Черкаський державний
технологічний університет

Військова Академія Збройних Сил
Азербайджанської республіки

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

Національний технічний університет
"Харківський політехнічний інститут"

Харківський національний
університет радіоелектроніки

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

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

ТЕЗИ ДОПОВІДЕЙ ДЕСЯТОЇ МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

24 – 25 листопада 2022 року

Том 1

Черкаси – Баку – Бельсько-Бяла – Харків – 2022

УДК 004 : 681.3

У збірнику подано тези доповідей десятої 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 Вченої ради Черкаського державного технологічного університету (протокол від 21.11.2022 № 6).

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

ПРОБЛЕМАТИКА СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ

Петренко П.Р.
Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна

За останні роки навчальні заклади України все більше переходять на дистанційне навчання, тож система навчання кардинально змінюється, як для учнів, так і для викладачів. З багатьох причин перехід на нову систему навчання відбувався не плавно, а в дуже швидкому темпі. Через це виникає ряд труднощів та проблем, одною з яких є технічне забезпечення [1].

Також дистанційне навчання потребує постійної комунікації та зворотного зв'язку кожного учасника навчального процесу. Вчителі повинні пояснити навчальний матеріал за допомогою цифрових технологій, контролювати виконання завдань та допомагати в їх розв'язанні. Тому сучасні педагоги мають якнайшвидше оволодіти методикою дистанційного навчання, яка зараз активно розвивається.

Метою роботи є розгляд та пошук вирішення знайдених проблем, а саме: проблема браку у вчителів та учнів сучасного обладнання для навчання [1]; проблема відсутності або часткового доступу до інтернет-зв'язку в деяких регіонах; проблема відсутності єдиної уніфікованої електронної платформи для навчання [2]; проблема відсутності безпосереднього контакту між викладачем та дистанційним студентом є серйозним недоліком дистанційної освіти [3].

В доповіді наведені результати опитування 2021 року по областям, щодо проблем дистанційного навчання. Також більш докладніше розглядається окремо кожна проблема та обирається найбільший ефективний шлях вирішення.

Список літератури

1. Нова українська школа. URL: https://nus.org.ua/news/tehnichne-zabezpechennya-najbilsha-problema-dystantsijnogo-navchannya/ (дата звернення: 24.10.2022)

2. Організація освітнього процесу із застосуванням технологій дистанційного навчання у 2020/2021 навчальному році: методичні рекомендації / за заг. ред. В.І. Шуляра. Миколаїв: ОІППО, 2020. 108 с.

3. Прибилова В. Проблеми та переваги дистанційного навчання у вищих навчальних закладах України. Проблеми сучасної освіти. 2013. URL: https://periodicals.karazin.ua/issuesedu/article/view/8791 (дата звернення: 24.10.2022).

ТЕХНОЛОГІЯ 3D-ВІЗУАЛІЗАЦІЇ НАВЧАЛЬНИХ МАТЕРІАЛІВ НА ОСНОВІ ВИКОРИСТАННЯ СЕРЕДОВИЩА UNITY3D

Пономаренко Є.О., Розломій І.О.
Черкаський національний університет ім. Б. Хмельницького, Черкаси, Україна

Онлайн-навчання є однією з неминучих тенденцій в освітньому секторі в усьому світі. Завдяки передовим і оновленим технологіям цей спосіб навчання став простішим. На сьогоднішній день існує багато інструментів, що значно спрощують даний процес, серед них: Google meet, Zoom, Skype, тощо. Та разом з приходом дистанційного навчання спостерігається тенденція зниження зацікавленості учнів у такому освітньому процесі.

Дослідження показали, що найбільш змістовне навчання відбувається, коли студенти залучені до справжньої діяльності, яка спонукає їх думати. Ця діяльність може включати використання віртуальних середовищ і моделювання, розробку моделей наукових явищ і використання допоміжних інструментів [1]. Пропонується дослідити технологію 3D-візуалізації навчання, що в перспективі може збільшити інтерес та бажання відвідування онлайн-занять. Для створення подібного середовища можна застосувати ігровий двигун Unity3D.

Цей ігровий двигун відомий своїм простим та зрозумілим середовищем розробки для інді та мобільних ігор. Але він є кросплатформеним, що дозволяє виконувати розробку майже для всіх популярних ігрових пристроїв. Одночасно з цим для Unity існують прості спеціальні інструменти, що дають можливість розробляти «мультиплеєрні» ігрові додатки. Крім цього, Unity є безкоштовним програмним забезпеченням.

Метою доповіді є дослідження та створення 3D-середовища для візуалізації навчального процесу та матеріалів.

В роботі проводиться дослідження існуючих способів та технологій дистанційного навчання для виявлення доступного функціоналу та його переваг і недоліків. На основі отриманих даних пропонується створити 3D-симуляцію навчального кабінету, куди зможуть доєднатися студенти та викладач, вибравши перед цим свого ігрового персонажа. Викладач матиме повний доступ до керування та демонстрації навчальних матеріалів. Студенти матимуть змогу заробляти бали, які можна буде використати у навчальному магазині. Такий процес навчання підвищить зацікавленість студентів до відвідування онлайн-занять.

Список літератури

1. Загальні відомості про Unity [Електронний ресурс]. – Режим доступу до ресурсу: https://www.informit.com/articles/article.aspx?p=2031153

ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ ФІКСАЦІЇ ТА КОНТРОЛЮ ВІДВІДУВАННЯ СТУДЕНТАМИ НАВЧАЛЬНИХ ЗАНЯТЬ ДЛЯ РІЗНИХ ГРУП КОРИСТУВАЧІВ

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

Автоматизація процесу фіксації відвідування студентами навчальних занять, згідно розкладу академічних груп, надасть можливість зменшити часові затрати на опрацювання цих даних та мінімізувати вплив людського фактору [1].

Метою доповіді є розглянути функціональні можливості інформаційно-аналітичної системи (ІАС) фіксації та контролю відвідування студентами навчальних занять для різних груп користувачів.

В доповіді представлено функціональні можливості ІАС для різних груп користувачів.

ІАС фіксації та контролю відвідування студентами навчальних занять складається з таких основних модулів: студент, група, розклад, аудиторний контроль, викладачі та статистика.

Всі учасники навчального процесу мають доступ до кожного модуля ІАС. Проте, в кожної групи учасників є свої дозволи та певні обмеження в доступі до інформації та функціональних можливостей системи. Доступ до системи надається за індивідуальним ключем.

Так, студент може отримати наступну інформацію: приналежність до академічної групи; список групи; по семестровий список дисциплін на навчальний рік; розклад занять на поточний семестр; перелік дисциплін та закріплених викладачів за ними.

Викладач має доступ до таких даних: по семестровий перелік дисциплін на навчальний рік; закріплені групи до кожної дисципліни та списки студентів кожної групи; розклад занять на навчальний семестр. Крім того, може формувати журнал відвідування як окремим студентом, так і групою в цілому, кожної окремої дисципліни.

Кафедра має доступ до даних, які доступні студентам та викладачам, а також може розподіляти викладачів, дисципліни та групи студентів, згідно їхнього навантаження. Має повну інформацію про студентів, які належать до кафедри. Може формувати та вести статистичний облік по студентам, групам, курсам, дисциплінам та викладачам кафедри.

Деканат має всі функціональні можливості що і кафедра. Крім того, може формувати та вести облік по студентам, академічним групам, дисциплінам, кафедрам, викладачам та курсам.

Список літератури

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

ЦИФРОВІЙ СТОРІТЕЛІНГ ЯК ПЕРСПЕКТИВНИЙ НАПРЯМ ФОРМУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ КОМПЕТЕНТНОСТЕЙ

Кірвас В.А.
Харківський гуманітарний університет «Народна українська академія»,
Харків, Україна

У наукових публікаціях сторітелінг розглядається як «спосіб передачі інформації і знань, а також спонукання до бажаних дій за допомогою повчальних історій». На сучасному етапі розвитку цифрових технологій традиційне оповідання все частіше замінюється цифровими (digital storytelling).

Дослідники відзначають потужний потенціал, популярність та перспективність технології цифрового сторітелінгу в освіті. Разом з тим, незважаючи на широкі можливості сучасного апаратного та програмного забезпечення, інтернет-сервісів констатується недостатнє їх використання педагогами для створення цифрових історій, що навчають, при викладанні інформаційно-комунікаційних технологій (ІКТ). При навчанні ІКТ оптимальною виявилася ротаційна модель (Rotation Model) змішаного навчання, а конкретніше, одна з її форм, що набуває найбільшої популярності, -- «перевернутий клас» (Flipped classroom). Онлайн навчання здійснюється, як правило, поза університетом: викладач надає доступ у мережі до електронних освітніх ресурсів (короткі відеоролики, презентації, аудіоподкасти, невеликі тексти з теми, що вивчається). Більшість людей навчаються найкраще, коли інформація представлена візуальним способом. Людський мозок краще сприймає аудіальні та візуальні аспекти, тому в ньому більше відкладаються саме відеокліпи. Однак відеокліпи мають бути короткими. Дослідження показують, що ефективність відео тривалістю понад шість хвилин різко падає. Деякі автори взагалі стверджують, що для сучасних учнів кліпи не повинні бути довшими за три хвилини. При цьому необхідно перейти від розуміння наочності як допоміжного засобу навчання до повноцінного використання візуального мислення учнів у процесі формування ІКК.

Дослідники стверджують, що цифровий сторітелінг сприяє ефективній взаємодії педагога з учнями, є ефективним інструментом, орієнтованим на підвищення інтересу до навчальної дисципліни, є методом популяризації знань та методом проектної діяльності учнів, що формує ІКК (цифрову грамотність, навички самостійної роботи з інформацією, самостійної мисленнєвої діяльності, візуалізації та ін.) необхідні в інформаційну епоху. Взагалі, слід зазначити, цифровий сторітелінг ефективний в освіті при взаємодії навчального контенту із педагогічними та цифровими технологіями. Викладачам треба володіти навичками роботи з мультимедійними пристроями, програмним забезпеченням для створення та редагування зображень, графіки, інфографіки, анімації, аудіо- та відеоматеріалів, що навчають. Потрібні дослідницькі, організаторські та презентаційні вміння, цифрова компетентність.

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ПЛАТФОРМИ HUMAN ШКОЛА У ЗАКЛАДАХ ОСВІТИ УКРАЇНИ

Доценко М.І.
Харківський національний університет ім. В. Н. Каразіна
Харків, Україна

Проблема забезпечення діджиталізації навчального процесу посідає надзвичайно важливе місце у системі нагальних питань розвитку сучасної загальної середньої освіти в Україні. Основними напрямками діджиталізації навчального процесу в закладах загальної середньої освіти традиційно виступають розробка електронних журналів та електронних щоденників [1], впровадження яких набуло особливої актуальності в умовах переходу шкіл на дистанційний формат роботи у зв'язку з запровадженням карантинних обмежень, зумовлених поширенням Covid-19, та військовим станом в Україні.

Перехід навчальних закладів України на дистанційний формат роботи мотивував українську Ed – tech компанію Human до розробки сучасної освітньої платформи, що мала б поєднувати в собі можливості проведення уроків у форматі відеоконференцій, простір для дистанційної комунікації, електронний журнал та електронний щоденник. Такою платформою стала Human Школа, якою станом на початок листопада 2022 р. вже користуються 2152 заклади загальної середньої освіти, 11 органів місцевої влади та 4 державні структури [2]. Окрім зазначених вище функцій, дана платформа має можливості збереження та синхронізації навчальних планів, видачі та повернення на доопрацювання домашніх завдань, проведення онлайн – тестувань суто на її базі, без використання додаткових платформ на кшталт таких як «На Урок» та «Всеосвіта», формування аналітики успішності окремого здобувача освіти чи усього класу загалом.

Метою доповіді є визначення проблем та перспектив запровадження та використання платформи Human Школа у закладах загальної середньої освіти України з огляду на її функціональні можливості та особливості інтерфейсу. У доповіді розглянуто специфіку функціональних можливостей та організації інтерфейсу платформи Human Школа для різних категорій учасників освітнього процесу (вчителі, здобувачі освіти, батьки, адміністрація навчального закладу тощо), визначено переваги, недоліки та перспективи її використання.

Список літератури

1. Бистрянцев М. В. Створення інформаційно – освітнього простору загальноосвітньої школи // Рідна школа. 2016. № 10. С. 19-24.

2. Human Школа. URL: https://www.human.ua/schools (дата звернення: 03.11.2022).

ІНТЕГРАЦІЯ ВЕБ-ТЕХНОЛОГІЙ У СИСТЕМУ УПРАВЛІННЯ НАВЧАННЯМ

Личагін Д.С., Яшина О.С.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

В часи глобалізації економічних та соціальних сфер життєдіяльності людини, окрему позицію в медійному просторі займають системи управлінням навчанням (Learning Management Systems, LMS). За їх допомогою можливо значно спростити та автоматизувати процес навчання. Функціонал LMS достатньо великий: зберігання навчального контенту, облік студентів, ведення статистики, викладення учбової інформації в зрозумілому користувачеві інтерфейсу, виконання навчальних завдань.

Але такі системи управлінням навчання мають суттєвий недолік, а саме обмежений функціонал із автоматизації перевірки об'ємних завдань. Як правило LMS мають можливість автоматично оцінити тестові завдання студентів, але не «вміють» оцінювати практичні роботи. Особливо ж, якщо мова йде про навчання мовам програмуванням, де найголовнішою запорукою успіху є практика. LMS, у своїй більшості, не можуть забезпечити перевірку та автоматичне оцінювання коду студентів.

Метою роботи є розробка плагіну для системи управління навчанням, таких як Moodle, eDX. Система управління навчанням має складну структуру та, окрім загального функціоналу, повинна мати можливість підключення сторонніх плагінів. Також необхідною умовою э гарно спроектоване API вебресурсу.

Для досягнення поставленої мети був спроектований плагін, який підключений до LMS. Функціонал плагіну включає анонімне ведення студентів, яке збільшує надійність та неупередженість оцінювання, за допомогою зав'язків за хеш-кодом. До основних функцій відносяться: автоматичне створення GIT-репозиторію, та покриття коду тестами; оцінювання коду за критеріями. Додаток має зручний та гнучкий дизайн. Було використано такі технології як JavaScript та фреймворк Angular для динамічного змінення DOM-елементів сторінок, Java для автоматизації доступу до системи контроля версії GIT для зберігання коду студентів..

Плагін дає можливість автоматизувати процес навчання студентів програмуванню з виконанням практичних завдань.

Список літератури

1. Юстик І. В., Гриценко В. Г., Подолян О. М. Аналіз можливостей використання систем управління навчанням в інформаційно-освітньому середовищі університету //Science and Education a New Dimension. Pedagogy and Psychology, IV (41). – 2016. – №. 86. – С. 11-15.

РОЗРОБКА ВЕБ-ДОДАТКУ ШКОЛИ З ГРИ НА МУЗИЧНИХ ІНСТРУМЕНТАХ

Кікоть М. С., Малєєва Ю. А.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

У наш складний час, коли у світі багато труднощів та проблем, одним із способів, який допомагає виявляти свої емоції та почуття, казати вагомі слова, щоб достукатися до інших, є музика. Музикотерапія належить до креативних видів терапії або арт-терапії та може зміцнити здатність до самовираження, підвищити самооцінку й упевненість у собі [1].

У зв'язку з війною в Україні наразі у багатьох дітей обмежена можливість набуття очної музичної освіти. Тому актуальним є створення засобів для дистанційного навчання грі на музичних інструментах [2]. У дистанційній формі навчання, крім можливості забезпечення оперативного зворотного зв'язку між учнем і вчителем на відстані за допомогою мережі, приваблює збільшення числа «ступенів свободи» у виборі темпу навчання, а також постійна актуалізація навчального матеріалу з меншими витратами відносно очної форми [3].

Метою доповіді є створення веб-додатку школи з гри на музичних інструментах, завдяки якому буде надано можливість дистанційного навчання грі на музичних інструментах учнів будь-якого віку з можливістю викладачам скоригувати матеріал й методи навчання під потреби кожного учня особисто.

В доповіді наведені результати дослідження актуальності даної тематики, переваги й недоліки вже існуючих веб-додатків з навчання музиці та їх функціоналу, а також тенденції розвитку таких веб-додатків у майбутньому. У розробленому веб-додатку запропоновано підхід до навчання, який базується на особистій увазі викладачів до учнів, адаптації матеріалів відповідно до потреб та навичок, а також містить елементи розважального характеру. Такий підхід сприятиме тому, що навчання музиці буде проходити у приємному та прийнятному учню темпі, за відсутності додаткового стресу, що відповідає принципам музикотерапії.

Список літератури

1. Український тиждень [Електронний ресурс]. – Фукс К. Музична медицина. – Режим доступу: https://tyzhden.ua/Science/241716.

2. Барановська, І. Г., Мозгальова, Н. Г., Барановський, Д. М., Бордюк, О. М. Використання засобів ІКТ у процесі дистанційного навчання майбутніх учителів музичного мистецтва. Наукові записки. Педагогічні науки. 2021. № 150. С. 21-37. Режим доступу: http://enpuir.npu.edu.ua/handle/123456789/35295. DOI: https://doi.org/10.31392/NZ-npu-150.2021.02.

3. Смульсон М. Л. Дистанційне навчання: Психологічні засади, Інститут психології імені Г.С. Костюка, 2012. 239 с.

ОСВІТНЯ ОНЛАЙН ПЛАТФОРМА ДЛЯ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ

Іванютенко Д. І., Лещенко Ю. О.
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

На даний час традиційною формою вивчення іноземних мов є граматико-перекладний метод, що багато в чому повторює процес вивчення «мертвих» мов, таких як латинь. Традиційний метод вивчення мов вважається застарілим, тому що результат досягається через тривалий час, що у сучасних умовах є одним з найважливіших факторів, бо може призвести до виникнення «мовного бар'єру» в іншомовному середовищі спілкування. Для підвищення засвоєння та розуміння мови створюється багато застосунків орієнтованих на CALL та MALL форми вивчення [1].

Метою доповіді є розроблення онлайн платформи для викладання іноземних мов та представлення результатів щодо її розробки.

Основна увага в доповіді приділена розробленій онлайн платформі для викладання іноземних мов, що дозволяє викладачеві якісно, докладно, в інтерактивній формі представити матеріали зі свого мовного курсу.

Найчастіше, в процесі навчання, використовуються методики, що включають в себе вивчення лексики та граматики, читання, розмовну практику [2]. Платформа дозволяє використовувати широкий вибір шаблонів для інтерактивного представлення курсу, з урахуванням індивідуального підходу до здобувача. Створивши курс на платформі, викладач може проводити індивідуальні консультації зі здобувачем, переглядати та корегувати виконання здобувачем завдань курсу, оцінювати рівень засвоєння та сприйняття кожної викладеної теми. За необхідністю, викладач може обирати необхідні завдання з курсу та включати їх в індивідуальну програму здобувача, що дозволяє надолужувати більш складні теми здобувачеві в коротші терміни.

Онлайн платформа для викладання іноземних мов дозволить здобувачеві, в дистанційному режимі, покращити знання з необхідної іноземної мови та спростити складний процес інтеграції в іншомовне середовище.

Список літератури

1. James W. Pagel, Stephen Lambacher, and David W. Reedy Instructors' attitudes towards CALL and MALL in L2 classrooms [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/301450942_Instructors%27_attitudes_towards_CALL_and_MALL_in_L2_classrooms

2. Красилич А.А. Особливості інтеграції інформаційних технологій в процесі навчання іноземній мові / А.А. Красилич // Актуальні проблеми іншомовної комунікації: лінгвістичні, методичні та соціально-психологічні аспекти: тез. доп. III Всеукр. наук.-мет. Інтернет-конф, 26 березня 2020 р. – Луцьк, 2020. –С. 32 – 34.

ВПРОВАДЖЕННЯ МОБІЛЬНИХ ТЕХНОЛОГІЙ В ОСВІТНІЙ ПРОЦЕС

Бельорін-Еррера О.М., Думанська А.С.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

Цифрова трансформація та цифровізація відкривають величезні можливості. Але вони також породжують багато ризиків. Те саме стосується нових технологій і активів цифрової економіки, в центрі яких знаходяться дані.

Практично кожна організація «переходить на цифрові технології» щодо багатьох бізнес-процесів та операцій.

Інтернет речей (IoT) розвивається запаморочливими темпами, і очікується, що до 2030 року загальна кількість підключених пристроїв збільшиться до 25,44 мільярда [1].

Кожен підключений до Інтернету пристрій у корпоративній мережі наражає організацію на ризик зламу IT-систем компанії. Зростає небезпека того, що неавторизовані сторони, більш відомі як «зловмисники», можуть отримати доступ до приватної чи службової інформації, викликати збої у роботі критично важливих служб або знищити бізнес.

По мірі того, як ризики множаться і трансформуються, змінюються і способи управління ними. Постійно з'являються нові продукти, послуги та партнери з консалтингу, кожен із яких прагне виділитися серед інших.

Метою доповіді є аналіз і порівняння сучасних підходів управління ризиками.

В доповіді розглянута загальна інформація щодо управління ризиками підприємства (ERM), управління, управління ризиками та дотримання вимог (GRC), інтегрованого управління ризиками (IRM).

Встановлено різницю між GRC та IRM з погляду програмного рішення [2]. З'ясовано, що інструменти та стратегії GRC розробляються за необхідності: коли з'являється новий регламент, часто впроваджується новий інструмент або стратегія для забезпечення відповідності.

Навпаки, інструменти та стратегії IRM інтегровані. IRM спирається на єдину інтегровану комплексну технологічну платформу для управління всіма ризиками організації.

Проаналізовано відмінності підходів оцінки ризиків IRM та ERM. Виявлено, що підхід до управління ризиками IRM включає в себе багато елементів ERM, але є більш цілісним.

Список літератури

1. https://financesonline.com/number-of-internet-of-things-connected-devices/.
2. https://blogs.gartner.com/john-wheeler/why-leading-software-vendors-are-dumping-grc-for-irm-2/

СЕКЦІЯ 2

ЗАСТОСУВАННЯ ТА ЕКСПЛУАТАЦІЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

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

ДОСЛІДЖЕННЯ ФУНКЦІЙ ТА СИНТЕЗ СТРУКТУРИ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ МАГАЗИНУ ОДЯГУ

Гудзь В. Р.
Черкаський державний технологічний університет, Черкаси, Україна

В даний час електронна комерція стає популярною у більшості країн, багато в чому це пов'язано з тим, що покупці все більше довіряють Інтернет-магазинам [1]. Основною метою будь-якого інтернет-магазину є залучення більшої кількості потенційних покупців та отримання більшої кількості продажів із найменшими витратами бюджету на рекламу.

Насправді найважливішим завданням є не збільшення відвідуваності як такої, а поліпшення показника конверсії відвідувачів у покупців. І одним із перевірених та надійних способів підняти продажі є покращення юзабіліті інтернет-магазину. Для покращення продажів і зручності роботи потрібно зробити роботу менеджерів простіше та зручніше; обробляти більше замовлень за одиницю часу; підвищити прибуток за рахунок оптимізації роботи. Також необхідний відповідний аналіз ринку товарів для збільшення продажів. [2]

Метою доповіді є дослідження функцій та синтез структури автоматизованої інформаційно-обчислювальної системи магазину одягу. В доповіді досліджено особливості, переваги та недоліки існуючих інтернет-магазинів з продажу одягу, досліджено функції та синтезовано структуру автоматизованої інформаційно-обчислювальної системи магазину одягу. Запропоновані в роботі рішення дозволять побудувати високопродуктивну автоматизовану інформаційно-обчислювальну систему підтримки пошуку товарів, маршрутів доставки, складів для зберігання товарів та підвищити ефективність надання послуг з продажу одягу, та знизити економічні витрати.

Список літератури

1. Актуальність інтернет мазазину збільшення юзабіліті - [Електронний ресурс]. Режим доступу - https://lemarbet.com/otkrytie-internet-magazina/yuzabiliti-internet-magazina-aktualnost-i-vliyanie-na-prodazhi/

2. Рейтинг магазинів для покупки одягу - [Електроний ресурс]. Режим доступу - https://www.pochtoy.com/shops/

ДОСЛІДЖЕННЯ ФУНКЦІЙ ТА СИНТЕЗ СТРУКТУРИ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ ТОВ "АГРЕЙН ТРАНС"

Руденко І. М.
Черкаський державний технологічний університет, Черкаси, Україна

В Україні, як і у світі, одним з найбільш болючих питань, що потребують першочергового розв'язання, є вирішення продовольчої проблеми. Виробництво зерна є ключовим для продовольчої безпеки людства. Нарощування його виробництва та більш раціональне його використання є однією з основних проблем сучасного сільського господарства України, як вирішальної умови поліпшення забезпечення населення продуктами харчування та подальшого економічного й соціального розвитку країни.[1]

Лідером перевезення зернових і зернобобових культур в Україні (у тоннах) є автомобільний транспорт, який перевозить зерно з полів на елеватори, залізничні станції та під'їзні колії станцій, морські порти, переробні підприємства та інші пункти. Велика частина зернових доставляється до місць навантаження на залізницю (залізничні станції, під'їзні колії станцій) саме автотранспортом і далі вже залізниця здійснює їхнє перевезення на експорт до морських портів. Таким чином на залізницю зернові та зернобобові культури зазвичай доставляються автомобільним транспортом.

Метою доповіді є дослідження функцій та синтез структури інформаційно-обчислювальних систем, зокрема інформаційно-обчислювальних систем вантажоперевізних компаній. В доповіді досліджено переваги та недоліки автоматизованої інформаційно-обчислювальної системи ТОВ "Агрейн Транс" та обрано основні математичні моделі що забезпечують роботу інформаційно-обчислювальної системи.[2]

Запропоновані в доповіді рішення дозволять побудувати високопродуктивну автоматизовану інформаційно-обчислювальну систему ТОВ "Агрейн Транс", що дасть можливість значно підвищити ефективність надання послуг з перевезення зернових та інших вантажів.

Список літератури

1. Українське зерно: стан та перспективи - [Електронний ресурс] -Режим доступу: http://repository.vsau.org/getfile.php/7127.pdf

2. О. В. Грицунов. Інформаційні системи та технології.

СИНТЕЗ КОРПОРАТИВНОЇ МЕРЕЖІ ПАТ "ЧЕРКАСИОБЛЕНЕРГО"

Тезетдінов В. А., Толмачов Д. К.
Черкаський державний технологічний університет

Основою інфраструктури сучасних підприємств є корпоративні мережі передавання даних. Дослідження структури різних корпоративних мереж показує, що сучасна мережа включає такі компоненти як: єдина для всіх підрозділів база даних, електронний документообіг, організація нарад, аудіо- та відеоконференції з віддаленими підрозділами, забезпечення користувачів високоякісним зв'язком на всіх рівнях [1].

Метою доповіді є синтез і моделювання корпоративної мережі ПАТ «Черкасиобленерго».

В доповіді детально розглядаються питання побудови моделі сервісу відеоконференцій підприємства на технологіях WebRTC та FreeSWITC [2]. Виконується моделювання багатофункціональної серверної структури для організації відеоконференцій в корпоративній мережі. Аналіз даних показує, що дана структура створює простір для селекторного, телекомунікаційного відеозв'язку та надає можливість підтримки комунікації в умовах реального часу без обмеження термінів і можливістю відображення документації, транслювання екрану організатора та учасників.

Основою побудови такого сервісу відеоконферернцій є Kurento Це медіа-сервер WebRTC і набір клієнтських API [3], що спрощує розробку передових відеопрограм для платформ www і смартфонів. Функції Kurento Media Server включають групові комунікації, перекодування, запис, мікшування, трансляцію та маршрутизацію аудіовізуальних потоків.

З'єднання між одноранговими вузлами корпоративної мережі встановлюються без спеціальних драйверів та плагінів і без будь-яких серверів-посередників[4]. Даний сервіс має ще багато інших переваг і являє собою аналог оркестратора великої кількості інших протоколів.

Список літератури

1. Mozilla for developers: Web Real-Time Communications. URL.: https://developer.mozilla.org/ru/docs/Web/API/WebRTC_API (Дата звернення: 05.11.2022).

2. BigBlueButton: Network Infrastructure Overview. URL.: https://docs.bigbluebutton.org/greenlight/gl-overview.html (Дата звернення: 05.11.2022).

3. L. L. Fernandez, M. P. Diaz, M. R. Benitez, F. J. Lopez, J. A. Santos, J.A. Catalysing the success of WebRTC for the provision of advanced multimedia real-time communication services, Intelligence in Next Generation Networks (ICIN), 2013 17th International Conference on , pp.23,30, 2013.

4. S. Loreto, Romano, S. Pietro, Real-Time Communications in the Web: Issues, Achievements, and Ongoing Standardization Efforts, Internet Computing, IEEE , vol.16, no.5, pp.68,73, 2012.

5. Тазетдінов Валерій Абударович, к.т.н., доцент, 050-4475198, valeriy.tazetdinov@gmail.com

МЕТОДИ КОНТРОЛЮ ТА УПРАВЛІННЯ КЛІМАТИЧНИМИ ПОКАЗНИКАМИ ПРИМІЩЕННЯ В IOT МЕРЕЖАХ

Чекаленко О. Л.
Черкаський державний технологічний університет, Черкаси

Темою є оптимізація методів контролю та управління кліматичними показниками приміщення в IoT мережах [1].

Ця тема є актуальною, тому що кожна людина хоче приходити в квартиру, будинок або офіс, та почувати себе в комфорті в любу пору року [2].

Тому потрібно розвивати даний напрям та оптимізувати вже існуючі методи.

Оскільки не має чітких обмежень у вартості і стандартизації, то вона є індивідуальною для кожного користувача.

Саме це робить розробку або вдосконалення цієї галузі досить актуальною темою у наш час.

Метою доповіді є дослідження кліматичної системи, що дозволяє керувати та контролювати поточний стан температури, вологості та атмосферного тиску з використанням методології «Інтернету речей».

Запропоновані в доповіді рішення дозволяють кожній людині покращити своє перебування в приміщенні, використовуючи автоматизовану системи контролю температури, вологості та атмосферного тиску.

Поки користувач системи займається своїми справами, система автоматично налаштовує роботу кондиціонеру, панелей обігріву та системи зволоження повітря.

Список літератури

1. Amer M. et al. Smart home energy management systems survey. International Conference on Renewable Energies for Developing Countries 2014.

2. Anvari-Moghaddam A., Monsef H., Rahimi-Kian A. Optimal smart home energy management considering energy saving and a comfortable lifestyle. IEEE Transactions on Smart Grid. 2014

КЛАСИФІКАЦІЯ ФУНКЦІЙ СИСТЕМ ЦИФРОВІЗАЦІЇ ВИРОБНИЧИХ ТА БІЗНЕС ПРОЦЕСІВ В АГРОПРОМИСЛОВОМУ КОМПЛЕКСІ

Чуєнко В. В.
Черкаський державний технологічний університет, Черкаси, Україна

Тотальна цифровізація сьогодні це фактична необхідність. Однією з галузей вітчизняної економіки, яка змогла закріпитися на ринку – це агропромисловий комплекс.

В концепції, затвердженій розпорядженням Кабінету Міністрів України від 03 березня 2021 року № 167-р, зазначається важливість «впровадження цифрового землеробства — принципово нової стратегії менеджменту, що базується на застосуванні цифрових технологій, та новий етап розвитку агросфери, пов'язаний з використанням геоінформаційних систем, глобального позиціонування, бортових комп'ютерів і смарт-устаткування, а також управлінських і виконавських процесів, здатних диференціювати способи обробляння, внесення добрив, хімічних меліорантів і засобів захисту рослин» [1]. Для прийняття правильного управлінського рішення фермер повинен володіти цифровими технологіями, такими як електронна карта полів, супутникові знімки, алгоритми диференційованої обробки поля, високотехнологічні датчики, мобільні програми та GPS-системи [2, 3].

Метою доповіді є розробка класифікації функцій комп'ютерних систем цифровізації виробничих та бізнес-процесів в агропромисловому комплексі.

В доповіді розглянуто важливість впровадження технологічних інновацій під час управління бізнес-процесами аграрних підприємств. Запропоновано класифікацію функцій систем цифровізації виробничих та бізнес процесів в агропромисловому комплексі.

Використання цифрових технологій в аграрних підприємствах дасть змогу якісно зберігати великий масив даних, проводити аналіз отриманих результатів, на підставі чого ухвалювати обґрунтовані рішення, які будуть сприяти мінімізації витрат, максимізації прибутку та підвищенню конкурентоздатності сільськогосподарського виробництва.

Список літератури

1. Кабінет Міністрів України. Розпорядження від 17 січня 2018 року № 67-р «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації», 2018.

2. Boltianskyi O. Environmental benefits of organic agricultural production. Молодь і технічний прогрес в АПК: Мат. Міжнародної науково-практичної конференції. Харків: ХНТУСГ. 2021. С. 206-209.

3. Маніта І.Ю. Питання цифровізації сільського господарства в Україні. Технічне забезпечення інноваційних технологій в агропромисловому комплексі: матеріали II Міжнар. наук.-практ. конф. Мелітополь: ТДАТУ, 2020.

СИМУЛЯЦІЯ ПОЛЬОТУ БПЛА ПО ЗАДАНОМУ МАРШРУТУ

Барсов В. І., Собора Г. О.
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

Планування маршруту польоту (ПМ), без зіткнення з перешкодами, є одним з основних питань при використанні БПЛА. Завдання ПМ істотно ускладнюється, якщо необхідно планувати маршрут, коли сенсорна система БПЛА виявляє динамічні або заздалегідь невідомі перешкоди, а система планування повинна опеативно локально змінити маршрут [1].

Одним з суттєвих підходів вирішення такого завдання є використання симуляторів польоту БПЛА на ПК, що також є альтернативним варіантом навчання операторів управляти БПЛА, що є актуальним завданням у теперішній час [2].

Симулятор може ідеально передавати фізику польоту моделі БПЛА тому квадрокоптер у реальному польоті буде поводитися саме так, як на екрані монітора під час тренувальних польотів [3]. При цьому для симуляції використовуються тривимірні математичні моделі реальних об'єктів планує-мого маршруту. Для повного аналізу результатів тестування програмного забезпечення симулятора використовуються дані отримані при тестуванні, які зіставляються з даними, що отримані під час синтезу системи управління БПЛА , наприклад, у середовищі Matlab Simulink.

Метою доповіді є викладення результатів реалізації системи симуляції польоту БПЛА по заданому маршруту.

В рамках цієї задачі було проведено аналіз існуючих програмних засобів які дозволяють проводити симуляцію пілотуємого або автономного польоту БПЛА по заданому маршруту із заданими характеристиками БПЛА. По результатах цього аналізу було розроблено програмне забезпечення та виконано моделювання тривимірних об'єктів на базі інструменту Unity 3D.

Для вирішення поставлених завдань були розроблені відповідні алгоритми.

Наводяться результати розробки та тестування системи, яка може відтворювати траєкторію руху БПЛА у пілотуємому або автономному польоті, згідно з відповідними математичними моделями, що були отримані у результаті моделювання системи в програмному середовищі MatLab Simulink.

Список літератури

1. Н. Л. Астахова, В. А. Лукашов. Дроны и их пилотирование. С чего начать :СПб.: БХВ-Петербург, 2021. — 224 с. ISBN 978-5-9775-6715-2

2. Як керувати квадрокоптером. URL: https://vcf.vn.ua › yak-navchitisya-keruvati-kvadrokopt (2021).

3. Симулятор квадрокоптера на ПК. URL: https://infocopter.ru/simulyator-kvadrokoptera-na-pk/ (2016).

