та практичного застосування.

Ці методи мають забезпечувати надійну ідентифікацію та автентифікацію користувачів з високою ймовірністю, а також унеможливлювати надання доступу нелегальним користувачам [3].

В доповіді наводяться результати огляду, переваги та недоліки динамічних і статичних біометричних методів. Необхідно відзначити, що найбільшу ефективність захисту забезпечують системи, в яких біометричні методи поєднуються з іншими апаратними засобами автентифікації або декількома різними типами біометричної ідентифікації. Комбінуючи різні способи біометричної і апаратної автентифікації, можна отримати надійну систему захисту (що підтверджується великою зацікавленістю, яку проявляють до цих технологій провідні виробники програмного забезпечення).

Список літератури

1. Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений – Пенза: Издательство Пензенского государственного университета, 2000, С.188.

2. Голубев Г. А., Габриелян Б. А. Современное состояние и перспективы разв тия биометрических технологий // Нейрокомпьютеры. Разработка. Применение. № 10, 2004, – С. 39 – 46.

3. Мироненко Є.В., Сєвєрінов О.В. Біометрична ідентифікація і автентифікація особи за геометрією обличчя, НТУ «ХПІ», 2020.

ОПТИМАЛЬНІ ДЕКОМПОЗИЦІЇ БАГАТОРОЗРЯДНИХ ЦІЛИХ ЧИСЕЛ

Просолов В.В., Мельникова О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Загальним завданням у впровадженні багатьох криптосистем з відкритим ключем є піднесення до степеню в деякій комутативній групі G, тобто оцінка продукту. Приклад груп включає (Z / nZ) для деякого цілого числа n, наприклад для перевірки підписів ElGamal або DSA; групи раціональних точок на еліптичних кривих над кінцевими полями, наприклад для перевірки підписів ECDS; і класові групи уявних-квадратичних порядків, наприклад для перевірки RDSA підписів [1 - 2]. Ми маємо k = 2 для верифікації DSA та ECDSA і k = 3 для верифікації ElGamal і RDSA. Більші значення k з'являються в протоколах фірмових знаків. У цій роботі ми допускаємо також k = 1 для алгоритмів; міркування ефективності можуть ігнорувати цей випадок. Добре відомо, що взагалі надмірно неефективно обчислювати повноваження g_i^{ei} окремо, а потім перемножувати їх. Натомість зазвичай застосовуються специфічні алгоритми для однократного піднесення до степеню.

Звичайний підхід для однократного піднесення до степеню поєднує всі елементи вхідної групи g_i один з одним на етапі попереднього обчислення, потім етап оцінки одночасно переглядає всі показники. У цій роботі ми обговорюємо альтернативний підхід, коли на етапі попередньої обчислювальної дії показники обробляються окремо. У цьому підході на етапі оцінювання використовується переплетення генераторів та експонентів для різних і, а не обробка декількох і одночасно.

Метою доповіді є вивченні та вдосконаленню методів n-кратної декомпозиції багаторозрядних числових значень.

В роботі розглянуто існуючі методи швидкого піднесення до степеню по модулю, які використовуються в сучасних криптоалгоритмах та алгоритми однократного піднесення до степеню по модулю. Проводиться порівняння алгоритмів піднесення до степеню для знаходження їх переваг та недоліків. Результатом дослідження розробленого алгоритму піднесення до степеню з декомпозицією є те, що він ефективніший за свої аналоги, якщо використовується фіксована основа, цю властивість можливо використовувати у деяких сучасних криптосистемах.

Список літератури

1. American National Standards Institute (ANSI). Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA). ANSI X9.62, 1998.

2. Federal Information Processing Standards Publication 186 – 4 (FIPS PUB 186 - 4). Digital Signature Standard (DSS) // U.S. Department of Commerce. Technology Administration, National Institute of Standards and Technology (NIST). — 2013. — 130 p.

АНАЛІЗ ПРАВИЛ КОРЕЛЯЦІЇ В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ПОДІЯМИ БЕЗПЕКИ

Овчаренко М.Ю., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день системи управління інформаційною безпекою та подіями безпеки (Security Information and Event Management, SIEM) є одними з найрозповсюдженіших систем управління інцидентами інформаційної безпеки тому, що вони здатні обробляти великі обсяги інформації про події в інформаційній системі від різних джерел в режимі реального часу та інформувати адміністратора про появу інцидентів інформаційної безпеки [1]. Проте кожен день в інформаційних системах відбуваються сотні та навіть тисячі подій, більшість з яких є результатами нормального функціонування системи та її користувачів, тож потрібно розробляти та впроваджувати правила, які будуть відділяти звичайні системні події від інцидентів безпеки, так звані правила кореляції.

Метою доповіді є аналіз існуючих правил кореляції в системах управління інформаційною безпекою та подіями безпеки та вибір оптимальних правил кореляції для використання в сучасних інформаційно-телекомунікаційних систем.

В доповіді були розглянуті існуючі правила кореляції, які можна об'єднати в дві групи – сигнатурні та несигнатурні. Несигнатурні правила, так звані «правила з коробки», розробляються постачальниками SIEM-систем та їх неможливо видозмінити, до них можна віднести статистичні правила, на графах, на нейронних мережах. На відміну від несигнатурних сигнатурні правила можливо видозмінити, що робить їх більш гнучкими та ефективними. До таких можна віднести кількісні (реагування на інцидент в залежності від кількості його появ в системі) та ймовірнісні (реагування на інцидент в залежності від ймовірності його появи в системі) [2, 3]. Таким чином впровадження правил кореляції в SIEM-систему призводить до зменшення часу реагування на інциденти та негативних наслідків, які можуть бути нанесені системі та її власникам, а використання сигнатурних правил дозволяє точніше налаштувати SIEM-систему під певні потреби та підвищити її керованість.

Список літератури

1. Ушатов В., Сєвєрінов О.В.. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. – Харків: ХНУРЕ, 2019. - С. 104–105. (2019).

2. Sievierinov O.V., Ovcharenko M.Y. Analysis of correlation rules in Security information and event management systems. *Computer and information systems and technologies*. 2020. P. 24-25.

3. Miller D. et al. Security information and event management (SIEM) implementation. – McGraw-Hill, 2011.

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Федюшин О.І., Юхименко В.І., Кожушко Д.Р.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день для тестування на проникнення існує безліч інструментів, що можуть бути включені до арсеналу фахівця з аудиту інформаційної безпеки, вибір найефективніших із них, стає досить складною задачею. Окрім завищених заявок постачальників, є мало емпіричних досліджень з метою порівняння, щоб проінформувати практикуючих про те, які інструменти можуть бути найбільш ефективними для їх потреб. Отже, головною метою цієї роботи є дослідити діапазон ефективності інструментів пен тестування з точки зору часу відгуку та охоплення. В роботі розглядається впровадження мережних систем виявлення вторгнень (NIDS) [1, 2] з відкритим кодом для отримання та збереження мережних цифрових доказів («відбитків») при робочих навантаженнях.

Архітектура запропонованої системи складається з двох мереж: перша є модельованою мережею Інтернету, друга – виробничою мережею. Кожна мережа має певні компоненти. Інтернет-мережа включає чотири машини, що виробляють трафік, і одну машину, що виробляє міжсайтові сценарії та атаки SQL-ін'єкцій проти веб-сервера [3]. Виробнича мережа складається з веб-сервера з вразливим веб-додатком для пропонованих атак, брандмауера з NIDS, включаючи Snort, Suricata та Bro-IDS, і, нарешті, Forensic-сервера. Як результат, запропонована система працює для моніторингу та криміналістичного вивчення переданого трафіку між обома мережами.

Отримані дані демонструють, що запропоновані NIDS можна використовувати як джерело цифрових доказів. Захоплені пакети, а також попередження, генеровані цими NIDS, можуть бути використані як сліди доказу відтворених атак. Однак вони мають проблеми доставки пакетів до своїх інтелектуальних аналізаторів. Проблема значною мірою пов’язана з функціями перехоплення, і ці функції потрібно вдосконалити, щоб усунути проблему. У дослідженні були написані сценарії для підвищення продуктивності інструментів та можливості збереження цифрових доказів. Результати експериментів показали, що запропонована конструкція системи може виконати багато завдань, включаючи отримання та збереження мережного трафіку VLAN як цінного джерела цифрових доказів.

Список літератури

1. Khraisat, A., Gondal, I. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20(2019). DOI: https://doi.org/10.1186/s42400-019-0038-7.

2. О.В. Сєвєрінов, А.Г. Хрєнов. Аналіз сучасних систем виявлення вторгнень. Системи обробки інформації, 6 (2014): 122-124.

3. О.В. Сєвєрінов, А.Г. Хрєнов. Аналіз сучасних методів атак на електронні ресурси органів військового управління. Наука і техніка Повітряних Сил Збройних Сил України, 3 (2015): 125-128.

VIRTUAL ENVIRONMENT FOR TRAINING AUDITORS WITH INFORMATION SECURITY

Fediushyn O.I., Yatsiuk O.O., Rusanov H.O.
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

At present, many universities in Ukraine are preparing specialists in the field of cybersecurity. Developing a successful educational program to train those interested in developing the cybersecurity skill set is difficult. Most institutions interested in these programs has deal with limited resources when designing an appropriate learning environment, limited teacher time to devote to maintaining systems, limited administrative support due to misunderstanding of these skills, and accidental (or deliberate) misuse of tools and skills.

Virtual machines (VM) support many of the cybersecurity competition and lab operations. Virtual laboratories allow emulating real cyber threats and rapid generation of multiple scenarios and infrastructures.

The goal of the study is to create a laboratory infrastructure that allows instructors to quickly create virtualized environments for simulating various cyber threats. The testing environment for this demo consists of a Windows 10 , Ubuntu 16.4 , Kali linux and OSSIM. OSSIM utilizes open source security tools to retrieve, organize, and display information from network assets. The sources of this information are called “data sources”. Events from data sources are parsed and normalized through plugins which associate each log event with an “Event Type,” sometimes referred to as a “plugin_sid”, which is the name of a field in the SIEM database [1, 2]. OSSIM uses database plugins which query databases and retrieve information, transforming that information into SIEM events.

The experiment is conducted in two phases. The first phase involves observing the performance of pre-selected penetration testing tools. The tools include service fingerprinting software and vulnerability scanners. Performance metrics such as number of services identified, response time, and number of vulnerabilities detected are captured and organized into various quantitative graphs and tables in order to precisely reflect the tools’ effectiveness.

In the second phase of the experiment, based on the attack surfaces provided by the first phase, various combination of attacks are deployed on the experimental hosts in order to acquire the highest privileges. Completed attacks together with potential moves are gathered and put into various attack tree diagrams for analysis so as to find out the most effective attacks against each host.

References

1. Sandeep K. B. The Operational Role of Security Information and Event Management Systems / K. B. Sandeep/ *IEEE Security and Privacy Magazine*, 2014. Vol. 12(5).–35 pp. DOI: https://doi.org/10.1109/MSP.2014.103.

2. Sievierinov O.V., Ovcharenko M.Y. Analysis of correlation rules in Security information and event management systems. *Computer and information systems and technologies.* 2020. P. 24-25.

АНАЛІЗ ВРАЗЛИВОСТЕЙ СУЧАСНИХ МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Якушко Я.А., Євгеньєв А.М.
Харківський національний університет радіоелектроніки, Харків, Україна

У міру розвитку комп'ютерних мереж і розширення сфер автоматизації, цінність інформації неспинно зростає. Державні секрети, комерційні, юридичні та лікарські таємниці все частіше стикаються з необхідністю запобігти несанкціонованому доступу до своїх систем і захистити транзакції в електронному бізнесі.

Біометричні ознаки, які використовуються для ідентифікації повинні мати наступні властивості: універсальність, унікальність, переваги, вимірність, ефективність, доступність, захищеність від підробки [1, 2].

Біометрична система вразлива для двох типів помилок: якщо система не розпізнає легітимного користувача - відбувається відмова в обслуговуванні та якщо самозванець невірно ідентифікується як авторизований користувач – йде повідомлення про вторгнення.

Найважливіший фактор мінімізації ризиків безпеки і порушення приватності, пов'язаних з біометричними системами, - захист біометричних шаблонів, що зберігаються в базі даних системи. Ці ризики можна до певної міри зменшити за рахунок децентралізованого зберігання шаблонів. Є два загальних принципів захисту біометричних шаблонів: трансформація біометричних характеристик і біометричні криптосистеми

Метою доповіді є порівняння методів сучасної біометричної ідентифікації з використанням математичної статистики (FAR і FRR), а також порівняння стійкості та незмінності біометричних даних.

В доповіді наводяться результати порівняльного аналізу методів сучасної біометричної ідентифікації [2]. Результати показують, що фальсифікація біометричних даних по сітківці ока – неможлива, в той час як підробка інших даних біометричної ідентифікації, або можлива, або поки що невідомо (по райдужній оболонці ока). Незмінність біометричної характеристики з плином часу буде високою у методах по райдужній оболонці ока та 3D-розпізнавання [3]. Для створення найбільш захищеної системи, методи біометричної ідентифікації слід комбінувати.

Список літератури

1. Дослідження та порівняльний аналіз методів аутентификации / Л.Є. Мартинова, М.Ю. Умніцин, К.Е. Назарова, І.П. Пересипкін. // Молодий вчений – 2016. – №19. – С. 91-121.

2. Біометрична аутентифікація: захист систем і конфіденційність користувачів [Електронний ресурс]. – 2012. – Дата звернення: 03.03.2021. Режим доступу до ресурсу: https://www.osp.ru/os/2012/10/13033122/.

3 Є.В. Мироненко, О.В. Сєвєрінов. Біометрична ідентифікація і автентифікація особи за геометрією обличчя. НТУ «ХПІ», 2020.

АНАЛІЗ МЕТОДІВ РЕАЛІЗАЦІЇ ЦІЛЬОВИХ АТАК НА ІНФОРМАЦІЙНІ СИСТЕМИ

Євгеньєв А. М., Дорофєєва К. І.
Харківський національний університет радіоелектроніки, Харків, Україна

Захист даних в інформаційних системах під час їх функціонування потребує не тільки дотримання політики безпеки, здійснення організаційних заходів чи технічного обслуговування засобів захисту, але й ефективного менеджменту, моніторингу, контролю та оцінки ризиків інформаційної безпеки. Однією із складових ефективного менеджменту інформаційної безпеки в інформаційних системах є правильне реагування на вразливості.

Цільові атаки, на відмінну від масових атак, характеризуються зломом і обходом захисту ІС з більш глибоким проникненням в систему [1,2].

Атака такого типу проводиться у декілька етапів: аналіз «поверхні» проникнення в інформаційну систему; експлуатація вразливості з установкою на пристрої жертви дистанційно керованого програмного забезпечення; закріплення в системі з придушенням засобів захисту, блокуванням контрольних систем і знищенням слідів проникнення; установка цільового ПО і його експлуатація.

Метою доповіді є обґрунтування підходів до розробки ефективної системи керування вразливостями для захисту інформаційних систем від цільових атак. В доповіді наводяться методи забезпечення захисту інформаційної системи, а також аналіз сучасних системи оцінювання ризиків та обґрунтовуються вимоги до наступних функцій самої системи [3]: відслідковування впливу вразливості на компоненти системи; забезпечення відтворюваності дії атак; Захист від цільових атак – це комплексна задача, яку не можна вирішити використовуючи один рівень захисту [4,5]. Для досягнення мети, потрібно застосовувати весь спектр засобів забезпечення інформаційної безпеки; тільки в цьому випадку можна підвищити можливість успішного виявлення і нейтралізації атак.

Список літератури

1. Cyber Risk Remediation Analysis // Systems Engineering Guide : [англ.]. — MITREruen, 2014. — P. 184—191. — ISBN 978-0-615-97442-2.

2. О.В. Сєвєрінов, А.Г. Хрєнов, А.О. Поляков. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі. Системи обробки інформації, 9 (2015): 101-104.

3. Левцов, В. Анатомия таргетированной атаки, часть 1 : [рус.] / Левцов, В., Демидов, Н. // Information Security. — 2016. — № 2. — P. 36—39.

4. Jeun, I. A practical study on advanced persistent threats // Computer Applications for Security, Control and System Engineering : [англ.] / Jeun, I., Lee, Y., Won, D.. — Springer Berlin Heidelberg, 2012. — P. 144—152. — doi:10.1007/978-3-642-35264-5_21.

5. Поддубний В.О., Сєвєрінов О.В., Пустомельник О.С. Менеджмент вразливостей як складова частина політики безпеки ІТС. Системи управління, навігації та зв'язку. Збірник наукових праць, 4.62 (2020): 55-58.

КРИПТОСИСТЕМИ НА ОСНОВІ ЛОГАРИФМІЧНОГО ПІДПИСУ

Колесніков М.Є., Халімов Г.З.
Харківський національний університет радіоелектроніки, Харків, Україна

Після того, як Вітфілд Діффі та Мартін Геллман представили ідею відкритих ключів шифрування, асиметрична криптографія різко стрибнула вперед. Існує багато криптосистем з відкритим ключем, але більшість з них вже зламано, а такі, що витримали перевірку часом, ґрунтуються на складності вирішення певних математичних задач.

Наприкінці 1970-х років Спірос Магліверас почав досліджувати використання в криптографії спеціальних факторизацій для кінцевих неабелевих груп, відомих як логарифмічні підписи [1]. Пізніше були опубліковані роботи, які описують розроблені ним криптосистеми - MST1, що базується на логарифмічних підписах, та MST2 на основі іншого типу накриття множин - так званих [s, r]-осередках.

Втім, на сьогодні нема відомих реалізацій MST1 або MST2. Нещодавно була розроблена нова криптосистема на відкритих ключах – MST3, що поєднує дві попередні та працює на основі логарифмічних підписів та випадкових накриттів кінцевих неабелевих груп. Для реалізації цієї системи були запропоновані 2-групи Судзукі [2].

Метою доповіді є розгляд алгоритму MST3, що базуватиметься на поєднанні 2-груп Судзукі та логарифмічних підписів, а також у доведенні того, що в практичній криптографії можна використовувати логарифмічні підписи та накриття для кінцевих груп.

В доповіді увага буде зосереджена на накриттях та методах їхнього ефективного генерування для великих кінцевих груп. Досліджуватиметься реалізація криптосистеми MST3 з відкритим ключем з 2-групами Судзукі. Завдяки їхній простій структурі, вони дозволяють вивчити безпеку системи та забезпечити ефективну реалізацію.

Буде представлено дослідження її безпеки. Використовуючи властивості групової операції у 2-групах Судзукі, а також властивості самих логарифмічних підписів, буде розроблена та застосована атака, що показує непридатність канонічних підписів в цій реалізації.

Список літератури

1. S. S. Magliveras. A Cryptosystem from Logarithmic Signatures of Finite Groups / Magliveras S. S. // Тези доповідей XXIX Середньозахідного симпозіуму з електронних мікросхем та систем. – Амстердам : видавничий дім «Elsevier», 1986 – С. 972—975. DOI: https://doi.org/10.1007/s10623-010-9369-9

2. G. Higman. Suzuki 2-groups / Higman G. // Ілінойський математичний журнал. – Дарем : видавничий дім «Duke University Press», 1963. Т. 7, №1. С. 79–96. DOI: https://doi.org/10.1215/ijm/1255637483.

МЕТОДИКИ ТЕСТУВАННЯ КВАНТОВИХ ГЕНЕРАТОРІВ ВИПАДКОВИХ ЧИСЕЛ

Коптєва М.В., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Квантові генератори випадкових чисел (КГВЧ) найбільш широке застосування знайшли в криптографії. Генератори, які використовуються в криптографічних додатках, повинні задовольняти жорстким вимогам. Бажано, щоб вони видавали дійсно випадкову послідовність чисел. КГВЧ генерують числа, випадковість яких гарантується законами фізики, тому їх можна назвати істино випадковими числами. Для перевірки статистичних властивостей випадкових послідовностей існує досить велика кількість методик тестування, але далеко не всі вони забезпечують стовідсотковий результат [1].

Отже виникає необхідність у детальному аналізі та зрівнянні найбільш відомих методик тестування КГВЧ.

Метою доповіді є проведення порівняльного аналізу сучасних методик тестування квантових генераторів випадкових чисел з використанням пакетів статистичних тестів NIST STS [2], Diehard [3], а також серії тестів FIPS 140-3 [4].

В доповіді надані результати тестування випадкової послідовності, що була отримана з використанням КГВЧ, методиками NIST STS, FIPS 140-3 та Diehard.

Отримані результати дозволили зробити висновок, що методики NIST STS та Diehard дозволяють провести більш детальне дослідження згенерованої послідовності випадкових чисел, так як вони дають найбільш повний статистичний портрет генератора. Ці методики рекомендовано використовувати для комплексного або поточного контролю генератора. Методика FIPS 140-3 надає менш розгорнутий результат тестування і може використовуватися для оперативного контролю генератора [5].

Список літератури

1. Задков В.Н., Владимирова Ю.В. Класичні та квантові генератори випадкових чисел. *Суперкомп'ютери*. 2013. № 2. С. 12-20

2. Ruhkin A.A. Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. *NIST Special Publication 800-22*, 2010.

3. Marsaglia G. Some Difficult-to-Pass Tests of Randomness. *Journal of Statistical Software 07*. 2002. DOI: 10.18637/jss.v007.i03

4. Security requirements for Cryptographic Modules. FIPS 140-3. – U.S. Department of Commerce. 2019. DOI: 10.6028/NIST.FIPS.140-3

5. Сєвєрінов О.В. Аналіз методів побудови генераторів псевдовипадкових послідовностей. *Системи обробки інформації,* 8 (2013): 198-201.

АНАЛІЗ ЗАХИЩЕНОСТІ КАБЕЛЬНИХ ЛІНІЙ ПЕРЕДАЧІ ДАНИХ ПЕРСОНАЛЬНОЇ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ МАШИНИ ВІД ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ

Перепадя В.І., Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Для типових моніторів сигнали з відеокарти передаються в аналоговому інтерфейсі по кабельній лінії зв'язку. Для передачі зображення на монітор використовуються сигнали інтенсивності для кожного з трьох основних кольорів - RGB (Red - червоний, Green - зелений, Blue синій), а також сигнали синхронізації горизонтальної (H) і вертикальної (V) розгорток. Склавши сигнали побічних електромагнітних випромінювань (ПЕМВ) каналів в просторі на виході розвідприймача можна отримати інформативний сигнал, що створює зображення , наприклад, тексту на екрані монітору. У загальному випадку такий сигнал досить просто декодувати зловмисникові навіть, коли в простір випромінюється сигнал тільки від одного з RGB каналу. При цьому втрачається тільки інформація про колір виведеного на екран зображення або тексту [1].

Метою доповіді є аналіз захищеності різних видів кабельних ліній зв'язку, що дозволить запропонувати засоби захисту від витоку інформації за рахунок побічних електромагнітних випромінювань.

В доповіді наводяться результати порівняння кабелів з трьома видами екранування. Діапазон частот: 10 – 1000 МГц.

