Черкаський державний
технологічний університет

Національний технічний університет
"Харківський політехнічний інститут"

Військова Академія Збройних Сил
Азербайджанської республіки

Університет технології і гуманітарних наук
(м. Бельсько-Бяла, Польща)

ДП «Південний державний проектно-конструкторський
та науково-дослідний інститут авіаційної промисловості»

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

ТЕЗИ ДОПОВІДЕЙ ДЕВ'ЯТОЇ МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

18 – 19 листопада 2021 року

Том 1

Черкаси – Харків – Баку – Бельсько-Бяла – 2021

УДК 004 : 681.3

У збірнику подано тези доповідей дев'ятої міжнародної науково-технічної конференції "Проблеми інформатизації". Розглянуті питання за такими напрямами: інформатизація навчального процесу; застосування, експлуатація та безпека функціонування телекомунікаційних систем та мереж; комп'ютерні методи і засоби інформаційних технологій та управління; методи швидкої та достовірної обробки даних в комп'ютерних системах та мережах; цивільна безпека (інформаційна підтримка); сучасні інформаційно-вимірювальні системи.

Затверджено до друку рішенням Науково технічної ради Черкаського державного технологічного університету (протокол від 04.11.2021 № 4).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

СЕКЦІЯ 1

ІНФОРМАТИЗАЦІЯ НАВЧАЛЬНОГО ПРОЦЕСУ

Керівник секції: д.т.н. проф. В. М. Рудницький, ЧДТУ, Черкаси
Секретар секції: к.т.н. доц. І. М. Федотова-Півень, ЧДТУ, Черкаси

ДОДАТОК ДЛЯ НАВЧАННЯ ШВИДКОЧИТАННЮ

Лещенко Ю.О., Горбатенко Є.О.
Національний аерокосмічний університет ім. М. Є. Жуковського
"Харківський авіаційний інститут", Харків, Україна

На даний час на зміну традиційним методам навчання (оволодіння інформацією) приходять нові методи з використанням інформаційних систем. Інформаційні системи стали привілеями людства у двадцять першому столітті та сприяють більш комфортному зберіганню та роботі з інформацією в мережі Інтернет [1].

Інформаційну систему можна віднести до інформаційних систем навчального призначення – адже головною метою буде надати користувачу майданчик з засобами оволодіння просунутими методами читання та опрацювання інформації. Окрім цього, інформаційна система повинна мати аналітично-оціночне значення – давати якісну оцінку навичкам користувача інформаційних систем, що були попередньо розраховані в кількісному еквіваленті.

За рахунок того, що інформація зосереджена в структурованому, попередньо опрацьованому, вигляді – підвищується швидкість оволодіння інформацією, тобто навчання, адже відсутня необхідність попередньо знаходити декілька авторитетних джерел інформації, та витрачати час на фільтрацію тексту та виділення основної його частини (процесу конспектування). Процес ознайомлення (читання) з інформацією, та уміння її обробки (перетворення інформації на дані) з метою визначення суті, головного, являється фундаментальним в житті сучасної людини, що прагне до інтелектуального розвитку.

Для реалізації додатку були використані такі програмні засоби: мови програмування JavaScript, HTML, CSS, СКБД MySql, phpMyAdmin, уніфікована мова моделювання UML. Реалізований веб-додаток дозволяє проводити тестування на швидкість читання (слів в хвилину), а також навчання на основі опрацьованих методик швидкочитання [2].

Створений веб-додаток буде поширюватись на умовно-безкоштовній основі, з метою навчання користувачів навику швидкочитання.

Список літератури

1. Програми для швидкочитання [Електронний ресурс] – Режим доступу: https://uk.soringpcrepair.com/software-for-speed-reading/.

2. Сайп, Р. Розвиток мозку: Як читати швидше, запам'ятовувати краще і добиватися великих цілей / Р. Сайп. – М. Манн, Іванов і Фербер, 2014. – 256 с.

ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА ФІКСАЦІЇ ТА КОНТРОЛЮ ВІДВІДУВАННЯ СТУДЕНТАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Паламарчук О.С., Паламарчук А.С.
Черкаський державний технологічний університет, Черкаси, Україна

Фіксація відвідування студентами занять, відповідно до їхнього навчального плану, здійснюється в журналах групи на кожному занятті старостою (заступником) та/або викладачем. Ці дані збираються та передаються в деканат для контролю та формування рейтингів успішності студентів. Оскільки цей процес здійснюється в ручному режимі, то часто присутній людський фактор, який впливає на точність та об'єктивність процесу фіксації. Автоматизація процесу фіксації зменшить часові затрати на опрацювання цих даних та вплив людського фактору [1].

Метою доповіді є розробка інформаційно-аналітичної системи (ІАС) фіксації та контролю відвідування студентами навчальних занять.

В доповіді представлено структуру системи, функціональні модулі та особливості її використання. Модуль *Студент* містить наступні дані: особисті дані, навчальні дані, контакти, посилання (на соцмережі та групи в мессенджерах). Модуль *Група* містить список групи та представлений у двох форматах: *академічна група* – для обов'язкових дисциплін та *збірна група* – для вибіркових дисциплін. Модуль *Розклад* містить розклад для академічної та збірної групи. Модуль *Аудиторний контроль* реалізований у вигляді застосунку для мобільного телефону. Студенту приходить повідомлення в застосунку, в якому вказано: № пари, її тривалість, аудиторія, корпус, назва дисципліни, вид заняття, ПІП викладача та послання для авторизації на даному занятті. Повідомлення надсилається після завершення поточної пари та перед початком наступної. В аудиторіях встановлені дисплейні термінали, на яких виводиться згенерований QR-код відповідно до кожного заняття та система фіксації присутніх абонентів. Студент через застосунок сканує QR-код на дисплейному терміналі та підтверджує свою реєстрацію. Після початку заняття система формує список присутніх студентів та надсилає його викладачу. В продовж заняття система в довільний час надсилає маркери для контролю відповідності зареєстрованих та присутніх в аудиторії студентів. Викладачі також використовують даний застосунок для реєстрації на заняття. Модуль *Статистика* надає можливість формувати звіти по кожному студенту, по групам, по дисциплінам, во викладачам та по часовим проміжкам. Модуль *Викладачі* містить дані кожного викладача, які поділені на кілька категорій: особисті дані, наукові дані, контакти, посилання на профілі та групи в соцмережах та мессенджерах).

Список літератури

1. Автоматизація вищих навчальних закладів // ОТС. – К.: ОТС. – Режим доступу [електронний ресурс]: http://www.otc.com.ua/files/ OTC_automation_VUZ.pdf.

РОЗРОБКА ВЕБ-ДОДАТКУ ДЛЯ ВІДЕОКОНФЕРЕНЦІЙ ІЗ ДЕТЕКТОРОМ ЕМОЦІЙНИХ СТАНІВ

Момот М.О., Зварич К.А.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

В теперішній час посилилося дослідження емоцій у взаємодії людина-комп'ютер. Завдяки успішній класифікації емоцій у режимі реального часу можна отримати миттєвий та правдивий зворотній зв'язок від користувачів, спростити сприйняття інформації від іноземних співбесідників, поліпшити обслуговування клієнтів, якість навчання, зрозуміти степінь залучення учнів [1]. Тому актуальною є проблема проведення відеоконференцій із детектором емоційних станів з можливістю відстеження та запису змін емоцій співбесідника для подальшого аналізу зворотного зв'язку.

Метою доповіді є дослідження існуючих додатків з функцією детектування обличь та емоцій людини з метою створення веб-додатку для відеоконференцій із детектором емоційних станів. **В доповіді** наводяться результати аналізу методів детектування обличчя людини; аналізу методів детектування емоційних станів людини; програмної реалізації веб-додатку, тестування додатку (тестування коду, тестування точності детектування обличчя людини, тестування точності детектування емоційних станів людини). В ході роботи було обрано MySQL для збереження даних про зміну емоцій співбесідника, сервер Open Server для розгортання БД та підтримки php-коду. Для реалізації був обраний алгоритм Віоли-Джонса [2], що використовується у FaceDetect API, оскільки даний метод має низьку кількість хибних спрацьовувань та високу точність детектування облич. Програмну частину було написано в середовищі розробки WebStorm мовою програмування високого рівня JavaScript із використанням бібліотеки React. Реалізовано такий функціонал:

1) створення кімнати для відеоконференції;
2) обмін повідомленнями;
3) обмін файлами;
4) налагодження відеозв'язку;
5) детектування емоційних станів у реальному часі;
6) запис даних про зміну емоційних станів до БД;
7) запис середньозваженої емоції дзвінку;
8) запис відеодзвінку.

Список літератури

1. James A. Coan, John J.B. Allen. Handbook of emotion elicitation and assessment // Oxford, UK: Oxford University Press, 2007 – 504 p.

2. Paul Viola, Michael J. Jones. Robust Real-time Object Detection. // Cambridge Research Labortory (CRL) 2001/01, Technical Report Series – Cambridge, Massachusetts 02142 USA, 2001. – 30 p. https://www.hpl.hp.com/techreports/Compaq-DEC/CRL-2001-1.pdf

МЕТОДИ ТА ЗАСОБИ ІНФОРМАТИЗАЦІЇ ПРОФЕСІЙНОЇ ПІДГОТОВКИ АВІАДИСПЕТЧЕРІВ

Сурков К.Ю., Суркова К.В.
Льотна академія Національного авіаційного університету,
Кропивницький, Україна

Інформатизація професійної підготовки авіадиспетчерів передбачає впровадження і застосування сучасних досягнень в галузі інформаційних технологій при виконанні всіх завдань навчання. Питанню інформатизації, всіх її аспектів присвячено багато наукових напрацювань, як теоретичного, так і практичного плану (В.П. Безпалько, М.І. Бєляєв, В.Ю. Биков, В.В. Гриншкун, І.В. Роберт, М.І. Жалдак, Г.М. Коджаспірова та ін.). Методи та засоби інформатизації освіти спрямовані на виконання багатьох завдань: організації негайного зворотного зв'язку між користувачем і засобами інформатизації і комунікації; комп'ютерної візуалізації навчальної інформації про об'єкти або закономірності процесів, явищ; комп'ютерного моделювання досліджуваного об'єкта або процесу та ін. [1].

Метою доповіді є формування комплексу методів та засобів інформатизації професійної підготовки авіадиспетчерів, який дозволить змоделювати середовище професійної діяльності авіадиспетчерів в навчання.

В доповіді наводяться особливості професійної підготовки авіадиспетчерів, які повинні враховуватися при відборі методів та засобів інформатизації (великий об'єм навчальної інформації, яку треба засвоїти за порівняно невеликий проміжок часу, необхідність моделювання професійної діяльності авіадиспетчерів з використанням часових і інформаційних умов професійної діяльності та ін.). Розглянуто критерії вибору методів та вимоги до створення засобів інформатизації. В якості засобів інформатизації запропоновано: веб-сайти професійного спрямування (наприклад, прослуховування реального радіообміну [2]), відео- та аудіозасоби, електронні засоби навчання (наприклад, автоматизована навчальна система з обслуговування повітряного руху, в якій реалізовано адаптивний підхід [3]) та ін. Комплекс методів та засобів інформатизації сприятиме формуванню середовища навчання наближеного до реального професійного середовища авіадиспетчерів.

Список літератури

1. Роберт И.В. Современные информационные технологии в образовании: дидактические проблемы; перспективы использования: монография. М.: ИИО РАО, 2010. 140 с.

2. Listen to the clouds. URL: http://listentothe.cloud (дата звернення: 24.10.2021)

3. Сурков К.Ю., Суркова К.В., Кущ О.В., Войченко Т.О. Модель дій диспетчера управління повітряним рухом для формування навчальної вибірки адаптивного тренажеру. *Новітні технології.* 2019. Випуск 1(8). С. 203-207. DOI: https://doi.org/10.31180/2524-0102/2019.1.08

АВТОМАТИЗАЦІЯ ПЕРЕВІРКИ ІНФРАСТРУКТУРНОГО РІШЕННЯ В ХМАРІ

Костромицький А.І., Калиняк І.Д.
Харківський національній університет радіоелектроніки, Харків, Україна

Сучасний розвиток організації навчальних процесів дедалі більше спонукає переходу повноцінного навчання до онлайн форми. Результатом цих розвитку є постійне збільшення кількості студентів завдяки розповсюдженню більш зручної форми навчання серед різних форм навчання на лекціях, курсах і т.п. Всесвітня пандемія також внесла несподівані корективи і змусила всіх терміново опановувати цифрові інструменти й нові педагогічні підходи для створення підґрунтя переходу більшості практичних завдань на дистанційну основу.

Відповідно до цього слід зазначити, що інтенсифікація навчального процесу хмарним технологіям через автоматизацію є вкрай важливим аспектом для перевірки розв'язання завдань дистанційного навчання.

Метою проведених досліджень є винаходження методу побудови повноцінної автоматизації перевірки завдань інфраструктурного рішення в хмарних технологіях на основі порівняння базисного та модифікованого стану хмарної інфраструктури після виконання студентом завдання по створенню певних ресурсів у хмарному середовищі.

Даний метод являє собою підрахунок різниці стану середовища між попередньо розгорнутими хмарними ресурсами для завдання та створеними студентами власноруч.

Метод перевірки складається з таких кроків, як запуск автоматизованого розгортання базисної інфраструктури завдання, розв'язання студентом завдання у хмарному середовищі та перевірки стана інфраструктури або шляху вирішення завдання студентом за ключовими етапами.

Серед переваг вищезгаданого методу автоматизації треба відмітити ріст швидкості перевірки завдань, універсальний підходу для створення методології автоматизації та зменшення ролі людського фактору під час перевірки завдання.

Список літератури

1. Лотоцька А. А., Пасічник О. А. Організація дистанційного навчання. Методичні рекомендації. 2020. С. 22–27, https://mon.gov.ua/storage/app/media/zagalna%20serednya/metodichni%20recomendazii/2020/metodichni%20recomendazii-dustanciyna%20osvita-2020.pdf

2. Johnson, L., Levine, A., & Smith, R. (2009). The 2009 Horizon Report. One Year or Less: Cloud Computing. Austin, Texas: The New Media Consortium, http://www.nmc.org/pdf/2009-Horizon-Report.pdf.

ОРГАНІЗАЦІЯ РОЗПОДІЛЕНОЇ ТЕМАТИЧНОЇ КОМУНІКАЦІЙНОЇ ПЛАТФОРМИ

Холєв В.О., Барковська О.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

Активна фаза трансформації традиційних бібліотек в розподілені електронні бібліотеки, задачею яких є збереження та накопичення великої кількості інформаційного контенту у структурованому вигляді [1], а також легкість доступу [2] до цільових даних обумовлює актуальність розробки розподіленої тематичної комунікаційної платформи, як такої, що забезпечить цілісність, достовірність та надійність зберігання та обробки текстового контенту із використанням енергоефективних високопродуктивних обчислювальних комплексів.

Метою роботи є забезпечення цілісності, достовірності та конфіденційності доступу цільової аудиторії до запропонованої [3] розподіленої системи збору та структурованого зберігання інформаційного контенту.

Цільовими користувачами запропонованої системи є науковці, наукові ментори, а також роботодавці, які прагнуть ділитися науковими напрацюваннями, а також дізнаватися про новітні наукові доробки від авторів. Система передбачає доступ автентифікованих експертів та студентів до віртуальних кімнат для спілкування та подальше автоматичне узагальнення обговорених тем.

Для забезпечення такого функціоналу у роботі запропонована багаторівнева система автентифікації (на основі обличчя та голосу) та метод прискореної обробки природної мови на основі систем із масовим паралелізмом.

Практичні результати можуть призвести до поглиблення та прискорення досліджень, до актуалізації стану наукових напрямків, а також для залучення молодих спеціалістів безпосередньо до виробничо-практичної роботи саме в області їх знань та інтересів.

Список літератури

1. J. N. Madhuri and R. Ganesh Kumar, "Extractive Text Summarization Using Sentence Ranking," 2019 International Conference on Data Science and Communication (IconDSC), 2019, pp. 1-3, doi: 10.1109/IconDSC.2019.8817040.

2. R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia and J. Fierrez, "Increasing the robustness of biometric templates for dynamic signature biometric systems," 2015 International Carnahan Conference on Security Technology (ICCST), 2015, pp. 229-234, doi: 10.1109/CCST.2015.7389687.

3. Barkovska, O., Pyvovarova, D., Kholiev, V., Ivashchenko, H., Rosinskyi, D. Information object storage model with accelerated text processing methods. // CEUR Workshop Proceedingsthis link is disabled, 2021, 2870, стр. 286–299.

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ ОСВІТИ ПРИ ДИСТАНЦІЙНІЙ ФОРМІ НАВЧАННЯ

Чеботарьова Д.В., Красніков В.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Пандемія COVID-19 суттєво вплинула практично на всі сфери суспільного життя, в тому числі і на систему освіти. Одним із способів стримування коронавірусної інфекції залишається соціальна ізоляція і її заходи потребують часткового або повного закриття освітніх установ [1], переведення навчального процесу в дистанційну форму та наявності певної інфокомунікаційної інфраструктури для його забезпечення.

Питання дистанційного навчання на сьогоднішній день має дуже важливе значення, але цей тип освіти має декілька вагомих недоліків. Основні проблеми дистанційної форми навчання: низький рівень технічного забезпечення здобувачів освіти та викладачів (обмежений доступ до комп'ютерів, брак сучасних мобільних пристроїв у викладачів та учнів, брак інтернет-зв'язку) [2]. Важливими також є проблеми вибору ефективної навчальної платформи та труднощі отримання здобувачами освіти необхідних практичних навичок на потрібному профільному обладнанні.

Метою доповіді є аналіз проблем інформатизації освіти та оптимізація освітнього процесу при дистанційній формі навчання.

В доповіді наводяться статистичні дані щодо інформаційної грамотності людей причасних до навчального процесу та технічних можливостей. Результати аналізу свідчать про те, що структура та особливості організації дистанційного навчання прямопропорційно впливають на ефективність навчання, а також мотивованість і успішність здобувачів освіти.

Для рішення основних проблем дистанційного навчання пропонуються: впровадження оптимізації технічного забезпечення навчальних закладів та інтегрування хмарних сервісів в заклади освіти, створення єдиної бази навчального контенту та єдиної освітньої платформи для навчальних закладів, розвиток та створення сучасних багатофункціональних віртуальних симуляторів, що дозволять дистанційно отримувати навики в роботі з потрібною профільною апаратурою та технологіями. Всі ці зміни ефективно вплинуть на дистанційне навчання та інформатизацію освітнього процесу.

Список літератури

1. Зенков А.Р. Образование в условиях пандемии: что показывает кризис? *ИМЭМО РАН.* 2020. DOI: https://www.imemo.ru/news/events/text/obrazovanie-v-usloviyah-pandemii-chto-pokazivaet-krizis.

2. Чепурко Г. І. Найбільшою проблемою дистанційного навчання називають технічне забезпечення – опитування. *Нова українська школа.* 2021. DOI: https://nus.org.ua/news/tehnichne-zabezpechennya-najbilsha-problema-dystantsijnogo-navchannya/.

АНАЛІЗ ПРОГРАМНОГО ТА ІНФОКОМУНІКАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОСВІТНЬОГО ПРОЦЕСУ

Чеботарьова Д.В., Осадча Ю.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Інформатизація освіти – це створення і використання інформаційних технологій для підвищення ефективності видів діяльності, що здійснюються в системі освіти [1]. Інформатизація освіти є важливим механізмом модернізації освітнього процесу, який спрямований на підвищення якості, доступності й ефективності освіти.

З ростом обсягу інформації, що необхідно опрацьовувати та аналізувати студентам і викладачам, зростає потреба в створенні програмного забезпечення різного плану: навчального (отримання та засвоєння нової інформації), діагностичного (для перевірки рівня отриманих знань), тренувального (закріплення пройденого матеріалу), імітаційного (вивчення основних структурних чи функціональних характеристик), моделюючого (навчання шляхом моделювання певної ситуації). Усе це програмне забезпечення може сприяти організації та індивідуалізації навчання, створенню більш комплексного підходу до вивчення певної дисципліни, та контролю прогресу навчання, особливо в умовах впровадження дистанційного навчання.

Метою доповіді є аналіз існуючого програмного, інформаційного та комунікаційного забезпечення освітнього процесу. Сьогодні з'являються можливості значної інтенсифікації спілкування, врахування індивідуальних нахилів і здібностей, розкриття творчого потенціалу викладачів і студентів, диференціації навчання відповідно до особливостей студентів тощо.

На даний момент у багатьох закладах освіти існує програмне забезпечення, що націлене на оцінювання знать студента. Для покращення та більш практичного використання програмного забезпечення можливо запропонувати розробки програмного забезпечення, що могло б поєднувати в собі як інформаційну складову, так і комплекс завдань у вигляді тестування і відкритих коротких відповідей після кожної теми. Це може покращити розуміння того, над чим необхідно додатково працювати для кращого розуміння опрацьованого матеріалу студентом.

Також можливе створення переліку додаткової літератури в форматі посилань на відповідні джерела, для спрощення пошуку.

Таким чином можна створити інтерактивний підручник для навчання у різних галузях, з проміжним контролем навчання.

Список літератури

1. Завальна І. Інформатизація освіти як чинник розвитку інформаційного суспільства. *Вісник Національного університету "Львівська політехніка"*. 2017. № 865. С. 211 – 214. DOI: http://science.lpnu.ua/sites/default/files/journal-paper/2018/jun/13265/34.pdf.

ВПРОВАДЖЕННЯ МОБІЛЬНИХ ТЕХНОЛОГІЙ В ОСВІТНІЙ ПРОЦЕС

Бельорін-Еррера О.М.
Національний технічний університет «ХПІ», Харків, Україна
Чепела С.П.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні інформаційні технології надають необмежні можливості та водночас викликають необхідність змін в організації навчального процесу.

Електронне навчання (e-learning) та все більш зростаюча роль мобільних пристроїв у повсякденному житті обумовили появу нового способу навчання, а саме – мобільного навчання. Функціональні можливості сучасних мобільних телефонів дозволяють організувати освітній процес з використанням спеціалізованих електронних підручників та курсів, адаптованих для перегляду та виконання на мобільних телефонах. Так, завдяки сучасним технологіям навчання стає набагато цікавішим та доступнішим.

Слід також зазначити, що більшість студентів технічно та психологічно готові до використання мобільних технологій в освіті.

Аналізуючи наукові джерела стосовно впровадження мобільних технологій у освітній процес [1-5], можна констатувати їх очевидну користь та доцільність.

Зокрема, використання мобільних технологій:

- дозволяє суб'єктам освітнього процесу вільно переміщуватись;
- розширює рамки навчального процесу поза межі навчального закладу;
- надає можливість навчатися людям з особливими потребами;
- не вимагає придбання персонального комп'ютера та паперової навчальної літератури;
- передбачає легке поширення навчальних матеріалів між користувачами завдяки бездротовим сучасним технологіям (WAP, GPRS, EDGE, Bluetooth, Wi-Fi);
- сприяє кращому розумінню та засвоєнню матеріалу, підвищує інтерес до навчання.

Список літератури

1. Hashemi M., Azizinezhad M., Najafi V., Nesari A. What is Mobile Learning? Challenges and Capabilities // Procedia – Social And Behavioral Sciences. 2011. № 30. P. 2477–2481.

2. Hockly N. Mobile learning // ELT J.: English Language Teaching J. 2013. № 67 (1). P. 80-84.

3. Jonas-Dwyer D.D., Clark C., Celenza A., Siddiqui Z.S. Evaluating Apps for Learning and Teaching // Intern. J. of Emerging Technologies In Learning. 2012. № 7 (1). P. 54 – 57.

4. Khaddage F., Lattenmann C. The future of mobile apps for teaching and learning / Berge, Zane L., Muilenburg, Lin Y.(Eds) // Handbook of mobile learning. NY: Routledge, 2013. P. 119–128.

СЕКЦІЯ 2

ЗАСТОСУВАННЯ ТА ЕКСПЛУАТАЦІЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Керівник секції: д.т.н. проф. С. Г. Семенов, НТУ "ХПІ", Харків
Секретар секції: к.т.н. С. С. Бульба, НТУ "ХПІ", Харків

DETERMINING THE SPEED OF INFORMATION TRANSMISSION IN THE FIELD COMPUTER NETWORKS IN THE PROCESS OF NETWORK DESIGN

Nastakalov A.R.
Military Academy of the Armed Forces of Azerbaijan Republic

Radio relay, troposphere and satellite communication channels are mainly used to provide field command points with uninterrupted data transmission. Due to the fact that the speed of information transmission here is limited by the technical parameters of the radio device, and also depends on the weather conditions and relief, the channels do not have high bandwidth for information [1, 2]. For this reason and to ensure the backup channels in the field conditions networks are built on the principle of mesh topology of communication. In field computer networks, it is important to determine the maximum speed for transmitting information from the server to each node in isolation, as well as to all nodes simultaneously in the network design process. This thesis presents a method for determining the speed of data transmission for each node in the field computer networks.

References

1. Борш, В. И., Коваль, В.В., Туманов Ю. Г. Вероятность безотказной работы оборудования радиодоступа к стационарным сетям электросвязи, *Аппаратура связи*. 2000. С. 29–31.
2. Muriel Médard, "Network Reliability and Fault Tolerance", Massachusetts Institute of Technology | MIT Department of Electrical Engineering and Computer Science, Laboratory for Information and Decision Systems, Cambridge, MA 02139, 2003.

UEFI FIRMWARE VULNERABILITIES

Zamytskyi E.S, Holubnychyi D.Yu.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

The purpose of the report is to show that the security of one of the most indispensable parts of a computer is still in danger. Regarding Unified Extensible Firmware Interface (UEFI) as a system, even nowadays, plenty of issues can be pointed out. One of

the main adversities with UEFI is that its codebase is usually provided by different producers, and existing ways of detecting the issues cannot be beneficial in each case. Preventing or detecting firmware threats could work only when the developer has access or control to both hardware and software stacks, for example, Microsoft and Apple can be put there. Otherwise, the developers will have to deal with some sorts of potential problem. Going directly to the root of vulnerabilities, UEFI updates are still the most effective method of infection. The thing is, that usual update not only includes main firmware updates but also delivers it to a variety of other destinations, like CPU, embedded firmware, and even hardware units inside a baseboard, which can be threatening. List of the main types of UEFI or BIOS vulnerabilities: **Malicious peripheral devices** – involves implanting peripheral devices during the delivery or production phases; **Nonsecure root of trust** – involves compromising the root of trust from OS through its communication interfaces with firmware; **Misconfigured protections** – involves a misconfiguration of a protection system to facilitate the possible bypass later on; **Unauthenticated UEFI/BIOS update process** – involves any modifications from the attacking side on the update image; **Outdated UEFI/BIOS with already known security issues** – even after patching firmware codebase, some developers still use the outdated version of the firmware, that is why it is still of the most common security failures in UEFI/BIOS firmware; **Implanted UEFI/BIOS updates** – involves jeopardizing a vendor website or application for delivering an infected update image.

Even nowadays, looking at the National Vulnerability Database, many issues can be detected on the UEFI or BIOS level. For example, the most recent ones are CVE-2021-21574 and CVE-2021-21555, which date back to the summer of 2021.

References

1. National Vulnerability Database: https://nvd.nist.gov/
2. Unified Extensible Firmware Interface Forum: https://uefi.org/specifications

ДОСЛІДЖЕННЯ ФУНКЦІЙ ТА СИНТЕЗ СТРУКТУРИ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ «ХЕСЕД ДОРОТ»

Хрульов М.В., Пестров Д.І.
Черкаський державний технологічний університет, Черкаси, Україна

На сьогоднішній день благодійні організації є важливою складовою частиною громадянського суспільства та вагомим сегментом соціального життя країни [1], а тому вони потребують чіткої інформаційної підтримки. Зокрема благодійні організації потребують автоматизації їх діяльності для інформаційного обслуговування – організованого безперервного технологічного процесу підготовки, видачі та надання допомоги особам, які її потребують.

Метою доповіді є дослідження функцій та синтез структури автоматизованої інформаційної системи благодійної організації «Хесед Дорот», призначеної для інформаційної підтримки та автоматизації діяльності, пов'язаної з наданням допомоги, фізичним особам та медичним закладам, які можуть

потребувати допомоги. В доповіді, відповідно до [2], досліджено функції автоматизованої інформаційної системи [3] благодійної організації «Хесед Дорот» та її підсистем, синтезовано структуру автоматизованої інформаційної системи. Описано математичну модель максимальної інтенсивності потоку заявок, на основі якої виконано розрахунок необхідної продуктивності серверу автоматизованої інформаційної системи благодійної організації «Хесед Дорот». Запропоновані в роботі рішення дозволяють побудувати високопродуктивну автоматизовану інформаційну систему благодійної організації «Хесед Дорот», яка в свою чергу дозволить швидко та якісно обслуговувати осіб, які потребують допомоги та вирішувати інші соціальні проблеми.

Список літератури

1. Як вірно благодійному фонду приймати та надавати допомогу. URL: https://www.prostir.ua/?blogs=yak-virno-blahodijnomu-fondu-pryjmaty-ta-nadavaty-dopomohu
2. Балашов Е. П. Эволюционный синтез систем М. : Радио и связь, 1985. 328 с.
3. Автоматизовані інформаційні системи для підприємств та організацій. URL: https://pidru4niki.com/12370107/informatika/

ІНТЕГРАЛЬНИЙ ПОКАЗНИК ЕФЕКТИВНОСТІ РЕПЛІКАЦІЇ ДАНИХ У МУЛЬТИХМАРНИХ СИСТЕМАХ

Козіна О.А.
Національний технічний університет «Харківський політехнічний інститут»

Висока доступність, надійність та запобігання блокуванню даних є найважливішими параметрами мультихмарних систем, що об'єднують у собі ресурси різних провайдерів хмарних сховищ даних. Хоча такі сховища можуть відрізнятися за моделлю даних, узгодженістю, моделлю підтримки транзакцій даних і ціною обслуговування, розгортання додатків і реплікація даних у трьох провайдерів призводить до більшої доступності на тлі складнощів з реплікацією даних та управлінням мережевої затримки [1, 2]. Тому пошук компромісу між узгодженістю та мережевою затримкою при різних механізмах розповсюдження оновлень даних є важливою науковою проблемою [3].

Метою доповіді є побудова математичної моделі розрахунку інтегрального показника ефективності механізму реплікації даних у географічно розподілених мультихмарних системах. В доповіді обґрунтовується необхідність оцінки корисності використання у мультихмарній системі різних протоколів реплікації, що впливають на мережну затримку доступу до актуальних даних, та відображують реалізовану модель узгодження даних. Наведені результати вимірювань часу відгуку під час оновлень даних, що було ініційовано користувачами, у трьох хмарних провайдерів свідчать про необхідність розгляду впливу мапи дата-центрів кожного хмарного провайдера на кількість реплік, що доцільно розташовувати загалом у кожного провайдера хмарних послуг. Запропоновано до складу інтегрального показника ефективності додати кількість реплік та показник їхнього географічного розосередження.

Список літератури

1. Wu Z., Madhyastha H. V. Understanding the Latency Benefits of Multi-Cloud Web-service Deployments. *ACM SIGCOMM Computer Communication Review*. 2013. Vol. 43, № 2. pp. 13-20. DOI: https://doi.org/10.1145/2479957.2479960

2. Eischer M., Straßner B., Distle T. Low-latency geo-replicated state machines with guaranteed writes. *PaPoC '20: Principles and Practice of Consistency for Distributed Data*. 2020. Article № 13. pp. 1–9. DOI: https://doi.org/10.1145/3380787.3393686

3. Mansouri Y., Toosi A. N., Buyya R. Data Storage Management in Cloud Environments: Taxonomy, Survey, and Future Directions. *ACM Computing Surveys*. 2017. Vol. 50, Issue 6, Article № 91, pp. 1–51. DOI: https://doi.org/10.1145/3136623

МОДЕЛІ ТА МЕТОДИ ПІДВИЩЕННЯ ТОЧНОСТІ НАВІГАЦІЇ ТА НАВЕДЕННЯ

Гуртовий О.О.
Харківський національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Використання різних систем навігації та методів наведення для орієнтації у просторі й визначення поточних координат ракети-носія при наявності перешкод та відсутності достатньої видимості призводить до значних похибок при отриманні навігаційної інформації. Тому виникає задача теоретичного дослідження комплексування навігаційних даних за технологією Data Fusion [1]. Однією з найважливіших складових вирішення цієї проблеми є багаторівнева технологія злиття даних з різних джерел для створення та розвитку метамоделі розподілених джерел даних, моделі об'єднання рішень [2]. Із завданнями підвищення точності навігації та наведення об'єктів ракетно-космічної техніки пов'язана необхідність розробки нових підходів і моделей для дослідження експериментальних даних, тому тема є актуальною та практично-значимою. Метою доповіді є розробка та опис моделей підвищення точності навігації та наведення, що враховує можливість отримання даних з різних навігаційних приладів, та дозволяє сумісно використовувати її за технологією Data Fusion, як в системі навігації так і в системі наведення, для забезпечення безперервної роботи всієї системи на різних фазах навігації. В доповіді формулюються завдання та мета дослідження, визначаються основні приватні завдання, пропонуються алгоритми комплексування навігаційних даних у системах керування об'єктів авіаційно-ракетної техніці.

Список літератури

1. Data Fusion [Электронный ресурс] / Jens Bleiholder, Felix Naumann, ACM Comput. Surv., v.41, 1, Article 1. 2008, 41 p. – Режим доступа: http://doi.acm.org/10.1145/1456650.1456651.

2. Shmelova, T., Sikirda, Y., Rizun, N., Kucherov, D., & Dergachov, K. (Eds.). (2019). Automated Systems in the Aviation and Aerospace Industries. IGI Global

ДОСЛІДЖЕННЯ І СИНТЕЗ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТОВ "ДЖОНСОН І ДЖОНСОН УКРАЇНА"

Тазетдінов В.А., Блажко Ю.С.
Черкаський державний технологічний університет, Черкаси, Україна

На сьогоднішній день комп'ютерні мережі є невід'ємною складовою частиною повсякденного життя. Як свідчить проведений аналіз мережа надзвичайно вразлива [1]. Вона може слугувати місцем витоку інформації, зміни конфігурації налаштувань та модифікації даних зловмисниками. Існує набагато більше загроз, тому стан захищеності мережі [2] вимагає значної уваги щодо забезпечення рівня захисту мережі з метою підтримування конфіденційності та цілісності даних. Для перевірки рівня безпеки та зміцнення мережі організації необхідно регулярно проводити оцінку вразливості всієї мережі [3].

Метою доповіді є дослідження і синтез структури комп'ютерної мережі ТОВ «Джонсон і Джонсон Україна». Зокрема розглядаються типи та надається класифікація різних видів комп'ютерних мереж, визначаються потреби та способи реалізації спроектованої мережі. Було виконано моделювання комп'ютерної мережі ТОВ «Джонсон і Джонсон Україна», яка здатна надавати якісний доступ до мережі Internet і забезпечувати інформаційні потреби організації у повному обсязі. Змодельована комп'ютерна мережа також забезпечує безпеку мережевого оточення за рахунок використання відмовостійкого мережевого обладнання та сучасного програмного забезпечення. Впровадження такої мережі на підприємстві ТОВ «Джонсон і Джонсон Україна» дозволить значно підвищити продуктивність праці і покращити рівень інформаційного обслуговування.

В доповіді виконано аналіз мережевих топологій та обрано варіант топології мережі «зірка», особливістю якої є висока швидкість передачі даних, надійність та простота реалізації.

Проведені в роботі дослідження комп'ютерних мереж дозволили змоделювати структуру комп'ютерної мережі ТОВ «Джонсон і Джонсон Україна» для її подальшої фізичної реалізації.

Список літератури

1. Кавун С. В. Інформаційна безпека: підручник / С. В. Кавун. - Харків : Вид. ХНЕУ, 2009. - 368 с.

2. Антонюк А. О., Жора В. В. Теоретичні основи моделювання та аналізу систем захисту інформації: [монографія] / А. О. Антонюк, В. В. Жора. - Ірпінь Національний університет ДПС України, 2010. - 310 с.

3. Балацька В.С., Шабатура М.М. Дослідження комп'ютерної мережі сканером вразливості Nessus. Вісник Львівського державного університету безпеки життєдіяльності. - 2019. - № 20. - С. 6-11. DOI: https://doi.org/10.20998/2522-9052.2018.1.04

АВТОМАТИЗОВАНА СИСТЕМА КОНТРОЛЮ НАДАННЯ ПОСЛУГ ВАНТАЖОПЕРЕВЕЗЕНЬ

Миронець І.В., Бойко М.Р.
Черкаський державний технологічний університет, Черкаси, Україна

У наш час різна діяльність різних компаній не обходиться без дуже тісної співпраці з компаніями, які займаються вантажоперевезеннями (транспортно-експедиційна компанія). Для багатьох компаній якісна, швидка, своєчасна доставка різного вантажу є одним з найважливіших факторів, які впливають на розвиток і стабільність даної компанії. Для приватних компаній високий рівень надання транспортних послуг є не менш важливим, тому що це запорука впевненості і повного спокою під час перевезення майна. Внаслідок цього, з кожним роком зацікавленість і попит на різні вантажоперевезення росте.

Компанії, які займаються транспортуванням, надають клієнтам все більш і більш широкий спектр послуг. При цьому, організація дає «стовідсоткову» гарантію їх високої якості. Спочатку шлях товару або вантажу бере початок з розробки концепції та оптимального маршруту, по якому буде рухатися вантаж, обчислення і розрахунку всієї вартості даної доставки, підготовки всієї необхідної документації. Потім визначаються транспортні та вантажні засоби, необхідні для даного товару. Далі відбувається оформлення необхідних дозволів, проводиться моніторинг руху товару з моменту початку шляху і до моменту, коли вантаж буде доставлений. Моніторинг здійснюється за допомогою системи контролю «Старший брат», яка може бути встановлена на мобільний пристрій будь-якого замовника. До функціональних можливостей даної програми належать: створення замовлення, відстеження замовлення, оплата замовлення, отримання інформації: про працівника, який виконує замовлення, про транспорт, переглянути історію замовлень.

Спектр послуг з вантажоперевезень:

— страхування вантажів, що перевозяться;
— транспортування великовагових і негабаритних вантажів;
— повна упаковка товару;
— при перевезенні застосовується система супутникової навігації, яка контролює вантаж протягом усього маршруту.

Вартість транспортування залежить від: ваги, габаритів, дальності транспортування товару, часу, витраченого на навантаження, вартості кілометражу, а також від компанії, яка надає дані послуги.

Список літератури

1. https://ru.wikipedia.org/wiki/%D0%93%D1%80%D1%83%D0%B7%D0%BE%D0%BF%D0%B5%D1%80%D0%B5%D0%B2%D0%BE%D0%B7%D0%BA%D0%B8
2. https://blankforma.com/nakladnaya-formata-a5/

КОМП'ЮТЕРИЗОВАНА СИСТЕМА УПРАВЛІННЯ ЗАСОБОМ РУХУ ДЛЯ ЛЮДЕЙ З ОБМЕЖЕНИМИ ФІЗИЧНИМИ МОЖЛИВОСТЯМИ

Хрульов М.В., Сидоренко В.Р.
Черкаський державний технологічний університет, Черкаси, Україна

За даними Всесвітньої організації охорони здоров'я близько мільярда людей в усьому світі мають фізичні обмеження. У Європі й Америці це кожен п'ятий. І оскільки вони мають менші шанси знайти роботу, рівень бідності серед цих людей вдвічі вищий за середній [1].