ПРОГРАМНИЙ КОМПЛЕКС МОДЕЛЮВАННЯ ПЕРЕХОПЛЕННЯ БПЛА У ЗОНІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кудрявцева М. С., Дергачова Д. К.
Харківський національний університет радіоелектроніки, Харків, Україна

Для дослідження процесів ефективності використання засобів протидії безпілотним літальним апаратам (БПЛА) у зоні об'єктів критичної інфраструктури необхідний програмний інструмент, що дозволяє провести моделювання процесів перехоплення. У якості такого інструменту пропонується використовувати складний програмний комплекс у якому будуть реалізовані функції моделювання роботи радіолокаційних станцій (РЛС), ймовірнісне моделювання появи БПЛА конкретного виду у зоні об'єктів критичної інфраструктури, моделювання його руху та моделювання використання різних засобів перехоплення. При моделюванні перехоплення БПЛА будуть використані моделі руху для різних видів БПЛА з урахуванням висоти польоту, моделі спостереження РЛС різних видів, а також реалізовані різні алгоритми скеровування засобів перехоплення різної вартості [1].

Розроблений програмний комплекс дозволить проводити оцінку ефективності за різними критеріями використання різних засобів перехоплення конкретних видів БПЛА, обирати необхідний алгоритм скеровування, створювати раціональний план перехоплення декількох БПЛА різними засобами [2]. У якості засобів розробки використана мова програмування Python, бібліотеки numpy, pandas, matplotlib.

Метою доповіді є побудова загальної архітектури програмного комплексу, основних алгоритмів функціонування програмних модулів, що реалізують функції системи перехоплення БПЛА, а також побудова моделі інформаційної взаємодії компонентів системи.

В доповіді приведені результати загальна архітектура системи, алгоритми функціонування програмних модулів, а також модель інформаційної взаємодії компонентів системи.

Список літератури

1. Цепляева Т.П., Поздышева Е. М., Поштаренко А. Г. Анализ применения беспилотных комплексов. [Текст] Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ». Харьков.- https:www.khai.edu/csp/portal//Archiv/OIKIT39/p_149-154.pdf. Дата звернення 27.10.2021 г.

2. Даник Ю.Г., Пулеко І.В., Бугайов М.В. Виявлення безпілотник літальних апаратів на основі аналізу акустичних та радіолокаційних сигналів//Вісник ЖДТУ. 2014, № 4 (71). С.71- 80.

КОНТРОЛЬОВАНА ПОСАДКА БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ З ВИКОРИСТАННЯМ ТЕХНІЧНОГО ЗОРУ

Жукевич А. Б., Соболь С. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

В даний час використання малих літальних апаратів (БПЛА) набуває все більш широкого використання: аеророзвідки в важкодоступних або небезпечних місцях і т.п. Здебільшого навігація апарата у таких випадках здійснюється з використанням системи глобального позиціонування GPS [1]. Але сигнали навігаційних мереж легко глушаться (спотворюються), що призводить до неможливості виконання поставленого завдання. У цьому випадку стає актуальним управління польотом БПЛА з використанням візуальної орієнтації за допомогою засобів технічного зору. До цього посуває висока швидкодія керуючих контролерів і поява малогабаритних відеокамер високого розділення. Серед інших одним із завдань автономної навігації є контрольована посадка БПЛА на заданий майданчик. У цьому завданні виділяється проблема контролю висоти до точки посадки, бо відсутність рішення цієї задачі може привести до безповоротної втрати літального апарату. Шляхів рішення обчислення відстані декілька[2], одним з можливих варіантів є використанням лазерних далекомірів[3]. Використання далекоміра істотно спрощує завдання виміру відстані до об'єкту стеження, дозволяючи уникнути великої кількості обчислень, які потрібні в запропонованих методах[2]. При виборі приладу необхідно звернути увагу на ключові характеристики далекоміра: принципи обробки інформації; робоча дальність виміру (до 1,5 км); розмір лазерної точки (до 60 мм), що зменшить вірогідність втрати майданчика; захист по мірі IP (захист від дощу, пилу і вологи).

У запропонованій доповіді розглянуті можливості побудови системи контрольованої посадки з використанням системи технічного зору за допомогою лазерного далекоміра. Запропоновані рішення дозволяють спростити побудову, захищають від перешкод системи у використанні системи GPS як природного, так і штучного характеру.

Список літератури

1. Weiss S. Monocular-SLAM-based navigation for autonomous micro helicopters in GPS-denied environments / S. Weiss, D. Scaramuzza, R. Siegwar // Journal of Field Robotics (USA). – 2011. – Vol. 28, № 6. – P. 854–874.

2. Нечіпоренко О. М. Система вимірювання висоти польоту квадрокоптера підвищеної надійності. [Електронний ресурс] / Вчені записки ТНУ ім. В. І. Вернадського. Серія: технічні науки. Авіаційна та ракетно-космічна техніка. – 2020. – Т.31 (70) Ч1 №3 – С.32 – 39. doi.org/10.32838/TNU-2663-5941/2020.3-1/06.

3. Жукевич А.Б., Жукевич О.А. Супровід наземного об’єкта за допомогою технічного зору. // «Світ наукових досліджень», Матеріали Міжнародної наукової інтернет конференції (м.Тернопіль, Україна – м.Переворськ, Польща, 29-30 вересня 2022 р.) – С.287-290. http://www.economy-confer.com.ua/full-article/3906/

ВИКОРИСТАННЯ БІНОКУЛЯРНОЇ СИСТЕМИ ТЕХНІЧНОГО ЗОРУ ДЛЯ СІНТЕЗУ АЛГОРИТМУ КЕРУВАННЯ РУХОМ МОБІЛЬНОГО РОБОТА НА БАЗІ ОДНОПЛАТНОГО КОМП'ЮТЕРА RASPBERRY

Онопрієнко С. І., Горбач О. С.
Національний аерокосмічний університет ім. М.Є. Жуковського – «Харківський авіаційний інститут»

Однією з основних проблем сучасних мобільних роботизованих комплексів є проблема керування рухом у середовище з перешкодами. Не дивлячись на те, що дана проблема являється досить фактично фундаментальною, актуальних способів вирішення вона не має навіть у сучасному світі. Для розв'язання цієї проблеми необхідно скласти рух мобільного робота [1].

Для побудови алгоритму визначення шляху необхідно мати дані о відстані до найближчих перешкод. Це досягається завдяки аналізу карти глибини. Побудувати карту глибини можна декількома способами: використовувати спеціальні лазерні далекоміри або дорогі датчики, які використовуються у LIDAR. Більш раціональним методом є використання одного з напрямків машинного зору - стереопару, яка також дозволяє побудувати карту глибини. Основна відмінність саме стереопари від інших напрямків машинного - синхронне використання двох камер для визначення відстані до об'єктів [2].

Метою доповіді є побудова алгоритму по створенню та аналізу карти глибини, завдяки яким мобільний роботизований комплекс зможе здійснювати безпечний рух у середовищі з перешкодами.

Для побудови карти глибини використовувався метод Semi-Global Block-Matching Algorithm, який полягає у пошуку спільних значень для кожного пікселю з зображень обох камер, що дає змогу реєструвати інформацію о відстані до об'єкта у кожен піксель [3]. І саме завдяки отриманим даним існує можливість створення методу керування рухом у середовище з перешкодами, який має значні переваги, у порівнянні зі своїми аналогами.

В доповіді приведені результати у вигляді карти глибини, яка була побудована завдяки використанню стереопари та результати калібрування стереопари.

Список літератури

1. G. Ryan, R. Roelofs. Simultaneous Localization and Mapping, Swarthmore College. Dept. of Engineering, 2013: http://thesis.haverford.edu/dspace/handle/10066/11713

2. P. Fankhauser, M. Bloesch, D. Rodriguez, R. Kaestner, M. Hutter, R. Siegwart. "Kinect v2 for Mobile Robot Navigation: Evaluation and Modeling", Proceedings of the 17th International Conference on Advanced Robotics, ICAR 2015

3. H. Hirschmuller. "Stereo Vision in Structured Environments by Consistent Semi-Global Matching", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. V. 2, CVPR 2006

НОВІ СТАНДАРТИ ЗВ'ЯЗКУ: ПЕРСПЕКТИВИ ВИКОРИСТАННЯ

Лаврут О. О., Лаврут Т. В., Богуцький С. М., Обіход Л. П.
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного,
Львів, Україна

Технологія мобільного зв'язку розвивається до нового покоління кожні 10 років. Сьогодні широко використовуються технології третього (3G) та четвертого (4G) покоління, що призвело до появи різноманітних мультимедійних комунікаційних послуг. Подальший технічний прогрес зробив реальністю появу п'ятого покоління (5G). Японська компанія DoCoMo запровадила комерційну послугу 5G, використовуючи свою систему мобільного зв'язку 5G 25 березня 2020 року.

В доповіді розглядаються переваги та можливості технології 5G, яка характеризується високою швидкістю передачі даних, високою пропускною здатністю, низькою затримкою і збільшеною кількістю підключень. Завдяки таким характеристикам 5G очікується покращення рівня послуги мультимедійного зв'язку у порівнянні з попередніми поколіннями, включаючи 4G. Дана технологія стане фундаментальною, у взаємозв'язку з розвитком технології штучного інтелекту та інтернету речей (IoT, Internet of Things). Це забезпечить не лише голосову і цифрову комунікацію, але й обміни великими масивами даних у реальному часі, який характерний для «Інтернету речей», телемедицини, управління «розумними містами», а також роботи автономних автомобілів. Фактично 5G – це перше покоління мобільних пристроїв системи зв'язку, які можуть підтримувати високочастотні діапазони вище 10 ГГц.

Очевидно, що в майбутньому 5G дозволить використовувати великі обсяги даних, штучний розум і хмарні комп'ютерні технології для вирішення різноманітних задач як особистого, так і державного рівня.

Список літератури

1. 5G Evolution and 6G. January 2022 (Version 4.0). URL: https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_v4.0.pdf (Дата звернення 04.02.2022).

2. 6G: що це таке і що нам відомо про цю технологію/ URL: https://itechua.com/news/171637 (Дата звернення 05.11.2022).

3. Lavrut O. Promising approaches and technologies for building control systems of force structures agencies. «Findings of modern engineering research and developments»: Scientific monograph. Riga, Latvia: "Baltija Publishing", 2022. P. 233-264. DOI https://doi.org/10.30525/978-9934-26-207-4-9.

4. Лаврут О.О., Лаврут Т.В., Климович О.К., Здоренко Ю.М. Новітні технології та засоби зв'язку у Збройних Силах України: шлях трансформації та перспективи розвитку. Наука і техніка Повітряних Сил Збройних Сил України.- Х., 2019.- Вип. 1 (34). 91-101 https://doi.org/10.30748/nitps.2019.34.13.

5. НАТО і завдання 5G 30.09.2020 URL: https://www.nato.int/docu/review/uk/articles/2020/09/30/nato-zavdannya-5g/index.html (Дата звернення 04.11.2022).

НОВІТНІ ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Лаврут О. О., Лаврут Т. В., Тягун О. О., Обіход Л. П.
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного,
Львів, Україна

Сьогодні інформаційні технології стали одним з найважливіших чинників, що впливають на ефективність управління підрозділами командирами різних рівнів Збройних Сил України. Інформатизації в оборонній галузі активно досліджуються та практично впроваджуються новітні інформаційно-телекомунікаційні технології [1, 2].

У силових структурах України ведеться активна робота щодо створення ефективної системи оперативного управління, зв'язку, розвідки та спостереження (C4ISR) з метою здійснення управління підрозділами в єдиному інфокомунікаційному просторі [1, 2].

Наявність в різних силових підрозділах різнотипних засобів зв'язку та телекомунікацій потребує вирішення питання їх сумісності, надійності та забезпечення гарантованої якості під час виконання завдань за призначенням. Відповідно, актуальним напрямом досліджень є аналіз сучасних методів та технологій побудови високошвидкісних та надійних систем управління силовими структурами України під час виконання ними завдань в умовах, що швидко змінюються, а також пошук та застосування нових технологій в інформаційно-телекомунікаційній мережі критичного призначення.

В доповіді розглядається можливість та пропонується використовувати технологій 5G та 6G [3, 4], що дозволить будувати надійні високошвидкісні мережі зв'язку критичного призначення, розширить можливості підрозділів силових структур в питаннях їх підготовки, тренування та застосування під час виконання завдань за призначенням.

Список літератури

1. Лаврут О.О., Климович К.О., Тарасюк М.Л., Антонюк О.Л. Стан та перспективи застосування сучасних технологій та засобів радіозв'язку в Збройних Силах України. Системи озброєння і військова техніка: науковий журнал.- Х., 2017.- Вип. 1(49).- С. 42-49.

2. Лаврут О.О., Лаврут Т.В., Здоренко Ю.М., Колесник В.О. Модель та метод управління інформаційними потоками у телекомунікаційній мережі тактичної ланки управління. Сучасні інформаційні технології у сфері безпеки та оборони. 2021. Вип 1(40)/2021. С. 13–26. DOI: 10.33099/2311-7249/2021-40-1-13-26.

3. 5G Evolution and 6G. January 2022 (Version 4.0). URL: https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_v4.0.pdf (Дата звернення 04.02.2022).

4. В Японии рассказали, когда запустят сети 6G. 29.01.2020. URL: https://newsmir.info/1970600 (Дата звернення 04.02.2022).

МЕТОД КОНТРОЛЮ ЯКОСТІ ЕЛЕКТРОЕНЕРГІЇ СИСТЕМ ЕНЕРГОЗАБЕЗПЕЧЕННЯ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Герасимов С. В.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна
Сорока В. В.
Державний університет інфраструктури та технологій, Київ, Україна

Безаварійне та ефективне функціонування телекомунікаційних мереж залежить від якості електроенергії систем їх енергозабезпечення [1]. Так, наявність вищих гармонійних складових в сигналах напруги і струму призводить до значної методичної похибки вимірювання потужності електроенергії. Це, в свою чергу, є причиною або появи збоїв в роботі телекомунікаційних мереж, або, навіть, до виходу із ладу їх складових елементів [2].

У доповіді показано, що для телекомунікаційних мереж критичними є зміни у характеристиках систем енергозабезпечення, які обумовлені впливом перешкод (переважно електромагнітного та радіотехнічного характеру), якістю сигналів напруги і струму при наявності проблем (збоїв) у енергопостачанні. Представлено результати аналізу сучасної літератури та наукових розробок у даній галузі, які обґрунтовують актуальність дослідження для забезпечення нормального функціонування телекомунікаційних мереж.

Метою доповіді є розробка методу оцінки впливу вищих гармонійних складових в сигналах напруги і струму на якість електроенергії систем енергозабезпечення телекомунікаційних мереж.

Запропонований метод контролю базується на оцінюванні переходів через нуль вищих і перших (основних) гармонійних складових кривих напруги і струму відповідно [3]. У доповіді наведено результати практичного застосування розробленого методу контролю.

Практичне використання запропонованого методу полягає у формуванні вимог до форми електричних сигналів напруги та струму, які використовуються в системах енергозабезпечення телекомунікаційних систем.

Список літератури

1. Яровий В.С., Радзівілов Г.Д., Кірвас В.В. Діагностика несправностей випрямних трансформаторів високочастотних джерел живлення на основі визначення особливостей струму. Наука і техніка Повітряних Сил Збройних Сил України. 2021. № 4 (45). С. 152–162. DOI: https://doi.org/10.30748/nitps.2021.45.19

2. 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

3. Herasimov S., Borysenko M., Roshchupkin E. Spectrum Analyzer Based on a Dynamic Filter. Journal of Electronic Testing. 2021. № 37. С. 357–368. DOI: https://doi.org/10.1007/s10836-021-05954-0.

МЕТОД ОЦІНКИ ЗМІНИ ПАРАМЕТРІВ ТРАФІКА ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Можаєв О.О., Пересічанський В.М.
Харківський національний університет внутрішніх справ, Харків, Україна
Можаєв М.О.
Науково-дослідний центр судової експертизи з питань
інтелектуальної власності Міністерства юстиції України, Київ, Україна

При різкому збільшенні завантаження мережі взаємозв'язок між якістю функціонування телекомунікаційної мережі, рівнями її керування й змінами параметрів мережі ще не має досить точних кількісних оцінок. От чому проблема зміни семантичної прозорості телекомунікаційної мережі залежно від використовуваного протоколу керування є **актуальним науковим завданням**.

Метою даної доповіді є проведення оцінки зміни параметрів трафіка телекомунікаційної мережі від рівнів керування при різних рівнях втрат пакетів у мережі.

У доповіді проаналізовано, як впливають різні рівні керування мережею на втрати переданої інформації при збільшенні навантаження мережі. При аналізі розглядалася найбільш важлива характеристика, що визначає семантичну прозорість мережі: ймовірність спотворення бітів інформації, що визначається величиною коефіцієнту помилок по бітах.

При порівнянні різних механізмів керування, які застосовувалися до мережі з інтеграцією служб, доведено, що при малих значеннях коефіцієнту помилок по бітах більш ефективним способом керування є керування від “кінця до кінця” у порівнянні з керуванням на ланці.

Якщо ж величина коефіцієнту помилок по бітах досягає значень десь близько до 10^{-5}, то виникає підвищена ймовірність помилки передачі інформації та стає необхідним змінити керування від “кінця до кінця” на керування від “ланки до ланки”, що за рахунок повторної передачі ушкодженої інформації приводить до підвищення навантаження.

Надалі бажано провести дослідження впливу інших параметрів навантаження на показники якості надання послуг у телекомунікаційній мережі.

Список літератури

1. Можаєв О.О. Аналіз повідінки черг маршрутизаторів у мережах передачі даних в залежності від типів трафіку / О.О Можаєв, Г.А. Кучук, А.А. Коваленко // Системи озброєння і військова техніка. – 2009. – № 2(18).– С. 103-105.

2. Stallings W. ISDN and Broadband ISDN. McMillan Publ. Co., N.-Y., 1992. – 633 p.

3. De Pricker M. Asynchronous Transfer Mode – Solution for Broad Band ISDN. Second Edition. Alcatel Bell. Antwerp. – 331 p.

ПЕРЕВАГИ ВПРОВАДЖЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ МОНІТОРІНГУ

Скачков І. В., Піскарьов О. М.
Харківський національний університет радіоелектроніки, Харків, Україна

Мета науки про данні – покращити процес прийняття рішень, знаходячи корисні неочевидні закономірності у великих масивах даних. Сьогодні наука про данні використовується практично у усіх сферах починаючи з реклами, завершуючи соціальними мережами.

Аналіз, моніторинг, якісне відображення даних та їх доступність на всіх рівнях керівництва/робітників які долучені до процесу в будь-яких сферах діяльності, а особливо на великих, має величезну важливість та великий коефіцієнт корисності, якій в перспективі впливатиме на збільшення доходу, покращення продуктивності, зменшення різних помилок та загального рівня організованості [1].

Окрім інших переваг сильно виділяються швидкість доступу до даних, доступність та мобільність, що дає можливість всебічно покращити та полегшити роботу як звичайних робітників так і керуючого апарату.

Актуальність впровадження автоматизованих систем моніторингу у будь яких сферах діяльності, а особливо на виробничих має величезну перевагу над їх відсутністю, тому що з недоліків є тільні фінансові та кадрові. До кадрових недоліків можна віднести: час на навчання та звикання до нововведень, а також змінення робітників чи їх обов'язків (чи їх перекваліфікація), або повна реструктуризація сфери з введенням такої системи [2,3].

Метою доповіді є дослідження переваг й недоліків впровадження автоматизованих систем моніторингу.

Переваг набагато більше ніж недоліків та коефіцієнт їх корисної дії в багато разів перевищує будь-який з недоліків. З течією часу технології та їх застосування змінюється на благо людини та всебічно покращують та полегшують як повсякденний так і робочій простір. Впровадження сучасних інформаційних технологій в елеваторній промисловості та зернопереробних підприємствах, дозволяє максимально знизити втрати сировини на підприємстві, зменшити енергозатрати й, як наслідок, зменшити собівартість продукту.

Список літератури

1. Тирни Б. Наука о данных / Джон Келлехер, Брендан Тирни. — «Альпина Диджитал», М.:2020. – 222 с.

2. Бахрушин В.Є. Методи аналізу даних: навчальний посібник для студентів / В.Є. Бахрушин. – Запоріжжя : КПУ, 2011. – 268 с.

3. Горянский В.Ф. Математико-статистические методы в анализе эффективности сельскохозяйственного производства / В.Ф. Горянский. – К.:Вища школа, 1980. – 176 с.

ЗАСТОСУВАННЯ СТАТИСТИЧНИХ ОЦІНОК В УПРАВЛІННІ ПРОЕКТАМИ З РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Філімончук Т. В., Іванісенко І. М., Судаков В. О.
Харківський національний університет радіоелектроніки, Харків, Україна

Управління проектами з розробки програмного забезпечення є досить суперечливою та складною сферою IT діяльності. З одного боку, управління проектами вважається частиною галузі знань програмної інженерії і, отже, до управління проектами мають бути застосовані стандартні інженерні підходи. Причини цього детально розібрано в [1], одна з них – специфіка розробки програмного забезпечення. Програмні продукти незважаючи на те, що їх можна класифікувати, порівнювати і навіть формувати класи та типи (ERP системи, сайти-візитки, форуми, соціальні мережі та ін.), за своєю природою є унікальними виробами. Основні інженерні методики спрямовані на процеси оптимізації виробничого ланцюжка одного й того самого виробу [2].

Метою доповіді є запропонований альтернативний підхід до використання статистичних оцінок. Замість аналізу та прогнозування загального плану проекту на основі глобальних високорівневих оцінок автори зосередилися на прийомах, які можуть допомогти менеджменту проекту приймати більш виважені рішення, і таким чином у приватних питаннях позитивно впливати на хід усього проекту в цілому.

В доповіді проводиться оцінка складності та реалізації проекту в людині/годинах (або аналогічних величин). На основі цих оцінок визначаються вартість та фінансові ресурси на проект. В результаті оцінка завдань є однією з найкритичніших діяльностей, що здійснюються менеджментом проекту, оскільки оцінка завдань впливає на всі інші критичні параметри (час та вартість). Результати показують, що непараметрична регресія має потенціал для коригування «планів» розробника, проте для повноцінного висновку будуть потрібні додаткові дослідження (більше вибірок з діючих проектних команд). Слід зазначити, що у цій роботі розбиралися ті ситуації, у яких виконавець одночасно й оцінював завдання і виконував її.

Список літератури

1. National Research Council та Natl Research Coun. Statistical Software Engineering. National Academy Press, 2020, 675 p.

2. Miguel A., Madria W., Polancos R.(2019). Project Management Model: Integrating Earned Schedule, Quality, and Risk in Earned Value Management, 2019, 622-628 pp.

РОЗРОБКА СИСТЕМИ КРУЇЗ-КОНТРОЛЮ З ВИКОРИСТАННЯМ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Горбачов В. О., Куліш Д. В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні автомобілі оснащуються великою кількістю електронних систем під управлінням SoC, що дозволяє комфортніше керувати транспортним засобом, зменшує кількість аварій, полегшує навігацію тощо. Одна з таких систем – це система круїз-контролю. Дана система допомагає підтримувати постійну швидкість автомобіля залежно від зовнішніх умов[1]. Зазвичай дана система реалізується на перепрограмованій FPGA, що дозволяє зменшити вартість продукту і залишає можливість оновлень в майбутньому

Метою доповіді є аналіз програмно-апаратних засоби реалізації сучасних систем круїз-контролю і шляхів вдосконалення даних системи.

Телекомунікаційні мережі дозволяють використовувати технологію GPS, що полягає в зв'язку приймача, встановленому на транспортний засіб, та системою супутників, і визначенні місцеположення даного транспорту. Також за допомогою мобільного зв'язку можна отримувати актуальну інформацію про погоду та дорожні мапи. Використовуючи вище вказані технології можна вдосконалити систему круїз-контролю, дану реалізацію ще називають прогностичним круїз-контролем. Прогностичний круїз-контроль поєднує в собі круїз-контроль із GPS і топографічними мапами, керує швидкістю автомобіля в різних типах місцевості та за різними погодними умовами [2]. Використання телекомунікаційних мереж разом з сучасними технологіями дозволяє системі круїз-контролю заздалегідь передбачати можливі зміни швидкості транспортного засобу і ефективніше адаптуватися до навколишніх умов.

В роботі пропонується спосіб вдосконалити систему круїз-контролю за допомогою технології GPS, цифрових дорожніх мап та актуального прогнозу погоди, що дозволить заздалегідь дізнаватися про дорожні умови, щоб збільшити ефективність роботи даної системи.

Список літератури

1. A. Galip Ulsoy Automotive control systems / A. Galip Ulsoy, Huei Peng, Melih Cakmakci // Cambridge University, New York, USA 2012. – 406 с.

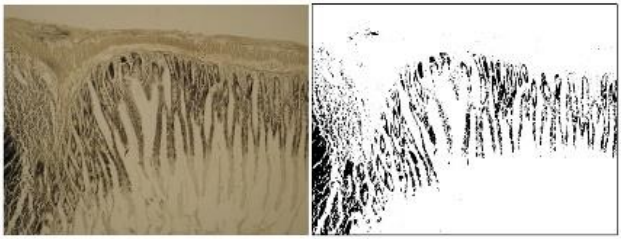
2. Peter Slowik Automation in the long haul: Challenges and opportunities of autonomous heavyduty trucking in the United States / Peter Slowik, Ben Sharpe // International council on clean transportation. 2018. – 30 с.

ВИЗНАЧЕННЯ ПОШКОДЖЕНИХ КЛІТИН КИШКІВНИКА ЗА ДОПОМОГОЮ МАТЕМАТИЧНИХ МЕТОДІВ ОБРОБКИ ЗОБРАЖЕНЬ

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

Для діагностики та оцінки ефективності лікування хронічних хвороб кишечника використовуються методи морфологічного дослідження, де визначається ступінь пошкодження клітин. Для цього проводиться фарбування клітин різними методами і за отриманими зображеннями оцінюється відсоток пошкоджених клітин на окремих ділянках мікропрепарату. Такий метод дослідження є дуже суб'єктивним і має багато похибок.

Метою доповіді є використання методів математичної обробки зображень для усунення суб'єктивності та підвищення точності аналізу. Пошкоджені клітини на зображеннях виглядають як крапки чорного кольору. Завданням дослідження було підрахувати клітини чорного кольору і оцінити їх відсоткову складову на зображенні. Приклад зображення показано на рис.1 а. Виділення чорних клітин (рис.1.б) та іхній підрахунок проводилося за допомогою пакету MATLAB.



а) б)

Рисунок 1 – Приклад зображення:
а) початкове зображення; б) зображення пошкоджених клітин

В результаті аналізу зображення виявлено, що пошкоджені клітини кишечника становлять 12% зображення.

Список літератури

1. Гонсалес Р. Вудс Р. Цифровая обработка изображений в среде MATLAB − [Текст] / Р. Гонсалес Р. Вудс. – М.: Техносфера, 2006 − 616 с.

2. GarginV, Radutny R, Titova G et al. Application of the computer vision system for evaluation of pathomorphological images. 2020 IEEE 40th International Conference on Electronics and Nanotechnology, ELNANO 2020 – Proceedings; 2020. 469-473.

3. Лилли Р. Патогистологическая техника и практическая гистохимия. – М.: Мир, 1969. – 645с.

КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ В БУДІВНИЦТВІ: ІНФОГРАФІКА ОГЛЯДУ ЛІТЕРАТУРИ

Григоров М. В., Фесенко Т. Г.
Харківський національний університет радіоелектроніки, Харків, Україна

Відомо, що реалізація будівельного проєкту передбачає інтеграцію значної кількісті даних і одночасно враховувати географію, умови розташування, існуючу інфраструктуру, а також широкий спектр вимог зацікавлених сторін. Від компанії забудовника вимагається інтеграція знань технологій розробки технічної документації, організації будівельних робіт, а також застосування сучасних засобів механізації і автоматизації. В будівництві використовуються інформаційно-комунікаційні технології: програми автоматизованого проектування (CAD); додатки віртуальної реальності; програмне забезпечення для планування та контролю проекту, управління ризиками; інформаційне моделювання будівель (BIM); інформаційна система управління проектами (PMIS) [1, 2] та ін. Тому перед забудовником постає завдання створення такої комп'ютерної системи, яка дозволить членам проектної команди (територіально віддаленим і міжфункціональним) обмінюватися даними через центральні сховища [3].

Метою доповіді є проведення аналізу досліджень з тематики «сучасні комп'ютерні технології управління в будівництві» та розробка інфографіки бібліометричних даних. Це дозволить з'ясувати існуючі дослідницькі акценти і обрати найбільш перспективні з точки зору сталоорієнтованого управління.

В доповіді наводяться результати пошукового запиту: «construction project», «contractor», «construction collaboration technologies», «communication technologies» у науково-метричній базі даних Scopus. Виявлено 35 документів за період 2005–2022 років. Програма VOSviewer відібрала 59 термінів і згрупувала їх у чотири кластера. До умовного кластера з IT-термінами увійшли: «surveys», «advanced visualization», «integration operations».

Список літератури

1. Фесенко Т. Г. Web-камера в системі мультимедійного комплексу офісу управління будівельними проектами. Вісник НТУ «Харківський політехнічний університет». Збірник наукових праць. Тематичний випуск: Автоматика та приладобудування. Харків: НТУ «ХПІ», 2008. № 56. С. 146–153.

2. Фесенко Т. Г. Модель вибору програмного забезпечення автоматизації бізнес-процесів офісу з управління будівельними проектами. Коммунальное хозяйство городов: Науч.-техн. сб. Київ: Техніка, 2008. Вып. 81. С. 359–365.

3. Нефьодов Л.І., Фесенко Т. Г. Інформаційна технологія організації офісу з управління будівельними проектами. Вісник НТУ «Харківський політехнічний університет». Збірник наукових праць. Тематичний випуск: Інформатика і моделювання. Харків: НТУ «ХПІ», 2008. № 24. С. 89–93.

ОРГАНІЗАЦІЯ ПРОГРАМНО-КОНФІГУРОВАНОЇ МЕРЕЖІ НА БАЗІ ПРОТОКОЛУ OPENFLOW

Іванісенко І. М., Пушкар А. І.
Харківський національний університет радіоелектроніки, Харків, Україна

У зв'язку з постійним розвитком та появою нових технологій, мережі потребують реалізації підвищених вимог до швидкості передачі та удосконалення інструментів, що використовуються для мережевого керування та моніторингу. Така ситуація спостерігається через появи нових функціональних та технологічних мереж, що має зворотний бік — ускладнення їх структури, адже оператори вимагають «розумніші мережі», але старі методи моніторингу та управління вже не справляються зі своїми функціями. Тому останнім часом зріс інтерес до програмно-конфігурованих мереж SDN (Software-Defined Networks), зараз вже відомими компаніями були запропоновано нові реалізації, які відкривають широкі можливості, наприклад організація мережі SDN із спільним застосуванням протоколу OpenFlow. Перевага представленої технології полягає в тому, що вона працює окремо від мережевих пристроїв та її контроль може здійснюватися операторами за допомогою стандартного сервера [2].

Метою доповіді є показати безперечні переваги використання програмно-конфігурованих мереж, і навіть їх взаємовигідної експлуатації з урахуванням сучасного протоколу OpenFlow. Для цього було відзначено принципи роботи стандарту, особливості функціонування комутаторів OpenFlow, позначено вигоди та переваги використання такої технології для подальшого розвитку телекомунікаційних систем.

В доповіді за матеріалами результатів проведених досліджень було доведено, що програмно-конфігуровані мережі на базі протоколу OpenFlow допоможуть розгортати сучасні корпоративні мережі зі складною інфраструктурою при мінімум витрат на їх обслуговування. Проведені тестування мережі SDN показали, що вибір такої технології дозволить IT-компаніям та іншим корпораціям підвищити ефективність мережевих пристроїв приблизно на 30% і настільки ж знизити витрати.

Список літератури

1. Коломеец, А. Е. Программно-конфигурируемые сети на базе протокола OpenFlow [Текст] / А. Е. Коломеец, Л. В. Сурков // Инженерный вестник. — 2014. — № 5. — С. 518–525.

2. Vaughan-Nichols, S. J. OpenFlow: The Next Generation of the Network? [Text] / S. J. Vaughan-Nichols // Computer. —2011. — Vol. 44, № 8. — P. 13–15.

АНАЛІЗ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ РЕСУРСІВ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ

Іванісенко І. М., Зінов'єв Б. М.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасна система управління характеризується високою інтенсивністю інформаційних потоків, причому вимоги до оперативності управління, своєчасного прийняття та доведення до виконавців рішень та завдання ній постійно підвищуються. Такі системи, як правило, є мультисервісними, тому що оперують різнорідною інформацією (дані, файли, аудіовізуальна інформація). Це зумовлює суттєву нестаціонарність потоків даних у мережі, інтенсивність яких в окремі періоди часу може істотно перевищувати середньостатистичні значення [1]. Разом з тим, при проектуванні систем управління розподіленими технологічними і транспортними комплексами пред'являються дуже високі вимоги, як за продуктивністю мережі, так і щодо надійності обслуговування абонентів. [2].

Метою доповіді є підвищення ефективності функціонування інформаційно-телекомунікаційної мережі за рахунок розробки та застосування методів адаптивного управління, що враховують флуктуаційний характер потоку даних у мережі та обмеження, накладені тактико-технічними вимогами.

В доповіді та роботі сформульовано математичну оптимізаційну задачу вибору найбільш ефективного мережевого протоколу. Для визначення ступеня ефективності передачі даних у телекомунікаційній мережі визначено та обґрунтовано вибір показників та критерію ефективності передачі даних у телекомунікаційній мережі та сформульовано оптимізаційне завдання вибору найбільш ефективного мережевого протоколу. Проведений аналіз основних вимог, що пропонуються до інформаційно-телекомунікаційної мережі (ІТМ), визначив, що існуючі інформаційні технології, на яких засновані методи управління розподілом трафіку в інформаційно-телекомунікаційних мережах, в умовах зростаючих обсягів циркулюючої інформації, а також при динамічній зміні структури системи передачі даних не здатні забезпечити вимоги до оперативності обміну інформацією.

Список літератури

1. Польщиков, К. А. Метод оценки эффективности управления информационными потоками в телекоммуникационной сети специального назначения [Текст] / К. А. Польщиков, О. Н. Одарущенко // Радіоелектронні і комп’ютерні системи. — 2018. — № 6 (33). — С. 269–276..

2. Huang, Q. A new convolution algorithm for loss probability analysis in multiservice networks [Text] / Q. Huang, K.-T. Ko, V. B. Iversen // Performance Evaluation. — 2019. — Vol. 68, № 1. — P. 76–87.

МЕТОД ПОПЕРЕДНЬОЇ ОБРОБКИ НЕЕЛАСТИЧНИХ ДАНИХ НА ВУЗЛАХ ВИСОКОМОБІЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Ткачов В. М., Фролов Д. Є., Яхно В. О.
Харківський національний університет радіоелектроніки, Харків, Україна

Задача передачі нееластичних даних (графіка, відео-, аудіопотоки) полягає у забезпеченні мінімальної затримки на проміжних вузлах між джерелом та одержувачем [1-2]. Нестиснені нееластичні дані вимагають значної ємності для зберігання та смуги пропускання. Окрім того, у високомобільних комп'ютерних мережах затримка може сягати 300 мс, тому, для інтенсивних потоків даних необхідно використовувати методи попередньої обробки з метою зменшення надмірності графічних, відео-, аудіоданих [3-4]. Одним із таких підходів є стиснення даних.