№	Вид кабелю, екрану	Ослаблення, дБ	$K_{екр}$, рази	Коефіцієнт зменшення відстані розвідки ПЕМВ
1	Оболонка	25-40	17.8-100	0,056-0,01
2	Оболонка з фольгою	70-100	$3{,}16x10^{3}$-10^{5}	$0{,}32x10^{-3}$-10^{-5}
3	Потрійний екран	105-120	$1{,}78x10^{5}$-10^{6}	$0{,}56x10^{-5}$-10^{-6}

Наведені дані показують, що мінімальне екранування - у кабелів, що мають в якості екрану одну тільки оболонку. Максимальне екранування - у кабелів з потрійним екраном (фольга + оболонка + фольга). Варто особливо відзначити, що за рахунок належного екранування кабелю, суттєво зменшується відстань розповсюдження небезпечного сигналу. Це, в свою чергу, дає підстави знехтувати дослідженням ПЕМВ, породженими кабелем, оскільки достатньо встановити необхідний радіус контрольованої зони, де рівень випромінювання сигналу буде відповідати нормам захисту.

Список літератури

1. Ликов Ю. В., Сягаєва О. А. Анализ источников ПЭМИ в современных ПЭВМ. *Радіотехніка*. 2012. № 169. С. 196–207. DOI: https://openarchive.nure.ua/handle/document/13738

АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ У СИСТЕМАХ «РОЗУМНОГО БУДИНКУ»

Д'якова Н.Є., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком інформаційних технологій прагнення людей підвищити рівень зручності та безпеки проживання в будинках стало більш реальним. Сучасні компанії надають покупцям широкий діапазон можливостей, які здатна виконувати система домашньої автоматизації. Це викликало збільшення попиту на високотехнологічні системи. Протягом останніх років концепція «Розумний будинок» почала стрімко розвиватися, що викликало виникнення виняткових проблем, основною з яких є підвищення загроз безпеці інформації. Проведений аналіз показав, що до основних загроз інформаційній безпеці «розумного будинку» відноситься порушення конфіденційності, цілісності та доступності інформації [1, 2].

Метою доповіді є проведення порівняльного аналізу загроз безпеки у системах «розумного будинку»

Проведений аналіз показав, що основними типами загроз безпеці в даних системах є виведення з ладу комунікаційного обладнання системи, витік персональної інформації або витік інформації про конфігурацію ІТ-систем «розумного будинку» [3, 4]. Розглядаються як внутрішні та зовнішні загрози. Виявлені загрози зіставляються з вразливостями системи, та визначаються, які властивості можуть порушувати ті чи інші загрози.

Для визначення необхідних засобів захисту проводиться оцінка ризиків. Ґрунтуючись на результатах проведеної оцінки ризиків, визначаються найбільш небезпечні загрози. На основі отриманих даних розглядаються захисні заходи для зниження ризиків, пов'язаних з реалізацією даних загроз [5].

Список літератури

1. Стариковский А.В. Исследование уязвимостей систем умного дома [Текст] /А.В. Стариковский, И.Ю. Жуков, Д.М. Михайлов, А.М. Толстая, Ф.В. Жорин, В.В. Макаров, А.Б. Вавренюк // Спецтехника и связь. 2012. №2. С. 55-57.

2. Liu, Y. Study on smart home system based on internet of things technology. In Informatics and Management Science IV; Du, W., Ed.; Springer: London, UK, 2013; Volume 207, pp. 73–81

3. О.В Сєвєрінов, В.М. Федорченко, В.І. Перепадя. Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків. Системи озброєння і військова техніка, 4 (2016): 42-45.

4. Adams, C. E. (2002). Home area network technologies. BT Technology Journal, 20(2), 53–72.

5. V. Poddubnyi, O. Sievierinov, O. Pustomelnik. Менеджмент вразливостей як складова частина політики безпеки ІТС. Системи управління, навігації та зв'язку. Збірник наукових праць, 4.62 (2020): 55-58.

АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ В СИСТЕМАХ БЕЗКОНТАКТНОЇ ПЕРЕДАЧІ ДАНИХ

Метик А.В., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Технологія NFC стає популярною в сучасному світі та з кожним днем її застосування набирає обертів. На сьогоднішній день існує безліч напрямків, де застосовується NFC, наприклад безконтактна оплата в магазинах, оплата проїзду, контроль якості, контроль доступу та інше.

На даний час існує безліч загроз безпеці інформації при безконтактній передачі даних [1, 2]. Основні з них зчитування приватної інформації та доступ до майна. Проблемами використання NFC-систем є:

- застосування небезпечного протоколу UDP;
- відсутність шифрування транзакцій між хостом і клієнтом;
- відсутність легкої автентифікації хостів і користувачів;
- надання дозволів відповідно до звичайних правил доступу.

Метою доповіді є аналіз методів захисту інформації при безконтактній NFC-передачі даних. На основі проведеного аналізу були отримані основні вразливості системи NFC до атак, та методи захисту від даних атак на систему [3, 4]. Аналіз показав, що одним з найпростіших методів захисту від атак на систему NFC є маленька відстань між засобом зчитування та пристроєм або карткою користувача. Але це ні в якій мірі не гарантує захисту даних.

Основним методом захисту NFC-передачі даних є створення захищеного каналу для NFC. Для створення загального секретного ключа між двома пристроями використовується стандартний протокол узгодження ключа Diffie-Hellmann з подальшим симетричним шифруванням 3DES або AES.

В якості додаткових методів захисту можуть використовуватись створення токенів при кожній передачі даних, а також використання специфічних протоколів формування ключів NFC.

Але на даний час методи захисту NFC-систем потребують подальшого вивчення та вдосконалення.

Список літератури

1. О.В Сєвєрінов, В.М. Федорченко, В.І. Перепадя. Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків. Системи озброєння і військова техніка, 4 (2016): 42-45.
2. О.В. Сєвєрінов, А.Г. Хрєнов, А.О. Поляков. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі. Системи обробки інформації, 9 (2015): 101-104.
3. Технология NFC в смартфонах и ее практическое использование [Электронный ресурс] - Режим доступа: http://www.ixbt.com/mobile/nfc-2013.shtml
4. What is NFC? Everything you need to know [Электронный ресурс]. - Режим доступа: http://www.techradar.com.

ВИКОРИСТАННЯ СУЧАСНОГО ТРАНСПОРТУ ДАНИХ У ЗАХИЩЕНИХ СЕРВЕРАХ

Калінін І.М., Власов А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В сучасному світі постійно підвищуються вимоги щодо обробки великих об'ємів інформації, з формуванням нових підходів щодо зберігання, передачі, сортування та обробки інформації. Використання звичних для користувачів способів передачі файлів, зокрема REST API, стає слабким місцем у побудові захисту сучасних інформаційних систем [1]. Це потребує включення додаткових об'ємів інформації від сервера до клієнта, які не є важливими. Використання нових сучасних транспортів даних дозволяє зменшувати об'єми інформації та трафіку в мережі, використання ресурсів для її обробки. Більшість сучасних транспортів мають вбудовані системи фільтрації та пагінації, які дозволяють використовувати схеми віртуального завантаження даних [2]. Це дозволяє користувачам не зберігати зайві дані на своїх пристроях. Побудова запитів до серверів або хмарних систем зберігання даних на стороні клієнта також дозволяє збільшувати швидкість передачі даних, поліпшувати досвід користувачів. Розробник з використанням побудови запитів на стороні клієнту завжди розраховує на збіжний результат, але при цьому необхідно мати передбачувану модель даних що надсилаються.

В сучасних системах для захисту даних використовують токени, миттєві паролі та двох факторна автентифікація [1, 3]. Використання JWT-токенів під час запитів до захищеного серверу дозволяє перевіряти дані користувачів під час кожного запиту. Але використання токенів з обмеженим терміном дії у REST API потребує від користувачів повторного вводу паролів та даних.

Метою доповіді є розгляд переваг та недоліків під час розробки та використання сучасних систем передачі даних, окремих функцій та концепцій захисту інформації. В доповіді наводяться пропозиції щодо впровадження JWT-токенів з обмеженим терміном дії для підвищення захисту інформації. Це дозволить оновлювати токен користувача з кожним запитом до серверу, уникати його копіювання та розповсюдження серед учасників, поліпшувати моделі даних, змінювати підходи до формування аналітики дій користувачів.

Список літератури

1. Алина Грицай. Використання технології Fingerprint для аутентифікації у вебзастосунках//Наука онлайн: Міжнародний електронний науковий журнал - 2018. - №7. [Електронний ресурс] – Режим доступу до ресурсу: https://nauka-online.com/ua/release/2018/7/

2. Markus Winand We need tool support for keyset pagination. [Електронний ресурс] – Режим доступу до ресурсу: https://use-the-index-luke.com/no-offset

3. Безпека JSON Web Tokens (JWT). [Електронний ресурс] – Режим доступу до ресурсу: https://cyberpolygon.com/ru/materials/security-of-json-web-tokens-jwt/

ВАЛІДАЦІЯ ВВЕДЕННЯ ДАНИХ ТА ОБРОБКА ПОМИЛОК

Гапон А.О., Федорченко В.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Валідація даних - це належне тестування будь-якого вводу, наданого користувачем або додатком. Будь який ввід даних має розглядатися як загроза і варто перевіряти всі дані, що вводяться користувачем [1]. Обробка помилок під час введення - це процес перевірки, який забезпечує надання даних: для обробки має бути правильний тип і формат даних; дані входять в очікуваний і допустимий діапазон значень; введення не інтерпретується як код, як у випадку з ін'єкційними атаками; введення не маскується під альтернативні форми, які обходять заходи безпеки. **Метою доповіді** є проведення дослідження механізмів валідації введення даних та обробка помилок в даних, наданих користувачем або додатком. Перевірку введення і обробку помилок виведення можна розглядати як два основних і ефективних механізми захисту, які можна використовувати для пом'якшення безлічі програмних атак [2]. Варто використовувати неповні повідомлення про помилки, що містять тільки необхідну інформацію. Рекомендується перенаправляти помилки і виключення в призначене для користувача і стандартне місце обробки помилок і в залежності від контексту того, де ви увійшли в систему. Момент, в якому вводяться дані, критично важливий. Введення можна перевірити на клієнті, на сервері або на обох. Також недостатньо перевіряти введення тільки на стороні клієнта, оскільки це можна легко обійти і забезпечити мінімальний захист або її відсутність.

Список літератури

1. Whitehatsec. URL: https://www.whitehatsec.com/glossary/content/input-validation.
2. Cheatsheetseries Owasp URL: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html.

МОДЕЛЬ ЗАХИСТУ ДАНИХ У ДЕЦЕНТРАЛІЗОВАНІЙ ІНФРАСТРУКТУРІ ВІДКРИТИХ КЛЮЧІВ

Шафоростов М.О., Власов А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Як показує систематичний огляд літератури, присвяченої використанню технології блокчейн у кібербезпеці [1], криптографія з відкритим ключем – одна зі сфер, які добре підходять для нових застосовань блокчейна. Для забезпечення можливості надійно зв’язати відкритий ключ із його володільцем наразі здебільшого використовується ієрархічна інфраструктура відкритих ключів із довіреними центрами сертифікації (за стандартом X.509). Проте через централізовану архітектуру цій інфраструктурі властива проблема єдиної точки відмови, що зумовлює ризик припинення роботи всієї інфраструктури за компрометації кореневого центру сертифікації.

Мета доповіді – дослідження моделі захисту даних із використанням технології блокчейн, яка дозволяє реалізувати інфраструктуру відкритих ключів у децентралізований спосіб. У доповіді обґрунтовується одночасне використання двох розподілених баз даних (ланцюжка блоків і бібліотеки сертифікатів); розкриваються ролі учасників у системі, що застосовує досліджувану модель захисту даних; пояснюються особливості деяких модулів системи Bitcoin, які дають змогу забезпечити роботу інфраструктури відкритих ключів без центрів сертифікації. Також наводяться висновки щодо стійкості досліджуваної моделі захисту даних до хибних сертифікатних запитів, випереджальної реєстрації та шкідливої поведінки майнера [2].

Список літератури

1. Taylor P. J. A systematic literature review of blockchain cyber security. *Digital Comm. and Networks*. 2020. Т. 6, № 2. С. 147–156. DOI: https://doi.org/10.1016/j.dcan.2019.01.005.

2. B. Qin et al. Cecoin: A decentralized PKI mitigating MitM attacks. *Future Generation CS*. 2020. Т. 107. С. 805–815. DOI: https://doi.org/10.1016/j.future.2017.08.025.

СПОСОБИ ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Круглова Д.С., Панченко В.І.
Національний технічний університет «ХПІ», Харків, Україна

Одним з найбільш значущих класів інформаційних систем, які підлягають захисту від комплексних деструктивних впливів, виступають корпоративні інформаційні системи. Від їх успішного функціонування багато в чому залежить ефективність багатьох сучасних підприємств і організацій. Це масштабовані системи, призначені для комплексної автоматизації всіх видів господарської діяльності компаній, а також корпорацій, які потребують єдиного управління. Такі системи часто засновані на поглибленому аналізі даних, широке використання систем інформаційної підтримки прийняття рішень, електронний документообіг та діловодстві. Вони мають певну специфіку як об'єктів захисту від комплексних деструктивних інформаційних впливів, які постійно удосконалюються. На сьогодні не є рідкістю масштабні мережеві атаки на інформаційну інфраструктуру підприємств і держав. Як приклад можна привести DDoS-атаку потужністю понад 300 Гбіт / с, проведену в 2013 році проти організації Spamhaus [1]. Попри всі спроби захисту корпоративних інформаційних систем від таких комплексних деструктивних впливів вони не мають тенденцій до зниження. Постійне розширення функціональності інформаційних систем і наростання залежності від інформаційної інфраструктури створює ситуацію, коли атаки на цю інфраструктуру можуть призводити до наслідків, яке можна порівняти з наслідками терористичної активності [2, 3].

Список літератури

1. Сименко І. Одна з найбільших DDoS-атак в історії [Електронний ресурс]. URL: https://habrahabr.ru/post/174483/

2. Алексєєва І.Ю. та ін. Інформаційні виклики національній і міжнародній безпеці. М .: ПІР-Центр, 2001. 328 с.

3. Томас Т.Л. Стримування асиметричних терористичних загроз, що стоять перед суспільством в інформаційну епоху // Світова спільнота проти глобалізації злочинності і тероризму. Матеріали міжнародної конференції. 2002.

АНАЛІЗ МІКРОПРОЦЕСОРНИХ СИСТЕМ РЕЛЕЙНОГО ЗАХИСТУ СИЛОВИХ ТРАНСФОРМАТОРІВ

Шамаєв Ю.П., Уваров В.М., Береда В.О.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба, Харків, Україна

В даний час більшість використовуваних в Україні пристроїв радіорелейного захисту та автоматики електроенергетичних мереж відносяться до покоління електромеханічних і мікроелектронних реле і не відповідають сучасним науково-технічним вимогам. Один з напрямків їх удосконалювання – використання мікропроцесорів для виконання функцій релейного захисту й автоматики силових трансформаторів.

Цифрові пристрої мають переваги у порівнянні із системами, виконаними на традиційній елементній базі, у тому числі більш широкі експлуатаційні показники і можливість інтеграції їх у системи керування електроенергетичними об'єктами.

Метою доповіді є обґрунтування застосування мікропроцесорів у системах радіорелейного захисту силових трансформаторів та аналіз застосовуваних в Україні мікропроцесорних пристроїв та систем радіорелейного захисту силових трансформаторів.

В доповіді наводяться результати аналізу функціональних можливостей мікропроцесорних пристроїв та систем різних виробників, що застосовуються у силових трансформаторах.

Сучасні мікропроцесорні термінали є багатофункціональними пристроями, що реалізовують функції релейного захисту, автоматики, вимірювання, управління вимикачем і сигналізації на рівні одного приєднання. Окремі термінали захистів, що об’єднуються в локальну мережу, утворюють нижчий рівень координованої системи управлінні енергооб’єктом. Мікропроцесорні термінали, що випускаються різними фірмами, мають значною мірою співпадаючі функціональні можливості і виконані відповідно до одних і тих же стандартів і рекомендацій Міжнародної електротехнічної комісії.

Таким чином, мікропроцесорні пристрої захисту силових трансформаторів перевершують електромеханічні і мікроелектронні по точності, функціональним можливостям, мають менші споживання, вагу, працезатрати на монтаж, наладку і технічне обслуговування. Наявність зв'язку з вищим ієрархічним рівнем дозволяє включити такі пристрої в автоматизовані системи управління технологічними процесами електроенергетичних систем.

АНАЛІЗ ТЕХНОЛОГІЙ І ЗАСОБІВ ПРОТИДІЇ КІБЕРБУЛІНГУ

Гайкова В.В.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Однією з найгостріших проблем сучасності, що обумовлена широким використанням можливостей нових інформаційних технологій, є загроза потенційного зіткнення людини (користувачів будь якого онлайн сервісу або пристрою, що має з'єднання з мережею) з агресивними нападками окремих представників мережевої спільноти, або їх об'єднань, що називають кібербулінгом.

Кібербулінг [1] може здійснюватися, як за допомогою використання окремих інструментів (соціальні мережі, електронна пошта, різноманітні месенджери, звичайні текстові повідомлення, форуми, комп'ютерні ігри та ін.), так і втілювати концепцію багаторівневої – інтегрованої травлі (одночасне застосування або навпаки блокування декількох інструментів). В любому випадку, принциповим є те, що будь-яке онлайн середовище, яке дозволяє обмінюватися інформацією, може стати технічною платформою для здійснення Інтернет-травлі, з характерними для неї можливостями, щодо моніторингу та протидії проявам булінгу [2].

Метою доповіді є стислий огляд основних передумов, цілей і технік застосування різних видів кібербулінгу, та аналіз можливостей існуючих технологій і засобів протистояння його проявам.

Наведено узагальнені результати досліджень основних проявів булінгу в кіберсфері та надано аналіз специфіки і властивостей декількох технічних платформ. Підкреслено, що в сучасному світі жертвою Інтернет-травлі може стати будь-хто. Звернено увагу, що ризик стати жертвою кібербулінгу не залежить від будь яких антропогенних та соціально-політичних факторів.

Запропоновано короткий огляд існуючих технологій і засобів протидії цьому явищу. Проведено порівняння їх ефективності. Систематизовано критерії, яким повинна відповідати сучасна і ефективна технологія протидії кібербулінгу.

Представлені приклади вдалої реалізації захисту користувачів у деяких найбільш популярних соціальних мережах. Акцентовано увагу на тому, що для протидії кібербулінгу, в переважній більшості випадків, використовують технології захисту на основі обмежень. Головна мета відповідних засобів захисту полягає у тому, щоб максимально локалізувати небажаний контент (з точки зору існування ознак кібербулінгу) [2].

Список літератури

1. What is cyberbullying? // nuedusec. URL: https://nuedusec.com/blog/cyberbullying/, 11.02.2020

2. Гайкова В. В. Дослідження явища кібербулінгу і аналіз шляхів протидії його проявам: Пояснювальна записка до дипломної роботи бакалавра / В. В. Гайкова; ХНУ імені В. Н. Каразіна. – Харків: [Б. В.], 2020. – 64 с.

ПРИНЦИПИ ПОБУДОВИ ТА ЛОГІКА РОБОТИ ЧАТ-БОТУ З ПРОТИДІЇ БУЛІНГУ

Гайкова В.В., Малахов С.В.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Стрімкий розвиток інформаційних технологій привносить в суспільство багато позитивних та корисних тенденцій, однак, нажаль, він має і свої «темні» сторони, що приховані від непосвячених в парадигму сучасного цифрового світу. Однією з таких сторін, є проблема булінгу, яка в наслідок своєї еволюції «перейшла» в режим «онлайн», та відкрила нову, неприваблиу сторінку в технологічної історії людства – сторінку кібербулінгу [1].

Процес протистояння булінгу в кіберсфері, обумовлює необхідність постійного вдосконалення всіх відомих технологій протидії, включаючи і навчальні технології (наприклад, всілякі ігри, інтерактивні уроки, відео та ін.), які спрямовані на завчасне коригування "мережевої поведінки" користувачів різних інформаційних систем і онлайн сервісів [2].

Метою доповіді є стислий огляд основних складових, структури, видів контентного наповнення і базових принципів логіки роботи підліткового інтерактивного інформаційно-навчального чат-боту з протидії кібербулінгу.

Розглянуто склад і структура бази даних обробки таргетованих тематичних запитів. Виконано стислий аналіз принципів адаптації форми і змісту контентного відклику (форми і складності надання інтерактивних відповідей), в залежності від характеристик поточного з'єднання, та властивостей використовуваної технічної платформи користувачів. Розглянуто питання, стосовно принципів формування і оновлення тезауруса, в залежності від цільових вікових груп.

Зроблено аналіз характеру взаємозв'язку поведінкових сценаріїв чат-боту з наявним контент наповненням.

Наведено спрощену структуру черги накопичення і формалізації вхідних запитів.

Запропоновано дослідний варіант алгоритму поведінкової логіки «запису–стирання», та розглянуто його основні складові.

Виконана спроба узагальнення складу ситуативних сценаріїв чат-боту в залежності від структури та типового змісту черги накопичення вхідних запитів. На закінчення підкреслено, що явище кібербулінгу є дуже недооціненим і тому являє собою серйозну проблему сучасності [2].

Список літератури

1. What is cyberbullying? // nuedusec. URL: https://nuedusec.com/blog/cyberbullying/, 11.02.2020

2. Гайкова, В., & Малахов, С. (2020). Дослідження явища кібербулінгу і шляхів протидії його проявам. *Комп'ютерні науки та кібербезпека*, *1*(1), 14-32. https://doi.org/10.26565/2519-2310-2020-1-02

ДОСЛІДЖЕННЯ КОМБІНОВАНОГО МУЛЬТИПЛЕКСУ БЛОКІВ СТЕГАНОКОНТЕТУ

Гончаров М.О., Нарежний О.П.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Відомо, що одним з ефективних напрямів забезпечення приховування фактів передачі і зберігання інформації, є застосування різних стеганографічних методів. В межах доповіді розглядається цифровий напрямок стеганографії, а саме, дослідження властивостей малоресурсного алгоритму інкапсуляції статичних цифрових зображень в інші статичні зображення (контейнери) різного типу (структури).

Метою доповіді є розгляд результатів моделювання процедур стеганографічної вставки зображень з використанням несиметричної внутрішньоблокової обробки даних (розміри субблоков зображення-контейнера перевищують розмірність блоків контенту).

Відзначено, що такий варіант обробки помітно ускладнює локалізацію елементів інкапсульованого контенту, та розширює діапазон можливих налаштувань алгоритму. Даний режим обробки вимагає використання додаткових службових маркерів, що забезпечують оперативне вилучення прихованого контенту на етапі його декодування.

Для протидії процедурам неавторизованого детектування і вилучення прихованого контенту використано спрощений механізм міжблокової обфускації (тільки для опорних блоків зображення контейнера) [1]. При цьому вихідні блоки стеганоконтента вбудовуються не послідовно, а відповідно до варіанту маски мультиплекса, що генерується, та є одним з елементів складеного ключа дешифрування (вилучення) прихованої інформації. Як і у разі внутрішньоблокової обфускації, інформація про номер поточного варіанта маски міжблокового мультиплексу, зазначається у відповідній позиції заголовку файлу стеганоконтейнера. Підкреслено, що використання дворівневого мультиплексу прихованого контенту значно підсилює стійкість алгоритму до спроб його нелегітимною екстракції.

Звернуто увагу на необхідність виключення цифрового дисбалансу в «порожніх» і «повних» контейнерах, що призводе до виникнення труднощів у роботі лічильника блоків-контейнерів під час декодування контенту, та спрощення аналізу вмісту стеганокадру. Для усунення зазначених недоліків використано заповнення відсутніх позицій «баластним» вмістом, які є вихідними значеннями коефіцієнтів перетворення блоків зображення контейнера.

