МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

ТИЖДЕНЬ НАУКИ-2021.
Факультет радіоелектроніки та телекомунікацій

Збірник тез доповідей щорічної
науково-практичної конференції викладачів, науковців,
молодих учених, аспірантів та студентів

19–23 квітня 2021 року

Електронне видання на DVD-ROM

м. Запоріжжя

УДК 621.3+004+519.6
Т39

Рекомендовано до видання Вченою радою
Національного університету «Запорізька політехніка»
(Протокол засідання вченої ради 10/21 від 12.04.2021)

Тези доповідей друкуються методом прямого відтворення тексту, представленого авторами, які несуть відповідальність за його форму і зміст.

Т39 **Тиждень науки-2021. Факультет радіоелектроніки та телекомунікацій.** Тези доповідей науково-практичної конференції, Запоріжжя, 19–23 квітня 2021 р. [Електронний ресурс] / Редкол. :В. В. Наумик (відпов. ред.) Електрон. дані. – Запоріжжя : НУ «Запорізька політехніка», 2021. – 1 електрон. опт. диск (DVD-ROM); 12 см. – Назва з тит. екрана.
ISBN 978-617-529-316-4.

Зібрані тези доповідей, заслуханих на щорічній науково-практичній конференції викладачів, науковців, молодих учених, аспірантів та студентів. Збірка відображає широкий спектр тематики наукових досліджень, які проводяться на факультеті радіоелектроніки та телекомунікацій Національного університету «Запорізька політехніка». Збірка розрахована на широкий загал дослідників та науковців.

ISBN 978-617-529-316-4.

ЗМІСТ

СЕКЦІЯ «РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ»

УДК 001.891.53

Поляков М.О.[1]
[1] проф. НУ «Запорізька політехніка»

ЦЕНТР ЕКСПЕРІМЕНТІВ У «ЗАПОРІЗЬКІЙ ПОЛІТЕХНІЦІ»

У даний час актуальна задача залучення абітурієнтів до нашого університету. Вона може бути вирішена шляхом популяризації досягнень науки та техніки. Мета цієї роботи - привернути увагу до бурхливого розвитку одного з напрямків у цій області, який має багато назв: «експеріментаніум», «музей цікавих наук», «науковий атракціон», «місце де наука стає цікавою» і багато інших.

Йдеться про те, щоб зібрати «під одним дахом» лабораторні установки для проведення експериментів, які наочно демонструють фізичні та технічні явища і процеси.

На території країн СНД такі музеї існують більше 10 років і демонструють сотні видовищних експериментів. Функціонують вони у Києві та Запоріжжі. Відомо про плани створення ще одного такого музею в Запоріжжі на базі колишнього Будинку побуту. Музеї залучають широку аудиторію та комерційно успішні, але вони не демонструють технічно складних експериментів, які є в нашому університеті. Наприклад штучні блискавки, віддалені лабораторії, танцюючи роботи, «вічні двигуни», 3D – принтери, розумні будинки та когнітивні телекомунікації – усе не перелічити.

Створення на базі «Запорізькій політехніки» центру експериментів «Політехекспериментаніум» дозволить на постійній основі проводити профорієнтаційну роботу в формі науково-розважальних шоу, тематичних шкільних екскурсій і так далі.

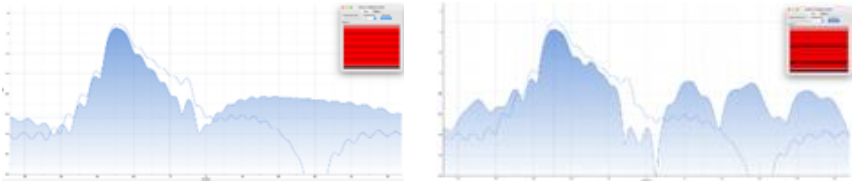
Вважаю, що завдання створення в нашому університеті такого центру вирішене в постановці та треба терміново переходити до наступних етапів. Наприклад пропоную створити робочу групу для підготовки ескізного проекту центру експериментів.

UDC 65.012.32:399.5
Deneka M.A[1], Bugrova T.I.[2]
[1] stud. gr. RT-217 NU «Zaporiz`ka Politekhnica»
[2] assistant professor NU «Zaporiz`ka Politekhnica»

ANTENNA WITH COSECANT PATTERN

Modern active phased antenna array consists of either several active elements or several thousands. There is a possibility of failure of one or more radiating elements during the operation. Antenna pattern can be significantly damaged. The level of damage depends on the percentage of affected elements and their location on the surface of the antenna aperture. We consider one-dimensional transmitting antenna array used in surface radars, such as radar 80K6T/90K6E. Element damage leads to significant distortion of the detection zone of the radar in the elevation plane. The scientific novelty of the work lies in using of synthesis method for complex coefficients of field distribution for the levelling of one or more broken elements. The method will allow to restore zone of detection of the radar targets and the accuracy detection of coordinates at the elevation plane. The goal is to improve the reliability and stability of the tactical and technical characteristics of the radar, which is very important for the advancement of the defense development. Radar 80K6T has one-dimensional array, which is built of open type radiating waveguides (W-lines). The use of a one-dimensional phased array makes the radar vulnerable to the failure of one or more elements. The simulation results and the effect on the shape of the pattern for several cases of failure of individual elements can be seen in Fig. 1. It shows that different elements have different degrees of influence on the formation of the pattern. ailure of the second element in general caused a decrease in the main lobe by 2 dB, which is equivalent to a decrease in the range of the radar in the main direction by ~ 12%. This is equivalent to a decrease in the detection range of the target by 48 km. In this case of failure we notice that these effects are summing up. The compensation for the impact of defective element is an urgent problem that needs solving. The introduction of the method of adjusting the phase distribution of the field in the aperture of the transmission grid will allow to restore the detection zones of the radar in the angular plane without interrupting the operation of the radar.

The algorithm of damaged pattern correction consists of uniform search for complex coefficients of distribution along a lattice which give the greatest correlation coefficient between the calculated and pattern at all undamaged elements. It should be noted that it makes sense to assess the degree of correlation not for all values of the spatial angle of view θ, but only in the interval of the main lobe - because the priority is the restoring of the level and shape of the main lobe.



a – 2nd broken element; b – 2nd, 7th 18th elements.
Figure 1 – Antenna pattern.

Mathematical modeling of antenna array and pattern correction was developed using the IDE Xcode. To speed up calculations, some of them were implemented on the GPU using the low-level API Metal.

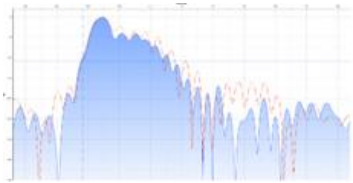


Figure 2 – Comparison of patterns without correction algorithm (red line) and with algorithm (blue line).

As can be seen from Figure 2, the correction method allows to reduce the level of oscillations of the pattern within the main lobe and level the gap of 5 dB in the direction of ~ 3º, as well as reduce the level of side petals as a whole. As was shown by mathematical modeling of the algorithm for the correction of defects in the amplitude-phase distribution of the antenna array, the proposed method allows to improve the antenna performance in the presence of defective elements. It is appropriate to establish different limits for estimating the correlation in the algorithm to obtain the greatest efficiency.

If you set the correlation limits only in the range of the main petal of the pattern, it allows you to get the best correction for the main lobe but will inevitably lead to some increase in the level of the lateral petal. An indisputable advantage of the proposed method of adjusting the phase distribution of the field in the grating aperture is the ability to restore the detection zone of the radar in the angular plane directly on the combat duty.

УДК 621.396.67
Бугрова Т.І.[1], Баранов В.А.[2]
[1] доц. НУ «Запорізька політехніка»
[2] студ. гр. РТ-218сп НУ «Запорізька політехніка»

РОЛЬ МЕТАМАТЕРІАЛІВ У КОНСТРУКЦІЇ MIMO АНТЕН

В наш час з'явилась зацікавленість до використання метаматеріалів (штучних середовищ з додатними та від'ємними електрофізичними параметрами) у конструкціях антен Усі типи середовищ можна поділити на 4 групи: DPS (діелектрик), ENG, MNG і DNG.

Рисунок 1 – Типи середовищ

В роботі досліджувались середовища типу ENG, MNG. Поява способу легкого виготовлення цих середовищ у вигляді метаматеріалів і надає можливість для їх використання при побудові антен. На відміну від вже відомих конструкцій з використанням метаматеріалів, особливість цієї роботи полягає у використанні метаматеріалу в антені MIMO типу. Поки що ці антени використовуються для 3G-4G зв'язку, тобто в діапазоні від 1800 до 2700 МГц; але за допомоги метаматеріалу є можливим розширення застосування антени MIMO до 5G-6G стандарту. Конструктивно це є антенною решіткою з елементом випромінювання у вигляді антени директорного типу, яку показано на рис.2.

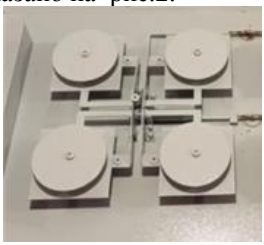
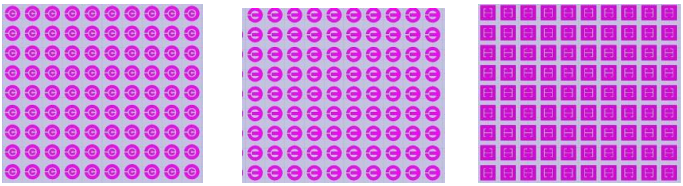


Рисунок 2 – Конструкція антени MIMO

Металевий директор антени MIMO замінено на директор із метаматеріалу, три варіанти геометрії якого зображено на рис. 3. Впродовж дослідження запропонованих структур за допомогою середовища електродинамічного 3D аналізу HFSS 17.2 вдалося виявити, що шляхом зміни розмірів, конфігурації та типу елементів метаматеріалу можна налаштовувати відповідну резонансну частоту антени і узгоджувати її з фідером живлення.

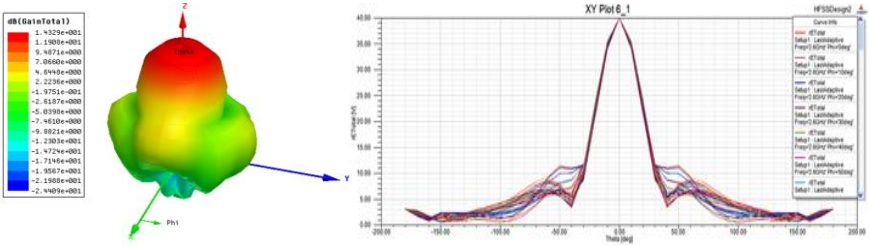


а б в

Рисунок 3 – Структури матеріалів: а,б-MNG матеріал; в-ENG матеріал.

Товщина елементів і відстань між ними регулюють ступінь металізації метаматеріалу, а значить, і рівень взаємодії з електромагнітним полем випромінювача. Значні зміни характеру впливу матеріалу також відбуваються при переході від елементів MNG-типу ($\varepsilon>0$, $\mu<0$), де переважають струми провідності, до матеріалу ENG-типу ($\varepsilon<0$, а $\mu>0$), де переважають струми зміщення. Встановлено, що в діапазоні 1,8 … 2,7 ГГц розміри елементів повинні знаходитись у межах 2…1,5 мм, а відстань між ними повинна бути порядку 250…500 мкм.

На рис. 4 показані 3D (а) і 2D (б) діаграми спрямованості антени. ЇЇ коефіцієнт підсилення змінюється від 14,3 дБ на частоті 2,6 ГГц до 19,7 дБ на частоті 3.2 ГГц.



а б

Рисунок 4 – Просторова діаграма спрямованості

Внаслідок застосування метаматеріалів в складі MIMO антен відбувається зміщення усіх характеристик антени у бік більш високих частот.

При цьому робочий діапазон частот антени розширюється до меж 1,8…3 ГГц, покращується узгодження антени з фідером (внаслідок чого коефіцієнт стоячої хвилі не перевищує значення 1,21). Потенційних виробників та споживачів цього інноваційного продукту можуть зацікавити зменшені лінійні розміри та маса антени MIMO у порівнянні з наявними аналогами на ринку антен з просторовим рознесенням.

УДК 621.396.67
Бугрова Т.І.[1], Зуєв Д.В.[2]
[1] доц. НУ «Запорізька політехніка»
[2] студ. гр. РТ-218сп НУ «Запорізька політехніка»

СИСТЕМА ДИСТАНЦІЙНОГО КЕРУВАННЯ МІКРОКЛІМАТОМ ВЕРТИКАЛЬНОГО ТЕПЛИЧНОГО КОМПЛЕКСУ ЗА ДОПОМОГОЮ GSM КАНАЛУ

Зараз багато хто, навіть геть далекі від сільського господарства люди, захоплено розповідає про вертикальні ферми. Однак з'явились у нашій країні й ті, хто від розмов перейшов до справ. І їхнім досвідом вже встигли зацікавитися в ОАЕ і навіть у Європі, звідки й прийшла до нас технологія вертикальних ферм. Їх розмір – від метрової шафи чи вантажного контейнера до великого тепличного комплексу. Головні переваги – економне використання площі й води, незалежність від погоди, прискорене дозрівання культур та можливість збирати врожаї цілий рік. Їх ключовий елемент – система дистанційного керування мікрокліматом по GSM каналу.