Станом на 1 січня 2020 року, в Україні 2,7 млн. осіб мали інвалідність, у тому числі 222,3 тис. осіб з I групою інвалідності, 900,8 тис. осіб з II групою інвалідності, 1416,0 тис. осіб з III групою інвалідності та 163,9 тис. дітей з інвалідністю [2]. Якби мільйон людей з обмеженими можливостями могли працювати, лише британська економіка зросла б на 1,7%, або на 64 млрд. доларів, свідчать дані доброчинної організації Scope [1].

Тому технології, які можуть допомогти людям з обмеженими фізичними можливостями ефективніше проявляти себе на робочому місті, а також поліпшити якість життя, без сумнівів, необхідні.

Метою доповіді є дослідження функцій та синтез структури комп'ютеризованої системи управління засобом руху для людей з обмеженими фізичними можливостями**.**

В доповіді досліджено підстави для розробки та переваги комп'ютеризованої системи управління засобом руху для людей з обмеженими фізичними можливостями. Досліджено функції та синтезовано структуру комп'ютеризованої системи управління засобом руху для людей з обмеженими фізичними можливостями на основі функціонально-структурного підходу [3]. Описано основні математичні моделі, на основі яких обрано обладнання, що забезпечить роботу системи.

Запропоновані рішення дозволять побудувати багатофункціональну комп'ютеризовану систему з допомогою якої люди з обмеженими фізичними можливостями матимуть змогу керувати засобом руху, а також поліпшити якість свого життя.

Список літератури

1. BBC NEWS Україна – [Електронний ресурс]. – Режим доступу : https://www.bbc.com/ukrainian/science/2016/02/160202_tech_disability_ko

2. Міністерство соціальної політики України – [Електронний ресурс]. – Режим доступу : https://www.msp.gov.ua/timeline/invalidnist.html.

3. Балашов Е. П. Эволюционный синтез систем / Е. П. Балашов. — М. : Радио и связь, 1985. — 328 с.

ВЕБ-ДОДАТОК АВТОРСЬКОЇ ФОТОСТУДІЇ «PHOTOLAB»

Лещенко Ю.О., Волощенко І.С.
Національний аерокосмічний університет ім. М. Є. Жуковського
"Харківський авіаційний інститут", Харків, Україна

У зв'язку зі стрімким розвитком технологій підприємства та компанії в різних сферах бізнесу зазнають ряд змін. В першу чергу ці зміни були спровоковані швидким ростом користувачів всесвітньої мережі Інтернет. За даними ресурсу Mediascope, на початок 2021 року понад 4,6 мільярда людей користуються Інтернетом, а аудиторія соціальних мереж перевищила позначку в 3,8 мільярда. Майже 60% світового населення вже онлайн, і є всі підстави вважати, що вже до кінця року половина всіх людей на планеті будуть користуватися соцмережами. Тому використання всесвітньої мережі Інтернет для розвитку будь-яких організацій і компаній життєво необхідно.

Найбільш доцільним рішенням для компаній, що займаються наданням послуг, є впровадження інформаційної системи з веб-інтерфейсом, що забезпечить стабільне надходження нових клієнтів, а також допоможе автоматизувати прийом заявок на придбання послуг, що, в свою чергу, призведе до зниження витрат.

Аналіз сфери фото послуг, використовуючи дані електронного картографічного довідника 2GIS на 2021 рік, показав, що в місті Харків є більше 40 фотостудій, але тільки 20 з них мають свій сайт.

Потреба у використанні інформаційних систем з веб-інтерфейсом в сфері фото послуг в Харкові обумовлена рядом причин:

- конкуренція в цій сфері зростає з кожним роком, у зв'язку з чим збільшуються витрати на залучення клієнтів;
- кількість клієнтів студії безпосередньо залежить від якості і швидкості взаємодії замовника і виконавця.

Для реалізації веб-додатку були використані такі програмні засоби: для розробки інтерфейсу використовували мову розмітки HTML, каскадні таблиці стилів CSS, динамічну мову програмування JavaScript та бібліотеку jQuery; для розробки та адміністрування бази даних використовували MySQL та PhpMyAdmin; для написання програмного коду та взаємодії з БД використовували мову програмування PHP.

Розроблений веб-додаток є повноцінним програмним продуктом для будь-якого веб-браузера та пристрою. Веб-додаток виводить необхідну інформацію про фотостудію, дозволяє коректним чином створити бронювання на обрану дату та час, з вказанням залу (ів) для проведення фотосесії у конкретного майстра, а також має функціонал управляння створеним бронюванням та додатковими послугами. За бажанням клієнт може переглянути портфоліо та особисту сторінку кожного майстра, вказати побажання або коментарі, щодо переглянутих робіт.

ВЕБ-ДОДАТОК ДЛЯ МЕРЕЖІ СПОРТИВНИХ ЦЕНТРІВ

Лещенко Ю.О., Міллер Д.Є.
Національний аерокосмічний університет ім. М. Є. Жуковського
"Харківський авіаційний інститут", Харків, Україна

Цифрова трансформація з кожним роком охоплює все більше різних сфер життя і бізнесу. Якщо бізнес хоче бути конкурентоспроможним звичайних інформаційних сайтів вже недостатньо, необхідні мобільні і веб-додатки, які не просто надають користувачам інформацію, а й дозволяють виконувати перелік необхідних користувачеві функцій: отримувати або замовляти товари або послуги, надавати інструменти та ін.

В сучасних умовах основним напрямком розвитку масового спорту та надання послуг населенню у сфері фізичної культури і спорту в Україні є фітнес-індустрія – надання комерційних послуг фізкультурно-спортивного характеру населенню.

Світовий процес активного розвитку фітнесу, зростання популярності занять фізкультурою і спортом для забезпечення життєздатності та працездатності сучасної людини, за останні чверть століття, розглядаються як революція в способі життя сучасної людини.

В Україні рівень фізичної активності населення в даний час досить низький. Так, якщо в США частка американців, які займаються фізичною культурою, становить 40 %, то число українців, за останніми даними, становить не більше 15,9 %.

В Україні сьогодні налічується більше тисячі фітнес-клубів. Сегмент фітнесу на українському ринку послуг є одним з найбільш динамічних. У низці заходів, спрямованих на оздоровлення українських громадян, першорядне значення набуває формування здорового способу життя та особистісної фізичної культури.

У Харкові працює велика кількість спортивних клубів. Більшість з них мають свої сайти але вони не дозволяють в повній мірі ознайомитись з послугами, що вони надають.

Розроблений веб-додаток слугує для надання інформації про мережу спортивних центрів з можливістю швидкого пошуку і перегляду необхідної інформації по усім послугам, що надають спортивні центри мережі. Веб-додаток дозволить спростити процеси залучення нових клієнтів та їх подальшу реєстрацію у мережі.

При розробці веб-додатку та його компонентів використовувалися: для розробки інтерфейсу – мова розмітки HTML, каскадні таблиці стилів CSS, динамічна мова програмування JavaScript та бібліотека jQuery; для розробки та адміністрування бази даних – PhpMyAdmin та MySQL; для написання програмного коду та взаємодії з БД – мова програмування PHP.

ІНТЕЛЕКТУАЛЬНА СИСТЕМА МОДЕЛЮВАННЯ ТРАФІКУ В ДИНАМІЧНІЙ ТРАНСПОРТНІЙ МЕРЕЖІ

Дергачова Д.К.
Харківський національний університет радіоелектроніки, Харків, Україна

Розв'язання задач управління трафіком є одним із основних в комплексі завдань інтелектуальних транспортних систем. Тому дослідження процесів моделювання міського трафіку, синтез сучасних систем моделювання, розробка засобів автоматичного управління трафіка є актуальною науковою проблемою [1].

Для вирішення завдань моделювання міського трафіку транспортних засобів для опису міських використовується динамічна транспортна мережа (ДТМ), що володіє низькою переваг, ураховує динамічні зміни умов та будується на основі реальної цифрової геоінформації [2].

В вузлах ДТМ розміщуються перехрестя, обладнані засобами керування: світлофорами шляховими позначками з регульованими параметрами на основі аналізу поточного стану ДТМ та обробки даних від систем технічного зору щодо інтенсивності трафіку. Транспортні засоби, генеруються у системі та розглядаються у якості, інтелектуальних агентів, що характеризуються початковим, поточним положенням, та положенням опису мети пересування, а також опис поведінки агенту по інтелектуальному визначенню раціонального маршруту руху по ДТМ з урахуванням ймовірних перешкод та затримок. При моделюванні трафіку ставиться завдання максимізації транспортного потоку у межах ДТМ.

Метою доповіді є побудова математичних моделей, алгоритмічного та програмного забезпечення для функціонування інтелектуальної системи моделювання трафіку за допомогою динамічної транспортної мережі.

В доповіді наводяться алгоритми побудови ДТМ, побудови початкового та поточного стану ДТМ та розміщення транспортних засобів, алгоритми оновлення стану ДТМ, алгоритми урахування динамічних впливів і перешкод, алгоритми статичної обробки результатів моделювання та їх програмна реалізація. Наведені дані показують, що розроблена система може бути ефективним інструментом для моделювання руху транспорту у міських умовах, та у подальшому бути використана для розробки методів автоматичного управління у різних ДТМ.

Список літератури

1. Sładkowski A., Pamuła W. (ed.). Intelligent transportation systems-problems and perspectives. – Cham: Springer International Publishing, 2016. – Т. 303. DOI: https://doi.org/10.1007/978-3-319-19150-8

2. Sakhapov R. L., Nikolaeva R. V. Smart Transport Systems as a Method to Improve the Sustainability of City Transportation Network //IOP Conference Series: Earth and Environmental Science. – IOP Publishing, 2021. – Т. 666. – №. 3. – С. 032004.

ПОБУДОВА ГІБРИДНОЇ СИСТЕМИ ЗВЯЗКУ НА ОСНОВІ ОПТИЧНОГО ЛАЗЕРНОГО АТМОСФЕРНОГО КАНАЛУ ТА РАДІОКАНАЛУ

Шило С.Г., Гейвах О.В.
Харківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна

При експлуатації інформаційно-телекомунікаційних мереж спеціального призначення в умовах зростання навантаження є характерними ситуації, коли їх перепускна здатність не задовольняє вимогам, що потребує необхідності нарощування переліку обладнання та використання додаткових ліній зв'язку. У разі рознесення в просторі окремих сегментів мережі поза межами окремої будівлі вирішення такого завдання пов'язане з необхідністю подолання ряду організаційних, технологічних та технічних складнощів. У якості шляху вирішення такої проблеми для організації єдиної мережі, що забезпечить необхідні показники оперативності та пропускної спроможності, можуть використовуватися як традиційні радіотехнології, що спираються на відповідні стандарти бездротового зв'язку, так і оптичні лазерні канали зв'язку. Для кожного з цих видів зв'язку притаманні свої переваги та недоліки. Тому переваги використання кожної з технологій можуть бути використані у разі побудови гібридної схеми, що поєднає переваги лазерних атмосферних каналів зв'язку та широкосмугових радіо засобів [1].

Метою доповіді є дослідження можливості побудови математичних моделей, що адекватно подають функціонування гібридної системи на базі атмосферної оптичної лінії зв'язку та широкосмугового радіоканалу. Пропонується два варіанти побудови гібридної системи. Лазерна лінія зв'язку та радіоканал, що функціонує під управлінням протоколу IEEE802.11n та виступають у якості холодного резерву, та поєднання лазерної оптичної лінії зв'язку та каналу міліметрового діапазону хвиль, що використовується як гарячий резерв.

Характеристики гібридної системи з холодним резервом пропонується визначати для передумови побудови як однолінійної системи масового обслуговування з двома можливими швидкостями обслуговування заявок та обмеженим часом її використання. Побудова математичної моделі для системи з холодним резервом дозволяє отримати такі характеристики, як розподілу часу роботи системи між режимами, середню довжини черги при роботі в кожному з режимів в довільний момент часу, а також середній час перебування заявки на обслуговування в системі.

Список літератури

1. Кременецька Я. А., Марков С. Ю., Морозова С. В., Морозов Д. М. Застосування інтеграції гібридних оптоелектронних технологій в телекомунікаціях наступного покоління/ Я. А. Кременецька, С. Ю. Марков, С. В. Морозова., Д. М. Морозов // Телекомунікаційні та інформаційні технології. – 2018. – №4(61). – С.20 – 31.

АНАЛІЗ ВИКОРИСТАННЯ ІНТЕГРОВАНИХ КОМУНІКАЦІЙ ДЛЯ САМОВІДНОВЛЕННЯ МЕРЕЖІ НА БАЗІ КОНЦЕПЦІЇ SMART GRID

Лебедєв В. О., Лебедєв О. Г., Носик А.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Методи і технології інтегрованих комунікацій мають високий пріоритет для створення сучасної енергосистеми. Її функціонування істотно залежить від збору даних, захисту і управління, наявності ефективно інтегрованої інфраструктури зв'язку.

В рамках концепції Smart Grid «розумна мережа» для досягнення ключових вимог сучасної енергосистеми, передбачається розвиток процесу самовідновлення мережі при аварійних ситуаціях [1]. Самовідновлювальна мережа повинна максимально мінімізувати збої за допомогою розгалужених систем збору даних і «розумних» пристроїв (smart devices), інтегрованої комунікаційної структури, реалізуючих спеціальні методи і алгоритми підтримки і прийняття рішень, які засновані в першу чергу на розподілених принципах управління [2].

Метою доповіді є аналіз впровадження, модернізація інтегрованих комунікацій для самовідновлення об'єктів енергомережі в рамках концепції Smart Grid.

В доповіді розглядаються можливість мережі при використанні передових інформаційних технологій, впровадження інтегрованих комунікацій самовідновлюватися, за рахунок постійного моніторингу, самодіагностики і самокоригування помилок, для підтримки високої якості і надійності електропостачання здійснювати миттєве усунення збоїв, переналаштовування розподілу потоків електроенергії з метою пом'якшення та запобігання збитку [3]. Близькі до реального часу отримання та передача даних забезпечуватимуть здатність мережі виявляти, аналізувати і автономно реагувати на несприятливі тенденції і умови. Інтегровані комунікації забезпечують контроль обладнання об'єктів енергомережі в режимі реального часу, реалізацію удосконалень локальної та централізованої протиаварійної автоматики (самовідновлювальні мережі).

Список літератури

1. «Grids 2030». A National Vision for Electricity's Second 100 years. Office of Electric Transmission and Distribution of USA Department of Energy, 2003.

2. European Commission Directorate-General for Research Information and Communication Unit European Communities: «European Technology Platform Smart Grids, Vision and Strategy for Europe's Electricity Networks of the future», European Communities, 2006.

3. Joe Miller. Understanding the Smart Grid Features, Benefits and Costs/Illinois Smart Grid Initiative — July 8, 2008.

ЕВРІСТИЧНИЙ МЕТОД ПРОСТИХ ПЕРЕТЕНІВ ДЛЯ ОЦІНКИ ПОКАЗНИКА ЖИВУЧОСТІ ВИСОКОМОБІЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Ткачов В.М., Коваленко А.А., Кучук Г.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Класичні задачі оптимізації невеликих високомобільних комп'ютерних мереж (ВМКМ) (до 10 вузлів) за графним принципом з урахуванням вимог щодо їх живучості вирішуються, як правило, ітеративними методами покроково, на кожному з яких необхідно визначити мінімальне значення перетину.

Кількість кроків для однієї пари вузлів може досягати п'яти. Тоді найпростішим рішення задачі визначення мінімального перетину отримується шляхом його перебору із деякої множини S, яка формується алгоритмом, приведеним у [1].

Скорочення затрат обчислювальних ресурсів на пошук мінімального перетину можливе при використанні евристичних методів перетворення структури мережі у множину $\hat{S} \subseteq S$, яка не містить перетинів. Таким чином, в основу евристичного методу формування $\hat{S}$ можна покласти виконання семи умов, відповідно до моделі [1]:

- лінії прив'язки вузлів a_s, a_t є простими перетинами S_1, S_r;

- вузли комутації, дотичні до a_s, a_t є простими значеннями S_2, S_{r-1}, тоді ранг даних простого перетину: $r(S_1) = r(S_2)$; $r(S_{r-1}) = r(S_r)$;

- кількість простих перетинів мережі відповідає рангу найкоротшого шляху $\hat{N}_S = r_\mu \geq 3$;

- кожний простий перетин $S_i \in \hat{S}$ включає елемент найкоротшого шляху;

- множина ребер, інцидентна вузлам комутації $a_k \in S_{i-1}$ (простий перетин S_{i-1} є вершинним), утворює простий перетин S_i;

- нехай ι – множина вузлів, які входять до $i-1$ $(i \geq 2)$, сформованих простим перетином. При формуванні простого перетину S_i вузли будуть потрапляти до нього, якщо вони не належать вказаній множині;

- якщо ребро з'єднує два вузли будь-якого зі сформованих простих перетинів, то воно не може входити до складу жодного простого перетину.

Список літератури

1. Ткачов В.М. Оптимізація мережного алгоритму функціонування комп'ютерних мереж підвищеної живучості на мобільній платформі на етапі їх проектування / В.М. Ткачов, А.А. Коваленко, Т.Г. Фесенко // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 3 (65). – С. 143-147.

IMPLEMENTATION OF AUGMENTED REALITY TOOLS IN E-COMMERCE SYSTEMS

Morozova A., Nosyk K.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Nowadays, to ensure development and competitiveness in e-commerce systems, the use of advanced information technology is resorted to in order to provide what is known as visual commerce [1].

Visual commerce is an integral part and the next generation of e-commerce, requiring not only the use of conventional static images, but also visual aids using augmented reality (AR) technology. This solution will allow goods to be viewed by overlaying a digital image of the item on the front or main camera image of a mobile device. In other words, this technology will allow customers to take a closer look at a potential purchase. Adding smooth product appearance effects, changing the environment or integrating augmented reality to promote a company using realistic models are just some of the things that technology is already capable of doing.

In a pandemic environment, the use of AR in online sales has a number of advantages, including the ability to interact with products without physical contact. In addition, AR tools will allow customers to feel confident while shopping online, trying a wider range of products than in a real shop.

The experience of several global brands has shown that the use of augmented reality stimulates customers to buy, increasing sales and the engagement of the target audience as well as generating UGC content. Researchers predict that by 2022, more than 120,000 shops will already be using AR technology, which in turn will improve the online shopping trend. [2]

The purpose of the report is to analyze the relevance of augmented reality (AR) technology in modern e-commerce systems and the feasibility of its implementation.

In the report the research of existing software products on the market for the creation and implementation of AR technology in e-commerce systems has been carried out. For this purpose, the hardware was also investigated, the criterion of their use was determined, and as a result, weaknesses, strengths and limitations of their use in certain subject areas were identified.

References

1. Одарченко А. М. Особливості електронної комерції та перспективи її розвитку в Україні / А. М. Одарченко, К. В. Сподар // Бізнес Інформ. - 2015. - № 1. - С. 342-346. - Режим доступу: http://nbuv.gov.ua/UJRN/binf_2015_1_57.

2. Волощук, К. Б., Волощук, Ю. О., Волощук, В. Р., & Богачик, С. В. (2019). Electronic commerce in Ukraine and basic innovative trends of its development. Podilian Bulletin: Agriculture, Engineering, Economics, 1(31), 98–109. DOI: https://doi.org/10.37406/2706-9052-2019-2-12.

COLLECTION AND PRIMARY PROCESSING OF MEDICAL AND BIOLOGICAL DATA

Yeroshenko O., Prasol I.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

The collection of data is the accumulation of them sufficiently in order to make an adequate decision or to obtain a statistically significant result. The amount of data is usually set in advance or determined by the analysis of intermediate results.

A very important component of collecting information is the processing of primary data. This is especially true when dealing with the measurement of biomedical signals. All these measurements, no matter how accurate they are, necessarily have some degree of error [1-4].

The error can also be due to the variability of the measured object itself, for example, fluctuations in human biological parameters during the study (daily biorhythms), lack of sufficient fixation of the human body at the time of anthropometric measurements, guidance on power grids during the removal of biopotentials (ECG, electromyography, electroencephalography). These errors are random.

Their influence on measurement accuracy can be reduced, if you increase the number of measurements of the object of study or increase the duration of each measurement.

Another type of error occurs when the equipment does not work properly, when laboratory equipment is calibrated, and when errors are made in calculations. The end results of such measurements turn out to be either overestimated in all cases, or underestimated, that is always unambiguously distorted.

The only way to avoid them it is to carefully monitor the health of medical equipment, monitor the correctness of the diagnostic, perform these calculations correctly.

References

1. Yeroshenko O., Prasol I., Trubitsyn O., Rebezyuk L. Organization of a Wireless System for Individual Biomedical Data Collection. International *Journal of Innovative Technology and Exploring Engineering*. 2020. Vol. 9. No. 4. Pp. 2418-2421. DOI: https://doi.org/10.35940/ijitee.D1870.029420

2. Yeroshenko O., Prasol I., Datsok O. Simulation of an electromyographic signal converter for adaptive electrical stimulation tasks. *Сучасний стан наукових досліджень та технологій в* промисловості. 2021. № 1 (15). С. 113-119. DOI: https://doi.org/10.30837/ITSSI.2021.15.113

3. 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

4. Ткачов В.М., Лебедєв В.О. Організація АОN-мережі розподілених сегментів реєстрації інформації для передачі Big Data. *Збірник тез доповідей 5 Міжнародної науково-технічної конференції «Проблеми Інформатизації»*. 13-15 листопада 2017 р. 2017. С. 35.

ЗАСОБИ ПОБУДОВИ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Барсуков А.І., Гук А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

На даний час існує велика кількість технологій зв'язку для бездротових сенсорних мереж, такі як LORA, SIGFOX, NB-IoT, Bluetooth LE, Wi-Fi, Weightless P та інші. Безпроводові технології – це технології зв'язку, які забезпечують передачу даних, використовуючи радіохвилі, інфрачервоне, лазерне або оптичне випромінювання. Основними їх особливостями є адаптивність до змін в умовах експлуатації – мінімальні витрати при розгортанні мережі на об'єкті і в подальшому її супроводі в процесі експлуатації. На даний час більшість ринків безпроводового зв'язку надають перевагу передачі невеликої кількості інформації між датчиком і пристроєм.

Метою доповіді є аналіз засобів та компонентів систем бездротового зв'язку для побудови сенсорних мереж. В доповіді проаналізовані стандарти бездротових систем зв'язку, модулі та технології використання бездротових мереж та проведений порівняльний аналіз роботи мережі за параметрами енергозбереження. Показаний принцип дії сенсорного вузла бездротової сенсорної мережі. Датчик збирає дані про аналогові матеріали, АЦП перетворює дані аналогових датчиків в цифровий код. Процесор (мікропроцесор або мікроконтролер) здійснює обробку наданих даних. Базова станція відправляє команди на сенсорні вузли, а сенсорні вузли виконують завдання, взаємодіючі один з одним. Після збору необхідної інформації сенсорні вузли відправляють дані на базову станцію. Після прийому даних від датчиків вузла, базова станція виконує обробку даних і відправляє оновлену інформацію користувачеві через Інтернет.

Для дослідження БСМ прийомо-передавача був проведений ряд експериментів з типовими варіантами топології мережі. Основними задачами проведення експериментів були перевірка працездатності запропонованої сенсорної мережі і оцінка її ефективності. В експериментах перевірялася робота мережі при прийомі даних від сенсорних вузлів, розташованих в двох приміщеннях, базова станція перебувала поза прямої видимості сенсорним вузлів, здійснювали збір даних. Топологія мережі мала вигляд «дерева» з двома гілками. Один із найоптимальніших варіантів для використання сенсорних мереж є моніторинг і контроль процесів роботи.

Слід зазначити, що використання бездротових сенсорних мереж вимагає низьких енергозатрат, щоб вони могли працювати довгий період без зміни джерела живлення.

Список літератури

1. Єрохін С.Д., Махров С.С. Протоколи маршрутизації в безпровідних сенсорних сетях: засновані на місці розташування вузлів і направлені на агрегацію даних // T Com Телекомунікації і транспорт. – 2013. – №3. – С. 44 – 47

2. Побудова та моделювання сенсорних мереж на сучасних інформаційних технологіях та забезпечення їх інформаційної безпеки / С. В. Толюпа, 2011

МЕТОД МОНІТОРИНГУ ТРАФІКУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ BIG DATA ДЛЯ МЕРЕЖ МОБІЛЬНОГО ЗВЯЗКУ

Гнип А.К., Торба А.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Моніторинг та аналіз мережного трафіку мають теоретичне та практичне значення для оптимізації мережних ресурсів та поліпшення роботи користувачів. Однак існуючі рішення, які зазвичай покладаються на високопродуктивний сервер із великою ємністю, не є масштабованими для детального аналізу великого обсягу даних про трафік [1]. Щоб задовольнити зростаючу вимогу до пропускної здатності, мобільні оператори розгортають більше мережевих ліній на рівні гігабіт, таких як 10G та 40G. У такому високошвидкісному середовищі, навіть з розвантажувальними мережними картами та оптимізованим кодом ядра, програмні системи моніторингу трафіку все ще недостатні для моніторингу в режимі реального часу. Єдиним варіантом для мереж з кількома лініями зв'язку 10 Гбіт/с є індивідуальна колекторна система, заснована на апаратному забезпеченні. Отже, доцільно створити гнучку систему моніторингу, засновану на масштабованій архітектурі апаратно-програмного забезпечення [2], щоб бути придатною до модифікації та доповнення вимог до моніторингу, а також до майбутніх збільшень швидкості.

Метою доповіді є обґрунтування методу, що полягає у використанні для аналізу отримуваних великих даних набору програм, що входять до моделі програмування MapReduce. Пропонується виконувати аналіз даних про трафік у чотирьох аспектах. Перш за все, це статистика мережного трафіку, яка обчислюється відповідно до різних індексів групування, таких як IP-адреси, протоколи транспортного рівня та п'ять кортежів TCP/IP. По-друге, це аналіз рівня застосунків: створювані записи потоку та записи сеансу на рівні програми надають можливість дослідити деякі алгоритми видобутку даних для видобутку інформації рівня застосунку та вивчення характеристики трафіку з точки зору програми. По-третє, аналіз постачальника веб-послуг: веб-трафік досліджується через стільникові мережі передачі даних з боку постачальника послуг, що відіграє важливу роль у мобільному Інтернеті. По-четверте, аналіз поведінки користувачів, для чого трафік характеризується та моделюється з боку мобільного клієнта та кінцевого користувача.

Список літератури

1. W. Xu, Y. Xu, C. H. Lee, Z. Feng, P. Zhang, and J. Lin. 2018. Data-Cognition-Empowered Intelligent Wireless Networks: Data, Utilities, Cognition Brain, and Architecture. *IEEE Wireless Communications 25*, 1 (February 2018), 56-63.

2. H. N. Dai, R. Wong, H. Wang, Z. Zheng, A. Vasilakos. (2019). Big Data Analytics for Large Scale Wireless Networks: Challenges and Opportunities.

МУРАШИНІ АЛГОРИТМИ ДЛЯ МАРШРУТИЗАЦІЇ В БЕЗДРОТОВИХ БАГАТОПЕРЕХІДНИХ МЕРЕЖАХ

Кметь О.І., Кулєшов Д.О., Партика С.О.
Харківський національній університет радіоелектроніки, Харків, Україна

Область бездротових багатоперехідних мереж (Wireless Multi-Hop Networks) важливий та перспективний напрямок досліджень на сьогоднішній день. Наприклад, досягнення в області сенсорних мереж дозволяють здійснювати широкий спектр моніторингу навколишнього середовища і розробляти додатки для відстеження різноманітних об'єктів. На маршрутизацію з декількома переходами в Multi-Hop Networks впливають нові вузли, що постійно додаються та видаляються з системи.

Ant алгоритм (мурашиний алгоритм) – це метод заснований на поведінці реальних мурах при пошуку їжі з використанням стратегії локального градиентного пошуку з феромонними слідами. Реалізація здійснюється шляхом подання мурах через мережеві пакети, а феромону – значеннями, присвоєними мережевим вузлам. Мурашина маршрутизація показала відмінну продуктивність для сенсорних і бездротових багатоперехідних мереж. Враховуються такі параметри, як рівень сигналу, якість зв'язку, коефіцієнт втрат та ін.

Метою доповіді є дослідження основних проблем маршрутизації повідомлень в бездротових багатоперехідних мережах через динамічно змінювані мережеві структури. Крім проблеми пошуку оптимального маршруту, існує також взаємний вплив використовуваного маршруту на інші маршрути. Це вимагає самоорганізованого підходу до вибору маршрутів, які є майже оптимальними на глобальному рівні, у відповідності з рішенням, заснованим на наявній локальній інформації. Для вирішення основних проблем такої маршрутизації розглянуто декілька методів: алгоритм GPSAL розроблений для MANET та WMN для зменшення кількості повідомлень маршрутизації з прискоренням відновлення маршруту за допомогою аналізу інформації про місцезнаходження вузлів, а також AARAI алгоритм мурашиної колонії з адаптивним покращенням на основі оптимізації колонії мурах та реалізований через багатоколійну маршрутизацію.

Список літератури

1. D. Caro, F. Ducatelle, and L. M. Gambardella, "AntHocNet: An adaptive nature-inspired algorithm for routing in mobile ad hoc networks," European Transactions on Telecommunications, vol. 16, pp. 443- 455, 2005.

2. Белевцов С.С. Балансировка нагрузки с использованием многоканальной маршрутизации / С.С. Белевцов, С.А. Партика, Ю.Ю. Завизиступ // Восьма міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління». – Полтава-Баку-Харків-Жиліна. – 2018 – С. 34.

МЕХАНІЗМИ БЕЗПЕКИ З прямою ПОСЛІДОВНІСТЮ ПОШИРЮВАНИХ СИГНАЛІВ СПЕКТРУ

Крят Д.С., Тимофєєв Д.І., Партика С. О.
Харківський національний університет радіоелектроніки, Харків, Україна

Зі збільшенням використання бездротового зв'язку стає все більш важливим надання безпечного та надійного зв'язку в присутності зловмисників. Безпека довгий час була складною проблемою в бездротових мережах, головним чином через широкомовний характер зв'язку, завдяки чому є прості, але досить ефективні методи щодо перешкоджання корисним комунікаціям між абонентами бездротової мережі.

Технології з розширеним спектром, такі як розширений спектр методом прямої послідовності (DSSS), були розроблені як ефективні контрзаходи проти деяких загроз, наприклад, атак подавлення.

Метою доповіді є дослідження щодо захисту каналу DSSS, використовуючи механізми DSSS з атрибутами фізичного рівня тому, що досі залишається відкритим питання щодо встановлення та поширення секретної послідовності між передавачем та приймачем, не будучи поміченою зловмисниками. Основна ідея використання схеми WDSSS полягає у використанні надмірності, властивої процесу розповсюдження DSSS, для вбудовування інформації про так звані водяні знаки watermarked DSSS. Такий підхід можна вважати контрзаходом проти зловмисника, який отримує розповсюджену послідовність для створення підроблених повідомлень.

В докладі також представлено та оцінено адаптивну схему DSSS, яка враховує як стійкість до перешкод, так і ефективність зв'язку, де відправник і приймач адаптивно змінюють схему модуляції та довжину послідовності зі зміною стану каналу.

Список літератури

1. J. S. Lee and L. E. Miller, CDMA Systems EngineeringHandbook, Norwood, MA: Artech House Inc., 1998.

2. M. Simon, J. Omura, R. Scholtz, and B. Levitt, Spread Spec-trum Communications Handbook, New York, NY: McGraw-Hill, 1994.

3. Іваненко Ю.В. Перспективи розвитку бездротових локальних мереж / Ю.В. Іваненко, С.О. Партика, Д.С. Крят // Збірник тез доповідей восьмої міжнародної науково-технічної конференції «Проблеми інформатизації». - Черкаси - Харків - Баку - Бельсько-Бяла. - 2020. - С. 54.

4. E. Zielinska and K. Szczypiorski, "Direct sequence spread spectrum steganographic scheme for IEEE 802.15.4," in Proceedings of the 3rd International Conference on Multimedia Information Networking and Security, Shanghai, China, 2011, pp. 586-590.

МЕРЕЖЕВІ АТАКИ ЗА ДОПОМОГОЮ СНІФФЕРІВ ПАКЕТІВ

Лапшов Д.К., Бровенко І.М, Партика С.О.
Харківський національній університет радіоелектроніки, Харків, Україна

Основною проблемою любого користувача комп'ютерної мережі є безпека цієї мережі, існує багато різноманітних мережевих атак та систем проти яких вони спрямовані, наприклад, атаки за допомогою сніфферу пакетів.

Сніффер пакетів є прикладною програмою, яка використовує мережеву карту, що працює в режимі коли всі пакети отримані по фізичним каналам відправляються в додаток для обробки, або promiscuous mode.

Promiscuous mode – це режим коли мережна плата дозволяє приймати всі пакети, незалежно від того, кому вони адресовані.

Сніффер використовується для аналізу трафіку та діагностики несправностей, він перехоплює всі мережеві пакети, які в свою чергу передаються через певний домен. Існують додатки які передають дані в текстовому форматі, наприклад FTP, тому за допомогою сніффера можна отримати конфіденційну інформацію.

Метою доповіді є огляд проблеми мережевої атаки за допомогою сніфферів пакетів та способів її вирішення. В докладі представлено метод пошуку та запобігання перехоплення даних в мережі завдяки використанню нешироковомовного запиту ARP до всіх вузлів мережі. Вузол, який працює в режимі promiscuous mode в мережі, буде кешувати локальну адресу із запиту ARP. Надалі передається повідомлення ping в мережі з локальною IP-адресою, але іншою MAC-адресою. У цьому випадку лише вузол, який має MAC-адресу (кешовану раніше), зможе відповісти на широкомовний ping.

Вузол в режимі promiscuous mode відповідає на повідомлення ping, оскільки має у своєму кеші правильну інформацію про хост, який надсилає запит ping.

Решта вузлів надішле ARP-зонд, щоб визначити джерело запиту ping. Таким чином, можна виявити вузол, на якому запущено сніффер та заблокувати йому доступ.

Список літератури

1. S. Dhar, I. Security, M. Team, and R. Infocomm, "Sniffers Basics and Detection Information Security Management Team," Secur. Manag., 2007.

2. D. D. R. P. Nimisha P. Patel, Rajan G. Patel, "Packet Sniffing : Network Wiretapping Packet Sniffing : Network Wiretapping," Pack. Sniff. Netw. Wiretapping, vol. 2, no. February, pp. 6–7, 2009.

3. I. Kaur, H. Kaur, and E. G. Singh, "Analysing Various Packet Sniffing Tools," Int. J. Electr. Electron. Comput. Sci. Eng., vol. 1, no. 5, pp. 65–69, 2014.

4. . Сердечний В.С. Мониторинг сетевого трафика и его модификация при помощи ndis filter drive / В.С.. Сердечний, С.А. Партика // Збірник тез доповідей шостої міжнародної науково-технічної конференції «Проблеми інформатизації». – Черкаси-Баку-Бельсько-Бяла-Харків. –2018. – С. 72.

МЕТОДИ ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ

Петрук В.В., Волошин І.А., Янковський О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

У зв'язку з величезним зростанням обсягів Інтернет-трафіку і появою нових його типів, а також для задоволення запитів на надання все більш різноманітного діапазону мережевих послуг, контроль за перевантаженнями став важливою проблемою в існуючих комп'ютерних мережах.

Контроль мережевих перевантажень, що дозволяє різним типам трафіку задовольняти заданим обмеженням якості обслуговування (QoS), стає дуже важливим.

Більша частина мережевих додатків вимагає прогнозування перевантаження, що насувається, ще до того, як воно виникло [1].

Перевантаження виникає в мережевих маршрутизаторах, коли кількість вхідних пакетів перевищує доступні мережеві ресурси, такі як буферний простір або виділена смуга пропускання. Це може привести до погіршення продуктивності мережі, наприклад, до тривалої наскрізної затримки, високої частки втрачених пакетів і можливого колапсу перевантаження через постійну повторну передачу втрачених пакетів по протоколу TCP [2].

Швидке розширення різноманітності використовуваних додатків в сучасних мережах значно ускладнює роботу механізмів контролю та запобігання перевантажень.

Метою доповіді є огляд сучасних методів запобігання перевантажень в комп'ютерних мережевих каналах та дослідження нових методів контролю стану черг маршрутизаторів за допомогою різноманітних характеристик трафіку. В докладі приведено аналіз факторів, що впливають на продуктивність комп'ютерних мереж та запропоновано метод управління чергами маршрутизаторів шляхом часткової заміни параметрів AQM.

Проведене імітаційне моделювання показало, що розширення кількості використовуваних параметрів сприяє значному зростанню пропускної здатності в IP мережах.

Список літератури

1. Jain R. "Congestion control in computer networks: Issues and trends," IEEE Network Magazine, May 1990, pp 24–30.

2. Партыка С.А., Разработка и исследование метода защиты от перегрузок в мультисервисных сетях. / С.А. Партика, Ю.Ю. Завизиступ // Збірник тез доповідей 5 Міжнародної науково-технічної конференції «Проблеми Інформатизації», – Черкаси–Баку–Бельсько-Бяла–Полтава. – 2017. – С. 46.

БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ У СОЦІАЛЬНИХ МЕРЕЖАХ

Шулінус О.А., Партика С.О., Завизіступ Ю.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

Соціальні мережі стали неминучим зв'язком серед підлітків та старшого покоління. В останні роки спостерігається значна популяризація сайтів соціальних мереж, особливо з точки зору адаптивності, а також популярність, як у ЗМІ, так і в наукових колах.

Присутня інформація на сайтах соціальних мереж використовується в соціальному, географічному та економічному аналізі.

Коли користувачі діляться особистою інформацією в цих соціальних мережах – ці платформи можуть зіткнутися з порушенням конфіденційності [1].

Метою доповіді є огляд основних напрямів розвитку методів безпеки та конфіденційності особистих даних у соціальних мережах.

Наведено огляд відкритих проблем, які все ще залишаються.

Розглянуті рішення щодо конфіденційності зазвичай зосереджуються на кількох аспектах конфіденційності, наприклад, надання візуального зворотного зв'язку та детальних налаштувань за допомогою добре сформованого та розробленого зручного та інформованого графічного інтерфейсу або створення автоматизованих, або стандартних політик конфіденційності. Нинішні припущення щодо збереження конфіденційності профілів користувачів не враховують рамки ідеології соціальної мережі.

Одним з основних рішень у збереженні конфіденційності та безпеки даних є анонімізація даних.

Анонімізація даних сама по собі є складною проблемою, в основному зосереджена на видаленні даних, для запобігання атак до персональних даних у вигляді інформації про атрибути, зберігаючи при цьому корисність уже загальнодоступних даних.

Також в доповіді розглянуто метод k-Anonymity, створений для збереження конфіденційності зазвичай орієнтований на дані соціальних мереж. Техніка k-Anonymity анонімізує кожну точку зразка в наборі даних таким чином, що конкретний екземпляр стає невідрізним від мінімум k-1 інших зразків у контексті до конкретної ідентифікованої соціальної інформації користувача, яка є у формі атрибутів. [2].

Список літератури

1. Oleksandr Bodriagov. Social Networks and Privacy. – 2015.

2. Brij B. Gupta. Gregorio Martinez Perez Dharma P. Agrawal Deepak Gupta. Handbook of Computer Networks and Cyber Security – 2020. – С. 265–270.