Список літератури

1. Morozov, D., Shaforostov, M., Malakhov, S., & Serbin, V. (2018). Подвійна обфускація трансформант малоресурсного стеганоалгоритма. Комп'ютерні науки та кібербезпека, 9(1), 22-34. Retrieved із https://periodicals.karazin.ua/cscs/article/view/12015

ДОСЛІДЖЕННЯ ПРОЦЕДУР ПОПЕРЕДНЬОЇ ПІДГОТОВКИ ВИХІДНИХ ДАНИХ ДЛЯ СТЕГАНОАЛГОРИТМА

Гончаров М.О.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Розглянуто питання попередньої обробки відеоданих, які забезпечують необхідні умови для поліпшення параметрів вставки приховуваного контенту при реалізації основних процедур дослідного стеганоалгорітма [1].

Метою доповіді є розгляд результатів моделювання процедур перетворень структури вхідних даних (потенційного контейнеру, та безпосередньо, зображення-контенту), що дозволяють забезпечити необхідні умови для одночасного вирішення двох завдань: - скорочення часу обробки (зменшення обчислювальної складності алгоритму); - ускладнення процедур аналізу і неавторизованої екстракції прихованого контенту.

Основним завданням етапу попередньої обробки даних, є зменшення кількості візуально малопомітних перепадів яскравості елементів вихідних зображень [2-3].

В цілому, ця процедура зводиться до реалізації згладжування малоінформативних областей зображень. Причому, в залежності від складності структури оброблюваних зображень (в даному випадку, значень ймовірності перепаду яскравості між сусідніми елементами [3]), параметри обробки можуть змінюватися.

Наведено результати моделювання для блоків розмірністю 3×3 елемента. Зазначено, що згладжене, зображення, формується шляхом циклічного повторення спеціальних процедур обробки, що застосовані до всього масиву вихідних даних (контейнера і контенту). Досліджено три варіанти реалізація процедур згладжування, з різним порядком взаємного порівняння складових елементів блоку, та різним способом перезапису їх змісту, при перевищенні заданих критеріїв подібності (відповідно для зображень контейнера і контенту).

Підкреслено важливість фактів локалізації присутності контурів та розглянуто можливість застосування симетричної і несиметричної предобробки вхідних масивів даних. Звернено увагу на те, що використовуваний механізм обробки характеризується простотою і забезпечує необхідні «стартові» умови для подальшого інкапсуляції стеганоконтента.

Список літератури

1. Morozov, D., Shaforostov, M., Malakhov, S., & Serbin, V. (2018). Подвійна обфускація трансформант малоресурсного стеганоалгоритма. Комп'ютерні науки та кібербезпека, 9(1), 22-34. Retrieved із https://periodicals.karazin.ua/cscs/article/view/12015

2. Зубарев Ю.Б., Дворкович В.П. Цифровая обработка телевизионных и компьютерных изображений. – М.: МЦНТИ, 1997. – 212 с.

3. Прэтт У. Цифровая обработка изображений. т.1,2. - М.: Мир, 1985. - 736 с.

ВЕРИФІКАЦІЯ ВІДБИТКИ ПАЛЬЦІВ ШЛЯХОМ МОДИФІКАЦІЇ АЛГОРИТМУ ДЕКОМПОЗИЦІЇ НАЙБЛИЖЧИХ МІНУЦІЙ

Мелкозьорова О.М., Малахов С.В.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

Розглядається проблематика, яка пов'язана з вирішенням завдань верифікації відбитків пальців [1]. Відзначено, що одним з можливих рішень, є використання методу знаходження найменшої найкоротшої відстані [2], якій дозволяє створити локальні структури для мінуцій, що входять в шаблон.

Метою доповіді є розгляд результатів моделювання процедур верифікації бази відбитків пальців, шляхом рішення задачі комівояжера з використанням модифікованого алгоритму декомпозиції оточення найближчих мінуцій.

Наведено змінений алгоритм рішення задачі методом гілок та границь, а саме вирівнювання і виключення дуг на кожному циклі пошуку оптимального маршруту. Верифікація базується на створенні локальних структур для кожної мінуції відбитку.

Підкреслено, що саме локальні структури мають стійкість до деформацій [3]. Проведено повний перебір шаблонів бази даних відбитків при їх верифікації цим методом.

Звернено увагу на те, що використання декомпозиції характерних ознак забезпечує більшу стійкість при дописуванні помилкових та стиранні справжніх мінуцій.

Підкреслено, що даний метод можна застосовувати для вирішення завдання верифікації відбитків пальців. До переваг даного методу можна віднести: - відносну простоту реалізації і швидкість обробки бази даних. Відзначено, що в ході експериментів, час на обробку всієї тестової бази даних склало порядку 42 с. У порівнянні з циліндричним кодом, повний перебір, тієї ж бази, займає близько 30 хв.

При вирішенні задачі верифікації, час повного перебору складає близько 2 хвилин, тоді як при обробці циліндричного коду, ця процедура може зайняти близько доби. До недоліків представленого методу слід віднести порівняно низьку точність отриманих результатів (EER = 33%). У зв'язку з цим підкреслено, що на отримання оптимальних умов для тестування програми необхідні серйозні витрати часу та ресурсів.

Список літератури

1. Melkozerova, O., Shlokin, V., Malakhov, S. Mathematical model of the biometric system of fingerprint authentication. Problems of informatization: abstracts of the reports of the seventh international conference on November 13-15, 2019, Pages. 92.

2. Мудров В.И. Задача о коммивояжере. – М.: Знание, 1969. - 61с.

3. Melkozerova, O., Rassomakhin, S. Identification of fingers on the basis of Hamiltonian cycles of local features. the Bulletin of KNU Series "Mathematical Modeling. IT. ACS". Bulletin of V. Karazin Kharkiv National University series «Mathematical Modelling. Information Technology. Automated Control Systems». 2019. Issue 44. Pages 51-65. https://periodicals.karazin.ua/mia/article/view/15767 - 20.06.2020.

ОСОБЛИВОСТІ СИНТЕЗУ ПОВЕДІНКОВИХ ПРОФІЛІВ HONEYPOT

Мелкозьорова О.М., Погоріла К.В.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

Розглядається проблематика протидії спробам неавторизованого моніторингу ресурсів корпоративної мережі за рахунок впровадження, в структуру що захищається, мережевих пасток (відомі, як Honeypot), які мають розширені можливості підтримки і корегування своїх поведінкових алгоритмів.

Метою доповіді є аналіз можливостей відомих Honeypot та розгляд особливостей синтезу відповідних поведінкових профілів для корегування роботи програмного аватару пастки на прикладі вузлу типу файл-сервер.

Підкреслено, що архітектура існуючих мережевих пасток, в цілому, достатньо добре відома [1], що в певній мірі обумовлює їх потенційну вразливість. Враховуючи це, звернено увагу на те, що наділяючи пастки більш варіативним сценарним контекстом і скорочуючи час мережевої експозиції можливо підтримувати їх потенціал в досить паритетному стані. Ці обидва напряму потребують більш щільної уваги (аналіз даних log-файлів і корегування алгоритмів роботи мережевого аватару пастки) зі сторони персоналу, та вимагають постійної підтримки його професійних компетенцій [2].

Зроблено акцент на те, що систематизація правил роботи мережевого аватару для кожної окремої пастки і періодична корекція наявних поведінкових профілів, є завданням, що важко формалізувати. В цьому сенсі, необачна уніфікація поведінкових профілів Honeypot, для кожного типу вузлів може суттєво полегшити зловмиснику ідентифікацію діючої пастки.

Тому наявність базового комплекту поведінкових профілів мережевих пасток, слід розглядати, не більше, як основу для подальшої модифікації її аватару під специфіку завдань, топологію та інші особливості кожної окремої мережі [3].

Підкреслено, що впровадження технології пасток не підміняє інших механізмів мережевої безпеки, а лише ефективно розширює наявний арсенал засобів мережевого моніторингу і протидії новим загрозам (насамперед, як інструмент попередньої розвідки і швидкого реагування на мережеві події).

Список літератури

1. Технология Honeypot, Часть 1: Назначение Honeypot. DOI: https://www.securitylab.ru/analytics/275420.php (дата звернення: 12.02.2021)

2. Рузудженк, С., Погоріла, К., Кохановська, Т., & Малахов, С. (2020). Особливості захисту корпоративних ресурсів за допомогою технології Honeypot. Комп'ютерні науки та кібербезпека, (4), 22-29. https://doi.org/10.26565/2519-2310-2019-4-03

3. Кохановська, Т., Нарежний, О., & Дьяченко, О. (2020). Дослідження можливостей технології Honeypot. Комп'ютерні науки та кібербезпека, 1(1), 33-42. https://doi.org/10.26565/2519-2310-2020-1-03

АНАЛІЗ МОЖЛИВОСТЕЙ СУЧАСНИХ HONEYPOT

Нарежний О.П, Мелкозьорова О.М.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Розглядаються питання моніторингу корпоративної мережевої активності на предмет виявлення ознак підготовки майбутнього вторгнення (атаки) до корпоративної мережі, шляхом організації і використання мережевих пасток (т.з. Honeypot), як на рівні окремих вузлів, так і цілої мережі пасток [1].

Метою доповіді є аналіз і узагальнення основних можливостей відомих Honeypot, та визначення особливостей їх подальшого розвитку, як засобу адаптивної протидії спробам атак, і вторгнень до корпоративних ресурсів.

Надано огляд особливостей використання різних програмних Honeypot і визначені їх основні класифікаційні ознаки.

Розглянуті особливості первинних налаштувань і умов функціонування декількох характерних комерційних засобів. За сукупністю результатів аналізу підкреслено, що основні переваги даної технології полягають в їх гнучкості та масштабованості.

Підкреслено, що архітектура відомих мережевих пасток, в цілому, достатньо відома, що обумовлює їх потенційну вразливість [2]. Звернено увагу на відсутність досконалих методик ідентифікації і швидкої компрометації мережевих пасток, які щільно обслуговуються персоналом, мають малий час експозиції, та підтримують можливість коригування їх поведінкових профілів [3].

Зроблено акцент на те, що тактика мережевої розвідки і методи здійснення атак постійно прогресують, тому, підтримку можливості адаптивної протидії Honeypot новим різновидам мережевих загроз, слід вважати одним із пріоритетних напрямків роботи для фахівців з питань корпоративної безпеки.

При цьому, впровадження Honeypot не підміняє собою інших технологій і інструментів безпеки, а лише ефективно розширює наявний арсенал протидії новим загрозам безпеки (перш за все, як інструмент швидкого реагування).

Підкреслено, що інтеграція Honeypot з іншими рішеннями безпеки корпоративних ресурсів (*Firewalls, IDS\IPS, DLP,* шифрування та ін.), є найбільш збалансованим варіантом підтримки потрібного рівня інформаційної безпеки.

Список літератури

1. Красоткин А. Черный лед // CHIP. – 2003. - №7. – С. 98-103.
2. Технология Honeypot, Часть - 2: Классификация Honeypot. https://www.securitylab.ru/analytics/275775.php (дата звернення: 12.02.2021)
3. Кохановська, Т., Нарежний, О., & Дьяченко, О. (2020). Дослідження можливостей технології Honeypot. Комп'ютерні науки та кібербезпека, 1(1), 33-42. https://doi.org/10.26565/2519-2310-2020-1-03

ПРИЙОМИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА ШЛЯХИ ПРОТИДІЇ ЇЇ ПРОЯВАМ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Погоріла К.В., Гайкова В.В.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Соціальну інженерію, в контексті проблематики забезпечення інформаційної безпеки (ІБ), можливо розглядати, як інструмент психологічного маніпулювання людьми з метою навмисного і системного створення умов для несвідомого виконання ними потрібних дій, або розголошення чутливої інформації (як корпоративної, так і особистої). Термін «соціальна інженерія», як акт психологічної маніпуляції, перш за все, пов'язаний з соціальними науками, але в наслідок масштабної інформатизації сучасного суспільства, його використання помітно поширилося і серед фахівців з питань ІТ та ІБ [1].

Метою доповіді є огляд основних передумов, цілей і технік застосування прийомів соціального інжинірингу, характерних для сучасних ІТ систем, та аналіз можливих шляхів протидії їх проявам. Розглянуто особливості соціального інжинірингу, як в контексті питань забезпечення вимог корпоративних політик ІБ, так в контексті проблематики протистояння кібербулінгу.

Підкреслено, що при використанні можливостей сучасних ІТ систем, кінцевою метою соціального інжинірингу, найчастіше є нелегітимні: - збір цільової інформації; - та\або доступ до потрібних функцій управління інформаційних систем; - та\або маніпулювання поведінкою людини (в т.ч. обслуговуючого персоналу цих ІТ систем та\або користувачів будь-яких онлайн сервісів). Звернено увагу, на той факт, що існує безліч способів реалізації відповідних атак, однак, всі вони мають загальний принцип - введення жертви в оману [1].

В доповіді розглянуто найбільш поширені, для сфери ІТ, техніки соціальної інженерії, перш за все: - «фішинг», «троянський кінь», «претекстінг» та «реверс-інжиніринг». Зроблено акцент, що основним способом захисту від проявів соціального інжинірингу є регулярні тренінги персоналу, та доступність актуальних регламентів і інструкцій з безпеки. Документація повинна регулярно оновлюватися і регламентувати дії співробітників для широкого кола інцидентів.

Технічна складова [2] протидії повинна передбачати підтримку актуальних версій програмного забезпечення та забезпечуватися коректним настроюванням елементів систем виявлення і запобігання атак (IPS\IDS), та засобів контентної фільтрації. Важливо максимально виважено обмежити права користувачів та сегментувати всі наявні ресурси.

Список літератури

1. Social Engineering: The Art of Human Hacking / Christopher Hadnagy. – Wiley Publishing, Inc., 2010. – 416 p.

2. Безопасная сеть вашей компании / Джон Маллери, Джейсон Занн и др.; пер. с англ. Е. Линдеманн. – М.: НТ Пресс, 2007. – 640 с.

ПЕРЕДУМОВИ, СПОСОБИ РЕАЛІЗАЦІЇ ТА ПРОТИДІЯ ІНСАЙДЕРСЬКИМ ЗАГРОЗАМ В СУЧАСНИХ УМОВАХ

Погоріла К.В.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

З кожним роком проблема розвитку кіберзлочинності, яка в своїх протиправних діях інтенсивно експлуатує людський фактор (соціальний інжиніринг) і використовує вразливості інформаційних систем, стає все більш актуальною. Це є наслідком цифровізації, практично всіх сфер діяльності сучасного суспільства. Особливу групу загроз в корпоративному сегменті безпеки посідає інсайд. Як свідчить дійсність [1], інсайдерські інциденти призводять до великих збитків, як репутаційного, так фінансового характеру.

Метою доповіді є, стислий огляд відомих випадків інсайду та аналіз основних передумов і способів його реалізації, характерних для сучасних інформаційних систем. Систематизовано можливі шляхи протидії його проявам.

Аналіз відомих випадків інсайду свідчить проте, що, як правило, інсайдери мають затверджені облікові дані та, нажаль, володіють більш високим рівнем довіри і повноважень доступу до наявних корпоративних ресурсів. В доповіді розглянуто три категорії інсайдерських загроз: - ненавмисні дії (*недбалість персоналу*); - свідома крадіжка облікових даних, що призводить до несанкціонованого доступу до чутливих ресурсів; - інсайдери-зловмисники, які навмисно завдають шкоди «своєї» організації. Звернено увагу на те, що за сукупністю мотивацій, що обумовлюють реалізацію цих загроз, є отримання будь-якої вигоди (*матеріальної, соціальної, репутаційної та ін.*), за допомогою продажу та\або оприлюднення чутливої інформації з метою досягнення бажаної мети. Підкреслена актуалізація проблематики інсайда, що обумовлено масовим переведенням співробітників на віддалений режим роботи, через пандемію COVID-19.

Розглянуті основні особливості організаційних і технічних методів протидії. Підкреслена важливість використання засобів контентної фільтрації, та розглянуто деякі принципові властивості відомих програмних і апаратних рішень.

Визначена необхідність постійного обмеження кількості користувачів, що мають доступ до конфіденційної інформації.

Зроблено висновок про те, що інсайдери продовжують являти собою постійну небезпеку корпоративнім даним, що обумовлює необхідність безперервного моніторингу цих питань та зміни тактики дій і оновлення положень корпоративної стратегії в області інформаційної безпеки.

Список літератури

1. Сергей Войнов. Инсайдерские угрозы 2020 года: как защитить конфиденциальную информацию в эру цифровизации. ComNews. 20.02.20. https://www.comnews.ru/content/204671/2020-02-20/2020-w08/insayderskie-ugrozy-2020-goda-kak-zaschitit-konfidencialnuyu-informaciyu-eru-cifrovizacii

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ

Прищепа О.Г.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

Наявність, а тем більш, використання ненадійного програмного забезпечення (в т.ч. того, що несе в собі ознаки не декларованих функцій), може суттєво знижувати рівень безпеки важливих та критичних інформаційних систем і цілих інфраструктур, до яких, можна віднести енергетичні, оборонні, транспортні, фінансові, комунікаційні та інше.

В сучасних умовах стрімкого технологічного розвитку, програмне забезпечення (ПЗ) стає все більш складнішим та більш об'ємним, а кількість пристроїв, які підключені до всесвітньої мережі, нестримно збільшується. Тому важливість забезпечення безпеки web-додатків збільшується в експоненційної залежності [1].

Крім того, швидке зростання обсягів одночасно виробленого ПЗ та постійне вдосконалення методів і способів його розробки, обумовлює потреби у швидкому, і безпомилковому виявленні та усуванні найбільш розповсюджених загроз.

Метою доповіді є аналіз сучасних методів пошуку вразливостей у web-додатках, та в цілому, ризиків, які пов’язані з найбільш розповсюдженими та\або суттєвими недоліками в захищеності існуючих веб-додатків.

Підкреслено, що головною метою є знаходження вразливостей, забезпечення безпеки зовнішніх інтерфейсів та самої безпеки мережі, тому що внутрішня частина веб-додатку може мати бази даних та додаткові мікросервіси.

Розглянуто характерні приклади виконання поширених різновидів атак на веб-ресурси і наведено рекомендації, стосовно організації захисту і зменшенню подібних ризиків, тобто виконання мінімізації ризиків веб-додатку.

Запропоновано склад, основні компоненти і основні способи реалізації статичного аналізу ПЗ.

Звернено увагу на той факт, що статичний аналіз не дає стовідсоткову впевненість в тому, що досліджене ПЗ є вразливим та\або зловмисним. Враховуючи це, зроблено висновок, що для забезпечення більш змістовного аналізу потрібно збирати якомога більше даних про структуру файлу, його можливі функції та ін..

Список літератури

1. .OWASP Foundation [Електронний ресурс] режим доступу: https://owasp.org/
2. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. - СПб.: Питер, 2020. - 448 с.
3. Яворски Питер. Ловушка для багов. Полевое руководство по веб-хакингу. - СПб.: Питер, 2020. - 272 с.

DDoS-АТАКИ: АНАЛІЗ ПОТЕНЦІЙНИХ СПОСОБІВ ЗАХИСТУ

Погоріла К.В., Рузудженк С.Р., Тесленко О.Ю.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

DDoS-атаки – найбільш поширений тип атак на сучасні комп'ютерні інформаційні системи [1]. Головною метою таких атак є перевантаження цільового корпоративного серверу (*серверу-жертви*), що призводить до тимчасової нездатності корпоративного ресурсу обробляти запити користувачів [2]. У доповіді розглянуто основні види DDoS-атак, що становлять загрозу втрати управління над ресурсом.

Перш за все, це атаки на додатки, що реалізуються з метою зміни або крадіжки чутливих корпоративних даних, а також атаки, які орієнтовані на порушення штатних режимів функціонування діючого каналу (-лів) зв'язку або протоколу (-лів) передачі даних.

Метою доповіді є розгляд та стислий аналіз основних типів найбільш відомих, на даний момент часу, DDoS-атак: – пінг-флуду, SMURF, HTTP- та осколкового флуду.

Представлено порівняльні характеристики визначених атак, в залежності від їх доступності на кожному рівні мережевої моделі OSI.

В межах доповіді звернено увагу на необхідність завчасного прийняття запобіжних заходів [3], вже на етапах конфігурації мережі [4-5] і запуску серверу, де збалансований вибір загальної стратегії захисту (*баланс між рівнем можливих наслідків інциденту, та рівнем і складністю впровадження заходів захисту, що залучаються*), допоможе не лише мінімізувати можливі наслідки неавторизованого втручання в роботу корпоративної IT-структури, а й чутливо знизити ризик проведення певних різновидів атак, що розглядаються.

Наведені приклади способів захисту для кожного з визначених типів DDoS-атак, які дозволяють виявляти атаку ще на початковій стадії, та запобігти її проведенню, і таким чином зменшити масштаби потенційних збитків. Авторами підкреслено особливу ефективність впровадження систем розподіленого захисту, що здатні відбити атаки достатньо великої потужності.

Список літератури

1. Хакеры по всему миру взвинтили цены на DDoS-атаки, ворованные данные и взломы серверов // URL: //cnews.ru/link/n521427, 11.01.2021

2. Иванов О. Что собой представляет DDoS-атака // URL: https://www.anti-malware.ru/analytics/Threats_Analysis/what-is-a-ddos-attack, 12.02.2021

3. Кибербезопасность: как защитить предприятие в эпоху Индустрии X.0 // URL: //cnews.ru/link/a16723, 13.02.2021

4. Безопасная сеть вашей компании / Джон Маллери, Джейсон Занн и др.; пер. с англ. Е. Линдеманн. – М.: НТ Пресс, 2007. – 640 с.

5. Chris Moore, Detecting Ransomware with Honeypot Techniques, DOI: https://ieeexplore.ieee.org/abstract/document/7600214

ОСОБЛИВОСТІ ІНТЕГРАЦІЇ ПІДСИСТЕМ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНИХ ДІЙ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ І КОМПЛЕКСАХ АВТОМАТИЗАЦІЇ

Сербин В.В.
ТОВ «NPS», Дніпро, Україна
Малахов С.В.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Сучасні комп'ютеризовані засоби діагностики і управління, які інтегровані до складу інформаційних систем і комплексів автоматизації, дозволяють підвищити загальний рівень безпеки їх експлуатації, мінімізуючи випадки виникнення позаштатних ситуацій, що виникають з вини обслуговуючого персоналу або дій неавторизованих осіб.

У цьому сенсі слід виділити роль і місце підсистем (засобів) захисту від несанкціонованих дій [1]. В якості характерних прикладів їх використання можна привести: - підтвердження процедур делегування повноважень зазначеним категоріям персоналу; - санкціонування виконання особливо важливих процедур управління (наприклад, підтвердження індикативних фінансових транзакцій); - ініціація запуску критичних технологічних процесів (наприклад, зміна поточного режиму роботи енергоагрегату); - забезпечення фізичного доступу до цінних вантажів, що транспортуються (віддалене спільне розблокування електронних пломб вантажу); - санкціонування змін в ієрархічній структурі ланок управління (наприклад, задіяння режиму «робота через інстанцію») і багато іншого.

Можливість підтримки зазначеного функціоналу, забезпечується шляхом комплексної інтеграції до складу «базових» систем і комплексів елементів підсистем (засобів) санкціонування повноважень. Глибина інтеграції, ступінь автономності, рівень делегованих повноважень і складність користувальницького інтерфейсу, таких підсистем (засобів) вимагають їх детального опрацювання на етапі формування технічного завдання.