GSM і GPRS модуль в проектах Arduino дозволяє підключатися до віддалених автономних пристроїв через звичайний стільниковий зв'язок. Модуль надає можливість відправляти команди на пристрої і приймати інформацію від нього за допомогою SMS-команд або через інтернет-з'єднання, відкрите по GPRS. GSM модуль використовується для розширення можливостей звичайних плат Arduino – відправка SMS, здійснення дзвінків, обмін даними по GPRS (рис.1).

Рисунок 1 – Під'єднання Arduino з GSM / GPRS Shield

В роботі був обраний модуль GSM/GPRS Shield, A6, який дозволяє працювати в мережах стільникового зв'язку за технологіями GSM/GPRS для

прийому/передачі даних, відправлення/отримання SMS (Short Message Service) і здійснення телефонного голосового зв'язку.

Для розширення можливої кількості підключених плат до Arduino використана плата Trema Shield. Trema Shield встановлюється на Arduino, а модулі підключаються проводами до колодок Trema Shield. Електромеханічне реле побудоване на базі «HF115F/005-1Z3BF», що і забезпечує його комутаційну здатність.

Реле модуля здатне комутувати вихідні ланцюги з напругою до 250 В змінного струму (AC), або до 30 В постійного струму (DC). В свою чергу силовий ключ (модуль) на двох польових транзисторах AOD4184 призначений для комутації навантаження з максимальною напругою до 36В і струмом до 15А при кімнатній температурі. Trema - модуль твердотільного реле (SSR-Solid-State Relay) – призначено для замикання вихідного ланцюга змінного струму (з номінальною напругою до 240 В), при подачі керуючого сигналу 5В постійного струму на вхід модуля.

Під'єднання лінійного приводу необхідно для керування закриттям/відкриттям фрамуг провітрювання при надмірних вологості або температурі. Підключення лінійного приводу здійснюється до Trema Shield. Для цього під'єднано два електромеханічних реле до четвертого виводу на Trema Shield. Після цього встановлюються перемички та під'єднується реле до лінійного приводу згідно з рисунком 2. Далі підводться зовнішнє живлення 12В.

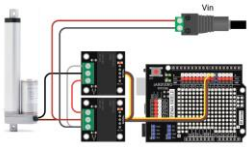
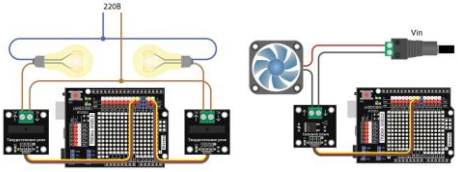


Рисунок 2 - Під'єднання лінійного приводу

Для забезпечення освітлення під'єднано два твердотільних реле (рис.3, а до виводів два та три плати Trema Shield).



а) б)

Рисунок 3 – Під'єднання освітлення (а) і вентиляції (б)

Для забезпечення вентиляції під'єднано силовий ключ до виводу п’ять плати Trema Shield (рис.3, б). До силового ключа підключається кулер,

пропустивши провід живлення (червоний) напряму до джерела живлення 12В, а провід GND вентилятора (чорний) в розріз між Trema Shield та силовим ключем.

Відомо, що величина врожаю і його якість, а також собівартість виробництва залежать від точного регулювання балансу таких факторів, як температура, LED освітленість, режим вологості повітря і субстрату, вміст кисню, CO_2 в приміщенні і доступних елементів живлення. Їх регулювання відбувається за допомогою системи дистанційного керування мікрокліматом вертикального тепличного комплексу .

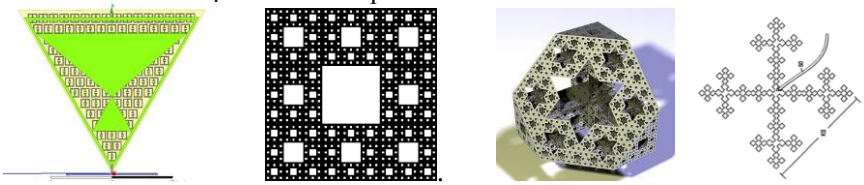
УДК 621.396.67
Бугрова Т.І.[1], Решетников О.О.[2]
[1] доц. НУ «Запорізька політехніка»
[2] студ. гр. РТ-919сп НУ «Запорізька політехніка»

ЗБІЛЬШЕННЯ ШВИДКОСТІ ПЕРЕДАЧІ ДАНИХ ПО 3G, 4G, 5G КАНАЛАХ МОБІЛЬНОГО ІНТЕРНЕТУ

В процесі збільшення швидкості передачі даних по каналах мобільного інтернету ми стикаємось із двома сер'йозними проблемами: недостатньо широка для забезпечення широкосмугового доступу робоча смуга частот та низький енергопотенціал системи передачі.

Для вирішення проблем використовуємо антенну решітку в якості антени з великим коефіцієнтом підсилення. В якості сукупності дискретних елементів антенної решітки пропонуються фрактальні антени.

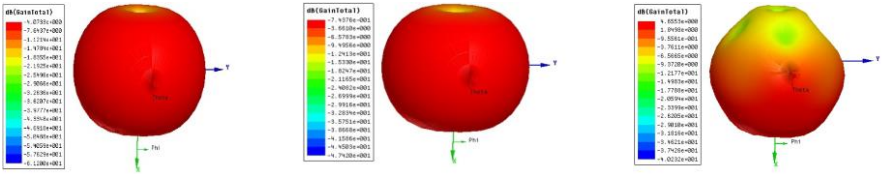
Фрактальна антена - це антена, активна частина якої має вигляд самоподібної кривої або будь-якої іншої фігури, що складається з подібних сегментів. Хоча ефективна електрична довжина є великою антени з фрактальних елементів самі по собі є фізично меншими в порівнянні з іншими типами через наявність реактивного навантаження.



а) б) в) г)

Рисунок 1 – Елемент решітки на основі фрактальної структури у вигляді модифікованої серветки (а) та килима Серпінського (б), губки Менгера (в), хреста Міньковського (г)

Перевагою фрактальних антен є їх багатодіапазонність і широкосмуговість при порівняно менших розмірах.



а) б) в)

Рисунок 2 – Просторові діаграми спрямованості елементів антенної решітки для частот 1,1 ГГц (а), 2,2 ГГц (б), 5,4 ГГц (в)

В якості квазіфрактальних структур можуть використовуватися серветки і килими Серпінського, криві Коха, хрести Міньковського, криві Гільберта, Пеано і ін., можна використовувати також 3D фрактали типу губки Менгера, які виготовляються за друкованою технологією (рис.1, а, б, г) або роздруковуються на 3D принтері (рис.1,в).

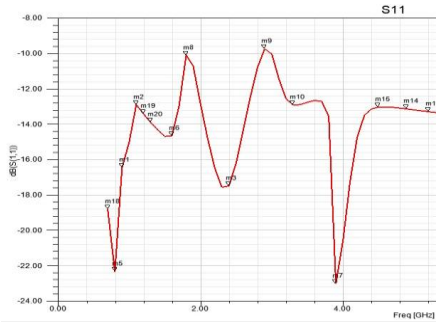


Рисунок 3 – Частотна залежність коефіцієнта відбиття елемента антенної решітки

В ході дослідження було побудовано та проаналізовано 3D модель фрактальної антени у вигляді модифікованої серветки Серпінського із застосуванням метаматеріалу ENG типу на зворотньому боці випромінювального елементу решітки (рис.1, а) в середовищі HFSS 17.2. Результати у вигляді просторової діаграми спрямованості показано на рис.2.

З рисунку 2 видно, що ширина головної пелюстки діаграми спрямованості є практично частотнонезалежною в широкому діапазоні частот (1,1…5,4 ГГц).

Очевидно (рис.3), що на частотах 0,9, 2,2 та 3,9 ГГц спостерігається досить якісне узгодження елементів решітки з лінією їх живлення, яке характеризується невеликими коефіцієнтами відбиття (-22,2 дБ, -17,8 і -23 дБ, відповідно). Застосування інших типів метаматеріалів паралельно з параметричною оптимізацією їх геометрії дозволить досягнути більш якісних показників узгодження.

Подальше дослідження вимагає врахування взаємодії елементів випромінювання між собою та вирішення проблеми спотворення діаграм спрямованості і розлаштування окремих елементів за рахунок цієї взаємодії.

УДК 631.674.6
Бугрова Т.І.[1], Числов Д.О.[2]
[1] доц. НУ «Запорізька політехніка»
[2] студ. гр. РТ-918 НУ «Запорізька політехніка»

АВТОМАТИЧНИЙ ПОЛИВ З КЕРУВАННЯМ ЧЕРЕЗ ІНТЕРНЕТ

В даний час системи автоматики все більше мігрують з промисловості в побутове середовище. Проникнення IoT в наше життя стало знамення теперішнього часу. Зараз навряд чи можна когось здивувати, розповівши про систему автоматичного поливу, побачену на сусідській ділянці, - такі системи з'явилися на ринку вже не один рік тому. Однак, дослідники продовжують вдосконалювати наявні розробки в бік їх здешевлення при масовому виробництві, збільшення їх надійності та розширення їх функціоналу при мінімальному втручанні користувача в сам процес керування, тому що навряд якому пересічному користувачеві сподобається велике занурення у процес регулювання поливу рослин на своїй присадибній або дачній ділянці.

У розглянутому нижче прикладі для підключення до інтернету використовується GPRS модем, що дозволяє «автолійці» виходити в мережу точно так же, як це робить звичайний мобільний телефон. При цьому обсяг переданих даних досить малий - тому система буде працездатна навіть в місцях з дуже слабким сигналом. На рис.1 наведено структурну схему комплексного рішення для дистанційного керування і моніторингу системи автополиву.

Контролер системи управління збирає дані з датчиків системи і за допомогою GPRS-модему передає їх на сервер. У відповідь він отримує від сервера команди для управління виконавчими пристроями системи

(поливальними клапанами, насосом і клапаном блокування доливання води в резервуар).

Користувач має доступ на сервер через веб-додаток з ПК або планшету чи смартфону. Центром системи є контролер ARDUINO MEGA (рис. 2).

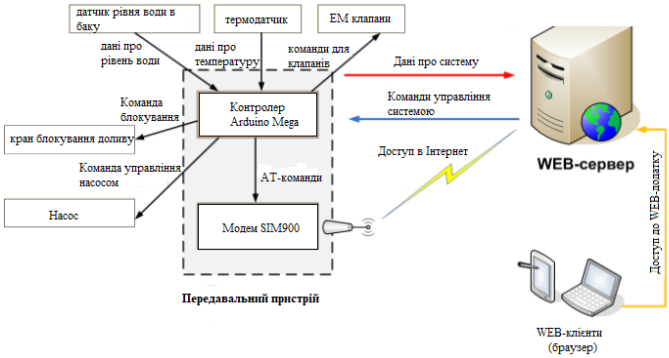


Рисунок 1 – Структурна схема системи управління

Рисунок 2 – Контролер ARDUINO MEGA.

Контролер управляє модемом SIM 900 (рис. 3). за допомогою АТ-команд, що передаються через COM-порт.

Рисунок 3 – Модем SIM 900

Таким чином здійснюється обмін даними з сервером.

Виникають випадки, коли модем може потрапити в «складну ситуацію». Іноді для того, щоб відновити його нормальну роботу, потрібно здійснити апаратне перезавантаження.

Для цього в систему додано модуль перезавантаження модему, який являє собою електромагнітне реле, через котре скомутоване живлення модему.

Сигнали від датчиків рівня води в резервуарі приймає модуль введення дискретних сигналів. Датчики мають вихід типу «сухий контакт».

Для того, щоб завести дискретні сигнали від датчиків в контролер, живимо їх напругою 24 В від блоку живлення. Модуль вводу даних представвляє собою дискретні входи з опторозв'язкою, що перетворює вхідний рівень напруги із 24 В у рівень в 5 В, який вже є зрозумілим для контролера.

Для вимірювання температури на вулиці до контролера підключений датчик DS18B20. Контролер проводить з ним обмін даними по інтерфейсу ONEWIRE.

Таким чином, представлена система керування поливом через Інтернет є досить дешевим і простим способом полити улюблені рослини. При цьому фізична присутність користувача вдома або на дачі не є обов'язковою.

УДК 621.391
Мороз Г. В.[1], Бурцева О. В.[2]
[1] старш. викл. НУ «Запорізька політехніка»
[2] студ. гр. РТ-910м НУ «Запорізька політехніка»

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ FSO ДЛЯ ПОБУДОВИ МЕРЕЖІ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

Сучасний світ інформаційних технологій стрімко розвивається. З кожним роком збільшуються обсяги передаваної інформації та зростають вимоги до швидкості і якості передачі даних. Це в свою чергу ставить питання про впровадження та розвиток новітніх технологій.