МЕТОДИ ОБРОБКИ ЗАПИТІВ В СИСТЕМАХ ПАРАЛЕЛЬНИХ БАЗ ДАНИХ

Бессараб Є.В., Дяченко В.О., Саліков Р.П.
Харківський національний університет радіоелектроніки, Харків, Україна

Підвищення продуктивності систем керування базами даних (СКБД) [1] є невирішеною проблемою та дуже актуальною зараз. Зі збільшенням кількості користувачів, що працюють з базою даних та нарощування обсягів інформації відповідно, потрібно підвищувати швидкодію баз даних для отримання прийнятного часу виконання на запит користувача. Ефективним рішенням та економічно обґрунтованою альтернативою однопроцесорним СКБД є паралельні СКБД, які одночасно функціонують на кількох процесорах. Дана технологія дозволяє об'єднати декілька персональних комп'ютерів малої потужності для отримання того ж рівня продуктивності, як і за однієї (значно потужніше). Таким чином, отримуємо виграш у масштабованості та надійності системи в порівнянні з однопроцесорною СКБД. На сьогоднішній день єдиним ефективним рішенням для обробки та зберігання надвеликих баз даних залишається використання паралельних систем баз даних з реплікацією інформації, що зберігається, яка забезпечує паралельну обробку різних запитів на багатопроцесорних обчислювальних системах. Також слід відзначити, що усі підходи до паралельної обробки запиту базуються на поділі навантаження між локальними вузлами системи в середній та кінцевій стадії формування плану виконання запиту. Врахування особливостей паралельної обробки запиту вже в початковій стадії компіляції дозволяє досягти низки переваг.

Зокрема, спрощується процедура розробки програмного забезпечення для паралельного оброблення запиту, забезпечується робота у складі гетерогенних СКБД, подальша обробка запиту допускає використання вже відомих методів паралельного обчислення.

Метою доповіді є аналіз існуючих паралельних архітектур здатних підтримувати функціонування СКБД.

Розглянуті відомі алгоритми з'єднання відносин у паралельних СКБД у випадках, що вимагають інтенсивної взаємодії між обчислювальними вузлами. Досліджено алгоритми та програмні засоби для паралельного виконання SQL - запитів, які забезпечують їхню сумісність із існуючими СКБД. Отримано апріорні оцінки часу виконання запитів.

Спираючись на результати отриманих досліджень виконано експериментальну оцінку методів та алгоритмів, які використовуються для розпаралелювання запитів у паралельних системах баз даних.

Список літератури

1. Гектор Гарсиа-Молина, Джеффри Д. Ульман, Дженнифер Уидом». Системы баз данных. Полный курс // К: Вильямс, 2018. – 1088 с.

МЕТОД АПАРАТНОГО ПРИСКОРЕННЯ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ

Дяченко В.О., Лебеденко В.Е., Шевченко Д.Ю., Тесленко Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Згорткова нейронна мережа (CNN) [1], популярний алгоритм машинного навчання, зарекомендувала себе як високоточний і ефективний алгоритм, який використовується в різних програмах, таких як розпізнавання рукописних цифр, візуальне розпізнавання та класифікація зображень. Найсучасніші CNN є інтенсивними обчисленнями, але їх паралельна і модульна природа робить такі платформи, як Field Programmable Gate Array (FPGA) [2], добре придатними для процесу прискорення. Як правило, згорткові нейронні мережі потребують дуже тривалого циклу розробки, щоб бути реалізованим або прискореним за допомогою FPGA, тому в даній доповіді пропонується інструмент генерації VHDL (VGT) [2], який за допомогою коду VHDL (архітектура CNN) може бути створений для різних моделей CNN.

Машинне навчання – це підхід з використанням штучного інтелекту, за допомогою якого машини навчаються подібно до того, як навчаються люди. Складність полягає в тому, що набір усіх можливих рішень з урахуванням усіх можливих вхідних даних занадто складний для опису.

Для вирішення цієї проблеми в області машинного навчання розробляються алгоритми, які знаходять знання з конкретних даних і досвіду на основі надійних статистичних даних. Сфера машинного навчання об'єднує багато різних підходів, таких як теорія ймовірностей, логіка, комбінаторна оптимізація, пошук, статистика, навчання з підкріпленням і теорія управління. Розроблені методи лежать в основі багатьох застосувань, починаючи від зору до обробки мови, прогнозування, розпізнавання образів, ігор, аналізу даних, експертних систем, і робототехніки.

Однією з ймовірних сфер застосування є сфера використання програмованих логічних матриць – це готові напівпровідникові пристрої, які складаються з 2D-масивів конфігурованих логічних блоків, які з'єднані за допомогою програмованої логіки. Проектування апаратного прискорювача — це процес, який підпорядковується вимогам цільової програми та кінцевої платформи реалізації. Як правило, вбудовані системи мають ряд вимог і підлягають певним обмеженням, таким як час, потужність і фізичний розмір. Ці обмеження вимагають серйозної оптимізації алгоритмів перед апаратною реалізацією

Список літератури

1. Y. Bengio, R. Ducharme, P. Vincent, and C. Janvin, "A Neural Probabilistic Language Model," *J. Mach. Learn. Res.*, vol. 3, pp. 1137–1155, 2003.

2. J. Qiu et al., "Going Deeper with Embedded FPGA Platform for Convolutional Neural Network," Proc. 2016 ACM/SIGDA Int. Symp. Field-Programmable Gate Arrays - FPGA '16, pp. 26–35, 2016.

МЕТОДИ СЕМАНТИЧНОЇ ОБРОБКИ ВЕБ-ДОКУМЕНТІВ

Кулєшов Д.О., Лебедєв О.Г.
Харківський національний університет радіоелектроніки, Харків, Україна

Класична задача інформаційного пошуку являє собою завдання пошуку документів, що задовольняють запит. На даний момент, крім цієї основної задачі, досліджується безліч суміжних завдань: фільтрація, класифікація і кластеризація документів, вилучення метаданих, ефективне ранжування, побудова мов запитів, пошук як в локальних реляційних базах даних, так і в гіпертекстових базах даних на зразок Інтернету, і багато іншого [1]. В даний час інформаційний пошук являє собою область науки, що бурхливо розвивається багато в чому завдяки безперервному розростанню Інтернету. Колосальна кількість документів в Інтернеті не тільки дає можливість знайти інформацію практично з будь-якого питання, а й ставить завдання пошуку потрібного документа серед незліченної кількості інших. Крім того, Інтернет характерний високою часткою тимчасової інформації, її неконтрольованим якістю та різнорідністю. Неможливість створення виразного каталогу вмісту Інтернету породила особливу категорію сайтів – пошукових систем, що дають можливість пошуку необхідної інформації. Під висловом «схожі документи» можна розуміти безліч речей. З одного боку, документи з незначними відмінностями, наприклад, з різним оформленням, безсумнівно, будуть схожими. З іншого боку, існують тексти, написані абсолютно різними мовами, незначно перетинаються навіть по використаних словах, але мають дуже велику семантичну схожість. Такі документи також можна назвати схожими.

Метою доповіді є аналіз існуючих методів семантичної оброки даних та запропоновано метод оцінки схожості документів на основі складових їх структурно-семантичних блоків, що дозволяє поліпшити якість розпізнавання дублікатів за рахунок збільшення середнього значення показника повноти, що дозволяє отримувати більш повну вибірку схожих документів на одних і тих же наборах даних. Схожість документів можна вважати абсолютною тільки в тому випадку, якщо вони повністю збігаються між собою. У всіх інших випадках чисельне вираження схожості знаходиться в інтервалі [0,1]. Незалежно від обраної метрики схожості документи вважаються майже-дублікатами, якщо схожість перевищує деякий, наперед заданий поріг. Також модифіковано алгоритм розбивки web-документів на структурно-семантичні блоки, що дозволяє виділяти логічні сегменти тексту, шляхом використання HTML-структури документа, необхідної для реалізації методу оцінки схожості документів на рівні блоків.

Список літератури

1.Леонченко П.Т. Отримання інформаційної статистики при пошуку схожих документів / П.Т. Леонченко Інтернет-Математика 2011, 2011 – 250 с.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ «РОЗУМНОГО БУДИНКУ»

Маслакова Н.Ю., Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Під «розумним будинком» розуміють систему, яка забезпечує безпеку та ресурсозбереження (зокрема і комфорт) всіх користувачів. У найпростішому випадку вона повинна вміти розпізнавати конкретні ситуації, що відбуваються в будинку, та відповідним чином на них реагувати: одна із систем може керувати поведінкою інших за заздалегідь виробленим алгоритмам.

Система може самостійно відключати електроприлади, переводити їх у сплячий режим за відсутності людей. За потреби система дозволяє в будь-який час переводити автоматичне керування обладнанням у ручному режимі.

Метою доповіді є виявлення загроз інформаційної безпеки, які є порушенням конфіденційності, цілісності та доступності інформації, а також позбавлення таких загроз як: атака хакерів, перехоплення інформації, віруси у системі, доступ зловмисника у зв'язку з крадіжкою прав.

В роботі було розглянуто основні вразливості системи «розумний будинок»: підключення мережі «розумного будинку» до Інтернету, неефективний захист трафіку, вразливості системи автентифікації [1] та ідентифікації. Також оцінені можливі наслідки загроз, таких, як порушення роботи центрального сервера, порушення конфіденційності інформації, збої в ПО системи. Дослідження були проведені з використанням шкали оцінки впливу загроз(високий, середній та низький вплив на систему).

Запропоновано варіанти того, як зробити розумний будинок безпечнішим за рахунок підвищення захищеності усіх слабких ланок, підвищення надійності під час автентифікації, надання доступу за спеціальними картами або чіпами [2], тощо.

Виходячи з результатів оцінки впливу загроз, найнебезпечнішими є ті загрози, у яких зловмисник може брати під контроль всю систему. Тому вкрай важливим є проведення заходів щодо захисту телекомунікаційної мережі, розмежування прав доступу користувачів.

Список літератури

1. G. Liashenko, A. Astrakhantsev, Implementation Biometric Data Security in Remote Authentication Systems via Network Steganography, Conference on Mathematical Control Theory, 2019, 257-273 pp. DOI: https://link.springer.com/chapter/10.1007/978-3-030-58359-0_14

2. Від розумних інструментів до інтелектуального простору. [Електронний ресурс]. Режим доступу: http://umnydom.kiev.ua/index.php?nma=catalog&fla=stat&cat_id=3&page=1&nums=24/

ЗАСТОСУВАННЯ ПРОГРАМНО-ВИЗНАЧЕНИХ МЕРЕЖ ДЛЯ ПІДТРИМКИ ТЕЛЕМЕДИЧНИХ КОНСУЛЬТАЦІЙ ПІД ЧАС ПАНДЕМІЇ COVID-19

Воробей К.В., Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Нова коронавірусна хвороба COVID-19 змінила суспільство, економіку та всю систему охорони здоров'я. І хоча ця пандемія поставила перед системою охорони здоров'я безпрецедентні виклики, вона досить швидко сприяла впровадженню телемедицини.

Телемедицина – це використання інформаційно-комунікаційних технологій для збору, упорядкування, зберігання, обміну та отримання медичної інформації.

Завдяки застосуванню цієї технології медичні працівники мають можливість надавати своєчасну медичну допомогу, використовувати всесвітню інформаційну базу даних та обмінюватися безцінним досвідом з колегами. Але сьогодні телемедицина стикається з обмеженнями звичайних IP-протоколів, що ускладнює забезпечення потрібного рівня якості обслуговування (QoS) для телемедицини через проблеми, пов'язані з перевантаженням мережі [1]. Аналогічно, медичні працівники, які використовують телемедицину, страждають від низької якості обслуговування (QoS) під час медичних консультацій з амбулаторними пацієнтами через збільшення використання Інтернету.

Метою доповіді є дослідження та побудова телемедичної архітектури на основі програмно-визначеної мережі (SDN) для забезпечення потрібного рівня якості обслуговування під час телемедичних консультацій.

Також додатково використовуються вторинні дані з наявних дослідницьких робіт у літературі [2], щоб створити дорожню карту застосування SDN для покращення рівня якості обслуговування в телемедицині під час пандемії COVID-19.

У доповіді наводяться результати дослідження, які представляють собою практичний підхід до застосування SDN в телемедицині для забезпечення необхідної пропускної здатності та полегшення передачі медичних даних у реальному часі.

Список літератури

1. Telesurgery QoS improvement over SDN based on a Type-2 fuzzy system and enhanced cuckoo optimization algorithm [Електронний ресурс] / M. R.Parsaei, H. R. Boveiri, R. Javidan, R. Khayami // Int J Commun Syst.. – 2020. – Режим доступу до ресурсу: https://doi.org/10.1002/dac.4426.

2. Bokolo A. Use of Telemedicine and Virtual Care for Remote Treatment in Response to COVID-19 Pandemic [Електронний ресурс] / Anthony Bokolo // Journal of Medical Systems. – 2020. – Режим доступу до ресурсу: https://link.springer.com/article/10.1007%2Fs10916-020-01596-5.

ВПЛИВ СЕКТОРНОСТІ АНТЕНИ НА ЄМНІСТЬ СТІЛЬНИКА МЕРЕЖІ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

Ємельянов В.В., Томак В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Проектування – один з найбільш складних та відповідальних етапів розгортання мереж стільникового зв'язку, оскільки він повинен забезпечувати можливу найближчу до оптимальної побудову мережі за критерієм: висока ефективність – найменша вартість.

Серед багатьох параметрів ефективності мережі параметр ємності є одним із основних, оскільки чим вище ємність мережі, тим строк окупності на її розгортання за рівних витрат коротше.

В роботах [1, 2] в якості міри підвищення ємності мережі зв'язку пропонується метод секторизації стільника без будь-яких пояснень.

Метою доповіді є визначення умов, за яких доцільно використовувати секторизацію стільників.

Оскільки секторизація пов'язана з використанням секторних антен, що мають кращі спрямовані властивості, то число соканальних базових станцій, які потрапляють в зону огляду діаграмою спрямованості антени, зменшується та рівень соканальних завад також зменшується, а співвідношення сигнал/завада збільшується, що дозволяє зменшити ємність стільника.

В доповіді розглянуто, що у разі незмінної кількості каналів в стільнику та однакових умовах, односекторний стільник обслуговує 1536 абонентів, а трисекторний – 1059 абонентів. Звідси висновок, що за умови незмінної кількості каналів в стільнику, секторизація призводить до зменшення ємності мережі. Зі збільшенням ємності стільника при секторизації необхідно враховувати, що при цьому змінюється розмірність кластеру. Відомо, що зі збільшенням секторності, розмірність кластеру зменшується, а число каналів на базову станцію збільшується.

Результати розрахунків за методикою [3] показали, що за умови однакових вихідних даних, для односекторного стільника розмірність кластеру дорівнює 9, а для трисекторного – 4. Тож отримали, що у випадку для трисекторної антени число каналів на одну базову станцію в 2,25 рази більше. Ємність мережі збільшиться. Отже, секторизація стільника підвищує ємність мережі за умови відповідної зміни розмірності кластеру.

Список літератури

1. Ратынский М.В. Основы сотовой связи / Д.Б. Зимина – М.: Радио и связь, 2000 – 248 с.

2. Системы мобильной связи: Учебное пособие для ВУЗов / В.П. Ипатов, В.К. Орлов, И.М.Самойлов, В.Н. Смирнов – М.: Горячая линия – Телеком, 2003. – 212 с.

3. Быховский М.А. Частотное планирование сотовых сетей подвижной радиосвязи//Электросвязь. – 1993. – № 8. – С. 30-32.

ЄМНІСТЬ СТІЛЬНИКА МЕРЕЖІ СТІЛЬНИКОВОГО МОБІЛЬНОГО ЗВЯ'ЗКУ З КОДОВИМ РОЗДІЛЕННЯМ КАНАЛІВ

Ємельянов В.В., Томак В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Проектування мереж стільникового мобільного зв'язку ведеться в напрямку забезпечення якісними послугами зв'язку абонентів на території розгортання мережі. Ємність стільника є одним з важливих параметрів, що визначають ефективність мережі зв'язку. Визначення її чисельного значення на первісному етапі розгортання мережі є вельми необхідним.

Метою доповіді є розгляд методів розрахунку кількості активних абонентів в стільнику (ємність стільника), що описані в [1, 2, 3, 4].

У доповіді відмічено, що метод, описаний в [1], при визначенні ємності стільника не враховує реальні фактори, що впливають на її величину, а саме, секторність стільника, коефіцієнт підсилення тощо.

Згідно методиці [2] з урахуванням низки факторів, ємність стільника може бути збільшена майже в 6 разів. Однак при цьому не враховуються такі фактори, як топологія траси поширення радіохвиль, швидкість передачі тощо. В роботі [3] наведено вираз для розрахунку кількості активних абонентів в стільнику. При цьому визначення величини виділеного частотного ресурсу надається однаковим для систем з FDMA, TDMA та CDMA, що на нашу думку не зовсім коректно.

Більшою мірою позитивні та негативні фактори враховуються в методі, що описаний в [4]. Однак, в цьому випадку не враховується швидкість передачі, для якої необхідно визначити кількість активних абонентів. Швидкість в стандарті IS-95 змінюється в межах від 1,2 кбіт/с до 9,6 кбіт/с.

Виходячи з того, що виграш у співвідношенні сигнал/завада при кореляційній обробці дорівнює 128 разів, можна визначити швидкість передачі інформації. В стандарті IS-95 частота символів псевдовипадкової послідовності дорівнює 1,22 мільйонів чипів/с.

Враховуючи ці величини, можна визначити, що номінальна швидкість передачі інформації дорівнює 9,6 кбіт/с.

Список літератури

1. Сукачев Э.А. Сотовые сети радиосвязи с подвижными объектами: учебное пособие. – 3-е изд. – Одесса: ОНАС им. А.С.Попова, 2013

2. Скляр Б. Цифровая связь. Практическое применение: Изд.2-е – Москва: Издательский дом «Вильямс», 2004.

3. Системы мобильной связи: Учебное пособие для ВУЗов / В.П. Ипатов, В.К. Орлов, И.М.Самойлов, В.Н. Смирнов – М.: Горячая линия – Телеком, 2003. – 212 с.

4. Быховский М.А. Исследование эффективности сотовых систем сухопутной подвижной связи с кодовым разделение каналов//Электросвязь. – 1995. – № 8.

МОДЕРНІЗАЦІЯ ТРАДИЦІЙНИХ ТЕЛЕФОННИХ МЕРЕЖ З ВИКОРИСТАННЯМ КОНЦЕПТУАЛЬНИХ ПРИНЦИПІВ NGN

Колтун Ю.М., Томак В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Одна із первісних причин появи мереж наступного покоління (NGN) є завершення життєвого циклу цифрових комутаційних станцій, що експлуатуються на традиційних телефонних мережах, і відповідна з цим потреба в радикальній модернізації цих мереж з метою надання всього комплексу нових інфокомунікаційних послуг. Процес такої модернізації зачіпає всі рівні телефонної мережі загального користування (ТМЗК), однак найбільш складні зміни відбуваються на рівні місцевих (міських (МТМ) і сільських (СТМ)) телефонних мереж [1].

Метою доповіді є аналіз принципів проведення модернізації або заміни функціонуючих комутаційних вузлів ТМЗК, а також засобів доступу до них, в аспекті здійснення переходу до NGN, що дозволить забезпечити передачу всіх видів інформації.

Зокрема у доповіді розглянуті загальні концептуальні особливості організації NGN. При цьому особлива увага приділена аналізу питань впровадження в NGN програмних комутаторів Softswitch. Проаналізовані технологічні принципи організації NGN на основі еволюційної стратегії, яка сприяє виконанню поступової модернізації платформи діючої МТМ до заданого рівня. Практична реалізація такої стратегії ґрунтується на впровадженні в структуру МТМ мультисервісних комутаторів доступу (МКД) і мультисервісних абонентських концентраторів (МАК) [2, 3]. Результатом такої модернізації МТМ вважається перехід до сучасної мережі NGN, яка забезпечить передачу всіх видів інформації (мови, даних і відео)

Також у доповіді надається методика аналізу і робиться відповідна оцінка продуктивності вузла доступу МТМ в мережі NGN з урахуванням запитів від різних груп користувачів.

Наведені результати дозволяють оцінити вимоги до продуктивності мультисервісного вузла доступу, який агрегує трафік мережі доступу МТМ на основі NGN.

Список літератури

1. Колтун Ю.М. Аналіз мережних сценаріїв організації NGN на базі телефонних мереж загального користування / Д.Ю. Войнов, Ю.М. Колтун // матеріали 6-ої міжнародної науково-технічної конференції «Проблеми інформатизації». – Черкаси – Баку – Бельсько-Бяла – Харків, 14 – 16 листопада, 2018 р. – С. 30.

2. Формирование NGN как наложенной сети: руководящий технический материал // Научно-технический центр «Протей», 2007 г. – 44 с.

3. Руководящий технический материал. Принципы построения мультисервисных местных сетей электросвязи // НТЦ Протей, Санкт-Петербург. Редакция 2.0, 2005. – 48 с.

ТЕНДЕНЦІЇ РОЗВИТКУ ГІПЕРКОНВЕРГЕНТНИХ ХМАРНИХ ОБЧИСЛЕННЬ ДЛЯ КОРПОРАТИВНОГО СЕКТОРУ

Коротіч А.В., Костромицький А.І.
Харківський національний університет радіоелектроніки, Харків, Україна

За період останнього десятиліття простежується стійка тенденція на розширення впливу технології хмарних рішень. За аналітичними даними все більше користувачів відходять від концепції використання традиційних сервісів, що розгортуються на власних технічних площах в сторону платформ на базі хмарних рішень для розміщення власних production середовищ.

Метою доповіді є аналіз розвитку ринку гіперконвергентних хмарних обчислень.

Під хмарними обчисленнями розуміється надання користувачеві комп'ютерних ресурсів і потужностей таким чином, що користувач не знає, які комп'ютери обробляють його запити, та під управлінням якої операційної системи це відбувається [1].

Незалежно від підходів, організації приступають до розгортання приватних хмар з двох основних причин: заради зниження витрат і створення більш гнучкого середовища IT. Першими на цей шлях ступають компанії, які потребують високого ступеня гнучкості інфраструктури і швидкого виділення інформаційних ресурсів. Хмари забезпечують динамічне виділення ресурсів за запитом для різних навантажень, використовують гетерогенну віртуалізовану інфраструктуру і мають високу масштабованість. Автоматизація процесів знижує кількість помилок, спрощує налаштування конфігурації безпеки, мереж і програмного забезпечення [2].

Згідно CloudTech, очікується, що витрати на публічні хмари зростуть з $229 млрд в 2019 році, до $500 млрд до 2023 року, при цьому очікуваний сукупний річний темп зростання складе 22,3%.

У 2021 році основними тенденціями розвитку хмарного ринку є: хмарні безсерверні обчислення; гібридні хмарні рішення; технології контейнеризації та Kubernetes.

Протягом 2020 та 2021 років хмарні обчислення зросли, оскільки робота стала віртуальною, а підприємства адаптувалися до глобальної пандемії, зосередившись на наданні цифрових послуг; у 2022 році, безсумнівно, відбудеться продовження швидкого впровадження та зростання.

Список літератури

1. Кононюк А. Е. Фундаментальная теория облачных технологий / А. Е. Кононюк. – Київ: Освіта України, 2018. – 620 с.

2. Тенденции развития облачных технологий [Електронний ресурс] – Режим доступу до ресурсу: https://pro-spo.ru/cloud-technology/3211-tendenczii-razvitiya-oblachnyx-texnologij.

СТВОРЕННЯ БІЗНЕС-ПРОЦЕСУ РОЗВИТКУ КОМПАНІЇ ЗВ'ЯЗКУ ШЛЯХОМ ЗАЛУЧЕННЯ АБОНЕНТІВ

Чеботарьова Д.В., Носач А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Інфокомунікаційна галузь сьогодні демонструє стійкі та високі темпи розвитку. Саме тому компаніям зв'язку для успішного функціонування на ринку необхідно велику увагу приділяти питанням розвитку. Крім надання послуг зв'язку абонентам, інфокомунікаційна компанія повинна постійно вирішувати багато інших задач: підвищення якості послуг, збільшення кількості абонентів, впровадження нових сучасних послуг, просування на ринку, створення умов для інвестицій тощо.

В умовах високої конкуренції на українському ринку одною з основних проблем останніх років для провайдерів є залучення абонентів до підписки на свої послуги [1]. Провайдери розробляють та впроваджують певні алгоритми утримання своїх клієнтів та залучення нових.

Проблемами дослідження різних аспектів лояльності на споживчому ринку займаються багато вчених. Однак питання, які стосуються поведінки клієнтів, а також формування лояльності на ринку послуг, а особливо на ринку мобільного зв'язку ще не достатньо вивчені [2].

Метою доповіді є аналіз особливостей розвитку інфокомунікаційних компаній та розробка моделі бізнес-процесу розвитку компанії зв'язку з урахуванням проблем залучення абонентів та створенням програми лояльності.

Створена модель бізнес-процесу дозволяє представити розвиток компанії та застосовані при цьому технології у вигляді діаграм, що забезпечують наглядність і повноту їх відображення; формувати на основі аналізу запропонованої моделі організаційно-управлінську структуру розвитку компанії; впорядковувати інформаційні потоки в компанії; розробляти рекомендації з побудови раціональних технологій роботи підрозділу компанії та її взаємодії з зовнішнім світом; аналізувати вимоги та планувати інновації і своєчасні поліпшення, адже саме це є залогом ефективного розвитку компанії на інфокомунікаційному ринку.

Список літератури

1. Мельник О. О. Проблема залучення абонентів до сучасних сервісних провайдерів. *International scientific e-journal ΛΌГОΣ.Online.* 2020. DOI: https://www.ukr-logos.in.ua/10.11232-2663-4139.16.44.html.

2. Чевжик М. О., Діброва Т. Г. Особливості формування програми лояльності на ринку мобільного зв'язку. *Актуальні проблеми економіки та управління : збірник наукових праць молодих вчених.* 2013. Вип. 7. DOI: https://ela.kpi.ua/bitstream/123456789/12496/2/2013_5_Chevzhyk.pdf.

БЕЗДРОТОВА МЕРЕЖА ЯК ЗАСІБ ЗВ'ЯЗКУ ДЛЯ ПРИСТОЇВ МЕДИЧНОГО ІНТЕРНЕТУ РЕЧЕЙ

Юр'єв Я.В., Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сьогодення диктує свої вимоги до галузі науки і техніки, серед яких, зокрема, підвищення мобільності апаратів та поширення функцій «розумних» ґаджетів на все нові предмети життєдіяльності людей. І сфера медичного обслуговування не є винятком. Навпаки, в теперішніх умовах глобального поширення нових небезпечних хвороб гостро постає питання безпеки не тільки пацієнтів, але й лікарів, які через нові розробки в науково-технічній галузі мають змогу зменшити контакти з хворими і тим самим убезпечити своє здоров'я та продовжувати виконувати свою роботу.

Одним з перспективних рішень цієї нагальної потреби є розширення використання «розумних» ґаджетів, а саме так званого медичного інтернету речей (Medical Internet of Things) [1]. І щоб забезпечити високу мобільність таких апаратів можна використовувати спроможності бездротового зв'язку, наприклад, стільникової мережі найсучасніших поколінь (4G/5G) для великих медичних систем або мережі Wi-Fi для відносно невеликих за площею об'єктів. На локальному рівні також можуть стати у нагоді технології Bluetooth та ІЧ-зв'язку.

Метою доповіді є застосування бездротових мереж для пристроїв медичного інтернету речей. Пропонується використання різноманітних «розумних» пристроїв та датчиків для пацієнтів, які можуть на відстані вести моніторинг необхідних параметрів стану здоров'я і сповіщати лікаря про небажані зміни [2]. Ці апарати можуть бути використані як у закладах охорони здоров'я, так й у домашніх умовах, здійснюючи підключення до мережі Інтернет через стільникову мережу або за бажанням через локальний Wi-Fi маршрутизатор. Для медичних закладів також може бути запропоновано інтегрування додаткових «розумних» пристроїв у вже звичні об'єкти діяльності медперсоналу (наприклад, ліжка чи діагностична апаратура) або повна заміна таких об'єктів новим технологічним інвентарем. У таких умовах має сенс використання для підключення пристроїв до мережі Інтернет технології Wi-Fi. У деяких випадках можливе запровадження більш локального зв'язку, який можуть надати технології Bluetooth або ІЧ-зв'язку.

Список літератури

1. What is IoT? [Електронний ресурс] // Oracle – Режим доступу до ресурсу: https://www.oracle.com/internet-of-things/what-is-iot/.

2. D. Jude Hemanth. Internet of Medical Things: Remote Healthcare Systems and Applications / D. Jude Hemanth, J. Anitha, George A. Tsihrintzis. – Хам: Springer, 2021. – 409 с.

ЗНАХОДЖЕННЯ ОПТИМАЛЬНОГО ІНФОРМАЦІЙНОГО НАВАНТАЖЕННЯ КОМПОНЕТІВ СВКС ЗА КОМПЛЕКСНИМ ПОКАЗНИКОМ

Кучук Н.Г., Бульба С.С., Шиман А.П.
Національний технічний університет «ХПІ», Харків, Україна

Самовідновлювальні комп'ютерні системи (СВКС) дозволяють автоматично виявляти збої у процесі функціонування системи та швидко відновлетися після них.

Метою доповіді є розрахунок оптимального інформаційного навантаження компонетів СВКС за комплексним показником. Отриманий результат у вигляді рівняння (1) дозволяє стверджувати про однозначне дотримання прийнятних оптимальних значень ступеня завантаження каналів компонентів СВКС χ_{accept}^{opt}, як мінімального середнього часу затримки пакетів при заданій допустимої ймовірності їх втрат, так і середньої максимальної ймовірності втрат пакетів P_{fail}^{accept} [1, 2].

$$\sum_{\alpha=0}^{n_i} \frac{n_i!}{\alpha!}\left(n_i\chi\right)^{-(n_i-\alpha)} = \sum_{\alpha=1}^{m_i-1}\left(\frac{\alpha(m_i-\alpha)}{n_i\chi}-1\right)\chi^{\alpha}, \quad i \in \overline{1,I}.$$

При заданому допустимому часі затримки пакетів залежать, як від необхідного значення ймовірності втрат пакетів P_{fail}^{accept}, так і від допустимого часу їх затримки T_{spec}^{accept}. Можна сказати, що затримки пакетів є функціями дискретних значень кількості каналів n і числа місць у черзі m.

Рівняння (1) є функцією однієї змінної χ. Це надає можливість незалежно визначити прийнятне значення ступеня завантаження каналу для кожного модуля мережі $\chi_{i\ reason}$. Але дані рівняння є трансцендентними. Тому отримати точний аналітичний розв'язок (1) не представляється можливим. Але ці рівняння можуть бути вирішені або чисельним, або графічним методом.

Чисельний метод рішення реалізований за допомогою програми Mathcad.

Список літератури

1. Н. Г. Кучук, С. С. Бульба., А. П. Шиман, А. М. Філоненко. Розрахунок ефективності використання обчислювальних ресурсів самовідновлювальної комп'ютерної системи. *Системи управління, навігації та зв'язку*, 2021, № 3(65) С. 92-95.

2. Shefer O.V., Alnaeri Frhat Ali. Optimum flow distribution in the network with adaptive data transfer. *Electronics and Control Systems*. 2020. No. 4(66). P.45-50. DOI: https://doi.org/10.18372/1990-5548.66.15254

СЕКЦІЯ 3

БЕЗПЕКА ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Керівник секції: д.т.н. проф. В. М. Рудницький, ЧДТУ, Черкаси
Секретар секції: к.т.н. доц. І. М. Федотова-Півень, ЧДТУ, Черкаси

SPAM RECOGNITION AND SPAMMERS DETECTION

Oliynyk V., Podorozhniak A., Liubchenko N.
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

Even 3 years ago, messengers and social networks occupied a big part of our lives, today due to the situation with Coronavirus and quarantine, the social and virtual world plays almost as important a role as the real one [1]. Along with the extreme growth in the popularity of messengers and social networks and the growth of the text stream on the Internet, there is the problem of recognizing, filtering spam and detecting and blocking spammers [2].

The **work is devoted** to solving the problem of spam detection and filtering, as well as the problem of detecting spammers and blocking them on social networks or messengers. For recognition we use a complex algorithm which includes 4 most popular methods of spam recognition: Naive Bayesian classifier, Method of reference vectors, Neural network based on Perceptron, Convolutional neural network [3, 4]. We place detected spammers in the cloud storage, so spammers' data is available to all working spam bots. In this paper we present the main stages of project development and test results of the obtained algorithms. Telegram messenger was chosen as a test platform, the developed spam bot can be implemented in several chats at once, users are recognized as spammers will be blocked in all chats in which the algorithm works (spam bot).

References

1. Krithiga R., Ilavarasan E. A Comprehensive Survey of Spam Profile Detection Methods in Online Social Networks. *Journal of Physics: Conference Series*, 2019, vol. 1362, 012111. https://iopscience.iop.org/article/10.1088/1742-6596/1362/1/012111.

2. Chaudhry S., Dhawan S., Tanwar R. Spam Detection in Social Network Using Machine Learning Approach. *REDSET 2019: Data Science and Analytics*, Springer, 2020, pp. 236–245. DOI: https://doi.org/10.1007/978-981-15-5830-6_20.

3. Liubchenko N., Podorozhniak A., Oliinyk V. Research of Antispam Bot Algorithms for Social Networks. *Proceedings of the 5th International Conference Computational Linguistics and Intelligent Systems (CoLInS 2021)*, vol. I, April 23 - 24, Kharkiv, Ukraine, 2021. – Aachen: Germany: *CEUR Workshop Proceedings*, vol. 2870, 2021. – pp. 822-832. *http://ceur-ws.org/Vol-2870/paper61.pdf*.

4. Oliinyk V., Podorozhniak A., Liubchenko N. Method of comprehensive spam recognition in social networks, *Проблеми інформатизації*: тези доповідей восьмої міжнародної науково-технічної конференції, 26-27 листопада 2020 року, т. 2, 2020, С. 39.

ДОСЛІДЖЕННЯ МЕТОДІВ ОБФУСКАЦІЇ ПРОГРАМНОГО КОДУ ТА ТЕХНОЛОГІЙ ЇХ ЗАСТОСУВАННЯ

Бабенко В.Г., Гуменюк М.В.
Черкаський державний технологічний університет, Черкаси, Україна

Одним з пріоритетних напрямків захисту інформації є захист програмних продуктів (ПП), при цьому це є більш трудомісткою операцією з більшими технічними обмеженнями [1]. Для обходу захисту програми в більшості випадків застосовують «реверсивну інженерію», що полягає у вивченні деякого готового програмного коду, а також документації на нього з метою розуміння принципу його роботи. Найвідомішим і популярним способом захисту від реверс-інжинірингу є обфускація [2].

Метою доповіді є дослідження методів обфускації програмного коду та огляд основних способів їх застосування.

У дослідженні наведено опис процесу перетворення програмного коду обфускатором та проведено аналіз режимів та алгоритмів обфускації. Особливу увагу приділено сучасним алгоритмам та методам захисту ПП на базі обфускації. У ході дослідження проведено роботу щодо пошуку ефективних рішень для побудови методики застосування методів обфускації коду, що забезпечить його стійкість щодо реверс-інжинірингу. Більшість методів обфускації використовують перетворення над даними, потоком коду або структурою формату і т.і. програмного коду. У порівнянні з шифруванням коду, обфускація має ряд переваг [2-4]: відсутність обмеження державними стандартами щодо довжини ключа; для шифрування ПП одним з найпопулярніших способів захисту є шифрування байт-коду; для того, щоб додаток працював, потрібно отримати доступ до його байт-коду; під час шифрування усіх вихідних кодів разом і використанні потокових алгоритмів шифрування, стає неможливим випадковий доступ до ділянок вихідного коду. Інструменти обфускації можуть працювати як з вихідним кодом або байт-кодом, так і з бінарним кодом. Проте обфускація двійкових файлів реалізується складніше і повинна працювати залежно від архітектури системи.

Список літератури

1. Barak B., Goldreich O., Impagliazzo R., Rudich S., Sahai A., Vadhan S. and Yang K. On the (im) possibility of obfuscating programs // Journal of the ACM. 2001. Vol. 2. No. 69. DOI: https://doi.org/10.1145/2160158.2160159.

2. Ding N., Gu D. A Note on (Im)Possibilities of Obfuscating Programs of Zero-Knowledge Proofs of Knowledge // Cryptology and Network Security. Lecture Notes in Computer Science. 2011. Vol. 7092. DOI: https://doi.org/10.1007/978-3-642-25513-7_20.

3. Goldwasser S., Rothblum G. N. On best-possible obfuscation // Journal of Cryptology. 2014. Vol. 27, No. 3. P. 480–505.

4. Mohsen R., Pinto A. M. Algorithmic information theory for obfuscation security // Proceedings of 12th International Joint Conference on e-Business and Telecommunications. 2015. P. 76-87.

АКТУАЛЬНІСТЬ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО КІБЕРПРОСТОРУ ДСНС УКРАЇНИ

Мельник О.Г., Мельник Р.П.
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, Черкаси, Україна

Забезпечення сталого та надійного функціонування телекомунікаційних мереж та загальносистемних серверів у мирний час та в особливий період – основне завдання кіберзахисту в Державній службі України з надзвичайних ситуацій (ДСНС України) [1].

Метою доповіді є вивчення питання кіберзахисту в ДСНС України.

Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України [2]. ДСНС України входить до складу сил безпеки, на які Конституцією та законами України покладено функції із забезпечення національної безпеки держави, а саме організації цивільного захисту України [3]. Оперативна доставка інформації в процесі повсякденної діяльності всіх галузевих служб і підрозділів ДСНС України, оперативна взаємодія з органами місцевого самоврядування в умовах децентралізації в Україні, іншими міністерствами та відомствами супроводжуються складними інформаційними процесами, більшість з яких мають конфіденційний характер.

Несанкціонований доступ до інформації, що обробляється та циркулює на об'єктах інформаційної діяльності та в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ДСНС України, а також витік інформації технічними каналами займають особливе місце за своїми небезпечними наслідками серед загроз, які можуть призвести до розголошення інформації.

Стратегічно правильним вирішенням проблеми захисту інформації є використання досягнень криптографії. Таким чином, перед нами ставилося важливе науково-технічне завдання – удосконалення методів та засобів захисту інформації ДСНС України від несанкціонованих дій, що можуть призвести до випадкових або умисних змін чи знищення інформації.

Список літератури

1. Про затвердження Положення з організації заходів забезпечення кібербезпеки в ДСНС: наказ ДСНС України від 01.10.2020 р. № 533.

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 р. № 447/2021.

3. Мельник О. Г. Розроблення методу захисту інформації інформаційно-аналітичних систем для здійснення управління силами та засобами цивільного захисту в умовах децентралізації / Мельник О. Г., Мельник Р. П. // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. Том 32 (71). Ч. 1. № 2, 2021. С. 188–193.

ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ОБ'ЄКТУ НА ОСНОВІ МОРФОЛОГІЧНОГО АНАЛІЗУ

Миронюк Т.В., Кривоус Г.В.
Черкаський державний технологічний університет, Черкаси, Україна

Актуальність даної теми стосується проблеми організації системи захисту інформаційного об'єкту (ІО) як від несанкціонованого доступу, так і від можливих дій зловмисника спрямованих на дестабілізацію цілісності, конфіденційності, доступності інформації [1]. Будь-який витік інформації може призвести до серйозних проблем для компанії – від значних фінансових збитків до повної ліквідації [2]. Одним із основних видів інформаційно-технічних впливів є руйнівні програмні впливи (РПВ). Саме дана загроза має найбільшу ймовірність здійснення для ІО [1, 3].

Метою доповіді є дослідження загроз безпеки інформаційного об'єкту та підвищення якості його захищеності шляхом вдосконалення його системи захисту на основі застосування розробленого способу проектування і побудови системи захисту інформаційного об'єкту від РПВ з використанням морфологічного аналізу для вибору раціонального рішення серед множини альтернатив.

У дослідженні наведено опис процесу дослідження актуальних загроз безпеки ІО та їх аналізу для подальшої побудови системи захисту ІО [3].