Метою доповіді є узагальнений огляд запропонованого рішення стиснення нееластичних даних як методу попередньої обробки нееластичних даних на вузлах високомобільної комп'ютерної мережі.

Загальною характеристикою більшості зображень є те, що сусідні пікселі корелюються і тому містять надмірну інформацію. Таким чином, суть попередньої обробки даних полягає в тому, щоб знайти менш корельоване уявлення зображення. Зниження надмірності реалізовано шляхом спрямованого видалення дублювання з вихідних даних однакових фрагментів. Метод враховує запас енергетичного ходу вузла мережі та його продуктивність.

Список літератури

1. Кучук Г.А. Выбор комбинаторного алгоритма оптимизации при управлении трафиком мультисервисной сети / Г.А. Кучук, А. А. Коваленко, О.О. Можаєв. // Системи обробки інформації. – 2015. – Вип. 10 (135). – С. 97-101.

2. Ткачов В.М. Метод передачі даних в комп'ютерній мережі проміжного зберігання даних складної інформаційної системи / В.М. Ткачов // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2017. – Т. 3 (43). – С. 117-119.

3. Ткачов В. М. Евристичний метод простих перетинів для оцінки показників живучості висомобільної комп'ютерної мережі / В. М. Ткачов, А. А. Коваленко, Г. А. Кучук // Дев'ята міжнародна науково-технічна конференція «Проблеми інформатизації». Т.1. – Черкаси - Харків - Баку - Бельсько-Бяла. – 18-19 листопада 2021 р. – С. 24.

4. Кучук Г. А. Метод параметрического управления передачей данных для модификации транспортных протоколов беспроводных сетей / Г.А. Кучук, А.С. Мохаммад, А.А. Коваленко // Системи обробки інформації. – 2011. – № 8(98). – С. 211-218.

МЕТОД ВИБІРКОВОЇ ОБРОБКИ ДАНИХ В ДЕГРАДУЮЧИХ ПОЛІНГОВИХ МЕРЕЖАХ

Ткачов В. М., Гунько М. А., Головін В. Д.
Харківський національний університет радіоелектроніки, Харків, Україна

Полінгові комп'ютерні мережі використовуються у якості комунікаційної платформи для розподіленого збору даних, попередньої обробки та передачі у визначені опорні вузли [1-2]. Як приклад, це може бути самоорганізуюча мережа для моніторингу пожежної ситуації в лісі, температурного режиму в ємностях тощо. Вузли полінгової мережі мають обмежений час функціонування за рахунок автономного джерела живлення. Відповідно, виникає актуальна задача перерозподілу обчислювальної потужності на етапі попередньої обробки даних у разі деградації вузлів мережі [3-4].

Метою доповіді є узагальнений огляд підходу пріоритезації, який лежить в основі вибіркової обробки даних в деградуючих полінгових мережах.

Сутність методу полягає в визначенні пулу функцій вузлів та встановлення кожній з них пріоритетів. Цей пул можна представити у вигляді матриці, на яку накладається матриця енергетичного запасу дії кожного з вузлів. Особливістю методу є можливість підключення найбільш вживаних методів статистичного прогнозування траєкторії роботу вузлів полінгової мережі, засновані на моделі Брауна, Хольта-Уїнтерса, методах еволюції для дво- і трипараметричних моделей та метод гармонійних значень.

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. V. Tkachov, M. Hunko, O. Morozova, A. Tetskyi and A. Nicheporuk, "Method to Determine Fault-Tolerant Performance Probability of High-Survivability Computer Network based on Mobile Platform," 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 1-5, doi: 10.1109/PICST54195.2021.9772202.

3. Матвийцив А.И. Анализ подходов к расчету конфигурации компьютерной сети / А.И. Матвийцив, А.А. Коваленко // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали шостої міжнародної НТК. – Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ДП «ХНДІ ТМ», 2016. – 21-22 квітня 2016. – С. 26-27.

4. Кучук Г.А. Модель процесса эволюции топологической структуры компьютерной сети системы управления объектом критического применения / Г.А. Кучук, А. А. Коваленко, А. А. Янковський. // Системи обробки інформації. – 2014. – Вип. 7(123). – С. 93-96.

НЕЛІНІЙНА ДИНАМІКА ТРАФІКУ ІЗ ЗАСТОСУВАННЯМ AQM RED

Андрос А. М., Партика С. О., Янковський О. А.
Харківський національний університет радіоелектроніки, Харків, Україна

З безпрецедентним зростанням мережі Інтернет, як за його розміром, так і за кількістю абонентів, проблема контролю заторів пакетів стає все більш важливою для уникнення колапсу перевантаження. Було запропоновано багато різноманітних підходів для вирішення цієї проблеми. Один з таких підходів полягає в контролі рівня перевантаження на кожному маршрутизаторі за допомогою механізму активного керування чергою (AQM) [1]. Механізми активного керування чергами це засіб кращого управління перевантаженням вузьких місць у мережі. Для контролю середнього розміру черги на перевантажених маршрутизаторах було запропоновано механізм випадкового раннього виявлення (RED) [2].

Метою доповіді є аналіз проблем нелінійної динаміки змішаного трафіку TCP та UDP. Представлено просту нелінійну модель з дискретним часом, яка використовується для фіксації динаміки взаємодії маршрутизатора RED із з'єднаннями TCP та UDP. Також продемонстровано, що система може мати нестабільну поведінку через нелінійну поведінку, притаманну TCP, а не через розрив імовірності відкидання пакетів як функції середнього розміру черги [3]. Крім того, було показано, що наявність трафіку UDP не просто забирає доступну пропускну здатність TCP-з'єднань, а суттєво змінює динаміку поведінки мережі.

Також було проведено дослідження впливу різних системних параметрів, таких як кількість TCP-з'єднань і затримка RTT на стабільність системи. Показано, що застосування налаштовуваних порогів RED створює основу для розробки схем AQM для покращення контролю рівня перевантаження.

Список літератури

1. V. Sharma and P. Purkayastha, "Performance analysis of TCP connections with RED control and exogenous traffic", Proc. of GLOBECOM 2001, pp. 39–57, San Antonio, TX, December 2001.

2. H. M. Alazemi, A. Mokhtar, and M. Azizoglu, "Stochastic modeling of random early detection gateways in tcp networks," in Proceedings от Globecom 2000, 2000.

3. C. V. Hollot, V. Misra, D. Towsley, and W. Gong, "On designing improved controllers for AQM routers supporting TCP flows", Proc. of IEEE INFOCOM 2001, Vol. 3, pp. 1510-1519, Anchorage, AK, 2001.

ПЕРЕВАГИ І НЕДОЛІКИ AQM

Чернов Б. Д., Партика С. О.
Харківський національний університет радіоелектроніки, Харків, Україна

Активне керування чергою (AQM) призначене для досягнення високого рівня використання каналу з низькою затримкою в чергах маршрутизаторів. Чисельні дослідження показують, що RED [1], один із найвідоміших AQM, не забезпечує значного приросту продуктивності, враховуючи складність, необхідну для правильного налаштування його параметрів. Деякі варіанти RED, такі як Adaptive RED [2], розроблені для забезпечення більш надійної роботи RED у більш широкому діапазоні умов існуючого трафіку, але теж мають деякі недоліки.

Метою доповіді є дослідження переваг і недоліків активного керування чергами маршрутизаторів. AQM можуть підтримувати значно меншу довжину черги, ніж у випадку черги з Drop Tail, що надає можливість розвантажити буфер та зменшити затримку в мережі. Різноманітні дисципліни AQM вимагають ретельного налаштування своїх параметрів для забезпечення гарної продуктивності. Однак, ці AQM не працюють оптимально з точки зору теорії управління [3]. Однією з основних проблем алгоритмів родини RED є те, що вони цілком залежать від оцінки довжини черги маршрутизатора. У період значного навантаження одне джерело може передавати пакети зі швидкістю більшою, ніж пропускна здатність вузького місця, що може призвести до створення черги так само легко, як і у випадку великої кількості джерел.

В доповіді представлено модель поведінки черги маршрутизатора для AQM з відкиданням та маркуванням пакетів для ілюстрації впливу TCP-трафіку на завантаження і поведінку перевантажених маршрутизаторів.

Експериментально показано, що коли методи AQM додатково використовують ECN, як метод сповіщення джерел TCP про перевантаження, приріст продуктивності AQM з точки зору пропускної здатності та затримки може бути значним порівняно з керуванням чергою з відкиданням пакетів.

Список літератури

1. V. Misra, W.-B. Gong,, D. Towsley, Fluid-based Analysis of a Network of AQM Routers Supporting TCP Flows with an Application to RED, Proc., ACM SIGCOMM 2000, pp. 151-160.

2. S. Floyd, R. Gummadi, S. Shenker, Adaptive RED: An Algorithm for Increasing the Robustness of RED's Active Queue Management, http://www.icir.org/ floyd/papers/ adaptiveRed.pdf, August 1, 2001.

3. L. Le, J. Aikat, K. Jeffay, F.D. Smith, The Effects of Active Queue Management on Web Performance, ACM SIGCOMM 2003, August 2003, pp. 265-276.

ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЇ «NaaS»

Волошин І. А., Партика С. О.
Харківський національний університет радіоеліктроніки, Харків, Україна

Вже настав день, коли корпоративні IT - фахівці можуть замовляти компоненти мережевої інфраструктури з меню опцій, налаштовувати їх відповідно до потреб свого бізнесу, а також підключати, запускати та керувати всім цим. Ця концепція називається "мережа як послуга" (NaaS), і на даний час вона існує у різних формах, в основному на арені постачальників послуг [1].

Метою доповіді є огляд технології «мережа як послуга», її реалізація, плюси та мінуси для користувачів, сценарії використання. Наведено огляд різноманітних проблем, які все ще залишаються, наприклад аспекти безпеки мережі, яка може стати серйозною проблемою при її використанні. Розглянуті такі питання як: пропускна здатність, час безвідмовної роботи, продуктивність, гарантований рівень обслуговування, як часто обладнання повинно оновлюватися, які інструменти повинен використовувати постачальник «NaaS» для управління ємністю та продуктивністю. Розглянута реалізація на прикладі одного з найбільших світових постачальників мережевих послуг компанії «Cisco».

В доповіді проведено аналіз перспектив подальшого розвитку «NaaS», так як дана технологія може відіграти важливу роль в подальшому розвитку хмарних мереж [2]. Наприклад, згідно з даними дослідницької компанії IDC, до 2024 року понад 75% мережевої інфраструктури на периферії та до 50% інфраструктури центрів обробки даних будуть використані в моделі « мережа як послуга». Великі підприємства впроваджують хмарні послуги для зберігання даних та центрів обробки даних для мобільності робочих місць. Крім того, зростання попиту на бізнес-модель на основі підписки в хмарних обчисленнях, NFV і SDN сприяло впровадженню NaaS серед великих підприємств. Зрозуміло, що перехід корпоративних клієнтів до хмарних сервісів є основним драйвером «NaaS». І хоча мережева індустрія лише зараз вирішує, як хмарний світ буде ефективно об’єднаний у мережу, NaaS може зіграти велику роль у майбутньому.

Список літератури

1. Costa, P., Migliavacca, M., Pietzuch, P., and Wolf, A. L. Naas: Network-as-a-service in the cloud. In Proceedings of the 2nd USENIX conference on Hot Topics in Management of Internet, Cloud, and Enter prise Networks and Services, Hot-ICE. (2012), volume 12.

2. Chou, Wu, and Li Li. “Methods and Infrastructure of Network-as-a-Service.” Network as a Service for Next Generation Internet, 2017, 25–50. doi:10.1049/PBTE073E_CH2.

ЧЕРГИ У МАРШРУТИЗАТОРАХ ТА AQM АЛГОРИТМИ

Філіппов В. В., Харченко О. А., Партика С. О., Янковський О. А.
Харківський національний університет радіоелектроніки, Харків, Україна

Комунікаційні мережі наступних поколінь будуть базуватися на парадигмі IP. Хоча швидкості сучасних мереж зростають експоненціально, їх пропускна здатність завжди відстає від зростання мережевого трафіку. Це означає, що з обмеженими ресурсами пропускної здатності слід знайти підходи для покращення продуктивність мереж, щоб задовольнити потреби критичних у часі та важливих додатків [1].

Коли занадто багато вхідних пакетів претендують на обмежені спільні ресурси, такі як буфер черги в маршрутизаторі та вихідна смуга пропускання, при передачі даних може виникнути перевантаження. Під час перевантаження велика кількість пакетів зазнає затримки або навіть втрачається через переповнення черги. Серйозні проблеми з перевантаженням призводять до погіршення пропускної здатності та великої кількості втрачених пакетів. Для забезпечення стабільності мереж при перевантаженнях була запропонована технологія Active Queue Management (AQM) [2].

Метою доповіді є розгляд сучасних методів боротьби з перевантаженнями. Розглянута проблематика перевантажень, а також можливе рішення у вигляді різноманітних алгоритмів AQM. Запропоновано алгоритм керування чергами маршрутизаторів, орієнтований на затримку, ключовим компонентом якого є масштабований механізм вимірювання параметрів трафіку в реальному часі. Алгоритм поєднує механізм вимірювання в реальному часі зі звичайною стратегією алгоритму RED та адаптивний підхід керування параметрами алгоритму Adaptive RED, завдяки чому відстежує сплески трафіку та відрізняє їх від природних коливань швидкості передачі даних.

Моделювання показує, що запропонований алгоритм функціонує ефективно та успадковує переваги алгоритму RED та алгоритму Adaptive RED в автоматичному налаштуванні параметрів на основі вимірювань параметрів трафіку.

Список літератури

1. Lujuan Ma, Xiaoping Liu, Huanqing Wang and Huanqing Wang "Congestion Tracking Control for Multi-Router TCP/AQM Network Based on Integral Backstepping" in Computer Networks journal. DOI: http://dx.doi.org/10.1016/j.comnet.2020.107278

2. Mahmud Etbega, M.E. Woodward, A. G. Ali and Hussein A. “A New Version of Adaptive RED with Reduced Dependency on Parameterisation”, Proceedings of the Fourth International Working Conference on Heterogeneous Networks (HETNETs’ 06), pp WP10/1- WP10/8, llkley, UK, September 2006.

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

ANALYSIS AND COMPARISON OF DATA PROTECTION PROTOCOLS OF WI-FI NETWORKS

Balagura D. S., Karavaiev V. M.
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

Information in the modern world is the most valuable asset both for individuals and for states, corporations and companies in various fields of activity. Wi-Fi networks are one of the most widespread technologies for wireless data transmission. It does not require physical connection to cables: all information is transmitted via radio channels in public access, so the use of this technology places high demands on data protection protocols circulating in Wi-Fi networks.

The purpose of the report is to define and analyze basic and advanced Wi-Fi network protection protocols, which is a basic condition for their safe use for data transmission of various levels of confidentiality.

The report reviews the basic, modern and promising protocols and mechanisms for ensuring secure connection and data transmission in WiFi networks: the basic outdated WEP protocol, its temporary improvement WPA, the most common today WPA2 protocol, as well as the next generation wireless network protection protocol WPA 3.

A comparative analysis of schemes, models, mechanisms, algorithms and key lengths in the specified protocols is carried out. The possibility and risks of using all and any of these protocols under certain predetermined conditions are determined. Conclusions are drawn regarding the further development of data protection protocols in next-generation WiFi networks, namely Wi-Fi 6, which is currently being implemented, and Wi-Fi 7, which is under development.

Thus, in wireless networks, cryptographic means are used to ensure the integrity and confidentiality of information. However, errors in security protocols lead to communications disruption and malicious use of information.

References

1. IEEE Std 802.11™-2020 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

2. WPA3™ Specification Version 3.0

3. Mariusz Bednarczyk, Zbigniew Piotrowskia, Military University of Technology, Gen. W. Urbanowicz 2 Str., 00-908 Warsaw, Poland “Will WPA3 really provide Wi-Fi security at a higher level?”

ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ Д ЛЯ ЗАХИСТУ АВТОМАТИЗОВАНИХ СИСТЕМ

Міценко С. А., Партицький О. В., Могильний О. А.
Черкаський державний технологічний університет, Черкаси, Україна

Інформаційні технології стали невід'ємною частиною нашого життя, у зв'язку з цим здійснюється автоматизація багатьох процесів життєдіяльності людини. Велика частина інформації зберігається в інформаційних системах, які необхідно захищати [3]. В атаках на інформаційні системи зловмисники використовують помилки в написанні та адмініструванні програм. Розробники ресурсів, які працюють з даними користувачів, зобов'язані їх захищати та запобігати можливості витоків. Однією з сучасних основних проблем є слабкий розвиток індустрії інформаційної безпеки, зокрема, створення засобів криптографії. В Україні, в даний час, у діючих системах захисту електронних даних використовуються закордонні криптографічні алгоритми і стандарти. Дослідження, що стосуються безпеки даних і застосування зарубіжних готових рішень – ризиковане, у зв'язку з цим необхідно формувати власні ресурси для безпеки інформації [1].

Метою доповіді є дослідження та реалізація алгоритму двофакторної аутентифікації для забезпечення захисту інформації в інформаційно-комунікаційних системах.

В доповіді досліджені алгоритми аутентифікації користувачів інформаційно-комунікаційних систем на основі другого фактору. Алгоритм двофакторної аутентифікації створено на основі генерації одноразового пароля, який обчислюється з використанням обраної тригонометричної функції для посилення захисту інформаційної системи [2]. Здійснено аналіз відомих алгоритмів і протоколів двофакторної аутентифікації, криптографічних алгоритмів і додатків для захисту інформації в інформаційних автоматизованих системах. Розроблено алгоритм двофакторної аутентифікації на основі програми-аутентифікатора та мобільного телефону, який генерує ускладнений набір функцій одноразового пароля для кожної окремої інформаційно-комунікаційної системи.

Список літератури

1. Folasade A. Brute-Force Attack Prevention in Cloud Computing Using One-Time Password and Cryptographic Hash Function // International Journal of Computer Science and Information Security (IJCSIS). – 2019. Vol. 17, № 2. – P. 7–19.

2. Prisha P. Commerce Security and Identity Integrity: The Future of Virtual Shopping// Advanced Science Letters, – 2020. Vol. 23, № 8 – P. 7849–7852.

3. Ussatova O. Two-factor authentication algorithm implementation with additional security parameter based on mobile application// International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME2019). – Guilin, China, 2019. – Vol. 89. – P. 84–86.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ СИМЕТРИЧНИХСЕТ-ОПЕРАЦІЙ

Рудницька Ю. В. Короткий Т. К.
Черкаський державний технологічний університет, Черкаси, Україна

Стрімкий розвиток систем криптоаналізу, в тому числі постквантового вимагає розробки нових та вдосконалення вже існуючих криптографічних систем [1]. Проведений огляд результатів дослідження СЕТ-операцій показав що синтезу симетричних двохоперандних багато розрядних операцій приділялося недостатньо уваги. Це пояснюється комбінаторним ростом кількості двохоперандних операцій при збільшенні розрядності навіть в порівнянні з одноопераднимі. Симетричні двохоперандні операції використовуються при побудові практично всіх криптоалгоритмів, тому необхідно проводити дослідження симетричних двохоперандних операцій криптографічного кодування [2]. Єдиним шляхом вирішення задачі синтезу і аналізу симетричних двохоперандних операцій криптографічного кодування є побудова спеціалізованої інформаційної технології.

Метою доповіді є побудова структури інформаційної технології моделювання та дослідження симетричних СЕТ-операцій, результати застосування якої забезпечать підвищення захищеності інформаційних систем критичної інфраструктури за рахунок створення нових можливостей для вдосконалення криптоалгоритмів.

В доповіді наводяться результати розробки і дослідження моделей СЕТ-операцій та методи їх синтезу. Приводяться алгоритми генерації послідовностей моделей СЕТ-операцій. Розглядаються технології оцінки згенерованих послідовностей.

Розроблена структура інформаційної включає: модуль (інтерфейс) введення вхідних даних і параметрів; підсистему управління режимами роботи; підсистему пошуку та формалізації корінних операцій; базу даних; базу знань; модуль синтезу СЕТ-операцій; модуль генерації послідовностей СЕТ-операцій; модуль статистичних досліджень; модуль узагальнених оцінок.

Список літератури

1. Svitlana Sysoienko, Iryna Myronets and Vira Babenko. Practical Implementation Effectiveness of the Speed Increasing Method of Group Matrix Cryptographic Transformation // Second International Workshop on Computer Modeling and Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), Zaporizhzhia, Ukraine, April 15-19, 2019. P. 402-412. Режим доступу: http://ceur-ws.org/Vol-2353/paper32.pdf

2. Рудницький В. М., Лада Н. В., Бабенко В. Г. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія. Монографія / Харків: ТОВ «ДІСА ПЛЮС», 2018. 184 с.

КЛАСИФІКАЦІЯ І ФОРМАЛІЗАЦІЯ СЕТ-ОПЕРАЦІЙ

Рудницький В.М.
Черкаський державний технологічний університет, Черкаси, Україна
Лада Н.В.
Університет Аделаїди, Аделаїда, Південна Австралія

Теорія криптографічного кодування (від англ. Cryptographic Encoding Theory - CET) - розділ криптографії що дозволяє представити групи підстановок мовою дискретної математики і забезпечує їх синтез класифікацію, та методологію досліджень.

Основним об'єктом дослідження в теорії криптографічного кодування є СЕТ-операції. СЕТ-операції реалізують пронумерований набір елементарних функцій, кожна з яких формує відповідний вихідний Сі-квант (ci-quantum від англ. cryptographic information quantum - криптографічний інформаційний квант). При кожному виконанні СЕТ-операції кількість вхідних і вихідних Сі-квантів співпадають.

СЕТ-операції можна класифікувати по кількості операндів.

Одноопераднa СЕТ-операції ($C(x)$) представляє собою набір елементарних функцій які перетворюють nCi-квантів вхідної інформації.

$$C(x) = C\left(f_1(x_1, x_2, ..., x_n), f_2(x_1, x_2, ..., x_n), ..., f_n(x_1, x_2, ..., x_n)\right);$$

Двохоперандна СЕТ-операція ($C(x, y)$) – це операція яка перетворює nCi-квантів першого операнда в nCi-кванти результату на основі однієї з декількох одноопераднних СЕТ-операцій, в залежності від значення другого операнда.

$$C(x, y) = C(C_1(x), C_2(x), C_3(x), ..., C_p(x));$$

$$C(x, y) = \begin{cases} C_1(x), \text{ якщо } y_1 = 0;\ y_2 = 0; ...; y_m = 0 \\ C_2(x), \text{ якщо } y_1 = 0;\ y_2 = 0; ...; y_m = 1 \\ ..... \quad ..... \\ C_p(x), \text{ якщо } y_1 = 1;\ y_2 = 1; ...; y_m = 1; \end{cases}$$

Трьохоперандна СЕТ-операція це операція яка перетворює nCi-квантів першого операнда в nCi-кванти результату на основі однієї з декількох двохоперандних СЕТ-операцій, в залежності від значення третьогого операнда.

$$C(x, y, z) = C(C_1(x, y), C_2(x, y), C_3(x, y), ..., C_p(x, y))$$

$$C(x, y, z) = \begin{cases} C_1(x, y), \text{ якщо } z_1 = 0;\ z_2 = 0; ...; z_v = 0 \\ C_2(x, y), \text{ якщо } z_1 = 0;\ z_2 = 0; ...; z_v = 1 \\ ..... \quad ..... \\ C_h(x, y), \text{ якщо } z_1 = 1;\ z_2 = 1; ...; z_v = 1; \end{cases}$$

В доповіді деталізуються результати класифікації СЕТ-операцій.

ВБУДОВУВАННЯ ІНФОРМАЦІЇ В МЕДИЧНІ ЦИФРОВІ ОБЄКТИ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В IoT

Розломій І.О.
Черкаський національний університет ім. Б.Хмельницького, Черкаси, Україна
Люта М.В.
Черкаський державний бізнес-коледж, Черкаси, Україна

Перспективним є використання інтелектуальних пристроїв у різних сферах діяльності масштабі держави, зокрема. Передача, обробка та зберігання інформації в інфраструктурі IoT пов'язані з необхідністю вирішення низки завдань забезпечення інформаційної безпеки. Основна складність полягає в тому, що інфраструктура IoT неоднорідна і включає безліч різних пристроїв, у тому числі з обмеженими обчислювальними ресурсами. Одним із підходів до вирішення даних завдань є вбудовування додаткової інформації в цифрові об'єкти, що передаються та зберігаються.

У доповіді наведено огляд методів вбудовування інформації в цифрові медичні дані для забезпечення безпеки в IoT, що включає методи стеганографічного вбудовування інформації.

Метою доповіді є огляд існуючих методів стеганографічного захисту медичних цифрових об’єктів. Пропонується стеганографічний метод захисту медичної інформації, що підходить для передачі даних в IoT в реальному часі, наприклад, для систем моніторингу здоров'я. Зображення-контейнер у колірному просторі RGB розбивається окремі площині. Дані, подані у вигляді двійкового вектора, розбиваються на три вектори рівної довжини, які згодом мають бути вбудовані у відповідні площині з використанням одного й того самого ключа. Два адресні вектори, а саме: вектор основної адреси (MAV) і додатковий адресний вектор (CAV), – використовуються як псевдовипадкові адреси для адресації розташування пікселів у процесі приховування інформації. Вбудовування даних відбувається методом заміни двох чи трьох молодших бітів. Додатково у зображення-контейнер впроваджується крихкий ЦВЗ, призначений контролю цілісності даних після передачі. Даний метод не вимагає великих обчислювальних ресурсів, що робить метод застосовним для IoT. Інший стеганографічний метод захисту електронної інформації про здоров'я пацієнта в «інтернеті речей», що поєднує в собі застосування інтерполяції та модульної арифметики.

Список літератури

1. Hassaballah, M., Hameed, M. A., Awad, A. I., & Muhammad, K. (2021). A novel image steganography method for industrial internet of things security. IEEE Transactions on Industrial Informatics, 17(11), 7743-7751.

ТЕХНОЛОГІЯ СТИСНЕННЯ АВТОРСЬКИХ ТЕКСТІВ ЗА ДОПОМОГОЮ МАТРИЧНИХ РЕШІТОК

Науменко С.В., Розломій І.О.
Черкаський національний університет ім. Б. Хмельницького, Черкаси, Україна

Обсяги інформації, яка циркулює в сучасному інформаційному просторі, неухильно зростають. Незважаючи на постійне зростання апаратних можливостей обчислювальної техніки, потреба в компактному зберіганні інформації, зокрема текстової, стрімко підвищується. Проблема надійного зберігання інформації і захисту авторських прав текстових документів набуває все більшої актуальності. Головною особливістю авторських текстів є певна надмірність.

Вирішити задачу ефективного зберігання інформації покликані методи стиснення інформації – перекодування даних з метою зменшення їхнього об'єму. Розробка нових алгоритмів стиснення даних та удосконалення існуючих – вкрай актуальне завдання на сьогоднішній день.

Зараз велика увага приділяється статистичним та словниковим методам стиснення даних. Статистичні методи дозволяють більш компактно кодувати значення, що часто зустрічаються, прагнучи домогтися ступеня стиснення, що визначається ентропією сигналу. Більшість існуючих алгоритмів стиснення інформації базуються на відомому алгоритмі стиснення Хаффмана. Проте, попри переваги, модифікації алгоритмів Хаффмана мають недолік – застосовувати цей алгоритм недоцільно для окремих слів чи маленьких текстів, оскільки розмір тексту на виході виявиться значно більшим, ніж розмір тексту на вході.

Мета доповіді полягає у розробці методу стиснення тестової інформації на основі використання матричної решітки. Матрична решітка є прототипом шифрувальної решітки Кардано та побудована шляхом частотного аналізу тексту та виконання операцій матричного криптографічного перетворення. Запропонований метод стиснення авторських текстів, який забезпечуватиме надійну передачу та зберігання інформації є придатним для використання в різних інформаційних системах котрі потребують збереження даних без надлишковості.

Список літератури

1. Розломій І.О. (2022) Метод побудови матричних решіток Кардано для стиснення інформації. Вісник ХНУ. Технічні науки. №1(305). С. 85–90. DOI: https://www.doi.org/10.31891/2307-5732-2022-305-1-84-89

2. Розломій І.О., Науменко С.В. (2022) Методологія використання матричних решіток Кардано для комплексних систем захисту інформації. Комплексне забезпечення якості технологічних процесів та систем. Т. 2. С. 201.

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ВИЯВЛЕННЯ ПРОМИСЛОВОГО ШПИГУНСТВА

Шинкаренко А.В., Розломій І.О.
Черкаський національний університет ім. Б.Хмельницького, Черкаси, Україна

При ринковій конкуренції актуалізується проблема промислового шпигунства, яке є формою недобросовісної конкуренції для незаконного отримання відомостей про розробки, технології та іншої інформації однієї компанії іншій.

Виявити факт шпигунства можна застосувавши блокчейн-технології, що дозволяють зафіксувати факт використання пристроїв організації з метою передачі, копіювання або вилучення інформації. Хеш-суму записують у новий, новостворений log-файл, тим самим формуючи ланцюжок пов'язаних один з одним файлів. Якщо хтось спробує підмінити log-файл після його вивантаження, то факт заміни буде відразу помічений при наступній перевірці. Якщо отримана хеш-сума не збіглася з підсумковою, це є очевидною ознакою того, що стався факт несанкціонованого доступу (НСД) щодо інформації.

Блокчейн можна уявити, як ланцюг, що складається із блоків [1]. У кожному блоці зберігається необхідна інформація і хеш-сума, отримана шляхом конкатенації хеш-суми попереднього блоку та хеш-суми від інформації, отриманої для цього блоку.

Для більш точної роботи системи кожен співробітник повинен ідентифікуватись у системі за допомогою двофакторної аутентифікації. Для неї даними можуть виступати біометричні дані, наприклад, відбитки пальців, обличчя, сітківка ока, крім того можна використовувати пароль, який створив співробітник.

Блокчейн виступає у ролі ланцюжка блоків, що зберігає інформацію про всіх співробітників організації. Цей ланцюжок змінити або підробити неможливо, оскільки зміна одного запису спричинить зміну всього наступного ланцюжка. На зміну всього ланцюжка знадобиться багато часу і обчислювальних ресурсів.

Така система дозволить відстежувати дії співробітників на робочих місцях та запобігти передачі секретних даних. Користувачі у цій системі можуть бути анонімними свідками процесу обміну ключами, можуть підтверджувати угоди.

Список літератури

1. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.

QRNG WEB SERVICE SECURITY TESTING

Hrinenko T.O., Koptieva M.V.,
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
Nariezhnii O.P.,
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine

Internet services have many advantages, but as the number of applications increases, so do the number of cyber threats. Not only the number of attacks on web resources is increasing, but also the economic consequences of such attacks. Improvement of methods and systems for protecting web resources from attacks is an urgent scientific problem.

The object of the research is the construction of a secure web service for the quantum random number generator (Quantum Random Number Generation, QRNG). The subject of the study is methods and means of evaluating the protection of the QRNG web service.

Web service (web-service) is a program on the Internet that provides a service or responds to a certain user request. The web service for QRNG [1] generates and provides a random sequence upon user request on the Website.

The purpose of the work is to increase the level of security assessment of the web service for QRNG due to the improvement of methods and means of detecting potential threats based on the analysis and research of the current state and prospective methods of assessing threats to information resources and global practices of implementing information security management systems.

A threat model and an intruder model for the QRNG web service were built, and the results of a comparative analysis of modern web service security testing methods were provided, such as: "Technical Guide to Information Security Testing and Assessment" NIST SP 800-115 [2]; OWASP security testing methodology [3]; OSSTMM security testing methodology [4]; PTES penetration testing performance standard [5].

References

1. Grinenko T.O., Narezhniy O.P., Gorbenko I.D. Methods for measuring the noise power spectral density of the random number generator quantum radio optical system // Telecommunications and Radio Engineering. – Volume 76, 2017, Issue 7. pp. 635-651.

2. NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment, [Electronic resource] - Access mode: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

3. OWASP Testing Guide [Electronic resource] / Elie Saad, Rick Mitchell, Matteo Meucc - Access mode: https://owasp.org/www-project-web-security-testing-guide/

4. Open Source Security Testing Methodology Manual (OSSTMM) - Access mode: https://www.isc2.org/

5. Penetration Testing Execution Standard (PTES) [Electronic resource] / [Chris Nickerson, Dave Kennedy, et al.] - 2014 - Access mode: http://www.pentest-standard.org/index.php/Main_Page

АУДИТ ЗАХИЩЕНОСТІ СИСТЕМИ ЗАХИСТУ ПІДПРИЄМСТВА

Гринченко О.С., Гринченко Т.О.
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», Кривий Ріг, Україна

У сучасних умовах, коли інформаційні системи пронизують усі сфери діяльності підприємства і відкриті для реалізації внутрішніх і зовнішніх загроз, проблема інформаційної безпеки стає дуже важливою [1]. В роботі досліджено та проаналізовано відомі вразливості для комп‘ютерних мереж на основі дротових та бездротових технологій.

Об’єктом дослідження є аудит інформаційної системи підприємства, що на теперішній час є одним з найважливіших аспектів безпеки.

Предмет дослідження – методи та засоби проникнення в комп‘ютерні мережі.

Головна мета аудиту інформаційної безпеки, це оцінка рівня безпеки інформаційних систем підприємства для загального управління ним з урахуванням перспектив його розвитку [2, 3].

Проведений аналіз показав, що загальна структура роботи з аудиту включає наступний набір питань, які необхідно розглянути:

описати модель побудови системи інформаційної безпеки (ІБ), яка враховує загрози, вразливості, ризики та контрзаходи для їх зменшення або запобігання;

розглянути підхід до аналізу та управління ризиками;

окреслити основні поняття аудиту безпеки та описати цілі його реалізації;

зробити аналіз основних міжнародних та українських стандартів, що використовуються в аудиті інформаційної безпеки;

продемонструвати можливість проведення аудитів ІБ за допомогою програмних засобів;

навести практичні рекомендації щодо проведення аудиту ІБ на підприємствах.

Описана структура роботи з системою аудиту обрана з метою максимальної орієнтації на практичне використання матеріалу, що розглядається.

Список літератури

Сєвєрінов, О. В., Шевцов В. О., Сокол-Кутиловська А. С.. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка - 2017. - № 1. - С. 65-68.

Аудит безпеки інформаційних систем. Журнал ISACA. URL: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/information-systems-security-audit-an-ontological-framework.

Поддубний В.О., Сєвєрінов О.В. Менеджмент вразливостей в системах управління інформаційною безпекою. – ВА ЗС АР; НТУ" ХПІ"; НАУ, ДП" ПДПРОНДІАВІАПРОМ"; УмЖ, 2021.

АНАЛІЗ РІВНЯ БЕЗПЕКИ WEB-РЕСУРСІВ

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

В роботі розглянуті методи оцінки рівня безпеки web-ресурсів.

Аналіз показав, що основні області, де сайт може бути вразливим: системне адміністрування, програмна частина та серверна частина [1].

Найбільш поширені атаки на веб-ресурси [2]: 1) отримання доступу до бази даних за допомогою впровадження SQL-коду (SQL Injection). У своїй найбільш поширеній формі дана атака дає доступ до конфіденційної інформації. Спосіб захисту – ретельно обробляти вхідні параметри, значення яких використовуються для побудови SQL-запиту. 2) Міжсайтовий скриптинг. XSS (Cross Site Scripting) – тип атаки, при якій зловмисник впроваджує шкідливі скрипти у форми введення. Найчастіше при даній атаки відбувається крадіжка Cookies, де деякі сайти зберігають логіни і паролі (частіше їх геш коди) користувачів, і відповідно зловмисник може отримати доступ до вашого аккаунту. Захист від даних атак – валідація вхідних параметрів, тобто перевірка змінних, щоб вони містили коректний введення.