Однією з таких технологій є оптика вільного простору. FSO (free-space optics) - вид оптичного магістрального зв'язку, що використовує електромагнітні хвилі оптичного діапазону, які передаються через атмосферу. Перевагами технології є передача даних на відстань до 30 км зі швидкістю до 2,5 Гбіт/с[1], несприйнятливість до електромагнітних завад, низький коефіцієнт бітової помилки (BER), відсутність бічних пелюсток, низькі витрати у порівнянні з оптоволоконними мережами, безліцензійна робота на великі відстані.

Бездротова оптика розглядається в якості рішення на ділянках останньої милі в умовах міської забудови (для зв'язку між багатоповерховими будинками, бізнес-центрами та вузловими точками мережі); для організації зв'язку від вузлів зв'язку оператора до базових станцій мереж стільникового зв'язку при великих обсягах переданого цифрового трафіку (4G, LTE); для зв'язку об'єктів, коли прокладка кабелю неможлива (промзони, гірська місцевість, залізниця) або вартість цієї прокладки велика; в якості тимчасового каналу зв'язку, а також у випадках, коли необхідно терміново організувати канал зв'язку (гарячий резерв); коли потрібно створити закритий канал зв'язку, що нечутливий до радіозавад і не створює їх (наприклад, у аеропортах, поблизу радіолокаторів, ліній електропередач); за необхідності зменшення затримок в порівнянні з кабельними лініями. Однак, існують певні недоліки, які уповільнюють процес популяризації технології FSO. На роботу системи негативно впливають опади, атмосферні явища та завади від фонових джерел світла.

FSO має одну основну умову: регіони повинні бути в межах прямої видимості базової станції. Сучасні смартфони не обладнані спеціальним оптичним трансивером. Тому в якості рішення запропоновано переданий оптичний сигнал перетворювати в електричний, та навпаки, за допомогою приймальних та передавальних базових станцій. Таким чином, дані на великі відстані будуть передаватися за допомогою оптичного сигналу, а від базової станції до абонента – за допомогою радіосигналу. Технологію можна комбінувати з традиційною інфраструктурою мобільного зв'язку, так у жителів віддалених населених пунктів до стільникового додасться ще й інтернет-зв'язок [2]. Основною проблемою для системи FSO є загасання сигналу, а його причиною – геометричні втрати та затухання в атмосфері. Геометричні втрати на трасі для лінії FSO залежать від ширини променя оптичного передавача θ, довжини його шляху L і площі апертури приймача A_r. Причиною затухань в атмосфері є опади та атмосферні явища.

Загальне загасання визначається наступним виразом:

$$\frac{P_r}{P_t} = \frac{d_2^2}{[d_1 + (L\theta)]} * \exp(-\beta L),$$

де P_t – потужність, що передається (мВт); P_r – потужність, що приймається (мВт); θ – розбіжність променя (мрад); β – загальний коефіцієнт розсіяння ($км^{-1}$).

Авторами роботи запропоновано новий метод передачі даних на основі технології FSO, що дозволить підвищити швидкість і якість зв'язк.

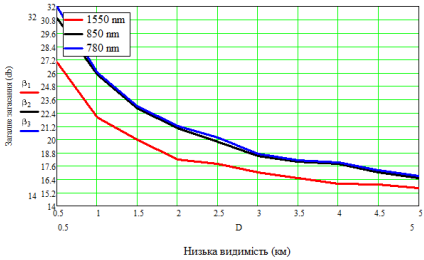


Рисунок 1 – Загальне загасання в умовах низької видимості

Запропонований метод задовільно працює в умовах опадів і атмосферних явищ, що доведено за допомогою моделювання. У майбутньому для покращення роботи системи необхідно вивчити питання, що допоможуть збільшити завадостійкість.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Rafael C. Gonzalez, and Richard E. Woods. Digital Image Processing. Prentice Hall, 3d Ed, 2009.

2. Free space optics system design. LightPoint-White Paper Series, 2009.

УДК 621.791.5

Костенко В.О.[1] , Булавчик В.П.[2]
[1] доц. НУ «Запорізька політехніка»
[2] студ. гр. РТ-917 НУ «Запорізька політехніка»

ДИСТАНЦІЙНЕ КЕРУВАННЯ ІНФОРМАЦІЙНОЮ ПАНЕЛЛЮ

В сучасному світі ми зустрічаємо рекламу на кожному кроці. З розвитком технологій та появою на ринку світлодіодів ми можемо побачити, як швидко вони здобувають авторитет в сфері реклами. В нашому випадку хочу розглянути саме світлодіодну панель, побудовану на принципі світлодіодної матриці. Такі панелі не завжди встановлюються в легкодоступних місцях і виникає досить гостре питання введення інформації. Було прийнято рішення побудувати портативний пульт дистанційного керування через радіоканал, як показано на рис. 1.

За даними статистики лідером з постачання мікроконтролерів на територію України є корпорація "Atmel", виходячи з цього будемо будувати наш пульт на базі мікроконтролеру «Atmega32». Оскільки він відповідає всім вимогам для забезпечення надійної роботи пристрою, має достатній об’єм Flash пам'яті програм, необхідну кількість ліній введення – виведення, необ-

хідні стандартні інтерфейси. Для відображення інформаційного тексту застосуємо рідкокристалічний індикатор з вбудованим драйвером «HD44780».

Рисунок 1.Дистанційне керування інформаційною панеллю

Для зменшення ліній зв'язку та економії ліній введення-виведення мікроконтролера використовується режим чотирьох бітного управління. Для роботи у вечірній і нічний час з пультом управління в індикаторі повинно бути передбачене підсвічування. У рідкокристалічних індикаторах застосовуються два види підсвічування: світлодіодна і люмінесцентна, враховуючи всі недоліки люмінесцентного підсвічування (необхідна напруга 100 вольт з частотою 400 Гц) вибір був зроблений в сторону світлодіодного підсвічування. Для організації її управління в схему введений польовий транзистор, який працює в ключовому режимі і керується мікроконтролером

Клавіатура є купленою та являє собою матрицю 3 × 4 з мембранних кнопок, підключається безпосередньо до мікроконтролера по семи лініях: три лінії стовпців і чотири лінії рядків. Ідентифікація натискання кнопок клавіатури здійснюється програмно в межах програмної оболонки.

Оскільки пульт управління повинен мати можливість працювати без наявності джерела живлення в ньому вбудована акумуляторна батарея. В зв'язку з цим необхідно встановити вхідний стабілізатор напруги, який забезпечить подачу безпечної для заряду літій - іонової акумуляторної батареї напруги. Акумуляторна батарея для нормальної і тривалої роботи пульта управління повинна мати ємність мінімум 800 мА / год. і забезпечувати вихідну напругу мінімум 6 Вольт.

Для зв'язку пульта управління зі світлодіодною панеллю відображення графічної інформації застосуємо модуль радіоканалу «XB24 – AWI – 001». Для зручності роботи і зменшення витрат на розробку програмного забезпечення застосовуємо модуль з вбудованим протоколом передачі. Радіомодуль з'єднується безпосередньо з мікроконтролером по універсальному інтерфейсу прийому - передачі даних UART і забезпечує зв'язок зі швидкістю 9600 біт / сек.

УДК 621.791.5
Костенко В.О. [1], Жуковська М.В.[2]
[1] доц. НУ «Запорізька політехніка»
[2] студ .гр.РТ-917 НУ «Запорізька політехніка»

ОРГАНІЗАЦІЯ КОНТРОЛЮ ОБМІНУ ІНФОРМАЦІЄЮ МІЖ ДВОМА ОФІСАМИ

Одним із пріоритетів при побудуванні мережі, слугує захищеність файлів, що передаються і приймаються. Для цих цілей під час організації мережі дуже добре підходить, з моєї точки зору, використанні VPN- доступу. Розглянемо більше детальніше його побудову та використання. VPN ((англ. Virtual Private Network - віртуальна приватна мережа) – ця технологія забезпечує зашифроване з'єднання між двома мережами або окремим користувачем та мережею, за її допомоги всі дані користувача при підключенні до Інтернету зашифровуються. Дана технологія дуже популярна, адже перш за все вона економічно вигідна. Розглянемо, наприклад, два офіси в різних точках міста. Для того, щоб об'єднати всі дані, що передаються між ними, ми можемо взяти та придбати персональну лінію, яка буде сполучати дані офіси, Але якщо взяти до уваги випадок, коли офіси знаходяться в різних містах, чи коли більшість співробітників працюють з дому у зв'язку з карантином, то дана технологія буде занадто дорогою і невигідною. Тому для збереження часу і грошей простіше організувати VPN- доступ для всіх співробітників, що працюють в офісі та за його межами наступним чином (рис.1). На рис. 1 зображено підключення до мережі двома способами: клієнт - мережа - віддалений доступ окремо взятих співробітників до корпоративної мережі організації через модем або загальнодоступну мережу. (Мережа – мережа- це об'єднання двох і більше офісів в єдину захищену віртуальну мережу за допомогою інтернет [1] озглянемо приклад підключення за допомогою OpenVPN (рис.2).

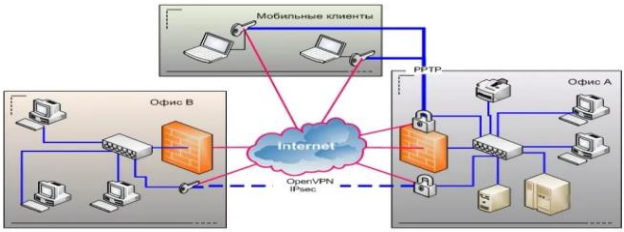


Рисунок 1– Приклад організації VPN- доступу для двох офісів з можливістю підключення співробітників, що працюють вдома.

Ця додаткова програма, яка встановлюється на робоче місце користувача (ноутбук/ комп'ютер) і забезпечує шифрування каналів типу « точка- точка» або « сервер- клієнт», була створена Джеймсон Йонаном у 2002 році. Вона підходить для багатьох ОС, таких як : Solaris, Open BSD, Free BSD, Net BSD, GNU / Linux, Apple Mac OS X, QNX, Microsoft Windows, Android, iOS [2]. Для шифрування і аутентифікації використовують бібліотеку OpenSSL, а також для передачі даних можуть використовувати UDP чи TCP. Зазвичай використовують TCP, бо він вважається стабільнішим тому, що пропонує функцію виправлення помилок (після відправлення мережевого пакета TCP очікує підтвердження перед його повторною відправкою чи відправленням нового пакета). UDP виправляє помилки, що робить його менш стабільним, але набагато швидшим. В даній програмі перш за все використовують UDP, спочатку йде з'єднання, але, якщо його встановити неможливо, тоді сервер переналаштовується на TCP.[3]. Без VPN-доступу співробітники не мають можливості приступити до роботи. Після встановлення програми користувач вводить свій логін і пароль, і цим самим забезпечує доступ до VPN. Переваги даного методу в його анонімності в мережі, шифруванні даних, можливості співробітникам працювати віддалено, маючи доступ до корпоративної інформації. На які умови варто звернути увагу при виборі VPN : для шифрування інформації варто вибирати рівень, який максимально захистить ваші приватні дані від сторонніх, дуже чудово може підійти – 256- бітове шифрування. Екстрене відімкнення від мережі: за допомогою цієї функції відбувається переривання мережі VPN , щоб запобігти витоку даних. (Захист від витоків DNS і IPv6).

Для тих, хто збирається працювати не тільки вдома, краще за все використовувати VPN - сервіс з серверами, що розташовані в усіх куточках планети. Це дає можливість відкрити доступ до різного виду контенту з будь – яких країн світу.

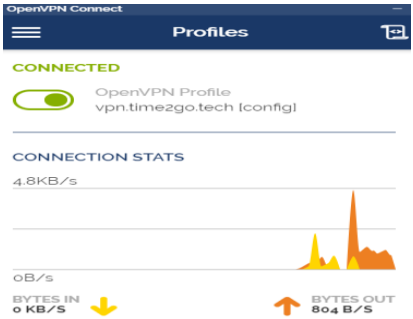


Рисунок 2– Підключення додатку VPN.