У ході дослідження проведено роботу, яка полягала у вдосконаленні системи захисту ІО шляхом введення в його структуру системи захисту від РПВ, побудова якої реалізована на основі розробленого способу проектування та побудови систему захисту інформаційного об'єкта від РПВ, яка в свою чергу, дозволяє визначити раціональну (зниження продуктивності ІО буде мінімальне) структуру системи захисту ІО від РПВ за рахунок використання методу морфологічної матриці при формуванні множин підсистем, що входять до складу системи захисту від РПВ. Проведений аналіз актуальних загроз та методів протидії для бізнес-структур показав, що захист інформації повинен здійснюватися комплексно, відразу по декількох напрямках. Чим більше методів буде задіяно, тим менше ймовірність виникнення загроз і витоку, тим стійкіше положення компанії на ринку.

Список літератури

1. Обнаружение утечек: анализ технологий DLP-систем. [Електронний ресурс]. – Режим доступу : https://hi-tech.ua/article/obnaruzhenie-utechek-analiz-tehnologiy-dlp-sistem/

2. Разрушающие программные воздействия: учеб.-методич. пособие; [под ред. М.А. Иванова]. М.: Изд-во НИЯУ МИФИ, 2011. 328 с.

3. Бардаков Я.А. Морфологічний аналіз як засіб вдосконалення системи захисту інформації / Я.А. Бардаков // Проблеми інформатизації: тези доп. шостої міжнародн. наук.-техн. конф., Черкаси, 14-16 листопада 2018 року. – Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ; 2018. – С. 10.

ВИЗНАЧЕННЯ СВІТІВ СПРИЙНЯТТЯ СЕМАНТИЧНОЇ СКЛАДОВОЇ ТЕКСТОВОГО КОНТЕНТУ ВЕБ-САЙТІВ В ІНФОРМАЦІЙНОМУ ПРОТИБОРСТВІ

Тарасенко Я.В., Підласий Д.А.
Черкаський державний технологічний університет, Черкаси, Україна

Відповідно до Стратегії кібербезпеки України [1] пандемія COVID-19 значно вплинула на роль телекомунікаційних систем та мереж у повсякденному житті та роботі громадян. Наслідки цих змін значно посилили вразливості процесів обробки інформації. Зокрема, текстовий контент веб-сайтів виступає зручним контейнером для впровадження деструктивного інформаційно-психологічного впливу злочинними організаціями. Протидія подібним впливам вимагає розробку надійних засобів оцінки ставлення пропагандиста до тексту зворотного інформаційного впливу [2]. Зокрема, важливим є процес автоматизованого пошуку тексту пропагандного дискурсу, що володіє ознаками психолінгвістичного портрету конкретного пропагандиста, до якого застосовуються заходи зворотного інформаційного впливу, а це вимагає визначення світів сприйняття семантичної складової тексту.

Метою доповіді є висвітлення спеціалізованого підходу визначення світів сприйняття семантичної складової текстового контенту веб-сайтів в рамках здійснення інформаційного протиборства, що дозволить підвищити ефективність протидії інформаційній пропаганді в мережі.

У доповіді наводяться результати аналізу веб-сайтів з ознаками інформаційно-психологічного впливу. Описується підхід визначення світів сприйняття семантичної складової тексту в рамках пропагандного дискурсу неблагонадійних веб-сайтів. Обґрунтовується доцільність використання методу квантово-семантичного психолінгвістичного аналізу [3] з метою конкретизації світу сприйняття контенту веб-сайту пропагандистом, що дозволить пришвидшити пошук усіх текстів, що належать конкретному пропагандисту та підвищити ефективність подальшого зворотного впливу на нього.

Список літератури

1. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"». [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text

2. Тарасенко Я. В. Засоби оцінювання ставлення пропагандиста до тексту зворотного психологічного впливу. *Вісник Вінницького політехнічного інституту.* 2021. № 4. С. 79-85. DOI: https://doi.org/10.31649/1997-9266-2021-157-4-79-85

3. Tarasenko Ya. The quantum-semantic psycholinguistic analysis method for the english-language text of propaganda discourse. *Advanced Information Systems*. 2019. Vol. 3, № 4. P. 62-68. DOI: https://doi.org/10.20998/2522-9052.2019.4.09

ПІДХІД ДО ФОРМУВАННЯ АНСАМБЛЮ КОДОВИХ СЛІВ НЕРОЗДІЛЬНОГО ФАКТОРІАЛЬНОГО КОДУ

Фауре Е.В., Щерба А.І., Махинько М.В.
Черкаський державний технологічний університет, Черкаси

Принципи нероздільного факторіального кодування з відновленням даних за перестановкою дозволяють реалізувати інтегрований захист інформації, що поєднує її завадостійке кодування та криптографічний захист від несанкціонованого доступу.

У роботі [1] представлено підхід до розпізнавання синхрослова-перестановки за умов впливу завад високої інтенсивності. Результат досягається за рахунок мажоритарної та кореляційної обробки даних, що приймаються з каналу зв'язку.

Пропонований підхід може бути використаний для організації інформаційного обміну, де як множина кодових слів використовується деяка підмножина перестановок заданої довжини з необхідними ансамблевими, статистичними, структурними властивостями.

У роботі [2] представлено підхід до побудови трьохетапного криптографічного протоколу, відмінна риса якого полягає в тому, що він використовує не тільки операції множення інформаційного вектору, перестановки, ключової перестановки та зворотних до них, а й нелінійні перетворення, що ґрунтуються на ідентичній циклічній структурі спряжених перестановок.

Метою цієї роботи є розробка підходу до формування ансамблю кодових слів нероздільного факторіального коду, що задовольняє заданому набору обмежень. Інформаційний обмін інформації відбувається в телекомунікаційних системах із короткими пакетами без застосування роздільних маркерів.

Наводиться приклад застосування розробленої процедури для практичної реалізації трьохетапного криптографічного протоколу на основі перестановок [2].

Список літератури

1. Faure, E., Shcherba, A., Stupka, B. Permutation-Based Frame Synchronisation Method for Short Packet Communication Systems. In Proceedings of the 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Cracow, Poland, 22-25 September 2021 (in press).

2. Shcherba, A., Faure, E., Lavdanska, O. Three-pass cryptographic protocol based on permutations. In Proceedings of the 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, Kyiv, Ukraine, 25 November 2020, pp. 281-284, Article number 9349343. https://doi.org/10.1109/ATIT50783.2020.9349343

ПРО ТОЧНІСТЬ АПРОКСИМАЦІЇ ЙМОВІРНОСТІ БІТОВОЇ ПОМИЛКИ

Щерба А.І., Щерба В.О.
Черкаський державний технологічний університет, Черкаси, Україна

Телекомунікаційні системи з нероздільним факторіальним кодуванням забезпечують інтегрований захист інформації від несанкціонованого зчитування та помилок у каналі зв'язку. Процедура циклової синхронізації є невід'ємною частиною усіх стандартних протоколів мережевої взаємодії. У роботі [1] запропоновано метод входження в цикловий синхронізм для систем з нероздільним факторіальним кодуванням в умовах впливу в каналі зв'язку завад високої інтенсивності. Метод базується на алгебраїчних та комбінаторних аспектах теорії кодування [2], використовує в якості синхрокомбінації перестановку довжини M, а також мажоритарну обробку прийнятих із каналу двійкових символів. Імовірність бітової помилки p_0^* в уточненій послідовності довжини $M \cdot \lceil \log_2 M \rceil$ після мажоритарної обробки l прийнятих фрагментів із вхідною бітовою помилкою у каналі зв'язку p_0, $p_0 \le 0{,}495$, розраховують за біномним розподілом

$$p_0^* = \sum_{i=(l+1)/2}^{l} C_l^i \cdot p_0^i \cdot (1-p_0)^{l-i} .$$

У випадках, коли $l \ge 1027$ стандартними засобами виконати такий розрахунок неможливо (такі значення l необхідні при $0{,}475 \le p_0 \le 0{,}495$).

Метою доповіді є отримання апроксимаційної формули для ймовірності бітової помилки p_0^* в уточненій послідовності.

Спираючись на роботу [3] показано, що

$$p_0^* \cong \Phi(x) + \frac{1-2\cdot p_0}{6\cdot\sqrt{l\cdot p_0\cdot(1-p_0)}}\cdot(x^2-1)\cdot\varphi(x) ,$$

де $x = -\sqrt{l}\cdot(0{,}5-p_0)/\sqrt{p_0\cdot(1-p_0)}$, а $\Phi(x)$ та $\varphi(x)$ - відповідно інтегральна та диференціальна функції Лапласа.

Наведено оцінку точності апроксимації ε, згідно з якою при $l \ge 1027$ і $0{,}4 \le p_0 \le 0{,}495$ значення $\varepsilon \le 1{,}15 \cdot 10^{-4}$.

Список літератури

1. Фауре Е.В., Швидкий В.В., Щерба А.І., Харін О.О. Ступка Б.А. Метод циклової синхронізації на основі перестановок. *Вісник Черкаського державного технологічного університету.* 2020. №4. С. 67-76. .

2. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки . –М.: Связь, 1979. – 744 с.

3. Сенатов В.В. О реальной точности аппроксимаций в центральной предельной теореме. *Сибирский математический журнал*, Т. 52, № 4, 2011. – С. 913-935.

АНАЛІЗ СТІЙКОСТІ АЛГОРИТМА ЦИФРОВОГО ПІДПИСА НА ЕЛІПТИЧНИХ КРИВИХ

Щербакова Ю.А.
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»

Серед всього спектра методів захисту даних від небажаного доступу особливе місто займають криптографічні методи. Сучасні методи шифрування гарантують практично абсолютний захист даних, але завжди залишається проблема надійності їх реалізації. Одним з способів захисту інформації від стороннього втручання є електронно-цифровий підпис.

Метою доповіді є проведення аналізу для дослідження надійності алгоритму цифрового підпису на еліптичних кривих (ЕК) ECDSA до основних алгоритмів криптоаналізу, в тому числі ρ-метода Полларда для розв'язання задачі дискретного логарифмування в групі точок ЕК над кінцевим полем.

Стійкість основного криптографічного перетворення, що використовується за генерування цифрового підпису на еліптичній кривій, визначає складність розв'язання задачі дискретного логарифмування в циклічній підгрупі $\langle P \rangle$ простого порядку n групи точок еліптичної кривої, тобто складністю розв'язання відносно k рівняння $Q = kP, Q \in \langle P \rangle, \ (1 < k < n)$.

Завдяки властивостям ЕК ускладнюється на кілька порядків. Довжина відкритого ключа при цьому зменшується мінімум вдвічі, що значно зменшує час генерації підпису з одного боку і об'єми пам'яті у відповідних базах даних з іншого. Наприклад, рівень безпеки у 80 біт (тобто для «злому» ЦП треба 2^{80} зразків) розмир відкритого ключа для ECDSA має бути 160 біт, а для DSA – 1024 біт. Це вплинуло на появу нового класу алгоритмів криптоаналізу, що враховують властивості групи точок ЕК. На сьогодні існують декілька видів атак на алгоритми ЦП, а саме:

1. Атака на основі відомого відкритого ключа (key-only attack).
2. Атака на основі відомих підписаних повідомлень (km attack).
3. Проста атака з вибором підписаних повідомлень (gcm attack).
4. Спрямована атака з вибором повідомлення (dcm attack).
5. Адаптивна атака з вибором підписаного повідомлення (adaptive chosen-message attack).

Список літератури

1. Ємець В., Мірошник А., Попович Р. Сучасна криптографія. Основні поняття. Львів-2003. 144 с.

2. Месси Дж. Л. Введення в сучасну криптологию // ТИИЄР. 1988. Т.76, №5. С. 24-42.

3. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка».

АНАЛІЗ ПІДХОДІВ ДО УПРАВЛІННЯ КІБЕРІНЦИДЕНТАМИ СИСТЕМ КРИТИЧНОГО ПРИЗНАЧЕННЯ

Давидюк А.В., Сергеєв С.М., Ткаченко В.В.
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

Системи критичного призначення є невід'ємними складовими об'єктів критичної інформаційної інфраструктури (далі-ОКІІ). Забезпечення безперервності функціонування таких систем є одним з завдань кіберзахисту на ОКІІ. Водночас одним з найважливіших з процесів кіберзахисту є процес реагування на кіберінциденти. Зокрема під час кібератаки від правильності та оперативності дій фахівців з кібербезпеки залежить величина завданого збитку, яка також може виражатися і у людських жертвах.

Враховуючи вищезазначене виникає необхідність використання кращих практик для реалізації цього процесу. За результатами аналізу існуючих підходів до реагування на кіберінциденти можна виділити наступні (табл. 1) [1-4].

Таблиця 1

NIST Framework (NIST Special Publication 800-61 Revision 2)	SANS Framework (Incident Handler's Handbook)	ISO/IEC 27035-1:2016	ISO/IEC 27001:2013 (Annex A.16.1)
1 Preparation	1 Preparation	1 Plan and Prepare	A.16.1.1 Responsibilities & Procedures
2 Detection and Analysis	2 Identification	2 Detection and Reporting	A.16.1.2 Reporting Information Security Events A.16.1.3 Reporting Information Security Weaknesses
3 Containment, Eradication and Recovery	3 Containment	3 Assessment and Decision	A.16.1.4 Assessment of & Decision on Information Security Events
	4 Eradication	4 Responses	A.16.1.5 Response to Information Security Incidents
	5 Recovery		
4 Post-Incident Activity	6 Lessons Learned	5 Lessons Learnt.	

У даній таблиці представлено результати репрезентативний порівняння етапів реагування відповідно до представлених методик, що дає можливість методичного формування власних підходів до реагування з урахуванням специфіки функціонування та ресурсів організації.

Список літератури

1. «NIST SP 800-61,» 2021. [Онлайновий]. Available: https://www.nist.gov/privacy-framework/nist-sp-800-61. [Дата звернення: 28 10 2021].

2. «Incident Handler's Handbook,» [Онлайновий]. Available: https://www.sans.org/white-papers/33901/. [Дата звернення: 28 10 2021].

3. «ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management,» 2016. [Онлайновий]. Available: https://www.iso.org/ru/standard/60803.html. [Дата звернення: 28 10 2021].

4. «ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT,» 2021. [Онлайновий]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Дата звернення: 28 10 2021].

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ БІОМЕТРИЧНИХ СКАНЕРІВ ВІДБИТКІВ ПАЛЬЦІВ ПРИ АВТЕНТИФІКАЦІЇ

Федюшин О.І., Морозов О.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті системи автентифікації без паролю на основі анатомічних особливостей людини.

Об'єктом дослідження є процес автентифікації користувачів за відбитком пальця (сканер FPM10A), що на теперішній час є одним з найпоширеніших [1,2]. **Предмет дослідження** – методи та засоби розпізнавання біометричних зображень за відбитками пальців.

Автоматичні системи перевірки відбитків пальців сканують палець для отримання вхідного зображення папілярного візерунку пальця. За рахунок відбиття світла від пальця, світло, що відбилося від хребтів потрапляє до матриці на сканері та формує зображення хребтів (сітку хребтів). Далі сканер робить оцінку орієнтації отриманого зображення і вирівнює за допомогою ключових точок візерунку.

Процес зіставлення ключових точок реалізується за допомогою наступних етапів: знаходження центру, переміщення, повороту і зміни масштабу. Одним з методів підвищення надійності автентифікації є покращення характеристик якості вихідного зображення [3].

Для цього рекомендується використовувати алгоритм, який складається з етапів сегментації, нормалізації, локального оцінювання, оцінювання частоти хребтів, потоншення.

В результаті проведеного порівняння оптичного механізму автентифікації з іншими механізмами за характеристиками складності, ефективності захисту та вартості було виявлено, що оптичний механізм на даний момент поступається ультразвуковому в надійності захисту, стійкості до зламу муляжем, але є більш простим в реалізації і дешевим.

З методів порівняння за відбитками пальців є найбільш ефективним метод порівняння на основі локальних ознак.

Список літератури

1. Jain, A., Hong, L., Pankanti, S., Bolle, R. An Identity Authentication System Using Fingerprints // ResearchGate. – 2013. – С. 67.

2. Piciucco, E., Di Lascio, E., Maiorana, E., Santini, S., & Campisi, P. (2021). Biometric recognition using wearable devices in real-life settings. Pattern Recognition Letters, 146, P.260–266.

3 Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2002). FVC2000: Fingerprint verification competition. IEEE transactions on pattern analysis and machine intelligence, 24(3), 402–412. https://doi.org/10.1109/34.990140.

ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНКИ І УПРАВЛІННЯ РИЗИКАМИ КІБЕР І ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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

Світові тенденції до посилення загроз кібер і інформаційної безпеки, підвищення рівня вразливості інформаційно-телекомунікаційних систем, обумовлюють необхідність розробки та впровадження нових стандартів та нормативних документів з кібер і інформаційної безпеки. При створенні системи управління інформаційною безпекою (СУІБ) постає питання вибору заходів захисту, що забезпечують зниження виявлених в процесі аналізу ризиків кібер і інформаційної безпеки без надмірних витрат на впровадження і підтримку цих заходів. Аналіз і оцінка ризиків безпеки дозволяє визначити необхідну і достатню сукупність заходів, спрямованих на зниження ризиків інформаційної безпеки, і розробити архітектуру СУІБ організації максимально ефективною для її специфіки діяльності.

Метою роботи є обґрунтування вибору методів оцінки ризиків безпеки, які задовольняють запропонованим у роботі критеріям.

На основі наведеного аналізу методів оцінки ризиків кібер і інформаційної безпеки, автори прийшли до висновку, що оптимальним варіантом для вибору методу управління ризиками в контексті забезпечення неперервності функціонування СУІБ, є, зокрема, адаптація та удосконалення відомих методів шляхом їх логічного поєднання з урахуванням переваг та мінімізації недоліків цих методів.

Крім того, при виборі методу оцінки ризиків безпеки необхідно враховувати низку чинників (критеріїв), які визначені у ході досліджень: наявність науково-методичного обґрунтування методу для проведення оцінки і управління ризиками; відповідність вимогам сучасних стандартам і нормативних документів у сфері створення систем управління інформаційною безпекою; простота проведення заходів з оцінки ризиків із можливістю залучення на окремих етапах оцінки ризиків (ОР) вузькоспеціалізованих фахівців; можливість застосування принципів системності та використання засобів структурного аналізу і автоматизованих методів прийняття рішень; можливість адаптації методу ОР до вимог організації залежно від її типу та розміру; можливість отримання результатів щодо ОР у якісному та кількісному представленні; вартість продукту, організаційно-штатна структура та форма власності організації, ступінь критичності інформації, що обробляється та інші.

Список літератури

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

МЕТОДИ ОПТИМІЗАЦІЇ СИНТЕЗУ СКЛАДНИХ СИГНАЛІВ ЗА ШВИДКОДІЄЮ І КОРЕЛЯЦІЙНИМИ ВЛАСТИВОСТЯМИ

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

До інформаційно-комунікаційних систем, особливо таких, що функціонують на об'єктах критичної інфраструктури, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування: достовірності і швидкодії передачі інформації, живучості, завадозахищеності, кібер-і інформаційної безпеки. Більшість зазначених систем відносяться до так званих багатокористувачевих систем. В процесі функціонування багатокористувачевих систем з кодовим поділом мають місце взаємні завади, які є наслідком одночасної роботи абонентів (користувачів) в загальній смузі частот. Для забезпечення максимально можливої сумісності абонентів повинні бути виконані вимоги до властивостей сигнатур. Іншими словами, при кодовому поділі необхідно так вибрати параметри сигналів, щоб рівень взаємних завад був як завгодно малим, саме таким чином буде забезпечена задана завадостійкість прийому сигналів [1].

Метою роботи є підвищення завадостійкості прийому і швидкодії процесів синтезу систем сигналів на основі отримання методів синтезу систем дискретних складних сигналів із заданими кореляційними, ансамблевими, статистичним, структурними, технологічними властивостями.

В доповіді наводяться результати щодо: отриманих методів синтезу низки класів сигналів, які засновані на застосуванні мінімаксного критерія щодо кореляційних властивостей сигналів; оптимізації за часом пошуку сигналів на основі методів для вирішення завдань цілочисельного лінійного програмування (метод «гілок і границь»).

Отримані і наведені у докладі результати дозволяють стверджувати, що застосування систем сигналів, які синтезовані із застосуванням запропонованих у роботі методів, призводить до поліпшення показників завадозахищеності, інформаційної безпеки, скритності інформаційно-комунікаційних систем, швидкодії передачі, завадостійкості прийому сигналів в умовах впливу різних видів перешкод та кібератак.

Список літератури

1. Gorbenko, I., Zamula, O. Devising Methods to Synthesize Discrete Complex Signals with required Properties for Application in Modern Information and Communication Systems. Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2021, 3, стр. 16–26.

THEORETICAL FUNDAMENTALS OF SYNTHESIS OF DISCRETE COMPLEX SIGNALS WITH NECESSARY PROPERTIES FOR APPLICATION TO INFORMATION AND COMMUNICATION SYSTEMS

Gorbenko I.D., Zamula O.A.
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine
Rodionov S.V.
Ukrainian State University of Railway Transport, Kharkiv, Ukraine

Information and communication systems (ICSs) must comply with increasingly stringent requirements to ensure the reliability and speed of information transmission, noise immunity, information security. This paper reports the methods to synthesize discrete complex cryptographic signals, underlying the construction of which are random (pseudo-random) processes; the methods for synthesizing characteristic discrete complex signals whose construction is based on using the nature of the multiplicative group of a finite field; the results of studying the properties of the specified signal systems. It is shown that the methods built provide a higher synthesis performance than known methods and make it possible to algorithmize the synthesis processes for the construction of software and hardware devices to form such signals. The win in the time when synthesizing nonlinear signals in finite fields using the devised method is, compared to the known method, for the period of 9,972 elements is 1,039.6 times.

The proposed method for synthesizing the entire system of such signals, based on decimation operation, outperforms the known method of difference sets in performance. Thus, for a signal period of 2,380 elements, the win in time exceeds 28 times.

It has also been shown that the application of such systems of complex signals could improve the efficiency indicators of modern ICSs. Thus, the imitation resistance of the system, when using complex discrete cryptographic signals with a signal period of 1,023 elements, is four orders of magnitude higher than when applying the linear signal classes (for example, M-sequences). For a signal period of 1,023 elements, the win (in terms of structural secrecy) when using the signal systems reported in this work exceeds 300 times at a period of 8,192, compared to the signals of the linear form (M-sequences).

The purpose of this work is to synthesize, based on the devised methods, discrete complex signals with the improved ensemble, correlation, structural properties, which could improve the performance indicators of ICS operation, namely, the performance of signal synthesis, information security, noise immunity of the system.

The results reported here suggest that the use of CS leads to improved indicators of noise immunity, information security, the secrecy of information and communication systems, noise immunity of signal reception under the influence of various types of interferences.

DESIGN OF INFORMATION SECURITY SYSTEM BASED ON PROGRAMMABLE LOGIC DEVICE

Koshman S., Piven A.
V. N. Karazin Kharkiv National University, Kharkov, Ukraine

As a result of increasing the capacity of computers and their capabilities, the number of cryptographic attack also increasing. Therefore, the design of hardware to protect information from unauthorized access is an urgent scientific task. The task of improving the reliability of the system's against unauthorized access to information is related to the need to study cryptographic protection methods, in particular the development and design of pseudorandom number generator (PRNG). One of the most important components of solving this problem is the use of programmable logic device (PLD), as an elemental base [1-3].

The purpose of the report is to ensure the required level if protection of the system information by the modeling and researching pseudorandom number generator based on PLD.

The report presents the results of a study of the main functions of cryptological systems. The above data show that with increase in the capacity of attackers, there is need of speed up the creation of keys or increase the length of the key for greater complexity of decryption. PRNG is an integral part of every cryptographic system and the quality of the protection results depends on it. The main qualities that should be endowed with PRNG are the long length of the repetition period and the number of generated numbers per unit time.

Currently, there are three types of PRNG by the method of obtaining numbers: hardware, tabular and algorithmic. The nature and direction of PRNG directly depends on the choice of the source of entropy used by the generator, and determines the cryptographic stability of the whole algorithm. The simulation results showed that the use of PLD allows to effectively implement different structures of PRNG, depending on the requirements for information security systems. The obtained results can be presented in the form of IP-cores, which allows to apply them in further projects on PLD.

References

1. A. Kuznetsov, Y. Gorbenko, A. Andrushkevych and I. Belozersev, "Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 203-206.

2. I. D. Gorbenko, V.I. Dolgov, V.I. Rublinetskii, K.V. Korovkin. "Methods of Information Protection in Communications Systems and Methods of Their Cryptoanalysis" *Telecommunications and Radio Engineering*, vol. 52, Issue 4, pp. 89-96, 1998.

3. I. Gorbenko, A. Kuznetsov, M. Lutsenko and D. Ivanenko, "The research of modern stream ciphers" *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, pp. 207-210, 2017.

ОГЛЯД МЕТОДІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНДУСТРІАЛЬНОЇ ПОЛІНГОВОЇ МЕРЕЖІ

Ткачов В.М.
Харківський національний університет радіоелектроніки, Харків, Україна
Морозова О.І., Тецький А.Г.
Національний аерокосмічний університет ім. М.Є. Жуковського "Харківський авіаційний інститут", Харків, Україна
Нічепорук А.О.
Хмельницький національний університет, Хмельницький, Україна

Одним із забезпечуючих напрямків розвитку сучасної індустрії є масове впровадження мікропристроїв для збору, обробки, передачі даних між вузлами технологічного обладнання та цілих систем [1-5]. Мережа передачі даних між такими пристроями є полінговою та вимагає наявності механізмів захисту для безпечного обміну даними.

Метою доповіді є огляд технологічної бази, яка реалізує засади кібербезпеки в зазначених індустріальних полінгових мережах.

В доповіді проаналізовано протоколи захисту маршрутизації у полінгових мережах, методи автентифікації на опорних вузлах, методи шифрування даних, підходи, спрямовані на виявлення аналізаторів трафіку та їх ізоляції в самоорганізуючих полінгових мережах.

Список літератури

1. Ткачев В.Н. Применение метода предотвращения коллизий при параллельной обработке данных в полинговых сетях контроля состояния сложных распределенных систем / В.Н. Ткачев, А.А. Коваленко, В.О. Лебедев // Третя міжнародна науково-технічна конференція «Проблеми інформатизації» 12-13 листопада 2015 року. – Черкаси–Баку–Бельсько-Бяла–Полтава. – 46 с.

2. Система послеаварийного мониторинга АЭС с использованием беспилотных летательных аппаратов: концепция, принципы построения / А. А. Саченко, В. В. Кочан, В. С. Харченко, М. А. Ястребенецкий, Г. В. Фесенко, М. Э. Яновский // Ядерна та радіаційна безпека. – 2017. – № 1(73). – С. 24-29

3. Кучук Г.А. Проблема захисту інформації при наданні її у разі виникнення надзвичайної ситуації / Г.А. Кучук. // Науково-методичні основи оцінки та управління техногенною безпекою при виникненні надзвичайних ситуацій. Науковий семінар. – Х.: НДПКТІ мікрографії, 26-27.05.2006.

4. Коваленко А.А. Підходи до синтезу інформаційної та технічної структури системи управління об'єктом критичного застосування / А.А. Коваленко // Проблеми та перспективи розвитку ІТ-індустрії. Тези доповідей VIII міжнародної науково-практичної конференції, 20-21 квітня 2017. – Харків: ХНЕУ імені Семена Кузнеця. – С. 26.

5. Пат. 118921 Україна, МПК H04W 64/00. Спосіб передачі цифрових даних мультикоптерною системою між сегментами розподіленої сенсорної мережі та базовою станцією / В.М. Ткачов, В.В. Токарєв - № u201704085; заявл. 24.04.2017; опубл. 28.08.2017. Бюл. № 16. 5с.

НЕОБХІДНІСТЬ ЗАХИСТУ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ В СУЧАСНИХ УМОВАХ

Носик А.М.
Національний технічний університет "ХПІ", Харків, Україна
Кучеренко Ю.Ф.
Харківський національний університет Повітряних Сил імені І. Кожедуба, Харків, Україна

В сучасних умовах функціонування нашої країни, при посиленні здійснення на неї впливу політичного, силового, інформаційного та психологічного характеру з боку Російської Федерації (РФ) дуже гостро стоїть питання щодо захисту інформаційної інфраструктури держави від впливу на неї інформаційних засобів (методів, програм), що наносять шкоду електронним ресурсам країни, різноманітним системам державного управління (телекомунікаційним системам, спеціального призначення, системам управління силових міністерств і таке інше), а також медіа простору та впливають на свідомість громадян і їх морально-психологічний стан.

За таких умов виконання заходів щодо захисту інформаційної інфраструктури держави має визначальне значення [1-4].

Метою доповіді є формування пропозицій щодо захисту інформаційної інфраструктури держави з урахуванням сучасних умов її функціонування.

В доповіді надані пропозиції щодо необхідності впровадження надійної адаптованої до умов ведення гібридної війни з боку РФ системи захисту інформаційної інфраструктури держави, яка б надійно функціонувала в умовах прояву жорстокого інформаційного протиборства з РФ і забезпечувала надійний контроль інформаційної інфраструктури держави. Рівень безпеки та надійності даної системи залежать не тільки від засобів і заходів, що обрані для захисту інформаційної інфраструктури держави але і від якості інтегрованого застосування цих заходів і методів для реалізації цільового ефекту системи щодо захисту електронних ресурсів, систем державного управління та медіа простору.

Список літератури

1. Закон України "Про основи національної безпеки України."//Відомості Верховної Ради України, 2003. - №39.

2. Странніков А.М. Інформаційна боротьба у воєнних конфліктах другої половини XX століття. // «Альтерпрес», 2006 – 191 с.

3. Медведєв В.К. Сучасна інформаційна війна та її обрис./ В.К. Медведєв, Ю.Ф. Кучеренко, О.М. Гузько // Системи озброєння і військова техніка. - 2008. –№ 1 (13).-С. 52-54.

4. Створення комплексної системи захисту інформаційних ресурсів у національній ґрід-інфраструктурі України / А.Г. Загородній, О.М. Боровська, С.Я. Свістунов, І.П. Сініцин, Є.С. Родін— К.: «Видавництво «Сталь», 2014. —374 с.

МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У ЗАСТОСУНКАХ НА ОСНОВІ ПЛАТФОРМИ .NET

Моруга Д. І., Ляшенко О. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Веб-застосунки є найпопулярнішим засобом для надання послуг, для багатьох установ. А платформа .NET є популярним рішенням для розробки веб-застосунків.

За наявною інформацією за допомогою .NET було побудовано принаймні 2 567 568 веб-застосунків[1].

.NET-це зростаюча екосистема. Це викликано тим, що у неї сильна галузева підтримка від Microsoft, у неї є якісні інструменти для розробників, і вона використовує кілька мов програмування. NuGet-це широко використовуваний менеджер пакетів .NET. Він містить принаймні 154 385 унікальних пакети, 1 663 564 версії пакетів і більш ніж 20 мільярдів завантажень пакетів на даний момент [2].

Через велику розповсюдженість веб застосунків вони є привабливою ціллю для зловмисників. Це погіршується появою державних послуг за допомогою веб сервісів, "ДІЯ" та інші.

Серед поточних вразливостях в .NET потрібно розділяти уразливості в самому .NET і в застосунках, які написані на основі .NET-платформи. У застосунках на платформі .NET тенденція виглядає так, що застосунки, як правило, не мають великої кількості уразливостей, але присутні вразливості несуть серйозну загрозу застосунку, вони можуть призвести до серйозних збоїв і збитків, якщо не будуть усунені.

Серед уразливостей самої .NET-платформи уразливості високого ступеня серйозності становлять 70,7% від загального числа, але для них доступно виправлення, завдяки оновленням від Microsoft.

Метою доповіді є аналіз засобів та методів доступних на платформі .NET і вирішено чи достатньо цього на поточний час та надані рекомендації щодо використання доступних засобів та методів.

В доповіді наводиться аналіз поточного стану про безпеку на платформі .NET, і засобів та методів забезпечення безпеки платформи та їхньої ефективності.

Список літератури

1. Java vs .NET: Who Will Rule the Future?. URL: https://www.yourteaminindia.com/blog/java-vs-net/ (дата звернення: 27.10.2021).

2. .NET open source security insights. URL: https://snyk.io/blog/net-open-source-security-insights/ (дата звернення: 27.10.2021).

ОЦІНКА КІБЕРРИЗИКІВ ПРИ ПОБУДОВІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ОРГАНІЗАЦІЇ

Маслакова Н.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

Проаналізована методологія оцінювання кіберризиків передбачає розробку індивідуальної моделі, яка дозволяє оцінити загрози у грошовому значенні, та виявляти їхній вплив на відхилення ключових показників діяльності організації від планових значень [1].

Метою дослідження є оцінювання кіберризиків, які використовують методи факторного і сценарного аналізу та імітаційного моделювання з урахуванням оцінки розподілу потенціальних втрат на основі наявних історичних даних та експертної оцінки базових компонентів.

В доповіді наводиться оцінка кіберризиків, яка включає в себе декілька етапів:

Етап 1. Розробка структури моделі оцінки кіберризиків: визначення ключових фінансово-економічних показників бізнеса для аналізу впливу ризиків на їх значення; виявлення потенційних кіберризиків, їх ризик-факторів та наслідків за допомогою методу «краватка-метелик»; визначення заходів за мінімізацією кіберризиків.

Етап 2. Створення моделі оцінки кіберризиків та заходів щодо мінімізації ризиків. Етап розробки моделі включає в себе внесення в існуючу фінансову/бюджетну модель: невизначеності, визваною кіберризиками; заходів управління ризиками. При внесенні невизначеності формуються параметри ризиків. Параметри ризиків задаються на основі декількох сценаріїв: оптимістичний сценарій (best case – BC); очікуваний сценарій (best estimate – BE); песимістичний сценарій (worst case – WC).

Етап 3. Аналіз результатів оцінки кіберризиків: визначення величини шкоди від кіберризиків; ранжування та пріоритизація кіберризиків; аналіз впливу ризиків на показники бізнесу та визначення ймовірності досягнення цільових значень показників з урахуванням ризиків.

Виходячи з цього можна зробити такі висновки, що важливо оцінювати не тільки надійність захисту даних, які надають цінність організації, а й створювати необхідні умови для управління кіберризиками.

Список літератури

1. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник — К.: ДУТ, 2015.— 288 с. http://www.dut.edu.ua/uploads/p_303_79299367.pdf

2. Віннікова І.І., Марчук С.В. (2018), «Кіберризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управлінні ним», Східна Європа: економіка, бізнес та управління, вип. 5 (16), с.110-114. - http://www.easterneurope-ebm.in.ua/journal/16_2018/21.pdf

КЛЮЧОВІ АСПЕКТИ БЕЗПЕКИ ЕКОСИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ

Кучук Г.А., Литвиненко Д.С., Росінський Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Інтернет речей (IoT) виводить концепцію безпеки на абсолютно новий рівень. Міркування безпеки вкрай необхідно враховувати у світі, де все можна «підключити», а фізичний контакт стає необов'язковим, та для роботи кінцевого пристрою використовуються словесні інструкції і навіть розпізнавання обличчя. Можна визначити дві категорії небезпеки, пов'язані з IoT [1]. Небезпеки першого типу безпосередньо пов'язані з традиційним використанням пристрою і включають такі речі, як перегрів, удари, звукові небезпеки тощо. Впровадження Інтернету речей у продукти може збільшити частоту виникнення цих небезпек. Увімкнення дистанційних операцій означає, що небезпеки такого роду більше не лімітовані фізичними обмеженнями. Небезпеки другого типу опосередковано пов'язані з пристроєм та його роботою, але можуть створити проблеми з безпекою через впровадження IoT. Ефектом каскаду може бути порушення властивостей або витік приватної інформації.

Розроблені на цей час правила та стандарти належним чином вирішують вищезазначені небезпеки, визнаючи першопричину цих небезпек та небачене застосування для існуючих продуктів. Одним з провідних секторів є побутова техніка. Необхідно також розглядати дрони та подібні пристрої, які можуть поранити людей або пошкодити фінансові активи. Широко виробляються автономні транспортні засоби, а також з'являються пристрої з підтримкою IoT для автомобільної промисловості, що створює ще один рівень проблем безпеки. Міжнародні та регіональні стандарти включають [1]: IEC61508, ISO26262, ISO12100, ISO13849, IEC60730-1, UL5500, CSA Z434, ANSI B11.

Метою доповіді є формулювання ключових аспектів, пов'язаних з оцінкою функціональної безпеки.

До них входять: елементи планування та дизайну; ризики та небезпеки; плани управління; рівні продуктивності (PL); рівні цілісності безпеки (SIL); режими, наслідки та діагностичний аналіз відмов (FMEDA); призначена відповідальність персоналу; сувора документація.

Оскільки IoT продовжує розвиватися, важливо залишатися в курсі стандартів ризиків і безпеки, щоб переконатися, що продукти відповідають нормативним вимогам і вимогам споживачів. Очікується, що оцінка безпеки IoT буде тісно поєднана з функціональною безпекою, яка була встановлена наприкінці 20-го століття для промислових середовищ.

Список літератури

1. O. Omolara, A. Abdulatif, O. Abiodun, M. Alawida, W. Alshoura, H. Arshad. (2021). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*. 112. 102494. 10.1016/j.cose.2021.102494.

БЕЗПЕКА ВИКОРИСТАННЯ ХМАРНИХ ПРОВАЙДЕРІВ ТА СПОСОБИ ЇЇ ДОСЯГНЕННЯ НА ПРИКЛАДІ ВИКОРИСТАННЯ CLOUD CUSTODIAN

Абіх І.В., Костромицький А.І.
Харківський національний університет радіоелектроніки Харків, Україна

У сучасному світі інформаційних технологій хмарні інфраструктури знаходять широке застосування у всіх розвинених країнах, забезпечуючи принципово нові, економічно ефективні можливості для бізнесу, управління, освіти і наукових досліджень [1].

Метою доповіді є аналіз безпеки використання хмарної інфраструктури. В роботі описано загальні принципи безпеки хмарних технологій та сервісів, а також визначено напрями реалізації цих питань зі сторони провайдера та користувача.

В доповіді також наводиться порівняння сторонніх рішень аналізу безпеки інфраструктури та приклад використання Cloud Custodian.

Користуючись хмарними сервісами провідного провайдера, клієнт, отримує більш високий рівень захисту і стабільності роботи для своїх систем, ніж у своїй локальній інфраструктурі.

Великі хмарні провайдери налаштовуючи свою інфраструктуру керуються світовими стандартами, такими як CIS Benchmark, HIPAA, PCI DSS, ISO 27001, NIST тощо.

Аналіз багатьох сценаріїв експлуатації вразливостей різних хмарних рішень призводить до висновку що найуразливіша частина в роботі з хмарою є користувач, який може неправильно налаштувати свою інфраструктуру. Великі провайдери використовують комплекс рішень даної проблеми: написання докладної документації, рекомендацій по налаштуванню того чи іншого ресурсу, проведення тренінгів, використання сервісів які сканують налаштовану інфраструктуру, на можливі вразливості і надають детальний звіт тощо. Крім цього є безліч сторонніх систем аналізу інфраструктури такі як Cloud Custodian, Dome9 та інші.

Cloud Custodian – дозволяє користувачам визначати політики для створення безпечної оптимізованої за вартістю хмарної інфраструктури. На мою думку, при правильному підході, чіткому розумінні технології і зваженому виборі постачальника, хмарні сервіси здатні забезпечити найвищій рівень надійності і захищеності.

Список літератури

1. Абіх І. В. Аналіз та порівняння організації хмарної інфраструктури різних провайдерів. Матеріали XXIV Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. матеріалів форуму. Т. 4. – Харків: ХНУРЕ. 2020. – 138 - 139 с.

РОЗРОБКА МЕТОДИКИ РОЗРАХУНКУ ІНФОРМАЦІЙНИХ РИЗИКІВ ПІДПРИЄМСТВА

Спєсівцева А.С., Золотарьов В.А.
Харківський національний університет радіоелектроніки, Харків, Україна

В умовах глобалізації забезпечення інформаційної безпеки на підприємстві є дуже важливим моментом і полягає в постійному контролі за джерелами виникнення потенційних загроз та необхідності здійснювати захист інформації будь-якими засобами.