Метою дослідження є аналіз поточний стан безпеки web-ресурсів. У разі низького рівня захищеності Web-застосунків можлива реалізація загрози з боку зовнішнього порушника, наслідком цього може стати необхідність виділення додаткового бюджету на роботи з мінімізації ризиків [3].

Мета аналізу захищеності web-ресурсів полягає в підвищенні рівня безпеки програми в умовах обмеженого бюджету. Для цього найкраще організувати процес аналізу ресурсу методом «сірого ящика» з використанням інструментального підходу до його обстеження з частковими перевірками, виконаними вручну.

За підсумком роботи, можна зробити висновок, що загальний рівень захищеності веб- застосунків недостатньо високий. Для підвищення рівня безпеки слід проводити аналіз, виходячи з області дослідження. Так, якщо мета аналізу полягає в демонстрації можливості проникнення, порушення штатного режиму роботи програми або демонстрації компрометації чутливої інформації, тоді аналіз варто організувати за принципом «чорного ящика» без обмежень по проведеним перевіркам.

Список літератури

1. Web Application Security Statistics [Електронний ресурс] – Режим доступу до ресурсу: http://projects.webappsec.org/f/wasc-wafec-v1.0.pdf.

2. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі //Системи обробки інформації. – 2015. – №. 9. – С. 101-104.

3. Lysakov V., Sievierinov O., Taran I. Security of Web Applications Using AWS Cloud Provider //COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES. – 2021.

ТЕСТУВАННЯ ВРАЗЛИВОСТЕЙ СУЧАСНИХ ВЕБ-РЕСУРСІВ

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

З кожним роком кількість веб-ресурсів та кількість конфіденційної інформації з якою вони взаємодіють стає все більшою. За рахунок цього розвивається велика кількість нових кіберзагроз. Тому безпека веб-ресурсів займає дедалі більшу нішу в сучасності. Тестування допомагає у пошуку вразливостей, запобіганню загроз та забезпеченню безпеки веб-ресурсів [1].

Метою доповіді є дослідження вразливостей веб-ресурсів, що найчастіше використовуються.

В результаті дослідження було розглянуто найбільші ризики для безпеки веб-ресурсів, такі як Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components тощо [2]. В доповіді розглянута одна з найпоширеніших вразливість - Injection, що включає в себе ін'єкції різних типів (SQL, LDAP, XPath, OS commands). Реалізовані на практиці SQL-ін'єкції.

В роботі було проведено тестування на можливість SQL-ін'єкцій [3]. Також розглянуті різні програми для тестування [4, 5]:

SQL Injection Fuzz Strings (з інструменту wfuzz) – Fuzzdb;

Bernardo Damele AG: sqlmap, інструмент автоматичного впровадження SQL(підтримка великої кількості баз даних, підтримка Linux і Windows);

Muhaimin Dzulfakar: MySqloit, MySql Injection takeover tool (підтримка Linux).

Проведений аналіз показав, що для тестування найбільше підходить SQL Injection Fuzz Strings [5]. Вона підтримується в операційних системах Windows, Unix і Linux, має багатий функціонал, видає результат у реальному часі. Головним недоліком MySqloit є відсутність структурованої документації.

Усі програми тестування дозволяють підвищити безпеку веб-додатків шляхом знаходження його вразливостей у вигляді SQL-ін'єкцій.

Список літератури

1. Поддубний В.О., Сєвєрінов О.В. Менеджмент вразливостей як складова частина системи управління інформаційної безпеки. – НТУ «ХПІ», 2020.

2. OWASP Top Ten | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 03.10.2022).

3. Gupta S. SQL injection attacks. Berkeley, CA : Apress, 2020. URL: https://doi.org/10.1007/978-1-4842-6505-5 (дата звернення: 04.10.2022).

4. Sqlmap: automatic SQL injection and database takeover tool. sqlmap: automatic SQL injection and database takeover tool. URL: http://sqlmap.org/ (дата звернення: 06.11.2022).

5. GitHub - dtrip/mysqloit: Mysqloit v0.2. GitHub. URL: https://github.com/dtrip/mysqloit (дата звернення: 06.11.2022).

ВИЯВЛЕННЯ АТАК НА ВЕБ-РЕСУРСИ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Дацюк Д.О., Федюшин О.І., Наконечний М.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Нині технологій штучного інтелекту все більше проникають у сферу кібербезпеки. З одного боку, ці технології використовуються для протидії атакам і нейтралізації загроз. Однак, опинившись у руках зловмисників, технології штучного інтелекту стають небезпечною зброєю та становлять серйозну небезпеку [1].

В роботі розглянуто методи виявлення атак на веб-ресурси за допомогою штучного інтелекту.

Об'єктом дослідження є веб-сервери, системи, що призначені для взаємодії з користувачами через мережу Інтернет та показники кібер-атак на такі системи.

Предмет дослідження – методи виявлення атак з використанням штучного інтелекту.

Збільшення кількості кібер-атак, спроб несанкціонованого доступу до систем зумовили інтеграцію систем виявлення, попередження вторгнень в інформаційні системи та технологій штучного інтелекту [2].

В роботі розглядаються програмні засоби виявлення та попередження вторгнень (Intrusion Detection and Prevention Systems). Здійснюється порівняльний аналіз існуючих систем виявлення та попередження вторгнень та оцінюються їх показники. Розглядається можливість застосування штучного інтелекту в системах попередження вторгнень (AI-IDS) [2, 3]. Інтеграція штучного інтелекту в системи IDS дозволяє значно підвищити стійкість веб-системи не тільки до атак на основі відомих сігнатур, а й виявляти заплутані атаки на основі невідомих шаблонів.

Проведений аналіз показав, що використання штучного інтелекту допомагає захистити веб-ресурси від основних кібератак, таких як загрози спуфінгу, фішингу та інші. Це дозволить автоматизувати багато рутинних завданнь, які сьогодні забирають час та ресурси, наприклад, виявлення аномальної поведінки або виявлення підозрілих користувачів у мережі.

Список літератури

1. Ушатов В., Сєвєрінов О. В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. – 2019.

2. A. Kim, M. Park and D. H. Lee, "AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection," in IEEE Access, vol. 8, pp. 70245-70261, 2020, doi: 10.1109/ACCESS.2020.2986882.

3. Сєвєрінов О. В., Хрєнов А. Г. Аналіз сучасних систем виявлення вторгнень //Системи обробки інформації. – 2014. – №. 6. – С. 122-124.

ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНОЇ СИСТЕМИ НА НАЯВНІСТЬ ВРАЗЛИВОСТЕЙ

Кравець А.О., Олешко І.В.
Харківський національний університет радіоелектроніки, Харків, Україна
Сухотеплий В.М.
Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків, Україна

Зі збільшенням інформатизації суспільства збільшується вплив від атак на інформаційно-комунікаційні системи (ІКС). Тому процес виявлення вразливостей під час побудови та експлуатації ІКС може покращити їх захищеність та попередити атаки різного типу [1]. В роботі розглянуто методи оцінювання інформаційно-комунікаційної системи на наявність вразливостей.

Об'єктом дослідження є інформаційно-комунікаційні системи.

Предмет дослідження – методи оцінювання інформаційно-комунікаційних систем на наявність вразливостей.

Для покращення та уніфікації процесу перевірки й оцінки систем пропонується розробка методики тестування ІКС на проникнення, яка б надавала єдину оцінку та порядок дій тестування системи.

В роботі розглядаються програмні вразливості та вразливості пов'язані з налаштуванням програмних засобів, організаційні, апаратні, технічні, інженерно-технічні вразливості не розглядаються, їх перевірка повинна виконуватися окремою методикою у відповідності до нормативних документів України. Здійснений аналіз програмних засобів (всі засоби що наведені є вільно розповсюджувальними) та методів аналізу ІКС за допомогою наведених інструментів.

На основі аналізу результатів оцінки засобів та методів формується методика оцінки ІКС на наявність вразливостей. Сформовано інструкції, щодо обробки результатів перевірки, для отримання якісної оцінки стійкості системи. Також розглядаються методи інтеграції запропонованої методики в СУІБ та КСЗІ згідно стандартів та нормативної документації [2].

Така методика може використовуватися як для перевірки системи під час створення/модернізації СУЇБ/КСЗІ, або як частина менеджменту вразливостей програмного забезпечення в ІКС [3].

Список літератури

Поддубний В.О., Сєвєрінов О.В., Менеджмент вразливостей як складова частина системи управління інформаційної безпеки // Проблеми інформатизації: восьма міжнародна науково-технічна конференція. 2020 Том 1: секції 1-3 с. 98.

Сєвєрінов О. В., Черниш В. І., Молчанова М. Є. Управління інформаційною безпекою згідно міжнародних стандартів //Системи управління, навігації та зв'язку.–К: ДП «ЦНДІ НіУ».-2011.–Вип. – 2011. – Т. 4. – №. 20. – С. 250-253.

Poddubnyi V., Sievierinov O., Pustomelnik O. Менеджмент вразливостей як складова частина політики безпеки ІТС //Системи управління, навігації та зв'язку. Збірник наукових праць. – 2020. – Т. 4. – №. 62. – С. 55-58.

АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ВЕБ-РЕСУРСІВ

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

В даний час автентифікація є важливою процедурою для забезпечення конфіденційності, цілісності та доступності інформації користувачів у будь-яких системах чи ресурсах. Вона використовується повсякчас та всюди для здійснення контролю, обмеження як фізичного доступу до об'єкту, так і доступу до інформації в самій системі.

Об’єктом дослідження є сучасні методи автентифікації користувачів.

Предмет дослідження – процес автентифікації користувачів у веб-ресурсах. [1,2].

Зростання кількості використовуваних застосунків та стрімкий розвиток технологій сьогодення зумовлюють необхідність пошуку нових, якісніших методів захисту особистих даних в інформаційних системах. Умовна безпечність та необізнаність користувачів в сфері інформаційної безпеки, збільшує ризик несанкціонованого доступу до розміщеної на захищеному ресурсі інформації. Науково та практично доведено, що користувач є найбільш уразливим елементом системи.

Метою роботи є аналіз методів автентифікації у web-застосунках, та визначення найбільш ефективних с точки зору інформаційної безпеки.

У роботі виконано огляд та аналіз методів автентифікації у веб-ресурсах. Проведено аналіз методів автентифікації за критеріями: затребуваності з боку користувача та розробника, складності користування цими методами автентифікації, наявністю реалізованого протоколу, сфері використання, також були визначені переваги та недоліки цих методів.

Запропонований для використання комплексний метод автентифікації у веб-ресурсах, заснований на використанні багатокрокової та багатофакторної автентифікації з застосуванням біометричних методів та методів машинного навчання [3, 4].

Список літератури

1. A Review on Authentication Methods. URL: https://hal.archivesouvertes.fr/hal-00912435/PDF/A_Review_on_Authentication_Methods.pdf (дата звернення: 05.11.2022).

2 Authentication. URL: http://www.webopedia.com/TERM/A/authentication.html (дата звернення: 25.09.2020).

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

4. Martovytskyi V., Sievierinov O., Liashenko O., Koltun Y., Liashenko S., Kis V., Sukhoteplyi V., Nosyk A., Konov D., Yevstrat D. (2022). Devising an approach to the identification of system users by their behavior using machine learning methods // Eastern-European Journal of Enterprise Technologies, 3 (117), 2022, pp. 23–34.

УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ АБОНЕНТСЬКИХ ПРИСТРОЇВ У КОРПОРАТИВНИХ МЕРЕЖАХ

Сидоренко З.М., Мартовицький В.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Мобільні пристрої широко увійшли в побут суспільства, широко розповсюджуються IoT пристрої, починаючи з розумного дому, закінчуючи індикаторами догляду за рослинами. Все більше особисті мобільні пристрої використовуються не тільки для повсякденних цілей, а в тому числі і для виконання завдань професійної діяльності. Проте за підвищеною гнучкістю та зручністю криються серйозні прогалини з інформаційної безпеки [1, 2].

Одними з найбільших проблем, з якими стикається більшість компаній є вірусні та фішингові атаки, автоматичне завантаження недозволених додатків, атаки через небезпечні мережі.

В роботі розглянуто методи та політики управління безпекою мобільних пристроїв.

Об’єктом дослідження є мобільні пристрої в корпоративній мережі.

Предмет дослідження – процес управління.

В роботі розглянуто політики використання мобільних пристроїв, такі як: BYOD, CYOD, COPE, COBO, їх переваги та недоліки [1, 3]. Проведений аналіз показав, що кожна з розглянутих систем дозволяє забезпечити базовий набір функцій безпеки інформації. Але гостро стоїть питання побудови системи управління безпекою мобільних пристроїв.

Розглянуто ризики інформаційної безпеки при використанні мобільних пристроїв та можливі заходи їх обробки. Показані основні компоненти системи управління безпекою мобільних абонентських пристроїв у корпоративних мережах для забезпечення необхідного рівня інформаційної безпеки та відповідності міжнародним стандартам.

Запропоновано створення моделі корпоративної мережі, яка б забезпечувала безпечне використання пристроїв з оптимальним поєднанням показників безпеки, зручності використання та ціни експлуатації.

Список літератури

1. Нечволод К., Сєвєрінов О., Власов А., 2019. Аналіз безпеки даних в emm системах. Системи управління, навігації та зв’язку. Збірник наукових праць. 3, 55 (Чер 2019), 131-134.

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

3. Sean Bianco, CYOD: What Is It and How Is It Different from BYOD? URL: https://www.parallels.com/blogs/ras/cyod/

МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ ОПЕРАЦІЙНИХ ПРОЦЕСІВ ОРГАНІЗАЦІЇ

Петренко О.Є., Кригін В.Р.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті методи та засоби забезпечення безперервності операційних процесів організації.

Об'єктом дослідження є аналіз операційної систем організацій, що на теперішній час є одними з розповсюджених. Предмет дослідження – методи та засоби в операційних системах.

Операційна система — це система, яка використовує матеріальні, інформаційні або фінансові ресурси(«вхід») для перетворення їх в результат («вихід») у вигляді продукції або послуг. Виробниче перетворення може бути пов'язане з перетворенням матеріалів в процесі промислового виробництва, зміна місця розміщення в процесі транспортування, обміном в процесі торгової операції, зберіганням як процесом складського обслуговування, фізіологічним перетворенням як результат медичного обслуговування, перетворенням інформації в процесі послуги телекомунікації. Таким чином, виробниче перетворення, тісно пов"язане з поняттям бізнес-процеса.

Організаційні методи. Їх сутність полягає в тому, що кожна діяльність повинна бути правильно організованою, тобто спочатку потрібно створити фірму, підібрати персонал, дати йому завдання, показати, як діяти, і вже після цього керувати його діями. Організаційні методи управління передують діяльності, створюють для неї необхідні умови, і відповідно є пасивними, забезпечуючи базу для активних методів.

Безперервність бізнесу - це здатність організації продовжувати поставку продуктів і послуг в прийнятні терміни з заздалегідь визначеною продуктивністю під час збою.

В результаті проведеного аналізу методів та засобів забезпечення безперервності операційних процесів організації я виділив створення плану по забезпеченню стратегії запобігання, реагування та відновлення.

Список літератури

1. Jain A., Roy J., Cimon Y., A model for improving organizational continuity. (2013). P. 67.

2. Rapl K.L., Gregg D.R. (2015). Business Continuity Planning: A Project Management Approach, P. 402.

3. БАЄВА О.В., НОВАЛЬСЬКА Н.І., ЗГАЛАТ-ЛОЗИНСЬКА Л.О. (2017). Менеджмент і адміністрування: в 2 ч. — Ч. ІІ. — Менеджмент: навч. посіб., 326.https://maup.com.ua/assets/files/lib/book/men_adm_2.pdf.

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКІВ ТА МЕТОДИ ЇХ ВИРІШЕННЯ

Донченко А.О., Петренко О.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті існуючі вразливості веб-додатків та методи та механізми їх захисту

Об'єктом дослідження є процес виявлення вразливостей веб-додатків, які можуть нанести великі катастрофічні наслідки.

Предмет дослідження – методи та засоби запобігання вразливостей веб-додатків.

Веб-додатки вже давно є улюбленими мішенями зловмисників. Вони можуть забезпечити доступ до цінної інформації. Крім того, їх можна порівняно легко використовувати. Успішна атака може мати катастрофічні наслідки, включаючи фінансові збитки, втрату репутації бренду та довіри клієнтів. Деякі організації вже не можуть відновитись після серйозного порушення безпеки.

При розробці веб-додатків, веб-розробник повинен приділяти час веб-безпеки, будувати логіку та тестувати програмне забезпечення на вразливості. Якщо не приділити увагу веб-безпеки зловмисники можуть скористатися вразливістю сайту в своїх цілях, після чого компаній, що володіє сайтом, може понести великі витрати.

Щоб запобігти атакам, необхідно не тільки володіти інформацією, щодо існуючих атак але своєчасно впроваджувати механізми захисту. За допомогою сайту CWE можна дізнатися про нові або старі вразливості та статистику проведених атак. Кожен веб-розробник повинен розуміти і заздалегідь будувати логіку безпеки сайту, яка включає захист від атак, таких як xss, csrf, sql та ddos. В роботі розглянуто механізми захисту для веб-додатків та зроблено їх аналіз. Для ефективної безпеки веб-сайту необхідно приділяти особливу увагу до розробки всього веб-сайту: до веб-застосунку, конфігурації веб-сервера, політик створення та оновлення паролів, а також коду на стороні клієнта.

Список літератури

1. B. Blakely and C. Heath. Security design pattern,techreport g031. OpenGroup, 2004.

2. A. M. Braga, C. M. F. Rubira, and R. Dahab. Tropyc: A pattern language for cryptographic software. PLoP, 1998.

3. C. Dougherty, K. Sayre, R. C. Seacord, D. Svoboda, and K. Togashi. Secure Design Patterns. Software Engineering Institute, 2009.

АНАЛІЗ ПЕРСПЕКТИВНИХ МЕТОДІВ ПОШУКУ ВРАЗЛИВОСТЕЙ У КОРПОРАТИВНИХ МЕРЕЖАХ

Руженцев В.І., Поздняков Р.О.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті основні методи пошуку вразливостей у корпоративних комунікаційних мережах.

Об'єктом дослідження є процес побудови та функціонування корпоративної мережі підприємства та пошук розповсюджених вразливостей, що протидіють нормальній роботі мережі.

Предмет дослідження – методи та засоби розпізнавання і пошуку розглянутих вразливостей.

Оцінка захищеності корпоративної інфраструктури потребує часу та високої кваліфікації фахівців з ІБ. Використовуються засоби аналізу захищеності - спеціальні системи, які в автоматизованому режимі виявляють відкриті мережеві порти та доступні служби, уразливості в програмному забезпеченні, а також недоліки конфігурації обладнання, серверів та засобів захисту. Сучасні засоби аналізу захищеності дозволяють проводити сканування інформаційних систем у різних режимах залежно від конкретного завдання — мережне сканування, системні перевірки, контроль за відповідністю стандартам безпеки [1].

Методи відкритого пошуку і керування вразливостей у мережі дозволяють здійснити безперервний, про активний та автоматизований процес, який забезпечує захист комп'ютерних систем, мереж та корпоративних програм від кібератак і порушень безпеки даних [2]. Для керування загрозами та вразливостями, використовується низка інструментів і рішень для запобігання кіберзагрозам та їх усунення або превентивних дій для їх адміністрування.

В результаті проведеного аналізу, та вивченню основних типів загроз було виявлено основні критерії методів пошуку вразливостей, до яких входять: виявлення й інвентаризація ресурсів, сканування вразливостей, керування виправленнями, керування конфігурацією, керування інцидентами та подіями безпеки, тестові атаки та аналіз існуючих кіберзагроз. Сумісні з даними критеріями методології охоплюють найбільших спектр захищеності корпоративної мережі, виявлення відповідних вразливостей і превентивне реагування відповідні інциденти ІБ.

Список літератури

1. А. В. Жилін, О. М. Шаповал, О. А. Успенський "Технології захисту інформації в інформаційно-телекомунікаційних системах" – Київ – 2020 – С.38

2. N. Olifer, V. Olifer "Computer Networks: Principles, Technologies and Protocols for Network Design – Wiley, 2006. – С. 933-940.

ТЕСТУВАННЯ БЕЗПЕКИ МОБІЛЬНИХ ЗАСТОСУНКІВ

Сєвєрінов А.В., Бойко К.А., Федорченко В.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Постійний розвиток інформаційних технологій призвів до того, що мобільні пристрої часто використовують в якості мобільного офісу. В пам'яті пристрою зберігаються контакти колег, корпоративна переписка, банківські реквізити, нотатки. Безпека цієї інформації залежить у тому числі і від наявності вразливостей у встановлених на пристрій застосунках [1]. Тому задача забезпечення надійного захисту мобільного пристрою являється критично важливою.

В роботі розглянуті методи тестування безпеки мобільних застосунків.

Об'єктом дослідження є методи забезпечення безпеки мобільних застосунків. Предмет дослідження – процес тестування засобів безпеки програмного забезпечення мобільних пристроїв.

Багато мобільних застосунків встановлені на самому пристрої або можуть бути завантажені на нього з онлайн-магазинів, таких як App Store, Google Play, Windows Phone Store та інших, безкоштовно або за плату. Безпека прикладних програм - це комплекс заходів, які спрямовані на аналіз, виявлення та усунення вразливостей у застосунках та забезпеченні їхньої безпеки.

Проведений аналіз показав, що забезпечення безпеки охоплює заходи підвищення безпеки програми, зазвичай шляхом пошуку, виправлення та запобігання вразливостей системи безпеки [2, 3]. Для цього використовуються методи виявлення таких вразливостей на різних етапах життєвого циклу додатків, таких як проектування, розробка, розгортання, модернізація, технічне обслуговування. На кожному з цих етапів користувач може зіштовхнутися з певними проблемами, що здебільшого виникають у результаті реалізації програм, які у свою чергу служать для забезпечення певних потреб користувача.

В результаті проведеного аналізу засобів тестування безпеки програмного забезпечення був визначений перелік методів для ефективного тестування та надійного виявлення вразливостей мобільних застосунків.

Список літератури

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

2. Penetration Testing [Електронний ресурс]. - 2022 - Режим доступу до ресурсу: https://www.imperva.com/learn/application-security/penetration-testing/.

3. What is penetration testing? [Електронний ресурс]. - 2022 - Режим доступу до ресурсу: https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/

КОГНІТИВНІ ТА ЗМІШАНІ МЕТОДИ ОЦІНКИ ЗАХИЩЕНОСТІ АВТОМАТИЗОВАНОЇ СИСТЕМИ

Заболотний В.І., Совенко Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

У роботі розглянуте порівняння методів оцінки захищеності системи при створенні КСЗІ.

Об'єктом дослідження є процес оцінки захищеності автоматизованої системі при створенні комплексної системи захисту інформації.

Предмет дослідження – різновиди методів оцінки захищеності системи.

При створенні на об'єкті інформаційної діяльності комплексу технічного захисту інформації треба обстежити інфраструктуру та оцінити захищеність системи. На сьогоднішній день не існує уніфікованого метода цієї оцінки [1].

Когнітивні методи основані на орієнтовних графах. Їхні вершини являють собою концепти, а стрілки показують причинно-наслідкові зв'язки. Кожен такий зв'язок має свій коефіцієнт, що показує вплив одного фактору на інший [2]. Щоб зменшити вплив суб'єктивності думок експертів доцільно використовувати сірі когнітивні карти, які відрізняються використанням інтервальних чисел і в наслідок цього мають більш достовірний результат.

Змішані методи оцінки захищеності використовують як кількісні, так і якісні ознаки. Змішаний метод CRAMM дозволяє не тільки оцінити захищеність системи, а й виявити контрзаходи щодо них та економічно обґрунтувати необхідність їх вживання [3]. Метод складається з трьох частин, кожна з яких потребує своїх вихідних даних, що ускладнює його.

Порівняння когнітивних та змішаних методів оцінки захищеності дає зрозуміти, що перші з них більш гнучкі і дешеві, а при використанні відповідних когнітивних карт дають гарний результат. Однак, змішані методи є найбільш точними і представлені у вигляді програмних продуктів, що дозволяє автоматизувати процеси оцінки. У той же час вони потребують великої кількості вихідних даних, що вимагає багато часу та ресурсів.

Список літератури

1. Андрухів А.І., Тарасов Д.О. Порівняння Методів Оцінки Захищеності Корпоративних Інформаційних Систем. – 2006. – С. 1.

2. Saliieva O., Yaremchuk Yu. Determining the level of security of the information security system based on cognitive modeling // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 1, pp. 42-49. https://doi.org/10.18372/2225-5036.26.14669.

3. Buchik S., Shalayev V. The analysis instrumental methods of identification of risks of information security information and telecommunication systems. https://doi.org/10.18372/2310-5461.35.11841.

МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ANDROID ДОДАТКІВ

Федюшин О.І., Стригунов С.С.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянута операційна система Android, її механізми безпеки та вектори атак на мобільні додатки.

Об'єктом дослідження є широкий спектр атак на мобільні додатки. Предмет дослідження – методи захисту від MITM атак.

З кожним днем з'являються все більше додатків, які спрощують людям життя, але передають та зберігають велику кількість конфіденційних даних таких як паролі, банківські дані або відомості про користувача [1]. Дуже важливо бути впевненим в безпеці цих даних.

Розробникам варто слідкувати за безпекою свого продукту, так як зловмисники шукають та використовують вразливості як операційної системи, так і самого додатку [2].

В результаті дослідження атаки MITM [3] на один з додатків популярного міжнародного маркетплейса було виявлено, що дані передаються не в захищеному вигляді та без засобів безпеки від емуляції та брутфорсу облікових записів клієнтів, що дає змогу зловмисникам наносити мільйони доларів збитків щомісячно.

В рамках запропонованого дослідження була вирішена задача з організації безпечного обміну інформації з урахуванням компрометації центральної сторони інформаційної системи. Розроблений спосіб обміну ключової інформації на основі розділення секрету, що враховує можливу MITM атаку з боку центральної частини інформаційної системи. Проведений комплекс заходів дозволяє частково децентралізувати процес розподілення ключів шифрування, був протестований та показав високу ефективність. Запропонована схема обміну може бути використана в мережах загального доступу для обміну конфіденційною інформацією.

Список літератури

1. B. Schmerl et al., "Architecture Modeling and Analysis of Security in Android Systems", Software Architecture, pp. 274-290, 2016.

2. Нечволод К., Сєвєрінов О.В. Аналіз захищеності системи Android для використання в корпоративному сегменті. – 2019.

3. P. Gadient, M. Ghafari and O. Nierstrasz, Web APIs in Android through the Lens of Security. 2020.

АНАЛІЗ ВЛАСТИВОСТЕЙ ДЕЦЕНТРАЛІЗОВАНОГО ПРОТОКОЛУ КОНСЕНСУСУ ІЗ ПІДВИЩЕНОЮ ПРОПУСКНОЮ ЗДАТНІСТЮ

Дубіна В.В., Олійников Р.В.
Харківський національний університет радіоелектроніки, Харків, Україна

З моменту появи Bitcoin [1] та алгоритму Proof-of-Work (PoW) було проведено величезну кількість досліджень у спробах знайти нові механізми досягнення консенсусу. Перегляду піддалося все: пропускна здатність мережі, масштабування мережі, стійкість до цілого класу нових атак, характерних для блокчейн-мереж. На даний момент існує не так багато проектів із потенційно цікавими рішеннями цих проблем, але на певну увагу заслуговує алгоритм візантійської відмовостійкості (Byzantine Fault Tolerant, BFT) та його реалізація у протоколі Tendermint [2].

Метою доповіді є загальний огляд протоколів децентралізованого консенсусу і аналіз властивостей протоколу із підвищеною пропускною здатністю. В доповіді розглянуто існуючі рішення і досліджено роботу вузлів децентралізованої мережі на основі Tendermint протоколу в умовах високих навантажень.

Tendermint протокол забезпечує виняткову продуктивність. Пропускна здатність, яка перевищує 1000 транзакцій за секунду, забезпечується навіть у несприятливих умовах, коли валідатори транслюють зловмисні дії [2].

Отримані результати показали, що на рівні 1000 запитів у секунду один вузол вже не здатен повністю покрити кількість прямих запитів до нього. Система намагається продовжити підтримувати консенсус, однак при таких високих навантаженнях на один головний вузол мережі обмежується кількість звернень, які він здатен обробити.

Оптимальним рішенням щодо підвищення ефективності роботи у таких умовах запропоновано виконувати розбалансування навантаження або використовувати rpc-вузлів, а не тільки окремих валідаторів мережі.

Список літератури

1. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. 9 p.

2. Kwon J. Tendermint: Consensus without mining //Draft v. 0.6, fall. – 2014. – Т. 1. – №. 11.

МОДЕЛІ І МЕТОДИ RANSOMWARE АТАК В КІБЕРПРОСТОРІ

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

В роботі розглянуті моделі і методи Ransomware атак в кіберпросторі.

Об'єктом дослідження є процес розпізнавання діяльності Ransomware атак в кіберпросторі.

Предмет дослідження – моделі і методи реалізації Ransomware атак.

Ransomware – це зловмисне програмне забезпечення, призначене для заборони доступу користувача або організації до файлів на їх комп'ютері. Шифруючи ці файли та вимагаючи викупу за ключ дешифрування, кібератаки ставлять організації в положення, коли сплата викупу є найпростішим і найдешевшим способом відновити доступ до своїх файлів[1,2]. Деякі варіанти атак додали додаткові функції, такі як крадіжка даних, щоб заохочувати жертв програм-вимагачів платити викуп. Програми-вимагачі швидко стали найпоширенішим і найпомітнішим типом шкідливих програм.

Щоб захиститись від зараження програмами-вимагачами, рекомендується зберігати пильність та використовувати програми безпеки. У жертв програм-здирників є три варіанти дій після зараження: можна заплатити викуп, спробувати видалити шкідливу програму або перезавантажити пристрій. Вектори атак, що використовуються троянами-здирниками, включають, в основному, протокол віддаленого робочого столу, фішингові повідомлення електронної пошти та вразливість програмного забезпечення [3].

В роботі розглянуті такі сімейства програм-вимагачів, а саме: Ryuk, Maze, REvil (Sodinokibi), Lockbit, DearCry, Lapsus$. Загалом вони відносять до типів вірус Locker та крипто-вимагач. Головна ідея вірусу Locker- це блокування робочого стола та покриття його банером з вимогою викупу. Крипто-вимагач – шифрує файли та змінює їх розширення, для розшифрування потрібно заплатити викуп. Сучасні варіанти програм-вимагачів зазвичай викрадають конфіденційні дані компанії перед їх шифруванням. В дослідженні проаналізовані основні вектори атак та способи їх детектування, розроблений фреймворк для класифікації та оцінки наслідків їх злочинної діяльності.

Список літератури

1. Liska A. Ransomware. Defending Against Digital Extortion / A. Liska, T. Gallo., 2017. – 174 с.

2. A. Hassan N. Ransomware Revealed / Nihad A. Hassan., 2019. – 229 с.

3.A. Grimes R. Ransomware. Protection Playbook / Roger A. Grimes., 2022. – 323 с.

ДОСЛІДЖЕННЯ МОДЕЛІ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ХМАРНИХ СЕРВІСІВ

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

В роботі розглянута модель безпеки розташування файлів у хмарному сховищі на основі використання двофакторної автентифікації та симетричного шифруванням.

Об'єктом дослідження є моделі безпеки при використанні хмарних сервісів.

Предмет дослідження – процес двофакторної автентифікації користувачів хмарних сервісів з використанням шифрування файлів при розміщенні у хмарному сервісі.

На сьогодні, сформувалося три основні моделі розгортання хмарних сервісів IaaS, PaaS та SaaS. Основним питанням, на сьогодні, є безпека даних користувача, що взаємодіє з хмарним сервісом [1, 2].

Для підвищення безпеки при використанні хмарних сервісів запропонована модель безпеки, що складається з двох складових:

використання двофакторної автентифікації (2FA) із застосуванням одноразового паролю (OTP);

шифрування файлів при розміщенні у сховищах хмарних сервісів.

Для визначення ефективності запропонованою моделі було проведено порівняння одноразового паролю, ПІН-коду та статичного паролю у якості системи автентифікації с розрахунком ентропії методів автентифікації [2]. Також, було проведено тести NIST для визначення ефективності алгоритмів шифрування AES, RC6, 3DES, MARS, DES, Blowfish, RC4, Twofish для запропонованої моделі.

В результаті проведеного дослідження було встановлено, що ентропія one-time password у більше ніж 2 рази краща ніж у статичного пароля, та 8 разів – ніж у ПІН коду. По результатам дослідження методів шифрування файлів найкращі показники має алгоритм AES.

Таким чином, запропонована модель безпеки даних вирішує проблеми захисту інформації користувачів хмарних сервісів і допомагає постачальнику хмарних послуг вибрати найбільш підходящий алгоритм шифрування.

Список літератури

1. National Institute of Standards and Technology [Електронний ресурс] – Режим доступу до ресурсу://www.nist.gov..

2. V. Prakash, A. Infant, J. Shobana, Eliminating vulnerable attacks using One-Time Password and PassText—Analytical study of blended schema, Universal Journal of Computer Science and Engineering Technology 1 (2010) 133-140.

3. Andrew Rukhin,Juan Soto,James Nechvatal and others. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST, Special Publication 800-22 Revision 1a, April2010, 131 p.

МОДЕЛЬ ТА МОВА ФОРМАЛЬНОГО ОПИСУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ

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

В роботі розглянуто моделі та мова побудови формального опису інформаційно-комунікаційної системи.

Об'єктом дослідження є інформаційно-комунікаційні системи.

Предмет дослідження – процес формального опису інформаційно-комунікаційної системи.

Під час побудови систем захисту інформації в інформаційно-комунікаційних системах (далі – ІКС) розробники повинні вирішувати безліч проблем пов'язаних з описом ІКС. Одна з таких проблем – створення опису ІКС та механізмів захисту, який би повністю відображав систему, інформацію та зв'язки між об'єктами системи [1].

В роботі запропонована модель формального опису ІКС з використанням об'єктного запису даних та графічного відображення за допомогою мов формального проектування. Така модель має вигляд у формі графу, вершини якого є об'єктами з регламентованим описом.

Розглянуто існуючі мови формального опису ІКС. Запропоновано структуру нової мови формального опису ІКС на заміну існуючим, так як вони не були розроблені під завдання опису ІКС, тому містять надлишковість полів та ускладнену структуру взаємозв'язків. Запропонована мова створена виключено під конкретні завдання: покращення зв'язності об'єктів, опис їх характеристик з погляду інформаційної безпеки.

В роботі розглядається можливість використання запропонованої моделі для симуляції кібератак. Кожна атака має «точку входу» за допомогою теорії графів можливо здійснювати обхід графу для визначення можливих шляхів горизонтального або вертикального розповсюдження кібератаки [2].

Запропонована модель може покращати точність опису ІКС, допомогти в моделюванні кібератак та пришвидшити розробку систем захисту інформації.

Список літератури

1. Гвоздьов Р. Ю., Сєвєрінов О. В., Караваєв В. М. Методика формального проектування комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – ХНУРЕ, 2021.

2. Поддубний В., Сєвєрінов О., Пустомельник О. Менеджмент вразливостей як складова частина політики безпеки ІТС // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2020. – Т. 4 (62). – С. 55-58.