Якщо виникає потреба в VPN - захисту для декількох пристроїв, то варто звернути увагу на функцію «Одночасної підтримки відразу декількох підключень»

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. https://justrust.ru/uk/vpn-cherez-set-obshchego-polzovaniya-chto-takoe-vpn-ili-kak-zashchitit-set/
2. https://ru.wikipedia.org/wiki/OpenVPN
3. https://www.cactusvpn.com/ru/beginners-guide-to-vpn/what-is-openvpn/#definition

УДК 621.372.542.29

Костенко В.О. [1], Калюжний А.Г. [2]
[1] доц. НУ«Запорізька політехніка»
[2] студ .гр.РТ-210м НУ «Запорізька політехніка»

ВИМІРЮВАННЯ ВОЛОГОСТІ ПРИ ПІДВИЩЕНІЙ ТЕМПЕРАТУРІ

Коректне вимірювання вологи в умовах підвищених температур є майже неможливою задачею для переважної більшості гігрометрів. Саме тому була розроблена схема вимірювача вологи при підвищених температурах (рис.1). Датчик вологості - ємнісний, диференційний. Його половини Cx1 і Cx2 включені відповідно в контури L4C9C14 та L5C13C15. Контури через котушки L2 і L3 пов'язані з контуром генератора, зібраного на транзисторі VT1. Частоту роботи генератора задає кварцовий резонатор ZQ1. Перший контур налаштований на частоту вище частоти генератора, другий - нижче. Отже, високочастотна напруга на першому контурі зростає, а на другому падає. При збільшенні вологості в повітрі збільшується ємність конденсатора, відповідно і всього контуру, резонансна частота контуру 1 (L4C9C14Cx1) наближається до частоти генератора. Контур 2 (L5C13C15Cx2) навпаки уходить від частоти генератора та залежить від вологості. Тому зміщення резонансної частоти пропорційне вологості. Вимірявши різницю частот визначають вологість. Напруга знімається з контурів 1 та 2, випрямляється відповідно випрямлячами на діодах V2, V4 і V3, V5, зібраними за схемою подвоєння напруги. При зменшенні вологості опір контуру зменшиться, а струм відповідно збільшиться. Сумарна вихідна напруга з конденсаторів C6 і C7 через резистори R6, R15 подається на міліамперметр PA1. Температурний дрейф компенсується конденсаторами C9 і C13, що мають негативний ТКЄ (температурний коефіцієнт ємності). Ці конденсатори розміщені у датчику. У положеннях «Нуль» і «Чутливість»

перемикача S2 контролюють відхилення стрілки приладу на початкову і кінцеву позначку шкали перед вимірюванням вологості. Живлення пристрою від батареї 1604 або від іншого джерела простійного струму на 9 вольт.

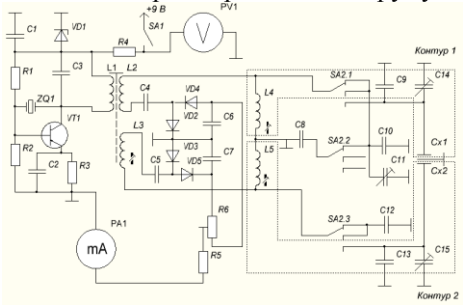


Рисунок 1– Схема вимірювача вологи

УДК 621.372.542.29
Селянінов В.В.[1], Логачова Л.М.[2]
[1] студ .гр. РТ-220м НУ «Запорізька політехніка»
[2] старший викладач НУ «Запорізька політехніка»

ЛАЗЕРНИЙ ЗВ’ЯЗОК

У зв'язку із стрімким зростанням обсягів даних, що передаються у радіоефірі, задіюються усе більш і більш високочастотні діапазони. Розв’язанням проблеми все більшого дефіциту радіоефіру може стати використання лазерного зв'язку. Використання лазерного випромінювання з несучою частотою до 1015 Гц могло б дуже сильно підвищити інформаційну ємність каналу зв'язку. Така ємність у багато разів перекриває практичні потреби.

Але є багато обмежуючих чинників, що грають важливу роль за практичного здійснення лазерного зв'язку. На практиці виникають серйозні труднощі технічного характеру. Вони пов'язані з відсутністю на даний час модуляторів, що мають досить широку смугу частот модуляції, а також швидкодіючих (малоінерційних) фотоприймачів. Проте, зовсім очевидна перспективність освоєння оптичного каналу зв'язку. Це б допомогло розв’язати, нарешті, проблему "тісноти" в ефірі, що дуже загострилася у наш час. Мовні станції, що використовують лазерний промінь, могли б працювати, анітрошки не заважаючи один одному, навіть якщо їхнє число збільшиться в сотні і тисячі разів.

Носієм інформації в лазерній системі є промодульований лазерний промінь. Приймач і передавач розташовані на деякій відстані один від

одного. Оскільки лазерний промінь поширюється в атмосфері, то в процесі передавання відбувається зменшення щільності енергії сигналу. Розсіювання енергії лазерного променя відбувається внаслідок відмінності коефіцієнта заломлення атмосфери від одиниці. На якість передавання впливають мікроскопічні часточки пилу, присутність у повітрі пару чи крапельок рідини, що викликають дифракцію чи інтерференцію сигналу. Чим менше таких перешкод, тим, зрозуміло, вища і якість зв'язку. Коливання температури чи випадання опадів (дощ, сніг) призводять до зміни щільності атмосфери, а отже, до розсіювання хвилі. Не виключена можливість і безпосередньої інтерференції сонячних з лазерними променями прямо в приймально-передавачі.

За потрапляння будь-яких великих предметів в область проходження променя (птахів чи листя) передача переривається на деякий проміжок часу.

Більшість лазерних систем працюють у дощ зі швидкістю випадання опадів до 8 см/год. й у снігопад - до 5 см/год., і практично в умовах суцільного туману.

Особливо варто згадати про чутливість системи до вібрації і руху. Для зниження вібрації систему розміщують на масивну опору (зазвичай сталеву чи бетонну, але ні в якому разі не на дерев'яну).

Як бачимо, використання лазерного зв'язку можливе навіть за наявності яких-небудь тимчасових перешкод на шляху променя, хоча виконання вимоги перебування приймально-передавачів в області прямої видимості є обов'язковим. Усі лазерні приймально-передавачі забезпечують передачу мережного трафіку зі статистичною вірогідністю більш ніж 99,9% у всьому припустимому діапазоні їхніх робочих швидкостей і відстаней.

Говорячи про перспективність лазерного зв'язку, відзначимо ще одну перевагу лазерного променя - його високу спрямованість. Звичайні радіостанції випромінюють у межах широкого тілесного кута. Застосовуючи спеціальні антени, можна домогтися спрямованості випромінювання. Однак ступінь спрямованості радіовипромінювання залишається істотно більш низькою в порівнянні зі спрямованістю лазерного променя. Завдяки високій спрямованості лазерного променя, можна здійснювати кілька каналів зв'язку на одній несучий. Крім того, зменшується небезпека небажаного перехоплення переданої інформації.

Підбиваючи підсумки, можна з упевненістю заявити, що є найширші перспективи застосування лазерів зв'язку в системах зв'язку і локальних мереж, для організації зв'язку між двома будинками. В даний час лазерна технологія розвивається в напрямку підвищення швидкості обміну і дальності зв'язку.

Так само варто відзначити, що лазерний зв'язок забезпечує високий рівень захисту інформації від несанкціонованого зчитування в той час, як

передача по радіо може бути перехоплена і записана навіть на великій відстані від передавача. Можна використовувати лазерну систему для організації тимчасового зв'язку без прокладки кабелю. Той самий тип з'єднання підходить і для застосування в системі дублювання зв'язку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Звелто О. Принципы лазеров [пер. с англ. Д.Н. Козлова, С.Б. Созинова и К.Г. Адамовича под науч. Ред Т.А. Шмаонова]. 4-е изд. СПб., М., Краснодар: Изд-во «Лань», 2008. 720 с.

2. Ю.А. Зингеренко. Оптические цифровые телекоммуникационные системы и сети синхронной цифровой иерархии. - Учебное пособие – СПб:НИУ ИТМО, 2013. – 393 с.

УДК 621.791.5

Калюжний А. Г.[1], Логачова Л. М.[2]
[1] студ .гр.РТ-210м НУ «Запорізька політехніка»
[2] старший викладач НУ «Запорізька політехніка»

ВИКОРИСТАННЯ ЛАЗЕРІВ В КРИМІНАЛІСТИЦІ

В сучасному світі лазери відіграють велике значення та застосовуються в багатьох сферах діяльності людини. Одне з таких місць – криміналістика, де в даний час широко застосовуються техніко – криміналістичні засобі і методи у основі яких лежать лазерні технології. Раніше, до використання лазерів, виконувати деякі слідчі дії було не можливо, або важко через те, що результат був потрібен в короткі строки, а на дослідження речових доказів чи загалом місця злочину – потрібно багато часу.

Застосування лазерної техніки у сучасній криміналістиці дозволяє розширити можливості ії подальшого використання у судової криміналістиці, а також у судової балістиці при вирішенні задач, пов'язаних з визначенням напрямку та відстані прямого кульового пострілу у умовах неочевидності методом візування з використанням лазерів і лазерних далекомірів (див. рис. 1). При цьому за допомогою лазерного променю можна визначити кут входу кулі в перешкоду і здійснити візування траєкторії її польоту навіть після рикошету від твердої поверхні, що дозволяє дізнатися звідки стріляли.

Нанесення прихованої лазерного маркування на внутрішню поверхню каналу ствола з полігональними нарізами з метою ідентифікації стрілецької зброї по слідах на відстріляних з нього кулях.

Прямий візуальний контроль неможливий або утруднений і викликає

Рисунок 1 - Лазерне візування

необхідність застосування спеціальних зчитувальних засобів.

Виявлення слідів дії додаткових факторів пострілу, таких як кіптява, порошинки і металеві частинки. Вони виглядають темно-сірими на світлому тлі навколишніх тканин під час опромінення поверхні об'єкта-мішені в зоні вогнепального пошкодження ІЧ–лазером і аналізу зображення в відбитих ІЧ–променях.

Опромінення об'єкта УФ–лазером здатне викликати його люмінесценцію, за рахунок якої можна виявляти мінеральні масла, що входять до складу рушничного мастила, зерна бездимного пороху або кіптява пострілу. За рахунок лазерного методу збудження люмінесценції виявляють відбитки пальців, мікро сліди крові, а також написи, печатки, штампи і ін., знищених хімічним травленням.

За допомогою методу спектроскопії комбінаційного розсіювання світла, при якому зразок опромінюється монохроматичним світлом можна ідентифікувати хімічний склад, або вивчати внутрішньо-молекулярні взаємодії. Аналіз проводиться за кілька секунд, а виявити можна навіть склад пото–жирової речовини, який у всіх індивідуальний.

Методи лазерної спектроскопії використовуються для дистанційного виявлення та ідентифікації слідів залишків вибухових речовин на поверхнях об'єктів-носіїв з метою вирішення оперативно–слідчих, пошуково–доглядових завдань, пов'язаних, наприклад, з прихованим пошуком і виявленням фізичних осіб (транспортних засобів), що переносять (перевозять) вибухові речовини, або виявленням терористів-смертників.

З використанням лідарних комплексів можна здійснювати дистанційне зондування атмосфери з метою визначення реальної хімічної обстановки на місці події в режимі реального часу, що дозволяють виявити витік і основні

компоненти вибухонебезпечних речовин, в тому числі летючих вуглеводнів, що знаходяться в повітряному середовищі.

Як бачимо, лазерам знайшли безліч призначень в криміналістиці, а методи їх застосування розширюються та покращуються.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Федоренко В.А. Актуальные проблемы судебной баллистики. Учебное пособие. – М.: Изд-во «Юрлитинформ», 2011 год, 208 с.

2. https://cyberleninka.ru/article/n/vozmozhnosti-primeneniya-lazerov-v-kriminalistike

УДК 621.372.542.29

Комір М. О.[1] , Логачова Л. М.[2]

[1] студ .гр. РТ-220м НУ «Запорізька політехніка»

[2] старший викладач НУ «Запорізька політехніка»

ЛАЗЕРНА ГОЛОГРАФІЯ

Ідеї голографії, її принципи та методи стали формуватися ще до створення лазеру. Ідея голографічного методу отримання зображень була висунута польським фізиком М. Вольфке у 1920 році.

У 1962 році фізик Ю.Н. Денисюк запропонував об’ємні голограми на основі товстошарових емульсій і розробив метод запису цих голограм в зустрічних світлових пучках. Голографія - спосіб отримання об'ємних зображень предметів на фотопластинці (голограмі) за допомогою когерентного випромінювання лазера. Голограма фіксує не саме зображення предмета, а структуру відбитої від нього світлової хвилі (її амплітуду і фазу). Для отримання голограми необхідно, щоб на фотографічну пластинку одночасно потрапили два когерентних світлових пучка: предметний, відбитий від об'єкту, що знімається, і опорний - приходить безпосередньо від лазера. Світло обох пучків інтерферує, створюючи на пластинці чергування темних і світлих смуг - картину інтерференції.

Розглянемо голограму Денисюка (див. мал. 1). Вона дозволяє робити кольорові тривимірні зображення. Побудова голограми відбувається за допомогою монохроматичного світла. В цьому процесі беруть участь дві хвилі. Перша - це хвиля джерела світла, якій надають плоску форму за допомогою спеціальних оптичних приладів. Вона називається опорна. Друга хвиля - це хвиля предметна, вона відбивається від об’єкта, з якого роблять голограму. Її хвильовий фронт повторює форму предмета. Опорна та предметна хвиля поширюються на зустріч одна одній та складаються.

Внаслідок цього виникає інтерференційна картина стоячої хвилі. Вона реєструється товстошаровою фотопластиною.

Для того, щоб можна було побачити отримане зображення його треба відновити. Це робиться за допомогою променя немонохроматичного світла, що розбігається. Тобто пучок світла, який ми посилаємо на дифракційну решітку, дифрагує на неоднорідних почорніннях голограми.