Метою доповіді є стислий огляд різних варіантів інтеграції елементів підсистеми захисту від несанкціонованих дій в структуру базової системи.

Розглянуто основні особливості реалізації алгоритмів відповідних підсистем і порядок роботи обслуговуючого персоналу.

Підкреслено, що при загальній схожості базових ідей і цільових установок, особливості проектування зазначених підсистем (засобів), в кожному конкретному випадку, мають свою, яскраво виражену специфіку та обмеження.

Список літератури

1. В. В. Сербин, С.В. Малахов // Захист від несанкціонованих дій в сучасних інформаційних системах. Проблеми інформатизації. VII МНТК. 13-15.11. 2019. Том 1: секції 1-3. – Ч.: ЧДТУ. – 2019. – С.119.

МЕТОДИ ПОЛІПШЕННЯ ПОКАЗНИКІВ ЗАВАДОЗАХИЩЕНОСТІ НА ОСНОВІ ВИКОРИСТАННЯ СКЛАДНИХ НЕЛІНІЙНИХ СИГНАЛІВ

Замула О.А.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна
Родіонов С.В.
Український державний університет залізничного транспорту, Харків, Україна

Продуктивним кроком, з точки зору нового напряму використання систем сигналів, є синтез систем нелінійних складних дискретних сигналів. Завдання забезпечення необхідних показників завадозахищеності на рівні джерела сигналів традиційно вирішуються на основі збільшення відношення потужності сигналу до потужності завади на вході приймального пристрою, а також поліпшення спрямованості антен передавача і приймача. Тому, може створюватися враження, що у багатокористувачевих системах для досягнення необхідних показників завадозахищеності, можуть бути застосовані будь-які системи сигналів. Така різниця між відомим результатом щодо визначення завадостійкості і впливу властивостей сигналів на завадостійкість обумовлено двома основними допущеннями. По-перше, передбачалося, що взаємна завада нормалізується, і, по-друге, її спектральна щільність у загальній смузі частот є рівномірною [1]. Однак, як перше, так і друге припущення можуть не виконуватися і це, у значній мірі, визначається властивостями систем сигналів, які застосовуються. Саме тому, авторами досліджуються системи сигналів, які, саме завдяки притаманним їм статистичним властивостям кореляційних функцій, можуть знайти широке розповсюдження у інфокомунікаційних системах (ІКС).

Метою доповіді є побудова математичних моделей нелінійних дискретних складних сигналів, які дозволять враховувати особливості ІКС. **В доповіді** наводяться результати обчислень статистичних характеристик різних кореляційних функцій, а також структурних властивостей низки досліджуваних сигналів у ІКС [2]. Наведені дані показують, що використання нелінійних складних дискретних сигналів, зокрема, тих які надаються у даній роботі, дозволяє суттєво підвищити завадозахищеність прийому сигналів у сучасних ІКС.

Список літератури

1. Ipatov, Valery P. Spread Spectrum and CDMA. Principles and Applications / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electro technical University ‘LETI’, Russia. – John Wiley & Sons Ltd, The Atrium, Southern Gate, Chi Chester, West Sussex PO19 8SQ, England.

2. ISCI’2020: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko, Victor A. Krasnobayev and Alexandr A. Kuznetsov. Ivan Gorbenko and Alexandr Zamula. Theoretical Basis of Synthesis of Complex Signal Quasiortogonal Systems. ASC Academic Publishing, USA, 2020, 308 p. – ISBN: 978-1-7362833-0-1 (Hardback), ISBN: 978-1-7362833-1-8 (Ebook).

ОПТИМІЗАЦІЯ ЗА ЧАСОМ СИНТЕЗУ СИСТЕМ ДИСКРЕТНИХ СИГНАЛІВ ДЛЯ ЗАСТОСУВАННЯ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ

Замула О.А.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна
Родіонов С.В.
Український державний університет залізничного транспорту, Харків, Україна

Світові тенденції посилення загроз інформаційної та кібербезпеки, підвищення рівня вразливості інфо - комунікаційних систем (ІКС) обумовлюють необхідність розробки та впровадження нових моделей, методів і технологій управління телекомунікаційними мережами, інформаційною безпекою, інформаційного обміну, методів синтезу нових класів складних дискретних сигналів - переносників даних з необхідними властивостями. Знаходження дискретних сигналів з необхідними характеристиками кореляційних функцій зводиться, по суті, до перебору всіх можливих послідовностей, що належать деякій системі сигналів, і відбору тих послідовностей, які задовольняють відомим оцінками. При цьому обчислювальна складність таких методів значна [1].

У роботі наведено теоретичні основи синтезу і аналізу низки систем складних сигналів [2], а також методи оптимізації синтезу зазначених сигналів із застосуванням методів дискретного програмування, а саме, методу гілок і границь. Крім того, з метою поліпшення показників продуктивності формування і обробки сигналів запропоновано і наведено метод оптимізації за часом процесу синтезу систем сигналів із застосуванням процедури децимації [3].

Метою доповіді є побудова математичних моделей синтезу низки класів нелінійних дискретних складних сигналів.

В доповіді наводяться результати обчислень часових витрат на синтез систем сигналів із застосуванням отриманих методів. Наведені дані показують, що використання нелінійних складних дискретних сигналів, зокрема, тих які надаються у даній роботі, дозволяє суттєво підвищити продуктивність синтезу сигналів у сучасних ІКС.

Список літератури

1. Sarvate, D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Parsley // IEEE Trans. Commun. – 1980. – Vol. Com 68 – P. 59–90.

2. Gorbenko, I., Zamula, A., Morozov, V. Information and communication systems based on signal systems with improved properties building concept systems with improved properties building concept 2019 CEUR Workshop Proceedings.

3. І.Д. Горбенко, О.А. Замула, Хо Чі Лик Методи синтезу і формування систем нелінійних дискретних сигналів для сучасних інформаційно-комунікаційних систем // Радіотехніка: Всеукраїнський міжвідомчий науково-технічний збірник – 2020 р. - Вип. 203. – С. 126 – 132.

ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ І КІБЕР БЕЗПЕКИ НА ОСНОВІ КОНЦЕПЦІЇ RMF

Замула О.А., Величко А.В., Левченко І.І., Ткачов П.П.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна
Родіонов С.В.
Український державний університет залізничного транспорту, Харків, Україна

На сьогодні, на перший план при вирішенні задач забезпечення інформаційної і кібербезпеки, а також приватності виходить створення системи управління інформаційною безпекою (СУІБ), яка охоплює всю інфраструктуру компанії. СУІБ забезпечує збереження конфіденційності, цілісності й доступності інформації за допомогою запровадження процесу управління ризиками та надає впевненості зацікавленим сторонам, що ризиками належним чином управляють. NIST США розробив та впроваджує, як методологічну основу забезпечення інформаційної та кібербезпеки, концепцію Risk Management Framework (RMF) [1].

Концепція RMF: впроваджує структурований гнучкий підхід до управління ризиками; акцентує увагу на управлінні ризиками, створенні умов для забезпечення безпеки та приватності в інформаційних системах на всіх етапах життєвого циклу проектування системи (SDLC), підтримки інформування про безпеку та приватність на постійний основі за допомогою безперервних процесів моніторингу безпеки, наданні інформації вищому керівництву та керівникам відповідних підрозділів для прийняття рішень стосовно ризиків щодо процесів, ресурсів, персоналу організації, які виникають під час експлуатації та використання систем.

Метою доповіді є формулювання пропозицій щодо розробки та впровадження нормативних документів системи захисту інформації, які забезпечують імплементацію вимог міжнародних стандартів в галузі безпеки інформаційних технологій, передовий практичній досвід інших країн в галузі безпеки інформації та кібербезпеки.

В доповіді, на основі аналізу і узагальнення положень концепції RMF, сформульовано принципи і запропоновано методи забезпечення інформаційної і кібербезпеки, наведено рекомендації відповідно до реалізації основних кроків концепції RMF, трансформації вимог нормативних документів системи технічного захисту інформації, впровадження нових моделей та вимог безпеки у практичну діяльність із захисту інформації державних органів, установ, організацій, підприємств та розробників систем та засобів захисту інформації.

Список літератури

1. NIST Special Publication 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations, 2018.

ВИКОРИСТАННЯ МАЙНІНГ-ФЕРМ ДЛЯ ЗАВДАНЬ ОПАЛЕННЯ ПРИМІЩЕНЬ

Губка О.С., Губка С.О.
Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний університет", Харків, Україна

Зараз спостерігається бурхливий ріст і розвиток різних криптовалют, а також суттєве збільшення їх вартості. Багато людей добувають криптовалюту в домашніх умовах. Однак існує кілька побічних проблем, пов'язаних з майнінгом [1] в домашніх умовах.

Перша - майнінг-ферми, як правило, споживають велику кількість електроенергії і, як наслідок, скидають надлишки температури в атмосферу [2].

Друга проблема - блоки живлення ферм виробляють достатньо великий рівень шуму, оскільки вимагають постійного охолодження, а для цього використовуються потужні і продуктивні вентилятори. Ці проблеми завдають істотної шкоди комфорту проживання в будинку, де встановлені майнінг-ферми.

Метою доповіді є скорочення негативних факторів майнінг-ферм в домашніх умовах.

Обидві проблеми достатньо просто можна вирішити, при цьому не погіршивши основні параметри ферм. Для цього пропонується здійснити доопрацювання блоків живлення майнінг-ферм шляхом видалення з них вентиляторів і установки "емуляторів" для коректної роботи блоків. Отримані блоки живлення встановлюються в контейнер-теплообмінник відповідного розміру і заливаються спеціальним струмонепровідним мастилом (рідиною), яке забезпечує відвід надлишку тепла з блоків живлення і відведення тепла в систему низькотемпературного опалення (наприклад, колектор теплої підлоги). Таким чином, практично повністю усувається шум, а надлишок тепла дозволяє частково або повністю компенсувати витрати на опалення будинку або ж гаряче водопостачання.

Як показали експерименти для будинку площею 100 м2, необхідна потужність блоків живлення майнінг-ферм близько 8-10 кВт / год. Крім усього перерахованого вище також підвищується безпека функціонування майнінг-ферм в цілому, оскільки охолодження самих температурно навантажених компонентів істотно поліпшується.

Список літератури

1. Плахин Н.С., Кошар К.Д. Майнинг: технологические, финансовые и социальные аспекты. Актуальные проблемы гуманитарных и социально экономических наук, 2018, №5 С. 109-112. - https://www.elibrary.ru/item.asp?id=32794957

2. Самохин В.И., Самохин, Д.В., Бабкин Е.Е., Петров И.М. Актуальность вопросов энергосбережения на майнинг-фермах // Силовое и энергетическое оборудование. Автономные системы. 2019. Т.2, Вып. 2 С. 102-110. DOI: 10.32464/2618-8716-2019-2-2-102-110.

АНАЛІЗ ПРОГРАМНИХ І АПАРАТНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Пластінін О.В., Філоненко А.М.
Національний технічний інститут "Харківський політехнічний Інститут",
Харків, Україна

В роботі наведено аналіз програмних і апаратних засобів захисту інформації, які є перспективним методом використанням в сфері інформаційних технологій. Метою цієї роботи є захищеність програмних і апаратних засобів захисту інформації, що є безпекою і захищеностю благополуччя, а часом і життя багатьох людей. Така плата за ускладнення і повсюдне поширення автоматизованих систем обробки інформації.

Під інформаційною безпекою розуміється захищеність інформаційної системи від випадкового або навмисного втручання, що завдає шкоди власникам або користувачам інформації.

Сучасна інформаційна система являє собою складну систему, що складається з великого числа компонентів різного ступеня автономності, які пов'язані між собою і обмінюються даними [1-5]. Практично кожен компонент може піддатися зовнішньому впливу або вийти з ладу. На практиці найважливішим є три аспекти інформаційної безпеки: 1) доступність; 2) цілісність; 3) конфіденційність. Порушення цих параметрів можуть бути викликані різними небезпечними впливами на інформаційні комп'ютерні системи.

Даний аналіз покладено в основу розроблених моделей і методів. Розроблені наступні множини моделей: моделі багатоверсійних систем, теоретико-множинні моделі оцінки надійності засобів захисту інформації, моделі надійності та функціональної безпеки програмно-технічних комплексів і апаратних засобів захисту інформації.

Перелічені множини моделей аналізу програмних і апаратних засобів захисту інформації покладено в основу розробленої множини методів: методу аналізу надійності програмних засобів захисту інформації за урахування вторинних дефектів, методу оцінювання надійності аналізу програмних і апаратних засобів захисту інформації; методів вибору параметрів аналізу ,методи верифікації, оцінювання та забезпечення надійності і функціональної безпеки програмних і апаратних засобів захисту інформації.

Список літератури

1/ http://www.tnu.in.ua, http://pmf.uad.lviv.ua,

2. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практичний.посібник./ За заг. ред. проф. Я.Ю. Кондратьєва. – К., 2004.

3. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2006.

4. К. Мандиа, К. Просис. Защита от вторжений. Расследование компьютерных преступлений.– М., 2005.

5. Луцкер А. Авторское право в цифровых технологиях и СМИ. – М., 2005.

КОМП'ЮТЕРНА КІБЕРБЕЗПЕКА З ВИКОРСТИННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Прищепенко Я.С., Подорожняк А.О.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

Штучний інтелект (ШІ) використовується в багатьох сферах людської діяльності. Машинний розум – це зручний, швидкий і часто більш вигідний в порівнянні з людиною інструмент [1]. Знайшлося йому застосування і в сфері кібербезпеки.

Так, за допомогою ШІ багато компаній забезпечують більш надійний захист своїх баз даних, розвантажуючи аналітичні відділи за рахунок автоматизації виконання рутинних завдань. Перевага ШІ – в його здатності працювати швидше людини і постійно розвиватися. Машинний розум здатний значно випереджати традиційні системи прогнозування та реагування. Так що завдяки тому, що компанії активно вивчають питання запровадження та застосування ШІ в рамках комплексу заходів щодо забезпечення кібербезпеки, якість прогнозування і швидкість реагування будуть рости [2].

Метою доповіді є побудова програми та використання алгоритмів штучного інтелекту, які дозволять виявити несанкціонований доступ до даних, які знаходяться на комп'ютері.

В доповіді наводяться результати виявлення штучним інтелектом проникнення в систему.

Для виявлення кібератак традиційно виділяють два підходи: детерміністський та імовірнісний. В рамках першого зазвичай використовують сигнатури – унікальні послідовності байтів, що описують шкідливі об'єкти (файли, процеси, мережеві з'єднання, ключі в системному реєстрі Windows, об'єкти синхронізації), які дозволяють однозначно ідентифікувати відомі кібератаки в автоматичному режимі. Другий підхід в основному використовується для блокування невідомих погроз або погроз нульового дня при націлених атаках, коли ми заздалегідь не знаємо індикаторів компрометації. Як випливає з назви, даний підхід дозволяє виявляти нові кібератаки з певною ймовірністю, залишаючи останнє слово за користувачем системи або фахівцем з кібербезпеки. Якраз імовірнісний підхід і відкриває широке поле використання ШІ для забезпечення кібербезпеки комп'ютерних систем.

Список літератури

1. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. – СПб.: Питер, 2018. – 480 с.

2. Шевченко А.С., Самойлов І.В., Пономарьов О.А., Науменко О.Г. Аналіз застосування штучних нейронних мереж у задачах виявлення кіберзагроз. *Збірник наукових праць ВІТІ*. 2018, № 4. С. 141–146. URL: http://www.viti.edu.ua/files/zbk/2018/17_4_2018.pdf

SECURITY MECHANISMS OF VOIP-TELEPHONY

Bilash D.A., Tkachov V.M.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

The security of transferring data has a significant impact on the popularity of services of any type of telephony. Therefore, theoretical research of the increase of the degree of security is the important topic of the development of transferring data on the Internet [1]. While most of the technical hurdles appear to have been overcome, security still constitutes a major concern.

The purpose of this work is to analyze methods of increasing the security of IP-telephony. The most popular methods are using IP-security (IPsec) and secure real-time transport protocol (SRTP). IPsec is a framework for securing IP communications by encrypting and authentication each packet. There are two types of working. In the first mode, only payload packets are encrypted. That is a reason why this mode is suited for host-to-host over LAN. In the second mode, the entire IP packet is encrypted. Also, every IP packet needs to be encapsulated in a new packet for routing these packets. This method can be used for network-to-network, network-to-host and host-to-host over the Internet. SRTP provides the ability to encrypt transmitted messages, authenticate them, verify their integrity and prevent the possibility of playback attacks. Playback attacks carried out with interception and key substitution). But there is an important point in the work of SRTP it is the need to support encryption on both sides between which data transfers.

There is another well-known security mechanism that has well-served data networks is the use of NATs. When it secures a connection via this mechanism it needs to access the NAT. But there are DoS attacks which can cause lost this access. Authentication and identification can be used to prevent these attacks [2-3].

Thus, the development of VoIP- telephony provides a wide area of research on the topic of securing data that is transferring via the local area networks and over the Internet. Future researching will focus on increasing the errors tolerance and decreasing the delays in encrypting transferred data.

References

1. Кучук Г.А. Многошкальное вейвлет-моделирование трафика мультисервисных сетей / Г.А. Кучук, О.О Можаєв, А.А. Коваленко // Радіоелектронні і комп'ютерні системи. – 2009. – № 6(40). – С. 231-239.

2. Tkachov V.M. Automated Controllers Functioning Criteria in Content Distribution Systems / V.M. Tkachov, V.E. Savanevych // Scholars Journal of Engineering and Technology. – Volume-2: Issue-3A. – Apr-May; 2014. – Pp. 491-497.

3. Ткачёв В.Н. Анализ показателей качества передачи речевых фрагментов через пакетные IP-сети. Вероятность их идентификации / 14-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке», 18-20 марта 2010 г.: Сб. материалов форума. Ч.1. Конференция «Телекоммуникации» – Харьков: ХНУРЭ, 2010. – С.177.

ORGANIZATION OF TELEWORKING VIA VPN TECHNOLOGY

Hvozdetska K.P., Tkachov V.M.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

The COVID-19 pandemic has globally imposed a number of restrictions on population interaction. Among these measures, one can be noticed everywhere - social distancing.

Taking into account the fact that this leads to the impossibility of carrying out the current activities, in many fields of activity the remote work became actual. Teleworking was before the pandemic, it was even provided for a long time in the labor code in our country.

Although it was popular mainly in the IT field, it was taken over and adapted in many fields of activity. Today, practically, the economic activities that implemented teleworking can afford to hire an employee who is far from their location [1, 2].

The purpose of the report is to analyze a technical solution for secure remote user operation using tunnelling technologies in computer networks.

One of these solutions is VPN technology - a virtual private network [3]. Through this tool, the data transferred through the Internet are encrypted at a low level over the entire course of them through the Internet communications nodes.

Once arrived at the destination, the data is decrypted by the destination system, this being the only system in the world that holds the decryption key.

References

1. N. Kuchuk, O. Mozhaiev, M. Mozhaiev and H. Kuchuk, «Method for calculating of R-learning traffic peakedness,» 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 359-362.

2. Kuchuk G. Resource-Oriented Approaches to Implementation of Traffic Control Technologies in Safety-Critical I&C Systems / G. Kuchuk, V. Kharchenko, A. Kovalenko, A. Shamraev // Green IT Engineering: Components, Networks and Systems Implementation. Studies in Systems, Decision and Control series. Kharchenko, V., Kondratenko, Y., Kacprzyk, J. (Eds.). Springer International Publishing Switzerland, 2017. 355 p. Chapter 15 – Pp. 313-337. ISBN 978-3-319-55595-9, DOI: 10.1007/978-3-319-55595-9.

3. Ткачов В.М. Аналіз методів забезпечення відмовостійкості оверлейних мереж / В.М. Ткачов, К.П. Гвоздецька // Проблеми інформатизації : тези доп. 8-ї міжнар. наук.-техн. конф., 26-27 листопада 2020 р., м. Черкаси, м. Харків, м. Баку, м. Бельсько-Бяла. Т. 1 / Черк. держ. технолог. ун-т [та ін.]. – Харків, 2020. – С. 44.

4. Tkachov, V., Bondarenko, M., Ulyanov, O., & Reznichenko, O. (2019, December). Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) (pp. 161-165).

INCREASING THE FAULT TOLERANCE OF THE APPLICATION THAT DETERMINES THE OCCUPANCY OF THE COMMUNICATION LINE

Hunko M.A., Tkachov V.M.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Today, the number of mobile device users is growing every day. More and more web applications and sites are moving to mobile platforms.

However, the main task of a mobile device is to make calls. It would be convenient for users to use a special application and monitor whether a contact is talking or not.

The purpose of this paper is to review the means and methods to improve the fault tolerance of the software, which allows to determine the occupancy of the communication line. Let us first separate two concepts:

- Fault tolerance is the ability of a system, if one or more servers fail, to continue operating within the required parameters.

- Fault tolerant systems are those that have full redundancy (the so-called second shoulder) and are able to operate without significant drawdown in the event of a complete failure of one of the data centers.

In this paper, we will talk about a fault-tolerant application. The main problem that may arise is a bad Internet connection or no connection at all. In the first case it is necessary to create your own overlay network to buffer and control the data. When transmitting through your own overlay network, you may lose data transfer speed, but in this case, you can guarantee lossless data exchange.

Also, to reduce the load on the network and, as a consequence, to increase fault tolerance, it is necessary to send the smallest possible amount of data (send only on request).

For future studies it is proposed to investigate the localization of this application (whether it will not contradict the laws of this or that country, violate human rights and freedoms), as well as the possibility of creating this application without using the Internet or in conditions of low-bandwidth network channel.

References

1. Tkachov, V., Hunko, M., Volotka, V.: Scenarios for Implementation of Nested Virtualization Technology in Task of Improving Cloud Firewall Fault Tolerance. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), pp. 759-763. IEEE (2019).

2. Hunko M.A., Tkachov V.M. Development of a module for sorting the ipaddresses of user nodes in cloud firewall protection of web resources. Дев'ята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційнокомунікаційних технологій та засобів управління». 2019. С. 30.

FEATURES OF USING EXTREME PROGRAMMING IN SOFTWARE DEVELOPMENT

Krasnikov V.O., Chebotarova D.V.
Kharkiv National University of Radio Electroniks, Kharkiv, Ukraine

Extreme Programming, Extreme Programming, XP - Agile development methodology that took the best from agile development practices and leveraged them to the maximum - hence the word “extreme” in the name. Unlike other programming methods that can be used in a wide variety of startups and businesses, and in organizing personal affairs, XP is used exclusively in software development. There are four processes in extreme programming: coding, testing, design, listening. This methodology is characterized by high quality, teamwork and high quality.

The purpose of the report is to highlight the features and nuances in software development using the extreme programming method.

XP has some special practices, the most famous of which is pair programming. The bottom line is that two developers simultaneously work on the code for one product function: first one writes, and the second observes and fixes errors, and vice versa. Thus, in the process of creation, there are two solutions, at each stage the best is chosen [1].

Pair practice is carried out according to the principle: two are better than one. Another feature of extreme programming is that tests are created and prepared first, and then the code and the product itself. In this case, the tests are written by the programmers themselves. Testing provides an opportunity to fix almost all errors at the development stage. The third feature is collective code ownership. Each programmer in the team has access to the product code and everyone can make changes to it. But if suddenly corrections and changes led to an incorrect or incorrect project robot, then the one who made these changes should fix it [2]. Extreme programming also involves working on smaller releases. Moreover, the shorter the releases, the better the quality of the product. So the integration of new parts is the main feature and advantage of this methodology. Adding new functions and capabilities to the system at the highest possible speeds. As soon as all tests are passed with a satisfactory result, that the function works as intended, it is integrated into the system.