МЕТОД ШИФРУВАННЯ НА ОСНОВІ БАГАТОПАРАМЕТРИЧНИХ ГРУП

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

В роботі розглянуто методи шифрування на основі багатопараметричних груп.

Об'єктом дослідження є алгоритми шифрування та електронного підпису на основі криптосистеми MST3.

Предмет дослідження – процес аналізу стійкості математичних перетворень на базі багатопараметричних груп.

Зі стрімким розвитком квантових технологій, квантових комп'ютерів, що базуються на цьому явищі, виникла необхідність у нових криптоалгоритмах, що будуть стійкими до квантового криптоаналізу.

Стійкість криптографічних систем на багатопараметричних групах базується на задачі розкладання елемента такої групи по набору елементів логарифмічною підпису. До теперішнього часу відома тільки одна реалізація криптосистеми MST3, побудованої за Абелевим центром групи Судзукі [1].

Проблема побудови багатопараметричних груп на практиці полягає в розробці ефективного алгоритму для відображень числа на групу і зворотного відображення з обчислювально простою груповою операцією.

В роботі розглядаються алгоритми побудови та використання криптосистеми MST3 для шифрування та електронного підпису [2, 3]. В роботі був виміряний час генерації ключових даних, виконання шифрування та розшифрування у порівнянні з криптосистемою RSA. Також наводиться час генерації ключових даних, створення та перевірки електронного підпису. Здійснюється аналіз щодо можливої стійкості проти квантовий алгоритму Шора – розв'язку дискретного логарифму в скінченному полі [4].

Список літератури

1. Khalimov G. et al. Encryption Scheme Based on the Automorphism Group of the Suzuki Function Field //2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T). – IEEE, 2020. – С. 383-387.

2. Haibo Hong, Jing Li, Licheng Wang, Yixian Yang, and Xinxin Niu. A Digital Signature Scheme Based on MST3 Cryptosystems. – 2014.

3. Khalimov G. et al. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement //2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4). – IEEE, 2021. – С. 204-211.

4. Marrtin Ekera Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. – 2020.

АНАЛІЗ ЗАСТОСУВАННЯ ГЕНЕРАТИВНО-ЗМАГАЛЬНИХ МЕРЕЖ У СФЕРІ КІБЕРБЕЗПЕКИ

Ляшенко О.С., Щербина Д.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті передумови виникнення генеративно-змагальної мережі (GAN), її архітектури та концепції основ безпеки системи, розглянуті найсучасніші методи захисту безпеки, які були налаштовані за допомогою GAN.

Об'єктом дослідження є спектр різних застосувань GAN у сфері кібербезпеки. Предмет дослідження – методи та підходи застосування GAN в атаках на інформаційні системи та їх запобігання.

GAN є відносно новою технологією, тому дослідження додатків безпеки на основі цієї технології також почалися нещодавно [1]. Застосування GAN для безпеки можна розглядати як дуже потужний крок вперед і цінний інструмент для аналізу та застосування до проблем кібербезпеки. На сьогодні GAN показали перспективу у створенні нових методів захисту у сфері кібервторгнення, виявлення зловмисного програмного забезпечення та захищеної стеганографії зображень, хоча відповідні дослідження були обмеженими. З точки зору атаки на безпеку, багато доступних досліджень було зосереджено на створенні шкідливих програм для IDS. Нові генеровані атаки або зловмисне програмне забезпечення надають інформацію про раніше невідомі атаки і, таким чином, допомагають оновити механізми захисту.

У роботі розглянуті останні дослідження GAN від стеганографії зображень і нейронної криптографії до генерації зловмисного програмного забезпечення з метою навчити систему краще захищатися під час несприятливих сценаріїв атак. Показані різні дослідницькі можливості для поєднання генеративно-змагальних мереж із кібербезпекою.

У роботі проведений аналіз різних типів і варіацій GAN, які використовувалися дослідниками для вирішення значущих сценаріїв безпеки [2]. Докладно розглядається використання GAN для покращення спостереження в таких сферах, як протоколи безпеки та посилення систем виявлення для боротьби з конфіденційністю даних, роботи над створенням кращої системи виявлення вторгнень, безпечної стеганографії зображень, нейронної криптографії та аналізу безпеки.

Список літератури

1. I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio «Generative Adversarial Networks» NIPS'14: Матеріали 27-ї Міжнародної конференції з нейронних систем обробки інформації, 2014, с. 2672–2680.

2. H. Chen, L. Jiang «Efficient GAN-based method for cyber-intrusion detection» arXiv, 2019.

ПОБУДОВА SIEM СИСТЕМИ ЗАХИСТУ ELASTICSEARCH

Гріненко Т.О., Федоров І.А., Калмиков Д.І.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Вразливості в системах інформаційних технологій (IT), недосконале програмне забезпечення, людський фактор – можуть призвести до серйозних втрат з боку бізнесу, а саме, зламу системи IT, крадіжки персональних даних тощо. Для запобігання або упередження інцидентів інформаційної безпеки були розроблені SIEM системи (Security Information and Event Management, SIEM). Технологія SIEM забезпечує аналіз у реальному часі подій (загроз) безпеки, що виходять від мережевих пристроїв та додатків, і дозволяє реагувати на них, з метою запобігання або зменшення істотних збитків.

На жаль, дуже мало підприємств розуміють важливість та необхідність використання SIEM систем для впровадження, підтримки, контролю та постійного вдосконалення системи менеджменту інформаційної безпеки підприємства. SIEM система фіксує всі події (збирає дані), що відбуваються в мережі, і надає їх користувачу в максимально зручному для сприйняття вигляді. Для кожного конкретного випадку та цілей, SIEM система виглядатиме порізному [1].

Метою доповіді є побудова лабораторної мережі з SIEM системою Elasticsearch [2, 3], що відповідає вимогам стандарту ISO/IEC 27001 [4], і надає можливість отримати навички роботи з SIEM системою, а саме: аналіз логів, реагування на інциденти інформаційної безпеки, розробка та обґрунтування правил моніторингу системи для утиліти Sysmon, розслідування інцидентів інформаційної безпеки, документування інцидентів, документування даних для аналізу.

В доповіді наведені результати аналізу міжнародного стандарту ISO/IEC 27001, результати аналізу та дослідження SIEM системи Elasticsearch, надано рекомендації щодо ефективної роботи з SIEM системою Elasticsearch, а саме: рекомендації з оптимальної конфігурації утиліти моніторингу системи Sysmon, наданий детальний опис алгоритму підняття стеку ELK (elasticsearch, logstash, kibana), наводиться демонстрація обробки та пересилання системних логів Windows 10 на logstash та їх аналіз через kibana.

Список літератури

1. https://softlist.com.ua/articles/chto-takoe-siem-sistema
2. https://www.elastic.co/
3. https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-22-04
4. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

ВИЯВЛЕННЯ ЗАГРОЗИ CVE-2020-1472 ЗА ДОПОМОГОЮ IDS/IPS SNORT

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

На теперішній час можливості систем виявлення вторгнень є необхідним критерієм щодо інфраструктури захисту інформації в корпоративної мережі компанії.

В роботі побудована модель корпоративної мережі компанії з контролером домену Active Directory та систему активного реагування на інциденти Snort [1].

Об'єктом дослідження є вразливість у протоколі автентифікації Netlogon, який використовується у контролері домену Windows Server.

Служба Netlogon RPC, яка використовується для автентифікації комп'ютера та користувача в Windows, також дозволяє комп'ютеру оновлювати пароль свого комп'ютера в домені. Через низку історичних причин ця служба не використовує стандартні протоколи автентифікації для автентифікації комп'ютера. Уразливість існує в нестандартному методі автентифікації. CVE-2020-1472 - це вразливість підвищення привілеїв із-за небезпечного використання шифрування AES-CFB8 для сеансів Netlogon [2]

Система запобігання вторгненням (IPS) є розширенням рішення IDS. IPS здатна автоматично налаштовувати брандмауер та скидати сеанси на основі загроз у реальному часі. Вона використовується для знаходження аномальної поведінки у мережі та виявлення вторгнень. [2, 3]

В доповіді розповідається робота алгоритму автентифікації Netlogon, як перевірити, чи вразливий ваш домен Active Directory до CVE-2020-1472, проведена робота з аналізу трафіку, який генерується зловмисником та написані правила реагування на цю вразливість.

Список літератури

1. Snort 3 is available! [Електронний ресурс] – Режим доступу: https://www.snort.org/.

2. Netlogon Elevation of Privilege Vulnerability CVE-2020-1472 [Електронний ресурс] – Режим доступу: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472.

3. Сєвєрінов О. В., Хрєнов А. Г. Аналіз сучасних систем виявлення вторгнень // Системи обробки інформації. – 2014. – №. 6. – С. 122-124.

4. Intrusion Detection System (IDS) [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/intrusion-detection-system-ids.

ТЕСТУВАННЯ ТА АНАЛІЗ РИЗИКІВ БЕЗПЕКИ КОНТЕЙНЕРІВ НА ОСНОВІ DOCKER

Федюшин О.І., Мороз А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті вразливості та ризики при використанні контейнерів на основі Docker.

Об'єктом дослідження є використання контейнерів на базі Docker, що зараз є одним із найпоширеніших типів. Предмет дослідження – тестування на вразливості контейнерів на основі Docker [1, 2].

При порівнянні звичайної технології віртуалізації та технології контейнерів Docker - основна різниця в технологіях, на яких базується Docker, а саме namespace та cgroups, що включає ізоляції процесів, файлової системи, пристроїв, між процесної взаємодії, мережі та обмеження ресурсів.

У середовищі Docker, кожен контейнер використовує ядро операційної системи, а сам контейнер є лише кілька процесів, запущених на host системі. Його безпека, особливо ізоляція, теоретично і практично відрізняється від традиційних віртуальних машин.

В результаті дослідження виявлено, що в порівнянні з технологією віртуалізації, контейнерна технологія Docker відрізняється гнучкістю і легкою вагою, і вона незамінна при просуванні хмарних додатків. Але прагнення високої ефективності приводить до втрати повної ізоляції. З точки зору безпеки маємо багато недоліків у порівнянні з технологією віртуалізації, а саме захист зображень контейнерів, безпека ядра, безпека мережі, безпека віртуалізації, безпека під час виконання та інші аспекти.

Для усунення недоліків в роботі з точки зору безпеки потрібно розглядати основні вектори атак, виходячи з яких можна запропонувати методи захисту [3, 4] (контроль доступу, ізоляція та обмеження ресурсів, сканування образів, моніторинг контейнерів, захист при передачі образів, аудит безпеки, контроль мережі та інші) та їх реалізації. Для моделювання атак було розгорнуто тестове середовище, оцінені потенційні вразливості та ризики безпеки. Основна ідея – автоматизація тестування за допомогою програмних засобів.

Список літератури

1. CVE -search results. CVE -CVE. URL: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=docker (дата звернення: 05.11.2022).

2. Docker: accelerated, containerized application development. Docker. URL: https://www.docker.com/ (дата звернення: 05.11.2022).

3. Kubernetes. Kubernetes. URL: http://kubernetes.com/ (дата звернення: 05.11.2022).

4. Безопасность Docker. Защита инфраструктуры на Docker. TECH GEEK. URL: https://tech-geek.ru/docker-security/ (дата звернення: 05.11.2022).

DEVELOPMENT OF INFORMATION PROTECTION METHODS IN OPTICAL TEXT RECOGNITION SYSTEMS

Bilozerskyi V.
National aerospace university H.E. Zhukovsky «Kharkiv aviation institute»,
Kharkiv, Ukraine

The development of innovative information processing methods, based on the use of artificial intelligence systems and deep learning neural networks, has significantly influenced both the emergence of the latest purely scientific approaches and algorithms, and the growth of practical applications in various fields of activity. In the task of image recognition, this, in particular, led to the introduction of algorithms and programs for optical text recognition (OCR). However, modern systems have a number of significant drawbacks. First of all, it is the scarcity of 100% guarantee of correct text recognition and the impact of the source data quality on the results of the program (for example, different lighting conditions when photographing documents, geometric distortion of images, noise effects, etc)[1]. But the key disadvantage is the complete or partial absence of measures to protect the recognized text information, in the case of sharing ones confidential data via open communication channels.

The objective of this research is to develop a combined method of information security in optical text recognition systems using QR codes and further masking the fact of data transmission via open communication channels using various methods of LSB steganography [2].

This research report presents the results of studies to assess the practical effectiveness of the proposed method both in terms of the reliability of transmitted data encoding/decoding and in terms of the information transmission secrecy [3]. The data show that the methods of encoding and hidden transmission of text information using QR codes and LSB steganography are universal and can be used to build new and to modernize existing optical text recognition systems.

References

1. Dergachov K., Krasnov L., Bilozerskyi V., Zymovin A. Data pre-processing to increase the quality of optical text recognition systems. Радіоелектронні і комп'ютерні системи. 2021. № 4(100). P. 183-198. DOI: https://doi.org/10.32620/reks.2021.4.15.

2. William P.. Assessment of Hybrid Cryptographic Algorithm for Secure Sharing of Textual and Pictorial Content. International Conference on Electronics and Renewable Systems (ICEARS). 2022. P. 918-922. DOI: 10.1109/ICEARS53579.2022. 9751932.

3. Dergachov K., Krasnov L., Bilozerskyi V., Zymovin A. Development of tools for information protection of optical text recognition systems. Радіоелектронні і комп'ютерні системи. 2022. № 2(102). P. 159-177. DOI: https://doi.org/10.32620/reks.2022.2.13.

ПОРІВНЯЛЬНИЙ АНАЛІЗ ДСТУ З КІБЕРЕЗПЕКИ

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

На сьогодні захист даних в комп'ютерних мережах становить одну з найбільш гострих проблем сучасного інформаційного простору і важливість цього питання лише зростає.

Нормативні документами що визначають основні функції системи захисту інформації постійно удосконалюються. З 1999 року Україна почала перехід на єдині критерії оцінки безпеки інформаційних технологій ISO 15408 [1], що застосовуються на світовому рівні, та визначила основні функції системи захисту інформації "Критерії захищеності інформації в комп'ютерних системах від несанкціонованого доступу" НД ТЗИ 2.5004-99 [2]. Але лише зараз цей перехід було остаточно проведено. З 1 листопада 2022 року набуває чинності пакет відповідних нормативних документів [3], а саме ціла низка ДСТУ, що стосуються кібербезпеки, в тому числі електронного цифрового підпису. Введення нових стандартів потребує аналізу. З одного боку виникає питання: що саме повинно змінитися. З іншого боку – як ці зміни вливають на стан кібербезпеки.

Взагалі, критерії визначають, що для перекриття загроз порушення конфіденційності, цілісності та доступності необхідно реалізувати в інформаційних технологіях комплекс засобів захисту інформації (сукупність інформаційних, інженерних і програмно-апаратних засобів, що забезпечують захист інформації).

Метою доповіді є порівняльний аналіз ДСТУ з симетричного та асиметричного шифрування (в тому числі електронний цифровий підпис) за останні 20 років [4] та надання рекомендацій щодо застосування ДСТУ за 2022 рік. Треба зазначити, що деякі ДСТУ були прийняті вперше і порівнювати їх можливо лише з відповідними міжнародними ISO [5].

Список літератури

1. Common Criteria for Information Technology Security Evaluation (CCITSE) V2.1 // 1998.

2. Критерії захищеності інформації в комп'ютерних системах від несанаційного доступу. НД ТЗИ 2.5004-99. DOI: https://tzi.com.ua/downloads/2.5-004-99.pdf

3. Про прийняття та скасування національних стандартів. DOI: ttps://zakon.rada.gov.ua/rada/show/v0185774-22.

4. Огляд законодавства України в сфері інформаційної безпеки. Ч. 9: Стандарти криптографічного захисту // 2015. DOI: https://digital.report/zakonodatelstvo-ukrainyi-standartyi-kriptograficheskoy-zashhityi/.

5. Перспективи застосування міжнародного стандарту ISO/IEC 15408 в Україні // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 3, 2001 р. DOI: https://ela.kpi.ua/bitstream/123456789/15319/1/03_p7.pdf

НЕОБХІДНІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ В СУЧАСНИХ УМОВАХ

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 силового, політичного та інформаційного характеру з боку Російської Федерації (РФ) дуже гостро стоїть питання щодо захисту інформації при функціонування різних інформаційних систем (систем як державного так і військового управління) від впливу інформаційних засобів (методів, програм), що наносять шкоду інформації, яка циркулює в них. За таких умов виконання заходів щодо захисту інформації в інформаційних системах (ІС) держави має визначальне значення [1-3].

Метою доповіді є формування пропозицій щодо визначення основних положень щодо захисту інформації в ІС, при їх функціонуванні в умовах жорсткого інформаційного протиборства з РФ.

В доповіді надані пропозиції щодо необхідності впровадження адаптованої системи захисту інформації (СЗІ) в ІС, з врахуванням дії конкретних загроз, що впливають на їх функціонування. З системних позицій до загроз, що впливають на інформацію в ІС відносяться наступні групи: люди; технічні засоби; моделі, алгоритми, програми; зовнішнє довкілля. Вибір стратегії захисту інформації в ІС в загальному виді повинен представляти собою пошук компромісу між необхідним ступенем захисту інформації в ІС та потрібними для реалізації цих цілей ресурсами. Таким чином, необхідність захисту інформації в ІС в сучасних умовах, визначається веденням жорсткого протиборства в інформаційній сфері з РФ та реалізовується через відповідну СЗІ, яка є сукупністю всіх засобів, методів та заходів, щодо захисту інформації в ІС.

Список літератури

1. Roy, Y. V., Mazur, N. P., & Skladannyi, P. M. (2018). Аудит інформаційної безпеки – основа ефективного захисту підприємства. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка, 1(1), 86-93. https://doi.org/10.28925/2663-4023.2018.1.8693

2. Війни інформаційної епохи: міждисциплінарний дискурс: монографія/ за ред. В.А. Кротюка. Харків: ФОП Федорко М.Ю., 2021. 558 с. ISBN 978-617-7664-71-9.

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.

ТЕХНОЛОГІЇ ПОКРАЩЕННЯ АУТЕНТИФІКАЦІЇ ЛЮДИНИ

Бовчалюк С.Я., Бондар О.Р.
Харківський національний університет радіоелектроніки, Харків, Україна

Обмеження доступу до особистих даних, чи конфіденційної інформації є невід'ємною складовою сьогодення. Наразі для вирішення цієї проблеми використовується значна кількість підходів, методів та алгоритмів, таких як паролі, ключі шифрування, якими може володіти певна група осіб, або ж біометричні дані, що є унікальними для кожної людини [1]. Проте зловмисники, які бажають отримати доступ до конфіденційних даних постійно вдосконалюють свої підходи: методи обходу захисту розвиваються дуже швидко, шахраї виманюють паролі користувачів обманом, системи основані на біометричних даних обходяться, хоча це і вимагає значних зусиль. Все це призводить до появи нових ризиків потрапляння особистих даних до небажаних рук, і вимагає перегляду і вдосконаленню існуючих методів аутентифікації.

Метою доповіді є аналіз існуючих методів аутентифікації людини, що широко використовуються у сучасному світі. Пропонується розгляд можливих варіантів їх удосконалення для забезпечення більшої надійності.

Класичні методи аутентифікації, зазвичай, базуються на статичних даних, це можуть бути паролі, фото обличчя, відбитки пальців [2]. Такі дані є очевидною ціллю, що необхідно подолати шахраям для доступу до отримання чужих даних. Останнім часом все частіше стала використовуватись двофакторна аутентифікація, яка вимагає від користувача, окрім основного, встановити ще один додатковий метод. Такий підхід безумовно значно покращив безпековий аспект аутентифікації, проте змушує балансувати між тим, щоб зробити процес більш надійним, але й не зробити його дуже складним та часовитратним для користувача. У доповіді наводяться перспективні підходи і технології для покращення результатів цього процесу. Різноманітні додаткові дані про користувача можуть зіграти визначальну роль в розвитку процесу аутентифікації. До прикладу, система може опиратись на місце знаходження людини за IP-адресою, ідентифікаційні параметри пристрою, з якого був здійснений вхід до системи, чи навіть дії, які виконує користувач, який вже зміг увійти до системи. Всі ці фактори можуть слугувати важливими індикаторами, для тимчасового блокування доступу, якщо людина використовує її з незвичного місця, чи робить невластиві їй речі.

Список літератури

1. Smith, R. E. Authentication: from passwords to public keys. Addison-Wesley. 2002.

2. Jha A., A A., Verma L. Biometric Authentication. YMER Digital. 2022. Т. 21, № 05. С. 1041–1049. URL: https://doi.org/10.37896/ymer21.05/b9 (дата звернення: 27.10.2022).

АНАЛІЗ МЕТОДІВ ТА ШЛЯХІВ ВИРІШЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Філіпчук П.П., Філіппенко І.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Термін «захист інформації» визначає сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації[1].

У широкому розумінні захист інформації являє собою протистояння користувачів, володільців інформації і зловмисників. Щодо певної інформації зловмисник виступає як суб'єкт, який незаконним шляхом намагається добути, змінити або знищити інформацію користувачів.

Метою доповіді є аналіз сучасних методів інформаційної безпеки інформаційно-телекомунікаційних систем в межах визначення рівня загроз.

В доповіді запропоновується системний підхід, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних та програмних засобів, організаційних заходів тощо). Комплексний характер дозволяє здійснити більш надійний захист від дій зловмисників, які прагнуть будь-якими засобами добути важливу для них інформацію[3].

Захищена інформаційно-телекомунікаційна система повинна володіти принаймні наступними властивостями[2]:

здійснювати автоматизацію певного процесу обробки інформації, включаючи всі аспекти цього процесу, які пов'язані з забезпеченням безпеки оброблюваної інформації;

успішно протистояти загрозам безпеки інформації, що діють в певному середовищі;

відповідати вимогам і критеріям загальноприйнятих стандартів із захисту інформації.

Отже, організація надійної та ефективної системи захисту є одним з найважливіших завдань щодо забезпечення збереження інформації в мережі. Застосування ефективних засобів захисту інформаційно-телекомунікаційних систем дозволить зменшити сумарні втрати від комп'ютерних злочинів, пов'язаних з несанкціонованим доступом до інформації.

Список літератури

1. Остапов С.Е. Технології захисту інформації: навч. посіб. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с.

2. С. Бармен. Розробка правил інформаційної безпеки / Бармен С. [Пер. з англ.] – М.: Вид-во "Вільямс", 2002. — 208 с.

3. Северина, С. В. Інформаційна безпека та методи захисту інформації. Вісник Запорізького національного університету, 2016. – 155-161 с.

АНАЛІЗ МЕРЕЖЕВИХ ПАКЕТІВ ЗА ДОПОМОГОЮ УТІЛИТИ TCPdump

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

Моніторинг і аналіз мережі являють собою важливі етапи контролю за роботою мережі. Для аналізу мережевих пакетів та перегляду їх змісту одним з найпотужніших методів вважається захоплення цих пакетів. За допомогою операції захоплення можливо завантажувати пакети, які проходять через мережеві інтерфейси [1].

Метою доповіді є аспекти аналізу мережевих пакетів за допомогою утиліти TCPdump, яка дозволяє інтерпретувати захоплені пакети в вигляді, доступному для розуміння людини. Ця утиліта створена для прослуховування та аналізу роботи комп'ютерної мережі. Утиліта складається з двох основних частин: частини захоплення та частини відображення захоплених пакетів.

Частина захоплення пакетів (при запуску) передає «дані вибору пакетів» безпосередньо бібліотеці захоплення пакетів, яка перевіряє вираз синтаксису, компілює його (у внутрішній формат даних), а потім копіює у внутрішній буфер програми мережні пакети, що проходять через вибраний інтерфейс і відповідають наданим умовам. Частина відображення пакетів вибирає захоплені пакети по одному з буфера і виводить їх (у вигляді, що сприймається людиною) у вигляді рядків інформації, відповідно до заданого (у командному рядку) рівня детальності. Якщо встановлено докладний аналіз пакетів, програма перевіряє для кожного пакета мережі, чи є у неї модуль розшифровки даних, і, у разі наявності, відповідною підпрограмою витягує (і відображає) тип пакета в протоколі або параметри, що передаються в пакеті [2].

В доповіді наводяться результати перевірки та виконання спостереження за мережевим трафіком, а також аналіз шаблонів трафіку, виявлення та усунення несправностей мережі, виявлення порушень безпеки в мережі, таких як несанкціоноване вторгнення, шпигунське програмне забезпечення або сканування наявного обладнання мережі.

Список літератури

1. Ед Вілсон. Моніторінг та аналіз мереж – New Jersey, USA, 2000; ISBN 5-85582-163-3. – 350 с.

2. Inspecting Network Traffic with tcpdump [Електронний ресурс] Режим доступу до ресурсу: https://www.rapid7.com/blog/post/2016/12/15/inspecting-network-traffic-with-tcpdump/

СИСТЕМА ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖІ IOV

Росінський Д.М., Волошин І.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Ідентифікувати різноманітні складні кібератаки в широкому діапазоні галузей, таких як Internet of Vehicles (IoV), зараз є дуже складним завданням. IoV – це комп'ютерна мережа транспортних засобів, яка складається з датчиків, приводів, мережевих засобів і систем зв'язку між транспортними засобами. Важливу роль в IoV відіграє комунікація. Транспортні засоби в мережі обмінюються та передають інформацію на основі кількох протоколів. Через бездротовий зв'язок між транспортними засобами вся мережа може бути чутливою до кібератак. Під час цих атак конфіденційна інформація може бути передана зловмисній мережі або фіктивному користувачу, що призведе до зловмисних атак на IoV. Традиційним системам виявлення вторгнень (IDS) стає дедалі важче виявляти нові, складніші атаки, які використовують незвичайні схеми. Щоб уникнути виявлення, зловмисники маскуються під типових користувачів,. Ці проблеми можна вирішити за допомогою глибокого навчання. Багато моделей машинного та глибокого навчання (DL) були реалізовані для виявлення зловмисних атак; однак основною проблемою залишається вибір функцій. Завдяки використанню навчальних емпіричних даних DL самостійно визначає ознаки вторгнення.

Метою доповіді є подання моделі вторгнення на основі DL, яка зосереджена на нападах типу «відмова в обслуговуванні» (DoS). Для оцінки та ранжирування ознак пропонується використовувати кластеризацію k-середніх. Після виділення найкращих функцій для виявлення аномалій застосовується нова модель Explainable Neural Network (xNN), що дозволить окремо класифікувати атаки в наборі даних CICIDS2019 і UNSW-NB15. Модель показала хороші результати щодо точності, запам'ятовування, оцінки F1. Для порівняння можна побачити, що запропонована модель xNN показала хороші результати після використання техніки підрахунку характеристик. У наборі даних 1 (UNSW-NB15) xNN показав хороші результати з найвищою точністю 99,3%, тоді як CNN набрав 85%, LSTM – 89%, а Deep Neural Network (DNN) – 91%. xNN досяг найвищої точності 98,7% під час класифікації атак у другому наборі даних (CICIDS2019); згорткова нейронна мережа (CNN) досягла 86%, довготривала короткочасна пам'ять (LSTM) досягла 89,5%, а DNN досягла 83%. Запропоноване рішення перевершило існуючі аналоги за точністю виявлення та класифікації.

Список літератури

1. Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles. IEEE Internet Things J. 2021, 9, 616–632.

2. Oucheikh, R.; Fri, M.; Fedouaki, F.; Hain, M. Deep Real-Time Anomaly Detection for Connected Autonomous Vehicles. Procedia Comput. Sci. 2020, 177, 456–461.

SAFETY SOLUTIONS FOR MySQL DATABASES

Bilash D.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Security of the data has a significant impact on the popularity of any type of service [1]. It is known that security is important part of building of application [2]. Programming languages are not an exception to this rule. The data of the programs are often stored in the database and the connection between a program and a database is vulnerable to unauthorized access. For example, Kotlin can connect to the database.

The purpose of this work is to describe one of the most triggering types of attacks on the applications, which were written using SQL databases – SQL injections.

The MySQL is a database, which consists of three main fields: login, password, and abstract key. The keys provide connections between the table with login and the table with abstract data about users. In addition, an essential factor in the effective functioning of databases is the protection of information.

SQL-injections is a computer attack method that uses a program vulnerability. This can lead to unauthorized access to sensitive data of database users. SQL injections can change relationships between tables and destroy the database.

To achieve data security, prepared statements can be used, in the programming language “Kotlin”. The PreparedStatement object is used to execute precompiled SQL queries with or without input (IN) parameters. Setters can be used for setting values in a query. PreparedStatement it automatically handles special characters and prevents SQL injection attacks. Prepared statements use question mark (?) as a placeholder for parameters (figure).

```
SELECT * FROM inf_cust JOIN login
ON inf_cust.cust_fid = login.cust_id
WHERE inf_cust.cust_fid = ? AND login.cust_id = ?;
```

Figure – Example of prepared statement query

References

1. Bilash D. A. Security mechanisms of voip-telephony / D. A. Bilash, V. M. Tkachov // Збірник тез доповідей одинадцятої міжнародної науково-технічної конференції "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління", 8-9 квітня 2021 року. - Том 2: секція 4. - Баку-Харків-Київ-Жиліна. - 2021. - С. - 78.

2. Bilash D. A. Analysis of methods of using the Raspberry PI platform in the training of computer engineers. Радіоелектроніка та молодь у XXI столітті : матеріали 25- го Міжнародн. молодіжн. форуму, 20-22 квітня 2021 р. Харків : ХНУРЕ, 2021. Т. 5, секція 4. С. 110–111.

NORMALIZATION AS A DATABASE SECURITY RULE

Chaika V., Bilash D.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Most of the applications use databases because it is an intelligible technology that provides storing and structuring information [1-2]. And the commonly used programming language for many projects which require manipulations with databases is a structured query language (SQL). If the database is not secure, cybercriminals will use SQL injections to change, steal, or delete data in the tables.

The main aim of this work is to point out the tactic of avoidance of database hacker attacks by normalization and compare it with existing solutions.

As stated above, SQL injections can injure applications by destroying tables or changing relationships between database components. However, these violent actions will not be effective if the database is created by following the normalization.

Normalization is a method of splitting data into many small logic tables connected using keys to make this data more structured. It makes tables more understandable and minimizes the quantity of using memory.

For example, a normalized database contains two tables – "users" and "password". If somebody got access to the table "users" by adding simple SQL code, the information will be useless. Because cybercriminals will only read the id and key that connect to another table if they do not know the database sequence. Also, deleting table "users" is impossible because it has links to another table.

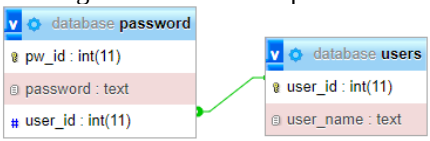


Figure – Database example

As you can see, normalization can help to avoid unauthorized access to databases because of distributed tables in a DB. Where a hackers get access to the table they need to know the structure of it.

References

1. Bilash D. A. Security mechanisms of voip-telephony / D. A. Bilash, V. M. Tkachov // Збірник тез доповідей одинадцятої міжнародної науково-технічної конференції "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління", 8-9 квітня 2021 року. - Том 2: секція 4. - Баку-Харків-Київ-Жиліна. - 2021. - С. - 78.

2. Bilash D. A. Analysis of methods of using the Raspberry PI platform in the training of computer engineers. Радіоелектроніка та молодь у XXI столітті : матеріали 25- го Міжнародн. молодіжн. форуму, 20-22 квітня 2021 р. Харків : ХНУРЕ, 2021. Т. 5, секція 4. С. 110–111.

SAFETY SOLUTIONS FOR SAVING PASSWORD USING HASH

Korovina D., Bilash D.
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

The cybercriminals can access the password that is stored in the database, and this is one of the biggest problems that your application can have [1-2]. You can avoid this vulnerability by using the most popular and useful algorithm nowadays. This is the use of a hash function to store the password. This way, the cybercriminals will not have access to your password, even if the whole website is hacked. Instead, they simply access the encrypted hash.

The purpose of this work is to show the password encryption`s risk and ways to avoid them. The vulnerability to rainbow tables (in circumstances when the password is brief and easy) and the brute-force attack technique are the dangers of any hashing scheme and compare these two methods of attacks in speech. In a brute-force attack, the attacker enters many passwords or passphrases with the intention of ultimately guessing the right one. This way, all possible passwords and passphrases are systematically checked by the attacker until the hacker find the correct one.

One of the improvements is to use salt in hash functions. The paper also consists comparing salt hash and unsalted one.

Before a password is hashed, random bits are added to each iteration as a cryptographic salt. Even if two people select the same password, salts produce individual passwords. By requiring attackers to recalculate hash tables using salts for each user, salts assist us in resisting assaults on hash tables.

This implies that even if the password hash is kept in a rainbow table, changing the password by adding a salt to the hash is still possible. Any user that uses the password "QWERTY" will have the same hash, hence the password can be readily cracked if a hacker possesses a rainbow table containing that hash's values. Hacking is made simpler because most individuals reuse or exchange passwords. As was already noted, putting a salt before or after the password lengthens it as well.

Therefore, storing passwords using hashes opens up a vast arena for research on the subject of data security. Future study will concentrate on the method that hashes passwords most effectively.

References

1. Bilash D. A. Security mechanisms of voip-telephony / D. A. Bilash, V. M. Tkachov // Збірник тез доповідей одинадцятої міжнародної науково-технічної конференції "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління", 8-9 квітня 2021 року. – Т. 2: с. 4. - Баку-Харків-Київ-Жиліна. 2021. С. 78.

2. Bilash D. A. Analysis of methods of using the Raspberry PI platform in the training of computer engineers. Радіоелектроніка та молодь у XXI столітті : матеріали 25- го Міжнародн. молодіжн. форуму, 20-22 квітня 2021 р. Харків : ХНУРЕ, 2021. Т. 5, секція 4. С. 110–111.

NULL POINTER EXCEPTIONS IN JAVA

Ripnyi M., Bilash D.
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

NullPointerException is the most common Java error. This error occurs when an object is not initialized and at the same time certain operations are attempted on it [1-2]. The main purpose of this paper is to describe this error and the most usable methods to avoid it and compare some of them.

The Java language has the null keyword. It was originally created to denote the absence of an object. Using this keyword, we can “partially” create an object. For example, when we do not yet know what its value will be. For example, in the case when we need a string, but its initialization will occur later during the program. "String str = null". The program will work, but as soon as we try to do something with an object that points to null, we immediately get a NullPointerException.

NullPointerException can occur even when you explicitly did not write anything like this in the code. But it always occurs because of a pointer to null.

The simplest, most obvious, and only way is to check the object for null before performing operations on it. With such a check, we can always be sure that the program will not throw a NullPointerException. Other popular method is to use class Optional. A container object which may or may not contain a non-null value. If a value is present, isPresent() will return true and get() will return the value.

```
if(optional.isPresent()) {
    //todo()
}

if(variable != null) {
    //todo()
}
```

Figure – Methods to fix NullPointerException

This exception can occur in every program you write, the main thing is to understand what it means and be able to find it. Future research will focus on other methods solving this question and deeply compare considered solutions.

References

1. Bilash D. A. Security mechanisms of voip-telephony / D. A. Bilash, V. M. Tkachov // Збірник тез доповідей одинадцятої міжнародної науково-технічної конференції "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління", 8-9 квітня 2021 року. - Том 2: секція 4. - Баку-Харків-Київ-Жиліна. - 2021. - С. - 78.

2. Bilash D. A. Analysis of methods of using the Raspberry PI platform in the training of computer engineers. Радіоелектроніка та молодь у XXI столітті : матеріали 25- го Міжнародн. молодіжн. форуму, 20-22 квітня 2021 р. Харків : ХНУРЕ, 2021. Т. 5, секція 4. С. 110–111.