В результаті, опорна хвиля трансформується в предметну.

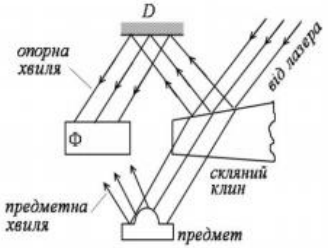


Рисунок 1 - Схема голографії Денисюка

Далі це поле трансформується в єдине тривимірне зображення. Ця голограма - це тривимірна дифракційна структура. Тому можливо використовувати для відновлення пучок білого світла, що розбігається.

На одну голограму можна записати зображення предмета для трьох довжин хвиль: червоної, зеленої, синьої. За відновлення голограми формуватимуться одразу три голографічних зображення, які в подальшому сформують одне кольорове зображення. Голографія знайшла дуже широке застосування у науці, техніці, культурі, в інших сферах життя і діяльності людини. Голографія застосовується для реєстрації і відтворення унікальних речей – історичних реліквій, творів мистецтва, голограмних портретів, голографічного кіно, голографічного телебачення.

В науці і техніці голографія застосовується для інтерферометрії. Особливість голографічної інтерферометрії полягає в тому, що хвильовий фронт, який досліджується, фіксується на голограмі. Допустимо, що зроблена голограма предмета. Після того, як з предметом відбулись деякі зміни (старіння, нагрівання, механічні дії тощо), воно ставиться на своє місце і порівнюється з голограмою. Якщо тіло (предмет) змінить свій стан, то хвильові фронти від предмета і його зображення, одержаного за допомогою голограми, будуть різними. Оскільки вони когерентні, то буде інтерференція, за характером якої можна зробити висновок про зміни в об'єкті.

Також, за допомоги голографії, можна робити носії пам’яті. Якщо об’єктом запису є оптичний транспарант, то записується не біт інформації, а ціле зображення. Одна і та сама ділянка реєстрованого матеріалу може вміщувати декілька накладених одна на одну голограм, які не впливають

одна на одну, якщо при записуванні кожен раз змінювати кут падіння опорного пучка. Зчитування проводиться за таких самих умов.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. http://www.dut.edu.ua/uploads/l_616_46603966.pdf
2. http://ena.lp.edu.ua/bitstream/ntb/26031/1/34-249-253.pdf

УДК 004.735

Самойлик С.С.[1], Шараєвська О.А.[2]
[1] доц. каф. РТТ НУ «Запорізька політехніка»
[2] студ. гр. РТ-918СП НУ «Запорізька політехніка»

ПИТАННЯ БЕЗПЕКИ ПЕРЕДАВАННЯ ДАНИХ В МЕРЕЖІ IOT LORAWAN

Використання інтернет речей (IoT) у повсякденному житті, надає звичайним користувачам абсолютно новий рівень комфорту. Але якщо елементи такої системи не будуть належним чином захищені від несанкціонованого втручання, то замість користі вони принесуть шкоду, надавши кіберзлочинцям лазівку для підриву інформаційної безпеки. Захист даних в будь-якій мережі IoT, незалежно від конкретного стандарту чи технології, повинен відповідати таким критеріям: End-to-end-конфіденційність даних користувача на рівні додатку; взаємна ідентифікація абонентського пристрою і мережі; перевірка цілісності даних при передавання на радіоінтерфейсу; конфіденційність сигнальної інформації (керуючих команд); безпечне зберігання ідентифікаторів абонентського пристрою і його повноважень; оперативне усунення знайдених вразливостей в ПО компонентів мережі та абонентських терміналів; можливість використання вітчизняних засобів криптографічного захисту інформації.

Для забезпечення захисту інформації, що передається та перевірки цілісності даних при передавання їх радіоінтерфейсу в мережі IoT LoRaWAN передбачена багаторівнева система безпеки (рис. 1).

1-й рівень. AES-шифрування на рівні додатку (end-to-end, тобто між абонентським терміналом і сервером додатків) за допомогою 128-бітного змінного сесійного ключа Application session key (AppSKey).

2-й рівень. AES-шифрування і перевірка цілісності повідомлень на мережевому рівні (між абонентським терміналом і сервером) за допомогою 128-64 бітного змінного сесійного ключа Network session key (NwkSKey).

3-й рівень. Стандартні методи аутентифікації і шифрування інтернет протоколу (IPsec, TLS і т. П.) При передавання даних по транспортній мережі

між вузлами мережі (базова станція, мережевий сервер, join-сервер, сервер додатків).

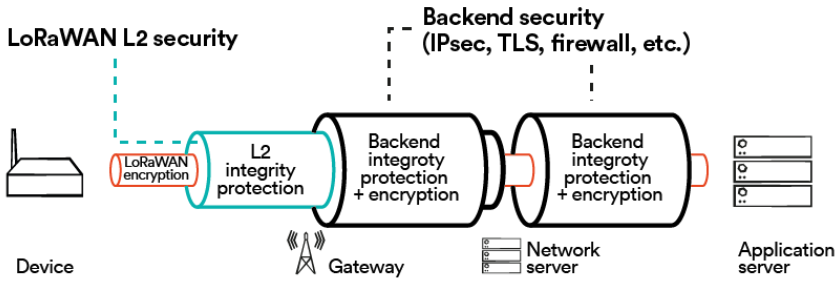


Рисунок 1 – Загальна схема безпеки даних в мережі LoRaWAN.

Таким чином LoRaWAN має всі фундаментальні складові, що необхідні та використовуються будь-якою сучасною технологією бездротового зв'язку. Власна безпека LoRaWAN, як це передбачено в специфікації, має супроводжуватися безпечної реалізацією і безпечним розгортанням цих пристроїв і / або мереж для підтримки вбудованих механізмів безпеки протоколу.

СЕКЦІЯ «МІКРО-ТА НАНОЕЛЕКТРОНІКА»

УДК 539.21
Куянцев Д.С.[1], Погосов В.В.[2]
[1] студ. РТ-317 НУ «Запорізька політехніка»
[2] д-р физ.-мат. наук, проф. НУ «Запорізька політехніка»

ВАРІАЦІЙНІ РОЗРАХУНКИ ПОВЕРХНЕВОЇ ЕНЕРГІЇ. ФУНКЦІЯ СМІТА

Сучасний стан нанотехніки вимагає активне втручання нанотехнологій. Роль поверхневих ефектів у процесах конденсації, випаровування та емісії заряджених частинок металу зростає зі зменшенням розмірів кластерів атомів. При цьому характеристики цих ефектів, такі, як коефіцієнт поверхневого натягу, робота виходу електронів та йонів, теплота випаровування самі починають залежати від розміру кластерів. Вимірювання поверхневої енергії завжди було складним. Тому особливим для наноелектроніки є розрахунок поверхневої енергії при моделюванні контактних явищ, а також острівцевих плівок на спеціальних підкладинках.

Однорідний твердий метал є складною фізичною системою корельованих електронів та йонів із сильною взаємодією між ними. Під час опису поверхні металу і властивостей металевих кластерів виникають значні проблеми, оскільки необхідно розглядати дуже неоднорідні системи. У найпростішому випадку йонна підсистема модулюється позитивним компенсувальним фоном (желе). У цьому разі розподіл іонів не залежить від просторового розподілу електронів і жорстко заданий. З наближенням низьких температур електронну підсистему метала або кластера можна також розглядати як неоднорідну вироджену електронну рідину на фоні східчастого желе.

Успішному розвитку теорії поверхневих властивостей металів сприяє самоузгоджена теорія рівноважного стану неоднорідного електронного газу – метод функціонала густини (див., наприклад, [1]). Метод функціонала густини ґрунтується на локальному наближенні для потенціалу обмінно-кореляційної взаємодії, і тому він дійсний для повільно змінної густини. В такому формулюванні – це найпростіша самоузгоджена модель, яка взагалі має зміст: вона нехтує йонною структурою за винятком дальнодійного притягання. Н. Ленг і В. Кон використовували модель желе як перший крок на шляху створення теорії металевої поверхні.

Поверхня металу, характеризується насамперед роботою виходу електронів, питомою поверхневою енергією та поверхневим стресом (або поверхневим натягом). Щоб їх визначити, треба знати розподіл електронної густини і самоузгодженого потенціалу поблизу поверхні. Питома поверхнева

енергія γ – це незворотна робота при нульовій температурі з поділу металу (наприклад, на дві частини) вздовж деякої площини. Ця енергія припадає на одиницю площі утворених поверхонь. Поверхневий натяг (або стрес) – це зворотна робота зі змінення поверхні (на одиницю).

Стандартна модель желе, запропонована ще Дж. Бардіним для однорідної електронної рідини, має істотні недоліки. Вона в цілому призводить до негативних значень як γ (для $r_s < 2a_0$), так і модуля стискання B (для $r_s > 6a_0$). У цьому сенсі її ще називають моделлю нестабільного желе. Дж.П. Педью і його співавтори запропонували модель стабільного желе, таку ж просту, як і попередня, але доповнили її введенням псевдопотенціальної поправки.

В даній роботі однопараметричну функцію вибирали у вигляді

$$n(x) = \bar{n}\begin{cases}\left(1-\frac{1}{2}\mathrm{e}^{bx}\right), & x \le 0\\ \frac{1}{2}\mathrm{e}^{-bx}, & x > 0\end{cases},$$

де параметр L характеризує ширину подвійного зарядженого (поверхневого) шару, $\bar{n}$ – концентрація електронів в глибині металу. Оптимальне значення параметру L знаходилось з вимоги мінімуму $\gamma(L)$.

Використаний варіант методу функціонала густини допускає незначну неоднорідність системи.

Розрахунки зроблено у двох моделях, а результати порівняно з експериментами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Погосов, В.В. Введение в физику зарядовых и размерных эффектов. Поверхность, кластеры, низкоразмерные системы [Текст] / В. В. Погосов. – М.: Физматлит, 2006. – 328 с.

УДК 535.343
Ківа К.Р.[1], Коротун А.В.[2]
[1] студ. РТ-310м НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

ПОВЕРХНЕВИЙ ПЛАЗМОННИЙ РЕЗОНАНС В ЕЛІПСОЇДАЛЬНИХ МЕТАЛЕВИХ НАНОЧАСТИНКАХ

В останні роки особливу увагу привертають способи формування металевих наночастинок та вивчення їх характеристик. Насамперед це зумовлене з перспективами їх використання в оптиці, хімії та біології. Зокрема, значний інтерес представляють високі оптичні нелінійності, викликані яскраво вираженим ефектом підсилення поля в околі наночастинок за рахунок плазмового резонансу.

Як відомо, у частинки сферичної форми такий резонанс один, а у сфероїдальної форми (еліпсоїд обертання) таких резонансів два. Це пов'язане з тим, що при відхиленні форми наночастинки від сферичної її поляризованість із скалярної величини перетворюється на тензорну. В результаті поверхневий плазмонний резонанс у такій частинці стає залежним як від орієнтації наночастинок відносно падаючого світла, так і від поляризації падаючого світла.

Тому задача про дослідження розмірної залежності частоти поверхневих плазмонів у металевих наночастинках у формі сплюсненого та витягнутого еліпсоїдів обертання є актуальною.

Вираз для частоти плазмових резонансів у сфероїдальних металевих наночастинках може бути записаний у вигляді

$$\omega_{\perp(\|)} = \sqrt{\mathcal{L}_{\perp(\|)}}\,\omega_p\,, \tag{1}$$

де ω_p – частота об'ємних плазмонів; $\mathcal{L}_{\perp(\|)}$ – коефіцієнти деполяризації еліпсоїда обертання, що визначаються як

$$\mathcal{L}_\perp = \frac{1}{2}\left(1-\mathcal{L}_\|\right), \quad \mathcal{L}_\| = \begin{cases} \dfrac{1-e_p^2}{e_p^3}\left(\ln\dfrac{1+e_p}{1+e_p} - 2e_p\right), & R_\perp < R_\|; \\ \dfrac{1+e_p^2}{e_p^3}\left(e_p - \operatorname{arcrg} e_p\right), & R_\perp > R_\|, \end{cases} \tag{2}$$

де $e_p \equiv \left|1 - R_\perp^2 / R_\|^2\right|$ – ексцентриситет; $R_{\perp(\|)}$ – поперечна (поздовжня) напівосі еліпсоїда.

Встановлено, що при деформації сферичної наночастинки у витягнутий або сплюснений еліпсоїд обертання, внаслідок анізотропії відбувається розщеплення поверхневого плазмонного резонансу. Це, в свою чергу, приводить до особливостей у поглинанні та розсіянні світла асиметричними металевими наночастинками.