Метою доповіді є визначення та оцінювання ризиків інформаційній безпеці для типової розподіленої інфокомунікаційної мережі підприємства.

Основний акцент зроблено на мінімізацію шкоди від кібератак, спрямованих на доступність програмно-апаратного комплексу інфокомунікаційної системи. Провідним методом для оцінювання та обробки ризиків був обраний якісний метод, як найбільш економічний, в умовах відсутності даних про кількість реалізованих атак на інфокомунікаційну систему за окремий проміжок часу. Ґрунтуючись на бізнес-процесах підприємства були виділені основні та другорядні активи, а також відповідні їм загрози інформаційній безпеці.

В роботі був проведений розрахунок ризиків інформаційній безпеці, заснований на виділенні цінних активів організації, ступеня потенційної шкоди під час реалізації загроз на такі активи та ймовірності реалізації загроз для аналізованої інфокомунікаційної мережі підприємства.

Також були виділені прийняті ризики, обробка яких не потрібна у зв'язку з тим, що фактична вартість їх мінімізації вища від реалізації відповідних їм загроз. Були запропоновані можливі заходи щодо мінімізації ризиків інформаційній безпеці, що включають:

систему резервного копіювання,
систему захисту від несанкціонованого доступу,
систему антивірусного захисту,
міжмережне екранування,
організаційні заходи фізичного захисту.

Була запропонована методика, яка дозволяє однозначно оцінити ризики інформаційній безпеці організації в умовах великого об'єму оброблюємої інформації та необмежного числа користувачів і потребує мінімальних фінансових вкладень. Застосування розглянутого методу на практиці буде сприяти ефективному виявленню основних загроз захисту безпеки та їхній мінімізації.

Список літератури

1. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. Berlin: ISO/IEC JTC 1/SC 27. 2013. 23p.

2. Дорофеев А.В. Менеджмент инфоромационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014.No 3 (4). С. 69–73.

АНАЛІЗ ТЕХНОЛОГІЙ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

Чеботарьова Д.В., Пестєрєва С.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

У зв'язку зі стрімким розвитком технологій інформація є більш доступною, зростають обсяги даних, що зберігаються та передаються в мережах, крім того переважна більшість даних є конфіденційними [1]. Підтримка безпеки даних дуже важлива, оскільки навіть невелика втрата даних може створити критичний вплив на організацію. Саме тому запобігання витоку конфіденційних даних є важливою актуальною задачею.

Традиційно організація впроваджувала такі методи, як формування політики в організації, впровадження брандмауера, віртуальної приватної мережі на кінцевих точках, але ці методи почали відставати, оскільки технології витоку і крадіжки даних постійно розвиваються. Тому виникла потреба в системі, яка могла б запобігти витоку даних.

Найкращим рішенням для запобігання ненавмисних витоків даних є впровадження автоматизованої корпоративної політики, яка виявляє захищені дані до того, як вони залишать організацію. До таких рішень відносять технології запобігання витоку конфіденційної інформації з інформаційних систем та мереж Data Loss Prevention (DLP).

Метою доповіді є аналіз компонентів і методів запобігання витоку інформації, а також розробка рекомендацій щодо використання цих методів при захисті інформації в інформаційних системах та мережах.

Методи DLP ідентифікують, відстежують та захищають передачу даних шляхом глибокої перевірки вмісту та аналізу параметрів транзакції (таких як джерело, призначення, об'єкт даних і протокол) із централізованою структурою керування [2]. Методи DLP виявляють та запобігають несанкціоновану передачу конфіденційної інформації.

В роботі описано важливість збереження конфеденційності інформації для організацій та можливі наслідки витоку корпоративних даних. Було проаналізовано та досліджено існуючі системи, що використовуються для захисту даних, та технології DLP з точки зору їх компонентів і методів, що використовуються в них, а також відмінності між ними.

Список літератури

1. Sheela Gowr. P, Kumar. N. Data Leakage Prevention System: A Systematic. *International Journal of Recent Technology and Engineering (IJRTE).* 2019. DOI: https://www.ijrte.org/wp-content/uploads/papers/v8i4/D690411841 9.pdf.

2. Data Loss Prevention R76 Administration Guide. Introduction to Data Loss Prevention. *Check Point Software Technologies Ltd.* 2014. DOI: https://sc1.checkpoint.com/documents/R76/CP_R76_DLP_WebAdmin/62453.htm.

ЗАСОБИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕНЯ ЗАХИСТУ ІНФОРМАЦІЇ НА СЕРВЕРАХ

Пономаренко Р.Д., Ляшенко О.С.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день на жорстких дисках файлових і термінальних серверів підприємств та корпоративних серверах баз даних (в тому числі інформаційних), зберігається і обробляється величезна кількість інформації.

Метою роботи є дослідження засобів забезпечення захисту інформації на серверах підприємств. Для мінімізації ризиків доступу до конфіденційної інформації і корпоративних даних неавторизованих для цього осіб застосовуються різні програмні та програмно-апаратні моделі засобів захисту, призначені для роботи в складі сервера компанії. У якості стандартної моделі безпеки використовується модель з трьох категорій: конфіденційність, цілісність, доступність.

Так одним з популярних таких засобів захисту є SSH-ключі – пару криптографічних ключів використовують для перевірки автентичності в якості альтернативи аутентифікації за допомогою пароля. Система входу використовує закритий (зберігається в таємниці надійним користувачем) і відкритий (може лунати з будь-якого сервера SHH) ключі, які створюють для аутентифікації [1]. В деякому роді, можна сказати, що даний засіб використовується в моделі істинності, та розділення доступу. Брандмауери – невід'ємна частина будь-якої конфігурації сервера. Навіть якщо програмне забезпечення має внутрішній захисний функціонал, фаервол забезпечить додатковий рівень захисту. Їх роботу також можна описати з використанням семи рівнів еталонної моделі взаємодії відкритих систем. Ще хотілося б відзначити популярний останнім часом VPN – спосіб створити захищене з'єднання між віддаленими комп'ютерами і поточним з'єднанням. Дає можливість налаштувати роботу з сервером таким чином, немов використовується захищена локальна мережа. Також останнім, проте не менш важливим, є зауваження, що велика частина безпеки лежить на аналізі розроблюваної системи.

Тож які б засоби захисту не хотілося б обрати, для початку все ж краще було б застосувати аудит, і на основі зібраних даних вже робити висновки. Але, як би там не було, завжди краще розібратися із засобами забезпечення безпеки на ранніх стадіях, адже чим пізніше будуть введені зміни – тим вони будуть дорожчими, не кажучи вже про збитки, які понесе організація, якщо зловмисники отримають доступ до серверів.

Список літератури

1. Лановий О. Ф., Кобзев І. В., Калякін С. В. Системи управління контентом і безпека WEB-сайтів //Системи обробки інформації. – 2010. – №. 3. – С. 38-41.

БЛОКЧЕЙН РІШЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У IoT

Філіппов В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Технологія блокчейну була передбачена промисловістю та дослідницькою спільнотою як цільова технологія, яка має відігравати важливу роль в управлінні, контролі та, головне, забезпеченні захисту пристроїв IoT.

Метою доповіді є розглядання можливих рішень забезпечення безпеки для IoT пристроїв у рамках технологій що використовуються у блокчейн.

Аутентифікація та цілісність даних. Згідно положень, дані, що передаються пристроями IoT, підключеними до мережі блокчейн, завжди будуть криптографічно підтверджені та підписані справжнім відправником, який має унікальній відкритий ключ і GUID, і таким чином має змогу забезпечити аутентифікацію та цілісність даних.

Аутентифікація, авторизація та конфіденційність. У смарт-контрактах блокчейна, що мають можливість надавати децентралізовані правила та логіку автентифікації, може бути зазначено, хто має право оновлювати та виправляти програмне або апаратне забезпечення IoT, скидати налаштування пристрою IoT, надавати нові пари ключів і т.д.

Крім того, конфіденційність даних також може бути забезпечена за допомогою інтелектуальних контрактів, які встановлюють правила доступу, умови та час, щоб дозволити певній особі чи групі користувачів або машин володіти, контролювати або мати доступ до даних у стані спокою чи під час транспортування.

Адресний простір. Блокчейн має 160-бітний адресний простір, на відміну від адресного простору IPv6, який має 128-бітний адресний простір. Адреса блокчейна — це 20 байт або 160-бітний хеш відкритого ключа, згенерованого ECDSA (алгоритм цифрового підпису з еліптичною кривою). За допомогою 160-бітної адреси блокчейн може генерувати та розподіляти адреси в автономному режимі для приблизно 1,46 * 1048 пристроїв IoT. Імовірність колізії адрес становить приблизно 1048, що вважається достатньо безпечним для надання GUID (глобального унікального ідентифікатора).

Список літератури

1. Minhaj Ahmad Khan, Khaled Salah. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*. 2018. С. 19-24. DOI: https://doi.org/10.1016/j.future.2017.11.022

2. Ruban V., Martovytskyi V.O., Kovalenko A.A., Lukova-Chuiko N.V. Identification in informative systems on the basis of users' behaviour. *8th International Conference on Advanced Optoelectronics and Lasers*. 2019. С. 574-577. DOI: https://doi.org/10.1109/CAOL46282.2019.9019446

АНАЛІЗ МОДЕЛІ КЛЮЧОВИХ ВРАЗЛИВОСТЕЙ IoT МЕРЕЖ

Аветісова К.А., Уманець М.С, Ляшенко О.С.
Харківський національний університет радіоелектроніки, Харків

У сучасному світі пристрої IoT стають все більш актуальними і виробляються все в більшому обсязі, але з ростом кількості випущених пристроїв зростають і вимоги до забезпечення безпеки цього обладнання [1].

Метою доповіді є побудова та подальший аналіз інформаційної моделі, яка відображає критичні вузли у захищеності IoT.

В доповіді наводяться результати аналізу захисту систем пристроїв та захисту мереж в цілому.

Додатки IoT поділяються на три категорії:

мобільні програми, які керують пристроями IoT;

прошивка IoT і вбудовані програми;

програми на відкритих платформах IoT (наприклад, програми, створені для Apple Watch).

Усі ці програми мають бути захищені, інакше є ризик отримати такі небажані наслідки, як:

неналежна або небезпечна експлуатація пристроїв IoT;

крадіжка конфіденційних даних, приватної інформації користувача або пов'язаної з програмою інтелектуальної власності;

пошкодження іміджу бренду компанії та погіршення якості обслуговування клієнта;

шахрайство та несанкціонований доступ.

До проблем захисту IoT мереж можна віднести [2]:

- забезпечення недостатнього рівня конфіденційності;
- використання загальної мережі без поділу на сегменти;
- використання слабкого шифрування та ненадійних протоколів;
- незадовільна пропускна спроможність пристроїв.

Модель що розглядається повинна враховувати всі проблеми які перелічені. У висновку треба зазначити, що вирішення вищеописаних недоліків є ключовою задачею для забезпечення належного рівня безпеки в IoT мережах та пристроях, досягнення якої може бути можливим тільки за рахунок покращення технічної бази пристроїв та чіткого сформованої політики безпеки.

Список літератури

1. Oliver Mack, Peter Veil. Platform Business Models and Internet of Things as Complementary Concepts for Digital Disruption // Phantom Ex Machina. — Cham: Springer International Publishing, 2016-10-20. — С. 71–85.

2. Ovidiu Vermesan, Peter Friess. Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds // Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds. — River Publisher, 2016. — С. 1–364.

СЕКЦІЯ 5

Керівник секції: д.т.н. проф. В. А. Краснобаєв, ХНУ, Харків
Секретар секції: д.т.н. доц. Н. Г. Кучук, НТУ «ХПІ», Харків

Підсекція 5.1. Методи швидкої та достовірної обробки даних в комп'ютерних системах та мережах

SYSTEM FOR EVALUATION OF MOBILE DEVICE PARAMETERS USING DECISION-MAKING THEORY

Kataieva E.Y., Samoilenko N.Y.
Cherkasy State Technological University, Cherkasy, Ukraine

The modern gadget market is so diverse that anyone can choose a smartphone for their set of requirements. It's not just about the design and interface, but also about the filling of the device. In order not to regret the purchase, it is recommended to decide on the priority functions of the smartphone before going to the cellular communication salon. Therefore, the choice of smartphone today is approached much more carefully than before, when the mobile phone was a simple means of communication. But it is not uncommon for the user to face the problem of choice when buying a device.

The urgency of the topic is due to the fact that the modern smartphone market is highly saturated, there is virtually no shortage of goods. Applying the theory of decision making can help to choose the best option. Decision making is a process used by an individual or organization to improve the future condition of that individual or organization. The tasks of decision-making include - the choice of the best option in the case where there are several possible options, and these options are evaluated by several criteria and criterion evaluations are contradictory. Over the past 50 years, decision theory, thanks to the development of powerful mathematical tools, has become an effective tool for supporting decision-making at various levels.

There are hundreds, if not thousands, of different smartphone models on the market today, and it's very easy to get lost in this variety. Therefore, there is a need to make a complex choice of the most suitable device, and the application of decision theory techniques can help make this choice.

References

1. http://www.dissercat.com/content/prinyatie-reshenii-pri-kachestvennykh-kriteriyakh-otsenki-alternativ - "Decision-making with qualitative criteria for evaluating alternatives".

2. https://postnauka.ru/books/9795 - «Step by step | Decision theory.

3. http://silverghost.org.ua/2015/11/29/osnovnye-xarakteristiki-mobilnyx-telefonov/ - «Main characteristics of mobile phones»

4. http://ek.ua/k122.htm - "Mobile phones: characteristics, types, types"

ANALYSIS AND USE OF WAYS TO IMPROVE THE QUALITY OF TRAFFIC TRANSMISSION IN INFORMATION SYSTEMS

Kataieva E.Y., Dzetsina E.V.
Cherkasy State Technological University, Cherkasy, Ukraine

One of the most urgent scientific tasks in the field of information technology is the transmission of real-time streaming traffic in compliance with a number of quality requirements. Since the data to be transmitted are different in nature and importance, it is necessary to have mechanisms that allow to solve the problem of resource allocation quickly, in accordance with the properties of those flows that are transmitted at a particular time through specific telecommunications nodes. To improve the quality of service of transmitted network traffic, it is important to find flexible methods of managing network resources to ensure their balanced loading and guaranteed quality of service for heterogeneous user traffic in networks. [2, 3]

The purpose of the report is to improve the quality of network traffic service based on the flexible allocation of computing resources of the router.

Based on the analysis of research, the main methods of solving certain problems of quality assurance are identified.

It is established that the existing algorithms of queuing service and mechanisms of channel resources allocation do not provide guarantees regarding the quality of streaming traffic service. The main direction of expanding the capabilities of the selected methods is to ensure the quality of multimedia traffic service based on the virtualization of the structure of network nodes, taking into account the priority of flows and requirements for the quality of their transmission.

A mathematical model of a network device is proposed. With the help of this mathematical representation it is possible to determine the main parameters of the system of virtual queues in order to analyze the efficiency of network resources, as well as to determine the parameters of the quality of service traffic flows of services.

Analyzing the obtained results, it is proved that under the conditions of deployment of virtual routers of class purpose, the technology of dynamic virtualization of the network device provides the possibility of assigning a minimum amount of computing resources of the router to ensure a given level of service and reduces flow latency.

References

1. Branden C. J. Lambrecht. Perceptual Quality Measure using a Spatio-Temporal Model of the Human Visual System / C. J. Branden Lambrecht and O. Verscheure // Proc. SPIE. – March, 2018. – Vol. 2668. – PP. 450-461.

2. Mykhailo Klymash. Features of the cloud services implementation in the national network segment of Ukraine // Information and Telecommunication Sciences, 2020. – pp. 31-38.

3. Tsybakov B.S. Self-Similar Processes in Communications Networks / B.S. Tsybakov, N.D. Georganas // Information Theory, 2020. – vol.44. – no.5. – PP.13- 25.

SYSTEM OF ANALYSIS AND CALCULATION OF CONCORDION COEFFICIENT IN IT PROJECT MANAGEMENT

Kataieva E.Y., Kozhokar O.R.
Cherkasy state technological university, Cherkasy, Ukraine

Project Management - a methodology for organizing, planning, managing, coordinating labor, financial and logistical resources during the project life cycle (project cycle), aimed at effectively achieving its goals through the use of modern methods, techniques and management technologies to achieve certain results in the project. composition and scope of work, cost, time, quality and satisfaction of project participants.

The main purpose of this work is to solve one of the main problems in projects, which can lead to its collapse, is the presence of issues that need to be addressed throughout the project life cycle.

At the project planning stage, a meeting is held with experts who determine the main features of the project. But it will be more effective if the degree of consensus of experts is also calculated. Experts can use different approaches to gather information. Among these approaches the most common are:

- expert surveys;
- brain storm;
- Delphi method;
- Crawford cards [5].

There are still many methods of expert questioning, but all survey results are inaccurate because the human factor plays an important role. Among the experts can be both highly qualified in a particular issue, and not quite qualified. The method of assessing the consistency of expert surveys will be able to confirm whether the opinions of experts are equivalent or consistent.

The scientific novelty of the work is that the results of the survey of experts will also be considered for consistency. The practical significance of the obtained results lies in the possibility of using and implementing software in project management using the concordance coefficient.

References

1. The essence and concept of the project [Electronic resource] - Access mode: http://pidruchniki.com/1057011647752/informatika/sutnist_ponyattya_proektu

2. Project Management (2006) [Electronic resource] - Access mode: http://library.if.ua/book/66/4896.html

3. Lectures on the discipline "Project Workshop" [Electronic resource] - Access mode: http://www.studfiles.ru/preview/5851333/

4. ProBusinessCenter [Electronic resource] - Access mode: http://www.probusiness.center/tests/project-management/basic-test/

5. Risk management in projects [Electronic resource] - Access mode: http://www.bookz.com.ua/4/9.htm 6. Expert assessment method [Electronic resource] - Access mode: http: // mirznanii. com / a / 165562 / metod-ekspertnikh-otsnok

ANALYSIS AND ASSESSMENT OF RISK TREATMENT METHODS OF DEVELOPMENT OF SOFTWARE APPLICATION

Kataieva E.Y., Trachenko V.V.
Cherkasy State Technological University, Cherkasy, Ukraine

In today's world, characterized by the vast amount of information resources and data that modern organizations and enterprises have and have at their disposal, more and more attention is paid to the problems of risk assessment methods. The main task of ensuring risk processing is solved due to the improvement information management process based on the implementation of various approaches and methods, compliance with regulatory requirements and the application of organizational measures. [2]

The methodology for determining risk assessment may be qualitative or quantitative, or some combination. Qualitative assessment is very often used to obtain the overall level of risk and to identify the main risks. [3]

The purpose of the report is to create an adapted methodology and generalize the existing methods of risk management, which will ensure the continuity and survivability of software applications.

The report considers the application of the expert method of risk assessment, which allows to clearly trace the impact of individual initial factors on the final result, to identify at the preliminary stage the most important risk factors, to take measures to minimize them. The method of expert assessments differs in the way of collecting information to build a risk curve. This method involves the collection and study of estimates made by different experts on the probability of different levels of losses. Estimates are based on all risk factors, as well as statistics.

In the course of the research the analysis of external risk was carried out. For this purpose the mathematical model and a technique of calculation of an integrated indicator of influence of external risk are developed, and also interrelation of this indicator with a choice optimum strategy of development is shown. Its high dynamism and uncertainty of factors require huge resources to build the capacity to counter threats. In this regard, to preserve the basic parameters of activity, the creation of prerequisites for improving efficiency can predict the impact of various factors based on the calculation of the integrated indicator.

References

1. Landoll D. The security risk assessment handbook: a complete guide for performing security risk assessments / Douglas J. Landoll. – Boca Raton: Auerbach Publications, 2020. – 504 p.
2. Rittinghouse J. W. Business continuity and disaster recovery for infosec managers / John W. Rittinghouse, James F. Ransome. – Oxford: Elsevier, 2019. – 408 p.
3. Spedding L. Business risk management handbook: a sustainable approach / Linda Spedding, Adam Rose. – Oxford: Elsevier, 2018. – 768 p.

MOBILE APPLICATION OF USER CALCULATION AND BUDGET FORECASTING

Pervuninsky S.M., Ocheretny O.S.
Cherkasy state technological university, Cherkasy, Ukraine

To effectively distribute their income and expenses, account for their assets and savings, everyone must have at least a minimum of accounting skills. Those who strive to optimize these processes and get the maximum benefit, need to constantly improve their financial literacy. The need to control own funds is one of the most important skills, especially given the impact of the economic crisis, the problem of financial stability of the country is quite relevant. However, at first glance, the issue of financial stability has long been something new and unexplored. The mobile phone has firmly entered our lives, changing, in a way, our attitude towards time. With the help of a mobile phone we can reduce distances, time intervals are reduced - if we need to talk to a person, we do not need to wait long, take a mobile phone and say as many souls as you want.

The urgency of the topic is due to the fact that the present has a fast pace of life and survives often costs are not fixed. The right tools for accounting and analysis of personal finances will be the basis of well-being and rapid accumulation of funds to achieve their goals. As a result of the work, a system for calculating own funds was developed. The developed system is an Android application written using the Ionic Framework. The system can store spending statistics, enter funds using bank cards, and calculate the graph using a moving average calculates the result.

References

1. Girish LS., Guruprasad H.S., Girish LS. Building Private Cloud using OpenStack. *Int. Journal of Emerging Trends & Technology in Computer Science*. 2014. P. 134 – 138.
2. Marc Farley. Rethinking Enterprise Storage: A Hybrid Cloud Model. / Marc Farley. *Microsoft Press*, 2013 pp. 24 – 28.
3. Kapadia, Amar, Kris Rajana, Sreedhar Varma. OpenStack Object Storage (Swift) Essentials. *Packt Publishing*, 2015 – pp. 184 – 187.
4. Single page apps in depth. http://singlepageappbook.com/goal.html.

РОЗРОБКА МЕТОДУ ДОСЛІДЖЕННЯ АЛГОРИТМІВ ЗБЕРІГАННЯ РОЗРІДЖЕНИХ МАСИВІВ В ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ

Філімонов Р.В., Бульба С.С.
Національний технічний університет «Харківський політехнічний інститут»

Стрімкий розвиток можливостей обчислювальних машин призвів до виникнення великої кількості областей в яких оброблюються масиви великих даних. Кожна область оперую власними даними які можуть мати певні характеристики які дають змогу пришвидшити їх обробку та покращити методи зберігання. Алгоритми зберігання даних дають змогу зменшити навантаження на обчислювальну техніку, а також пришвидшити доступ до елементів масиву що

зберігається. До таких специфічних масивів, що потребують спеціальних методів зберігання відносяться розрідженні масиви. **Метою доповіді** є розробка методу дослідження алгоритмів зберігання розріджених масивів в обчислювальних системах, що дасть змогу зменшити кількість пам'яті для зберігання, та пришвидшить доступ до елементів масиву. В доповіді розглядаються існуючі алгоритми зберігання та обробки розріджених масивів, та методи їх дослідження. Під розрідженим масивом ми розуміємо великі масиви даних більшість елементів якого не несуть корисної інформації, або не використовуються, а отже ми можемо їх не зберігати у пам'яті. Але оброку таких масивів необхідно проводити у повному обсязі. У більшості випадків розрідженні масиви зберігаються у вигляді: зв'язного списку, двійкового дерева, масиву вказівників, хешування. Кожен з представлених методів має як переваги так і недоліки, а отже необхідно розробити метод їх дослідження для отримання найкращого результату.

Список літератури

1. Parallel Sparse Matrix - Vector and Matrix – Transpose - Vector Multiplication Using Compressed Sparse Blocks
2. Джордж А., Лю Дж. Численное решение больших разреженных систем уравнений. – М.: Мир, 198.

РОЗРОБКА ТА ДОСЛІДЖЕННЯ СИСТЕМИ ФІЛЬТРАЦІЇ ЗОБРАЖЕНЬ З ВІДЕОКАМЕР СПОСТЕРЕЖЕННЯ ЗА ДОПОМОГОЮ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

Хомініч М.М., Бульба С.С.
Національний технічний університет «Харківський політехнічний інститут»

У сучасному світі швидкий розвиток обчислювальних технологій дав змогу отримувати велику кількість інформації яка поступає з навколишнього середовища. Отримуючи інформацію виникає необхідність в створенні методів її обробки для подальшого використання. Однією з найпоширенішою, є інформація з камер спостереження. Для обробки та фільтрації такої інформації існує багато методів та систем, але для отримання найкращого результату виникає необхідність в їх модифікації та створені системи під конкретний випадок.

Метою доповіді є розробка та дослідження системи фільтрації зображень з відеокамер спостереження за допомогою вейвлет-перетворення , що надасть змогу покращити отримане зображення для подальшої обробки. В доповіді розглядаються існуючі методи фільтрації зображень з камер відеоспостереження на основі вейвлет перетворення. Дослідження системи фільтрації в залежності від вхідної інформації, та очікуваного результату для подальшої обробки. На сьогоднішній день вейвлет перетворення застосовується у великій кількості областей: Обробки експериментальних даних, стиснення даних, механізмах аналізу, системах передачі даних, цифровій обробки сигналів, обробки зображень. Саме методи обробки зображень дають змогу проводити фільтрацію потоку відеокадрів.

Список літератури

1. Gagnon L. and Lina J.M. Symmetric Daubechies' wavelets and numerical solutions of NLS2 equations. J. Phys.A: Math. Gen. 27, 1994, pp. 8207-8230.

2. Новиков Л.В. Основы вейвлет-анализа сигналов. Учебное пособие. СПб.: Изд. ООО "МОДУС+", 1999, 152 с.

3. Kaiser J. A Friendly Guide to Wavelets. Birkhauser. Boston, 1994.

4. Daubechies I Comm. Pure Appl. Math. 41 906 (1988); IEEE Trans. Inform. Theory 36 961 (1990); Ten Lectures on Wavelets (CBMS) (Philadelphia: SIAM, 1991)

ВИЛУЧЕННЯ ТА АНАЛІЗ ДАНИХ В СУДОЧИНСТВІ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ OLAB ТА DATA MINING

Ільїна І.В., Полонець К.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Значною ознакою інформаційного суспільства є наявність величезних обсягів різнорідних даних у різних предметних галузях, що дозволяє вирішити завдання пошуку нових знань, тобто отримання нових фактів, залежностей та прихованих кореляцій, і навіть вирішення низки аналітичних завдань, як прогнозування, перевірка статистичних гіпотез, розрахунок агрегатних показників тощо.

Метою доповіді є огляд алгоритмів і технологій для вилучення та аналізу даних, таких як структури архівів, документів та процес судочинства; побудова інформаційної моделі, а саме виявлення основних об'єктів та їх характеристик у частині судочинства, загальної та варіативної частини всіх видів судових справ; аналіз HTML-сторінок сайтів судів та реалізація HTML-парсеру та аналізатора тексту для отримання наборів даних судочинства; вирішення різноманітних аналітичних завдань на отриманому наборі даних на прикладі системи судочинства за допомогою технологій OLAP та Data Mining [1]; розробка методів покращення судової системи за допомогою системи підтримки прийняття рішень [2].

В доповіді наводяться результати дослідження – результати реалізації парсеру для отримання вмісту HTML-сторінок, аналізатор тексту, заснований на відстані Левенштейна, алгоритмі шинглів і регулярних виразах, а також була побудована інформаційна модель даних судочинства. У майбутньому планується вирішення завдань інтелектуального аналізу за допомогою технологій OLAP та Data Mining.

Список літератури

1. Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP / Барсегян А.А., Куприянов М.С., Степаненко В.В., Холод И.И .– СПб. : БХВ-Петербург, 2010. – 384 с.

2. Бідюк П. І. Комп'ютерні системи підтримки прийняття рішень / П. І. Бідюк, О. П. Гожий, Л. О. Коршевнюк. – Київ: ННК "ІПСА" НТУ "ХПІ", 2010. – 340 с.

ДОСЛІДЖЕННЯ СПОСОБІВ ВДОСКОНАЛЕННЯ МЕТОДУ ПІДВИЩЕННЯ СТІЙКОСТІ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ СИСТЕМ КОМП'ЮТЕРНОЇ КРИПТОГРАФІЇ

Сисоєнко А.А.
Черкаський державний технологічний університет, Черкаси, Україна

Для вирішення задач моделювання складних криптографічних систем та об'єктів, широко використовуються псевдовипадкові послідовності для оцінки швидкості та стійкості криптоперетворень [1].

Під час криптоперетворень для формування ключових послідовностей, основною перевагою криптографічного перетворення є висока швидкість реалізації криптоалгоритмів.

На основі якісних показників псевдовипадкових послідовностей [2, 3], проводяться дослідження методів оцінки якості псевдовипадкової послідовності синтезованої на основі операцій криптографічного перетворення інформації та підвищення стійкості псевдовипадкових послідовностей до лінійного криптоаналізу, являються актуальною проблемою [4].

Метою доповіді є теоретичне обґрунтування способів вдосконалення методу підвищення стійкості псевдовипадкових послідовностей для систем комп'ютерної криптографії.

За результатами дослідження встановлено, що сучасні вдосконалені методи криптографічного захисту інформації показуть, що одним із перспективних шляхів підвищення стійкості псевдовипадкових послідовностей для систем комп'ютерної криптографії є використання логічних операцій криптографічного перетворення інформації на основі комбінації генераторів псевдовипадкових чисел .

Список літератури

1. Криптографическое кодирование: методы и средства реализации (часть 2): монография / В.Н. Рудницкий, В.Я. Мильчевич, В.Г. Бабенко, Р.П. Мельник, С.В. Рудницкий, О.Г. Мельник. – Х.: Изд-во ООО «Щедрая усадьба плюс», 2014. – 224 с.

2. L'Ecuyer P., Simard R.,. Chen E. J, Kelton W. D. An object-oriented random-number package with many long streams and substreams. Operations research. 2002. Vol. 50. No. 6. P. 1073–1075.

3. Фауре Е.В., Сисоєнко С.В., Миронюк Т.В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення. Системи управління, навігації та зв'язку: зб. наук. праць. Полтава: Полтавський нац. техн. ун-т ім.. Юрія Кондратюка, 2015. Вип. 4 (36). С. 85–87.

4. Фауре Е. В., Сисоєнко С. В. Метод підвищення стійкості псевдовипадкових послідовностей до лінійного криптоаналізу. The scientific potential of the present: proceedings of the International Scientific Conference (St. Andrews, Scotland, UK, December 1, 2016) / ed. N. P. Kazmyna. NGO «European Scientific Platform». Vinnytsia: PE Rogalska I. O., 2016. P. 119–122.

APPLICATION OF ASYMPTOTIC METHODS TO COMPUTATION OF ATOMIC FUNCTIONS: EXPANSIONS, ERRORS ESTIMATION AND PRACTICAL IMPLEMENTATION

Brysina I.V., Makarichev V.O.
National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine

Now, different data processing algorithms are based on application of special mathematical tools such as wavelets, algebraic and trigonometric polynomials, splines, etc. Here, we consider other special ones.

Atomic functions, which are compactly supported solutions of linear functional differential equations with constant coefficients and linear transformations of the argument, are non-classic constructive mathematical tools. Their application varies from generalized Taylor series theory [1, 2] to methods of digital image processing [3, 4]. The atomic functions considered have a set of convenient properties that makes them useful practical tool. For this reason, fast and precise computation of their values is of particular interest.

In this research, we consider application of asympotic methods to computation of atomic functions and related objects, especially atomic wavelets. **They aim** of the current research is to obtain asymptotic formulas and estimate errors of their usage. We apply methods of atomic function theory in combination with methods of Fourier analysis.

In this talk, we present the obtained results, as well as discuss their practical usage. We show that application of them to discrete atomic transform, which is a core of the algorithm DAC (discrete atomic compression) [3, 4], provides fast digital image processing in combination with low additional resource expenses. Also, we compare the results obtained with other approaches and provide a comprehensive discussion.

References

1. Rvachev V.L., Rvachev V. A. Non-classical methods of approximation theory in boundary value problems. – Kyiv, "Naukova dumka" Publ., 1979. – 196 p.

2. Rvachev V. A. Compactly supported solutions of functional-differential equations and their applications. *Russian Math. Surveys*, 1990, Vol. 45, No. 1, pp. 87 – 120.

3. Lukin V., Brysina I., Makarichev V. Discrete Atomic Compression of Digital Images: A Way to Reduce Memory Expenses. In: Nechyporuk M., Pavlikov V., Kritskiy D. (eds) *Integrated Computer Technologies in Mechanical Engineering. Advances in Intelligent Systems and Computing*, vol 1113. Springer, Cham, 2020, pp. 492 – 502. DOI: https://doi.org/10.1007/978-3-030-37618-5_42.

4. Viktor O. Makarichev, Vladimir V. Lukin, Iryna V. Brysina, Benoit Vozel, Kacem Chehdi. Discrete atomic compression of satellite images: a comprehensive efficiency research. *Proc. SPIE 11862, Image and Signal Processing for Remote Sensing XXVII*, 118620Q (12 September 2021); DOI: https://doi.org/10.1117/12.2599895.

АНАЛІЗ МЕТОДІВ СИНТЕЗУ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО КОДУВАННЯ ДЛЯ ПОБУДОВИ ГРУП НЕСИМЕТРИЧНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ ПОДВІЙНОГО ЦИКЛУ

Рудницький В.М., Лада Н.В.
Черкаський державний технологічний університет, Черкаси, Україна
Лада С.В.
Головне управління ДСНС України у Черкаській області, Черкаси, Україна

Одним із основних напрямків сучасних досліджень по підвищенню якості криптоалгоритмів, як не парадоксально, полягає в забезпеченні розробників систем захисту інформації додатковими можливостями, або додатковими інструментальними засобами. Під даними можливостями можна розглядати операції криптографічного кодування (криптографічного перетворення) які є складовими частинами з яких будуються крипто алгоритми. Слід зазначити що збільшення кількості операцій криптоперетворення, не залежно від процента їх використання, приводить до збільшення теоретичної варіативності і складності алгоритму.

При дослідженні двохоперандних операцій криптографічного кодування, які дозволяють перестановку операндів місцями, було встановлено що операції діляться на симетричні операції криптоперетворення, які частково досліджуваліся. В свою чергу несиметричні. двохоперандні операції криптографічного кодування діляться на операції подвійного та потрійного циклу криптографічного перетворення.

На сьогоднішній день розроблені методи синтезу груп симетричних модифікованих операцій додавання за модулями [1, 2].

Дані методи побудовані на основі дублювання одноопераднних двохрозрядних операцій базової групи. В процесі дослідження було встановлено, що методи синтезу груп симетричних операцій криптографічного кодування можна використати для синтезу груп несиметричних операцій криптографічного кодування подвійного циклу.

Список літератури

1. Лада Н. В., Козловська С. Г., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій додавання за модулем чотири. Центральноукраїнський науковий вісник. Технічні науки. Збірник наукових праць. Кропивницький: КНТУ, 2019. Вип. 2 (33). С. 181–189. DOI: https://doi.org/10.32515/2664-262X.2019.2(33).181-189

2. Лада Н. В., Рудницький С. В., Зажома В. М., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій правостороннього додавання за модулем чотири. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2020. № 1 (59). С. 93-96. - DOI: https://doi.org/10.26906/SUNZ.2020.1.093

DEVELOPMENT AND MODELING OF SPECIALIZED MEANS OF DIGITAL INFORMATION PROCESSING

Koshman S., Kinchyk A.
V. N. Karazin Kharkiv National University, Kharkov, Ukraine

The development of modern high-speed means of digital information processing (MDIP) is a very actual and important task. This is due to a significant increase in digital information.

First of all, this is due to the rapid digitalization of modern society. Recent studies show that a significant increase in the speed of modern specialized MDIP is limited by the use of positional numbering system (PNS), which is used to present information in almost all MDIP.

This is primarily due to the presence of inter-bit relationships in PNS and the limited use of tabular arithmetic. However, quite positive results in improving the speed of implementation of arithmetic operations gives the use of non-positional system of residual classes (RSC) as a number system MDIP [1]. In addition, the use of programmable logic integrated circuits (PLIC) or FPGA as an element base, allows you to effectively implement non-traditional architectures of specialized MDIP, which significantly expands the use of RSC [2-3].

The **purpose** of the report is to study the results of simulation modeling of specialized digital information processing tools, which is presented in the RSC.

The report analyzes the positional and non-positional number systems, identifies their advantages and disadvantages, presents the features of the use of RSC in the creation of specialized MDIP on the basis of PLIC.

The main stages and features of designing specialized MDIP in RSC are presented. It is shown that the regular structure of PLIC allows to effectively implement MDIP in RSC, the structure of which is presented in the form of separate computational paths, and also provides the maximum level of parallelism when performing arithmetic operations.

The results of MDIP modeling in RSC showed that due to the properties of RSC and the structural organization of PLIC, the speed of arithmetic operations increases significantly.

This confirms the effectiveness of non-positional codes in the creation of specialized MDIP.

References

1. 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.

2. I. Ya. Akushskii and D. I. Yuditskii. "Machine Arithmetic in Residual Classes". Sov. Radio, Moscow, 1968, 440p.

3. A. Yanko, S. Koshman and V. Krasnobayev, "Algorithms of data processing in the residual classes system," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 117-121.

RESEARCH OF DATA CONTROL METHODS PRESENTED IN A MODULAR NUMBER SYSTEM

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

Scientific researches were conducted in recent years, identify promising ways to improve the performance of computer systems, which are based on the use of the modular number system (MNS) [1]. However, in existing researches little attention is paid to issues devoted to the implementation of operations of data control in the MNS. One of the disadvantages of MSS is that there are no simple signs of the output of the result of operations outside the operating range. This requires additional time to implement the error control process. This circumstance reduces the effectiveness of the use of MNS.

The purpose of the report is to develop and comparative analysis the data control methods that are presented in the MNS.

The report shows at the heart of the majority of control methods of data are based on the analysis of information, that is on comparison of data. It is possible to allocate three groups of methods of comparison of numbers in MNS. The first group includes methods of direct comparison, based on the conversion of numbers from a code MNS at position number system.

To the second group of methods, can assign the methods based on the definition (allocation) or the formation of special features, the so-called positional features of the non-positional code. The third group of methods includes methods based on the principle of zeroing. Results of a research of control methods of the data in MNS which are carried out in article have shown that the existing control methods of data in MNS based on use of application of the zeroing procedure reduce control time. Applications of this method provides obtaining reliable result of control of data in MNS. The essence of the method of error control is to use the procedure of pair number zeroing with the preliminary selection of digits. This makes it possible to increase the efficiency of the procedure for data zeroing in comparison with other control methods up to 30%.

The practical significance of the results obtained is that, in comparison with the existing methods of error control in MNS, the error detection time is more than halved. This circumstance makes it possible to increase the overall efficiency of the use of MNS in the creation of CSC [2].

References

1. A. Yanko, S. Koshman and V. Krasnobayev, "Algorithms of data processing in the residual classes system," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 117-121.

2. 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.

ДОСЛІДЖЕННЯ СПОСОБІВ РЕАЛІЗАЦІЇ АРИФМЕТИЧНИХ ОПЕРАЦІЙ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

Кошман С., Краснобаєв В., Ковальчук Д., Кузнецова Є.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

Тенденція розвитку сучасних інформаційних систем обумовлює розробку нових та вдосконалення існуючих методів обробки даних. Це пов'язано зі стрімким зростанням об'ємів інформації та необхідністю підвищення швидкодії обробки цієї інформації. Одним з перспективних напрямків обробки цілочислових даних є застосування системи залишкових класів (СЗК), яка завдяки своїм властивостям дозволяє підвищити швидкодію реалізації арифметичних операцій [1]. При цьому, на відміну від позиційної системи числення, яка використовує лише суматорний принцип реалізації арифметичних операцій, СЗК, завдяки властивості малорозрядності залишків, дозволяє ефективно використовувати декілька принципів реалізації арифметичних операцій: суматорний, табличний та принцип кільцевого зсуву [2].