ОГЛЯД ЗАГРОЗ ТЕЛЕКОМУНІКАЦІЙНИМ СИСТЕМАМ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Пугач К.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У гібридних конфліктах головними цілями є: контроль над суспільством, вплив на свідомість, маніпулювання людьми, відповідальними за прийняття важливих рішень у державі. Ворог прагне маніпулювати основними цінностями, мотиваційними факторами, а також стратегічною, комунікаційною та критично-важливою інфраструктурою країни. Доповідь присвячена огляду комплексних реалізацій засобів атак.

Вплив на критичні об’єкти інфраструктури і на суспільство призводить до деструктивних для системи держави змін (порушень функціонування

Аналіз засобів масової інформації продемонстрував значні наслідки масового використання широкомасштабних негативних соціально-політичних інформаційних кампаній. Навіть якщо інформація не створює свідомої зміни у переконаннях, вона може вплинути на інтерпретацію майбутньої інформації. Це може допомогти внутрішньому агресору, який бажає вплинути на хід конфлікту, щоб послабити підтримку цільового уряду. Кіберагресія часто приховує свої мотиви, прикриваючись технологічними методами, які можуть маскувати свої маніпулятивні цілі. Методи приховування включають у себе анонімні претензії на владу, новини, маніпульовані напівправдою, повторення повідомлень, перевантаження інформацією, кібер-псевдоопераці (уряд видає себе за повстанців), маріонетки (урядові агенти, які грають роль онлайн коментаторів), а також астротерфінгу (створення фальшивих масових рухів).

Ефективне запобігання та виявлення інформаційно-психологічних дій противника в кіберпросторі та наше швидке реагування вимагають створення національних центрів протидії інформаційним та кібератакам.

Заходами нейтралізації деструктивних інформаційно-кібернетичних ефектів та їх джерел є:

попередження власників (якщо вони відомі) Інтернет-ресурсів про обмеження щодо поширення фейкової, неправдивої інформації з рекомендацією її видалення, якщо інформація завдає шкоди суб’єктам та об’єктам національної безпеки (особі, суспільству, державі);

створення публічних реєстрів для ненадійних/підозрілих ресурсів.

Список літератури

1. Podorozhniak, A., Liubchenko, N., Kvochka, M., Suarez, I. (2021), "Usage of intelligent methods for multispectral data processing in the field of environmental monitoring", Advanced Information Systems, Vol. 5, No. 3, pp. 97-102. https://doi.org/10.20998/2522-9052.2021.3.13

СЕКЦІЯ 5

Керівник секції: д.т.н. проф. В. А. Краснобаєв, ХНУ, Харків
Секретар секції: к.т.н. О. М. Бельорін-Еррера, НТУ «ХПІ», Харків

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

ДОСЛІДЖЕННЯ ФУНКЦІЙ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ ТОВ "ЛАВЕНТА"

Яковлев О.О.
Черкаський державний технологічний університет, Черкаси, Україна

У сучасних умовах підприємства взуттєвої промисловості отримали великі можливості удосконалення системи планування та управління виробництвом для різкого підвищення загальної ефективності виробничо-господарської діяльності. Ці можливості забезпечені, з одного боку, відносною свободою вирішення тактичних та оперативних питань з управління виробництвом, а з іншого - застосуванням комп'ютерних засобів для вироблення оптимальних планово-управлінських рішень [1].

Складність та динамічність виробничих процесів, ускладнення продукції та її технології пов'язані з об'єктивною необхідністю використання у плануванні виробництва сучасних засобів обчислювальної техніки.

Метою доповіді є дослідження особливостей, переваг та недоліків існуючих інформаційно-обчислювальних систем [2], зокрема інформаційно-обчислювальних систем взуттєвих підприємств. Досліджено функції автоматизованої інформаційно-обчислювальної системи ТОВ "Лавента" та обрано основні математичні моделі що забезпечують роботу інформаційно-обчислювальної системи.

Запропоновані в доповіді рішення дозволяють синтезувати автоматизовану інформаційно-обчислювальну систему ТОВ "Лавента", що дасть можливість значно підвищити продуктивність праці та якість документів, а також скоротити чисельність працівників.

Список літератури

1. А.В.Олійник, В.М.Шацька Інформаційні системи і технології у фінансових установах Навчальний посібник - Львів: "Новий Світ-2000", 2006 - 436 с
2. І.К.Карімов Інформаційно-обчислювальні системи в економіці - Дніпродзержинськ «ДДТУ» 2013

EVALUATION OF MULTIVARIATE QUALITY CONTROL CHARTS IN THE COMPLEX ANALYSIS OF NATURAL WATER

Tychkov V.V., Tovstopyat V.O.
Cherkasy State Technological University, Cherkasy, Ukraine

A multivariate control charts is a control charts for evaluating a process at the level of two or more characteristics. Based on such charts, multivariate quality control is carried out - quality control in which each unit that is checked must meet the requirements for more than one characteristic. As a measuring unit, an immersion sensor was developed; in which ion-selective electrodes are placed [1]. A chalcogenide iron-selective electrode was used to determine total iron (Fetotal), a combined pH-electrode was used for the hydrogen indicator (pH), a combined nitrite-selective electrode was used for nitrites (NO2−), a redox electrode was used for redox potential, and for total salinity - a salinity sensor with a current interface and a digital temperature sensor. 50 measurements of chemical and physical indicators of natural water were carried out, sequentially switching the measuring device with electrodes.

The purpose of the report is the analysis of multivariate quality control charts in the analysis of natural water.

We choose two criteria (pH, Fetotal) of natural water quality in three dimensions, the so-called coordinate criteria. Then we fix the set of values of the remaining (non-coordinate) criteria (NO2−). Fixing different sets of non-coordinate criteria, we obtain the corresponding two-variate sections. A similar procedure is carried out for another pair of coordinate criteria. Based on the constructed two-variate sections, in the case of a small number of criteria (three), we obtain a visual representation of the entire multivariate set of possible estimates in order to make the best choice in it. Multivariate quality control charts of three indicators (pH, Fetotal, NO2−) were constructed in the software complex STATISTICA 10: Hotelling T2 control charts of all three indicators, Hotelling T2 control charts for monitoring the average values of two indicators relative to the third, MEWMA charts for all three indicators, MEWMA charts for controlling the average values of two indicators relative to the third, CUSUM charts of all three indicators, multi-variate flow with X-bar and MR charts of all three indicators, multi-variate flow with X-bar and R charts and with X-bar and S charts for control values of two indicators relative to the third. The material presented in this report shows the possibility of solving problems in the field of natural water quality control.

References

1. V.V.Tychkov, V.Ya.Galchenko, R.V.Trembovetskaya, (2018). “Technical and technological bases for achieving environmental safety of sustainable development”, in: Global Partnership for Local Sustainable Development: Modern Trends and Best Practices / ed. by L.O.Petkova, O.Yu.Berezina, A.Kryński, (Czestochowa, Poland, 2018), 160-171.

COMPARISON OF RECURSIVE Rd- AND QUASI-DETERMINISTIC LPτ-SEQUENCES USING DISCREPANCY FOR THE CONSTRUCTION OF UNIFORM MULTIDIMENTIONL DoE's

Tychkova N.B., Halchenko V.Ya.
Cherkasy State Technological University, Cherkasy, Ukraine

Scientific research on the construction of efficient uniform designs that fill the search space so that the experimental points are evenly distributed throughout the research domain is actively conducted and so far, it has been proven that, the best results are achieved using Sobol's quasi-sequences.

The purpose of the report is a comparative analysis of uniform multidimensional computer designs of experiments on recursive Rd-sequences and designs on Sobols LPτ-sequences using indicators of generalized discrepancies and graphic visualization based on Voronoi diagrams.

The report presents the results of comparing options on Rd-sequences with graphic visualization based on Voronoi diagrams and Sobol's LPτ-sequences using indicators of centered, wrap-around and weighted discrepancies for the construction of uniform five-, six-, seven- and eight-dimensional computer designs experiments [1-2]. However, the search for necessary combinations of sequences for multidimensional designs based on Sobol's quasi-sequences requires cumbersome and time-consuming research due to the need to implement it by means of sifting through a large number of candidate options among potentially possible ones, but does not guarantee that a positive result will be obtained in the end. For greater visibility of the uniformity of the generated sequences, a graphic representation of them in the form of two-dimensional projections was used. Finding successful designs with low divergence rates and correspondingly perfect projection properties is very important for practice. Note that the use of combinations of LPτ-sequences nevertheless shows the best results due to a good choice of guide numbers.

Список літератури

1. V.Ya.Galchenko, M.D.Koshevoy, R.V.Trembovetskaya, (2022). Homogeneous plans of multi-factory experiments on quasi-random R-Roberts sequences for surrogate modeling in a vortex style structuroscopy. *Radio Electronics, Computer Science, Control*. 62 (3), 22–30. https://doi.org/10.15588/1607-3274-2022-3-2

2. V.Ya.Halchenko, R.V.Trembovetska, V.V.Tychkov, N.B.Tychkova. "Evaluation of the effectiveness of uniform multidimensional designs of experimental based on Sobol's quasi-sequences", in: All-Ukrainian scientific-practical Internet conference young scientists "Metrological aspects of decision making in terms of work on technogenic dangerous objects". (Kharkiv, KhNADU, 4 November 2022).

АРХІТЕКТУРИ ПОБУДОВИ АВТОМАТИЗОВАНИХ СИСТЕМ АНАЛІЗУ ВЕЛИКИХ ДАНИХ

Міценко С.А., Комісаренко Н.А., Корнієнко А.Д.
Черкаський державний технологічний університет, Черкаси, Україна

Big Data – це загальний термін для будь-якого набору даних, настільки великих або складних, що виявляється важко обробляти їх із використанням традиційних методів управління даними, таких як, системи управління реляційними базами даних [2]. Тривалий час реляційні системи управління базами даних (РСУБД) вважалися універсальним рішенням, але експоненціальне зростання обсягів, швидкості та неоднорідності даних показали непридатність РСУБД для використання в системах зберігання та аналізу великих даних. Наука про дані передбачає використання методів для аналізу великих обсягів даних і виокремлення знань, що містяться в них [1].

Метою доповіді є апробація етапів доступу, очищення і завантаження в системи зберігання та аналізу великих даних, а також видача практичних рекомендацій щодо реалізації зазначених етапів.

В доповіді проведено аналіз архітектури побудови систем зберігання та аналізу великих даних. Показано, що на початкових етапах доцільно використовувати дистрибутиви для розгортання розглянутих систем з урахуванням пакетної або потокової обробки даних [4]. Зроблено огляд застосовності чотирьох видів NoSQL баз даних. З використанням стандартних і сторонніх Java-бібліотек апробовано методи веб-сканування і веб-скрепінгу, як додаткові методи отримання зовнішніх даних. Апробовано доступ до Інтернет джерел відкритих даних з використанням JSON і CSON. Розроблено алгоритми отримання інформації про відкриті набори даних, скачування наборів та їхнього очищення [3]. Апробовано два способи завантаження даних у розподілену файлову систему Hadoop – системи зберігання та аналізу великих даних, розгорнутої на основі Hortonworks HDP. Досліджений комплекс технологій, алгоритмів та їх реалізацій показав працездатність і можливість його застосування при подальших дослідженнях у галузі великих даних.

Список літератури

1. Kumar V. Introduction to Data Mining / V. Kumar, M. Steinbach, P.Tan. – Harlow: Pearson Education, Inc., 2018. – 736 p.

2. Martsenyuk V. On an approach of the solution of machine learning problems integrated with data from the open-source system of electronic medical records: Application for fractures prediction. // Artificial Intelligence and Soft Computing. Springer International Publishing. – 2019., №22, P. 228-239.

3. Pirracchio R. Big data and targeted machine learning in action to assist decision in the icu. // Anaesthesia Critical Care Pain Medicine. – 2019, Vol. 38. No. 4. P. 377-384.

4. Oliveira A. Retinal vessel segmentation based on fully convolutional neural networks. // Expert Systems with Applications. – 2018, Vol. 112. P. 229–242.

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В БЛОКЧЕЙН-СИСТЕМАХ

Міценко С.А., Неділя В.В., Строгуш О.А.
Черкаський державний технологічний університет, Черкаси, Україна

Масове використання засобів обчислювальної техніки в структурі господарської, фінансової та економічного управління, а також розвиток всесвітньої електронної комерції та бізнесу призводять до постійно зростаючого розвитку інформаційних технологій, що сприяє безперервному розширенню спектра загроз безпеці інформації, оброблюваної в інформаційних системах. Серед найперспективніших методів забезпечення зберігання, обробки та захисту даних можна виділити методи, що враховують застосування хмарних платформ – розроблених із застосуванням технології блокчейн [2]. Необхідність обробки даних у блокчейн-системах передбачає новий еволюційний етап забезпечення безпеки інформації та висуває до інформаційних систем додаткові вимоги, пов'язані зі специфікою даних, появою нових технологій обробки інформації та появою завдань, специфічних для сучасного етапу розвитку інформаційних технологій [1].

Метою доповіді є забезпечення достовірності даних під час їх обробки в блокчейн-системі.

В доповіді продемонстровано модель виявлення актуальних загроз порушення інформаційної безпеки даних. У межах створення моделі встановлено та формалізовано залежність між: загрозами, актуальними для даних, що обробляються в блокчейн-системі; збитком від потенційних загроз блокчейн-системі; ступенем небезпеки порушення окремих характеристик безпеки (достовірності); ступенем важливості даних. Розширено клас методів забезпечення достовірності даних у частині виявлення недостовірних персональних даних при їх введенні в блокчейн-систему [3]. Формалізовано поведінку користувача та доведено можливість виявлення аномалій у поведінці користувача за допомогою штучних нейронних мереж.

Список літератури

1. Atzei N. A survey of attacks on Ethereum smart contracts (SOK). International Conference on Principles of Security and Trust. – Springer, Berlin, Heidelberg. – 2019. P. 164-186.

2. Kozin I.S. Providing personal data protection based on the block chain technology // Fourth Conference on Software Engineering and Information Management (SEIM-2020) (April 13, 2020). – P. 10–16.

3. Lou W. SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks / W. Lou, W. Liu, Y. Fang // INFOCOM 2020. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE. – 2020. – Vol. 4. – P. 2404-2413.

4. Yeremenko O.S. Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET / O.S. Yeremenko, Ali Salem Ali // Radioelectronics and Informatics. – 2018. – № 1 (68). – P. 26-29.

INVESTIGATION OF THE QUALITY OF PSEUDORANDOM SEQUENCES SYNTHESIZED ON THE BASIS OF MODULO TWO ADDITION OPERATIONS

Sysoienko A.A., Sysoienko S.V.
Cherkasy State Technological University, Cherkasy, Ukraine

The use of the latest technologies increases the requirements for the quality of the output sequences of pseudorandom numbers, which are the basis of ensuring data confidentiality in the development of new methods of cryptographic information protection for computer cryptography systems [1].

The study of the quality of a pseudorandom sequence synthesized on the basis of operations of cryptographic transformation of information is an urgent problem of the modern development of information technologies [2, 3, 4].

The purpose of the report is research and analysis of methods for assessing the quality of pseudorandom sequences, the synthesis of which is carried out based on the use of modulo two addition operations [4], for computer cryptography systems. For the computational experiment, we have selected 24 two-digit operations that form a mathematical group.

The essence of the experiment is to encode data with two random operations that are included in the selected group, followed by adding the results of encoding according to modulo two of the PRS.

According to the results of the experiment, it was found that adding modulo two transformation results increases the quality of pseudorandom sequences, since there is no inverse transformation mechanism.

References

1. Gnatyuk, S., Burmak, Y., Berdibayev, R., Aleksander, M., Ospanova, D.: Method for developing pseudo-random number generators for cryptographic applications in 5g networks. Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique&quot., 4(12), 151–162 (2021). https://doi.org/10.28925/2663-4023.2021.12.151162

2. Faure, E. V., Shcherba, A. I., Lavdansky, A. A.: Analysis of the correlation properties of sequences of (pseudo) random numbers. Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy, 1(18), 142–150 (2015). http://nbuv.gov.ua/j-pdf/Nitps_2015_1_32.pdf

3. Lavdansky, A. A., Faure, E. V.: Combination method for generating a sequence of pseudorandom numbers. In: Proceedings of the 16th International Scientific and Technical Conference on System Analysis and Information Technology: SAIT-2014, Kyiv, May 26-30, 2014, pp. 403–404. NNK «IPSA» NTUU «KPI», Kyiv (2014). http://sait.kpi.ua/books/sait2014.ebook.pdf/view

4. Lanskyh, Ye. V., Sysoenko, S. V., Pustovit, M. O.: Evaluation of the quality of pseudorandom sequences based on the use of modulo two addition operations. Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy, 4(21), 147–150 (2015)

МЕТОД АНАЛІЗУ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРОТИДІЇ ДЕСТРУКТИВНОМУ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ

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

Сьогодні спостерігається зростання рівня інформаційно-психологічного впливу деструктивного характеру на усі суспільні категорії. Існуючі інноваційні інформаційні технології, які призначені для боротьби з деструктивним інформаційно-психологічним впливом потребують постійного вдосконалення, тому дослідження, спрямовані на аналіз їх ефективності є актуальними. Зокрема, важливою науковою задачею є аналіз ефективності застосування методів формування категоріального комплексу критеріїв психолінгвістичного портрету пропагандиста, які лежать в основі подібних інформаційних технологій. В такому випадку, особливу увагу необхідно приділити критеріям морфологічно-синтаксичної категорії, семантичної категорії [1] та дискурсивної категорії, які разом складають категоріальний комплекс критеріїв. При цьому, враховуючи доведену достовірність застосування кореляційного аналізу для дослідження категоріальних відмінностей [2], було вирішено використати цей підхід в основі методу.

Метою доповіді є розробка методу аналізу ефективності застосування повного категоріального комплексу критеріїв психолінгвістичного портрету пропагандиста з метою оцінювання інформаційних технологій протидії деструктивному інформаційно-психологічному впливу, які реалізується на основі методів формування кожної категоріальної складової.

В доповіді наводиться метод дослідження ефективності на основі кореляційно-регресійного аналізу, що дозволило оцінити рівень зміни особистісних категоріальних характеристик психолінгвістичного портрету після проведення дій, націлених на протидію деструктивному інформаційно-психологічному впливу. Отримані результати доводять надійність методів квантово-семантичної стеганографії з урахуванням декількох контент-критеріїв. Виявлені статистичні дані, щодо зміни компонентів кожної складової категоріального комплексу дозволяють в подальшому ситуативно підвищувати ефективність інформаційної технології.

Список літератури

1. Tarasenko Ya. Content-criteria of psycholinguistic portrait's semantic category for researching the group propaganda. *Ukrainian Scientific Journal of Information Security*. 2020. Vol. 26, № 1. P. 5-13. DOI: https://doi.org/10.18372/2225-5036.26.14526

2. Васюк К.М. Психолінгвістичний аналіз граматичної будови брехливого повідомлення. *Психологічний часопис*. 2019. Том 5, № 3. С. 222-234. DOI: https://doi.org/10.31108/1.2019.3.23

ЗАСТОСУВАННЯ МЕТОДУ ГОЛОВНИХ КОМПОНЕНТІВ В МАШИННОМУ НАВЧАННІ

Бєльков Б.О., Коротка Є.О., Мірошкіна І.В.
Черкаський державний технологічний університет, Черкаси, Україна

Основою будь-кого алгоритму машинного навчання є дані. Часто дані містять велику кількість різних характеристик, що значно ускладнює їх інтерпретацію, візуалізацію і, відповідно, розуміння. Тому виникає необхідність у зниженні розмірності вихідної задачі за рахунок відкидання "зайвих" характеристик [1].

Одним із основних методів зниження розмірності даних для задач машинного навчання є метод головних компонентів (МГК). В методі застосовуються прості матричні операції з лінійної алгебри та статистики, щоб отримати проекції початкових даних меншої вимірності (шукається напрямок з максимальною дисперсією і дані проектуються на цей напрямок) [2].

Метою доповіді є дослідження ефективності застосування методу головних компонент в різних задачах машинного навчання. Розглядалися дві відомі задачі. Перша – візуалізації даних відомої задачі про квіти ірисів. Розглядався набір даних про квіти ірисів трьох сортів, який складався з 50 зразків кожного сорту. Для кожного зразка приводилося чотири ознаки. Візуально зобразити такий набір даних можливо лише у чотиривимірному просторі. Застосування МГК дозволило знизити розмірність даних до двох ознак та візуалізувати їх у вигляді двомірного графіка.

Друга задача – це оптимізація даних для розпізнавання рукописних цифр. Дані складалися з 1797 чорно-білих зображень розміром 8×8 пікселів, тобто мали 64 ознаки. Було визначено час тренування і точність моделі регресії для даних без зменшення розмірності.

Загальний час склав 12,3 секунди, точність розпізнання 0,9697. Зменшили розмірність набору даних настільки, щоб зберегти 90% дисперсії. В результаті чого час тренування моделі був прискорений більше ніж на 90% до 1,1 секунди, точність розпізнання упала незначно – на 0,8% до 0,9613. Застосування методу головних компонентів показало ефективність як в якісній, так і в кількісній оптимізації великих об'ємів даних. Але слід пам'ятати, що цей метод добре працює тільки у випадку лінійного розподілу даних.

Список літератури

1. Бізнес-аналітика багатовимірних процесів [Електронний ресурс] : навч. посіб. / Т. С. Клебанова, Л. С. Гур'янова, Л. О. Чаговець [та ін.] ; Харківський національний економічний університет ім. С. Кузнеця. – Електрон. текстові дан. – Харків: ХНЕУ ім. С. Кузнеця, 2018. – 271 с. : іл. http://ebooks.git-elt.hneu.edu.ua/babap/index.html

2. Leskovec J. Mining of Massive Datasets /Jure Leskovec, Anand Rajaraman, Jeffrey David Ullman. Second edition. – Cambridge University Press, 2014. – 476 p. DOI: https://doi.org/10.1017/CBO9781139924801

МЕТОДИ АНАЛІЗУ КЛАСТЕРНИХ СТРУКТУР У БАГАТОВИМІРНИХ ОБ'ЄМАХ

Карапетян А.Р., Цоколенко А.С.
Черкаський державний технологічний університет, Черкаси, Україна

Однією з основних задач практично у всіх галузях людської діяльності на сьогоднішній день є аналіз багатовимірних даних. Багатовимірні дані це результат чисельних досліджень, технічних показників, узагальнення економічної та фінансової інформації тощо. Необхідність обробки, аналізу та адекватного трактування цих даних породила таку інтенсивно розвивається наукову дисципліну, як аналіз багатовимірних даних (Data Analysis). Однією з найважливіших складових цього напрямку є кластерний аналіз [1], який розглядає різні способи групування об'єктів усередині хмари багатовимірних даних. Методів та алгоритмів кластерного аналізу на сучасному етапі існує дуже багато, вони постійно розвиваються та відрізняються великою різноманітністю.

Метою доповіді є дослідження комплексу алгоритмів візуалізації та візуальної аналітики, що дозволяє вивчення кластерних структур у багатовимірних об’ємах даних без застосування алгоритмів кластеризації, що вносять зміни до вхідних даних. Для аналізу кластерних структур багатовимірному об’ємі даних пропонується використовувати методи відображення точок вихідного багатовимірного простору на вкладені в цей простір різноманіття меншої розмірності. Даний підхід базується на побудові карток SOM (Self-Organised Maps), що самоорганізовуються, застосуванні методу головних компонент PCA і побудові пружних карт Elastic Maps. Для реалізації повної та послідовної обробки багатовимірного масиву даних вищезазначені методи та підходи вишиковуються в послідовність методів та алгоритмів, що застосовуються, утворюючи єдиний технологічний ланцюжок обробки даних. Застосування такого ланцюжка дозволяє отримати інформацію про кластерну структуру досліджуваного об’єму багатовимірних даних на різних рівнях глибини аналізу та деталізації інформації.

Список літератури

1. Van der Maaten L.J.P.; Hinton G.E. Visualizing High-Dimensional Data Using t-SNE. Journal of Machine Learning Research 9 (Nov 2008). Pp. 2579–2605

2. Hinton G.E., Roweis S.T. Stochastic Neighbor Embedding. In Advances in Neural Information. Processing Systems. Vol. 15. Pp. 833–840, Cambridge, MA, USA, 2002. The MIT Press.

МЕТОДИКА РОЗРАХУНКУ ОЦІНКИ РИЗИКУ УДАРУ БЛИСКАВКИ ЗАСОБАМИ MS EXCEL

Чичужко М. В., Івченко П. А., Чичужко В.О.
Черкаський державний технологічний університет, Черкаси, Україна

Україна як майбутній член Європейського союзу взяла на себе відповідальність поступово гармонізувати свою нормативно-технічну базу з нормативними документами європейської спільноти. Це стало причинило прийняття і в галузі блискавкозахисту цілої низки документів, що прийшли на заміну вітчизняному. Відповідно до нового нормативного документа, для того щоб оцінити чи потрібен захист будівлі, необхідно здійснити розрахунок ризику. Алгоритм розрахунку наведений в цьому ж документі. Але через велику кількість схожих формул виникає природна необхідність автоматизувати цей процес. Вирішенням цієї проблеми є методика побудови моделі розрахунку оцінки ризику удару блискавки в будівлю та її реалізація комп'ютерною програмою.

Аналіз останніх досліджень і публікацій може показати що у сучасній науці використання програмних продуктів для створення математичних моделей є широковживаною практикою. Як прилад використання в якості інструмента для її створення MS Excel наводиться в статтях [1], [2].

Метою доповіді є розробка методики оцінки ризику удару блискавки та подальшого експорту отриманих результатів в попередньо створений шаблон, відповідно до нормативних документів, на основі документа MS Word.

В доповіді наводяться приклади розв'язання задач для розрахунку оцінки ризику, які можна звести до декількох основних типів: такі, що повертають значення або посилання на значення з таблиці чи діапазону а також виконують пошук зазначеного елемента в діапазоні та повертають відносну позицію цього елемента; процедура оцінки ризику відповідно до нормативного документа.

Список літератури

1. Горда І. М. Комп'ютерне моделювання процесу механічного руху тіла засобами MS EXCEL / І. М. Горда, Л. О. Флегантов // Інформаційні технології і засоби навчання. - 2015. - Т. 47, вип. 3. - С. 99-109. - Режим доступу: http://nbuv.gov.ua/UJRN/ITZN_2015_47_3_10.

2. Імітаційне моделювання інвестиційних ризиків засобами MS Excel та MathCAD / В.В. Гавриленко, О.А. Шумейко // Екон.-мат. моделювання соц.-екон. систем. — 2007. — Вип. 12. — С. 211-220.

РОЗРОБКА МЕТОДІВ ПОПЕРЕДНЬОЇ ОБРОБКИ ДАНИХ У СИСТЕМАХ ОПТИЧНОГО РОЗПІЗНАВАННЯ ТЕКСТУ

Білозерський В.О.
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна
Дергачова Д.К.
Харківський національний університет радіоелектроніки, », Харків, Україна

За допомогою засобів розпізнавання образів вирішуються дві найбільш актуальні задачі: виявлення та розпізнавання обличь, а також оптичне розпізнавання тексту (OCR). Виділення цифрового текстового шаблону зі знімка знаходить багато корисних застосувань. Серед них - оцифрування паперових архівів, верифікація паспортів, розпізнавання номерних знаків транспорту тощо. Значні досягнення у вирішенні задач розпізнавання та класифікації об'єктів базуються на використанні сучасних методів та алгоритмів побудови та навчання глибинних нейронних мереж (ГНМ). Найважливішу роль серед них відіграють згорткові нейронні мережі (ЗНМ), які дозволяють довести показники якості рішень до 99 % [1]. Хоча, існують серйозні обмеження, які впливають на результат обробки зображень, а саме: низька якість фото знімків, недостатня освітленість сцени, геометричні спотворення та ряд інших факторів [2].

Метою доповіді є формулювання сучасної концепції підвищення якості роботи систем оптичного розпізнавання тексту за рахунок використання комплексу алгоритмів попередньої обробки зображень текстових документів.

В доповіді наводяться результати досліджень впливу різноманітних негативних факторів на точність розпізнавання та запропоновано комплекс алгоритмів, спрямованих на підвищення якості роботи оптичних систем розпізнавання тексту для їх подолання [3]. Наведені дані показують високу ефективність запропонованих технічних рішень. Попередня обробка вихідних даних за представленим методом дозволяє досягти точності розпізнавання тексту у межах 99.5-99.8%, незважаючи на недостатню освітленість сцени, геометричні спотворення, шуми та ряд інших факторів.

Список літератури

1. Krizhevsky A. ImageNet Classification with Deep Convolutional Neural Networks. Communications of the ACM. 2017. Vol. 60, no. 6. P. 84–90. DOI: 10.1145/3065386..

2. Karthick K., Ravindrakumar K., Francis R., Ilankannan S. Steps Involved in Text Recognition and Recent Research in OCR. International Journal of Recent Technology and Engineering (IJRTE). 2019. Vol. 8, iss.1. C. 3095-3100. Retrieval Number A2670058119/19©BEIESP.

3. Dergachov K., Krasnov L., Bilozerskyi V., Zymovin A. Data pre-processing to increase the quality of optical text recognition sys-tems. Радіоелектронні і комп'ютерні системи. 2021. № 4(100). P. 183-198. DOI: https://doi.org/10.32620/reks.2021.4.15.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИКОНАННЯ ПРОЦЕДУР ПРОЦЕСУ ВИВЧЕННЯ І ВПРОВАДЖЕННЯ ДОСВІДУ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ ЧЕРЕЗ ЗАСТОСУВАННЯ ПОЛОЖЕНЬ ТЕОРІЇ ІНФОРМАЦІЇ

Серпухов О.В., Макогон О.А., Сергєєв О.С., Маєр Л.В., Головенко Я.Є.
Військовий інститут танкових військ Національного технічного університету «Харківський політехнічний інститут», Харків, Україна

Вивчення та впровадження досвіду (ВВД) підготовки і застосування ЗС України є вкрай необхідним для виявлення закономірностей та тенденцій розвитку воєнного мистецтва, практики воєнних дій і вироблення рекомендацій командирам (начальникам) щодо розвитку ЗСУ, інших складових сил оборони держави, удосконалення порядку їх об'єднаної підготовки та проведення об'єднаних операцій (бойових дій) [1].

Найбільш трудомістким є збір первинної інформації, яка знаходиться на тактичному рівні системи ВВД. У зборі цієї інформації задіяні безпосередні учасники бойових дій, що обумовлює певні труднощі. І якщо знайти засоби для збереження інформації в польових умовах технічно можливо, то виникнення психологічних “блоків“ значно знижують рівень релевантності, повноти, достовірності та адекватності інформації.

Доповідь присвячена розробці методики збору первинної інформації, яка знаходиться на тактичному рівні системи вивчення і впровадження досвіду підготовки і застосування ЗС України.

З точки зору основних положень теорії інформації проведено аналіз інформації системи ВВД та оцінити рівень її якісних характеристик. На основі аналізу функціонального перетворення інформації при всебічному забезпеченні бою у плані спостереження (зборі інформації) виділені потоки за видами інформації. Механізм перетворення інформації у системі ВВД формалізований за принципом “чорної скрині“. Розроблений зразок опитувального листа для відповіді збору первинної інформації, яка знаходиться на тактичному рівні системи вивчення і впровадження досвіду підготовки і застосування ЗС України [2].

Список літератури

1. Доктрина з вивчення та впровадження досвіду у Збройних Силах України. – Головне управління доктрин та підготовки Генерального Штабу Збройних Сил України спільно з центром оперативних стандартів і методики підготовки Збройних Сил України, 2022. – 34с.

2. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон ; пер. с. англ. под ред. Р. Л. Добрушина и О. Б. Лупанова; с предисл. А. Н. Колмогорова. – М. : Издательство иностранной литературы, 1963. – 832 с.

МЕТОДИ СТИСНЕННЯ АУДІОДАНИХ У СИСТЕМАХ АУДІОАНАЛІТИКИ

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

При збереженні, передачі крізь локальну мережу або у хмарне середовище аудіоданих, зазвичай використовуються певні алгоритми стиснення аудіоданих [1]. Розрізняють методи стиснення із втратами та без втрат. Метод стиснення без втрат означає архівування аудіозапису з використанням алгоритмів, при яких дані не втрачаються та можливе відновлення аудіозапису з бітовою точністю [2]. Прикладами кодеків, які використовують стиснення без втрат, є FLAC (Free Lossless Audio Codec) та ALAC (Apple's Lossless Audio Codec). Метод стиснення з втратами припускає, що немає сенсу зберігати повну інформацію про аудіозапис. Наприклад, людське вухо може не почути тихих звуків після гучних або занадто високих і занадто низьких частот [3]. Прикладом кодека стиснення з втратами є MPEG 1 Layer III (Moving Picture Experts Group 1 Layer III) або просто MP3.

Метою доповіді є дослідження методів стиснення аудіоданих у системах аудіоаналітики, а саме методів стиснення із втратами та без втрат. Для аналізу результатів використовуються методи на основі кодеків FLAC та MP3.

В доповіді наводяться результати аналізу методів стиснення аудіоданих у системах аудіоаналітики. Наведені дані показують, що пріоритетним методом стиснення аудіоданих у багатоцільвій системі аудіоаналітики є метод стиснення без втрат, так як він дозволяє досягти більш високих показників точності. Але, у випадку однозначного функціоналу системи, метод стиснення з втратами дозволяє досягти конкурентного показника точності, та значного зменшити обсяг даних, що обробляються. Додатково, в залежності від типу інформації, що зберігає система аудіоаналітики, використання методу стиснення аудіоданих з втратами дозволяє вирішити проблеми, пов'язані з забороною отримання або зберігання приватних аудіоданих у деяких країнах.

Список літератури

1. Kovalenko, A., & Poroshenko, A. (2022). Analysis of the sound event detection methods and systems. Advanced Information Systems, 6(1), 65–69. https://doi.org/10.20998/2522-9052.2022.1.11

2. Ulacha, G., & Wernik, C. (2020, March). A High Efficient Cascade Coder with Predictor Blending Method for Lossless Audio Compression. In 2020 Data Compression Conference (DCC) (pp. 395-395). IEEE.

3. Kim, B., & Rafii, Z. (2018, September). Lossy audio compression identification. In 2018 26th European Signal Processing Conference (EUSIPCO) (pp. 2459-2463). IEEE.

МЕТОДИ ТА ІНСТРУМЕНТИ ВИДОБУТКУ ВЕБ-КОНТЕНТУ

Ільїна І.В., Філенко В.П.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день Інтернет включає в себе величезні та постійно зростаючі обсяги даних. Але іноді через їх неоднорідність, слабку структурованість або повну відсутність структурованості, пошук потрібної інформації перетворюється на важке і трудомістке завдання [1]. У більшості випадків користувачі Всесвітньої павутини можуть отримати веб-дані шляхом перегляду та пошуку за ключовими словами, скориставшись відомими пошуковими системами, однак у такого методу є обмеження. Веб-сторінки − це гіпертекстові документи, які містять як текст, так і гіперпосилання на інші документи, що в результаті поверне велику кількість нерелевантної інформації. Використання програмних засобів автоматичного видобутку веб-контенту також не обходиться без деяких труднощів, таких як, наприклад, невідповідність типу даних для програми [2], тому роботу цих засобів часто доводиться поєднувати з ручним втручанням оператора.

Метою доповіді є ознайомлення з концепцією веб-видобутку, огляд та порівняння методів та інструментів вилучення даних, а також представлення варіантів вирішення проблем, з якими стикаються користувачі в процесі автоматичного видобутку знань з Інтернету.