СЕКЦІЯ «МЕТРОЛОГІЯ»

УДК 004.3
Василенко О.В.[1], Сніжной Г.В.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] д-р техн. наук, завідувач кафедри МіНЕ НУ «Запорізька політехніка»

РОЗРОБКА УЧБОВОГО СТЕНДУ НА БАЗІ ПРОГРАМОВАНОГО ІНТЕЛЕКТУАЛЬНОГО РЕЛЕ EASY E4 ДЛЯ ПІДГОТОВКИ СТУДЕНТІВ СПЕЦІАЛЬНОСТЕЙ 152 «МЕТРОЛОГІЯ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНА ТЕХНІКА» ТА 153 «МІКРО- ТА НАНОСИСТЕМНА ТЕХНІКА»

Програмовані інтелектуальні реле (ІР) є одним з різновидів програмованих логічних контролерів (ПЛК). Застосування інтелектуальних реле дозволяє значно спростити схеми керування електроустаткуванням, підвищити їх надійність. Для завантаження (прошивки) готових програм в пам'ять мікроконтролера використовуються інтерфейси типу RS-232, RS-485 або Ethernet, що дозволяє також здійснювати зв'язок з автоматизованими системами керування верхнього рівня. Деякі моделі програмованих інтелектуальних реле дозволяють нарощувати можливості комунікації за допомогою спеціальних модулів розширення.

Розроблений стенд призначений для дослідження принципів автоматизації технологічних процесів на базі інтелектуального реле easyE4 фірми Mueller/Eaton (рис.1). Стенд оформлений у вигляді шафи промислового виконання.

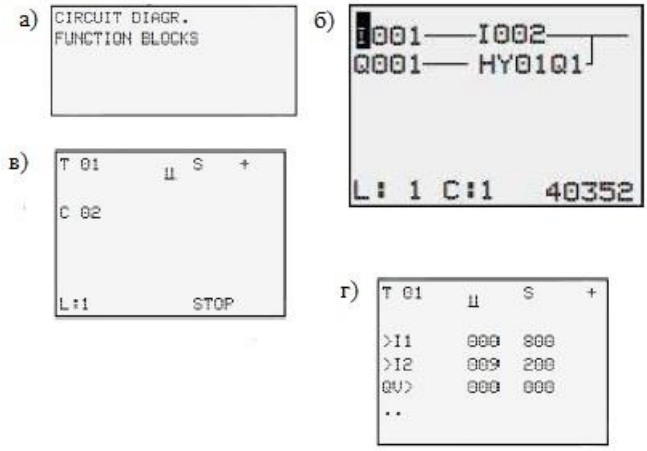
Рисунок 1 – Вид стенду на базі інтелектуального реле easyE4.

Всередині шафи розміщені автоматичні вимикачі, блок живлення та електронне реле керування EASY-E4-UC-12RC1 із MFD. На лицевій панелі

стенду розміщені органи керування та сигналізації: кнопки, перемикачі, потенціометр, LED лампи тощо.

Перед включенням пристрою необхідно перевірити джерела живлення, входи, виходи і будь-які пристрої розширення і з'єднання Ethernet, щоб переконатися в їх правильному підключенні. При відсутності програми, реле запускається в режимі STOP. Вся інформація на дисплеї буде відображатися англійською мовою, якщо в пристрої задані заводські настройки. Якщо в реле є виконувана програма, то пристрій запуститься в режимі RUN. Також слід переконатися в тому, що в реле керування використовується дійсна програма, а також у відсутності помилок периферійних пристроїв, які приведуть до режиму STOP.

Для того, щоб скористатися функцією програмування безпосередньо на пристрої , треба вибрати меню «PROGRAM». Це меню (рис. 2) буде доступно тільки в тому випадку, якщо реле easyE4 має стандартні налаштування та/або коли в реле збережена програма, створена на мові програмування EDP.



а) вибір вигляду програми; б) принципова схема;
в) функціональні блоки; г) приклад програми.
Рисунок 2 – Меню програмування стенду на базі реле easyE4.

Використання типових програм дає можливість легко навчитися основам роботи із системами на основі IP, швидко перевірити правильність написаної програми, а крім цього, відкриває можливість для зміни умов завдання в режимі реального часу. Вартість комплектуючих, монтажу та супроводу учбового стенду становить порядку 14 000 гривень.

УДК 004
Kolodka A.[1], Snizhnoi G.[2]
[1] Consultant “Easy Online Solutions“ LTD
[2] Doctor of Technical Science, head of chairs MNE NU “Zaporizhzhia Polytechnic”

METHODS FOR REPELLING DDOS ATTACKS AND NETWORK OPTIMIZATION UNDER HIGH LOADS

With the constantly growing volume of transmitted information in the world, the problem of its high-speed transmission is acute. Network devices have both software and hardware limitations for transmitting network traffic. Quite often, these limits can cause collisions and interfere with each other. In order to avoid such situations, it is required to clearly understand the network construction model, the type of transmitted data, the data transfer rate. Correct determination of the parameters of incoming and outgoing data streams allows you to optimize the software and hardware by changing the parameters of their operation by configuring the limits and buffering parameters.

Consider a data center with an edge router connected to the Internet at a bandwidth speed of 100 Gbps. To analyze data flows, we will use ElastiFlow software, which consists of a bundle of ElasticSearch, LogStash, and Kibana packets. This complex allows you to fully assess the load on any flow or on the total flow interactively or over a period of time. Also, these complex can be attached to the Grafana or other data collection tool to provide a wider list of alerting and informing options.

During this software package usage, the analysis showed suspicious data streams transmitted over UDP protocol for the NTP service and it exceeds more than 6Gbps of bandwidth speed usage. Although this protocol is used only for time synchronization on devices and the bandwidth speed as well as the amount of such data should be several times less. With the help of this software package, we make a selection by the addresses of devices that produce illegitimate data transfer and block the streams with firewall rules. Thus, we eliminate the problem caused by the DDOS attack.

However, for a legitimate data stream, some devices may be overloaded with the number of interrupts due to the fragmentation of data packets. This problem can cause a denial of access to the device and its complete blocking. So we've used the provided software package to analyze the packet fragmentation for different protocols and data sources. To resolve this issue, we've re-configured the device operating system kernels to enable bundling of multiple packages - pooling, before making a request to the kernel. This prevents CPU time over-usage for simple data translation requests.

Applying such an analysis and network optimization, it was possible to eliminate the illegitimate data flow of 6 Gbps, which is 6 % of whole data traffic, which can be seen on the incoming (fig. 1) and outgoing (fig. 2) bandwidth speed graphs at the time between 11:00 and 11:30. Also, such analysis reduced the load on devices by 50-70 %.

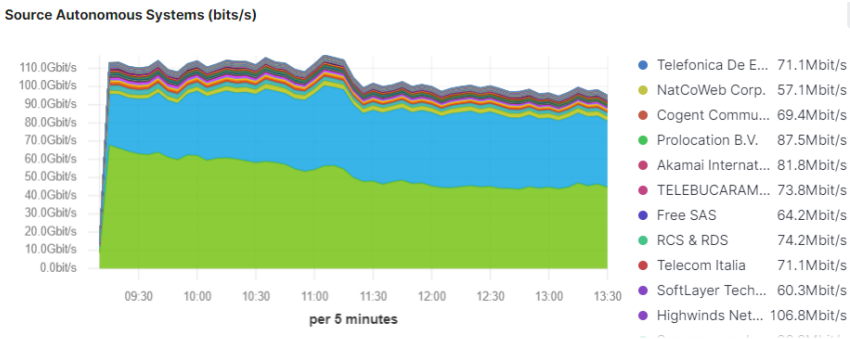


Figure 1 – Incoming data bandwidth utilization

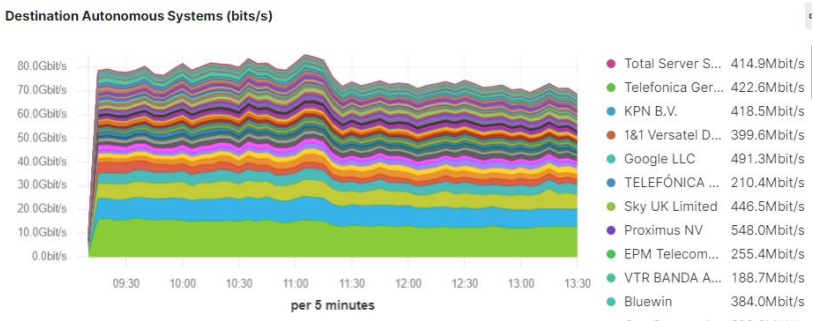


Figure 2 – Outgoing data bandwidth utilization

Such data flow analysis systems make it possible to quickly identify and eliminate network attacks and collisions. Data collection can be performed from multiple sources and aggregated into a single database, which allows to consolidate and visualize the data flow, as well as configure the system of notifications, warnings, and alerts about network events at all levels of the OSI model.

УДК 004.51
Гринчак Є.Г.[1], Василенко О.В.[2]
[1] студ. РТ-410 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ЕТАПИ ОПТИМАЛЬНОГО ПРОЕКТУВАННЯ САЙТУ

До сайтів можна використовувати критерії оптимальності та етапи проектування, як до будь-якого об'єкту матеріального світу. Критерії оптимальності традиційно розбиті на групи, які знаходяться у протиріччі одна до одної: якість та ціна; при цьому ціна не обов'язково має вартісний характер. Якість має в собі безліч підкритеріїв, головним з яких можна вважати ергономічність, для її максимізації необхідно дотримуватися правил оптимального проектування.

Визначимо процедуру оптимального проектування сайтів:

формування технічної пропозиції та технічного завдання;

визначення основних функцій (критеріїв якості, об'єму робіт);

розробка базового людино-машинного інтерфейсу (Human-Machine Interface, HMI) – (синтез системного рівню);

використання CASE-підходу для інтеграції модулів та інтерфейсів (структурний синтез);

визначення основних інструментів (параметризація);

розробка сайту згідно технічного завдання (ТЗ): робочий та технічний проект, декомпозиція та аналіз, композиція та аналіз, за необхідності оптимізації – повернення на рівні 5, або навіть 3;

розміщення сайту та прикінцеве тестування (натурний експеримент, «пуско-налагоджувальні» роботи), при необхідності оптимізації – повернення на рівні 5, 3, або навіть 1, в залежності від об'єму змін та вимого замовника;

підписання замовником прийому проекту, запуск проекту.

Розглянемо деякі етапи більш детально: 1. Після узгодження ТЗ, визначаються основні функції. Сучасний комерційний сайт є не просто набором пов'язаних гіперпосиланнями сторінок, а своєрідний інструмент для вирішення певного кола завдань, яке в залежності від призначення сайту може бути різним, тому дуже важливо ще до початку створення сайту визначити, які саме опції на сайті будуть потрібні, щоб досягти поставлених цілей з максимальною ефективністю.

2. В ході прийняття рішень необхідно виконувати все більше операцій і розглядати все більше даних, тому, якщо HMI розроблено на основі аналізу кращих варіантів його практичного застосування в конкретній галузі і з урахуванням певних базових принципів, він може поліпшити і спростити процедуру обробки інформації, щоб оператори швидше і точніше виконували

свої обов'язки в частині контролю та поточних завдань в технологічних і виробничих процесах.

3. Проблема зв'язку різномовних, різнорідних за кодом і середовищем програм загострилася у зв'язку зі швидкою зміною архітектури комп'ютерів, появою розподілених, клієнт-серверних середовищ тощо. Виявилася неоднорідність мов програмування (МП) в сенсі як уявлення в них типів даних, так і платформ комп'ютерів, на яких реалізовані відповідні системи програмування, а також в різних способах передачі параметрів між об'єктами в різних середовищах – маршаллінгом даних через різні види операторів віддаленого виклику. Єдиного підходу до вирішення проблеми інтерфейсу не існувало. Стандарт ISO/IEC 11404-1996 визначив підхід до вирішення питань інтерфейсу всіх видів МП за допомогою універсальної мови LI (Language Independent). Однак до теперішнього часу потужної інструментальної його підтримки не існує.

4. Є інструменти груп back-end та front-end. Front-end – це та частина, з якою користувач буде безпосередньо взаємодіяти, для неї доцільно використовувати HTML і CSS [1]. Back-end – це найважливіша частина, оскільки в ній виконується вся логічна частина сайту. Тут вибір мови проектування дуже широкий, але фаворитом є мова Python. Для збереження інформації доцільно використовувати бази даних, найбільш практичною і простою є PostgreSQL основна мова написання – SQL.

5. Для злагодженої роботи back-end і front-end рекомендовано використовувати API-інтерфейси, що в майбутньому дасть нам можливість розширювати можливості функціоналу [2].

6. Для безперервного доступу до ресурсу доцільно розміщувати його на сервісах хостингу або VPS, для цього слід використовувати інструменти Nginx або Apache, Gunicorn або UWSGI (Daphna – якщо сервер асинхронний). Кінцеве тестування проводиться для вчасного виявлення проблем, тут буде доцільно використовувати UNIT-тести, а також інші функції тестування конкретних вузлів і підсистем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Розуміння основ роботи API і REST API [Електронний ресурс] – Режим доступу: https://sebweo.com/rozuminnya-osnov-roboti-api-i-rest-api-korotkij-vstup/.

2. Яка різниця між FRONT-END та BACK-END [Електронний ресурс] – Режим доступу: https://lgs.lviv.ua/yaka-riznytsya-mizh-front-end-back-end.