Метою доповіді є дослідження особливостей побудови обчислювальних засобів, що функціонують у СЗК, при використанні різних принципів реалізації арифметичних операцій.

В доповіді розглянуто три принципи технічної реалізації арифметичних цілочислових операцій у СЗК: суматорний, що заснований на основі використання малорозрядних двійкових суматорів; принцип кільцевого зсуву, що заснований на основі використання кільцевих регістрів зсуву і табличний (матричний) принцип, який заснований на використанні постійних запам'ятовуючих пристроїв.

На базі розглянутих принципів у роботі було розроблено методи реалізації арифметичних операцій. Порівняльний аналіз показав, що обчислювальні пристрої, які будуються на базі табличних методів реалізації арифметичних операцій, мають найбільшу швидкодію, однак при цьому збільшується кількість обладнання (кількість логічних елементів матричного пристрою).

Також показано, що з ростом розрядної сітки, що є характерним для сучасних обчислювальних пристроїв, ефективність застосування СЗК зростає.

Список літератури

2. Amir Sabbagh Molahosseini, Leonel Seabra de Sousa, Chip-Hong Chang. Embedded Systems Design with Special Arithmetic and Number Systems. – *Springer International Publishing*, 2017, X, 389p.

3. Краснобаев В. А., Кошман С. А., Чеснок В. А., Янко А. С. Табличный метод обработки цифровой информации в системе остаточных классов. *Сучасні ін-формаційні системи*. 2018. Т. 2, № 1. С. 38–42. DOI: https://doi.org/10.20998/2522-9052.2018.1.07

РОЗРОБКА МАТЕМАТИЧНОГО АПАРАТУ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВОЇ ПОСЛІДОВНОСТІ БЕЗ ВИКОРИСТАННЯ РЕЗІСТРА ЗСУВУ

Рисований О.М., Лещенко Р.В., Шевченко А.Г.,
Олійник А.С., Ярещенко О.В.
Національний технічний університет «Харківський політехнічний інститут»

Генератори псевдовипадкових послідовностей, які виконані на регістрах зсуву з зворотними зв'язками, використовуються в всіх системах криптографії, технічного контролю та діагностики, в імітаційному моделюванні і в інших системах.

Недоліком схем з лінійністю зворотних зв'язків є короткий період генерування послідовностей, а в разі застосування таких пристроїв при діагностування складних цифрових систем, це і не можливість розпізнавання станів більше двох. Такі стани характерні для контролерів шин, шинних формувачів, мікросхем пам'яті.

Метою доповіді є дослідження матриць зв'язків та станів для розробки генератора псевдовипадкових послідовностей без використання регістра зсуву.

В доповіді наведено, що при розробці основних положень нелінійного генератора опір зроблено на математичному апараті класичного генератора з лінійними зворотними зв'язками.

Розглянуті матриці зв'язків для поліномів різних ступенів з різними вільними членами поліномів P(X) різних ступенів. Для всіх degP(X) = 4-10 виявлені всі періоди генерування. Виявлено, що вільний член полінома P(X) не знаходиться в матриці зв'язків першого ступеня. Однак - це початковий (перший) стан матриці станів, який ніколи не входить в матрицю зв'язків першого ступеня.

Наведені матриці вихідних станів та зроблено висновок, що для реальних схем генераторів потрібно використовувати поліноми, які мають максимальний період генерації. Показані математичні відносини матриць зв'язків, на основі яких наведено формулу генерування, яка дозволяє не використовувати регістр зсуву.

Список літератури

1. Рысованый А.Н. Метод генерирования нелинейной псевдослучайной последовательности без использования обратных связей/ А.Н. Рысованый // Системи управління, навігації та зв'язку. – Полтава : ПНТУ ім. Ю. Кондратюка. –2018. – №4 (50).– С. 144-146.

2. Лидл Р. Конечные поля / Р. Лидл, Г. Нидеррайтер. – М. : Мир, 1988. – 822 с.

3. Кнут Д.Э. Искусство программирования: Получисленные алгоритмы / Кнут Д.Э. – М. : Вильямс, 2007. – Т. 2. – 832 с.

ОЦІНКА ЕФЕКТИВНОСТІ ПРОМІЖНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У МУЛЬТІХМАРНИХ СИСТЕМАХ

Рисований О.М.
Національний технічний університет «Харківський політехнічний інститут»
Козін М.Д.
Харківський національний університет радіоелектроніки

Показано, що впровадження та використання ефективних алгоритмів обробки аварійних збоїв при синхронізації даних усередині географічно розподілених систем навіть одного хмарного провайдера є завданням з нетривіальними ad-hoc рішеннями. [1,2].

У мультихмарних системах функції керування взаємодією між сховищами різних провайдерів хмарних послуг виконує проміжне програмне забезпечення (ППЗ).

Показано, що при виборі архітектури мультихмарної системи необхідно розглядати не лише параметри Угоди про рівень послуг (англ. SLA – Service Level Agreement), можливі затримки мережі та показники продуктивності кожного хмарного провайдера, а й додатково оцінки ефективності функціонування ППЗ.

Обґрунтовано, що до цих оцінок обов'язково слід відносити чисельні показники спроможності ППЗ керувати поведінкою та взаємовідносинами усіх хмарних провайдерів під час збоїв та втрати можливості синхронізувати дані у їхніх ресурсах.

Для цього у роботі пропонується використовувати коефіцієнт рівня відповідності R_L. Кількісно R_L. відображає ступінь досяжності практично отриманого виміряного проміжку часу $t_a(real)$, що виникає від моменту збою до повного відновлення доступу до актуальних даних у сховищах всіх провайдерів, з урахуванням змін у даних, що було ініційовано користувачами протягом цього проміжку, мінімально можливому теоретичному (або мінімально допустимому для кінцевих користувачів) інтервалу часу $t_a(theor)$, що необхідний для відновлення доступу до актуальних даних.

Тобто, за допомогою коефіцієнта рівня відповідності R_L можливо оцінювати якість реалізації впровадженого у ППЗ алгоритму відновлення доступу до даних у мультихмарній системі.

Список літератури

1. Venkatesan V. Effect of replica placement on the reliability of large-scale data storage systems/ V. Venkatesan, I. Iliadis, X. Hu, R. Haas, C. Fragouli // 2010 IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems. – 2010, pp. 79-88, doi: 10.1109/MASCOTS.2010.17.

2 Warner J. October 21 post-incident analysis. [Електронний ресурс] – Режим доступу: https://github.blog/2018-10-30-oct21-post-incident-analysis/.

РОЗРОБКА СИСТЕМИ ДЛЯ ПРОВЕДЕННЯ ЗМАГАНЬ З ПРОГРАМУВАННЯ НА БАЗІ МІКРОСЕРВІСІВ Т А КОНТЕЙНЕРИЗАЦІЇ

Рисований О.М., Мурейко С.А., Дмитрук К.С.
Національний технічний університет «Харківський політехнічний інститут»

З розвитком програмного забезпечення і інтернету взагалі, все більше і більше рутинної праці заміщається скриптами, або іншим програмним забезпеченням [1, 2].

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 розробник хоче автоматизувати процес збірки модулів у мікросервісному проекті, або проведення змагань з програмування [3].

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

Метою доповіді є побудова системи, яка дозволяє будувати додаток або код у спеціально виділеному середовищі, враховуючи особливості додатку, або у випадку коду, мову програмування. Та використання даної системи у змаганнях з програмування.

В доповіді наводяться результати швидкості виконання додатків або коду, порівняння з можливими частковими аналогами. Наведені дані показують, що швидкість та автономність системи дозволяє її використовувати у різних умовах та середовищах.

В зв'язку з тим чинності набувають можливість масштабування системи для використання її у великих за габаритами системах, що є однієї із головних переваг.

Список літератури

4. Kleppmann, Martin. Designing Data-Intensive Application [Текст]: учеб. пособие / Martin Kleppmann. – New York: O`Riley, 2015.

5. Newman, Sam. Building Microservices [Текст]: учеб. пособие / Sam Newman. – New York: O`Riley, 2017.

6. Рысованый А.Н. Метод генерирования нелинейной псевдослучайной последовательности без использования обратных связей/ А.Н. Рысованый // Системи управління, навігації та зв'язку. – Полтава : ПНТУ ім. Ю. Кондратюка. –2018. – №4 (50).– С. 144-146.

ПЕРЕВАГИ NODE.JS В РОЗРОБЦІ САЙТІВ ТА ЇХ СЕРВЕРНОЇ ЧАСТИНИ

Рисований О.М., Жорняк В.Р.
Національний технічний університет «Харківський політехнічний інститут»

Платформа Node або Node.js - програмна платформа, яка заснована на движку V8 (здійснює трансляцію JavaScript в машинний код), що перетворює JavaScript з вузькоспеціалізованого мови в мову загального призначення. Платформа Node.js додає можливість JavaScript взаємодіяти з пристроями введення-виведення через свій API, написаний на C ++, підключати інші зовнішні бібліотеки, написані на різних мовах, забезпечуючи виклики до них з JavaScript-коду.

Платформа використовується в IT-індустрії в якості середовища для розробки серверних додатків. Пакетний менеджер npm забезпечує стрімкий розвиток екосистеми Node.js. Зараз в ньому понад 500 тисяч опенсорсних пакетів, і кожен день з'являються нові.

Метою доповіді є дослідження сильних сторін JavaScript і Node.js.

Платформа Node.js підтримує ефективні механізми введення-виведення, використання яких не блокує виконання основного коду програми. Це говорить про те, що Node.js - це по-справжньому швидка платформа.

Справа в тому, що читання і запис файлів – це одна з найважливіших завдань серверів. Платформа Node.js справляється з цим завданням дуже добре. Для того щоб створювати фронтенд- і бекенд-додатки, досить знати одну мову - JavaScript.

Платформа Node.js використовується великими компаніями, такими, як Uber, LinkedIn, Netflix і Facebook. Node.js-додатки є крос-платформеними. Їх можна запускати на Windows, Mac і Linux.

При розробці на NodeJS використовуються подієво-орієнтоване і асинхронне програмування. Це платформа для виконання коду на сервері, на базі якої можна, користуючись самостійно підібраними фреймворками і бібліотеками, створити саме те, що потрібно. Серед популярних Node.js-фреймворків можна відзначити Express.

Висновок, Node.js цілком можна назвати відмінною платформою, що дозволяє користуватися JavaScript для бекенд-розробки.

Список літератури

1. Рысованый А.Н. Метод генерирования нелинейной псевдослучайной последовательности без использования обратных связей/ А.Н. Рысованый // Системи управління, навігації та зв'язку. – Полтава : ПНТУ ім. Ю. Кондратюка. –2018. – №4 (50).– С. 144-146.

2. Лидл Р. Конечные поля / Р. Лидл, Г. Нидеррайтер. – М. : Мир, 1988. – 822 с.

3. Кнут Д.Э. Искусство программирования: Получисленные алгоритмы / Кнут Д.Э. – М. : Вильямс, 2007. – Т. 2. – 832 с.

МЕТОД АВТОМАТИЗАЦІЇ ТЕСТУВАННЯ API ЧЕРЕЗ ІНТЕРФЕЙС КОРИСТУВАЧА

Коршун О.В.
Національний технічний університет «Харківський політехнічний інститут»

Інформаційні технології демонструють швидкий зріст за останні 10 років. Створюється багато різних технологій та застосунків. В наші дні WEB сфера є однієї з найпопулярніших сфер технологій, бо зараз майже всі технології потребують інтернет. Зараз кожен бізнес використовує інтернет та WEB технології для своєї реалізації. Для кожного бізнесу час дорівнює гроші. Це є причиною швидкого розвитку та популяризації швидкої розробки ПЗ.

В наші дні майже кожен бізнес використовує веб-застосунки. Кожен веб-застосунок має свій API, який потребує тестування. Якщо не тестувати API, то застосунок буде працювати не правильно, або взагалі не буде працювати. Це може бути причиною патері грошей для бізнесу. Також заради прибутку треба розробляти та тестувати API якомога швидше. Це надає можливість обійти конкурентів та достигати різних успіхів для бізнесу.

Є різні підходи до швидкого тестування API. Одним з таких є автоматизування API тестів для швидкого тестування старого функціонала при додаванні нового. При використовуванні даного підходу тестувальник повинен мати прямий доступ до API, якій тестується, бо без прямого доступу не можливо розробляти автоматизовані тести. Прямий доступ надає можливість виконувати запроси до API, та отримувати відповідь від серверу застосунка. Інколи тестувальник не має прямого доступу до API, або отримання доступу забирає багато часу, якого не має для тестування вчасно, яке бажає замовник зі сторони бізнесу.

Останній варіант отримання доступу у цьому випадку який може бути – це доступ до API через інтерфейс користувача. При роботі за API через інтерфейс користувача тестувальник може використовувати метод автоматизації тестування API через інтерфейс користувача. Цей метод вирішує проблему з доступом та часом який може буте витрачено на отримання доступу, та надає можливість почати тестування якомога швидше. Недолік цього методу у тому, що тести, які працюють через інтерфейс користувача будуть повільніше ніж звичайні API тести, також можуть бути складніші для написання. Найбільша перевага даного методу це більш реальна імітація реального користувача, яка робить тестування біль точнішим, розширює тестове покриття, завдяки чому можна знайти критичні баги.

Отже, ми можемо зробити висновок, що коли тестувальник не має прямого доступу до API, та йому потрібно писати прості невеличкі тест, він може використати метод автоматизації тестування API через інтерфейс користувача. Це вирішує проблему з витраченим часом на отримання доступу, та надає можливість вчасно закінчити тестування.

РОЗРОБЛЕННЯ ЗАСОБІВ АНАЛІЗУ НАВАНТАЖЕННЯ КОМПОНЕНТІВ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА В РЕАЛЬНОМУ ЧАСІ

Потрух Д.О., Кучук Г.А.
Національний технічний університет «Харківський політехнічний інститут»

В наш час неможливо представити існування світу без обчислювальних технік. Куди не дивись, повсюди можна побачити комп'ютери у різноманітних представленнях. Будь то касові апарати, прилади для зчитування штрих-кодів, банкомати та ін. Також на сучасних підприємствах використовуються комп'ютери для проектування і виробництва різноманітної продукції. І для цього необхідно спеціальне програмне забезпечення. Так як, комп'ютерний парк може не оновлюватись довгий час, а для програм з'являються нові версії, він починає поступово зменшувати темп роботи. Причиною повільної роботи можуть бути різні фактори, такі як засміченість системи, наявність вірусів, відмова одного з компонентів. Через ці проблеми при виконанні певної операції витрачається велика кількість ресурсів системи і, як слід, операції виконуються довше ніж потрібно.

В даній роботі виконується розробка застосунку для аналізу навантаження комп'ютерної системи. Дана програма призначена зчитувати показники навантаження таких комп'ютерних елементів як: оперативна пам'ять, центральний процесор та жорсткий диск. За допомогою цієї програми можна відслідкувати, що саме може бути причиною повільної роботи, і як слід потенційно загальмовувати процес виробництва.

Для розробки програми було обрано мовний пакет Microsoft .NET Framework версії 4.7.2. В даному мовному пакеті реалізовано компонент лічильника продуктивності «PerformanceCounter», який дозволяє зчитувати дані з лічильників зазначених вище комплектуючих, а також виводити статистику для більш детального аналізу. Так само при розробці програми було використано сучасну методологія об'єктно-орієнтованого програмування, яка дозволяє при необхідності легко виправляти помилки програми або вносити новий функціонал, при цьому майже не змінюючи вже існуючий.

Програма має два види виведення результатів навантаження на комплектуючі: на екран консолі або збереження результатів в файл на диску (в форматі Microsoft Excel з виведенням графіків) для подальшого їх аналізу. Розроблена програма працює на будь-яких комп'ютерах під керуванням операційної системи Windows XP SP1 та вище.

Так як програма консольна, вона споживає мало ресурсів і не вимагає установки. Досить просто завантажити "exe" файл і запустити його. Це дає можливість швидко і без проблем запускати її на старих і нових комп'ютерах, що є хорошим рішенням проблеми діагностики навантаження на системах без подальшого впливу чоловічого фактору. Роботу було виконано в рамках дипломного проектування магістра за спеціальністю комп'ютерна інженерія.

ВИКОРИСТАННЯ МЕТОДІВ АНАЛІЗУ ДАНИХ ДЛЯ ОЦІНКИ ЕФЕКТИВНОСТІ ІНФОРМАТИЗАЦІЇ ЗАКЛАДУ ОСВІТИ

Ільїна І.В., Бабенко Є.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Інформатизація освіти передбачає широке впровадження і застосування інформаційно-комунікаційних технологій при здійсненні навчальної, наукової та управлінської функцій, притаманних освітній галузі. Інформатизація у закладах освіти має дві сторони – це інформатизація самого освітнього процесу й інформатизація управління ним. Але з розвитком техніки постає проблема, що пов'язана з використанням та обробкою великих обсягів інформації, яка необхідна для управління та функціонування закладу [1]. Для вирішення цієї проблеми доцільно використовувати методи оперативного та інтелектуального аналізу даних.

Метою доповіді є аналіз даних навчального закладу з використанням сучасних методів [2], які дозволять проаналізувати показники ефективності інформатизації навчального процесу, а також особливості використання розглянутих методів у випадках низької достовірності даних, їх перевірка за допомогою інтерв'ювання співробітників навчального закладу. **В доповіді** наводяться результати дослідження – аналіз очікуваної ефективності інформатизації навчального процесу, що отримана за допомогою методів аналізу даних, наведені емпіричні дані, які вилучені з існуючої бази даних закладу (можливе отримання помилкових або недостовірних даних, що обумовлено наявністю людського фактору та іншим причинам), та дані, які отримані за допомогою інтерв'ю. **Результати дослідження** показують, що, в цілому, позитивний ефект є, але він нижче, чим очікувалося, через деякі фактори, а саме: неоптимізовані системи, низька кваліфікація деяких співробітників, потрібність дублювати деякі матеріали у паперовій формі, потрібність вводити дані з помилками через недосконалість системи.

Список літератури

1. Жмурко І. Л. Інформатизація як інструмент модернізації вищої освіти в Україні / І. Л. Жмурко. // Актуальні проблеми використання інформаційних технологій в освітньому процесі коледжів і технікумів. – Вінниця: ВТЕК КНТЕУ. – 2019. – С. 48.

2. Ilina I., Ruban I., Mozhaiev M. Researching priority directions in the area of Data mining. *Системи управління, навігації та зв'язку*. Полтава: ПНТУ, 2020. №4(62). С. 59–63.

МЕТОДИ КЛАСИФІКАЦІЇ ОЗНАК АУДІОСИГНАЛІВ

Порошенко А.І., Коваленко А.А.
Харківський національний університет радіоелектроніки, Харків, Україна

В галузі аудіоаналітики гостро відчувається необхідність розв'язку задачі класифікації об'єктів [1]. Розв'язок цієї задачі дасть змогу істотно розширити можливості аудіоаналітичних систем. Задача аудіоаналітики складається з двох послідовних складових: детектування початкового аудіосигналу та класифікація його

ознак [2]. Методи класифікації повинні забезпечувати систематизацію об'єктів класифікації за певними вибраними ознаками [3]. Кількість значень ознак визначає кількість класифікаційних угруповань, що утворюються за цією ознакою.

Метою доповіді є дослідження методів класифікації ознак аудіосигналів різних типів, таких як автомобільна сигналізація, биття металу та музика. Для аналізу результатів використовуються методи на основі класифікатора Баєса, метод опорних векторів, GMM метод та згорткова нейронна мережа. В доповіді наводяться результати аналізу методів класифікації ознак аудіосигналів різних типів. Наведені дані показують, що використання баєсова класифікатора є неефективним завдяки помірним дискримінаційним властивостям ознак аудіосигналів. Використання GMM як класифікатора не дозволяє досягти високих показників точності розпізнавання, в порівнянні з іншими методами. Недоліками методу опорних векторів для класифікації ознак аудіосигналів є його нестійкість до шумів, складність побудови ядер та відсутність відбору ознак. Серед нейронних мереж найбільшу ефективність показують згорткові нейронні мережі, але вони є дуже вимогливими з точки зору формалізації архітектури мережі.

Список літератури

1. Коваленко, А.А. Використання прихованих марковських моделей в системах розпізнавання мови [Текст] / А.А. Коваленко, А.І. Порошенко // Проблеми інформатизації. Тези доповідей восьмої міжн. НТК. –26-27 листопада 2020. – С. 54.

2. Порошенко А.І. Методи та підходи до детектування аудіоподій різних типів [Текст] / А.І. Порошенко, А.А. Коваленко // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали одинадцятої міжнародної НТК. – 8-9 квітня 2021. – Т.2. – С. 114.

3. Ручков Є.В. Оцінювання безвідмовності резервованих структур «2-з-3» і «1-з-2» з урахуванням засобів оброблення інформації та комунікацій [Текст] / В.С. Харченко, А.А. Коваленко, Є.В. Бабешко, А.І. Порошенко // Сучасні інформаційні системи. – Харків: НТУ «ХПІ», 2020. – Том 4, № 4. – С. 77-83. doi: 10.20998/2522-9052.2020.4.11

ВИКОРИСТАННЯ АНСАМБЛЮ НЕЙРОННИХ МЕРЕЖ ДЛЯ ЗМЕНШЕННЯ ДИСПЕРСІЇ

Кучук Н.Г., Корягіна П.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сьогодні достатньо поширеним є прогнозування явищ та тенденцій з допомогою нейронних мереж. Оскільки нейронні мережі не є лінійними, вони можуть бути чутливі до специфіки навчальних даних та можуть формувати різні набори вагів при кожному навчанні, що призводить до неточності прогнозів. Для зменшення дисперсії можна використовувати ансамблі нейронних мереж. Ансамбль нейронних мереж є сукупністю двох та більше навчальних алгоритмів з метою підвищення точності прогнозування. **Метою доповіді** є аналіз методів зменшення дисперсії у нейронних мережах на основі існуючих досліджень. Результати дослідження показали що, об'єднання прогнозів від декількох нейронних

мереж додає зміщення, яке у свою чергу, протидіє дисперсії однієї моделі нейронної мережі. У результаті ми маємо прогнози, що менш чутливі до специфіки даних навчання, вибору схеми навчання та випадковості одного циклу навчання[1, 2]. Ансамбль є алгоритмом навчання з учителем, оскільки він може бути навчений і потім використаний для передбачення, через це навчений ансамбль являє собою єдину гіпотезу – припущення, що було сформоване під час навчання нейронної мережі. Ця гіпотеза може не знаходитись у просторі гіпотез моделей, з яких побудований ансамбль, що дозволяє збільшити гнучкість функцій ансамблю. Ця гнучкість, гіпотетично, може призвести до перенавчання на тренувальних даних, але на практиці, деякі типи ансамблів, особливо беггінг, схильні зменшити проблеми пов'язані з перенавчанням.

У підсумку можна підкреслити, що ансамблі схильні виявляти кращі результати, якщо існує суттєва різниця в моделях. Через це, багато ансамблів намагаються підвисити різницю у моделях що комбінують. Хоча, як було наведено вище, використання різних алгоритмів строгого навчання більш ефективне.

Список літератури

1. Bishop C. Neural Networks for Pattern Recognition / Christopher Bishop. – New York: Oxford University Press Inc., 1995. – 482 с.
2. Kuncheva L., Whitaker C. Measures of diversity in classifier ensembles and Their Relationship with the Ensemble Accuracy // Machine Learning. — 2003. — Т. 51, вид. 2.

ДОСЛІДЖЕННЯ ПОВЕДІНКИ КОРЕЛЯЦІЙНИХ ФУНКЦІЙ БАГАТОВИМІРНОЇ ЛІНІЙНОЇ СИСТЕМИ

Калінін Є.І., Лисиця Д.О., Рибальченко А.О.
Національний технічний університет «Харківський політехнічний інститут»

В теорії аналізу багатовимірних випадкових величин завдання кореляційного аналізу є важливими при побудові і реалізації багатьох систем контролю, моніторингу та діагностики. В процесі вирішення цих завдань визначення наявності та характеру статистичного взаємозв'язку досліджуваних випадкових величин є пріоритетним напрямком. Застосування класичного математичного апарату кореляційного аналізу широко використовується в припущенні про приналежність випадкового процесу, що спостерігається, багатовимірному нормальному закону розподілу [1, 2]. На практиці такі передумови кореляційного аналізу виконуються далеко не завжди і, швидше за все, є зручною математичною ідеалізацією досліджуваних процесів. **Мета доповіді** – оцінка можливості формування розриву парних та непарних складових кореляційної функції та обґрунтування даного явища. Завдання дослідження полягають у побудові принципів отримання парних та непарних складових кореляційної функції багатовимірної лінійної системи з аналізом їх безперервності в узагальненому сенсі.

Отримані результати: побудова принципів отримання парних та непарних складових кореляційної функції багатовимірної лінійної системи з аналізом їх безперервності в узагальненому сенсі; запропоноване тлумачення подібних

виразів як границі послідовності безперервних функцій, що забезпечує їх безперервність в узагальненому сенсі та усуває виниклу суперечливість в даному випадку. Практична значущість роботи полягає у побудові моделі взаємної кореляції узагальнених координат лінійної системи з урахуванням особливостей поведінки кореляційних функцій.

Список літератури

1. Tuzlukov V. P. (2002) Signal Processing Noise, CRC Press LLC, Boca Raton.
2. Mourad Barkat (2005) Signal Detection and Estimation, Artech House, Boston

МЕТОД АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Кучук Н.Г., Семенова А.С.
Національний технічний університет «Харківський політехнічний інститут»

Тестування на проникнення використовується для пошуку недоліків у комп'ютерних системах з метою вжиття відповідних заходів безпеки для захисту даних та підтримки функціональності. На етапі проектування програмісти та системні архітектори, керуючись вимогами, розробляють високорівневий дизайн системи. Створення і тестування прототипу із залученням цільової групи - найкращий спосіб оцінити новий проект і зрозуміти, чи буде він успішним як комерційний продукт. Тестування прототипу надає можливість ґрунтовно вивчити проект на самому початковому етапі робіт і внести необхідні зміни відповідно до поставлених цілей [1, 2].

Проведення автоматизованого тестування забезпечує повноцінну працездатність продукту після його випуску. Тестування прототипу дозволяє знизити ризики розробки шляхом раннього виявлення невідповідностей бізнес-вимогам, «вузьких місць» в структурі додатки, зручності для користувачів і дефектів логіки функціоналу додатка ще до початку розробки. Своєчасні зміни виконані на етапі прототипування, допомагають запобігти коштовні переробки системи на стадіях розробки. Завдяки кваліфікованій роботі QA інженерів, тестування прототипу дозволить розрахувати потенційні витрати на кожному етапі створення продукту і визначитися з найбільш ефективною моделлю розробки. На етапі проектування QA інженер починає створювати тестову документацію. Створення тестової документації значно покращує якість продукту за рахунок більш тісної співпраці, уточнення деталей при розробці плану тестування і документації. Після завершення тестування наявність тестової документації дозволяє перевірити, наскільки успішно були проведені всі етапи тестування.

Список літератури

1. Web Application Performance: 7 Common Problems and How to Solve Them – Режим доступу : https://stackify.com/web-application-problems/

2 Ian Molyneaux The Art of Application Performance Testing, 2nd Edition / Ian Molyneaux – O'Reilly Media, Inc.

МЕТОДИ ГОЛОСОВОЇ ІДЕНТИФІКАЦІЇ

Іващенко Г.С., Коваль Д.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Однією з актуальних задач розвитку інформаційних технологій є забезпечення надійного захисту інформації шляхом автентифікації користувачів. Способи автентифікації можна розділити на парольну (перевіряється знання користувачем унікальної інформації), автентифікацію з використанням апаратного ключу та біометричну автентифікацію.

Біометричні методи дозволяють ідентифікувати людину за ознаками, пов'язаними з її фізіологічними особливостями. Наприклад, геометрична будова руки, відбитки пальців, райдужна оболонка ока, характеристики і особливості мови та почерку (рукописного, клавіатурного чи комп'ютерного) та інші. Для мовної ідентифікації людини необхідно мати шаблон, з яким порівнюватиметься голосовий ключ. Порівняння ключа і шаблону може проводитися за такими характеристиками, як амплітуда і потужність (гучність), часові, частотні (тембр), енергетичні, фазові характеристики [1]. Існують різні методи ідентифікації за голосом: на основі моделі Гаусових сумішей, прихованих Марківських моделей, шляхом аналізу мел-частотних кепстральних коефіцієнтів [2]. Для аналізу даних найбільшого поширення набули засоби обчислювального інтелекту, такі як штучні нейронні мережі (ШНМ), серед архітектур яких для голосової ідентифікації доцільним є використання багатошарового персептрону та карт Кохонена, що здатні до самоорганізації [3].

Метою роботи є дослідження методів ідентифікації людини за особливостями голосу та розробка програмного забезпечення для реалізації порівняльного аналізу методів голосової ідентифікації.

Розглянута програмна платформа ML.NET, що надає доступ до засобів машинного навчання TensorFlow.

Здійснені порівняння методу аналізу розподілу мел-частотних кепстральних коефіцієнтів та методу на основі карт Кохонена. Особливістю методики навчання нейронної мережи є вибір основного нейрона, що дозволяє зменшити кількість ітерацій і, як наслідок, скоротити час навчання та виконання порівняно з відомими рішеннями.

Список літератури

1. Бідюк П. І., Бондарчук В. Сучасні методи біометричної ідентифікації. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник.* 2009. № 1 (18). С. 137–146.

2. Заковряшин А. С., Малинин П. В., Лепендин А. А. Применение распределений мел-частотных кепстральных коэффициентов для голосовой идентификации личности. *Известия Алтайского государственного университета*. 2007. № 5 (81). С. 156–160.

3. Меньшаков П. А., Мурашко И. А. Методика голосовой идентификации на основе нейронных сетей. *Доклады Белорусского государственного университета информатики и радиоэлектроники*. 2017. № 4 (106). С. 12–18.

МЕТОДИ ПРОГНОЗУВАННЯ РОЗВИТКУ ПАНДЕМІЙ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ З УРАХУВАННЯМ ЗОВНІШНІХ ФАКТОРІВ

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

У сучасному світі дуже актуальною є проблема обробки даних, що описують динаміку розвитку пандемії. Своєчасне вжиття медичних та організаційних заходів з урахуванням вірогідного початку чи закінчення хвиль захворювання у найближчому майбутньому, дозволить зменшити навантаження на медичні заклади, зменшити кількість інфікованих серед населення та знизити тиск на економіку.

Дані стосовно динаміки числа інфікованих можуть буди представлені у вигляді часових рядів, які можуть бути описані математичними моделями, для обробки яких доцільним є використання технічних засобів.

На даний момент існує багато методів прогнозування часових рядів, проте серед них слід виділити підходи, засновані на засобах машинного навчання, які дозволяють в автоматичному режимі підлаштовувати моделі під нові дані, а також враховувати зовнішні фактори.

Метою роботи є дослідження методів прогнозування динаміки розвитку пандемій з урахуванням зовнішніх факторів за допомогою моделей машинного навчання на основі штучних нейронних мереж.

У якості вхідних даних використані часові ряди з даними о кількості осіб, що захворіли, кількості тих, хто помер, одужав чи пройшов курс вакцинації.

Для забезпечення автоматизації аналізу та прогнозування використана командна оболонка Jupyter Notebook, яка надає зручний інтерфейс для роботи з засобами машинного навчання Tensorflow та візуалізації результатів у вигляді таблиць та графіків.

Для вирішення завдання прогнозування розвитку пандемій використані моделі згорткових нейронних мереж (CNN) [1], рекурентних нейронних мереж (RNN) [2] та мереж з довгою короткостроковою пам'яттю (LSTM) [3].

Список літератури

1. Mehtab S., Sen J., Dasgupta S. Robust Analysis of Stock Price Time Series Using CNN and LSTM-Based Deep Learning Models. *4th IEEE Conference on Electronics, Communication and Aerospace Technology ICECA'20*. 2020. P. 1481–1486. DOI: https://doi.org/10.1109/ICECA49313.2020.9297652.

2. Recurrent Neural Networks [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.ibm.com/cloud/learn/recurrent-neural-networks.

3. Olah C. Understanding LSTM Networks [Електронний ресурс] / Christopher Olah. – 2015. – Режим доступу до ресурсу: http://colah.github.io/posts/2015-08-Understanding-LSTMs/.

ПОРІВНЯЛЬНИЙ АНАЛІЗ РІШЕНЬ ЗАДАЧІ КОММІВОЯЖЕРА НА ОСНОВІ ОБЧИСЛЮВАЛЬНОГО ІНТЕЛЕКТУ

Іващенко Г.С., Онищенко О.І.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день проблема пошуку маршрутів залишається актуальною, адже має високу трудомісткість вирішення та її різновиди зустрічаються у багатьох сферах людської діяльності. Для опису таких задач доречним є використання теорії графів, серед класичних проблем якої найбільш поширеною є вирішення задачі комівояжера. Порівняльний аналіз рішень задачі комівояжера різними методами для однакових даних дозволяє досліджувати нові та порівнювати вже існуючі методи побудови шляху.

Оскільки задача комівояжера відноситься до класу NP-важких задач, при пошуку рішень широкого розповсюдження набули алгоритми на основі засобів обчислювального інтелекту. Дані алгоритми здебільшого відносяться до евристичних, і тому не гарантують знаходження найкращих вирішень, але дають змогу отримувати наближені рішення за прийнятний час в умовах високої обчислювальної складності [1]. На практиці, при застосуваннях задачі комівояжера нерідко вагомими факторами є як час, так і точність отриманого рішення, що спонукає до розробки нових варіацій відомих методів вирішення та викликає необхідність їх порівняльного аналізу.

Метою роботи є аналіз реалізацій алгоритмів на основі підходів обчислювального інтелекту для вирішення задачі комівояжера, з метою виявлення закономірностей, що позитивно впливають на час та точність пошуку рішень.

Розглянуті генетичний алгоритм та алгоритм мурашиної колонії, через можливість їх гнучкого налаштування.

Для вирішення задачі запропоновано оцінювати вплив початкових параметрів: розмір популяції та ймовірність мутації в випадку генетичних алгоритмів; кількість штучних мурах (агентів), їх початкове розташування, підбір коефіцієнтів ваги шляху та феромону у випадку імітації мурашиної колонії. Для оцінки ефективності мурашиних алгоритмів також слід проаналізувати вплив встановлених правил оновлення феромону агентами, наявності рангової системи та можливості паралельного пошуку кращого шляху [2]. При аналізі використання варіантів генетичних алгоритмів особлива увага приділяється дослідженню залежностей часу та точності рішень від обраних реалізацій основних генетичних операцій: селекції, схрещування та мутації.

Список літератури

1. Kokash N. An introduction to heuristic algorithms. The Advances in Computer Science: an International Journal. 2014. Vol. 3, №5. ACSIJ-2014-3-5-560.

2. Dorigo M., Birattari M., Stützle T. Ant Colony Optimization. Artificial Ants as a Computational Intelligence Technique. IEEE Computational Intelligence Magazine. 2006. Vol. 1, №4. P. 28–39. DOI: 10.1109/CI-M.2006.248054.

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ПРОГНОЗУВАННЯ ЧАСОВИХ РЯДІВ НА ОСНОВІ ОБЧИСЛЮВАЛЬНОГО ІНТЕЛЕКТУ

Іващенко Г.С., Понамарьов В.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Проблема вибору методу прогнозування часових рядів на основі обчислювального інтелекту залишається актуальним завданням, оскільки результат прогнозування залежить від різних параметрів, таких як обсяг та достовірність необхідної початкової інформації, зміна середовища, в якому протікає процес, доступність необхідних обчислювальних засобів.

В даний час активно розвиваються підходи на основі методів машинного навчання, такі як штучні нейронні мережі, генетичні алгоритми та штучні імунні системи. Штучна нейронна мережа – обчислювальна система, яка побудована за принципом функціонування біологічних нейронних мереж [1]. Генетичний алгоритм – евристичний алгоритм випадкового пошуку, який використовується для вирішення завдань оптимізації та моделювання шляхом підбору, комбінування та варіації шуканих параметрів з використанням механізмів, аналогічних природному відбору [2]. Штучні імунні системи –обчислювальні парадигми, що побудовані на основі опису різних аспектів функціонування біологічної імунної системи [3]. Перевагами цих підходів є адаптивність, масштабованість, швидкість навчання, можливість самонавчання і здатність створювати гібридні моделі з використанням інших методів.

Метою роботи є аналіз методів короткострокового прогнозування стаціонарних часових рядів з урахуванням зовнішніх числових факторів на основі засобів обчислювального інтелекту, таких як штучні нейронні мережі, генетичні алгоритми та штучні імунні системи.

Для аналізу обрано часові ряди даних онлайн-продажу квитків у кінотеатр. Відповідність вхідних даних до умови стаціонарність дозволяє отримати точніші дані прогнозу, на відміну від прогнозування нестаціонарних часових рядів. Досліджується використання штучної нейронної мережі (перцептрон), генетичного алгоритму (шляхом відновлення функціональної залежності, що описує часовий ряд) та штучної імунної системи (модель клонального відбору).

Список літератури

1. Morariu N., Iancu E., Sorin V. A neural network model for time series forecasting. *Romanian Journal of Economic Forecasting*. 2009. № 4. С. 213–223.

2. Mahfoud S., Mani G. Financial Forecasting Using Genetic Algorithms. *Applied Artificial Intelligence*. 1996. Т. 10, № 6. С. 543–565. DOI: https://doi.org/10.1080/088395196118425.

3. Andrews P., Timmis G. Inspiration for the Next Generation of Artificial Immune Systems. *Springer Lecture Notes in Computer Science*. 2006. Т. 3627. С. 126–138. DOI: https://doi.org/10.1007/11536444_10.

ГІБРИДНІ МЕТОДИ РІШЕННЯ ТРАНСПОРТНОЇ ЗАДАЧІ

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

Транспортна задача або задача маршрутизації транспорту (ЗМТ) представляє собою задачу знаходження маршрутів постачання з найменшою вартістю, які проходять через набор географічно розподілених споживачів, з урахуванням ряду додаткових обмежень. Ця проблема займає центральне місце в областях транспортних перевезень, переміщення та логістики. Вирішення такого роду задач дозволить зекономити ресурси на вантажоперевезеннях багатьом організаціям, наприклад службам швидкої допомоги, інтернет-магазинам, оптовим базам, автотранспортним підприємствам та компаніям, що займаються вантажоперевезеннями.

Наявність обмежень, які необхідно враховувати при побудові маршруту, призводять до можливості представлення задачі у вигляді одного з типів існуючих ЗМТ. ЗМТ відноситься до класу NP-повних задач, що накладає обмеження розмірності задачі для доцільного застосування точних детермінованих алгоритмів. Зокрема, для вирішення завдань великої розмірності отримали поширення евристичні та мета-евристичні алгоритми, а також їх можливі комбінації [1]. Але через особливості в обчисленнях для однієї і тієї ж задачі такі алгоритми можуть генерувати різні рішення, як правило, наближені до найкоротшого.

Метою роботи є аналіз гібридних алгоритмів для вирішення ЗМТ з обмеженням на вантажопідйомність та кількість транспортних засобів та їх обов'язкове повернення до початку маршруту. Дане обмеження створює додаткову умову – обсяг вантажу на кожному маршруті не повинен перевищувати заданого ліміту (однакового для всіх маршрутів). Таким чином, метою вирішення задачі стає не тільки знаходження найкоротших маршрутів, а й мінімізація їх кількості.