В доповіді наведено перелік проблем автоматичного вилучення тексту та слабоструктурованих даних із веб-сайтів [3], значна кількість яких пояснюється простим порушенням стандартів та рекомендацій щодо верстки вебсторінок і розмітки HTML, неоднорідністю інформації або наявністю дублікатів даних. Проблема навігації, коли інформація розміщується на декількох сторінках або на сторінці з динамічним підвантаженням контенту, вирішується використанням бібліотек мов програмування, здатних імітувати поведінку людини (прокручування сторінки, натискання клавіш і т. і.).

Список літератури

1. Mebrahtu, A., Srinivasulu, B. Web Content Mining Techniques and Tools. International Journal of Computer Science and Mobile Computing. Vol. 6, Issue 4, April 2017, pp. 49-55.

2. Han, J., M. Pei, Kamber, J.. Data Mining: Concepts and Techniques. Third edition. Morgan Kaufmann Publishers, 2006, pp. 8-15.

3. Ruban, I., Ilina, I., Mozhaiev, M. Researching priority directions in the area of Data, Control navigation and communication systems, 2020, no. 4(62), pp. 59-63. DOI: 10.26906/SUNZ.2020.4.059.

МЕТОДИ АНАЛІЗУ ШВИДКОСТІ ПАРАЛЕЛЬНОЇ ОБРОБКИ ІНФОРМАЦІЇ У GRID СИСТЕМАХ

Ільїна І.В., Костенко О.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Географічно розподілені обчислення (GRID)− технологія розподілених обчислень, в якій обчислювальна система представлена у вигляді з'єднаних мережею обчислювальних вузлів, слабопов'язаних, гомогенних та гетерогенних комп'ютерів, що працюють разом для виконання великої кількості завдань. GRID застосовується для вирішення завдань, які потребують значних обчислювальних ресурсів [1]. Останні дослідження в галузі GRID-систем торкаються багатьох проблем, пов'язаних з інфраструктурою (моніторинг та інтеграція систем) до впровадження та аналізу результатів роботи конкретних GRID-систем у сфері хмарних обчислень. Однак, незважаючи на широке поширення GRID-систем та велику кількість присвячених їм публікацій залишається відносно мало освітленим питання аналізу продуктивності та визначення повного спектру факторів, що впливають на швидкість обробки даних у цих системах [2,3].

Метою доповіді є аналіз та оцінка факторів, що впливають на швидкість паралельної обробки інформації у географічно розподілених інформаційних системах.

До предметної області дослідження відноситься проведення аналізу існуючих методів розрахунку часу та швидкості обчислень у GRID-системах, визначення залежності швидкості обчислень у GRID-системах від кількості обчислювальних вузлів, розробка методів оцінки оптимальних безпосередньо для прискорення обрахунків кількості обчислювальних вузлів у GRID-системах та розробка методик, що дозволяють проводити оцінку часу обчислень та прискорення обрахунків у GRID-системах.

Список літератури

1. Balasangameshwara J., Nedunchezhian R. A hybrid policy for fault tolerant load balancing in grid computing environments. // Journal of Network andComputer Applications, Volume 35, Issue 1, January 2012, P. 412–422.

2. Castellano M., Stifini R. Knowledge sharing in biomedical imaging using a grid computing approach. // Computational Modelling of Objects Represented in Images: Fundamentals, Methods and Applications III, Taylor & Francis Group UK, 2012, P. 257-260 Taylor & Francis Group UK, 2012, P. 257-260

3. Zhao G., Bryan B.A., King D. Large-scale, high-resolution agricultural systems modeling using a hybrid approach combining grid computing and parallel processing. // Environmental Modelling & Software, Volume 41, March 2013, P. 231–238.

АНАЛІЗ МОДЕЛЕЙ ПЕРЕДАЧІ ДАНИХ ДЛЯ СИСТЕМИ РОЗУМНОГО БУДИНКУ

Чумак В.І., Філіппенко І.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Розумний будинок (англ. smarthome) – це автоматизована система, що складається із сукупності датчиків, виконавчих пристроїв, здатних виконувати дії, та програмного забезпечення для реалізації певних повсякденних завдань без участі людини [1], а також систематизування і зберігання даних та їх обробку за певний термін часу.

Робота «розумного будинку» передбачає декілька обмінів даними: між елементами системи та між користувачем і системою.

Обмін даними між елементами системи може відбуватися дротовим та бездротовим шляхом за допомогою різноманітних протоколів. Популярні протоколи передачі даних у системі розумний будинок [2-3]:

- дротовий зв'язок використовує протоколи X10, C-Bus;
- бездротовий зв'язок використовує протоколи Z-Wave, ZigBee, Wi-Fi, Thread, Bluetooth Low Energy (BLE).

Також обмін між користувачем і системою теж може відбуватися дротовим (безпосередньо при введені даних через пристрої системи) та бездротовим шляхом (наприклад, через мережу Інтернет).

Мета доповіді - структурування, аналіз та порівняння моделей передачі даних для системи розумного будинку, а також виявлення основних переваг та недоліків цих моделей.

В доповіді запропоновані технології та таблиці аналізу моделей передачі даних для системи розумного будинку, наведені наявні приклади реалізації цих технологій.

Запропоновані технології дають можливість автоматизувати процеси збору даних та методів подальшого аналізу цих даних з метою обрання підходящої для Вас системи розумного будинку.

Список літератури

1. Розумний дім [Електронний ресурс] Режим доступа: https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B7%D1%83%D0%BC%D0%BD%D0%B8%D0%B9_%D0%B4%D1%96%D0%BC

2. Дементьев А. Д. «Умный» дом XXI века [Текст] / А. Д. Дементьев – М. : Litres, 2016. - 168 с.

3. Уинг Ч. Как работает ваш дом [Текст] / Ч. Уинг – К. : ДМК-Пресс, 2016. – 206 с.

4. Філіппенко І.В. Огляд графічних бібліотек для вбудованих платформ [Текст] / І.В. Філіппенко, В.Р. Корнієнко, Г.К. Кулак, Харків, «Радіоелектроніка та інформатика», 2020, №1 – 2020 с 47-53.

ДОСЛІДЖЕННЯ ОСОБЛИВОСТІ АЛГОРИТМУ МУРАШИНИХ КОЛОНІЙ

Кучук Н.Г., Лисиця Д.О.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

Мета доповіді – оцінка можливості формування оптимального маршруту в умовах заданих обмежень.

Особливості алгоритму мурашиних колоній при висунутих обмеженнях:

1. Механізм позитивного зворотного зв'язку використовується для того, щоб пошук безперервно сходився і, нарешті, наближався до оптимального рішення.

2. Кожен індивід може змінювати навколишнє середовище, вивільняючи феромони, і кожен індивід може сприймати зміни навколишнього середовища в реальному часі, і індивіди опосередковано спілкуються через це середовище.

3. У процесі пошуку використовується метод розподілених обчислень, і кілька користувачів одночасно виконують паралельні обчислення, що значно підвищує обчислювальну потужність та ефективність роботи алгоритму.

4. Евристичний ймовірнісний метод пошуку нелегко потрапити до локального оптимального рішення, і легко знайти глобальне оптимальне рішення.

Результати дослідження відображені на рис. 1., а саме співвідношення між найкоротшою відстанню TSP та кількістю ітерацій.

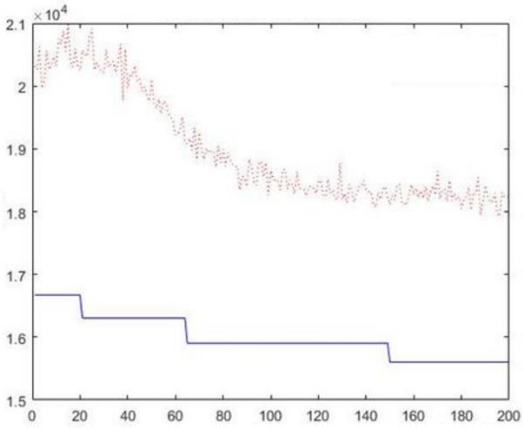


Рисунок 1 – Співвідношення між найкоротшою відстанню TSP та кількістю ітерацій

Список літератури

1. Van Trees H. L., Bell K. L., and Tiany Z. (2013) Detection Estimation and Modulation Theory, 2nd Edition, Part I, Detection, Estimation, and Filtering Theory, John Wiley & Sons, New York.

МОДЕЛІ АДАПТИВНИХ ЦИФРОВИХ ФІЛЬТРІВ НА FPGA

Дубов І.Г., Філіппенко І.В.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день існує багато радіоелектронних виробів, ефективна робота яких неможлива без використання адаптивних фільтрів. Адаптивну фільтрацію застосовують якщо фільтри з фіксованими параметрами не можуть виконати поставлену задачу, наприклад, якщо умови фільтрації змінюються, тому вимоги до фільтра не можуть бути сформульовані заздалегідь [1,2]. Частотна характеристика адаптивних фільтрів автоматично регулюється або модифікується відповідно до певного критерію, що дозволяє фільтру адаптуватися до змін характеристик вхідного сигналу.

Мета доповіді – порівняльний аналіз алгоритмів адаптації для побудови моделі адаптаційного фільтру ехокомпенсації.

Адаптивні алгоритми базуються на теорії оптимальної винерівської фільтрації. На даний час використовуються алгоритм Ньютона, алгоритм якнайшвидшого спуску і алгоритм за критерієм найменших квадратів. До простих відносяться різновиди градієнтних адаптивних алгоритмів за критерієм найменшого квадрата, такі як Least Mean Square, LMS, його нормалізованої версії Normalized LMS, NLMS. До складних можна віднести різновиди рекурсивних алгоритмів за критерієм найменших квадратів Recursive Least Squa, Matrix Inversion Lemma, MIL та QR-розкладання. Проміжний клас утворюють алгоритми афінних проекцій, а саме Affine Projections, AP. Існують також швидкі, тобто обчислювально ефективні алгоритми Fast AP, FAP і швидкі RLS-алгоритми, включаючи сходові.

Аналіз існуючих методів адаптивної фільтрації показав, що алгоритми відрізняються як обчислювальною складністю, так швидкістю збігу. На основі аналізу була запропонована модель цифрового адаптивного фільтра на основі RLS алгоритму. Також можна зробити припущення, що задовільні результати реалізації моделі запропонованого цифрового фільтру можуть бути отримані при використанні ПЛІС.

Список літератури

1. Солонина А.И., Арбузов С.М. Цифровая обработка сигналов. Моделирование в MatLab. СПб.: БХВ-Петербург, 2008. 816 с

2. Смит С. Цифровая обработка сигналов. Практическое руководство для инженеров и научных работников. М.: Додэка-XXI, 2011. 720 с.

3. Зотов В.Ю. Проектирование цифровых устройств на основе ПЛИС фирмы Xilinx в САПР WebPACK ISE. М.: Горячая линия–Телеком, 2003. 624 с.

ПРОБЛЕМАТИКА СЕЛЕКЦІЇ ТА КЛАСИФІКАЦІЇ АУДІО ПОДІЙ У ЗАШУМЛЕНОМУ СЕРЕДОВИЩІ

Пушко В.В., Сердюк Н.М.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком обчислювальних систем, розробкою та нещодавньою появою на ринку спеціалізованих процесорів стала можливою практична реалізація методів побудови нейромереж глибинного навчання. Серед найбільш популярних завдань, які вирішуються нейронними мережами, виділяються завдання виявлення та класифікації як визначених, так і невизначених елементів у великих масивах даних які вже існують, так і таких що надходять у реальному часі від безлічі джерел. На сьогоднішній день існує багато архітектур нейронних мереж, однак серед найбільш поширених можна виділити згорткові нейронні мережі (CNN) і згорткові рекурентні нейронні мережі (CRNN), та їх основні алгоритми виявлення та класифікації.

Метою доповіді є аналіз надійності застосування згорткових та згортково-рекурентних нейронних мереж при роботі із зашумленим джерелом.

В доповіді наводяться результати аналізу погіршення помилки мережі при навмисному введенні джерела шуму у джерело аудіоданих [1]. Наведені дані показують, що низький рівень зашумленості потоку має незначний вплив на рівень помилки нейромереж обох архітектур. Однак, по досягненню певного порога рівень помилки починає різко зростати і незабаром досягає неприйнятних значень. Також хотілося б відзначити, що нейромережа CRNN демонструє трохи більшу надійність, ніж CNN [2]. Це пов'язано з тим, що на відміну від нейромереж CNN в CRNN мережах на додаток використовується функція «довгої короткочасної пам'яті» (long short-term memory, LSTM). Таким чином, наділяючи мережу можливістю запам'ятовувати значення як на короткі, так і на довгі проміжки часу.

Список літератури

1. Адаван С., Параскандоло Г., Пертила П., Хейттола Т., Виртанен Т. (2016) Обнаружение звуковых событий в многоканальном звуке с использованием пространственных и гармонических характеристик. В: Материалы семинара по обнаружению и классификации акустических сцен и событий 2016 г. (DCASE2016), стр. 6–10.

2. Santos, Rodrigo & Kassetty, Ashwitha & Nilizadeh, Shirin. (2021). Disrupting Audio Event Detection Deep Neural Networks with White Noise. Technologies. 9. 64. DOI:10.3390/technologies9030064.

Підсекція 5.2. Цивільна безпека (інформаційна підтримка)

ЗАХИСТ ІНФОРМАЦІЇ ПІД ЧАС УПРАВЛІННЯ СИЛАМИ ТА ЗАСОБАМИ ПРИ НАДЗВИЧАЙНИХ СИТУАЦІЯХ

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

Забезпечення захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій є невід'ємною частиною державної політики національної безпеки. Попередження виникнення надзвичайних ситуацій, швидка їх ліквідація з найменшим оптимальним залученням сил і засобів має особливе значення для фізичного і морального стану населення, а також економіки самої країни. В будь-якому випадку всі ці стратегічні та тактичні дії ДСНС України супроводжуються складними інформаційними процесами.

Метою доповіді є вивчення питання захисту інформації в структурі ДСНС України.

Вимоги до рівня захисту інформації в ДСНС України почали зростати зі збільшенням кількості хакерських атак від зловмисників. Забезпечення сталого та надійного функціонування телекомунікаційних мереж та загальносистемних серверів у мирний час та в особливий період – основне завдання кіберзахисту в ДСНС України [1], оскільки більшість інформаційних процесів під час управління силами та засобами при надзвичайних ситуаціях мають конфіденційний характер. Оперативність, достовірність і засекреченість інформації має надзвичайне значення для безпеки людей та забезпечення національної безпеки в цілому. Окрім цього, забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України [2].

На сьогодні серед множини методів захисту інформації особливе місце займають криптографічні методи [3], що, на відміну від інших, спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її оброблення, передавання і зберігання. Тому необхідно шукати нові групи операцій криптографічного перетворення, що забезпечать підвищення якості систем захисту 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. Melnyk R., Melnyk O. Improving the Cryptographic Protection of Confidential Information in the Management of Civil Protection Forces and Means // Вісник Кременчуцького національного університету імені Михайла Остроградського. Вип. 1 (132), 2022. С. 108–114.

МЕТОДИ КЕРУВАННЯ БЕЗПЕКОЮ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ КРИТИЧНОЮ ІНФРАСТРУКТУРОЮ

Нечипоренко О.В., Ткач В.І.
Черкаський державний технологічний університет, Черкаси, Україна

Автоматизована система управління (АСУ) технологічними процесами – це сукупність технічних і програмних засобів, призначених для автоматизації технічних і програмних засобів, а також автоматизації процесів керування технологічним обладнанням на промислових підприємствах [3]. Суб'єкти інформаційної інфраструктури, які використовують АСУ можна розглядати, як критичні інфраструктури (КІ). Серйозною загрозою для таких підприємств – можливість втручання терористичних, екстремістських і вороже налаштованих груп в управління АСУ технологічним процесом КІ для приведення їх у непрацездатний стан [1]. Кількість випадків злому промислових інформаційних систем продовжує зростати. Певною мірою цьому приділено особливу увагу в ЗМІ, а також зацікавленість підприємств у захисті виробництва.

Метою доповіді є підвищення ефективності інформаційної безпеки АСУ технологічним процесом в умовах деструктивних впливів за рахунок використання ризик-орієнтованого підходу.

В доповіді розроблено теоретико-множинну модель АСУ технологічним процесом КІ, що відрізняється наявністю опису взаємодії активів різних рівнів, схильних до загроз інформаційної безпеки. Модель відображає логічну та фізичну структури взаємодії між активами, а також вплив на АСУ КІ, що дає змогу здійснити аналіз характеристик технічних і програмних засобів та технологічних процесів. Розроблено спосіб оцінювання ризиків інформаційної безпеки АСУ КІ, яка відрізняється об'єднанням в єдине моделі та алгоритмів з оцінювання збитків і можливості реалізації загрози [2]. Запропонований метод, відрізняється аналізом активів із застосуванням моделі АСУ КІ, оцінкою актуальних ризиків інформаційної безпеки із застосуванням оригінальної методики, а також різними підходами до опрацювання ризиків в умовах багаторівневої ієрархічної структури.

Список літератури

1. Evancich, N. Attacks on Industrial Control Systems / N. Evancich, J. Li // Cybersecurity of SCADA and Other Industrial Control Systems. Advances in Information Security. – 2019. – Vol. 66. – P. 95–110.

2. Zegzhda D.P. Approach to APCS Protection from Cyber Threats / D.P. Zegzhda, T.V. Stepanova // Automatic Control and Computer Sciences. – 2021. – no. 49(8). – P. 659–664.

3. Wei Y.C. Performance Evaluation of the Recommendation Mechanism of Information Security Risk Identification / Y.C. Wei, W.C. Wu, Y.C. Chu // Neurocomputing. – 2020. – no. 279. – P. 48–53

УПРАВЛІННЯ ЛОГІСТИЧНИМИ РИЗИКАМИ У ПРОЦЕСАХ ТИЛОВОГО ЗАБЕЗПЕЧЕННЯ ВІЙСЬК (СИЛ)

Альбощій О.В.
Національна академія Національної гвардії України, Харків, Україна

Тилове забезпечення відіграє важливу роль як у повсякденній діяльності військових формувань так і при виконанні ними завдань за призначенням. Актуальність дослідження ризиків тилового забезпечення обумовлена комплексом чинників, пов'язаних із характером і масштабами сучасних бойових дій, збільшенням можливостей засобів розвідки супротивника, широким використанням інформаційних технологій в управлінні військами.

Метою доповіді є аналіз логістичних ризиків при тиловому забезпеченні військ, їх ідентифікація та управління ними в сучасних умовах. Очевидно, логістичні витрати пов'язані не лише із використанням коштів і матеріальних засобів при виконанні логістичних операцій, що є об'єктивною складовою, а й з можливим нераціональним витрачанням коштів і засобів, що є суб'єктивною складовою, втратами внаслідок дії непереборних сил, тощо. Аналіз логістичних процесів тилового забезпечення військ (сил) показує, що, в цілому, наявними є базові логістичні витрати та небезпеки. В той же час, з'являються специфічні небезпеки. Вони обумовлені, головним чином, намаганнями супротивника знищити ресурси (матеріальні засоби) чи, принаймні, максимально ускладнити їх доставку до місць призначення.

Традиційні ризики, які притаманні процесам закупівлі, зберігання, доставки, розподілу ресурсів різного роду, є достатньо дослідженими та прогнозованими. Підходи до управління такого роду ризиками є напрацьованими. Стосовно ж ризиків, пов'язаних із впливом супротивника на процеси тилового забезпечення, необхідні подальші дослідження. Ризики мають розглядатися в контексті рішень, що приймаються відповідними командирами. При цьому, заздалегідь мають виявлятися потенційні небезпеки, досліджуватися варіанти реагування на них. Для прийняття рішень у конкретній ситуації, необхідна оперативна та достовірна інформація щодо існуючих небезпек, їх ідентифікації, оцінювання, розподілу. Наразі, представляють інтерес шляхи отримання та обробки розвідувальної інформації, зокрема від безпілотних апаратів для цілей тилової розвідки.

Список літератури

Альбощій О.В. Управління ризиками логістичного забезпечення як напрямок удосконалення системи логістики / О.В. Альбощій, С.О. Каплун, С.О. Павленко // Щоквартальний науковий журнал «Честь і закон». 2019. № 2(69). - С. 63-68. DOI: https://doi.org/10.33405/2078-7480/2019/2/69/177922.

МЕТОДИЧНІ ЗАСАДИ АВТОМАТИЗАЇ ПРОЕКТУВАННЯ РІДКИХ КОМПОЗИЦІЙНИХ МАТЕРІАЛІВ ДЛЯ ЕКРАНУВАННЯ ЕЛЕКТРОМАГНІТНИХ ПОЛІВ

Бурдейна Н.Б., Бірук Я.І.
Київський національний університет будівництва і архітектури Київ, Україна

Дослідження виконані в останні роки демонструють перспективність застосування рідких матеріалів для екранування електромагнітних полів [1, 2]. Але проектування захисних сумішей стикається з низкою проблем. Ці суміші є композиційними, складаються принаймні з трьох компонентів, що мають різні магнітні та електрофізичні властивості. Крім того, потрібно враховувати параметри полів, які потребують екранування. У загальному випадку у процесі проектування захисного матеріалу необхідно враховувати електрофізичні властивості матриці, магнітні та електрофізичні властивості кожного з екрануючих наповнювачів та їх концентрації.

Для визначення ефективності матеріалу, виходячи зі співвідношень електродинаміки суцільних середовищ, необхідно попередньо розрахувати магнітні та електрофізичні властивості кінцевого матеріалу, оскільки вони не є стандартними і відсутні у довідковій літературі. Магнітні властивості сумішей розраховуються, виходячи зі співвідношення Лорентца. Діелектрична проникність − за допомогою співвідношення Максвелла-Гарнетта. Якщо потрібно врахувати форму частинок наповнювача, то застосовується формула Оделевського. Оптимізація співвідношень усіх критичних показників у матеріалі практично неможлива, тому важливо автоматизувати процес раціонального обирання співвідношення вмісту та властивостей композиту потрібних товщин та захисних властивостей.

При проектуванні рідких композиційних матеріалів для екранування електромагнітних полів пропонується розробити програмне забезпечення, яке розраховує магнітні властивості та діелектричну проникність складу композитів шляхом перебору. В якості середовища розробки обрано Visual Studio 2019, мови програмування – C#. Вихідні дані про параметри компонентів композитів, результати розрахунків магнітних властивостей та діелектричної проникності сумішей заносяться до СУБД SQAL Server.

Список літератури

1. Glyva, V., Bakharev, V., Kasatkina, N., Levchenko, O., Levchenko, L., Burdeina, N., Guzii, S., Panova, O., Tykhenko, O., & Biruk, Y. (2021). Design of liquid composite materials for shielding electromagnetic fields. Eastern-European Journal of Enterprise Technologies, 3(6 (111), 25–31. https://doi.org/10.15587/1729-4061.2021.23147

2. Tudose Ioan Valentin, Mouratis Kyriakos,d Ionescu Octavian Narcis, Romanitan Cosmin, Pachiu, Cristina, Popescu Marian, Khomenko Volodymyr, Butenko Oksana, Chernysh Oksana, Kenanakis George, Barsukov Viacheslav Z., Suchea Mirela Petruta, Koudoumas Emmanouel, Novel Water-Based Paints for Composite Materials Used in Electromagnetic Shielding Applications, Nanomaterials, 2022, 12(3), 487

МОДЕЛІ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДОСЛІДЖЕННЯ ВПЛИВУ ВІЙСЬКОВИХ ЗАГРОЗ НА ЛОГІСТИКУ ПОСТАЧАННЯ ОЗБРОЄННЯ В ЗОНУ ВОЄННОГО КОНФЛІКТУ

Федорович О.Є., Рибка А.В., Чмихун Є.К., Соловйов В.С., Поліщук Є.В.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Логістична складова є основною компонентою в постачанні озброєння та військової техніки в зону воєнного конфлікту. Розміщення виробників озброєння та складів з військовою технікою на дальній відстані від зони конфлікту призводить до довгих, іноді заплутаним, логістичним ланцюгам постачання, які з можливості виникнення воєнних загроз мають великі ризики. Тому актуальна тема докладу, в якому наведені результати дослідження впливу воєнних загроз на довгі логістичні ланцюги постачання озброєння та військової техніки [1, 2].

Метою доповіді є розробка комплексу моделей та методів, які реалізовані за допомогою прикладної інформаційної технології, для дослідження впливу воєнних загроз на логістику постачання озброєння в зону воєнного конфлікту. **В доповіді** аналізуються логістичні ланцюги з можливими вразливостями, які збуджуються при появі воєнних загроз. В якості прикладу вразливостей можна віднести наступні [3]: моральне та фізичне старіння транспортних вузлів та магістралей; наявність вузьких пропускних місць (мости, транспортні розв'язки, тощо); близькість транспортних магістралей та вузлів до зони воєнного конфлікту. Аналізується логічна послідовність, яка пов'язана з появою воєнних загроз: воєнна загроза → збудження вразливостей → поява збитків → формування множини превентивних заходів. Формуються раціональні маршрути руху військових вантажів в зону воєнного конфлікту в умовах виникнення загроз. Досліджується вплив загроз на збудження вразливостей та оцінюються рівні збитків. Оптимізується та обирається множина превентивних заходів для нейтралізації впливу воєнних загроз.

Список літератури

1. Value stream analysis in military logistics: The improvement in order processing procedure / R. Acero et al. // Applied Sciences. 2020. Vol. 10. No. 1. Article ID 106. DOI: https://doi.org/10.3390/app10010106.

2. Наконечний О. Аналіз умов та факторів, що впливають на ефективність функціонування системи логістики сил оборони держави // Системи управління, навігації та зв'язку. Збірник наукових праць. 2019. Т. 3. №. 55. С. 48-57. DOI: https://doi.org/10.26906/SUNZ.2019.3.048

3. Федорович О. Є., Прончаков Ю. Л. Метод формування логістичних транспортних взаємодій для нового портфелю замовлень розподіленого віртуального виробництва // Радіоелектронні і комп'ютерні системи. 2020. № 2. С. 102-108. DOI: https://doi.org/10.32620/reks.2020.2.09.

ВИБІР МЕТОДУ ПОПЕРЕДНЬОЇ ОБРОБКИ ЗОБРАЖЕНЬ У СИСТЕМАХ ПОСТАВАРІЙНОГО МОНІТОРИНГУ

Микусь М.А., Васюхно С.І.
Національний університет оборони України імені Івана Черняховського,
Київ, Україна

Основним критерієм для систем поставарійного моніторингу є мінімізація часу на проведення екстрених заходів по захисту населення, зведення до мінімуму кількості постраждалих і збитків, а також оперативна оцінка можливості відновлення функціоналу об’єктів у зоні аварії.

В свою чергу, вирішення даних завдань суттєво залежить від якості первинної інформації від системи поставарійного моніторингу, зокрема від якості розпізнавання об’єктів на зображень, отриманих з місця аварії. Вихідні зображення спотворені шумами апаратури сканування, дискретизації або каналами передачі даних, мають нерівномірні яскравість і контрастність. Це призводить до розривів лінійних об'єктів, руйнування символів, маскування складних об'єктів. Тому необхідна попередня обробка зображення, що включає в себе вирівнювання загального яркісного фону зображення, усунення високочастотних перешкод і різного роду пошкоджень, виконання контрастування, бінарного та інших функціональних перетворень [1].

Алгоритми попередньої обробки зображень поділяються на різні групи в залежності від класифікатора ознаки. Всі алгоритми попередньої обробки або повинні покращувати якість зображень, або перетворювати його до виду, найбільш зручного для подальшої обробки. Незважаючи на кілька десятиліть досліджень до теперішнього часу немає єдиного методу, який можна вважати хорошим для всіх типів зображень, оскільки на результат сегментації зображення впливає безліч факторів, таких як однорідність, просторові характеристики, безперервність, текстура та зміст зображень. Отже, вибір алгоритму та методу попередньої обробки та сегментації зображень мають величезний вплив на значення критерію точності, як виявлення об'єктів на зображенні, так і на результати розпізнавання.

Метою доповіді є проведення аналізу підходів до вибору алгоритмів та методів при проведенні попередньої обробки зображень у системах поставарійного моніторингу.

У доповіді розглянуті алгоритми і методи попередньої обробки зображень, зосереджено увагу на їх перевагах та недоліках, варіантах класифікації, а також проаналізовані існуючі підходи до вибору того чи іншого методу, орієнтуючись на різноманітні характеристики отриманого зображення.

Список літератури

1. A. Sharif Razavian, H. Azizpour, J. Sullivan, and S. Carlsson, “Cnn features off-the-shelf: an astounding baseline for recognition,” in Proc. of the IEEE Conf. on Comp. Vision and Pattern Recognition Workshops, 2014, pp. 806–813.

МОДЕЛІ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДОСЛІДЖЕННЯ ЛОГІСТИКИ РЕЛОКАЦІЇ ПІДПРИЄМСТВ ПІД ЧАС ВОЄННОГО СТАНУ

Федорович О.Є., Рибка К.О., Лещенко Ю.О., Попов А.В.,
Сломчинський О.В.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

Під час воєнного стану більша кількість підприємств оборонно-промислового комплексу країни потрапили у зону воєнного конфлікту. Виникла проблема, яка пов'язана з релокацією (евакуацією) підприємств. Для цього необхідно провести комплекс заходів логістичного характеру, які пов'язані з демонтажем технологічного обладнання, транспортуванням та розміщенням підприємств для налаштування у короткі терміни виробництва продукції необхідного для країни [1]. Звідси виникає актуальність дослідження, результати яких демонструються у даній доповіді.

Метою доповіді є розробка комплексу моделей та прикладної інформаційної технології для дослідження логістичних процесів релокації підприємств під час воєнного стану. **В доповіді** досліджуються заходи, які пов'язані з послідовністю логістичних дій у ланцюгу [2]: вибір нового місця локації підприємства → демонтаж обладнання підприємства → підготовка до переміщення підприємства на нове місце → транспортування обладнання → розміщення та монтаж обладнання → проведення пусконалаштувальних робіт → запуск виробництва. Вибір нових площ здійснюється за допомогою оптимізаційної задачі з багатокритеріальним представленням основних показників (час, витрати, ризики). Для дослідження переміщення підприємства на нове місце локації створена агентна імітаційна модель, яка враховує різнорідність транспортної мережі. При цьому враховуються загрози воєнного часу, множина вразливостей транспортної мережі, ризики транспортування [3].

Список літератури

1. Моделювання логістичного процесу евакуації промислового підприємства у воєнний час / О. Є. Федорович, Ю. Л. Прончаков, К. О. Рибка, Ю. О. Лещенко // Авіаційно-космічна техніка і технологія. 2022. № 3. С. 84-93. DOI: https://doi.org/10.32620/aktt.2022.3.09.

2. Вибір постачальників для виробництва високотехнологічної продукції з урахуванням довгих логістичних ланцюгів постачання вантажів / О. Є. Федорович, Ю. Л. Прончаков, К. О. Рибка, Ю. О. Лещенко // Авіаційно-космічна техніка і технологія. 2021. № 5. С. 75-81. DOI: https://doi.org/10.32620/aktt.2021.5.10.

3. Modeling the impact of threats and vulnerabilities in transport logistics of a developing enterprise / O. Fedorovich, Yu. Pronchakov, Yu. Leshchenko, A. Yelizieva // Радіоелектронні і комп'ютерні системи. 2021. № 3. С. 29-36. DOI: https://doi.org/10.32620/reks.2021.3.03.

Підсекція 5.3. Сучасні інформаційно-вимірювальні системи

ДОСЛІДЖЕННЯ ЕКСПЛУАТАЦІЙНИХ ТА МЕТРОЛОГІЧНИХ ХАРАКТЕРИСТИК П'ЄЗОЕЛЕКТРИЧНОГО КРОКОВОГО ДВИГУНА

Назаренко А.О., Бондаренко М.О.
Черкаський державний технологічний університет, Черкаси, Україна

П'єзоелектричні мотори застосовуються у виробництві напівпровідників та їх тестуванні, для нанолітографії, нанометрології, в скануючих зондових мікроскопах та у космічних апаратах як виконавчих механізмів, а також для роботи в умовах наявності сильних магнітних полів [1].

Актуальність застосування п'єзоелектричних моторів у різних прецизійних вимірювальних та стежачих системах, регульованими величинами яких є кутове та лінійні переміщення, пояснюється кількома факторами. Це, перш за все, їх висока роздільна здатність (аж до 0,1 нм), можливість самозупинення ланки, максимальна тривалість безвідмовної роботи, а також їх висока надійність. П'єзоелектричні мотори мають ряд переваг над електромагнітними: відсутністю випромінюваних магнітних полів і несхильністю до їх впливу; можливістю мініатюризації; широким діапазоном частот обертання та моментів на валу; вогнестійкістю; відсутністю обмоток; простий технологією виготовлення та, як наслідок, вищою ефективністю. У той же час за зовнішньою конструктивною простотою п'єзоелектричного двигуна ховається ціла низка фізичних явищ, які складно взаємопов'язані між собою [2].

Метою доповіді є встановлення раціональних параметрів п'єзоелектричних крокових двигунів шляхом дослідження їх експлуатаційних та метрологічних характеристик, чим підвищити їх надійність, чутливість, а також зменшити їх собівартість та ресурсоємність.

У доповіді проводяться розрахунки раціональних габаритів п'єзокерамічного крокового двигуна та наводяться результати досліджень експлуатаційних та метрологічних характеристик таких двигунів, що дозволило зменшити крок такого п'єзокерамічного мотора в 4,5 рази. Адекватність модельних розрахунків підтверджується експериментальними дослідженнями. При цьому показано, що отримані результати можуть використовуватися при проектуванні п'єзокерамічних крокових двигунів широкої номенклатури.

Список літератури

1. V.Sharapov, Piezoceramic sensors (New York: Springer Verlag: 2011).

2. S.F.Petrenko, P′ezoelektrycheskiy dvihatel (Piezoelectric motor) (Kyiv, Korniychuk, 2002) [In Russian].

ОПТОЕЛЕКТРОННА ВИМІРЮВАЛЬНА СИСТЕМА ГЕОМЕТРИЧНИХ ПАРАМЕТРІВ ОБ'ЄКТІВ СПОСТЕРЕЖЕННЯ

Грабов О.О.
Черкаський державний технологічний університет, Черкаси, Україна

Тенденції економічного розвитку сьогодні так чи інакше пов'язані з підвищеними вимогами до забезпечення точності, особливо в приладобудуванні, в яких зазначений параметр гарантує насамперед надійність, довговічність та якість продукції, що випускається [1].

Комплекс завдань, що вирішуються при розробці конкретних технологій виконання вимірювань з оцінки та контролю геометричних параметрів корпусних конструкцій досить різноманітний і часто вимагає застосування, креативних рішень, нестандартних прийомів, а іноді суміщення різних засобів вимірювання для реалізації однієї вимірювальної задачі.

Актуальність розробки нових сучасних підходів [2] при виконанні контрольно-вимірювальних завдань з метою підвищення точності контролю геометричних параметрів об'єкта в процесі будівництва, монтажу, виготовлення та налагодження не викликає сумнівів і безумовно має як теоретичне, так і практичне значення

Метою доповіді є дослідження методів підвищення точності вимірів геометричних параметрів об'єкта з використанням оптоелектронних інформаційно-вимірювальних систем за рахунок комплексування результатів вимірів.