УДК 004.51
Довгаль А.О.[1], Іваницький І.С.[1], Василенко О.В.[2]
[1] студ. РТ-318 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

РОЗРОБКА HMI СИСТЕМ АВТОМАТИЗАЦІЇ НА БАЗІ SCADA

Основні принципи, якими слід користуватися при розробці систем автоматизації:

рівень автоматизації конкретного технологічного процесу повинен бути економічно доцільним;

при виборі технічних засобів автоматизації слід надавати перевагу тим засобам, що виготовляються серійно і є засобами вітчизняного виробництва;

місце встановлення технічних засобів автоматизації повинно відповідати умовам їх експлуатації (вибухо- та пожежобезпеки, агресивності навколишнього середовища та ін.);

не переобтяжувати щити чи пульти операторського пункту надмірною кількістю приладів, краще використати засоби централізованого контролю, регулювання та керування – мікроконтролери чи керуючі мікропроцесорні комплекси, тобто використовувати багаторівневу автоматизацію, яка має 3-4 ієрархічні рівні;

для кращого моніторингу та візуалізації процесів в режимі реального часу використовувати спеціалізовані програми, наприклад, SCADA.

Людино-машинний інтерфейс (*Human-Machine Interface, HMI*) систем автоматизації технологічних процесів (АСТП), систем моніторингу, багатьох систем автоматичного регулювання (САР), наприклад, систем SMART HOUSE, клімат-контролю тощо, інформаційно-вимірювальних систем (ІВС) та систем автоматичного керування (САК, *Automatic Control System*, ACS), реалізуються за допомогою SCADA (*Supervisory Control and Data Acquisition*).

SCADA є потужним засобом автоматизації збору та візуалізації інформації, яка надходить з сенсорів вимірювальних систем (ВС), встановлених на об’єкті автоматизації. Системи SCADA використовуються для моніторингу та керування установками або обладнанням у таких галузях, як телекомунікація, керування водою та відходами, енергетика, переробка та транспортування нафти та газу, виробництво, де необхідно мінімізувати присутність людини в цехах (хімічна галузь, атомна енергетика тощо).

Трирівнева САР із SCADA, яку встановлено на персональному комп’ютері автоматизованого робочого місця (АРМ) оператора, наведено на рис.1. Як бачимо, інформація від сенсорів з об’єкту автоматизації передається через програмований логічний контролер (ПЛК) на АРМ.

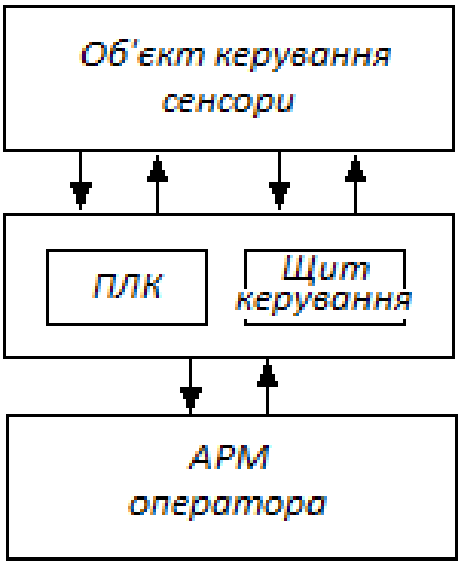


Рисунок 1 – Схема трирівневої автоматизованої системи.

Частина сигналів візуалізується одразу на щиті управління/керування, який встановлено, наприклад, в цеху на виробництві. АРМ може бути віддаленим від об’єкту керування, в залежності від фізичної реалізації та протоколів зв'язку, на відстань від сотень метрів, до кілометрів.

Реалізувати подібний проект можна як за допомогою «промислової» SCADA, наприклад Trace Mode [1], або на базі міні-SCADA для Android, наприклад KaScada [2].

За допомогою MasterOPC Modbus серверу [3] було організовано вивід на екран графіків зміни температури з вимірювальної системи на ArduinoUno, та реалізовано регулювання температури через пристрої силової електроніки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. SCADA/HMI software: TRACE MODE 6 IDE. [Електронний ресурс] – Режим доступу: http://test-automatyka.pl/?page_id=272&lang=en.

2. Mini-SCADA для Android, KaScada [Електронний ресурс] – Режим доступу: https://apkpure.com/ru/hmi-kascada-modbus/ru.kablov.kascada.

3. MasterOPC Modbus Server [Електронний ресурс] – Режим доступу: https://opc-server.com/

УДК 621.316.71
Сергієнко О.Ю.[1], Рева В.І.[2]
[1] студ. РТ-310м НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

АВТОМАТИЗОВАНА СИСТЕМА ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

У даній роботі представлені результати дослідження автоматизованої системи захисту від несанкціонованого доступу, імплементованої в систему розумний будинок «Smart-House». Така система виконує функцію автоматичного моніторингу стану датчиків і модулів встановлених у будинку, з можливістю дистанційного керування через Internet або GSM-зв'язок, а також має систему безпеки з функцію оповіщення власника про порушення периметру. Автоматизована система має великий діапазон застосування: від офісу, квартири до приватного будинку із земельною ділянкою з декількома будівлями. Точками контролю доступу можуть бути двері, ворота, шлагбауми, місця на парковці, ліфти або інші фізичні перешкоди, де отримання доступу може бути проконтрольовано електронікою

Було здійснено проектування цієї автоматизованої системи, виконано синтез концептуальної моделі. Система не тільки виконує автоматичну функцію контролю датчиків і точок контролю, але й має підсистему візуалізації, на основі якої користувач має можливість відстежувати та контролювати поточний стан усієї системи. Крім цього, користувач може отримувати інформацію та керувати охоронною системою за допомогою GSM зв'язку. Основною ознакою, за якою система приймає рішення про дозвіл доступу є ідентифікатор користувача. В якості ідентифікаторів використовуються автономні носії ознак допуску: магнітні картки. Також застосовуються безконтактні карти, або безконтактний доступ з використанням GSM–модуля.

Система реалізується на платі Arduino MEGA 2560, Internet shield (W5100). На модулі також встановлені: карта пам'яті для зберігання *html* версії сторінки, через яку виконується дистанційний контроль; 8-ми канальній модуль реле, який керує виконавчими пристроями, датчиками руху, силовим навантаженням, датчиками. Для відправки повідомлень використовується GSM-модуль SIM900. У якості виконавчих пристроїв контролю доступу використовуються запірні або керовані перегороджуючі пристрої: замки, засувки і автоматичні ворота.

Передачу інформації про стан датчиків та охоронної сигналізації до головної системи виконує спеціальне програмне забезпечення. Інформація про будь-які зміни в системі виводиться на дисплей в Online-режимі,

дублюється на html сторінку, а у разі спрацювання сигналізації - надсилається SMS повідомлення.

До переваг системи порівняно з аналогами можна віднести можливість тонкого налаштування чутливості системи, підбір елементної бази з низьким енергоспоживанням, можливість в будь-який момент часу виконувати операції вручну, також є можливість розширити систему та обновляти ПО. Система ремонтопридатна, оскільки всі елементи системи модульні.

Технологічними особливостями є:

- Віддалене ручне керування системою за допомогою GSM;
- Відображення в браузері журналу подій, причин спрацювання сигналізації, статистичних даних;
- Можливість добавляти і видаляти користувачів за допомогою Веб-інтерфейсу.

Згідно визначених критеріїв якості, синтезовано структурну схему системи (рис. 1).

Рисунок 1 – Блок схема автоматизованої системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Воробйов О.І. Проектування, монтаж, технічне обслуговування установок пожежної сигналізації: [навчальний посібник] / Воробйов О.І. – Львів: Сполом, 2003. – 138 с.

УДК 530.18
Атинакова В.Р.[1], Сніжной Г.В.[2]
[1] студ. гр. РТ-317, НУ «Запорізька політехніка»
[2] д-р техн. наук, завідувач кафедри МіНЕ НУ «Запорізька політехніка»

ВИКОРИСТАННЯ ПРИЛАДІВ MPS MP17XA В ІМПУЛЬСНИХ БЛОКАХ ЖИВЛЕННЯ

Блок живлення є невід'ємним елементом електронного приладу. Перші імпульсні блоки живлення були сконструйовані після винаходу котушки, яка працювала зі змінним струмом. Після випрямлення напруги утворюються прямокутні імпульси з високою частотою, подаються на фільтр виходу низької частоти. Імпульсні блоки живлення перетворюють напругу, віддають потужність на навантаження. Розсіювання енергії від імпульсного блоку майже не відбувається. Його компактність і мала вага також дає перевагу над трансформаторними блоками при однаковій потужності.

При проектуванні імпульсного блоку живлення необхідно враховувати безліч різних аспектів, особливо пов'язаних з безпекою, продуктивністю, розміром, вагою тощо. Ланцюги управління для імпульсних блоків живлення більш складні, ніж в лінійних, тому багато розробників впроваджують інтегровані модулі в блоки живлення. За величиною вихідної потужності джерела живлення можна розділити на: малопотужні (від 1 до 50 Вт), середньої (від 50 до 400...500 Вт), великої (від 500 Вт до 5...10 кВт) і надвеликої потужності (понад 10 кВт) [1].

В даний час управління потужними імпульсними джерелами живлення здійснюються системами на основі контролерів, операційних підсилювачів, керованих джерел опорної напруги, компараторів, таймерів тощо. Для підвищення рівня інтеграції деякі з аналогових мікросхем вибираються багатоканальними. При всіх перевагах аналогової системи управління (можливість заміни окремих компонентів при виході з ладу, порівняно невелика вартість), вона має і певні недоліки. Перш за все, така система містить велику кількість компонентів, що знижує надійність, підвищує трудомісткість в налаштуванні тощо.

Перехід на цифрову елементну базу зумовило впровадження цифрового управління. Як результат, на практиці реалізується два варіанти: комбінована (змішана) та цифрова система управління.

Одним із прикладів неізольованого вихідного стабілізатора живлення змінного/постійного струму є серія приладів MPS MP17xA [2].

Стабілізатор первинної боку MP173A забезпечує точне регулювання постійної напруги (CV) без оптрона. Він підтримує топології понижуючого, підвищує, знижувальні-підвищувального і зворотного каналів. Вбудований в пристрій польовий МОН-транзистор на 700 В спрощує конструкцію і знижує

вартість. Ця функція оптимізує роботу пристрою для автономних додатків з низьким енергоспоживанням, таких як побутова техніка і резервне живлення. Функції захисту включають теплове відключення (TSD), блокування зниженої напруги VCC (UVLO), захист від перевантаження (OLP), захист від короткого замикання (SCP) і виявлення розімкнутого контуру.

На рис. 1 показана практична схема MP173A, в якій він регулює понижуючий перетворювач, що складається з котушки індуктивності (L1), діода (D1) і конденсатора (C4). Резистори (R1 і R2) утворюють подільник напруги, який забезпечує напругу зворотного зв'язку (вивід FB), замикаючи контур управління.

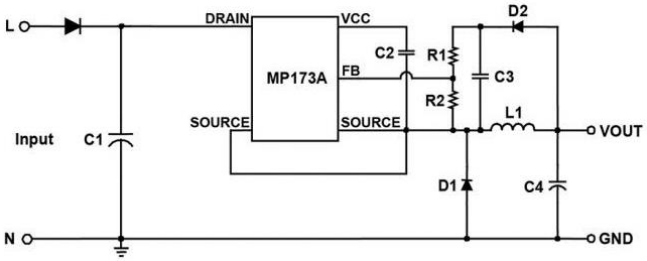


Рисунок 1 – Схема застосування MP173A.

При розробці сучасних імпульсних джерел необхідно врахувати багато важливих технічних особливостей: підвищена частота перетворення (80...250кГц), створення обов'язкових умов для безаварійного включення і виключення, наявність швидкодіючої і надійного захисту від перевантажень, необхідність ефективного відводу тепла, електромагнітну сумісність.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Эраносян С.А. Электронные компоненты для мощных импульсных источников питания / С.А. Эраносян, В.В.Ланцов // Силовая электроника. – 2006. – № 2. – С. 32-38.

2. https://www.monolithicpower.com/en/switching-power-supply – міжнародна компанія з виробництва електронних виробів Monolithic Power Systems (MPS).

УДК 658.56
Єпіщенков В.В.[1], Сніжной Г.В.[2]
[1] студ. гр. РТ-418сп, НУ «Запорізька політехніка»
[2] д-р техн. наук, завідувач кафедри МіНЕ НУ «Запорізька політехніка»

ВХІДНИЙ КОНТРОЛЬ ЯК ЕЛЕМЕНТ СИСТЕМИ УПРАВЛІННЯ ЯКІСТЮ ПРОДУКЦІЇ ПРОМИСЛОВОГО ПІДПРИЄМСТВА

Посилення конкуренції та економічна криза внаслідок світової пандемії COVID-19 обумовлює потребу у безперервному вдосконаленні системи управління якістю (СУЯ). Важливим елементом СУЯ є вхідний контроль (ВК) продукції, який проводиться для запобігання запуску у виробництво продукції, що не відповідає вимогам нормативно-технічної документації (НТД).