В роботі розглядаються комбінації генетичного алгоритму та таких класичних методів вирішення ЗМТ [2], як алгоритм збережень Кларка-Райта, жадібний алгоритм, метод гілок та меж. Класичні алгоритми пропонується використовувати для створення початкової популяції, в якій генотип кожної особини містить кілька маршрутів, що складаються з упорядкованої підмножини клієнтів. Для забезпечення роботи генетичного алгоритму необхідно модифікувати проблемно-орієнтовані оператори мутації та схрещування в залежності від обраного класичного алгоритму.

Список літератури

1. Golden L., Raghavan S., Wasil A. The Vehicle Routing Problem: Latest Advances and New Challenges. 2008. P. 29–48.

2. Toth P., Vigo D. Vehicle Routing Problems, Methods and Applications. Second Edition. 2014. P. 87-97.

ПРОБЛЕМА ВИБОРУ АЛГОРИТМУ ПОШУКУ НАЙКОРОТШОГО ШЛЯХУ В ЛАБІРИНТАХ

Іващенко Г.С., Солонцевой Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Задача проходження лабіринтів досить поширена – у якості лабіринту може бути представлена як і будівля з великою кількістю приміщень, розташованих на різних поверхах з численними варіантами переходів між ними, так і локації у ігрових програмних застосунках з відкритим світом. При проектуванні ігрового штучного інтелекту однією з проблем є реалізація пересування неігрових персонажів (NPC) по локаціям.

Локації можуть бути представлені у вигляді лабіринтів, для опису яких доцільним є використання теорії графів. Найпоширенішими задачами теорії графів є різні варіанти пошуку найкоротшого маршруту: що проходить через усі задані точки, з необхідністю повернення у початкову точку, чи маршрут між двома обраними точками. Вибір оптимального шляху із безлічі можливих варіантів його побудови залежить від структури графу та урахування зовнішніх факторів. Найкоротшим шляхом у лабіринті може бути як і шлях, який потребує найменшу кількість пересувань так і шлях, який витрачає менше певного ресурсу, наприклад, часу, енергії, тощо [1].

Алгоритми пошуку шляху на графах відрізняються між собою наборами правил прийняття рішень у ході виконання. У деяких випадках на вибір шляху алгоритмом впливають попередньо вказані зовнішні фактори системи. Наприклад, певні обмеження на перехід між клітинами лабіринту, або системи зі змінюваними умовами із плином часу.

Метою доповіді є аналіз роботи алгоритмів пошуку найкоротшого шляху у лабіринтах.

Для цього реалізовано застосунок на основі фреймворку Spring на мові програмування Java [2]. Даний застосунок приймає у якості вхідних даних певний лабіринт, а також дозволяє обрати алгоритм пошуку найкоротшого шляху у даному лабіринті. Застосунок відображає користувачеві шлях, обраний алгоритмом, та час, який було витрачено на його пошук. У ході аналізу досліджено використання жадібних алгоритмів (Дейкстри, пошук A*, алгоритми Пріма та Крускала), а також засоби обчислювального інтелекту (генетичний алгоритм, мурашиний алгоритм, імітація відпалу та штучні нейронні мережі Хопфілда та Кохонена).

Список літератури

1. Євстігнєєв В. А. Итеративные алгоритмы глобального анализа графов. Пути и покрытия. Применение теории графов в программировании. 2005. Т. 3, № 1. С. 138–150.

2. Walls C. Spring Boot in Action. Manning Publications. 2015. С. 264. ISBN–9781617292545.

МЕТОД ПОПЕРЕДНЬОЇ ОБРОБКИ ДАНИХ ЕЛЕКТРОЕНЦЕФАЛОГРАМИ

Іващенко Г.С., Чернов Д.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Технологія електроенцефалограми (ЕЕГ) існує протягом більшої частини минулого століття, але порівняно недавно вона стала доступною для широкого використання. У кінці XX та на початку XXI сторіччя ЕЕГ вийшла на споживчий ринок, коли були створені компанії, що є на сьогоднішній день найбільшими виробниками ЕЕГ-обладнання. Це забезпечило доступ до використання ЕЕГ-пристроїв користувачами у різних сферах, зокрема, в медичних, академічних, споживчих дослідженнях, охороні здоров'я тощо [1].

Основним етапом аналізу ЕЕГ-даних є виявлення різних типів мозкових хвиль: альфа, бета, гамма, дельта і тета хвилі. Кожен з цих типів хвиль може бути виявлений з неопрацьованого ЕЕГ-сигналу та характеризує різний стан людського мозку [2]. Але для подальшого аналізу, наприклад, виявлення патернів, що відповідають тим чи іншим діям користувача, необхідна обробка вхідного сигналу. Вимірювання ЕЕГ-даних може проводитись при наявності у приміщеннях великої кількості електричних пристроїв, які призводять до появи викривлень у вимірюваннях, через це виникає необхідність у попередній обробці вхідного сигналу. Підготовлені вхідні дані можуть бути у подальшому оброблені за допомогою методів машинного навчання для автоматичного аналізу даних електроенцефалограми [3].

Метою роботи є визначення методу обробки даних електроенцефалограми для отримання типів хвиль мозку з необробленого сигналу, а також виконання обробки для подальшого аналізу сигналу засобами машинного навчання. Пропонується зазначений метод на основі апаратних можливостей модуля ThinkGear ASIC від компанії NeuroSky, який може надавати по Bluetooth необроблений ЕЕГ-сигнал. Програмна частина виконує збереження вхідних даних, після чого виконує їх обробку у вигляді застосування Min-Max нормалізації, отримання періодограми Уелча для отримання спектральної густини потужності, визначення сили діапазону хвиль мозку за допомогою правила Сімпсона для отримання площі під кривою графіка спектральної густини потужності.

Список літератури

1. Mahsa Soufineyestani, Dale Dowling, Arshia Khan. Electroencephalography (EEG) Technology Applications and Available Devices. *Department of Computer Science, University of Minnesota Duluth*. 2020. DOI: https://doi.org/10.3390/app10217453

2. Teplan M. Fundamentals of EEG Measurement. *IEEE Measurement Science Review*. 2002. Vol. 2. P. 1–11. DOI: https://www.measurement.sk/2002/S2/Teplan.pdf

3. Yang Si. Machine learning applications for electroencephalograph signals in epilepsy: a quick review. *Acta Epileptologica*. 2020. Vol. 2, Article number: 5. DOI: https://doi.org/10.1186/s42494-020-00014-0

МОДЕЛЬ ВИКОРИСТАННЯ СОПРОГРАМНИХ ПРИМІТИВІВ У ВБУДОВАНИХ СИСТЕМАХ НА БАЗІ ARM ПРОЦЕСОРІВ

Корнієнко В.Р., Філіппенко І.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Soft-realtime вбудовані рішення на базі ARM процесорів знаходять широке застосування у системах IoT мереж, керування та взаємодії з користувачем (Human-Interface Panels). Зростаючі потреби з боку функціоналу, що має бути представлений у пристрої, ставлять нові задачі для розробників вбудованого програмного забезпечення з боку інструментарію та побудови архітектури.

Метою доповіді є огляд та реалізація моделі розподілу задач у системі з використанням сопрограм з C++20, що дозволяють виконати лінеаризацію коду програми, забезпечити гнучкий механізм передачі керування від задачі до задачі та зменшити потенційні можливості для виникнення стану гонки у програмі.

Згідно до існуючих даних, сопрограмні моделі на момент 2019-го року були використані у більше ніж 400 000 пристроїв[1].

В доповіді наводяться аналітичні обгрунтування запропонованої моделі використання сопрограм для програмування вбудованих систем. Наведено експериментальні данні що до використання супутніх примітивів для збільшення потенціальних місць, де модель може бути застосована. У рамках виконання інтеграції з існуючими рішеннями запропоновано набір примітивів для роботи з послідовними інтерфейсами на базі архітектури Device-Driver-Component[2].

Згідно до майбутніх варіантів дослідження запропоновано варіанти для інтеграції моделі з існуючими бібліотеками вбудованих файлових систем, таких як littlefs та FatFs.

Наведені данні показують, що сопрограмна модель програмування дозволяє суттєво зменшити розміри прошивки за рахунок внутрішніх оптимізацій компілятора, відмовитися від RTOS або інтегруватися у її API для створення пулу потоків, що розділяють між собою конкретні фрагменти периферійної та користувацької взаємодії.

Список літератури

1. Nishanov G. A proposal to add coroutines to the C++ standard library (Revision 1) [Електронний ресурс] / Gor Nishanov // ISO ++. – 2014. – Режим доступу до ресурсу: https://isocpp.org/files/papers/n3985.pdf.

2. Robenko A. Practical Guide to Bare Metal C++ [Електронний ресурс] / Alex Robenko // github.io. – 2014. – Режим доступу до ресурсу: https://arobenko.github.io/bare_metal_cpp/.

МЕТОДИ ПРОЕКТУВАННЯ РЕКУРСИВНИХ ЦИФРОВИХ ФІЛЬТРІВ

Волков Є.І., Філіппенко І.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Цифрова фільтрація є одним з найбільш потужних інструментальних засобів цифрової обробки сигналів (ЦОС). Розробники все частіше застосовують програмовані логічні інтегральні схеми ПЛІС для цифрової фільтрації через можливість виробляти потокову обробку сигналу на високих частотах [1]. Досягти високої швидкості обчислень можна з допомогою методів паралельних розрахунків, зручних реалізації на ПЛИС. FPGA Xilinx останніх поколінь дозволяють реалізовувати більш ефективні порівняно з сигнальними процесорами алгоритми ЦОС.

Метою доповіді є аналіз методів проектування рекурсивних цифрових фільтрів (ЦФ) у цілісному просторі станів з урахуванням основних факторів, що визначають їх реалізацію.

В доповіді розглядаються основні аспекти, які необхідно враховувати розробки цифрових фільтрів.

Головним чином складність цифрових фільтрів, що містять помножувачі, суматори, регістри та інші допоміжні пристрої визначається множниками [1]. Складність і швидкодія самих розумно-жителів визначаються розрядностями коефіцієнтів і внутрішніх змінних у фільтрі. Тому ці розрядності необхідно вибирати мінімально можливими.

Найчастіше на практиці при побудові різних систем ЦОС широко застосовуються ЦФ з постійними коефіцієнтами. Використання повноцінних помножувачів при розробці таких ЦФ є невиправдано витратним, особливо при великій їх кількості та високій розрядності. При проектуванні ЦФ для систем, що реалізуються на ПЛІС ставляться завдання отримання необхідних частотних характеристик при мінімальній кількості кристалічних ресурсів.

Неоптимальне вирішення цієї задачі призводить до нераціонального витрачання площі кристала, до невиправданого збільшення споживаної потужності, зниження швидкодії, перешкоджає розміщенню системи ЦОС на одному або малому числі кристалів і, зрештою, підвищує вартість виробу. Таким чином, створення методики проектування рекурсивних ЦФ з урахуванням основних факторів, що визначають їх апаратну реалізацію на ПЛІС, є актуальною науково-технічною проблемою.

Список літератури

1. Зотов В.Ю. Проектирование цифровых устройств на основе ПЛИС фирмы Xilinx в САПР WebPACK ISE. М.: Горячая линия–Телеком, 2003. 624 с.

2. Смит С. Цифровая обработка сигналов. Практическое руководство для инженеров и научных работников. М.: Додэка-XXI, 2011. 720 с.

3. Солонина А.И., Арбузов С.М. Цифровая обработка сигналов. Моделирование в MatLab. СПб.: БХВ-Петербург, 2008. 816 с.

PLATFORM DEVELOPMENT FOR INTEGRATION WITH THE "ZOHO" CRM SYSTEM

Kuchuk N., Kravchenko R.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Today's businesses are dependent on IT. Every part of the business now needs an Internet connection to work, not just for movies during breaks; from e-mail, instant messaging and VoIP, to ERP and CRM back office - not to mention the importance of digital marketing and e-commerce channels. We will dwell on CRM systems in more detail. CRM (Customer Relationship Management) is not a software product and not a technology. This is not even a set of products. CRM is a concept and business strategy aimed at building a sustainable business, the core of which is a "customer-oriented" approach [1, 2].

This strategy is based on the use of advanced management and information technology, through which the company collects information about its customers at all stages of its life cycle (attraction, retention, loyalty), draws knowledge from it and uses this knowledge for its business by building mutually beneficial relationships with them [3].

The result of the strategy is to increase the company's competitiveness and increase profits, as a well-built relationship based on a personal approach to each client, allows you to attract new customers and help keep the old ones.

This report presents a study of CRM-system, an overview of those that currently exist, the main functions required for this platform, the requirements for this platform, the stages of technology development of the web platform, the choice of local service, programming language, framework and environment programming, functional testing of the web application.

The analysis of programming languages is carried out, on the basis of which the choice was made in favor of programming language C # as the main development language, Swing technology as a means of creating a graphical interface and MySQL database as a means of storing information.

The report also highlights the results of database development, with a description of all tables and their purpose, developed an interface, designed the server and client part of the web service.

The created platform and system components meet the declared functional and modern technical requirements and are ready for wide use.

References

1. Лаврищева Е.М., Грищенко В.Н. / Сборочное программирование. Основы индустрии программных продуктов / 2-изд. Дополненное и переработанное. – Киев: Наук. думка, 2009.– 372с.–ISBN 978-966-00-0848-1.

2. Шнайдер Р. / Microsoft SQL Server 6.5. Проектирование высокопроизводительных баз данных, – М.: Лори, 2010. – 361 с.

3. Грофф Дж., Вайнберг П. SQL: полное руководство. К: BHV, 2005. – 608 с.

Підсекція 5.2. Цивільна безпека (інформаційна підтримка)

CYBERSPACE AS A FIFTH DOMAIN OF MILITARY OPERATIONS

Hashimov E.G., Aliyev K.R.
Military Academy of the Armed Forces of the Republic of Azerbaijan

The development and widespread use of information technology in all areas, including the military, requires increased attention to cybersecurity when planning military security. In the Military Doctrine of the Republic of Azerbaijan, one of the tasks of the Armed Forces and other armed formations only in peacetime is to ensure information security [1]. However, it should be borne in mind that information security from the point of view of cybersecurity exists not only in peacetime, but also in all three security conditions defined in the Military Doctrine of Azerbaijan Republic, that is, "peacetime", "real threat" and "war (armed conflict) ". It can be concluded that in the Military Doctrine of the Republic of Azerbaijan there is a need to consider the adoption of the concepts of cyberspace and cybersecurity from the point of view of information security. There is no doubt that Armenia will not be able to restore its Armed Forces for a long time after the shameful defeat in the Second Karabakh War. However, Armenia will continue to strive for asymmetric warfare and may launch cyberattacks against Azerbaijan. The dynamic development of Azerbaijan in terms of technology and infrastructure creates favorable conditions for cyber attacks. Moreover, Azerbaijan may be subject to cyber attacks not only from the Republic of Armenia, but also in the interests of other state and non-governmental organizations.

Currently, the main threats in cyberspace come from APT (Advanced Persistent Threat) groups. The APT groups are believed to have been formed by Russia (BEAR), North Korea (CHOLLIMA), China (PANDA), Iran (KITTEN) and Vietnam (OCEAN BUFFALO). APT targets typically cover finance, healthcare, manufacturing, telecommunications, energy, aerospace and aviation industries, government agencies, as well as political, scientific and national security spheres [2]. Given that Azerbaijan borders on two countries suspected of cyberattacks (Iran and Russia), and is pursuing reforms in all these areas, the possibility of becoming a cyber target in any area is inevitable.

What is an advanced persistent threat (APT)? An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization, evade existing security measures and fly under the radar. Executing an APT attack requires a higher degree of customization and sophistication than a traditional attack.

Adversaries are typically well-funded, experienced teams of cybercriminals that target high-value organizations. They ve spent significant time and resources researching and identifying vulnerabilities within the organization.

The goals of APTs fall into four general categories:

- Cyber Espionage, including theft of intellectual property or state secrets
- eCrime for financial gain
- Hacktivism
- Destruction [2].

Modern wars fought with advanced technology increase the importance of cyberspace in battle. Some countries have already adopted the idea of using cyberspace as part of their military strategy. It is no coincidence that cyberspace was also recognized as a field of operations at the 2016 NATO Warsaw Summit. In particular, cyberspace has become the fifth space for military operations, along with air, sea, land and space [3]. Assigning cyberspace the same status as other domains means that it should be treated in the same way when defining capabilities and strategies for defenses and attacks.

Located in a region of geopolitical importance, Azerbaijan must be prepared for cyber threats and adapt its national security strategies to modern cyberspace-focused military doctrines. The possibility of government support for Advanced Persistent Threat (APT) groups in neighboring countries requires accelerating the process.

The most effective fight against APT groups in Azerbaijan can be developed jointly or separately with the Computer Incident Response Team (CIRT). The first step for this could be the inclusion of cyberspace as a separate area in the Military Doctrine of the Republic of Azerbaijan, and then the creation of the necessary platform for the management of cyber operations.

References

1. http://www.e-qanun.az/framework/19722
2. https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/
3. https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

DEFINITION OF CYBER TERRORISM AND DIFFERENCE TO CYBER WARFARE

Mahmudov N.V.
War College of the Armed Forces of the Republic of Azerbaijan

Introduction. During the last two decades the infrastructure of modern western economies has changed fundamentally. The reliance on computer networks has increased, not only in the service sector but also in the high-technology economy. The state system as a whole depends on computers, electronic data storage and transfers, and highly integrated communications networks. The result is the rapid development of a new form of critical infrastructure and hence the emergence of a vulnerability to new threats, grouped in this article as 'cyber-threats'. As new technologies have been developed, terrorists and other actors used the internet as their weapon. The Internet does not rely on territorial boundaries, nation-states or other institutional bodies. Identification and law enforcement seems to be a bigger challenge for the

future. The seemingly limitless boundaries of cyber space have allowed virtually anyone to launch an attack from a remote and anonymous location. If somebody discovers however this attack, it is not clear who is responsible or moreover, if somebody would be able to deal with this cyber attack. At the same time our increasing dependence on cyberspace has brought new risks, risks that key data and systems on which we now rely can be compromised or damaged, in ways that are hard to detect or defend against [1].

Cyber technology can be used to attack the machinery of state, financial institutions, the national energy and transport infrastructure, and public morale [2]. While some actions may appear aggressive and warlike, they may not necessarily be intended as acts of war. The cyber activities of terrorists, spies and organised criminals can be harmful but they do not necessarily constitute acts of cyber warfare. Operating behind false IP addresses and the use of foreign servers allows cyber activists almost complete anonymity and a relative impunity. Cyber technology gives a disproportionate power to small and otherwise relatively insignificant actors and furthermore it allows mixing of military and civilian actors. This operation without boundaries is blurred between physical and the virtual and power can be exerted by states or non-state actors, or even by proxy.

Cyberspace is an apolitical space and might be a security challenge for governments, commercial enterprises and for private individuals as well. Even an international organisation may be a victim of threats in cyberspace, because all branches in our life rely heavily on digital communication and information transfer infrastructure. These challenges are often called cyber security. In addition, media and politicians often discuss cyber warfare in terms of alarming anecdotes which often seem closer to the world of science fiction than public policy. A Chatham House Report used the term 'cyber war*fare*' in order to focus discussion on activities which are 'warlike' but which may or may not be 'war' *per se*. 'Warfare' is a more open-ended term, more useful in exploring an environment that is not only virtual but also largely uncharted. The report identifies the essential characteristics of cyber warfare as a strategic phenomenon by describing the actions of cyber attackers and the reactions of defending governments and by analysing the 'ends, ways and means' of cyber warfare. As a result it proposes the following definition:

Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target [3].

The Cyber Warfare definition says nothing about the distinction between the different levels. A Cyber attack could occur on many different levels. The US Commission on Critical Infrastructure

Protection mentioned five different levels:

- A cyber-attack on the specific database of an owner/operator;
- A cyber-attack for the purpose of gaining access to a network;
- A cyber-attack for the purpose of espionage;

• A cyber-attack for the purpose of shutting down service;

• A cyber-attack for the purpose of introducing harmful instructions [4].

The basic cyber-attack tools are common between a nation-state led cyber-attack and

recreational hacker. Therefore, every cyber-attack has to be judged with a proportional answer. In order to understand whether a hostile action in cyberspace is warlike, it is necessary not just to observe the event but also to understand the actor's intent. The three most probable reasons for cyber-attacks are:

Firstly, fear factor: the most common denominator of the majority of terrorist attacks is a terrorist's wish to create fear in individuals, groups, or societies. Secondly, spectacular factor: spectacular attacks should create direct losses and result in a lot of negative publicity and finally the vulnerability factor: some of the most effective ways to demonstrate an organisation's vulnerability is to cause a denial of service to the commercial sever or the defacement of an organisation on their web page [5].

Cyber terrorism is an attractive option for modern terrorists, who value its anonymity, its potential to inflict massive damage, its psychological impact, and its media appeal. Before discussing threats from cyber terrorism, it would however be helpful to define this threat. Andrew M. Colarik and Lech J. Janczewski define cyber terrorism in their book as follow: Cyber terrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data result in violence against non-combatant targets [6].

Gabriel Weimann described other reasons in his article for cyber terrorism angst. It is the combination of psychological, political and economic forces who promote the fear of cyber terrorism. First, the psychological impact might be even greater than the effect of a conventional bomb because of the lack of understanding of cyber terrorism. Second, the promotion of fear with the impact of mass media headlines and cyber terrorism such as the following: 'Cyber-Attacks by Al Qaeda Feared, Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say.' published in the Washington Post in June 2003. Mass media do not often distinguish between adventure hackers and cyber terrorists. The third factor is the big business earning money from the fear of other people. Cyber terrorism merges two spheres together: terrorism and technology. Security consultants are highly motivated to increase the belief that every single network in a company is relevant for the national security. Cyber terrorism is therefore a strong expression to underline this belief and to increase the IT security spending [7]. This explanation does not distinguish between cyber terrorism and cyber crime. Not every act against somebody to gain money is a cyber terroristic act. Therefore one needs clarity about terrorism and activities concerning cyber.

Terrorism is defined as follows: Violence or the threat of violence used and directed in pursuit of, or in service of, a political aim [8]. Dorothy Denning a professor of computer science, tried to be more precise about the definition of cyber terrorism. She used his definition in numerous articles, and in her testimony on the subject before the congressional House Armed Services Committee: Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks

against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not [9]. The lack of a clear and coherent definition of cyber terrorism is obvious. Mass media and journalists are looking more for sensationalism than to define a new term related to terrorism and computer networks. Currently it is very common to create new words simply by placing the words 'cyber', 'computer' or 'information' before another word. This tendency is neither helpful nor useful to cope with a new challenge or threat in a more connected world.

Decisions makers need a common framework to handle this complex topic. International operational definitions of cyber threats like cyber vandalism, cyber crime, cyber espionage, cyber sabotage, cyber terrorism and cyber warfare might be the first step for cooperation on several levels.

Conclusion. The importance of cyber space as an environment to conduct various operations against states or non-state actors is increasing. Cyber terrorists may use the Internet as a source for information sharing and recruitment. "Cyber war" tend to be a catchword for politicians and especially for media. The lack of a coherent definition of cyber terrorism is still there. States were not able to define different levels of cyber activities. Although there are existing definitions for different activities, it will take a long time for a global common understanding of this relatively new threat from cyberspace.

As a result, cyber terrorism is one level in several cyber activities and is generally an attack with a high impact on the society.

References

1. The Rt Hon Francis Maude MP, Minister for the Cabinet Office and Paymaster General, "The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world", November 2011.

2. A.H Cordesman and J.G Cordesman, *Cyber threats, information warfare and critical infrastructure protection: defending the US homeland* (W.: Praeger Publishers, 2002), 87.

3. Paul Cornish "On Cyber Warfare", Chatham House Report, November 2010: vii

4. A.H Cordesman and J.G Cordesman, *Cyber threats* (W.: Praeger Publishers, 2002),

5 . Lech J. Janczewski and Andrew M. Colarik, Cyber Warfare and Cyber Terrorism (New York: Hersey, 2008), xv.

6. *Lech J. Janczewski and Andrew M. Colarik, Cyber Warfare and Cyber Terrorism (New York: Hersey,* 2008), xiii.

7. Gabriel Weimann, "Cyber terrorism: the sum of all fears?", Studies in Conflict & Terrorism, Vol. 28, No. 2, March-April 2005, pp. 131 - 132.

8. B. Hoffman, Inside Terrorism (New York: Columbia University Press, 1998).

9. Gabriel Weimann, "Cyber terrorism", p. 135.

CAUSES AND CONSEQUENCES OF THE ISOLATION OF ARMENIA AND A WAYOUT FROM THE SITUATION

Mammadzada V.M., Imamverdiyev E.R., Hasanov J.M.
Military Academy of the Armed Forces of the Republic of Azerbaijan, Baku

Historically, the policy of isolation has been a mean of influence and power used by states to limit trade and economic activities across borders in order to achieve certain political results. Although it has been argued that isolation policy is an effective political tool, the number of isolation cases is growing and this mechanism is becoming increasingly popular. Today, the isolationist policies of Ukraine against Crimea, Israel against Gaza, the United States against Cuba and North Korea, the Gulf countries against Qatar, Georgia against Abkhazia and South Ossetia, Azerbaijan and Turkey against Armenia are ongoing processes.

After Armenia's claim to Azerbaijan's Karabakh region in 1988, official Baku froze transit links with Yerevan. In doing so, Azerbaijan sought to prevent separate Armenian support for the Karabakh region. The policy of isolation (blockade) gradually applied by Azerbaijan to Armenia since 1988 was officially announced on September 4, 1989 [1]. The local clashes between the parties turned into large-scale military operations with the independence of Azerbaijan and Armenia in 1991. In 1991-1994, during the war, Armenia pursued a policy of ethnic cleansing by occupying 20% territory of Azerbaijan. The Armenian occupation factor and the humanitarian crisis it has caused (IDPs and refugees) have become a strong unifying factor for Azerbaijanis, as well as causing official Baku to take a tough stance against Yerevan. The war radically changed the attitude of Azerbaijanis to the Armenian people. At the official level and in public opinion in Azerbaijan, the Armenian state became an enemy. This ideology, forming a fundamental element of the military doctrine, was sought by international organizations and all states to condemn and isolate the aggressor. Seeing that international law did not work and no punitive measures were applied against the occupier, Azerbaijan formed a policy of isolation against Armenia in the "UN +" format on the basis of 4 UN Security Council resolutions (822, 853, 874 and 884). Turkey has joined the process against Yerevan since 1993, increasing geopolitical pressure on Yerevan, first by closing its land border and then its airspace. Armenia's aggressive policy led to the strengthening of military relations between Azerbaijan and Turkey and the establishment of a common regional strategy [2]. Turkey refused to normalize relations with Armenia until the liberation of the occupied territories of Azerbaijan [3], forcing Yerevan to comply with international obligations and norms. At the same time, besides Turkey, Pakistan and Saudi Arabia also condemned Armenia's aggressive policy and announced that they would not establish diplomatic relations with it. Azerbaijan and Turkey see their isolationist policy against Armenia as a mechanism for "forcing and punishing the aggressor" as a mean of influence that does not contradict international humanitarian law and is legitimate. Azerbaijan's isolation policy against Armenia consists of two important components:

1. The implementation of regional projects bypassing Armenia (Baku-Tbilisi-Ceyhan oil pipeline, Baku-Tbilisi-Erzurum gas pipeline, Trans-Anatolian gas pipeline, Trans-Adriatic gas pipeline, Baku-Supsa oil pipeline, Baku –Tbilisi – Kars railway, etc.).

2. Establishment of cooperation formats against Armenia (for example, Azerbaijan-Georgia-Turkey, Azerbaijan-Iran-Turkey, Iran-Azerbaijan-Russia, Georgia-Ukraine-Azerbaijan-Moldova, etc.).

While Azerbaijan is realizing its transit potential in the region, its main goal is to reduce the economic feasibility of new alternative projects, being a donor country that provides loans to countries participating in these projects (the Baku-Tbilisi-Kars railway to Georgia and the Qazvin-Rasht-Astara railway to Iran, for example).

It should be noted that the closure of the Azerbaijani and Turkish borders for Armenia is not the only source of this country's economic problems. Having open borders with only Georgia and Iran not only limit Armenia's integration into the world economy, but also increase security risks. Today, about 70% of Armenian cargo is transported through Georgia, and the rest through Iran. Moreover, the closure of the Moscow-Sukhumi-Tbilisi-Yerevan railway as a result of the Georgia-Abkhazia conflict (1992) and the Georgia-South Ossetia conflict (2008) deepened the Armenian blockade.

Due to Armenia's maximalist policy (claims) based on the ethno-psychology of the Armenian people (uncompromising), the isolation policy did not promote peace between the parties and did not resolve the conflict, but the 30-year isolated policy of Azerbaijan and Turkey against Armenia's occupation policy paid off. Through its mega-projects, Azerbaijan has transformed the logistics system in the region to its advantage, increased its transit potential and isolated Armenia from all projects, creating a crisis in the socio-economic, socio-political, demographic and other spheres and made it a cornered country. Just as the United States and its coalition forces launched a symbolic war against Baghdad (2003) and Belgrade (1999) after long-term sanctions against Iraq and Yugoslavia, after pursuing a long-term policy of isolation against Armenia, Azerbaijan's military intervention in the Karabakh conflict, in which the irreconcilable interests of the power centers clashed, was symbolic, and in a short time period (44 days) the occupation and aggression were ended and Yerevan was forced to sign a capitulation act (November 10, 2020). As a result of its victory in the Second Karabakh War, Azerbaijan changed the balance of power in the region and formed new geopolitical realities. According to Article 9 of the Declaration of the Tripartite Agreement signed between the parties on November 10, 2020, the Zangazur Corridor will be implemented, in which case the mutual isolation policy in the region will end and the integration process of the region will begin. In this context, the only way out of the deepening multilateral crisis in Armenia against the background of isolation is to recognize the territorial integrity of Azerbaijan, sign a peace agreement with it and renounce territorial claims to neighboring countries.

References

1. Caucasus Edition. Journal of Conflict Transformation.18 Jul 2016. https://caucasusedition.net/review-of-isolation-policies-within-and-around-the-south-caucasus/

2. Azərbaycan Respublikasının Hərbi doktrinası. Bakı: "Hüquq ədəbiyyatı" nəşriyyatı, 2010. 36 səh. https://ebooks.az/view/hnUPcmw0.pdf

3. Svante E. Cornell. Turkey and the Conflict in Nagorno Karabakh: A Delicate Balance. Middle Eastern Studies. Published By: Taylor & Francis, Ltd. (Jan. 1998). Vol. 34, № 1. pp. 51-72 (22 pages).

ПРОБЛЕМИ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЇ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

Рєзнік Я.В., Малінін О.П.
Харківський національний університет радіоелектроніки, Харків, Україна

Одним із найперспективніших методів біометричної безконтактної ідентифікації людини є технологія розпізнавання обличчя.

Технологія розпізнавання обличчя є потужним інструментом для боротьби зі злочинністю та шахрайством. Система розпізнавання обличчя використовує біометрію для отримання інформації про риси обличчя з фотографії або відео. Вона звіряє інформацію з базою даних відомих облич, шукаючи відповідність. Розпізнавання обличчя може допомогти встановити особу людини, але це також викликає проблеми з конфіденційністю [1].

Метою доповіді є дослідження ризиків використання технології розпізнавання обличчя стосовно конфіденційності та можливі шляхи їх усунення. Для цього було розглянуто випадки її несанкціонованого використання та законодавчих заборон [2], проаналізовано основні аргументи критиків та запропоновано шляхи подолання існуючих проблем.

Ще в 2011 році дослідники з Університету Карнегі-Меллона показали, що розпізнавання обличчя може збільшити ризики конфіденційності. У першому тесті, який вони провели, їм вдалося ідентифікувати людей на веб-сайті знайомств, де учасники не використовували свої справжні імена. У другому експерименті вони виявили особистості студентів, які йшли по кампусу, зв'язавши зображення їхніх облич із зображеннями їхніх профілів у Facebook. Фотографії облич студентів також зрештою змусили дослідників вгадати їхні особисті інтереси та, в деяких випадках, їхні номери соціального страхування [3].

Розпізнавання обличчя надає великі переваги у багатьох сферах людської життєдіяльності. Це являє собою великий прогрес технології штучного інтелекту, відкриваючи нові напрямки розвитку науково-технічного, економічного та громадського життя.

Список літератури

1. Joel Ericsen. Responsible AI: Facial Recognition and Scientific Responsibility [Електронний ресурс] // AAAS. – 2019. – Режим доступу до ресурсу: https://www.aaas.org/events/responsible-ai-facial-recognition-and-scientific-responsibility.

2. Cities Where Police Are Banned From Using Facial Recognition Tech [Електронний ресурс] // InnotechToday – Режим доступу до ресурсу: https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/.

3. Techniques and Challenges of Face Recognition: A Critical Review [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S1877050918321252.

ДОСЛІДЖЕННЯ МОДЕЛЕЙ УПРАВЛІННЯ ТРАНСПОРТНОЮ МЕРЕЖЕЮ IP/MPLS

Мазепа К.М., Іванісенко І.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Останнє десятиліття в галузі активно обговорювалася проблематика уніфікованого управління транспортними мережами. Було прийнято рішення двигатися еволюційно, розвиваючи досить успішну мультипротокольну комутацію за мітками - MPLS. А ось MPLS-TP – новий спосіб побудови опорних систем, у яких послуги передачі даних виступають у ролі клієнта по відношенню до пакетного транспорту, при чому MPLS-TP інваріантна до технології клієнта. Причиною появи MPLS-TP було стремління адаптувати MPLS для роботи на рівні існуючих операторських магістральних мереж. При реалізації операторського класу Ethernet буде відбуватися інкапсуляція Ethernet-трафіку в пакетах MPLS-TP, якщо він надає традиційні послуги цифрової телефонії, створюються вже впроваджувані в цьому голові псевдо лінії PWE3, куди й поміщається TDM-трафік [1].

Метою доповіді є дослідження та аналіз методів управління транспортними наборами п'ятого покоління в відповідності з запропонованою концепцією, обґрунтована актуальність додаткових засобів управління для трафіку реального часу, критичних к задержкам, сформульовані вимоги щодо якості обслуговування для механізмів і технологій IP/MPLS. Показано, що є два підходи до управління інформаційними комунікаціями – централізоване фіксоване управління та децентралізована динамічна самоорганізація. [2]

У рамках дослідження управління транспортними vмережами обґрунтована актуальність додаткових засобів управління трафіком реального часу, критичних затримань, сформульовані вимоги щодо якості обслуговування для механізмів і технологій IP/MPLS.

Показано, що проектування транспортних мереж NGN для пакетної передачі мультимедійної інформації реального часу вимагають механізми тунелювання MPLS, управління якими здійснюється на базі математичних моделей розрахунку ймовірно-часових характеристик (ЙЧХ). Для цього розроблена модифікована математична модель механізму тунелювання у транспортній мережі, досліджені ефекти фрагментації та зцеплення в пакетах, що передаються в тунельною мережею.

Список літератури

1. Goldshtein A.B. Two approaches for telecommunication networks management // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 3. С. 57-63.

2. 5G Mobile and Wireless Communications Technology. — Cambridge University Press, June 2016. — ISBN 9781107130098.

СЕКЦІЯ 6

СУЧАСНІ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ СИСТЕМИ

Керівник секції: д.т.н. проф. В. Б. Кононов, ХНУПС, Харків
Секретар секції: к.т.н. доц. Ю. І. Рафальський, ХНУПС, Харків

UNLIMITED AIRCRAFT WITH RENEWABLE ENERGY SOURCE

Tuz V.V., Vivsyaniy O.O.
Cherkasy State Technological University

Modern technologies do not stand still and are constantly evolving. Part of such technology is an unmanned aerial vehicle. Yesterday, unmanned aerial vehicles were fantastic, and today they are used in almost all spheres of human activity. To date, they have demonstrated their versatility and rational use[1-3].

In recent years, unmanned aerial vehicles (UAVs) and in particular multicopters (MC) have been the subject of research by many scientific communities, military and civilian companies. Due to their versatility and the ability to program algorithms for their operation, a wide range of tasks can be performed using a multicopter, for example: object search, building survey, observation, etc[2]

The main problem of unmanned aerial vehicles is the range, so the main purpose of the work is to increase the length of stay of UAVs in the air through the use of renewable energy sources, namely - solar panels.

The drone has a battery capacity of 2.7 A. The UAV has a range of 2000 m, using the battery, the range will increase 4 times, and taking into account the additional weight of the battery, the actual range will be about 6000 m

After calculations, it became clear that the installation of a solar battery will extend the flight, but the weather also directly affects the range, and other factors that affect the energy efficiency of unmanned aerial vehicles, the solar battery can feed other energy consumers on the drone

Reference

1. Нго К.Т., Соленая О.Я., Ронжин А.Л. Анализ подвижных роботизированных платформ для обслуживания аккумуляторов беспилотных летательных аппаратов // Труды МАИ. Выпуск № 95/

2. Губанова А.Р., Теслева А.П. Анализ возможности использования солнечных батарей в Кузбассе // Современное состояние и проблемы естественных наук. Секц. 10. С. 556. http://earchive.tpu.ru/bitstream/11683/17790/1/conference_tpu-2015-C57-242.pdf

3. Галимуллина Э.Э., Абзалилова Ю.Р. Системы повышения эффективности солнечных батарей // Альманах современной науки и образования. Тамбов: Грамота, 2016. № 12. С. 31-35. ISSN 1993-5552. http://scjournal.ru/articles/issn_1993-5552_2016_12_08.pdf

ВИКОРИСТАННЯ МЕТОДІВ ПРОГНОЗУВАННЯ ПРИ РОЗВ'ЯЗАННІ ЗАВДАНЬ УПРАВЛІННЯ МЕТРОЛОГІЧНИМ ЗАБЕЗПЕЧЕННЯМ СУЧАСНИХ ЗРАЗКІВ ТЕХНІКИ

Кононов В.Б., Рафальський Ю.І., Лук'янчиков А.А.
Харківський національний університет Повітряних Сил ім. Івана Кожедуба

Для забезпечення своєчасного метрологічного обслуговування сучасних зразків техніки бажано вдосконалити управління силами й засобами метрологічного забезпечення та здійснювати прогнозування стану засобів вимірювальної техніки. Це особливо важливо в сучасних умовах розвитку України, які характеризуються появою новітніх зразків техніки, суттєвим розвитком інформаційних технологій, що вимагає і суттєвої якісної заміни обладнання. Таким чином, наукове обґрунтування прогнозування потреби з метрологічного обслуговування засобів вимірювальної техніки сучасних зразків техніки та визначення необхідної кількості обслуги шляхом розробки відповідних математичних моделей є актуальним науково-технічним завданням.

Методи прогнозування в загалом базуються на двох підходах: евристичному та математичному. Евристичні моделі формуються експертами на основі цільової установки, представленої інформації, досвіду, інтуїції та знань експерта (методи типу інтерв'ю, генерації ідей; метод ранжування; метод вагових коефіцієнтів; методи послідовних або попарних порівнянь; метод "Дельфи" та ін.). Недоліком методів експертних оцінок являються суб'єктивність оцінки та залежність їх застосування від наявності експертів, знайомих з ситуацією, яка прогнозується.

Для підвищення точності та достовірності прогнозу доцільно використання комбінованих методів, при цьому бажано використання декількох варіантів прогнозу, які розраховані на основі різних підходів або альтернативних джерел інформації. При прогнозуванні потреби для метрологічного обслуговування засобів вимірювальної техніки сучасних зразків техніки будемо виходити з того, що відома необхідна статистична інформація як за кількість замовлень для метрологічного обслуговування сучасних зразків техніки різних типів у різні проміжки часу, так і за значеннями факторів, які впливають на цю кількість замовлень.