References

1. Подходы к разработке ПО: как правильно выбрать методологию разработки программного обеспечения [Електронний ресурс] // ISsoft. – 2019. – Режим доступу до ресурсу: https://issoft.by/blog/podkhody-k-razrabotke-po-kak-pravilno/.

2. Kent B. Test-Driven Development By Example / Beck Kent. – Boston: Addison-Wesley Professional, 2002. – 240 p. DOI: https://ptgmedia.pearsoncmg.com/images/9780321146533/samplepages/0321146530.pdf

МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У SCADA СИСТЕМАХ

Бовчалюк С.Я., Ляшенко О.С., Зятько С.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні системи контролю та збору даних (SCADA) є надзвичайно важливими для моніторингу та управління виробництвом, передачею та розподілом електроенергії. У епоху Інтернету речей SCADA перетворився на великі, складні та розподілені системи, які, крім нових загроз, схильні до звичайних. Для своєчасного та ефективного виявлення зловмисників надзвичайно помітним є механізм виявлення в режимі реального часу, здатний боротися з різними формами атак. Такий механізм повинен бути розподіленим, недорогим, точним, надійним та безпечним, з низькими накладними витратами на зв'язок, тим самим не втручаючись у роботу промислової системи.

Метою доповіді є аналіз існуючих методів та моделей виявлення вторгнень в складні системи керування. Пропонуються дві розподілені системи виявлення вторгнень (СВВ), які здатні виявляти атаки, що відбуваються в SCADA системі. Запропоновано архітектуру, засновану на системі виявлення вторгнень периметра в режимі реального часу (СВВПвРЧ), яка забезпечує основні можливості кібер-аналізу та виявлення, відповідаючи за постійну оцінку та захист електронного периметру безпеки кожного об'єкту інфраструктури. В якості частини СВВПвРЧ, було розроблено застосунок на мові Python. За час реалізації проекту було розроблено та протестовано два нові модулі, які базуються на One-Class SVM з використанням наборів даних з невеликого тестового стенду, який був створений, забезпечуючи засоби для імітації системи SCADA, що працює як у звичайних умовах, так і під впливом кібератак. Перший метод може відрізнити реальні від помилкових тривог, за допомогою методу із значеннями за замовчуванням для параметрів M та I в поєднанні з рекурсивним методом кластеризації. Цей метод сильно відрізняється від усіх подібних методів, які вимагають попереднього вибору параметрів із використанням перехресної перевірки або інших методів, що поєднують результати класифікаторів одного класу. Другий метод здатний виконувати виявлення вторгнення з високою точністю та низькими накладними витратами в часовому вікні, адекватному характеру систем SCADA.

Два представлені методи добре працюють за кількома сценаріями атак. Потрібно балансувати між високою точністю, низькою швидкістю помилкової тривоги, вимогами до спілкування в режимі реального часу та низькими накладними витратами в складних і, як правило, стійких ситуаціях атаки, необхідна комбінація декількох методів.

Список літератури

1. Казьміна Д.Р. Інтелектуалізація сучасних SCADA-систем / Д.Р. Казьміна, О.С. Ляшенко // VIII Міжнародна науково-технічна конференція «Проблеми інформатизації», 2020. – Т. 2 (4). – С. 66.

СЕКЦІЯ 5

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ЦИВІЛЬНІЙ БЕЗПЕЦІ

Керівник секції: д.т.н., проф. В. В. Косенко, ДП "ПДПРОНДІАВІАПРОМ"
Секретар секції: к.т.н., доц. Є. В. Доронін, ХНЕУ, Харків

ПИТАННЯ ЙМОВІРНОСТІ ЗНИЖЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ ТЕХНОГЕННОГО ХАРАКТЕРУ

Нестеренко С.В.
Харківський національний університет міського господарства
імені О. М. Бекетова, Харків, Україна

Прискорення темпів зростання масштабів господарчої діяльності, а також кількості великих виробничих комплексів, концентрації на них обладнання і установок великої потужності, використання у виробництві великої кількості потенційно небезпечних речовин постійно збільшує вірогідність виникнення техногенних аварій, які надають велику шкоду не тільки особам, які зайняті у виробництві, але й навколишньому середовищу [1].

Метою доповіді є проведення аналізу та вивчення питання ймовірності зниження НСТП при застосуванні дозвільної системи на виробництвах для запобігання аварій і катастроф.

Надзвичайні ситуації техногенного характеру виникають на хімічно небезпечних об'єктах, радіаційно небезпечних об'єктах, вибухопожежонебезпечних та пожежонебезпечних об'єктах, а також гідродинамічно небезпечних об'єктах. За останні 25 років значно зросла, також, небезпека від аварій і катастроф на виробництві і транспорті. На ситуації загальнодержавного рівня припадає близько 1 %, а регіонального - 4 % від загальної кількості аварій.

Подальше удосконалення дозвільної системи повинно здійснюватись на основі компромісу спрощення отримання дозволів і підтримки високого рівня вимог безпеки. Також велике значення має постійне навчання і перенавчання персоналу основним вимогам безпеки, викладених заводом-виробником в інструкціях з охорони праці, а також виконання вищевказаних робіт кваліфікованим персоналом [2].

Таким чином застосування дозвільної системи є важливим чинником у справі із зниження ймовірності виникнення надзвичайних ситуацій техногенного походження на виробництві, запобіганню аварій і катастроф.

Список літератури

1. Березюк О. В., Лемешев М. С. Безпека життєдіяльності: навчальний посібник.– Вінниця: ВНТУ, 2011. – 204 с.

2. Постанова КМУ від 26 жовтня 2011 р. № 1107 «Про затвердження Порядку видачі дозволів на виконання робіт підвищеної небезпеки та на експлуатацію (застосування) машин, механізмів, устаткування підвищеної небезпеки» (із змінами).

ІНФОРМАЦІЙНА КОМП'ЮТЕРНА СИСТЕМА МЕНЕДЖМЕНТУ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ ГОТЕЛЬНОГО ПІДПРИЄМСТВА

Сєріков Я.О., Сєрікова К.С.
Харківський національний університет міського господарства
імені О. М. Бекетова, Харків, Україна

Під безпекою життєдіяльності об'єкта в даному разі розуміється такий його стан в системі «готельне підприємство – середовище функціонування» з позиції забезпечення його здатності до стійкості існування й розвитку в умовах внутрішніх і зовнішніх загроз, дій комплексу непередбачуваних і важко прогнозованих негативних факторів [1].

Виходячи з такого визначення, до функцій, що забезпечуватимуть необхідний рівень безпеки життєдіяльності готельного підприємства, повинні бути реалізовані в такій інформаційній комп'ютерній системі, відносяться такі:

- виявлення та ідентифікація;
- попередження реалізації;
- зниження ефекту реалізації;
- нейтралізація; - припинення;
- локалізація;
- усунення загроз різного характеру дії [2].

Конкретно, відносно розглядуваного об'єкта, кінцевим завданням, метою такої інформаційної комп'ютерної системи є забезпечення безпеки гостей, персоналу, а також захист інформації, що є однією з найважливіших проблем готельного бізнесу на даний час [3]. Приймаючи до уваги комплексність і різнонаправленість завдань, є логічним формування архітектури такої системи за такими напрямками, тобто підсистемами: інформаційна комп'ютерна підсистема, що забезпечує інформацією в реальному масштабі часу постійне спостереження, належну обробку інформації, що відноситься до стану зовнішнього, навколишнього середовища об'єкта; інформаційна комп'ютерна підсистема, що забезпечує необхідними даними відносно внутрішнього стану безпеки функціонування об'єкта. Ця підсистема повинна включати складові, що стосуються надання інформації як стану безпеки технологічних процесів, виконання співробітниками своїх функціональних обов'язків, так і відносно захисту майна готельного підприємства; - інформаційна підсистема, завданням якої є забезпечення захисту інформації, що являє собою комерційну таємницю.

Список літератури

1. Сєріков Я.О., Коженевські Л. Ф. Безпека Життєдіяльності – Секюрітологія. Проблеми, завдання, шляхи вирішення: монографія. Харків : ХНАМГ, 2012. Ч. 2 332 с.

2. Сєрікова К. С., Сєріков Я.О. Інформаційні технології в забезпеченні безпеки при надзвичайних ситуаціях в готелях. VII міжнар. наук.-техн. конф. «Проблеми інформатизації». Черкаси – Баку – Бельсько-Бяла – Харків, 2019. Т. 3, С. 84.

3. Дement'єва С.В. Отельный менеджмент. Ольборг : Інститут історії, міжнародних і соціальних досліджень Ольборгського університету, 2011. 160 с.

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ІНСТРУМЕНТ ЗАХИСТУ РОЗРОБОК І НАУКОВИХ ДОСЯГНЕНЬ ГО ЗАКЛАДУ ВИЩОЇ ОСВІТИ

Сєріков Я.О.
Харківський національний університет міського господарства
імені О. М. Бекетова, Харків, Україна

На сьогодні якість, насиченість інформації, адаптування змісту дисциплін до зміни виробничого середовища в наданні освітніх послуг студентам закладом вищої освіти (ЗВО) є фактично одним з основних показників, що визначають його рейтинг.

В умовах широкої доступності до мережі Інтернету доступ до навчального процесу, наукової роботи вищого навчального закладу стали доступними практично кожному користувачу ІТ-технологій. У зв'язку з цим на одному з чільних місць знаходиться завдання забезпечення інформаційної безпеки освітніх, наукових матеріалів, іншої інформації, в тому числі обмеженого доступу, а також і самої ІТ-інфраструктури ЗВО від випадкових або спрямованих атак [1]. При вирішенні цього завдання необхідно враховувати ряд проблем, основними з яких є наступні [2]:

Проблема №1. Різні групи користувачів інформаційної системи вищого навчального закладу.

Проблема №2. Трансформація способів доступу і концепція «Будь-який пристрій».

Проблема №3. Захист інформаційних систем і інформації обмеженого доступу

Оскільки периметр традиційної мережі кампусу ЗВО є умовно окресленим і продовжує розмиватися, то і його інформаційне середовище поступово втрачає межі. Смартфони, планшети та ін. пристрої для одержання інформації з інформаційної мережі ЗВО активно змінюють навчальний процес, надаючи можливість доступу до навчально-методичних матеріалів з будь-якої точки простору. Все це направлене на підтримку й підвищення рівня конкурентоспроможності вищого навчального закладу при одночасному ускладненні завдання забезпечення належного рівня інформаційної безпеки. Таким чином, для забезпечення конкурентної переваги ЗВО в сучасних умовах необхідна розробка такої системи інформаційної безпеки, яка повинна забезпечувати реалізацію політики безпеки у всіх напрямках його роботи.

Список літератури

1. Крат Ю.Г., Шрамкова И. Г. Основы информационной безопасности : Уч. пособие. / ГОУ ВПО «Дальневосточный государственный университет путей сообщения». Хабаровск, Изд-во ДВГУПС, 2008. – 114 с.

2. Сєріков Я. О. Завдання забезпечення інформаційної безпеки вищого навчального закладу в проблемі підвищення рейтингу підготовки фахівців / Материалы VI Междунар. науч-теорет. Интернет-конф. «Місто. Культура. Цивілізація.» Харків : ХНУГХ, 2014. С. 175 – 178.

МОДЕЛЮВАННЯ ПРОЦЕСІВ ТЕПЛОПЕРЕНОСУ В ТЕРМОЕЛЕКТРИЧНИХ ПЕРЕТВОРЮВАЧАХ В УМОВАХ ЕКСПЛУАТАЦІЇ

Курська Т.М.
Національний університет цивільного захисту України, Харків, Україна

Однією з основних умов функціонування безпечної та надійної роботи атомних електростанцій (АЕС), а також систем електропостачання в цілому, є надійне функціонування систем управління технологічними процесами енергетичного комплексу.

Температурні вимірювання мають особливе значення не тільки для автоматичного регулювання технологічних процесів, а і систем контролю в цілому [1]. Температурні вимірювання складають близько третини усіх вимірювань на енергетичних об`єктах. Тому проблема надійності та вірогідності показань температурних перетворювачів є актуальною і має великий вплив на безпечну експлуатацію АЕС.

Однією з похибок при температурних вимірювань засобами контактної термометріє є неідеальний контакт спаю термоперетворювача з середовищем або матеріалом. Причини цих похибок можуть бути різні: деформації матеріалів, термічна напруга, виникнення тріщин в зоні контакту, невідповідність розмірів спаю термопари та термометричного вікна та ін.

Аналіз досліджень впливу цих факторів показав, що задачі, пов`язані з впливом неідеальності спаю термоперетворювачів на температурні вимірювання в умовах експлуатації є актуальними і не розглянуті на теперішній час у повній мірі.

Метою доповіді є побудова математичної моделі «спай термоперетворювача-проміжний шар-середовище», яка дозволить враховувати особливості впливу основних чинників, що є джерелом похибок в умовах неідеального контакту спаю та матеріалу на результати вимірів температури [2].

В доповіді наводяться розроблені моделі для аналізу впливу негативних чинників на похибку температурних вимірювань, які можуть використовуватись для подальшої корекції умов виміру, умов монтажу термоперетворювачів та ін.

Наведені моделі дозволять виявити причини похибок термоперетворювачів в агрегатах АЕС і мінімізувати їх.

Список літератури

1. Курська Т.М. Дослідження сучасних систем термоконтролю на об`єктах стратегічного призначення. Актуальні проблеми пожежної безпеки та запобігання надзвичайним ситуаціям в умовах сьогодення. 2020. С. 169–172. URI: http://repositsc.nuczu.edu.ua/handle/123456789/11955.

2. Курская Т.Н. Повышение точности температурного контроля с помощью СДТ на объектах энергетики. Проблеми надзвичайних ситуацій. 2009. Випуск 10. С. 112–118. URI: http://repositsc.nuczu.edu.ua/handle/123456789/2694.

ПІДВИЩЕННЯ БЕЗПЕКИ ВІЙСЬКОВОЇ СЛУЖБИ ШЛЯХОМ УДОСКОНАЛЕННЯ ЕЛЕМЕНТІВ РЕЧОВОГО МАЙНА ВІЙСЬКОВОСЛУЖБОВЦЯ

Галавська Л.Є., Котюх М.В.
Київський національний університет технологій та дизайну, Київ, Україна
Прохоровський А.С., Швиданенко О.А.
ТОВ «РА.ДА», Київ, Україна

На сьогодні, у час відстоювання територіальної цілісності нашої держави внаслідок збройного конфлікту на території українського Донбасу питання розвитку та постійного вдосконалення системи речового забезпечення військовослужбовця залишається відкритим. Адже на ефективність виконання повсякденних службових завдань й поставлених бойових задач та на безпеку військової служби в цілому впливає не лише рівень підготовки військовослужбовця, а й якісні характеристики екіпірування та рівень динамічної відповідності та комфортності речового майна.

Значні фізичні навантаження та випадки знаходження військовослужбовця протягом тривалого відрізку часу в обмеженому просторі бойової техніки пов'язані з ризиком накопичення вологи у підодяговому просторі, розвитку патогенної мікрофлори (бактерії, гриби) та появи неприємного запаху поту. Тому нижня білизна військовослужбовця є першим, особливо важливим, шаром у складі речового майна, що сприяє оптимізації мікроклімату тіла, вологообміну та швидкому висиханню шкіри.

Метою роботи є удосконалення конструкції та функціональності нижньої білизни, що дозволить підвищити безпеку військової служби в умовах бойових дій в районі Операції Об'єднаних сил.

У доповіді наведено аналіз існуючих зразків нижньої білизни військовослужбовців Збройних сил України, інших військових формувань та правоохоронних органів [1] на підставі затверджених технічних умов на виготовлення нижньої білизни, до складу якої входять труси [2] та фуфайка з короткими рукавами [3]. Запропоновано удосконалену конструкцію нижньої білизни з використанням інноваційного виду сировини (волокон «DEO-W») для її виготовлення.

Список літератури

1. Про затвердження Зразків військової форми одягу та загальних вимог до знаків розрізнення військовослужбовців та ліцеїстів військових ліцеїв. Наказ Міністерства Оборони України. Електронний ресурс: https://ips.ligazakon.net/document/view/RE30915?an=709.

2. Труси з трикотажного бавовняного кулірного полотна. Технічні умови ТУ 14.1-00034022-086:2015. Електронний ресурс: https://www.mil.gov.ua/content/tenders/TO_trousers.pdf.

3. Фуфайка (з короткими рукавами) з трикотажного бавовняного кулірного полотна. ТУ У 14.1-00034022-081:2015. Електронний ресурс: https://www.mil.gov.ua/content/tenders_2019/tu_f_bav.pdf.

ВПРОВАДЖЕННЯ НОВІТНІХ ТЕХНОЛОГІЙ В ПРОЦЕС РОЗМІНУВАННЯ ВОДНИХ АКВАТОРІЙ УКРАЇНИ

Соловйов І.І., Стрілець В.М.,Стецюк Є.І.
Національний університет цивільного захисту України, Харків, Україна

Друга світова війна відзначалася широким застосуванням мінної зброї сторонами протистояння: СРСР, Румунією, Німеччиною (і навіть формально нейтральною Болгарією). Кількість мін усіх типів, виставлених супротивниками з 1941-го по 1944-й на Азовському та Чорному морях, становила 37 407 штук [1]. З них на СРСР (Чорноморський флот) припадало 10 745 мін. Зокрема, 8 388 було поставлено в оборонних мінних загородженнях біля своїх баз, решту — на морських комунікаціях противника [2].

Процес очищення Азовського та Чорного морів від мін тривав не один рік, утім, остаточно назвати його завершеним не можна й до цього часу. Іноді все ще трапляються вибухи й гинуть кораблі.

Відомо про три підтверджені аварійні випадки з кораблями Чорноморського флоту, що сталися вже після війни через плаваючі міни: йдеться про один підводний човен та два торпедні катери.

Ще шість випадків вважаються ймовірними. Так, у 1949-му поблизу Севастополя на міні підірвався суховантаж «Анатолий Серов», у 1951-му під Новоросійськом — «Бакинский комсомолец», а у 1959-му на траверзі Сочі — «Краснодон».

Метою доповіді є ознайомлення з аналізом надзвичайних ситуацій, які відбулися внаслідок підводного розташування вибухонебезпечних предметів, які залишилися у водних акваторіях після Першої та Другої світових війн та військової агресії Росії на сході нашої країни.

В доповіді наводиться детальний опис багатоцільової системи керування човнами UAPS 20 A, яка дозволяє одночасне керування до 15 автономних (безпілотних) човнів з відстеженням центральною моніторинговою станцією (CMS) всіх 15 човнів та безпілотних модульних систем ULISSE, які разом з програмним забезпеченням ORAMIN дозволяють планувати та оцінювати ефективність зачистки/глушіння вибухонебезпечних предметів; дозволяють створити нелінійний алгоритм оцінки ефективності імітації сліду корабля у порівнянні зі справжнім слідом; проводити ідентифікацію та визначення місць розташування акустичних та магнітних мін.

Список літератури

1. Robert A. Forczyk. Sevastopol 1942, vonManstein'striumph. Osprey: Oxford 2008. P. 121-123. Availableat: https://www.amazon.com/Sevastopol-1942-Mansteins-triumph-Campaign/dp/1846032210

2. Howard S. Levie. MineWarfareatSea. MartinusNuhoffPudlishers, 1992. P. 119. Availableat: https://www.amazon.com/Mine-Warfare-Sea-Howard-Levie/dp/079231526X

РОЗРОБКА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПОПЕРЕДЖЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ ТА ПОЖЕЖ В ЕНЕРГОПЕРЕВАНТАЖЕНИХ ПРИМІЩЕННЯХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вовчук Т.С., Шевченко Р.І.
[1]Національний університет цивільного захисту України, Харків, Україна
Зобенко О.О.
Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля НУЦЗУ, Черкаси, Україна

Проведений аналіз статистики пожеж в Україні показує стійку тенденцію до збереження кількості пожеж від джерел запалення електричного походження.

Незважаючи на розвиток сучасних апаратів захисту електричні розетки залишаються одним з місць, де в наслідок появи великого перехідного опору можуть відбуватися значні тепловиділення. Підвищення температури штепсельного з'єднання може стати причиною самозаймання деталей розеток та оздоблювальних матеріалів.

Водночас питанням зменшення небезпеки роз'ємних контактних з'єднань не приділено значної уваги [1-5], тому необхідно здійснити пошук інформаційних та технічних рішень, які б дозволили попередити виникнення загорань внаслідок надмірного нагрівання контактів електричних розеток.

Для попередження небезпечного тепловиділення запропоновано обладнати електричну розетку температурними запобіжниками, які спрацьовуватимуть при перевищені допустимої температури з'єднання і припинятимуть подальше нагрівання шляхом розмикання електричного кола.

З метою обрання оптимальних характеристик температурних запобіжників необхідно розробити інформаційну технологію, яка здатна визначити умови, при яких забезпечуватиметься нормальна робота з'єднання штепсель-розетка для тривалих максимально допустимих навантажень та відбуватиметься розмикання електричного кола за умови досягнення граничного значення температури.

Список літератури

1. Умная Wi-Fi розетка TP-Link HS110 URL: http://www.era.kh.ua/power/filters/tp-link-hs110--115168.html.

2. Broadlink SP Contros умная Wi-Fi розетка. URL: http://www.mybuy24.net/catalog/umnyy-dom/broadlink-sp-contros-umnaya-wi-fi-rozetka/

3. Беспроводная розетка Chuango E5 Wi-Fi. URL: http://www.antaresgroup.ru/en/product/gprs-wi-fi-besprovodnaja-rozetka-chuango-e6/

4. Fibaro Wall Plug FGWPE-101 управляемая розетка URL: http://www.mybuy24.net/catalog/umnyy-dom/fibaro-wall-plug-fgwpe-101-upravlyaemaya-rozetka.

5. GSM розетка с дистанционным управлением ДУ и датчиком температуры «Домовой» URL: http://ohrana.ua/ppk/gsm-rozetka-domovoj.html.

АКТУАЛЬНІСТЬ ПИТАННЯ РОЗРОБКИ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПОПЕРЕДЖЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ З ВИКОРИСТАННЯМ БАГАТОФУНКЦІОНАЛЬНИХ ЗАХИСНИХ ПРИСТРОЇВ

Мирошниченко А.О., Шевченко Р.І.
Національний університет цивільного захисту України, Харків, Україна

Однією з серйозних загроз сучасного суспільства є тероризм. Майже щоденно здійснюються терористичні акти, унаслідок яких гинуть люди. Більшість цих злочинів здійснюються як з використанням вибухових пристроїв, так і шляхом розпилення небезпечних хімічних речовин. Нерідко це саморобні, нестандартні пристрої, що їх складно виявити, знешкодити або ліквідувати. Крім цього, сучасною тенденцією є створення таких пристроїв, в яких вибухова частина ініціює викид небезпечних речовин. В більшості випадків такі терористичні пристрої є малогабаритними [1-3].