У доповіді наводяться результати огляду існуючих методів оцінки геометричних параметрів оптичними та оптоелектронними засобами вимірювання [3], виконано аналіз впливу складових похибки; визначено потенційні можливості підвищення точності вимірювань оптоелектронними інформаційно вимірювальних систем. представлено метод узгодження систем координат засобів вимірювання та вимірюваного об'єкта з використанням прийомів аналітичної геометрії. Досліджено метод стабілізації системи координат об'єкта у момент проведення вимірювань для мінімізації впливу кліматичних та динамічних факторів впливу.

Список літератури

1. Unified Spatial Metrology Network (USMN), URL: https://www.kinematics.com/spatialanalyzer/usmn.php. Access: 01.11.2022.

2. A.S.Grishkanich, E.Kolmakov, D.Redka, K.Tsvetkov. "Speed scanning system based on solid-state microchip laser for architectural planning", in: Proceedings of SPIE - The International Society for Optical Engineering. "Remote Sensing Technologies and Applications in Urban Environments II", (2017).

3. G.W.Johnson, S.E.Laskey, S.Robson, M.R.Shorts. "Dimensional & Accuracy Control Automation In Shipbuilding Fabrication: An Integration Of Advanced Image Interpretation, Analysis And Visualization Techniques", in: XX Congress ISPRS-2004. (Istanbul, Turkey, 2004).

КЕРОВАНА ГІБРИДНА ТЕХНОЛОГІЯ АДИТИВНОГО ВИРОБНИЦТВА ВИСОКОЯКІСНИХ ІНДИВІДУАЛЬНИХ ІМПЛАНТАТІВ З БІОСУМІСНИХ ПОЛІМЕРНИХ МАТЕРІАЛІВ

Ощепков Н.О., Рудь М.П.
Черкаський державний технологічний університет, Черкаси, Україна

Використання технологій адитивного виробництва в медицині є одним з найбільш перспективних застосувань. Нові підходи та методи тривимірного друку (3D-друку) біоімплантів щодалі ширше використовуються в медичних закладах світу. Проте масове використання цих методів обмежена складністю технології та великою вартістю обладнання [1].

Технології 3D-друку дозволяють не лише швидше розробляти нові біоконструкції, але й виготовляти їх, пропонуючи на вимогу пацієнтів індивідуальне біомедичне рішення. Така технологія має значну перспективу для виготовлення, наприклад, біокаркасів зі складною архітектурою та геометрією, які спеціально розроблюються для використання в регенеративній медицині. Наступним великим нововведенням у цій галузі стане розроблення біосумісних та гістіогенних матеріалів для 3D-друку з полімерами на біологічній основі [2].

Метою доповіді є розроблення універсальної автоматизо-ваної технології та створення на її основі пристроїв 3D-друку індивідуальних імплантатів та медичного інструменту з біосумісних полімерних матеріалів.

У доповіді для досягнення поставленої мети вперше розроблено універсальну апаратну платформу для технологій FDM та SLS, що дозволяє створювати композиційні структури. Також розроблено та застосовано новий метод контролю подачі пластику зі зворотнім зв'язком, який базується на алгоритмі послідовного оцінювання зсуву негаусових асиметрично-розподілених випадкових величин. Метод дозволяє підвищити точність дозування філаменту в 1,8-2,1 рази, підвищити міцність зчеплення між шарами на 33-38% та зменшити витрати матеріалів на 10-15% [3].

Список літератури

1. Ю.М.Нижник. "Технології сучасного 3D-друку та перспективи їх застосування", в: XV Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Ефективність інженерних рішень у приладобудуванні». (Київ, КПІ ім. Ігоря Сікорського, 10-11 грудня 2019).

2. E.Yang, S.Miao, J.Zhong, Z.Zhang, D.K.Mills, L.G.Zhang, (2018). Bio-based polymers for 3D printing of bioscaffolds. *Polymer Reviews*, 58 (4), 668-687.

3. О.Г.Новаковский, М.П.Рудь, В.С.Антонюк, М.О.Бондаренко, (2020). Підвищення якості поверхонь виробів, отриманих методом 3D друку. *Вісник Національного технічного університету України «Київський політехнічний інститут».* 61 (2), 52-57. DOI: https://doi.org/10.20535/1970.60(2).2020.221450.

ДОСЛІДЖЕННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ КЕРУВАННЯ ДОРОЖНІМ РУХОМ

Петренко І.О., Трембовецька Р. В.
Черкаський державний технологічний університет, Черкаси, Україна

Світовий розвиток новітніх цифрових технологій обміну інформацією та застосування інтелектуальних систем керування дорожнім рухом веде до значної зміни технологічних, наукових та практичних підходів до організації раціонального дорожнього руху в густонаселених містах [1].

Існуючі математичні моделі управління автотранспортними потоками ґрунтуються на детермінованій основі, у диференціальних рівняннях яких закладені емпіричні початкові та граничні умови (часто-густо суперечливі), які пов'язані з визначенням типу автотрафіку та пропускної спроможності транспортного потоку за умов максимального навантаження. Це призводить до недостатньої пропускної спроможності в годинник пік смуг руху автотранспорту на певних ділянках, і, в той же час, факт істотної недозавантаженості інших смуг дорожнього руху [2].

В той же час, поступове впровадження розумних світлофорів як IoT-пристрою дасть змогу спроектувати та впровадити сучасну інтелектуальну комп'ютерну систему керування дорожнім рухом, яка може оперативно відстежувати дорожню обстановку та автоматизувати оптимальні рішення диспетчерами центрального пульта керування дорожнім трафіком мегаполісу.

Метою доповіді є розроблення інноваційної цифрової мікроконтролерної мережевої системи (на прикладі світлофорного об'єкту), яка здатна адаптивно реагувати на завантаженість дорожнього трафіку та змінювати часові фази взаємодії цієї системи із сусідніми узгоджуючими системами.

У доповіді показано результат створення мобільної інтелектуальної системи керування дорожнім рухом, до складу якої входить режим адаптивного світлофора на LED-екрані [3]. Так, авторами розроблена інтелектуальна система керування дорожнім рухом в якості колективного технічного IoT-пристрою, який вираховує поточну дорожню обстановку та дозволяє у режимі он-лайн диспетчерським службам дорожнім рухом надавати рекомендації щодо автоматичного (або, за необхідності, ручного) регулювання режиму пропуску транспортних потоків.

Список літератури

1. T.Bellemans, B.De Schutter, B.De Moor, (2002). Models for traffic control. *Journal A*. 43 (3-4), 13–22.

2. S.Hoogendoorn, H. van Zuylen, M.Schreuder, B.Gorte, G.Vosselman, “Microscopic traffic data collection by remote sensing”, in: 82nd Annual Meeting of Transportation Research Board (TRB), (Washington D.C., 2013).

3. J.Jin, X.Ma, (2015). Adaptive group-based signal control by reinforcement learning. *Transportaion Research Procedia*. 10, 207–216.

ДОСЛІДЖЕННЯ ТА РОЗРОБЛЕННЯ АВТОМАТИЧНОЇ СИСТЕМИ КОНДИЦІОНУВАННЯ В ПОЛЬОВИХ УМОВАХ

Смірнова К. М., Туз В.В.
Черкаський державний технологічний університет, Черкаси, Україна

Особливе місце серед транспорту займають мобільні комплекси. Мобільні комплекси є важливим елементом під час виконання завдань різними службами. Системи кондиціювання у цих комплексах є невід'ємною частиною загальної системи життєзабезпечення та передбачає підвищені вимоги щодо надійності та ефективності [1].

При розробці мобільних комплексів доводиться заощаджувати вільний простір усередині комплексу, який значно обмежений. Всі ці фактори вимагають розробки особливої системи кондиціювання, призначеної на вирішення конкретних завдань. Вирішення такої важливої задачі допоможе забезпечити спеціальні служби та силові структури більш надійною системою кондиціювання, що відповідно покращить якість їх роботи, а в деяких випадках і боєздатність, і обороноздатність [2]. Отже, розробка автоматизованої системи кондиціювання для застосування в польових умовах, є актуальним завданням

Метою доповіді є розробка автоматизованої системи кондиціювання для застосування в польових умовах.

У доповіді наводяться результати дослідження основних елементів системи кондиціювання мобільних комплексів, що потребують спеціалізованого доопрацювання для застосування в польових умовах, існуючі методи тепловіддачі конденсаторів охолоджувальних систем. За допомогою комп'ютерного моделювання визначено найбільш ефективний методи тепловіддачі кондиціонерів. Розроблено структурна схема систем кондиціювання в польових умовах. Приведені методики розрахунку [3] основних параметрів автоматизованих системи кондиціювання.

Список літератури

1. A.Shinykulova, Y.Mailybayev, D.Isaykin, U.Umbetov, I.Kossyakov, (2020). Optimization of tourist transportation. *Journal of Theoretical and Applied Information Technology*. 98 (19), 3032-3042. E-ISSN 1817-3195.

2. A.Kossyakov, A.Shinykulova, G.Ivanov, B.Omarova, S.Omarova, Z.Zhusupbekov, (2021). Development of an automation program and PID controller coefficients testing for optimal controlling the air heating/cooling process in mobile complexes. *Journal of Theoretical and Applied Information Technology*. 99 (4), 946-956. E-ISSN 1817-3195.

3. H.Fazlollahtabar. Reliability Models of Complex Systems for Robots and Automation. CRC Press, Abingdon, UK, 2018.

ДОСЛІДЖЕННЯ СИСТЕМИ КЕРУВАННЯ ЕКЗОСКЕЛЕТОМ

Степанчук М. І., Туз В. В.
Черкаський державний технологічний університет, Черкаси, Україна

В даний час для вирішення проблем людей з обмеженими можливостями застосовуються медичні екзоскелети, які є справжніми помічниками. Слово «екзоскелет» перекладається як «зовнішній скелет», без якого люди з переломами хребта та різними травмами кінцівок просто втратили надію на можливість знову стати повноцінними членами суспільства [1]. У всьому світі проводиться дослідження та ведуться розробки екзоскелетів. Цей пристрій кріпиться зовні тіла і виконує необхідні функції.

Сучасний екзоскелет є складною технічною системою, вивчення якого базується на різні галузі науки: механіки, кібернетики, електроніки тощо. Системи керування приводами екзоскелетів застосовуються у багатьох областях дії людини, для реалізації руху яких за кожним ступенем рухливості ланок використовується роздільний керований електропривод [2].

Метою доповіді є розробити математичну модель динаміки екзоскелету з урахуванням нелінійних елементів електроприводів та методи керування електроприводами екзоскелету, що забезпечують його рух з необхідною точністю під дією зовнішніх збурень, нелінійних компонентів та невизначених параметрів динамічної моделі.

У доповіді наводяться результати дослідження існуючих науково-технічних розробок у галузі динамічної моделі руху екзоскелета та управління ним для людей з обмеженими можливостями нижніх кінцівок. Проведено моделювання системи керування електроприводами екзоскелета при роботі в умовах стохастичних зовнішніх збурень [3], невизначених параметрів динамічної моделі та нелінійних елементів у вигляді тертя та пружності.

Список літератури

1. K.Anam, A.A.Al-Jumaily, (2012). Active exoskeleton control systems: State of the art. *Procedia Engineering*. 41, 988-994.

2. S.Qiu, et al. ”Intelligent algorithm tuning PID method of function electrical stimulation using knee joint angle”, in: 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. (London, 2014).

3. E.O.Freire, F.G.Rossomando, C.M.Soria, (2018). Self-tuning of a neuroadaptive PID controller for a SCARA robot based on neural network. *IEEE Latin America Transactions*. 16 (5), 1364-1374.

МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ КОМБІНОВАНИХ ДАТЧИКІВ ДЛЯ ВИМІРЮВАННЯ ТИСКУ І ТЕМПЕРАТУРИ

Сугак М. В.
Черкаський державний технологічний університет, Черкаси, Україна

У зв'язку з розширенням сфер застосування датчиків фізичних величин, виникла необхідність створення низки суміщених датчиків[1] тиску та температури, стійких до впливу екстремальних зовнішніх факторів, зокрема температури, агресивного середовища, вібрацій та прискорень. Такі зовнішні фактори характерні для глибоких нафтових свердловин, авіації, ракет-носіїв та ін. Тому при розробці необхідно враховувати вплив зовнішніх факторів на чутливі структури датчиків, які проявляються у зниженні надійності, міцності, збільшенні похибки за рахунок генерації механічних та теплових деформацій у вузлах та елементах датчиків, які дуже важко виміряти та врахувати.

Слід зазначити, що в даний час найбільш перспективними стають багатофункціональні мікроелектронні датчики[2], які дозволяють проводити одночасне вимірювання декількох фізичних величин в одній точці. При цьому моделі та конструкції є розподіленими багатовимірними структурами, які дуже складно моделювати. Особливу роль у процесі їх проектування набувають методи математичного моделювання, застосування яких дозволяють суттєво скоротити терміни та витрати на розробку датчиків

Метою доповіді є розробка та впровадженні сучасних принципів математичного моделювання в область компонентів комбінованих датчиків тиску та температури.

У доповіді наводяться результати огляду проведеного дослідження, яке виявило, що існують розрізнені дорогі програми та методики[3], що дозволяють моделювати теплові та деформаційні поля у датчиках. На жаль, ці ліцензійні програми, засновані на звичайно різницевих методах, дуже дорого коштують, крім того, вони трудомісткі в освоєнні. Тому традиційний інженерний підхід до розрахунку елементів датчиків, доповнений практичними результатами, дозволяє ефективно моделювати ДДТ. Представлено математичну модель з компенсації впливу зовнішніх факторів

Список літератури

1. Process Control of Technological Processes. URL: https://www.ispatguru.com/process-control-of-technologicalprocesses/?utm_source=rss&utm_medium=rss&utm_campaign=process-control-oftechnological-processes. Access: 01.11.2022.

2. Контрольно-вимірювальні прилади та автоматика. Honeywell Україна, URL: http://www.iac.honeywell.com. Access: 01.11.2022.

3. Z.Bayasilova, P.Mikhailov, M.Baktybayev, M.Tatiyeva, A.Seidildayeva, (2018). Multi-functional sensors for control systems and monitoring. *International Journal of Mechanical Engineering and Technology (IJMET).* 9 (13), 959–967.

ДОСЛІДЖЕННЯ ТА УДОСКОНАЛЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ВИЯВЛЕННЯ ДЕФЕКТІВ У БУДІВЕЛЬНИХ СПОРУДАХ

Тіпалов М.С., Туз В.В.
Черкаський державний технологічний університет, Черкаси, Україна

Більшість великогабаритні залізобетонні будівельні конструкції є плоскопаралельними структурами (стіни, перекриття та ін.), до яких відсутній двосторонній доступ. З цієї причини ультразвуковий неруйнівний контроль таких об'єктів можливий, як правило, тільки із застосуванням ехоімпульсного методу контролю. Однак за допомогою традиційних одноканальних приладів у більшості випадків здійснити такий луна-контроль не вдається[1].

Ультразвуковий неруйнівний контроль застосовується не до всіх марок бетону [2], та для плоско паралельних конструкцій. Разом з тим, у зв'язку з розвитком монолітного будівництва, все частіше з'являються конструкції з нестандартною поверхнею, що приводить до неможливості контролювати якість конструкції існуючими приладами. Розробка ультразвукового приладу для контролю нестандартних поверхонь конструкцій є актуальною задачею.

Метою доповіді присвячена дослідженню та удосконаленню автоматизованої системи виявлення дефектів у будівельних спорудах.

У доповіді наводяться багатофункціональний ультразвуковий томограф будівельних конструкцій для складних поверхонь бетонних конструкцій. Представлена конструкція адаптивної ультразвукової антеної решітки, конфігурацію якої можна довільно змінювати, адаптивно підлаштовуючи під форму поверхні контрольованого виробу. Досліджено безеталонний спосіб [3] вимірювання швидкості поширення ультразвукових коливань, заснований на обробці сукупності сигналів, що дозволяють підвищити достовірність та точність визначення координат дефектів та габаритів виробу.

Список літератури

1. H.G.Kraus, (1983). Generalized Synthetic aperture, focused transduser, pulse-echo, ultrasonic scan data processing for non-destructive inspection. *Ultrasonics*. 21 (l), 118.

2. V.K.Kachanov, I.V.Sokolov, A.A.Sinitsyn, R.V.Kontsov, M.B.Fedorov, (2017). Application of «Focusing in a Point» Algorithm for Standard-Exclusion Measurement of Ultrasound Velocity in the Process of Tomography of Concrete Product». *Journal of Engineering and Applied Sciences. Asian Research Publishing Network (ARPN)*. 12 (24), 7172-7178. ISSN 1819-6608.

3. S.Pudovikov, A.Bulavinov, R.Pinchuk. “Innovative Ultrasonic Testing (UT) of Nuclear Components by Sampling Phased Array with 3D Visualization of Inspection Results”, in: 8th International Conference on NDE in Relation to Structural Integrity for Nuclear and Pressurised Component “JRC-NDE 2010”, (Berlin, 2010).

РОЗРОБЛЕННЯ ТА ДОСЛІДЖЕННЯ АВТОМАТИЧНОЇ ФОТОЕЛЕКТРИЧНОЇ СИСТЕМИ ЕЛЕКТРОЗАБЕЗПЕЧЕННЯ

Шевченко Д.І., Туз В.В.
Черкаський державний технологічний університет, Черкаси, Україна

Потреби населення та промисловості в електричній енергії обмежені запасами нафти та газу, що призводить до необхідності використання поновлюваних джерел енергії. В даний час одним із найважливіших завдань електроенергетики є забезпечення надійного, безперебійного електропостачання всіх промислових та побутових об'єктів [1].

Розвиток малих сонячних фотоелектричних установок, що працюють як паралельно з мережею, так і в автономному режимі, може покращити електропостачання побутових споживачів ефективніше та швидше, ніж розвиток великої енергосистеми. Тому робота, присвячена дослідженню та вдосконаленню обладнання малої сонячної фотоелектричної установки є актуальною та має велике практичне значення [2].

Теми є актуальною у зв'язку з тим, що: досліджено малі фотоелектричної установки в умовах тропічного клімату. Не виявлено оптимізацію структури ФЕУ з неорієнтованої сонячної батареї (СБ), гелевого акумулятора та інвертора при різних напругах елементів. Недостатньо досліджена та не висвітлена у науково-технічній літературі робота однофазних інверторів з низьким коефіцієнтом гармонік та швидким способом регулювання напруги у фотоелектричній установки.

Метою доповіді є створення автономної системи електропостачання для тропічних умов на основі фотоелектричної установки.

У доповіді наводяться результати дослідження малих фотоелектричних установ в умовах тропічного клімату. Досліджено варіантів структурних схем [3] та вибір оптимальної схеми. Створено модель фотоелектричної установки, що враховує активно – індуктивну характер навантаження та кліматичні умови. Розроблено швидкодіючу схему регулятора напруги інвертора, що забезпечує точність стабілізації напруги у широкому інтервалі навантажень та температур з низьким коефіцієнтом нелінійних спотворень.

Список літератури

1. Сонячна електростанція, URL: http://ishop.sutem.com.ua/articles/topics/solar_energy/SES. Access 01.11.2022.

2. Renewable energy players leading the way in Ukraine, URL: https://www.kyivpost.com/technology/renewable-energy-players-leading-wayukraine.html. Access 01.11.2022.

3. Є.Р.Куцаченко, К.С.Клен, “Вибір параметрів фотоелемента для моделювання сонячної панелі”, в: Матеріали Всеукраїнської Науково-практичної конференції «Новітні Технології Сучасного Суспільства» (НТСС-2018) (Київ, 21 (6), 2018).

АВТОМАТИЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ СТАНУ ЛЮДИНИ

Яценко Ю.Ю., Туз В.В.
Черкаський державний технологічний університет, Черкаси, Україна

Сучасний спорт найвищих досягнень потребує безперервного вдосконалення методів та технологій побудови програми підготовки у тренувальному процесі з урахуванням індивідуальних особливостей організму спортсмена, заснованих на обліку його психофізіологічного стану та фізичної працездатності [1].

У процесі тренувань за фізичних навантажень фізіологічний резерв організму поступово знижується. Хоча відомо, що функціональне регулювання систем організму людини взаємопов'язане і зачіпає всі системи організму, оцінювати фізіологічний резерв спортсмена лише за одним обмеженим набором фізіологічних показників недостатньо. Оцінювати фізіологічний резерв необхідно за комплексом показників [2], що відбивають функціонування життєво важливих систем організму. Проте відсутні дослідження, присвячені міжсистемним взаємозв'язкам показників діяльності систем організму та його динаміці. Все це підтверджує актуальність розробки системи моніторингу та оцінки стану спортсмена у реальному режимі часу, яка дозволить йому спостерігати та контролювати діяльність різних систем організму.

Метою доповіді є Автоматизація системи моніторингу стану людини, що дозволяють комплексно вивчати фізіологічний резерв спортсмена під час тренувального процесу в реальному часі.

У доповіді наводяться результати дослідження формування комплексу приватних показників для оцінки фізіологічного резерву спортсмена, що відбивають метаболізм організму та функціонування систем організму спортсмена в умовах тренувального процесу при фізичних навантаженнях. представлена узагальнена структура просторово-розподіленої системи біотехнічної системи та структури підсистеми знімання, реєстрації, обробки та аналізу біомедичних сигналів [3] для оцінки фізіологічного резерву спортсмена.

Список літератури

1. L.R.Keytel, J.H.Goedecke, T.D.Noakes, H.Hiilloskorpi, R.Laukkanen, L.Van Der Merwe, E.V.Lambert, (2005). Prediction of energy expenditure from heart rate monitoring during submaximal exercise. *J Sports Sci*. 23(3), 289–297.

2. M.T.Nguyen, et al. "Development of a method and a system for evaluation sportsman's physiological reserves", in: AIP Conference Proceedings. (AIP Publishing, 2140 (1), 2019).

3. J.Gu-Young, Yu Kee-Ho, K.Nam-Gyun. "Continuous Blood Pressure Monitoring using Pulse Wave Transit Time", in: International conference on Control, Automation and systems "ICCAS 2005" (2005).

ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ АЛГОРИТМУ ДІАГНОСТУВАННЯ НЕСПРАВНОСТЕЙ СИСТЕМ УПРАВЛІННЯ

Грекуляк М.В.
Відокремлений структурний підрозділ Національного авіаційного університету «Льотна академія Національного авіаційного університету»
Кропивницький, Україна
Кухтін М.О.
Військовий інститут танкових військ Національного технічного університету «Харківський політехнічний інститут», Харків, Україна

Процес діагностування несправностей систем управління різного призначення направлений на визначення як поточного технічного стану, так і виявлення можливої несправності при його зміні протягом визначеного часу в процесі експлуатації [1]. Ознаками технічного стану систем управління можуть бути певні значення кількісних і якісних характеристик, для яких визначені допустимі області змінювання. Залежно від фактичних значень цих характеристик розрізняють наступні види технічного стану систем управління: справне або несправне; працездатне або непрацездатний; правильно функціонує або неправильно функціонує [2].

Метою доповіді є розробка пропозицій до удосконалення алгоритму діагностування несправностей систем управління різного призначення.

У доповіді пропонується при діагностуванні несправностей систем управління застосовувати наступні методи [3]: метод перевірок за елементами; метод групових перевірок; метод середніх точок; метод зовнішнього огляду; метод заміни елемента на завчасно справний; метод виключення; метод тестового діагностування; метод користування таблицею або карткою опорів, режимів та сигналів; метод порівняння елемента зі справним елементом (еталоном); комплексне використання усіх вказаних методів.

Наведено результати впровадження сучасних методів і систем діагностування, доведено можливість зведення до мінімуму кількості несправностей і тривалості їх усунення за рахунок прогнозування змін у технічному стані.

Список літератури

1. Яровий В.С., Радзівілов Г.Д., Кірвас В.В. Діагностика несправностей випрямних трансформаторів високочастотних джерел живлення на основі визначення особливостей струму. *Наука і техніка Повітряних Сил Збройних Сил України*. 2021. № 4 (45). С. 152–162. DOI: https://doi.org/10.30748/nitps.2021.45.19

2. Daki O., Herasimov S., Zubrytskyi H. Digital Correlation Method For Power Measurement. *Information Processing Systems*. 2020. № 4 (163). С. 15–26. DOI: https://doi.org/10.30748/soi.2020.163.02

3. Herasimov S., Borysenko M., Roshchupkin E. Spectrum Analyzer Based on a Dynamic Filter. *Journal of Electronic Testing*. 2021. № 37. С. 357–368. DOI: https://doi.org/10.1007/s10836-021-05954-0

АНАЛІЗ СИСТЕМИ ТЕРМОРЕГУЛЮВАННЯ СПЕЦІАЛЬНОЇ ТЕХНІКИ

Червотока О.В., Чередніков О.М., Лаппо І.М.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Чернігів, Україна

Одним із завдань забезпечення високої готовності зразків спеціальної техніки є аналіз систем їх терморегулювання і розроблення нових та удосконалення відомих методів і засобів вимірювання температури із заданими метрологічними характеристиками [1]. На етапі проведення вимірювань можна виділити наступні основні завдання: встановлення раціональної номенклатури параметрів, що підлягають вимірюванню та контролю; встановлення вимог до точності вимірювань і діапазонів вимірювань; розробка методів вимірювання та визначення складу засобів вимірювальної техніки; встановлення вимог до засобів вимірювальної техніки, призначених до застосування при створенні, експлуатації та випробовуванні зразків спеціальної техніки тощо [2].

Одним із основних факторів, який впливає на точність вимірювання, є температура [3]. Проблема забезпечення необхідної точності вимірювальної інформації про стан сучасних видів військової техніки та засобів вимірювання температурних характеристик на етапах їх розробки, виробництва і експлуатації потребує проведення аналізу умов застосування.

Метою доповіді є аналіз систем терморегулювання спеціальної техніки, дослідження метрологічних характеристик вимірювача та розробка пропозицій щодо застосування мікропроцесору для корекції похибок вимірювання температури.

У доповіді розглянуті засоби вимірювальної техніки та способи вимірювання температури і типи температурних датчиків в мікропроцесорних системах терморегулювання. Показані особливості побудови систем терморегулювання в умовах відсутності теплообміну тіл з навколишнім середовищем та наведено модель мікропроцесорного вимірювача температури.

Список літератури

1. Будова та види датчиків температури в кліматичних системах [Електронний ресурс]. – Режим доступу: https://ds-electronics.com.ua

2. Бурсала О., Голуб В., Чередніков О., Чуприна В., Коваленко І. Визначення показників експлуатаційної надійності авіаційної техніки з врахуванням рекомендацій ІСАО. *Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*, 2021, 9 (3), С. 25-35. DOI: https://doi.org/10.37701/dndivsovt.9.2021.04

3. Подорожняк А. О., Клименко А. М. Дослідження мікропроцесорної системи контролю температури серверної кімнати. *Системи управління, навігації та зв'язку*, 2017, № 2 (42), С. 51-54. [Електронний ресурс]. – Режим доступу: http://journals.nupp.edu.ua/sunz/article/view/667

ПРОПОЗИЦІЇ ЩОДО АНАЛІЗУ РАДІОЕЛЕКТРОННИХ СИСТЕМ ЯК ОБ'ЄКТА КОНТРОЛЮ

Ольховіков Д.С.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

Функціонування радіоелектронних систем залежить від їх справного технічного стану. Під час експлуатації технічний стан може змінюватися як прогнозовано (згідно результатів проведення діагностування) або відбуватися непрогнозоване змінювання (навидь вихід із ладу) [1]. Тому під час експлуатації радіоелектронних систем необхідна відповідна апаратура для контролю технічного стану [2]. При цьому важливо розробити алгоритм для проведення аналізу радіоелектронних систем для визначення їх технічного стану [3].

Метою доповіді є розробка пропозицій до алгоритму аналізу радіоелектронних систем для визначення їх технічного стану.

У доповіді показано, що апаратура контролю радіоелектронних систем за призначенням складається, як правило, із генератора вхідних сигналів і аналізатора характеристик вихідного сигналу цих систем (як об'єкта контролю). Обгрунтована доцільність і можливість створення алгоритму, за яким оцінюється змінення технічного стану радіоелектронних систем під час експлуатації.

З метою підвищення достовірності та оперативності контролю технічного стану радіоелектронних систем запропоновано використання комбінованого алгоритму. Цей алгоритм передбачає використання результатів визначення відхилень невеликої кількості найбільш суттєвих параметрів контролю як вхідного сигналу, так і застосування оптимального методу обробки відгуку на вхідні впливи (вихідного сигналу). Передбачено використання результатів визначення середнього значення вихідного сигналу, а для інтегральної оцінки технічного стану – зміна всіх інших параметрів контролю – метод, заснований на визначенні середньоквадратичного значення вихідного сигналу неузгодження.

Список літератури

1. Яровий В.С., Радзівілов Г.Д., Кірвас В.В. Діагностика несправностей випрямних трансформаторів високочастотних джерел живлення на основі визначення особливостей струму. *Наука і техніка Повітряних Сил Збройних Сил України*. 2021. № 4 (45). С. 152–162. DOI: https://doi.org/10.30748/nitps.2021.45.19

2. Daki O., Herasimov S., Zubrytskyi H. Digital Correlation Method For Power Measurement. *Information Processing Systems*. 2020. № 4 (163). С. 15–26. DOI: https://doi.org/10.30748/soi.2020.163.02

3. Herasimov S., Borysenko M., Roshchupkin E. Spectrum Analyzer Based on a Dynamic Filter. *Journal of Electronic Testing*. 2021. № 37. С. 357–368. DOI: https://doi.org/10.1007/s10836-021-05954-0

СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ЕЛЕКТРИЧНИМ ОПАЛЕННЯМ БУДИНКУ

Ігнатюк Є.О., Лещенко Ю.О.
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

На сьогоднішній день концепція «Розумний дім» – це область, яка стрімко розвивається, і на це є декілька причин [1]. По-перше, це обумовлено необхідністю в комфортних умовах життя та роботи, а по-друге, енергозбереженням, раціональним та грамотним використання теплової енергії.

У будь-якій системі управління опаленням, оптимальним завданням є управління температурою в приміщенні та створення, у відповідності до призначення приміщень, комфортних для людей умов. Тому невід'ємним елементом системи «Розумний будинок» є система для керування температурою приміщення [2].

Метою доповіді є розробка системи для ефективного керування температурним режимом в приміщенні.

В доповіді викладено ідею цього проекту, що полягає в тому, щоб розробити таку систему управління температурою приміщення, яка б не тільки регулювала температуру в дистанційному режимі, але і автоматично вмикалась і вимикалась, в залежності від температури та навколишніх умов. Дистанційне керування опаленням, в залежності від численних внутрішніх і зовнішніх умов, дозволяє досягти значної економії енергоресурсів та створити комфортний мікроклімат в приміщенні. Таким чином, створюється зональний клімат, коли власник може встановити параметри мікроклімату окремо для кожної зони.

Для реалізації цієї системи був використаний комплекс з герметичних датчиків температури DS18B20, мікропроцесор ESP8266 та реле. Забезпечення передачі даних відбулось за допомогою програми на мові C++.

Розроблена система дозволяє вимірювати температуру приміщення за допомогою датчиків, забезпечувати користувачеві відслідковування температури приміщень, налаштовувати бажану температуру в кожній кімнаті, забезпечувати економію електроенергії за рахунок вимкнення системи, вмикати і вимикати опалення у відповідності з бажаним температурним режимом та сповіщати користувача про критичний рівень температури в приміщенні.

Список літератури

1. Кращі системи "Розумний будинок" по виробниках 2022 року. ТОП 5 надійних та якісних систем "Розумний будинок" рейтингу [Електронний ресурс] – Режим доступу: https://vencon.ua/ua/articles/reyting-sistem-umnyy-dom-po-proizvoditelyam

2. Що таке «розумний будинок» і навіщо він потрібен? [Електронний ресурс] – Режим доступу: https://stylus.ua/uk/articles/528.html

ФУНКЦІОНАЛЬНИЙ КОНТРОЛЬ ДИСКРЕТНИХ ПРИСТРОЇВ

Павлик Г.В.
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

Комп'ютерні системи знаходять широке застосування в різних галузях науки і техніки при побудові систем керування, регулювання, передачі та обробки дискретної інформації. Для забезпечення необхідного рівня якості їх функціонування і надійності застосовуються різні підходи: вдосконалення існуючих та організація принципово нових систем, їх апаратних і програмних засобів, створення алгоритмічного, апаратно-програмного, контрольно-діагностичного забезпечення, розробка та застосування методів і засобів функціонального і тестового діагностування на етапах проектування, виготовлення та експлуатації комп'ютерних систем і їхніх компонентів.

Розробка діагностичного забезпечення є складною задачею, тому що необхідно задовольняти цілому ряду найчастіше суперечливих вимог до швидкодії, апаратурних витрат, надійності функціонування і т.д. Тому одержує поширення системний підхід до дослідження та проектування структури засобів діагностування, що дозволяє врахувати множину факторів і знайти оптимальну реалізацію системи. Також певну проблему представляє контроль складних цифрових систем у зв'язку з великою кількістю можливих станів і труднощів моделювання та значна функціональність. Типові задачі: пошук мінімальних тестів, вибір оптимального складу перевірок та ін. є логіко-комбінаторними задачами з перебором значної кількості варіантів [1, 2].

Метою доповіді є підвищення ефективності контролю і діагностування шляхом розробки методів формального перетворення діагностичних моделей в автоматизованих системах контролю за рахунок вибору оптимальної структури контрольно-діагностичного забезпечення. Розроблений метод функціонального контролю дискретних пристроїв, заснований на комбінаторному підході до класифікації об'єктів. Пошук оптимального рішення серед заданої множини варіантів надзвичайно складний і вирішується шляхом перебору, однак у більшості задач такий повний перебір нездійсненний. Для зменшення кількості варіантів, що розглядаються, на множині всіх об'єктів вводяться відношення еквівалентності й множина всіх об'єктів розбивається на класи еквівалентності.

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 Anal-ysis / T. Knuppel, M. Blanke, J. Stergaard // International Journal of Robust and Nonlinear Control, 2014. – V. 24. – P. 1446 – 1465.

УЧАСНИКИ КОНФЕРЕНЦІЇ (крім секції 4)

ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

Військова Академія Збройних Сил Азербайджанської республіки, Баку, Азербайджан

Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна

Державне підприємство "Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості", Харків, Україна

Державний біотехнологічний університет, Харків, Україна

Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Чернігів, Україна

Державний університет інфраструктури та технологій, Київ,, Україна

Національний технічний університет України "Київський політехнічний інститут ім. Ігора Сікорського", Київ, Україна

Київський національний університет будівництва і архітектури Київ, Україна

Київський національний університет імені Тараса Шевченка, Київ, Україна

Криворізький фаховий коледж Національного авіаційного університету, Кривий Ріг, Україна

Льотна академія Національного авіаційного університету, Кропивницький, Україна

Національна академія Національної гвардії України, Харків, Україна

Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, 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

Національний університет оборони України імені Івана Черняховського, Київ, Україна

Університет Аделаїди, Аделаїда, Південна Австралія

Університет технології і гуманітарних наук, Бельсько-Бяла, Польща

Харківський гуманітарний університет «Народна українська академія», Харків, Україна

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

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

Харківський національний університет радіоелектроніки, Харків, Україна

Черкаський державний бізнес-коледж, Черкаси, Україна

Черкаський державний технологічний університет, Черкаси

Черкаський національний університет імені Богдана Хмельницького, Черкаси, Україна

Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України, Черкаси, Україна

ЗМІСТ

Наукове видання

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

Тези доповідей
десятої міжнародної науково-технічної конференції
24 – 25 листопада 2022 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 23.11.2022 Формат 60 × 84/16
Ум.-вид. арк. 7,75. Тираж 200 пр. Зам. 1123-22
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**