Природно вважати, що у якості цих факторів виступають кількості зразків сучасних зразків техніки, які оснащені відповідними типами засобів вимірювальної техніки. В цьому випадку будемо використовувати статистичні методи прогнозування, які засновані на моделях множинного регресійного аналізу.

Список літератури

1. Carrasco Pena J. A. Supplier selection as a change process: a grounded theory approach: A thesis submitted for the degree of doctor of philosophy. / J. A.Carrasco Pena. – A Coruña : The University of A Coruña, 2008. – 376 p.

ШЛЯХИ ВИБОРУ ЗАСОБІВ ВИМІРЮВАЛЬНОЇ ТЕХНІКИ ПРИ ВИЗНАЧЕННІ МЕТОДИКИ ПОВІРКИ ТЕРМОПЕРЕТВОРЮВАЧІВ

Кононова О.А., Бабич О.О., Зарічняк Є.М.
Харківський національний університет Повітряних Сил ім. Івана Кожедуба

Науковий і технічний рівень вимірювання визначаються рівнем розвитку засобів вимірювальної техніки.

Електричні та радіо вимірювання, базуються на вимірюваннях електромагнітних величин. При цьому, основними напрямами якісної сторони розвитку засобів вимірювальної техніки в радіотехніці є:

підвищення точності вимірювання;

автоматизація процесів вимірювання;

підвищення швидкодії і надійності вимірювальних приладів;

зменшення споживаної потужності живлення і габаритів всіх засобів вимірювальної техніки.

Вимірювання струму і напруги є основними при дослідженні різних пристроїв і при контролі їх роботи.

Проте в радіотехніці переважаюче значення має вимірювання напруги, а до вимірювання струмів в даються в окремих випадках. Це обумовлено тим, що для опису роботи різних радіотехнічних пристроїв використовують переважно напругу, а не струми, тому експериментально доводитися вимірювати цю напругу. Вимірювання напруги в електронних схемах відрізняються від подібних вимірювань в електричних ланцюгах, що пояснюється специфічними особливостями електричних сигналів, використовуваних в електроніці і радіотехніці:

виключно широкою областю частот - від постійних до СВЧ (2ггц);

великий діапазон вимірюваних значень напруги - від доль мікровольта до десятків кіловольт;

малою потужністю джерела напруги.

Напруга та струм є основними енергетичними параметрами сучасних електронних систем і їх значення необхідно завжди точно знати та підтримувати в певних межах при експлуатації складних технічних об'єктів (СТО). При цьому, одними із розповсюджених засобів вимірювальної техніки (ЗВТ) є термоперетворювачі струму та напруги.

В доповіді розглянуті шляхи вибору засобів вимірювальної техніки при визначенні методики повірки термоперетворювачів.

Список літератури

1. Кононов В.Б. Instrumentation and general principles of sensors Part 1. Навчальний посібник. (англійською мовою) - Харків: ХНУ ПС, 2018. – С. 62.

МЕТОДИКА ОБҐРУНТУВАННЯ МЕТРОЛОГІЧНИХ ХАРАКТЕРИСТИК ЗАСОБІВ ВИМІРЮВАЛЬНОЇ ТЕХНІКИ ПРИ ПОТОЧНОМУ РЕМОНТІ ЗАСОБІВ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ

Сакович Л.М., Гиренко І.М., Мирошниченко Ю.В.
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київський політехнічний інститут ім. Ігора Сікорського"

В доповіді запропонована методика визначення метрологічних характеристик засобів вимірювальної техніки діагностичних параметрів засобів спеціального зв'язку згідно з вимогами до ремонтопридатності.

Методика призначена для обґрунтованого завдання метрологічних характеристик засобів вимірювальної техніки, використовуваних при поточному ремонті засобів спеціального зв'язку агрегатним методом, з метою мінімізації вартості одиничного ремонту, обладнання апаратних зв'язку й ремонтному органі – пункті технічного обслуговування і ремонту у місцях постійного знаходження й автоматизованого телефонного зв'язку в польових умовах – при певних обмеженнях що задається в нормативно – технічної документації. Запропонована методика відрізняється від відомих розширенням реалізованих типів умовних алгоритмів діагностування і комплексним використанням всіх видів надлишковості засобів вимірювальної техніки при розробці діагностичного забезпечення, що дозволяє обґрунтувати вимоги до засобів вимірювальної техніки й мінімізувати їх вартість без втрати якості поточного ремонту.

Методика є основою аналітичних і алгоритмічних засобів розробки метрологічного й діагностичного забезпечення поточного ремонту засобів спеціального зв'язку в умовах ремонтного органу, а також обслугою безпосередньо в апаратних зв'язку з використанням штатних засобів вимірювальної техніки засобів вимірювальної техніки. Її доцільно застосовувати в проектних організаціях при розробці метрологічного й діагностичного забезпечення перспективних зразків засобів спеціального зв'язку, а також у процесі модернізації ремонтного органу для зниження вартості одиничного ремонту при задоволенні вимог до показників ремонтопридатності. Позитивний результат досягається науково обґрунтованим вибором мінімально необхідного значення ймовірності правильної оцінки результату вимірювання діагностичних параметрів за рахунок реалізації сучасних досягнень теорії дискретного пошуку й вимірювань, а також використанням особливостей засобів спеціального зв'язку, обумовлених їх надлишковістю, які не враховуються у відомих методиках.

Список літератури

1. Сакович Л.М. Методика визначення вимог щодо метрологічних характеристик засобів вимірювання діагностичних параметрів техніки зв'язку для забезпечення її ремонтнопридатності / Л.М. Сакович, Ю.С. Василюк // Зв'язок. – № 3. – 2015. – С. 47–53.

THE ROLE OF TECHNICAL MEANS IN THE SECOND KARABAKH WAR

Hashimov E.G., Karimov Y.Sh.
Military Academy of the Armed Forces of the Republic of Azerbaijan

Though one year passed after the end of the second Karabakh War the study of the results of the war are still actual. Because the operations which were carried out in the complex terrain together with different types of troops are analyzed and new information comes out. Carring out battles in the plain area from the front line and then the principle of from bottom to up warfare in the mountainous and wood lands solved many issues like gaining air previllage from the first days of the war and maintaining it until the end. The use of modern high precision weapons with great destructive power, the ability of the highly trained crew decided the fate of the war in a short period of time. The long running negotation process for resolving the conflict has not led to the certain results, but made the military solution of the conflict innevitable. Both sides paid special attention to the armament of the Army, allocated large sums of money, as if it was race of armament. Before the war in the ranking of the world armies in 2019, the US publication "Global Fire Power" ranked Azerbaijan 52nd, and Armenia 96th among 137 countries. [2] Azerbaijan which is at least 3-4 times stronger than Armenia in terms of economic opportunities and human resources, was approached by double standarts. In fact, by not having such a big difference in the rankings of the armies the position was taken to force Azerbaijan to reconcile with the current situation saying that there is no military solution to the conflict. However the second Karabakh War which lasted 44 days proved this approach to be false. The basis of Azerbaijan's superiority was provided by the availability of modern weapons and technical means.

AN 2 aircaraft were converted into UAVs and special air operation was carried out as fake air target. The location of enemy's anti-aircraft missiles which fired at the air target was determined and destroyed. From the first days of the war air superiority was ensured. The long-term defence and camera survelliance system prepared by the enemy was destroyed. The reserves in the depth of the defence at deployment point and roads were destroyed before being used in advance. All this was possible by the use of Turkish made "Bayrakdar TB 2" and Israili made strike type "Harop" and anti-tank SPIKEs, which were used for the first time during 44 day war.[1] The use of missiles and artillery interaction with other fire fighting vehicles accelareted the collapse of the enemy. During the war the enemy made extensive use of various Russian made EW means, including "Repelent", "Krasukha", and "Manushak". With the capabilities of modern means in the armament of the Azerbaijani Army it was not so difficult to locate and neutralize the enemy's EW means. The role of modern weapons and technical means in achieving victory was undeniable. The second Karbakh War demonstrated the model of 21st century modern wars. Simultainously it showed that the tanks were practically useless on the battlefield. After the second Karabakh War many countries were forced to reconsider the military doctrines, the future armament of the army and the development of the military industrial complex. The principle of the modern warfare requires not the superiority of quantity and quality but intelligence. The second Karabakh War was organized and carried out on this principle.

References

1. Karimov, Y. Collection of information on missile and artillery weapons : Y. Karimov – Bakı, Military Publishing House,- 2019. – p. 112 .
2. https:// bizim.media.com
3. Kərimov, Y Ş. Raket və artilleriya silahları haqqında məlumatlar toplusu: Y. Kərimov – Bakı, Hərbi nəşriyyat,- 2019. -112 s.

METHODS OF EFFECTIVE DETECTION OF UNMANNED AERIAL VEHICLES

Hashimov E.G, Maharramov R.R.
Military Academy of the Armed Forces of the Republic of Azerbaijan

An analysis of the Patriotic War in 2020, as well as recent local wars, has shown that in order to combat UAVs, it must first be detected as soon as possible. During the war, due to the small number of Armenian stations against modern Azerbaijani air defense systems, the obsolescence of these stations, as well as the weak combat skills of the staff, Azerbaijan was unable to detect most of the air defense systems in a timely manner. In the first days of the war, as a result of Azerbaijan's correct combat tactics, the positions of the Armenian air defense units were quickly discovered and destroyed. As a result, the air advantage in the Patriotic War passed completely to the side of Azerbaijan. As a result of the rapid detection and targeting of enemy units on the front line and in-depth reserves, they were quickly neutralized by armed drones, artillery units, aviation units and other units. At the same time, the Armenian Armed Forces have not been able to actively use obsolete unmanned aerial vehicles. Thus, enemy UAVs were immediately detected by Azerbaijani detection stations, destroyed immediately by air defense units, as well as other units. An important aspect of effective control of anti-aircraft missiles is their early detection by air defense units. Early detection of UAVs helps missile defense units save time and make the right decisions against it.

There are many different methods for detecting UAVs. Each method differs in advantages, disadvantages, conditions of use, accuracy and other parameters. The main methods of detecting UAVs are: **1. Acoustic detection of UAVs.** This method detects the sound of UAV engines and blades through modern sound detection sensors and compares them with pre-recorded sounds. Currently, the world produces very sensitive sensors that can detect UAVs remotely [1]. **2. Electro-optical detection of UAVs.** It is possible to detect UAVs by electro-optical methods [2]. When an unmanned aerial vehicle approaches, a special program adjusts them for small air targets and records a video of the UAVs approaching the object [3]. **3. Radar detection of UAVs.** Radar stations (RLS) are an active means of monitoring airspace. The role of radar stations in controlling the airspace of Azerbaijan during the Patriotic War was very large. Thus, the radar deservedly transferred its tasks to anti-aircraft missile systems (ZRK) or other types of troops for the detection, identification and destruction of anti-aircraft missiles that entered our airspace. The airspace control of the radar is very reliable,

but the effective detection of UAVs by radar with a small effective reflection area remains unresolved [4]. **4. Detection of UAVs by radio frequencies.** Nearby UAVs are detected by stations using radio frequency signals. Although it is possible to detect, locate and even analyze UAVs in this way, it is not possible to detect UAVs flying autonomously. **5. Detection of UAVs by infrared rays.** The method of detection of UAVs by infrared radiation allows to detect the heat emitted by UAV engines. **6. The multi-sensor detection method of UAV** is the most effective method of detecting UAVs using different methods at the same time and allows their high-precision detection [2].

Despite the fact that various types of detection methods are currently used in the world to detect UAVs, a complete solution to the problem of their detection is one of the main tasks of modern military science.

References

1. Finn A & Franklin S (2011). Acoustic sense & avoid for UAV's. In proceedings of the 7th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Adelaide, Australia, 6–9 December.

2. Yusuf Mutlu GENÇ, Erdem ERCİYES. İnsansız Hava Araçları (İHA) Tehditleri ve Güvenlik Yönetimi. Türkiye İnsansız Hava Araçları Dergisi– 2020; 2(2); 36-42.

3. Абидова Нозима (ГУП «UNICON.UZ»). Анализ способов противодействия агрессивным дронам. 6 səh. https://ictnews.uz/wp-content/uploads/2020/01/2.pdf.

4. Макаренко С. И., Иванов М. С. Сетецентрическая война - принципы, технологии, примеры и перспективы. Моногр. - СПб.: Наукоемкие технологии, 2018. - 898 с.

СПРОМОЖНОСТІ ОГЛЯДОВИХ РАДІОЛОКАТОРІВ ЩОДО ЗАБЕЗПЕЧЕННЯ РАДІОЛОКАЦІЙНОГО СПОСТЕРЕЖЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Кузнєцов О.Л., Карлов В. Д., Карлов А.Д.
Харківський національний університет Повітряних Сил імені І. Кожедуба

Можливості оглядових радіолокаторів щодо виявлення безпілотних літальних апаратів (БПЛА) на малих та гранично малих висотах є обмеженими. Ідентифікація класу БПЛА як правило здійснюється за наступними ознаками: дальність виявлення; висота польоту; швидкість польоту; характер траєкторії польоту [1]

У доповіді визначено, що використання оглядових радіолокаторів для виявлення тактичних міні-БПЛА є недоцільним і невиправданим. Недоцільним – через надзвичайно низькі можливості з виявлення означеного типу цілей, а невиправданим – через невідповідність масштабів задач, для вирішення яких первісно проектувались і розроблялися такі радіолокатори. Вирішення завдань з виявлення міні-БПЛА частково здатні виконувати лише рухомі радіовисотоміри. При цьому суміщення завдань з виявлення міні-БПЛА з основними завданнями, для вирішення яких призначені радіовисотоміри, є неможливим [2]. Враховуючи це, а також їхні характеристики мобільності, склад апаратури та її вартість,

використання радіовисотомірів для забезпечення радіолокаційного спостереження БПЛА тактичного призначення є також недоцільним. Радіолокаційне спостереження БПЛА оперативного призначення на висотах понад 5000 метрів радіолокаційними засобами оглядового типу є цілком можливим та може бути реалізовано на дальностях від десятків кілометрів до понад 100 кілометрів.

Список літератури

1. Кутовий О. П. Тенденції розвитку безпілотних літальних апаратів / О. П. Кутовий // Наука і оборона. – 2000. - №4. – С. 39-47..

3. Олещук М. М. Параметри причорноморських тропосферних радіохвилеводних каналів виявлення БЛА / М. М. Олещук, О. В. Бєсова, С. Г. Леушин // Наука і техніка Повітряних Сил Збройних Сил України. – 2021. – Вип. № 1(45). – С. 129-135.

ПРОБЛЕМИ ВПРОВАДЖЕННЯ ЗАСОБІВ МАЛОЇ ТА МІКРОГЕНЕРАЦІЇ ГЕНЕРАЦІЇ В КОНТЕКСТІ ЗАПРОВАДЖЕННЯ ІНФОРМАЦІЙНОЇ КОНЦЕПЦІЇ SMART GRID В СИСТЕМАХ ЕЛЕКТРОПОСТАЧАННЯ

Ключка К.М., Бондаренко О. М.
Черкаський державний технологічний університет, Черкаси, Україна

В теперішній час, згідно з прагненням України щодо впровадження європейської концепції Smart Grid «інтелектуальні мережі» в поєднанні з тенденцією розосередження джерел генерації електричної енергії, впровадження засобів малої та мікрогенерації повинно бути поєднано з всебічним розвитком інформаційно-вимірювальних систем у складі систем електропостачання [1].

Метою доповіді є порівняльний аналіз та огляд результатів досліджень способів підвищення ефективності функціонування засобів малої енергетики та мікроенергетичних систем в поєднанні з сучасними інформаційно-вимірювальними системами. Основна увага, при виявленні кола проблем, була приділена питанню сумісності функціонування традиційних засобів релейного захисту в мережах середньої та високої напруг при підключенні до таких мереж малих та мікроелектростанцій.

При проведенні дослідження було виявлено, що при проектуванні сучасних систем електропостачання з розосередженою генерацією, релейний захист неодмінно має бути пристосований функціонувати у складі інформаційно-вимірювальної системи. Підставою цьому є широке впровадження мікропроцесорних комплектів керування до складу оперативних кіл сучасних схем релейних захистів [2]. Використання методів цифрової обробки результатів вимірювання струмів, напруг та інших електричних величин, разом з широкими можливостями гнучко опрацьовувати отриману інформацію (постійний моніторинг із записом та накопиченням інформаційних сигналів про аварійні режими, недопустимі перевантаження тощо) може бути безпосередньо використано в майбутніх контрольно-інформаційно-вимірювальних системах SmartGrid, що в підсумку має дати відчутне підвищення ефективності функціонування систем електропостачання в сучасних умовах.

Список літератури

1. European Smart Grids Technology Platform. Vision and Strategy for Europe's Electricity Networks of the Future. – Luxembourg: Office for Official Publications of the European Communities, 2006. – 40 p.
2. Релейний захист і автоматика: Навч. посібник / С. В. Панченко, В. С. Блиндюк, В. М. Баженов та ін.; за ред. В. М. Баженова. – Харків: УкрДУЗТ, 2021. – Ч. 2. – 276 с.

МЕТОД ВИСОКОТОЧНОЇ ДІАГНОСТИКИ РОБОЧИХ ПАРАМЕТРІВ АВТОМОБІЛЯ В ПРОЦЕСІ ЙОГО РУХУ

Туз В.В., Усіченко М.І.
Черкаський державний технологічний університет, Черкаси, Україна

На сьогоднішній день практично всі випущені двигуни внутрішнього згоряння обладнані електронною системою керування (ЕСКД). Автовиробники приділяють особливу увагу цій системі, так як домогтися високої потужності двигуна при одночасному зниженні витрат палива і виконанні жорстких екологічних вимог можливо тільки за допомогою дуже точного і своєчасного дозування палива і ефективного підпалювання паливно-повітряної суміші на всіх режимах роботи двигуна. [1-3].

Процес діагностування електронних систем керування двигуном(ЕСКД) є одним з найскладніших видів робіт при технічному обслуговуванні і поточному ремонті автомобіля, що вимагає від виконавця знань конструкції двигуна внутрішнього згорання, пристрої та роботи ЕСУД, вміння користуватися діагностичного обладнанням і технічною документацією, а також практичних навичок в ремонті і обслуговуванні автомобілів. Як показувала практика, системи самодіагностики автомобілів в теперішній час недосконалі, тому питання діагностування та прогнозування відмов ЕСУД актуальні і вимагають подальшого опрацювання та розвитку[1-2].

Метою доповіді є розробка методу високоточної діагностики робочих параметрів автомобіля в процесі його руху для зменшення трудомісткості діагностичних робіт. В доповіді розглядається метод високоточної діагностики автомобіля. Застосування розробленої методики діагностування елементів ЕСКД на станціях технічного обслуговування автомобілів дозволяє зменшити трудомісткість діагностичних робіт, скоротити час, витрачений на пошук несправності, і знизити витрати на підтримку автомобілів в технічно справному стані.

Список літератури

1. Баженов Ю.В., Каленов В.П. Диагностирование электронных систем управления двигателем // Фундаментальные исследования. – 2014. – № 8-1. – С. 18-23.
2. Кузнецов, А.С. Техническое обслуживание и диагностика двигателя внутреннего сгорания / А.С. Кузнецов. - М.: ИЦ Академия, 2011. - 80 с.
3. Павленко Е.А. Повышение эффективности эксплуатации автомобилей на основе создания инновационного диагностического комплекса: дис. ...канд. техн. наук: 05.22.10 / Павленко Евгений Александрович. - Липецк, 2010. - 207 с.

ДОСЛІДЖЕННЯ ТА РОЗРОБКА ЕЛЕКТРОМЕХАНІЧНОЇ СИСТЕМИ КЕРУВАННЯ РУХОМ ТРАКТОРА З ВИКОРИСТАННЯМ GPS

Туз В.В., Щербина М.О.
Черкаський державний технологічний університет, Черкаси, Україна

Найважливішим завданням сільськогосподарського виробництва є забезпечення подальшого зростання продуктивності праці при збереженні високої якості виконання сільськогосподарських робіт.

Одним з найбільш ефективних засобів підвищення продуктивності є впровадження систем точного землеробства, при використанні яких здійснюється диференційоване внесення доз добрив, норм висіву. Реалізація такого підходу стала можливою завдяки появі систем глобального позиціонування, розвитки бортової електроніки. [1-3].

Одним з найбільш важливих елементів системи точного землеробства є система підрулення, що дозволяють здійснювати управління рухом без участі водія. Останнім часом на ринку з'явилися вітчизняні системи, проте їх вартість вище зарубіжних аналогів.

Застосування імпортних систем неможливе у вітчизняних тракторах, крім цього, варто відзначити високу вартість імпортних систем для сільськогосподарських підприємств [1-2].

Таким чином, актуальність теми визначається необхідністю виробництва більш досконалих систем керування рухом трактора з використанням gps.

Метою доповіді є підвищення ефективності роботи трактору на основі застосування електромеханічної системи керування рухом трактора з використанням gps.

В доповіді наводяться математичні моделі керування трактором та його механіко-математична модель. Представлена система керування рухом трактора з використанням gps та досліджено програмне забезпечення і інтерфейс взаємодії з користувачем. Проведені дослідження підтвердили працездатність розробленої системи

Список літератури

1. Авдонина, І. А. Точне землеробство - стратегія ефективного розвитку сільського господарства / І. А. Авдонина // Науковий вісник Технологічного інституту - філії ФГБОУ ВПО Ульяновська ГСХА ім. П.А. Столипіна. - 2015. - №14. - С. 5-10.

2. Доросінскій, Л. Г. Основи і принципи побудови інерціальних навігаційних систем / Л.Г. Доросінскій, Л. А. Богданов // Сучасні проблеми науки та освіти. - 2014. - №5. - С. 34-39.

3. Методи супутникового і наземного позиціонування. Перспективи позиціонування. Перспективи розвитку технологій обробки сигналів / Д. Дардарі, Е. Фаллетті, М. Луїзі; під ред. Д. Дардарі. М.: Техносфера, 2012. - 528 с.

ДІАГНОСТИЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМ КОНТРОЛЮ

Павлик Г.В.
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

Зростання складності та високі темпи розвитку комп'ютерних систем, впровадження їх в усі сфери діяльності визначають актуальність проблеми підвищення їх відмовостійкості та живучості. Для скорочення часу визначення працездатності технічних об'єктів і пошуку місця відмови в них необхідно розробляти діагностичне забезпечення - комплекс взаємопов'язаних правил, методів, алгоритмів і засобів, необхідних для здійснення діагностування на всіх етапах життєвого циклу об'єкта [1, 2].

Метою доповіді є аналіз методів розробки діагностичного забезпечення автоматизованих систем контролю.

В доповіді розглянуто особливості задачі, що розглядається.

Показано, що розробка діагностичного забезпечення є складним завданням, тому що засоби контролю й діагностики повинні задовольняти цілому ряду найчастіше суперечливих вимог по швидкодії, апаратурним витратам, надійності функціонування й т.д.

Багато задач: пошук мінімальних тестів, вибір оптимального состава перевірок і ін. є логіко-комбінаторними задачами. Трудомісткість класичних алгоритмів і методів рішення цих завдань змушує шукати нові підходи й розробляти більше ефективні методи.

Для скорочення трудомісткості розробки діагностичного забезпечення, зменшення тривалості процесу, підвищення якості проектування, зменшення витрат на його розробку розроблені програмно-апаратні засоби [3,4], що дозволяють автоматизувати процес розробки діагностичного забезпечення, скоротити строки розробки і підвищити його якість за рахунок формування мінімальних тестових послідовностей та спрощення схеми контролю.

Список літератури

1. Peleska J. Industrial–Strength Model–Based Testing–State of the Art and Current Challenges / J. Peleska // EPTCS 111, 2013. – P. 3 – 28.

2. Knuppel T. Fault Diagnosis for Electrical Distribution Systems using Structural Analysis / T. Knuppel, M. Blanke, J. Stergaard // International Journal of Robust and Nonlinear Control, 2014. – V. 24. – P. 1446 – 1465.

3. Пат.112425, Україна, МПК G 06 F 11/30. Автоматизована система контролю/ Косенко В.В., Дергачов В.А., Павлик Г.В./ Заявка № U201607955; заявл. 18.07.2016: опубл. 12.12.2016, Бюл. № 23.

4. Комп'ютерна програма «COMBITEST» / Павлик Г.В., Доценко Н.В., Сіроклин В.П.: свід. про реєстр. автор. права на твір № № 108343.– Зареєстр. в Держав. службі інтелектуальної власності України 30.09.2021.

МАТЕМАТИЧНА МОДЕЛЬ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-ДІАГНОСТИЧНОЇ СИСТЕМИ КОНТРОЛЮ ТЕХНІЧНОГО СТАНУ ЗАСОБІВ ВОДНОГО ТРАНСПОРТУ

Гаценко Л.В.
Державний університет інфраструктури та технологій, Київ, Україна

Джерелами інформації про технічний стан засобів водного транспорту (ЗВТ) є результати вимірювання параметрів контролю, наприклад, напруги, струму, частоти, тобто, фізичних характеристик [1]. Таким чином, розробка моделі сучасної інформаційно-діагностичної системи (ІДС) представляє собою актуальну задачу раціонального вибору та об'єднання вимірювальних датчиків, засобів вимірювання та обробки вимірювальної інформації для прийняття рішення щодо технічного стану та подальшої експлуатації ЗВТ.

При створенні мобільної ІДС для контролю технічного стану різних типів ЗВТ пропонується використовувати однотипні вимірювальні датчики [2]. У цьому випадку суматорами вимірювальної інформації виступають засоби вимірювання, а датчиками – джерела інформації про параметри контролю та діагностування ЗВТ [3].

Метою доповіді є побудова математичної моделі раціонального вибору та об'єднання складових ІДС для контролю технічного стану ЗВТ.

У відомих математичних моделях раціонального вибору та об'єднання вимірювальних датчиків [1] – [3] не враховані можливості об'єднання раціональної номенклатури засобів вимірювання в окрему систему, не розглядається раціональне їх розміщення та взаємодія за допомогою каналу загального користування. У доповіді запропонована модель, яка передбачає розташування у просторі вимірювальних датчиків, блоку збору та обробки даних і шини передачі даних з метою виконання потрібних вимог до техніко-економічних показників ІДС для контролю технічного стану ЗВТ.

Список літератури

1. Herasimov S., Gridina V. Method justification nomenclature control parameters of radio systems and purpose of their permissible deviations. *Information processing systems*. 2018. Vol. 2 (153). Pp. 159–164. DOI: https://doi.org/10.30748/soi.2018.153.20.

2. Герасимов С. В. Модель оцінки похибки обробки інформації у навігаційних системах крилатих ракет в умовах невизначеності. *Наука і техніка Повітряних Сил Збройних Сил України*. 2019. № 2 (35). С. 151–157. DOI: https://doi.org/10.30748/nitps.2019.35.19.

3. Герасимов С. В., Шапран Ю. Є., Кірвас В. В. Розробка та дослідження методу розрахунку достовірності вимірювального контролю параметрів радіотехнічних систем морського транспорту. *Системи озброєння і військова техніка*. 2017. Вип. 4 (52). С. 5–10.

МОДЕЛЬ РОЗНЕСЕНОЇ РАДІОЛОКАЦІЙНОЇ СИСТЕМИ ВИЯВЛЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Герасимов С.В., Кириченко Д.Л.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба, Харків, Україна

У зв'язку з розширенням географії застосування та збільшенням кількості фірм-виробників намітилося лавиноподібне зростання чисельності використання безпілотних літальних апаратів (БпЛА) [1]. Зростає кількість проектів зі створення автоматизованих транспортних систем і комплексів доставки вантажів на базі БпЛА. Тому, за оцінкою експертів, необхідно вживати заходи для забезпечення безпеки при організації управління польотом БпЛА.

Очевидна недостатність такої системи контролю за польотами БпЛА, особливо поблизу аеропортів, місць масового скупчення громадян, об'єктів, що охороняються. Таким чином, виникла необхідність створення незалежної об'єктивної системи контролю за польотом БпЛА. Оскільки така система повинна бути працездатною в будь-яких погодних умовах і цілодобово, то створювати її потрібно на основі радіолокаційних датчиків [2, 3].

Метою доповіді є розробка моделі рознесеної радіолокаційної системи виявлення малопомітних БпЛА.

У доповіді обґрунтовано, що при моделюванні такої системи виникає завдання виявлення та вимірювання координат широкого класу повітряних цілей з малими величинами ЕПР і відносно низькими радіальними швидкостями польоту. При моделюванні пропонується використовувати теорію понадкороткоімпульсної радіолокації. Наведено основні перевагами даної теорії:

висока роздільна здатність за дальністю за рахунок малого імпульсного діапазону елемента розрізнення та мінімального рівня бічних пелюсток функції селекції за дальністю;

можливість побудови алгоритму селекції рухомих цілей без використання ефекту Доплера, а, отже, відсутність «сліпих швидкостей» у можливому діапазоні швидкостей польоту БпЛА.

Список літератури

1. Герасимов С. В. Модель оцінки похибки обробки інформації у навігаційних системах крилатих ракет в умовах невизначеності. *Наука і техніка Повітряних Сил Збройних Сил України*. 2019. № 2 (35). С. 151–157. DOI: https://doi.org/10.30748/nitps.2019.35.19.

2. Радиоэлектронные системы: основы построения и теория: справочник / под ред. Я. Д. Ширмана. М.: Радиотехника, 2007. 512 с.

3. Асавалюк А. В., Герасимов С. В., Рощупкін Є. С. Похибки визначення повного вектора швидкості в єдиній прямокутній системі координат системою оглядових станцій радіолокації з різною точністю. *Системи озброєння і військова техніка*. 2017. Вип. 2 (50). С. 53–56.

ГОЛОВНІ ПЕРЕВАГИ СЕПАРАБЕЛЬНОГО ПРОГРАМУВАННЯ ДЛЯ БАГАТОМІРНИХ ЗАДАЧ ПОБУДОВИ МОБІЛЬНОЇ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНОЇ СИСТЕМИ

Альошин Г.В.
Українська державна академія залізничного транспорту, Харків, Україна
Коломійцев О.В.
Національний технічний університет "ХПІ", Харків, Україна
Кулєшов О.В., Клівець С.І., Третяк В.Ф.
Харківський національний університет Повітряних Сил імені І. Кожедуба, Харків, Україна

На даний час питанням вибору ефективного методу розв'язання задач математичного програмування у математиці присвячені численні публікації. В задачах підвищення ефективності мобільних інформаційно-вимірювальних систем (МІВС) суттєву роль грають методи і алгоритми розв'язання задач, які у значній мірі визначають їх реалізацію і якість. Вибір кращого методу для таких задач звичайно формулюються у вигляді математичного програмування за списком показників якості. Одним із методів рішення багатомірних задач може бути умовне сепарабельне програмування, де складність задачі росте пропорційно їх розміру, в той час, як у відомих методі Вульфа і інших задачах, вона зростає у квадраті і більше. Однак, при всій універсальності, недоліки методу Вульфа саме у лінеарізації всіх функцій, що призводить до суттєвого зменшення кроку ітерації за кожним параметром і збільшення числа ітерацій [1, 2]. Більшість постановок задач підвищення ефективності і оптимізації ІВС вміщують цільову функцію за головним показником системи і функцію зв'язку, яка звичайно буває вартістю, або витратним показником.

За умови, коли є нечіткий показник вартості, доцільно лінеарізувати лише функцію зв'язку. Тоді, для спрощеного розв'язання задачі (у аналітичному вигляді) достатньо мати сепарабельну цільову функцію, яку можна перетворити у сепарабельну однотипну функцію.

Метою доповіді є представлення головних переваг сепарабельного програмування для багатомірних задач побудови МІВС.

В доповіді приведені особливості нового методу сепарабельного програмування. Отримані переваги методу можливо застосовувати до рішення задач оптимізації однофункціональних і багатофункціональних МІВС.

Список літератури

1. Aloshyn, H.V., Kolomiitsev, O.V., Kulieshov, O.V., Kulahin, K.K. and Tkachov, A.M. (2018), The method of parameters optimization of the multifunctional laser information-measuring system on the multiplicity of signals, structures and technical parameters, *Science and Technology of the Air Force of Ukraine*, No. 1(30), pp. 73-79. https://doi.org/10.30748/nitps.2018.30.10.

РЕАЛІЗАЦІЯ ЕЛЕМЕНТІВ ІНТЕЛЕКТУАЛЬНИХ ЕНЕРГЕТИЧНИХ СИСТЕМ

Бовчалюк С.Я., Любацький А.В.
Харківський національний університет радіоелектроніки, Харків, Україна
Піскарьов О.М.
Державний біотехнологічний університет, Харків, Україна

Енергетична система України знаходяться у стані оновлення і модернізації. При цьому слід зауважити, що на даний момент чітко визначеної цілісної стратегії її розвитку запропоновано так і не було. Основні напрямки розвитку енергетики, що базуються на застосуванні елементів технології Smart Grid, яка є загальновизнано. стратегією розвитку енергетичного сектору США та Європейського союзу, викладені в [1]. Деякі підходи і технології, що підходять під визначення Smart Grid і пропонуються для реалізації в Україні викладені у роботах науковців, наприклад [2, 3].

Метою доповіді є побудова елементів збору, вимірювання і обробки даних, а також керування в інтелектуальних електричних мережах, на базі керуючих автоматів з паралельною архітектурою.

У доповіді наводяться результати формування перспективного підходу до вдосконалення керуючих автоматів паралельної дії шляхом уведення математичного апарату нечіткого логічного висновку. Також розглядається доцільність використання процедури аналізу комбінацій заборонених станів команд керування автомату паралельної дії [4] та можливість аналізу заборонених комбінацій не тільки внутрішніх змінних автомату, але й станів зовнішнього середовища.

Реалізація вказаних можливостей дозволить значно розширити функціональні можливості керуючих автоматів паралельної дії та більш активно застосовувати ПЛК ПД, що побудовані на їх базі, для створення технічних засобів технології інтелектуальних мереж – Smart Grid.

Список літератури

1. B. Stognii, O. Kyrylenko, O. Prahovnyk, S. Denysiuk, "The evolution of intelligent electrical networks and their prospects in Ukraine", Technical Electrodynamics, vol. 5, pp. 52-67, 2012.

2. Тимчук С. А. Синтез оптимальной структуры распределительных электрических сетей при неопределенности исходной информации : монография / С. А. Тимчук, Н. М. Черемисин. – Харьков: ООО «В деле» 2016. – 270 с.

3. Stanislav Bovchaliuk. The Architecture of Fuzzy Logic Automat of Parallel Action for the Intelligent Smart Grid Networks / S. Bovchaliuk, S.Tymchuk, S. Shendryk, V. Shendryk // New Technologies, Development and Application III. NT 2020. Lecture Notes in Networks and Systems, vol. 128. Springer, – 2020. – P. 462–468.

4. Бовчалюк С. Я. Модели, методы и средства информационной технологии параллельного логического управления объектами железнодорожной автоматики: Дис. … канд. техн. наук: 05.13.06. – Харьков., 2008. –203 с.

МЕТОДИ ЗБОРУ ТА ОБРОБКИ БІОМЕДИЧНИХ ПОКАЗНИКІВ ЛЮДИНИ ЗА ДОПОМОГОЮ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ

Рижов І.В., Барковська О.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

Діагностика функціональних станів людини на основі аналізу електроенцефалограм, електрокардіограм, електроміограм та інших показників - важливий напрямок розвитку апаратно-програмних комплексів [1-2], які є поєднанням вимірювальних приладів з обчислювальними пристроями і програмою, що забезпечує керування роботою вимірювального приладу і супроводжуючих пристроїв, зняття і зберігання отриманої інформації, її перетворення і аналіз, представлення результатів у числовому, графічному чи текстовому вигляді. Комп'ютерна реєстрація і аналіз біомедичних показників повинні вміщувати наступні основні етапи: планування експерименту, підготовка апаратури і пацієнта до обстеження, реєстрація показників, перегляд отриманих записів з усуненням артефактів, фільтрація сигналів і обчислювальний аналіз з отриманням результатів у числовому і графічному вигляді, аналіз отриманих даних і формування заключення.

Метою роботи є визначення послідовності методів попередньої обробки біомедичних сигналів для виявлення характеристичних точок для діагностики викривлення хребту на основі аналізу існуючих досліджень.

Попередня обробка біосигналу включає в себе аналогові та цифрові перетворення, найважливішими з яких є згладжуюча фільтрація, режекторна фільтрація для уникнення наводок, смугова фільтрація для шумоподавлення та деякі спеціальні операції: корекція базової лінії, фільтрація коротких імпульсних завад, автоматичне регулювання підсилення та ін. Результат аналізу виявили, що при обробці біосигналів потрібне ослаблення перешкод за допомогою цифрових фільтрів нижніх частот. Застосування методів частотної смугової на початковому етапі попередньої обробки біосигналів забезпечує зниження погрішностей детектування характерних точок майже на 27%, що призводить до більш точнішої інтерпретації даних.

Список літератури

1. Y. Jusman, J. H. Lubis, A. N. N. Chamim and S. N. A. M. Kanafiah, "Feature Extraction Performance to Differentiate Spinal Curvature Types using Gray Level Co-occurrence Matrix Algorithm," 2020 3rd International Conference on Information and Communications Technology (ICOIACT), 2020, pp. 337-341, doi: 10.1109/ICOIACT50329.2020.9332067.

2. Axak, N., Rosinskiy, D., Barkovska, O., Novoseltsev, I. Cloud-fog-dew architecture for personalized service-oriented systems // Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018this link is disabled, 2018, стр. 78–82.

УЧАСНИКИ КОНФЕРЕНЦІЇ (крім секції 4)

ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

Азербайджанський технічний університет, Баку, Азербайджан
Військова Академія Збройних Сил Азербайджанської республіки, Баку, Азербайджан
Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна
Військовий коледж Збройних сил Азербайджанської Республіки, Баку, Азербайджан
Головне управління ДСНС України у Черкаській області, Черкаси, Україна
Державне підприємство "Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості", Харків, Україна
Державний біотехнологічний університет, Харків, Україна
Державний університет інфраструктури та технологій, Київ,, Україна
Державний університет телекомунікацій, Київ, Україна
Інститут кібернетики імені В. М. Глушкова НАН України, Київ, Україна
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут ім. Ігора Сікорського", Київ, Україна
Київський національний університет імені Тараса Шевченка, Київ, Україна
Льотна академія Національного авіаційного університету, Кропивницький, Україна
Національна академія Національної гвардії України, Харків, Україна
Національний авіаційний університет, Київ, Україна
Національний аерокосмічний університет імені М. Є. Жуковського "Харківський авіаційний інститут", Харків, Україна
Національний технічний університет "Харківський політехнічний інститут", Харків, Україна
Представництво "Оракл Іст Сентрал Юроп Сервісис Б.В.", Київ, Україна
Український державний університет залізничного транспорту, Харків, Україна
Університет технології і гуманітарних наук, Бельсько-Бяла, Польща
Харківське представництво генерального замовника – ДКА України, Харків, Україна
Харківський національний автодорожній університет, Харків, Україна
Харківський національний економічний університет імені С. Кузнеця, 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
Хмельницький національний університет, Хмельницький, Україна
Черкаський державний технологічний університет, Черкаси
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України, Черкаси, Україна

ЗМІСТ

Наукове видання

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

Тези доповідей
дев'ятої міжнародної науково-технічної конференції
18 – 19 листопада 2021 року
Том 1

Відповідальний за випуск *В. М. Рудницький*
Технічний редактор *І. А. Лєбедева*
Комп'ютерне складання та верстання *Н. Г. Кучук*

Підписано до друку 11.11.2021 Формат 60 × 84/16
Ум.-вид. арк. 8,25. Тираж 200 пр. Зам. 1111-21
Адреса оргкомітету: бульвар Шевченка 460, м. Черкаси, 18006, Україна
Черкаський державний технологічний університет

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**