Напружена воєнно-політична ситуація, в умовах якої наша держава відстоює власну територіальну цілісність і суверенітет, характеризується значним зростанням рівня таких загроз зловмисних дій, як вчинення терористичних актів і диверсійних операцій на території України, спрямованих на дестабілізацію економіки, підрив стабільності в суспільному житті і функціонуванні транспортних та інформаційних комунікацій, формування негативної думки про нездатність державних інститутів захистити своїх громадян. Особливий резонанс набувають події, що відбуваються в місцях масового скупчення людей, тобто аеропортах і вокзалах, метрополітенах і площах, торгових центрах і супермаркетах, театрах і розважальних центрах, стадіонах і кінотеатрах, в місцях проведення концертів, спортивних змагань і політичних маніфестацій [4, 5]. Тому особливої актуальності на часі набувають наукові дослідження з розробка нових інформаційних технологій попередження надзвичайних ситуацій терористичного характеру в місцях масового перебування людей з використанням спеціальних захисних пристроїв різного функціонального призначення.

Список літератури

1. Xiao T., Horberry T., Cliff D. (2015) Analysing mine emergency management needs: a cognitive work an alysis approach // International Journal of Emergency Management (IJEM). Vol. 11. P. 191–208.

2. Toan Dang Qua.(2015) Train-the-Trainer Trauma Care Programin Vietnam // Journal of Conventional Weapons Destruction. Vol. 19. P,12-24.

3. Operation Viking Hammer. URL: https://en.wikipedia.org/wiki/Operation_Viking_Hammer

4. LTTE used CS Gas to attack Soldiers. URL: http://lankadailynews.com/2008/09/ltte-cs-gas-attack-soldiers/

5. Europol, TE-SAT 2016, European Union Terrorism Situation and Trend Report 2016, 2016. doi:10.2813/525171

РОЗРОБКА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПОПЕРЕДЖЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ МЕДИКО-БІОЛОГІЧНОГО ХАРАКТЕРУВ РЕГІОНІ З НЕСТІЙКИМИ ПРИРОДНО-КЛІМАТИЧНИМИ УМОВАМИ

Прокопенко О.В., Шевченко О.С., Шевченко Р.І.
Національний університет цивільного захисту України, Харків, Україна

Стрімке поширення у світі епідемії COVID-19 змушує вкотре переглянути існуючі підходи до проблеми протидії надзвичайним ситуаціям медико-біологічного характеру [1].

Загальний підсумок - світова система протидії небезпеці, яка, в силу відсутності попередніх малих спалахів, не мала превентивного запобігання на стадії вакцинації населення, виявилась не спроможної у короткий термін та в рамках окремої території локалізувати поширення епідемії та мінімізувати людські жертви [2, 3]. Втім світовий досвід доводить, що жорсткі заходи, насамперед з організації індивідуального карантину первинних та вторинних джерел поширення медико-біологічної небезпеки дали позитивну тенденцію щодо стримання подальшого розвитку небезпеки. Прикладом врахування та системного поширення попереднього досвіду боротьби з небезпека медико-біологічного характеру є створення системи інформаційної підтримки населення та дій управління заходами протидії DORSCON, яка уявляє собою систему з кольоровим кодуванням, яка показує поточну ситуацію із захворюванням [4,5]. Втім запропоновані у роботах підходи залишили поза увагою проблему управління станом існуючих критично необхідних ресурсів, з урахуванням інформації, яка надходить з зони поширення небезпеки у разі виникнення нестійких погодно-кліматичних умов.

Об'єктивна складність процесів попередження надзвичайних ситуацій медико-біологічного характеру, а також потреба у ефективній протидії стрімкому поширенню у світі епідемії COVID-19 породжують необхідність розробки інформаційної технології попередження надзвичайних ситуацій медико-біологічної характеру, особливо в регіонах з нестійкими (складними) погодно-кліматичними умовами, шляхом запровадження технології ресурсно-критичного управління заходами попередження на основі QR-кодування.

Список літератури

1. Shakhnovich I.V (2006) Modern wireless technology. M. 288 p.

2. Vishnevsky V.M, Portnoy S.L, Shakhnovich I.V. (2009) WiMAX Encyclopedia: The Road to 4G M. 472 p.

3. Pospelov B.B, Shevchenko R.I (2011) Development of information and communication technologies for the civil protection system of Ukraine in emergency situations. / Emergency problems. Sat. of sciences. Kharkiv Ave. P. 135-142.

4. Model Gleam. (2020). URL:http://www.gleamviz.org/model/.

5. Nature Outlook 555, S2-S4 (2018) Infection forecasts powered by big data URL:https://www.nature.com/articles/d41586-018-02473-5

КЕРУЮЧІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПОПЕРЕДЖЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ НА ОБЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Пруський А.В., Сидоренко В.Л., Власенко Є.А..
Інститут державного управління та наукових досліджень
з цивільного захисту, Київ, Україна
Шевченко Р.І., Стрілець В.В.
Національний університет цивільного захисту України, Харків, Україна

Рівень терористичної загрози в світі нині досить високий. Від неї потерпають як країни, де тривають збройні конфлікти (передусім на Близькому Сході та в Африці), так і країни Заходу, що до останнього часу вважалися цілком безпечними з огляду на розвинену систему правоохоронних органів і спецслужб. Протидіяти цим загрозам стає дедалі важче [1,2]. З метою протидії надзвичайним ситуаціям (далі - НС) терористичного характеру (далі - ТХ) на об'єктах критичної інфраструктури (далі - ОКІ), в провідних країнах світу відбувається підготовка вузькоспеціалізованих фахівців [1,2].

При цьому, в країнах, які розвиваються, попередження НС на ОКІ, покладено на рятувальні підрозділи загального профілю, які для цього не мають ані спеціальної рятувальної техніки, ані вузькопрофільних фахівців [3-5].

Метою доповіді є опис керуючих інформаційних технологій попередження надзвичайних ситуацій терористичного характеру на об'єктах критичної інфраструктури. Управління НС ТХ є безперервним просторово-часовим процесом, головною метою якого є недопущення катастрофічної події в будь-якій з форм терористичного акта.Аналіз протікання процесу НС на ОКІ дозволив розробити специфічну схему управлінського впливу на процес поширення НС. Застосування цієї схеми в свою чергу дозволило розробити специфічну структурно-логічну модель управління НС ТХ на ОКІ.

Остання складається з двох контурів управління, а саме: контуру повсякденного (штатного) забезпечення безпеки та контуру екстреного реагування (надзвичайна ситуація).

Список літератури

1. Paul Gill, Zoe Marchment, Emily Corner &NoémieBouhana (2020) Terrorist Decision Making in the Context of Risk, Attack Planning, and Attack Commission, Studies in Conflict & Terrorism, 43:2, pp. 145-160, DOI: 10.1080/1057610X.2018.1445501

2. Захист критичної інфраструктури в умовах надзвичайних ситуацій: монографія / С.І. Азаров, В.Л. Сидоренко, С.А. Єременко, А.В. Пруський, А.М. Демків; за заг. ред. П.Б. Волянського. Київ, 2021. 375 с. іл.

3. Operation Viking Hammer. URL: https://en.wikipedia.org/wiki /Operation_Viking_Hammer

4. LTTE used CS Gas to attack Soldiers. URL: http://lankadailynews.com/2008/09/ltte-cs-gas-attack-soldiers/

5. Europol, TE-SAT 2016, European Union Terrorism Situation and Trend Report 2016, 2016. doi:10.2813/525171

РОЗРОБКА СПОСОБУ ОТРИМАННЯ МОДУЛЮ CDS/CDTE/CU/AU НА ГНУЧКІЙ ПІДКЛАДЦІ, ПРИЗНАЧЕНОГО ДЛЯ РЕЗЕРВНОГО ЖИВЛЕННЯ СИСТЕМ ПОПЕРЕДЖЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Дейнеко Н.В.
Харківський національний університет цивільного захисту України,
Харків, Україна

Аналіз надзвичайних ситуацій показує, що однією з проблем локалізації та ліквідації наслідків є відключення електроенергії через пошкодження ліній електропередач. Тому необхідно забезпечити аварійні джерела живлення або ж використовувані інструменти повинні працювати автономно.

Сучасні системи безпеки і контролю споживають лише невелику частину від загального споживання енергії об'єкта, їх безперебійну роботу забезпечує наявність електрики в мережі.

Як правило, такі системи безпеки мають резервне джерело живлення на випадок аварійного припинення електропостачання в мережі але, в більшості випадків, його заряду вистачає не більше, ніж на 24 години [1]. У такому випадку, стає актуальним використання сонячних елементів [2].

Особливої уваги заслуговують сонячні елементи на гнучкій підкладці, що можуть бути виготовлені на металевій фользі або поліамідній підкладці.

Метою доповіді є розробка технології створення ефективного сонячного модулю на основі телуриду кадмію на гнучкій підкладці.

В доповіді наводяться результати дослідження отриманих експериментальних зразків мікромодулів на гнучкій підкладці з послідовно з'єднаними сонячними елементами на основі CdS/CdTe/Cu/Au .

Для розуміння впливу на ефективність всього мікромодуля виходу з строю одного або декількох сонячних елементів в процесі експлуатації проведено аналіз вихідних параметрів і світлових діодних характеристик одиничних сонячних елементів двох мікромодулів.

Встановлено, що в процесі експлуатації одного з модулів відбулося шунтування сонячного елементу, що призвело до зниження ефективності всього мікромодуля до 3,9 %. Максимальна ефективність отриманих зразків мікромодулів становила 5,3 %.

Список літератури

1. William Stallings, Chapter 69 – Physical Security Essentials, Editor(s): John R. Vacca, Computer and Information Security Handbook (Third Edition), Morgan Kaufmann, 2017, Pages 965-979.

2. Khrypunov G. et al. Increasing the efficiency of film solar cells based on cadmium telluride // Eastern-European Journal of Enterprise Technologies. – 2016. – Т. 6. – №. 5 (84). – С. 12-18.

ПОКРАЩЕННЯ САНІТАРНО-ПОБУТОВИХ УМОВ ПРАЦІВНИКІВ ПІДПРИЄМСТВ ШЛЯХОМ ВДОСКОНАЛЕННЯ НОРМ ВИДАЧІ МИЮЧИХ ЗАСОБІВ

Квітковський Ю.В.
Товариство з обмеженою відповідальністю
«Харківський електромашинобудівний завод», Харків, Україна

На даний час в Україні існують нормативні документи, які визначають загальні умови використання миючих засобів (мило, пральні порошки тощо), що видаються працівникам промисловості [1, 2]. Кодексом законів про працю України (ст.165) передбачена безплатна видача мила та інших знешкоджувальних засобів на роботах, пов'язаних із забрудненням, за встановленими нормами.

Але щодо кількості миючих засобів, що повинні видаватися працівникові, існує правова лакуна, оскільки нормативні документи, що регламентували ці питання у радянські часи, були складені майже 100 років тому [3, 4] і на території України їх дія припинена. В той же час нових нормативних документів з цього питання поки не складено і не затверджено. Є лише рекомендації фахівців з охорони праці закріпити норми видачі миючих засобів у колективному договорі. Причому орієнтуватися рекомендовано саме на вищевказані радянські нормативи.

Метою доповіді є розгляд питання щодо недостатнього рівня нормативного забезпечення санітарно-побутових умов працівників у частині стосовній видачі миючих засобів, недостатності існуючих норм видачі, а також викладення пропозицій щодо відповідного вдосконалення норм видачі миючих засобів для працівників промислових підприємств, зокрема підприємств машинобудівної галузі, і необхідності створення нормативної бази, що регулює видачу миючих засобів згідно із сучасними умовами.

Список літератури

1. Технічний регламент мийних засобів. Затверджений постановою Кабінету Міністрів України від 20.08.2008 р. № 717 (у редакції постанови Кабінету Міністрів України від 12 червня 2013 р. № 408)

2. ДСанПіН 2.2.9.027-99. Санітарні правила і норми безпеки продукції парфумерно-косметичної промисловості. Затверджений Постановою Головного державного санітарного лікаря України від 01.07.1999 №27

3. Постановление Народного комиссариата труда СССР «Список категорий рабочих и служащих, которым должно выдаваться спецмыло на дом (в количестве 1 ф. в месяц) сверх мыла, находящегося в предприятиях при умывальниках (ст. 141 Кодекса законов о труде)» от 20.09.1923 № 80

4. Постановление Народного комиссариата труда СССР «Список категорий рабочих по металлопромышленности, коим должно выдаваться спецмыло на дом (в количестве 1 ф. в месяц) сверх мыла, находящегося в предприятиях при умывальниках» от 26.06.1923 № 270/775.

ВИЗНАЧЕННЯ ОСВІТЛЕНОСТІ ПРИМІЩЕНЬ З ВИКОРИСТАННЯМ СВІТЛОДІОДНИХ СВІТИЛЬНИКІВ

Доронін Є.В.
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна
Бондаренко С.В.
Національна академія національної гвардії України, Харків, Україна

Освітлення відіграє важливу роль у житті людини. Біля 90 % інформації сприймається через зоровий канал, тому правильно виконане раціональне освітлення має важливе значення для виконання усіх видів робіт.

Стан освітлення виробничих приміщень відіграє важливу роль і для попередження виробничого травматизму.

На сьогодні велику роль відводять світлодіодним світильникам, які дозволяють створити достатньо рівномірне освітлення приміщень та заощадити значну кількість електроенергії у порівнянні з традиційними світильниками. Завдяки значній площі потужні світильники світлодіодні стрічки дають менше тіней.

Це важливо при роботі з дрібними деталями, при наборі тексту, в роботі візажиста і перукаря, складальна годинників.

Термін служби ламп і світильників оцінюється в 30-50 тисяч годин. Лампи розжарювання служать близько 1000 годин, галогенки – 3-5 тисяч, люмінесцентні світильники – 10-12 тисяч.

При розрахунку освітленості приміщення світлодіодними світильниками враховуються: освітленість робочої поверхні, геометричні розміри приміщення

В залежності від призначення приміщення для нього діють свої норми освітленості. Деякі приміщення не потребують яскравого світла.

Метою доповіді є визначення методики розрахунку кількості світлодіодних світильників для забезпечення нормативної освітленості виробничих приміщень.

В доповіді наводяться результати розрахунків освітленості віробничих приміщень з використанням сучасних світлових приладів для забезпечення нормативних значень освітлення приміщень різного призначення.

Приведений метод розрахунку дозволяє оцінити кількість світлдодіодних світильників для забезпечення нормативних значень освітлености виробничих приміщень різного призначення.

Список літератури

1. ДБН В.2.5-28:2018. Природне і штучне освітлення. Київ : Мінрегіонбуд України, 2018. 137 с.

2. Третьяков О. В., Доронін Є. В., Пономаренко Р. В., Безсонний В. Л. Основи охорони праці. Харків : ТОВ «Планета-Прінт», 2020. 588 с.

ВИПРОБУВАННЯ ДОСЛІДНОГО ЗРАЗКА УСТАНОВКИ АВТОМАТИЧНОГО ПОЖЕЖОГАСІННЯ СКЛАДІВ ВИБУХОВИХ РЕЧОВИН

Федюк І.Б., Чернуха А.М.
Національний університет цивільного захисту України, Харків, Україна

У доповіді наведені результати експерименту по визначенню можливості застосування нових дренчерних установок пожежогасіння, що працюють в режимі «постріл» для гасіння пожеж складів вибухових речовин та боєприпасів та методів їх обробки.

Використанні матеріали досліджень та данні, що викладені в джерелах [1-4]. За підсумком експерименту отримані данні наведені в таблиці 1. Інформаційна обробка результатів дозволила отримати статичний стандарт випадкової величини відхилень та параметрів установок для практичного використання залежно від конкретних умов застосування.

Таблиця 1 – Експериментальні та розрахункові значення параметрів витікання води з резервуара в режимі „Постріл”

№ серії	$P_н$, МПа	$V_ж/V_б$, %	$t_э$, с	$P_к$, МПа	$t_э/ t_{T,min}$	$\beta \cdot 10^2$	$v_{max} \cdot 10^5$ см/с
А	0,1	2	3	0,4	5	6	7
1	1	62	2	0,38	5,18	3,73	1,316
2	0,95	75,6	2,1	0,23	4,497	4,94	1.32
3	0,78	56	2,8	0,343	6,76	2,19	1,104
4	0,7	64	3	0,252	6,12	2,67	1,06
5	0,62	51	3,3	0,3038	5,49	3,32	1,257
6*	0,7	83	6,1	0,119	9,9	1,02	1,1
7*	0,7	72	4,7	0,196	8,688	1,32	1,088

Дослідження дозволяють проводити подальші роботи для розробки захисту місць зберігання вибухонебезпечних речовин на випадок виникнення пожежі.

Список літератури

1. Коваленко А. А., Кучук Г. А. Методи синтезу інформаційної та технічної структур системи управління об’єктом критичного застосування. *Сучасні інформаційні системи*. 2018. Т. 2, № 1. С. 22–27. DOI: https://doi.org/10.20998/2522-9052.2018.1.04

2. Федюк І.Б.Методика гасіння пожеж на складах вибухових речовин та боєприпасів за допомогою нової установки автоматичного пожежогасіння швидкісного спрацювання // Збірник наукових праць ХУПС,Вип.1 (7). Харків:2006. С. 216.

3. Налимов В.В.Теория эксперимента. Москва:Наука.- 207 с.

4. Федюк І.Б., Чернуха А.М. Вибір місць розташування зрошувачів установок автоматичного пожежогасіння штабелів вибухонебезпечних речовин // Збірка наукових праць. НУЦЗУ. 2019. № 47. С. 187-192.

РОЗРОБКА БЕЗПРЕСОВИХ МЕТОДІВ ВИГОТОВЛЕННЯ І РЕМОНТУ ТОНКОСТІННИХ ВИРОБІВ ВЕЛИКИХ РОЗМІРІВ

Савченко М.Ф., Мягков В. Ю.
Харківський національний економічний університет імені С. Кузнеця, Харків, Україна

При виготовленні штампуванням тонкостінних, а особливо, великогабаритних, більших за 1 м, виробів, або при проведенні їх ремонтних робіт виникають проблеми з можливістю використання традиційного пресового обладнання [1-3].

Це обумовлено, перш за все, як відсутністю обладнання, так і низькою точністю виробів через появу дефектів в процесі штампування, гофрів (бухтин) на поверхні і локальних стоншень стінок виробів.

Метою доповіді є дослідження можливостей існуючих методів безпресового штампування та ремонту для розробки нових технологій з використанням імпульсних джерел енергії в процесі штампування і ремонту тонкостінних виробів великих розмірів.

Безперечні переваги з існуючих методів використання імпульсних навантажень для формоутворення оболонок або їх елементів мають методи з використанням горючих газових сумішей, створених у спеціального типу малогабаритних газогенераторів безпосередньо в зоні виготовлення виробів або їх ремонту.

Це дозволяє значно зменшити витрати на виробництво виробів, яке здійснюють безпресовим штампуванням, наприклад, локальним деформуванням з можливістю регулювання інтенсивності імпульсних навантажень в широких межах та безпекою їх створення.

Список літератури

1. Савченко Н. Ф.. Сыромятников П. А. Особенности выбора методов изготовления крупногабаритных деталей с использованием приемов регулирования технологических несовершенств // Вестник Харьковского национального технического университета сельского хозяйства имени Петра Василенко. – "Технический сервис АПК, техника и технологии в сельскохозяйственном машиностроении". – Харьков: ХНТУСХ, 2011. – Вып. 118. – С. 254–258.

2. Савченко Н. Ф.,Андилахай А. А. Совершенствование ремонтных работ крупногабаритных конструкций с использованием метода локальной штамповки // Защита металлургических машин от поломок: сб. научных трудов ПГТУ. – Мариуполь, 2014. Вып.16. С. 104–108.

3. Савченко Н. Ф. Беспрессовая штамповка как вариант адаптационного развития предприятия // Ресурсосбережение и энергоэффективность процессов и оборудования обработки давлением в машиностроении и металлургии: труды IV научно-технической конференции, 7-9 ноября 2012 г., Харьков. – Х.: НТУ "ХПИ", 2012. С. 98 – 100.

ЗМЕНШННЯ ЕКОЛОГІЧНОГО РИЗИКУ ЗАБРУДНЕННЯ ДОВКІЛЛЯ З ВИКОРИСТАННЯМ ПРОГНОЗУВАННЯ НА БАЗІ РЕЗУЛЬТАТІВ ЕКОМОНІТОРІНГУ

Адаменко М.І.
Уманський національний університет садівництва, Умань Україна.
Дармофал Е.А.
Харківська державна академія фізичної культури

Стрімке зростання антропогенного навантаження на довкілля призводить до постійного зростання ризику зміщення екологічної рівноваги у бік глобальної екологічної катастрофи. На сьогоднішній день, навіть без статистичних довідок, легко помітити швидке зростання кількості та головне «якості» природних катаклізмів. Однак ще одну рису «помсти природи» на наш погляд поки що недостатньо уваги притягає у наукової спільноти. Це фактор поширення географічних меж розповсюдження означених надзвичайних ситуацій. На нашу думку дані процеси є результатом суперпозиції впливу обох різновидів факторів. Наявність означеної проблеми та її місце у ряді проблем всесвітнього значення вже ні в кого не викликає сумнівів.

Широке обговорення цієї світової екологічної ситуації, яка веде людство до катастрофи руйнування основ забезпечення життєдіяльності висвітлюється не тільки в публіцистиці, а і в науковій літературі [1-4].

Мета доповіді: розробка теоретичних основ створення оптимальної системної мережі моніторингу виникнення та характеристик протікання означених надзвичайних ситуацій у всьому світі.

Слід відзначити те, що така системна мережа, у всіх країнах світу, повинна підпорядковуватись єдиному всесвітньому науковому центру з постановки задач та прогнозування і аналітичної обробки результатів.

У доповіді запропоновані основи побудови математичних моделей, які дозволять, враховуючі аналіз вже отриманих даних «глобального» моніторингу, розробити первинне науково обґрунтоване глобальне завдання, щодо напрямів проведення екологічних досліджень та моніторингу за єдиною всесвітньою програмою.

Список літератури

1. Адаменко М. І., Кацман М. Д., Білецька Є.С. Аналіз існуючих математичних моделей і комп'ютерних програм для прогнозування розповсюдження забруднюючих речовин в атмосфері. *Системи обробки інформації»*, 2018. № 1 (152). С. 155-1622.

2. Дідух Я.П. Основи біоіндикації. Київ : Наукова думка, 2012. 344 с.

3. Adamenko N. Darmofal E. Analysis of partitioning of a man-machine system in order to decrease adverse health effects of electromagnetic fields / Modern Science - Moderní věda. Praha: Česká republika, Nemoros, 2015 No.6. c.202-207.

4. Адаменко М. І. Кучук Н.Г. Моделювання розповсюдження шкідливих речовин / Проблеми інформатизації. Матеріали третьої міжнародної НТК. – Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельско-Бяла: УТіГН; Полтава: ПНТУ, 2015. – 84 с., с. 63

ОСОБЛИВОСТІ ДЕРЖАВНОГО МОНІТОРИНГУ ВОД ПРИ ДОСЛІДЖЕННІ АНТРОПОГЕННОГО НАВАНТАЖЕННЯ НА ОБ'ЄКТИ ГІДРОСФЕРИ

Коваленко С.А., Пономаренко Р.В.,
Національний університет цивільного захисту України, Харків, Україна
Третьяков О.В.
ТОВ «Іпріс-Профіль», Харків, Україна

У зв'язку з постійним розвитком промисловості відбуваються викиди забруднюючих речовин у атмосферне повітря, у поверхневі водні об'єкти та захоронення відходів. Таким чином, у безперервному режимі відбувається забруднення об'єктів навколишнього середовища.

Метою доповіді є визначення об'єктів, завдань, виконавців та відповідальності при проведенні державного моніторингу поверхневих водних об'єктів задля збереження і відтворення водних ресурсів.

У 2018 році Кабінет Міністрів України затвердив Порядок здійснення державного моніторингу вод, який вод здійснюється з метою забезпечення збирання, обробки, збереження, узагальнення та аналізу інформації про стан поверхневих водних об'єктів, прогнозування його змін та розроблення науково обґрунтованих рекомендацій для прийняття рішень у галузі використання, охорони вод та відтворення водних ресурсів.

Об'єктами державного моніторингу вод є: масиви поверхневих вод, в тому числі прибережні води та зони, які підлягають охороні; масиви підземних вод, в тому числі зони, які підлягають охороні; морські води в межах територіального моря та виключної морської економічної зони України, в тому числі зони, які підлягають охороні.

Згідно Порядку [1] державний моніторинг вод поділяють на декілька видів: діагностичний моніторинг, операційний моніторинг, дослідницький моніторинг та моніторинг морських вод.

Діагностичний моніторинг створено з метою оцінки впливу антропогенного навантаження на поверхневі та підземні водні об'єкти.

Операційний моніторинг проводять щороку з метою оцінювання змін, що відбуваються у екологічному та хімічному станах поверхневих водних об'єктів та підземних вод.

Дослідницький моніторинг проводять лише для поверхневих водних об'єктів з метою встановлення причин, як призводять до неможливості досягнення екологічних норм для вказаних об'єктів.

Моніторинг морських вод здійснюється для територіального моря та виключної морської економічної зони України.

Список літератури

1. Про затвердження Порядку здійснення державного моніторингу вод: Постава Кабінету Міністрів України від 19 вересня 2018 р. № 758 Київ: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/758-2018-%D0%BF#Text(датазвернення10.03.2021).

ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ СПОСОБУ ШВИДКОЇ ЛІКВІДАЦІЇ ЛЬОДЯНИХ ЗАТОРІВ НА РІЧКАХ

Третьяков О.В.
ТОВ «Іпріс-Профіль», Харків, Україна
Гарбуз С.В.
Національний університет цивільного захисту України, Харків, Україна

Затор льоду – явище льодового режиму річки в період замерзання, що позначається нагромадженням крижин під час льодоходу в вузьких місцях. Буває найчастіше під час весняного льодоходу, але відмічається і восени. Часто буває причиною льодоставу. При заторі, як і при зажорі, вище по течії, від місця його утворення спостерігається підйом, а нижче – зниження рівня води [1].

Метою доповіді є розробка теоретичного обґрунтування способу швидкого руйнування льодової криги за допомогою дискретного струменю великої швидкості на річках в період льодоходу.

Великий успіх з руйнування різноманітних твердих матеріалів мають імпульсні технології на основі відповідних водометів [1].

Імпульсний викид води можна розглядати при створенні водомету для руйнування льодової криги з великою дальністю дії.

Основним дестабілізуючим фактором струї, який запускає зовнішні механізми її руйнування є турбулентність. Боротьба з турбулентністю шляхом забезпечення більш плавної течії біля стінок каналу і сопла зміщують початок процесу турбулентності, але не усувають її.

Традиційні гідродинамічні підходи не дозволяють суттєво впливати на турбулентність, наприклад, перешкоджати розвитку сильної турбулентності за допомогою штучно створеної дрібномасштабної (ДМ) турбулентності. Перенос енергії ДМ турбулентними флуктуаціями не залежить від сили тертя, а визначається виключно силами інерції.

Результати комп'ютерного моделювання показали, що при швидкості витікання з сопла 10 м/с інтенсивність турбулентності в перерізі поблизу решіток достатньо висока і місцями досягає 60%, а в перерізі середньої частини свободного простору камери була на рівні 30% і практично рівномірною по всьому перерізу.

До початкових параметрів конструкції водомету відносяться тільки діаметр водяного заряду і швидкість вилиту струї.

Список літератури

1. Лаврентьев, М. А., Антонов Є. Г., Войцеховский Б. В. Вопросы теории и практики импульсных водяных стру. Новосибирск: Ин-т гидродинамики СО АН СССР. 1961. 347 с.

СОЦІАЛЬНИЙ ТА ІНДИВІДУАЛЬНИЙ ПОЖЕЖНИЙ РИЗИК У БУДІВЛЯХ І НА ТЕРИТОРІЇ ОБ'ЄКТУ

Третьяков О.В.
ТОВ «Іпріс-Профіль», Харків, Україна
Доронін Є.В.
Харківський національний економічний університет імен С. Кузнеця, Харків, Україна

При аналізі проблеми небезпеки (будь-якого об'єкту) з'являються два основні поняття – небезпека і безпека, які потребують відповідних визначень (хоча, здається, очевидним, що «безпека» є просто відсутність всілякої «небезпеки»).

До цих двох понять треба додати ще одне – «ризик», навколо якого в останні десятиріччя серед фахівців ведеться жвава полеміка. Це поняття у деякому ступеню пов'язує два перші поняття. Так утворюється основна тріада понять теорії ризик і безпеки, яка активно формується і розвивається в наш час: «небезпека – ризик – безпека».

Метою доповіді є визначення методичних підходів для оцінки соціального та індивідуального ризику у будівлях і на території об'єкту.

Критерії за якими оцінюється ступінь ризику від провадження господарської діяльності та визначається періодичність здійснення планових заходів державного нагляду (контролю) у сфері техногенної та пожежної безпеки означені в [1].

Для об'єктів, в яких перебуває значна кількість людей, соціальний пожежний ризик визначають за умови, коли в процесі виникнення пожежі може постраждати в результаті дії небезпечних факторів пожежі не менше 10 осіб.

Соціальний пожежний ризик $R_{в.о.с}$ у приміщені об'єкта виробничого призначення залежить від надійної роботи системи сповіщення про пожежу(R_c), імовірності присутності людей в приміщені, критичного часу пожежі (τ_k) та імовірності евакуації людей за цей час ($P_{ев.л}(\tau_{п.е})$), а також від надійності роботи технічних споряджень, які спрямовані на забезпечення безпечної евакуації людей ($P_{без.л}(\tau_k)$):

$$R_{в.о.с} = R_{в.о.б} \cdot R_c \cdot P_{пр.л} \cdot \left(1 - P_{ев.л}\left(\tau_{п.е}\right)\right)\left(1 - P_{без.л}\left(\tau_k\right)\right) \le \left[R_{в.о.с}\right].$$

Список літератури

1. Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності та визначається періодичність здійснення планових заходів державного нагляду (контролю) у сфері техногенної та пожежної безпеки Державною службою з надзвичайних ситуацій. Постанова Кабінету Міністрів України від 05.09.2018 р. № 715 веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/715-2018-%D0%BF#Text (дата звернення 10.03.2021)

САНІТАРІЯ ТА ГІГІЄНА ЗАКЛАДІВ ГОТЕЛЬНО-РЕСТОРАННОГО ГОСПОДАРСТВА У ПЕРІОД КАРАНТИНУ

Безсонний В.Л.
Харківський національний економічний університет імен С. Кузнеця,
Харків, Україна

На даний момент у всьому світі, в тому числі і в Україні, поширюється гостра респіраторна інфекційна хвороба COVID-19. Всесвітня організація визнала її пандемією, прирівнявши з такими історичними хворобами як чума і холера.

З огляду на ситуацію, Кабінетом Міністрів України були введені карантинні заходи, щоб протидіяти поширенню коронавірус, які в першу чергу спрямовані на призупинення або обмеження діяльності суб'єктів господарювання. Саме під ці обмеження і підпадають заклади ресторанного господарства (громадського харчування). Роботу закладів призупинили до окремого розпорядження і дозволили тільки самовивіз і кур'єрську доставку страв і напоїв з ресторанів і кафе.

Також керівники закладів, які працюють в умовах карантину, крім стандартного контролю якості в закладі, повинні забезпечити ряд додаткових профілактичних і протиепідемічних заходів.

Персонал обов'язково повинен бути забезпеченим всім необхідним для миття рук: рукомийники, достатня кількість мила, одноразові рушники для витирання рук, спиртовмісні антисептики.

Сушарки для рук не підходять для використання в зонах приготування їжі. Тому треба подбати про достатню кількість одноразових рушників для витирання рук. Антисептики з дозаторами повинні бути на видному місці, щоб кожен міг ними скористатися. Встановити частоту миття рук кожні 15 хвилин і обробку спиртовмісних антисептиками не рідше ніж раз на 3 години і після кожного контакту з сирими продуктами, використання туалету, прибирання тощо. Мити руки потрібно перед надяганням рукавичок, між зміною рукавичок і після зняття.

У закладі потрібно проводити вологе прибирання з використанням миючих і дезінфікуючих засобів не рідше ніж раз на 3 години і обов'язково після закінчення зміни. Також проводити обробку поверхонь, місць контакту рук (ручки дверей, крани, тачскрін терміналів програми для ресторану або кафе і т. д.) дезінфікуючими засобами.

Список літератури

1. Про захист населення від інфекційних хвороб. Закон України від 06.04.2000 № 1645-III / Офіційний вісник України від 12.05.2000 — 2000 р., № 17, стор. 5, стаття 690, код акта 15781/2000.

2. Про забезпечення санітарного та епідемічного благополуччя населення. Закон України від 24.02.1994 № 4004-XII. / Відомості Верховної Ради України від 05.07.1994 — 1994 р., № 27, стаття 218.

ПІДВИЩЕННЯ БЕЗПЕКИ УМОВ ПРАЦІ ДЛЯ ПРАЦІВНИКІВ ТРАНСПОРТНОЇ ГАЛУЗІ НА ОСНОВІ РОЗРАХУНКУ СУМАРНОГО РИЗИКУ

Третьяков О.В., Гармаш Б.К., Григор'єва Є.С.
Український державний університет залізничного транспорту,
Харків, Україна

Критерії безпеки, які враховують усі теоретичні і практичні аспекти забезпечення безпечної праці, мають базуватися на науково обґрунтованій теорії професійного та виробничого ризику. Оцінка ризику – це процес визначення ймовірності збитків шляхом аналізу потенційних небезпек і оцінки існуючих умов уразливості, які можуть становити загрозу чи шкоду власності, людям, засобам до існування і навколишньому середовищу, від якого вони залежать [1]. Передбачається врахування як мінімум двох типів ризику: реального і потенційного [2].

Існує необхідність на науковій основі реалізації на практиці вимог відомого принципу ALARA: рівень ризику має бути настільки низьким, наскільки це можливо у даних економічних і соціальних умовах [3].

Метою доповіді є розробка методу визначення рівня небезпеки для працівників у робочій зоні за умов сумісної дії шкідливих факторів різних класів на основі інтегрального показнику – виробничого ризику.

В доповіді наводиться обґрунтування доцільності використання методу визначення рівня небезпеки для працівників у робочій зоні, який базується на перетворенні «доза – ефект», що дозволяє розрахувати сумарний ризик при наявності сумісної дії шкідливих факторів різних класів.

Був проведений аналіз за результатами атестації робочих місць на основі алгоритму перетворення параметрів середовища у показник виробничого ризику на базі карт умов праці працівників кранового цеху виробничого підрозділу «Локомотивне депо основа».

В результаті проведених розрахунків та їхнього аналізу встановлено, що системний підхід, який базується на оцінці ризиків, обумовлених специфікою процесів у транспортній галуз, є основним напрямком підвищення безпеки умов праці.

Список літератури

1. ISO/IEC Guide 73. Risk Management – Vocabulary. URL: https://www.iso.org/standard/44651.html).

2. Третьяков О. В., Гармаш Б. К., Халмурадов, Білецька Є. С. Ризик-орієнтований підхід до визначення умов праці окремих категорій працівників транспортної галузі. Системи управління, навігації та зв`язку. ПНТУ, **2020.** Вип. 59 (1). С. 120–126.

3. Moghissi A.A., Narland R.E., Congel F.J. Eckerman K.F. Methodology for environmental human exposure and health risk assessment. Exposure and Hazard Assessment Toxic chem. Michigan, USA. 1980. P. 471–489.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМУНІКАЦІЙНИХ ПРИМІЩЕНЬ ПРИ ЗАГРОЗІ ВИБУХУ

Васильченко О.В., Семенов А.В.
Національний університет цивільного захисту України, Харків

У промислових будівлях категорій "А" і "Б" в разі аварійного вибуху в комунікаційних приміщеннях (коридорах, тунелях), де після подолання легкоскидних конструкцій (ЛСК) поширюється ударна хвиля (УХ) і будівельні конструкції піддаються її впливу, їхня поведінка буває непередбачуваною.

Комунікаційне приміщення можна уявити як напівзамкнений простір (канал), в якому енергія УХ розсіюється повільніше, ніж у великому приміщенні. При цьому підвищуються втрати енергії на нагрів повітря і тертя при взаємодії УХ зі стінками каналу.

Метою доповіді є аналіз математичної моделі руху ударної хвилі в довгому комунікаційному приміщенні (каналі).

Існують емпіричні залежності для розрахунку характеристик головної ударної хвилі (ГУХ) в каналі з жорсткими стінками [1]. Їх аналіз показує, що якщо протилежні стінки конструктивно різні і з різних матеріалів, але їх відносна деформація при впливі УХ невелика ($R2 \approx R1$; $E2 \approx E1$), то поширення УХ в каналі відбувається за механізмом утворення ГУХ.

Якщо ж одна зі стінок каналу рухлива і/або легко деформується ($R2 < R1$; $E2 < E1$), то наведений імпульс, що діє на неї, зменшується. Отже, зменшується швидкість віддзеркаленої ударної хвилі (ВУХ), збільшується зона формування плоского фронту ГУХ, і при цьому фронт УХ як би розгортається в сторону нежорсткій стінки. Тиск на цю стінку додатково збільшується, що може привести до її руйнування.

Але одночасно з цим порушується і геометрія плоского фронту головної ударної хвилі, а для формування нового плоского фронту потрібна зона довжиною в 4-8 характерних розмірів перетину каналу.

Запропонована модель дозволяє обґрунтувати спосіб підвищення безпеки в комунікаційних приміщеннях об'єктів підвищеної небезпеки за допомогою такого розташування ЛСК, що перешкоджатиме утворенню головної ударної хвилі, сприяти зниженню надлишкового тиску на фронті ударної хвилі і її загасання.

Список літератури

1. Васильченко А.В., Рябинин И. Н., Ковалевская Т. М. Анализ воздействия ударной волны на строительные конструкции в коммуникационных помещениях // Проблеми надзвичайних ситуацій: Сб. науч. тр. – Вып.22.– Харьков: НУГЗУ, 2015. – С. 19-23.

2. Бейкер У. и др. Взрывные явления: оценка и последствия: в 2-х кн. Кн. 1. Пер. с англ. : Под ред. Я.Б.Зельдовича, Б.Е.Гельфанда. – М.: Мир, 1986. – 319 с.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ ПОЖЕЖНОЮ БЕЗПЕКОЮ ВАЖЛИВИХ ОБ'ЄКТІВ

Альбощій О.В.
Національна академія Національної гвардії України, Харків, Україна

Серед об'єктів військового господарства є велика кількість таких, що відіграють важливу роль у тиловому забезпеченні. До них відносяться, зокрема, склади військової частини, на яких зберігаються матеріальні засоби номенклатури різних служб. Організації та проведенню заходів технічного та організаційного характеру, спрямованих на підтримання належного рівня пожежної безпеки військових складів, на практиці приділяється велика увага. В той же час, існують певні технологічні обмеження у методах управління пожежною безпекою, які використовуються на практиці. Традиційні підходи до процесів управління пожежною безпекою, які використовуються на практиці переважно, передбачають контроль повноти та якості виконання вимог керівних документів і нормативно-правових актів з питань пожежної безпеки. Якщо такі вимоги на об'єкті виконані, то стан пожежної безпеки вважається задовільним. Суттєвим недоліком такого підходу є те, що він не передбачає повної ідентифікації та кількісного оцінювання ризиків, які можуть призвести до виникнення загоряння та пожежі. А тому, існує потреба теоретичних досліджень щодо подальшого удосконалення процесів управління пожежною безпекою. Спираючись на сучасні тенденції у технологіях управління пожежною безпекою [2], показана доцільність застосування ризик-орієнтованого підходу на об'єктах, які можна віднести до об'єктів категорії "важливі", та потребують посиленої уваги.

Метою доповіді є представлення методичного підходу до ризик-орієнтованого управління пожежною безпекою та інформаційного забезпечення процесів ризик-орієнтованого управління пожежною безпекою об'єктів складського господарства військової частини.

В доповіді наводяться результати досліджень щодо можливості "візуалізації" пожежних ризиків, їх картографування [1]. Обгрунтовані відомості, які мають бути відображені у картці пожежних ризиків, як формі картографування ризиків. Показана форма такої картки та її основне призначення.

Список літератури

1. Альбощій, О. В., Павленко С. О., Павлов Я. В., Писаревський С. В. Дослідження методичних аспектів підвищення надійності зберігання матеріальних засобів для забезпечення військ шляхом управління ризиками // Щоквартальний науковий журнал «Честь і закон» № 2(73). – Х.: НАНГУ, 2020.. – С.135-143. DOI: https://doi.org/10.33405/2078-7480/2020/2/73/207156.

2. S. Kravtsiv, O. Sobol. Development of model F integral fire riskmanagement by correlation-registration analysis / Economics, entrepreneurship, management / vol. 5, № 1, 2018. - С.81-86. DOI: https://doi.org/10.23939/eem2018.01.081.

R-ОБ'ЄКТИ ЯК СХЕМИ З ФУНКЦІОНАЛЬНИХ ЕЛЕМЕНТІВ

Маматова Д.В., Лісін Д.О.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

R-functions were created by V. L. Rvachev in the process of developing mathematical tools for problem describing a geometrical object with equations. Rvachev functions are real-value functions based on methods of Boolean algebra, for example equation of conjunction and disjunction are shown below:

$$f \vee g = f + g + \sqrt{f^2 + g^2}; \; f \wedge g = f + g - \sqrt{f^2 + g^2}.$$

If functions f and g are defining some geometrical regions, meaning that they are equal to zero on the boundaries, positive inside said region and negative outside, then $f \vee g$ describes union of these regions, while $f \wedge g$ describes their intersection [1].

In particular, they can be used for description of complex geometrical objects with arbitrary shapes.

In virtue of their excellent constructive abilities, R-functions found wide applications; studies involving R-functions are successfully conducted in Ukraine [2].

The purpose of the research is to develop intuitive and time-saving software for creating R-objects.

Description of complex objects consists, in terms of R-functions, is a straight-line program. Straight-line program can be converted into a logic circuit and vice versa. Developed software uses a circuit computation model for constructing R-objects as it offers a more visual representation. R-object is presented in a form of directed acyclic graph where nodes are either inputs, logic gates or macroses. A graph is constructed by dragging needed node on the form and connecting it with existing nodes.

Output graph is parsed then into the straight-line program, code of which can be used to draw 3D function in the relevant software [3]. Nodes have several customizable parameters, such as maximum and minimum inputs, type of node, and text. R-object can be saved in STL format and opened for work later.

Список літератури

1. Рвачев В.Л. Теория R-функций и некоторые ее приложения. Киев: Наук. Думка, 1982. 552с.

2. Максименко-Шейко К. В. R-функции в математическом моделировании геометрических объектов и физических полей : монографія. Харьков: ІПМаш НАН України, 2009. 305 с.

3. Лісін Д.О. Комп'ютерна програма «Система візуалізації та побудови сітки на поверхні геометричних об'єктів, які описані за допомогою математичних засобів теорії R-функцій «RFPreview» / Свідоцтво про реєстрацію авторського права на твір. 2012. № 45951.

ВИКОРИСТАННЯ СОНЯЧНИХ КОЛЕКТОРІВ В СИСТЕМІ ОПАЛЕННЯ ТА ГАРЯЧОГО ВОДОПОСТАЧАННЯ ПРИВАТНОГО БУДИНКУ

Абеленцева К.В., Мягкохліб К.Б.
Харківський національний університет імені В.Н.Каразіна Харків, Україна

В роботі визначено принцип дії сонячних колекторів, проведено їх порівняння та виконано розрахунок системи опалення та гарячого водопостачання приватного будинку з вакуумним колектором [1, 2].

Значну роль у вирішенні цього питання можуть зіграти дослідження в напрямку енергетичної ефективності та енергозбереження. Усе це потребує створення відповідних нових технологій і нових наукових розробок, зокрема використання сонячних колекторів (рис. 1).

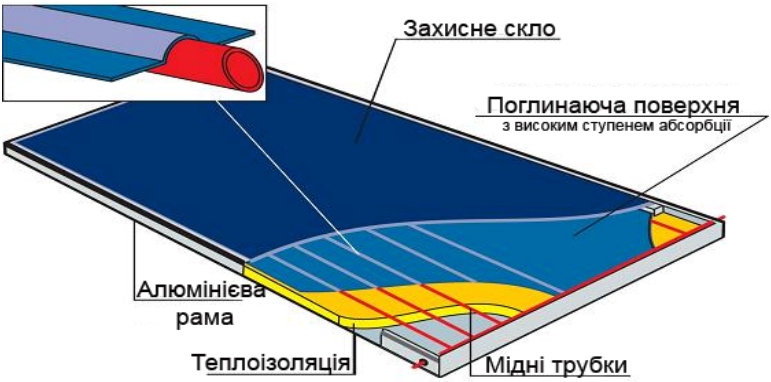

Рис. 1. Сонячний колектор

В роботі було зроблено аналіз експлуатації і розрахунків сонячних колекторів.

В результаті проведення серії розрахунків визначена кількість сонячних панелей сонячних колекторів, що необхідна для часткового опалення та гарячого водопостачання типового приватного будинку.

Список літератури

1. Маляренко В.А. Основи теплофізики будівель та енергозбереження. – Х.: «Видавництво САГА», 2006. – 484 с.

2. Энергосбережение в системах теплоснабжения вентиляции и кондиционирования воздуха: Справ. Пособие/ Л.Д. Богуславский, В.И. Ливчак, В.П. Титов и др. под общей редакцией Л.Д. Богуславского. – М.: Стройиздат, 1990. – 624 с.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ЦИВІЛЬНІЙ БЕЗПЕЦІ

Гришкевич М.М.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна

Розвиток науки і техніки на сучасному етапі важко уявити собі без використання обчислювальної техніки та інформаційних технологій. Жодна сфера людської діяльності не обходиться без їх допомоги [1].

У сучасних умовах персональний комп'ютер можна використати для розв'язання різноманітних задач забезпечення пожежної безпеки та цивільного захисту, охорони праці тощо. Персональний комп'ютер дає можливість систематизувати великі об'єми даних та автоматизувати обробку різноманітних статистичних даних у різних галузях науки [2].

Можливість виконувати свою роботу на відстані стала провідним засобом у подоланні пандемії.

Технології безпеки торкаються як зовнішньополітичних ситуацій так і внутрішніх конфліктів між громадянами. На сучасному етапі розвитку набувають значної гостроти проблеми соціально-політичної напруженості в країнах із перехідною економікою. Причинами цього є незадовільні умови життя, праці, розрив у рівні забезпечення життя між різними прошарками населення, низький показник освіти і культури, зіткнення інтересів релігійного й ідеологічного характеру[3].

Метою доповіді є аналіз впливу модернізації інформаційних технологій на якісь захисту громадян від найрізноманітніших небезпечних ситуацій, включаючи стихійні лиха.

В доповіді наводяться історичні факти зафіксовані по даній темі та проводиться паралель із сьогоденням. Також наявні результати аналітичної роботи та можливі нововведення щодо поліпшення цивільної безпеки за допомогою сфери ІТ. Наведенні дані у доповіді показують, що технології є ледь не найголовнішим предметом забезпечення безпеки, а також розлядають можливу майбутню повномірну залежність технологій з безпекою.

Список літератури

1. Антошкін О., Хазанова Я. Приклад використання інформаційних технологій при викладанні дисциплін у галузі «цивільна безпека». http://91.234.43.156/bitstream/123456789/10032/1/%D0%A2%D0%B5%D0%B7%D0%B8%20%D0%90%D0%BD%D1%82%D0%BE%D1%88%D0%BA%D1%96%D0%BD.pdf

2. О. Г. Левченко, О. В. Землянська, Н. А. Праховнік, В. В. Зацарний. Безпека життєдіяльності та цивільний захист. http://www.caravela.kiev.ua/files/file/03_natural_technical/02_reclama_block_bgd_cc_levchenko_2019.pdf

3. Маляров М. В., Гусева Л. В., Паніна О. О., Піксасов М. М., Журавський М. М.. Інформатика та інформаційні технології у цивільній безпеці. http://repositsc.nuczu.edu.ua/handle/123456789/547

МОДЕЛЮВАННЯ ПОШИРЕННЯ ЕЛЕКТРОМАГНІТНИХ ПОЛІВ ЕНЕРГЕТИЧНОГО ОБЛАДНАННЯ У ПРИМІЩЕННЯХ ТА НА ТЕРИТОРІЯХ

Левченко Л.О., Кужавський Д.С.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна

Постійне зростання споживання електронного обладнання висуває підвищені вимоги як до надійності функціонування, так і до електромагнітної безпеки в місцях з великою кількістю такого обладнання. Електромагнітне випромінювання — потужний фізичний подразник, що впливає і на саме електронне обладнання, так і на біологічні об'єкти, в тому числі й організм людини. Найбільш дієвим способом прогнозування електромагнітної обстановки, як в приміщенні так і на території поблизу енергетичного обладнання, є моделювання просторових розподілів електричних і магнітних полів. Використання розрахункових методів визначення електричних і магнітних складових електромагнітних полів надає змогу не тільки оцінити внесок окремих джерел у загальний електромагнітний фон, а й раціоналізувати або оптимізувати загальні схеми розміщення обладнання з точки зору електромагнітної безпеки.

Метою доповіді є визначення математичних моделей, які дозволять враховувати особливості просторових поширень електромагнітних полів найбільш типових джерел.

В доповіді наводяться результати вимірювань рівнів електромагнітних полів. Наведенні дані показують, що моделювання просторових розподілів електричних і магнітних полів необхідно здійснювати з урахуванням геометричних характеристик джерела поля (локалізоване або розосереджене), фізичної природи поля. При їх моделюванні враховувати залежності зміни напруженості поля. Магнітне поле промислової частоти можна вважати квазістаціонарним з прийнятною похибкою розрахунків, що дозволяє використовувати в розрахунках закон Біо-Савара.

При моделюванні магнітного поля електричних машин доцільно використовувати сферичну систему координат, поверхня машини середнього радіуса є базовою сферою.

При цьому враховуючи, що усе сучасне електротехнічне обладнання має магнітні поля наступних типів: дипольне, дипольно-квадрупольне та дипольно-октупольне, тому для мінімізації похибок моделювання є обов'язковим врахування сферичних гармонік магнітного поля [1].

Список літератури

1. Глива В.А., Ніколаєв К.Д., Колумбет В.П., Левченко Л.О. Методологія дослідження низькочастотних електромагнітних полів в умовах сталого розвитку технологій. *Системи управління, навігації та зв'язку*. 2017. № 6 (46). С. 219–223.

ЗАСТОСУВАННЯ МЕТОДІВ РАДІОТЕРМОГРАФІЇ В ТЕЛЕМЕДИЦИНІ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Черепньов І.А.
Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна

Незважаючи на те, що загальна кількість надзвичайних ситуацій (НС) зареєстрованих на території України в 2020 році найнижче за останні 10 років, на більшій частині регіонів країни рівень ризиків виникнення НС природного та техногенного характеру та ризиків збитків від них залишаються практично незмінними та досить високими [1]. Крім того, як це зазначено в цій же роботі значно зросла кількість вибухів і пожеж, які супроводжували НС техногенного походження та зафіксовано зростання більш ніж у шість разів суми завданих надзвичайними ситуаціями збитків. Як відомо що люди які знаходяться в зоні дії вражаючих факторів пожеж і вибухів з високою часткою ймовірності можуть загинути або отримати серйозні травми, які часто мають комбінований характер.

Метою доповіді є обґрунтування доцільності використання методів радіотермографії в телемедицині для діагностики та оперативного корегування процесу лікування в умовах надзвичайних ситуацій.

В доповіді наведено аргументацію, щодо використання методів радіотермографії, результати експериментальних досліджень по використанню радіометрів в сфері медицини катастроф.

На підставі міжнародного досвіду накопиченого фахівцями медицини катастроф сформульовано поняття "золота година", тобто це проміжок часу (60 хв), що вимірюється від моменту отримання постраждалим ушкоджень до моменту транспортування до закладу охорони здоров'я, протягом якого надання медичної допомоги постраждалому є найбільш ефективним. У разі, коли потерпілі отримали внутрішні пошкодження організму необхідно здійснювати постійний моніторинг зміни його стану і реакцію на процес лікування. Променева діагностика може призвести до негативних наслідків і має значні обмеження за віком та станом конкретних пацієнтів. Тому, в медицині катастроф як доповнення, а в певних випадках і альтернатива, використовується радіотермографія. Цей метод має низку переваг у порівнянні з загальноприйнятими методами діагностики [2]: неінвазивність; повна відсутність іонізуючого та інших видів випромінювання; висока інформативність; можливість застосування протягом тривалого проміжку часу; непотрібність спеціальної підготовки людини до обстеження; можливість повної автоматизації процесу дослідження та інші.

Автор тез приймав участь у експериментальних дослідженнях по використанню радіометрів в сфері медицини катастроф з точки зору впливу на ефективність вимірів наявності: гіпсу, марлевих пов'язок, некротичних тканин, струпів та ін. [3]. Одночасно була перевірена ефективність діагностичної системи побудованої на основі радіометрів, які працюють в мм і см діапазо-

нах радіохвиль при здійсненні оперативних терапевтичних заходів потерпілого при пожежі який отримав численні опіки третього ступеня і в тому числі нижніх кінцівок.

В ході радіометрії, яка проводилася при накладених на тканини пов'язках була виявлена термоампутація гомілок і стоп. На підставі отриманої інформації були скоригований обсяг і склад терапії, що дозволило уникнути ампутації і досягти одужання.

Результати експериментів дозволили зробити висновки про те, що: ороговілі шари епідермісу, волосяний покрив, легкий одяг наявність некротичних тканин і струпів, сухих марлевих, плівкових і гіпсових пов'язок практично не впливають на якість радіояркісного зображення, а отже і на достовірність діагностики потерпілого; панорамне і детальне термографування може стати вельми корисним в травматології, інтенсивної терапії, фізіотерапії, медицині катастроф та інших галузях медицини; отримані в процесі сканування дані дозволяють здійснювати контроль зміни стану організму потерпілого в динамічному режимі.

Список літератури

1. Інформаційно-аналітична довідка про виникнення НС в Україні упродовж 2020 року. Державна служба України з надзвичайних ситуацій: вебсайт. URL: https://www.dsns.gov.ua/ua/Dovidka-za-kvartal/119288.html (дата звернення 31.01 2021).

2. Черепнев И.А., Лупиков В.С, Ляшенко Г.А. Основные требования к диагностической аппаратуре на основе измерения собственных электромагнитных излучений биологических объектов. Системи управління навігації та зв'язку. 2011. Вип.4 (20). С. 124 – 131.

3. Экспериментальное обоснование медико-технических требований к аппаратуре радиотеплового картирования биологических объектов / Л.Ф. Кучин та ін. Збірник наукових праць ХВУ, 2002. Вип.1(39). С. 126–130

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПОЛІПШЕННЯ ЗДОРОВ'Я МОЛОДІ УКРАЇНИ: «ЗА" І "ПРОТИ"

Вамболь С.О., Черепньов І.А.
Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна

В багатьох країн світу, і в тому числі Україні, в останні десятиліття розвиваються дві негативні тенденції, які створюють серйозну загрозу економічній складовій національної безпеки держави [1]. А саме: стрімке старіння населення і погіршення фізичного і психічного стану молоді, яку традиційно відносять до так званої допризовної категорії. Цей процес посилюється значним поширенням таких вкрай небезпечних факторів як куріння, систематичне вживання алкоголю і наркотиків, низької якості занять фізичною культурою в закладах вищої освіти. І найнебезпечніше те, що не дивлячись на деяке зниження споживання алкоголю населенням України в цілому, країна як за-

значено в роботі [2] займає перше місце по дитячому пияцтву та алкоголізму. Викликає занепокоєння і вживання підлітками наркотиків. За даними опитування, проведеного в 2010 році перше вживання наркотичних речовин у 32% опитаних здійснилося у віці 12 -16 років [1].

За даними соціального моніторингу розповсюдження хімічних та нехімічних форм залежності серед молоді м. Харкова [2] був зроблений висновок про те, що на момент 2018 р.: оцінка гостроти проблеми алкоголізму та наркоманії залишається стабільно високою; на фоні загальної стабілізації споживання наркотиків відбувається внутрішня трансформація, яка проявляється у збільшенні споживання одних речовин і зменшенні інших; зросло число регулярних споживачів наркотиків.

Метою доповіді є висвітлення проблематика ведення здорового способу життя серед молоді та вплив інформаційних технологій на виникнення залежності від Інтернету.

В доповіді наведено аналіз позитивного впливу інформаційних систем на освітню діяльність та надано негативні приклади залежності від Інтернет мереж .

Для боротьби з цими негативними тенденціями використовувати апробовані ще в кінці XIX століття методи масового впровадження в молодіжну середу фізичного виховання і спорту, активної боротьби за здоровий спосіб життя. Доволі часто висловлюється пропозиція щодо поширення серед студентської молоді знань про важливість здорового способу життя, можливості використання методів, що коригують і зберігають здоров'я на основі застосування інформаційних технологій. Не відкидається ефективність інформаційних систем з точки зору ведення освітнього процесу і високого впливу на широку аудиторію учнів.

Але на нашу думку не можна використовувати виключно інформаційні технології, бо кожна п'ятнадцята особа (6,54 %), яка має досвід роботи в Інтернеті, набуває залежність від нього вже в підлітковому віці (за цим показником Інтернет як об'єкт зловживання наближається до каннабіноїдів – гашишу, марихуани тощо).

А з огляду на те, що 97% підлітків і молодих людей віком від 15 до є активними користувачами Інтернету у значної кількості цих людей рано чи пізно можуть з'явитися фізичні і психологічні відхилення від норми. І в такій ситуації, як сказав давньоримський письменник та оратор Луцій Анней Сенека (відомий під іменами Сенека Старший): «Деякі ліки небезпечні самих хвороб».

Список літератури

1. Інформаційно-аналітична довідка про виникнення НС в Україні упродовж 2020 року. Державна служба України з надзвичайних ситуацій: вебсайт. URL: https://www.dsns.gov.ua/ua/Dovidka-za-kvartal/119288.html (дата звернення 31.01 2021).

2. Черепнев И.А., Лупиков В.С, Ляшенко Г.А. Основные требования к диагностической аппаратуре на основе измерения собственных электромагнитных излучений биологических объектов. Системи управління навігації та зв'язку. 2011. Вип.4 (20). С. 124-131.

УДОСКОНАЛЕННЯ НАУКОВО-МЕТОДИЧНОГО АПАРАТУ ДЛЯ ПРОВЕДЕННЯ ЕКОЛОГІЧНОГО МОНІТОРИНГУ ЛІСІВ

Машков О.А., Пашков Д.П.
Державна екологічна академія післядипломної освіти та управління,
Київ, Україна

На сучасному етапі розвитку світового суспільства виникає ряд завдань що пов'язані з розробкою нових науково-методичних підходів та їх реалізація для проведені екологічного моніторингу з метою комплексного вивчення та проведення оцінювання стану лісів, а також контролю за станом лісних екосистем з ефективним їх застосуванням. Особливо важним є проведення екологічного моніторингу в важкодоступних та горяних масивах Карпат, де утруднено спостереження під час відновлення ушкоджених ділянок лісних масивів [1, 2].

В останнє десятиліття Україна багато уваги приділяє екологічному моніторингу та контролю за станом лісових масивів, а також вивчення біологічних ресурсів за допомогою оптико-електронних засобів дистанційно-пілотованих літальних апаратів (ДПЛА) [2]. У зв'язку з цим виникає необхідність розробки сучасних дистанційних методів оцінки стану та дослідження особливостей ландшафту для проведення найбільш ефективного контролю лісових екосистем. Це мають велике значення в справі охорони навколишнього середовища та раціонального природокористування, проектування лісових ділянок, таксації лісів, а також проектування заходів з охорони, захисту і відновлення лісів [1, 2].

Метою доповіді є висвітлення особливостей запропонованих науково-методичний апарат та моделей, які дозволять враховувати особливості контролю стану лісових масивів та здійснювати оцінювання для їх таксації. В зв'язку з цім, в доповіді розглядаються можливості ДПЛА для проведення екологічного моніторингу для оцінювання стану лісних масивів та вирішення екологічних завдань на основі обробки багатоспектральних знімків для якісного проведення екологічного контролю. Крім цього в доповіді запропоновано науковий підхід до визначення екологічного стану дерев для їх таксації оптико-електронними засобами, особливістю якої є оцінювання стану покрову дерев за допомогою обробки знімків в різних спектральних діапазонах по спектрально-енергетичним параметрам відбитого та власного випромінювання лісного покрову.

Список літератури

1. Боголюбов В.М. Моніторинг довкілля / [В.М. Боголюбов, М.О. Клименко, В.Б. Мокін та ін.] за редакцією В.М. Боголюбов і Т.А. Сафронова / – Херсон: Грінь Д.С. – 2011. – 530 с.

2. Севко О.А. Аэрокосмические методы в лесном хозяйстве / О. А. Севко. – Минск: БГТУ, 2005. – 170 с.

МЕТОДИ ТА ПІДХОДИ ДО ДЕТЕКТУВАННЯ АУДІОПОДІЙ РІЗНИХ ТИПІВ

Порошенко А.І., Коваленко А.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Відеоаналіз став стандартною функцією багатьох охоронних систем, але аудіоаналіз продовжує залишатися рідкісним явищем, незважаючи на наявність як самого аудіоканалу в пристроях, так і доступних обчислювальних потужностей для обробки звукової інформації. Проте, аудіоаналіз має деякі переваги в порівнянні з відеоаналізом, а саме вартість обладнання (мікрофонів) і його обслуговування значно дешевше, ніж відеокамер, та при роботі системи в режимі реального часу потік даних аудіоінформації значно менше за обсягом, ніж потік даних з відеокамер, що пред'являє більш лояльні вимоги до пропускної здатності каналу передачі даних.

Системи аудіоаналітики можуть бути особливо затребувані для міського спостереження, де можна автоматично почати транслювати живе відео на поліцейський пульт з місця виникнення певної ситуації [1]. Технології аудіоаналітикі також можуть використовуватися при вивченні відеозапису та визначенні подій.

Метою доповіді є дослідження та аналіз методів детектування аудіоподій різних типів, таких як постріли, биття скла та крик. Для аналізу результатів використовуються методи на основі стандартного відхилення нормованих значень потужностей блоків, на основі застосування медіанного фільтру для значень потужностей блоків та на основі динамічного порогу для значень потужностей блоків [2].

В доповіді наводяться результати аналізу методів детектування аудіоподій різних типів. Наведені дані показують, що перевагами методу на основі стандартного відхилення нормованих значень потужностей блоків є його стійкість до зміни рівня шуму та можливість детектування повільно мінливого сигналу, аналізуючи середнє значення нормованих блоків потужності.

Проте, метод на основі застосування умовного медіанного фільтру для значень потужностей блоків детектує аудіоподії на 6,36% точніше, але є досить складним та вимогливим для технічного обладнання. Метод на основі динамічного порогу для значень потужностей блоків є найпростішим, тобто може бути реалізованим при первинній обробці.

Список літератури

1. Choi, W., Rho, J., Han, D. K., & Ko, H. (2012). Selective background adaptation based abnormal acoustic event recognition for audio surveillance. In Proceedings - 2012 IEEE 9th International Conference on Advanced Video and Signal-Based Surveillance, AVSS 2012 (pp. 118-123).

2. Atrey, P.K. & Maddage, Namunu & Kankanhalli, Mohan. (2006). Audio Based Event Detection for Multimedia Surveillance. 5. V - V. 10.1109/ICASSP.2006.1661400.

ЗАСТОСУВАННЯ КОМПЛЕКСІВ РАДІОМОНІТОРИНГУ ДЛЯ КОНТРОЛЮ ЗА МЕРЕЖЕЮ РАДІОЗВ'ЯЗКУ

Іохов О.Ю., Каплун Є.О.
Національна академія Національної гвардії України, Харків, Україна

Серед головних завдань на сучасному етапі боротьби з тероризмом є створення ефективної системи розвідки у складі антитерористичних структур [1]. Однією з основних її підсистем має бути система радіомоніторингу за роботою засобів радіозв'язку, яка дозволить викривати систему управління терористів і видавати інформацію, необхідну для роботи засобів радіоелектронної боротьби [2].

Засоби радіоконтролю, які входять до сучасних комплексів радіомоніторингу, повинні забезпечувати виконання таких функцій:

– пошук і пеленгування джерел радіовипромінювань (радіозасобів);

– вимірювання параметрів сигналів (центральної частоти, зайнятої смуги частот, девіації частоти тощо) та визначення режимів роботи радіозасобів;

– розпізнавання джерел радіовипромінювання та складання описів непізнаних (незареєстрованих) джерел;

– визначення місця знаходження джерела радіовипромінювання;

– розпізнавання джерел радіозв'язку, здійснене за результатами вимірювання параметрів сигналів шляхом порівняння з еталонами, що зберігаються у банку даних;

– настроювання апаратури контролю на радіовипромінювання за пеленгом і частотою;

– первинна обробка результатів вимірювання;

– придушення, у разі необхідності, засобів зв'язку, інших радіозасобів (наприклад, радіовибухівок);

– розрахунок за результатами вимірювань відношення сигнал/завада у пункті приймання.

Список літератури

1. Тимочко О.І., Герасимов С.В., Лабунець В.О., Климович О.К. Оцінювання завада захищеності радіоканалу зв'язку безпілотного літального апарату у міських умовах // Військово-технічний збірник. – Л.: НАСВ. – 2018. – Вип. 18. – С. 14-18.

2. Івченко М.М., Герасимов С.В. Метод оцінки швидкості передачі інформації технологією MPLS за протоколом TCP проводових телекомунікаційних мереж // Наука і техніка Повітряних Сил Збройних Сил України. – 2019. – № 4(37). – С. 93-98. – https://doi.org/10.30748/nitps.2019.37.13.

УЧАСНИКИ КОНФЕРЕНЦІЇ (секції 3 – 5)

ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

Азербайджанське вище військове училище імені Гейдара Алієва, Баку, Азербайджан

Азербайджанський технічний університет, Баку, Азербайджан

Білоруський державний технологічний університет, Мінськ, Білорусь

Військова Академія Збройних Сил Азербайджанської республіки, Баку, Азербайджан

Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Полтава, Київ, Україна

Державне підприємство "Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості", Харків, Україна

Державний університет інфраструктури та технологій, Київ, Україна

Інститут державного управління та наукових досліджень з цивільного захисту, Київ, Україна

Інститут електродинаміки Національної академії наук України, Київ, Україна

Інститут систем управління Азербайджанської Національної академії наук, Баку, Азербайджан

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ", Київ, Україна

Київський національний економічний університет імені Вадима Гетьмана, Київ, Україна

Київський національний університет імені Тараса Шевченка, Київ, Україна

Київський національний університет технологій та дизайну, Київ, Україна

Міністерство Оборони Азербайджанської республіки, Баку, Азербайджан

Національна академія Національної гвардії України, Харків, Україна

Науково-виробниче підприємство ХАРТРОН-АРКОС ЛТД, Харків, Україна

Національний авіаційний університет, Київ, Україна

Національний аерокосмічний університет імені М. Є. Жуковського "Харківський авіаційний інститут", Харків, Україна

Національний технічний університет України імені Ігоря Сікорського "КПІ", Київ, Україна

Національний технічний університет "Харківський політехнічний інститут", Харків, Україна

Національний транспортний університет, Київ, Україна
Національний університет оборони України імені Івана Черняховського, Київ, Україна
Національний університет цивільного захисту України, Харків, Україна
Національний юридичний університет імені Ярослава Мудрого, Харків, Україна
Національний університет "Полтавська полытехніка імені Юрія Кондратюка", Полтава, Україна
Полтавська державна аграрна академія, Полтава, Україна
Полтавський коледж нафти і газу Полтавського національного технічного університету імені Юрія Кондратюка, Полтава, Україна
Сумський державний університет, Суми, Україна
ТОВ «Інріс-Профіль», Харків, Україна
ТОВ «Novel Projects & Solutions (NPS)», Дніпро, Україна
ТОВ «Харківський електромашинобудівний завод», Харків, Україна
Українська інженерно-педагогічна академія, Харків, Україна
Український державний університет залізничного транспорту, Харків, Україна
Уманський національний університет садівництва, Умань, Україна
Університет технології і гуманітарних наук, Бельсько-Бяла, Польща
Харківська державна академія фізичної культури, Харків, Україна
Харківський національний економічний університет імені Саймона Кузнеця, Харків, Україна
Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна
Харківський національний університет внутрішніх справ, Харків, Україна
Харківський національний університет імені В.Н. Каразіна, Харків, Україна
Харківський національний університет міського господарства імені О. М. Бекетова, Харків, Україна
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна
Харківський національний університет радіоелектроніки, Харків, Україна
Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ, Україна
Центральноукраїнський національний технічний університет, Кропивницький, Україна
Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля Національного університету цивільного захисту Україн, Черкаси, Україна

ЗМІСТ

НАУКОВЕ ВИДАННЯ

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей
одинадцятої міжнародної науково-технічної конференції
(8 – 9 квітня 2021 року)
Том 2: секції 3 – 5

Відповідальний за випуск *В. В. Косенко*
Технічний редактор *І. А. Лєбедева*
Коректор *В. В. Богомаз*
Комп'ютерне складання та верстання *Н. Г. Кучук*

Підписано до друку 02.04.2021 Формат 60 × 84/16
Ум.-вид. арк. 7,5. Тираж 150 пр. Зам. 402-21

Адреса оргкомітету: вул. Сумська, 130а, Харків, 61023, Україна
Державне підприємство " Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості "
тел. +38 (057) 704 10 47

Віддруковано з готових оригінал-макетів у друкарні ФОП Петров В.В.
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис № 24800000000106167 від 08.01.2009.
61144, м. Харків, вул. Гв. Широнінців, 79в, к. 137, тел. **(057) 778-60-34**
e-mail: **bookfabrik@mail.ua**