Взагалі до завдань вхідного контролю належить перевірка документації на продукцію, контроль відповідності продукції тощо. Для укріплення технологічної дисципліни, покращення якості та підвищення надійності продукції, що випускається, у відповідності вимогам міжнародного стандарту ISO 9001:2015 ефективної організаційної структурою є постійно діюча комісія по виконанню вхідного контролю якості продукції (ВКЯП). Заходи проведення вхідного контролю рекомендовано розробляти згідно вимог наступних документів:

– ISO 9001:2015. «Системи управління якістю. Вимоги»;

– ГОСТ 16504-81 «Система державних випробувань продукції. Випробування і контроль якості продукції. Основні терміни та визначення»;

– ГОСТ 3.1502-85 «Єдина система технологічної документації. Форми і правила оформлення документів на технічний контроль.»;

– ГОСТ 24297-87 «Вхідний контроль продукції. Основні положення»;

– Р50-609-40-01 «Рекомендації. Технологічне проектування технічного контролю», тощо.

Опис та зміст усіх потрібних заходів повинні відображатися в Стандарті підприємства. Стандарт встановлює основні положення по організації, проведенню робіт і оформленню результатів вхідного контролю матеріалів, сировини, напівфабрикатів і комплектуючих виробів, для запобігання запуску у виробництво продукції постачальників, не відповідної вимогам договорів на постачання. Вимоги Стандарту є обов'язковими для всіх структурних підрозділів підприємства, в першу чергу це: відділ головного технолога (ВГТ), відділ матеріально-технічного постачання (ВМТП), відділ технічного контролю (ВТК), комісія з вхідного контролю (КВК), структурний підрозділ підприємства (СПП), центральна заводська лабораторія (ЦЗЛ), центр технічного аудиту (ЦТА), тощо. Переліки

продукції, що підлягає вхідному контролю, погоджують з ВТК, ЦЗЛ, ЦТА і затверджуються Головним інженером.

Основні поняття, терміни і визначення, які використовуються у Стандарті, відповідають ДСТУ ISO 9000, ГОСТ 16504: вибірковий контроль - контроль, при якому рішення о контрольованій сукупності або процесі приймають по результатам перевірки однієї або кількох вибірках; вид контролю - класифікаційне угруповання контролю за певною ознакою; вхідний контроль - контроль продукції, що надійшла на підприємство від постачальника для використання у виробництві; контроль якості продукції - перевірка кількісних та (або) якісних характеристик властивостей продукції, тощо. Відповідальність за виконання вимог Стандарту несуть керівники підрозділів згідно матриці відповідальності.

Вхідний контроль проводиться з метою запобігання запуску у виробництво продукції, що не відповідає вимогам НТД. При цьому вид контролю і об'єм вибірки визначають, виходячи із стабільності якості продукції постачальників та важливості даного параметра (вимоги) для функціонування підприємства. Рекомендується стратифікувати ВК за СПП. Наприклад конструкторські служби підприємства - по виробах, призначених для комплектації; технологічні служби підприємства - по сировині, матеріалам і напівфабрикатам.

Результати вхідного контролю та лабораторних досліджень контролер ВТК заносить у журнал реєстрації результатів, завіряє підписом і печаткою. На прийняту продукцію оформляється акт вхідного контролю (АВК), який містить остаточні висновки про якість продукції і є підставою для запуску її у виробництво або визнання її невідповідності.

Продукція, яка визнана невідповідною встановленим вимогам за результатами комісійного приймання, передається у ізолятор браку до вирішення питання про її заміну або повернення постачальнику. На невідповідну продукцію оформляється попередження про брак, яке направляється начальнику ВМТП.

Для комплексного управління якістю необхідне узгодження різних елементів процесу виробництва. Всі елементи контролю вимагають об'єднання в єдину СУЯ та визначаються великою кількістю чинників, які безпосередньо впливають на якість продукції, що випускається підприємством.

УДК 004.453
Пєхотін Д.А.[1], Сніжной Г.В.[2]
[1] студ. гр. РТ-318сп, НУ «Запорізька політехніка»
[2] д-р техн. наук, завідувач кафедри МіНЕ НУ «Запорізька політехніка»

АВТОМАТИЗАЦІЯ РОЗГОРТАННЯ КОНТЕЙНЕРНОГО ДОДАТКУ В РОБОЧОМУ СЕРЕДОВИЩІ НА БАЗІ AMAZON WEB SERVICES

Amazon Web Services (AWS) є дочірньою компанією Amazon, яка надає платформи для хмарних обчислень на вимогу приватним особам, компаніям та урядам з розподіленою оплатою по мірі використання. [1]. Технологія дозволяє абонентам мати у своєму розпорядженні повноцінний віртуальний кластер комп'ютерів (група комп'ютерів, об'єднаних високошвидкісними каналами зв'язку, що представляє з точки зору користувача єдиний апаратний ресурс), який завжди доступний через Інтернет. Віртуальні комп'ютери AWS мають більшість атрибутів реального комп'ютера, включаючи апаратні пристрої (процесор, відеокарту, локальну та оперативну пам'ять, жорсткий диск або SSD-накопичувач); операційну систему на вибір; прикладні програми, такі як веб-сервер, база даних, CRM і т. д. Кожна система AWS також віртуалізує консольний ввід/вивід (клавіатура, дисплей і миша), що дозволяє користувачам AWS підключитися до своєї системи AWS за допомогою браузера. Браузер виступає як вікно у віртуальний комп'ютер, дозволяючи користувачу входити в систему, налаштовувати та використовувати свої віртуальні системи так само, як справжній, фізичний комп'ютер.

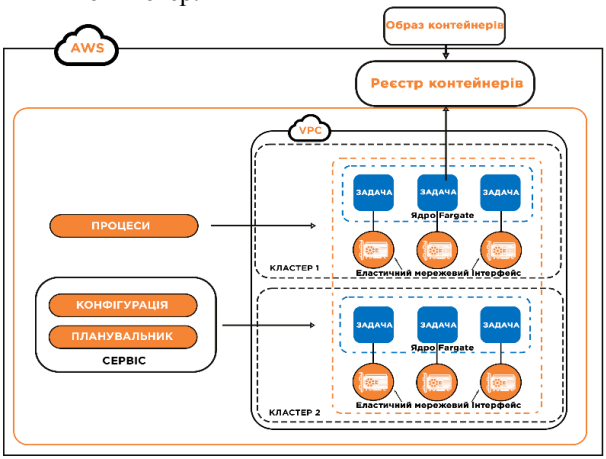


Рисунок 1 – Архітектура середовища Amazon ECS, що працює на AWS Fargate.

Служба Amazon Elastic Container Service (Amazon ECS) – це високомасштабована та швидка служба управління контейнерами, яка спрощує запуск, зупинку та управління контейнерами в кластері. Контейнери використовують для виконання окремих процесів або процесів у службі. Служба - це конфігурація, яка дозволяє запускати та підтримувати визначену кількість одночасний процесів в кластері. Можливо запускати налаштовані конфігурації та сервіси в безсерверній інфраструктурі керованій ядром AWS Fargate (рис. 1). Є можливість запланувати розміщення контейнерів у кластері залежно від потреб до ресурсів, політик ізоляції та вимог к доступності.

ECS можна використовувати для створення узгодженого середовища розробки та робочого середовища, управління та масштабування пакетних робочих навантажень, а також для створення складної архітектури на основі моделей мікросервісів.

Amazon ECS - це регіональний сервіс, який спрощує роботу контейнерів в декількох зонах доступності в межах одного регіону для пришвидшення роботи служб та постійного стабільного доступу, наприклад в регіоні Париж знаходиться три ЦОД (зони доступності). Після того, як кластер починає працювати, можливо створювати конфігурацію, яка визначає, як образи контейнерів будуть працювати в кластерах. Створення конфігурації також використовується для запуску процесів або створення служб. Образи контейнерів можуть зберігатися і завантажуватися з реєстрів контейнерів, наприклад Amazon Elastic Container Registry. Можливо створювати кластери Amazon ECS в новому або існуючому VPC (це комерційний сервіс хмарних обчислень, який надає логічне ізольований розділ в AWS). Сервіси AWS використовуються для автоматизації розгортання веб-сайту в робоче середовище, цей підхід надає переваги в вигляді швидкого оновлення, простоти розгортання, безперебійну та якісну роботу продукту що важливо для сайтів з великою аудиторією.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html – документація Amazon Elastic Container Service.

УДК 004.3
Червоненко А.О.[1], Сніжной Г.В.[2]
[1] студ. гр. РТ-410м НУ «Запорізька політехніка»
[2] д-р техн. наук, завідувач кафедри МіНЕ НУ «Запорізька політехніка»

СИСТЕМА АВТОМАТИЧНОГО ВМИКАННЯ РЕЗЕРВУ ЕЛЕКТРОПОСТАЧАННЯ НА БАЗІ ПРОГРАМОВАНОГО ІНТЕЛЕКТУАЛЬНОГО РЕЛЕ EASY E4

Пристрої автоматичного вмикання резерву (АВР) призначені для відновлення живлення споживачів шляхом автоматичного приєднання резервного джерела, для автоматичного вмикання резервного устаткування в виробничих процесів, технологія яких не допускає навіть короткочасне переривання живленні.

Рисунок 1 – Інтелектуальне реле EasyE4.

Існує велика кількість таких систем, які в основному побудовані на базі програмованих логічних контролерів ПЛК. Інтелектуальне реле (рис. 1) – це один з видів програмованих логічних контролерів, головна перевагою яких є низка вартість подальшої модернізації. Програмування здійснюється за допомогою середовища EasySoft7, наприклад, на мові FBD (функціональні блокових діаграм).

Система АВР електропостачання на базі програмованого інтелектуального реле EasyE4 АВР виключає можливість замикання між собою двох незалежних джерел живлення один на одного. Передбачена наявність не тільки електричного, але і механічного блокування комутаційних апаратів.

Так, наприклад, у разі підключення джерела безперебійного живлення (ДБЖ) до виходу АВР, узгодження між собою діапазонів вхідної напруги обох пристроїв дозволяє забезпечити своєчасне перемикання на резервну

мережу при відхиленні напруги основної живлячої мережі за задані значення, та, тим самим, виключити тривалу роботу ДБЖ при справній резервній мережі.

УДК 530.145+678.9
Курбацький В.П.[1], Коротун А.В.[1], Погосов В.В.[2], Упир А.П.[3]
[1] доц. НУ «Запорізька політехніка»
[2] проф. НУ «Запорізька політехніка»
[3] студ. гр. РТз 417

РОЗРАХУНОК ПОВЗДОВЖНЬОЇ РОЗДІЛЬНОЇ ЗДАТНОСТІ СКАНУВАЛЬНОГО ТУНЕЛЬНОГО МІКРОСКОПА

Робота сканувального тунельного мікроскопа (СТМ) заснована на явищі тунелювання електронів крізь потенціальний бар'єр. Коли зонд наближається до поверхні зразка на відстань приблизно 1 нм, електрони починають тунелювати через проміжок між ними. Тунельний струм, що змінюється в процесі сканування, є тим сигналом, який використовують для формування контрасту зображення [1].

Сила тунельного струму дуже сильно залежить від відстані між зондом і зразком, що обумовлює високу чутливість приладу. Гранична роздільна здатність СТМ в нормальному до зразка напрямку z визначається шумами і складає приблизно 10^{-3} Å [2]. Розділення у площині xy обмежується розмірами області локалізації тунельного струму на поверхні зразка. Метою роботи є оцінка граничної роздільної здатності СТМ в цьому напрямку.

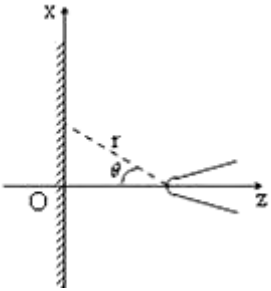


Рисунок 1 – Тунельний перехід в СТМ.

Рівняння Шредингера в області між вістрям зонду і поверхнею зразка (рис. 1) має вигляд

$$\Delta\psi - \kappa^2\psi = 0\,, \tag{1}$$

де $\kappa \equiv \sqrt{2mU_0}/\hbar$, U_0 – висота потенціального бар'єру, яка приблизно дорівнює характерному значенню роботи виходу 5 еВ (eV набагато менше цієї величини і складає кілька десятих електрон-вольта), V – напруга зміщення між зондом і зразком, e – заряд електрона, m – його маса, $\hbar$ – стала Планка. Розв'язок цього рівняння

$$\psi = A\exp(-\kappa r)/r\,,\ A = const\,. \tag{2}$$

Знехтуємо відбиванням електронів від поверхні зразка, тобто будемо вважати, що всі електрони, які тунелюють до поверхні, дають внесок в струм. Потік електронів через поверхню зразка

$$j \sim |\psi|^2 \cos\theta = A^2 z\exp(-2\kappa r)/r^3\,. \tag{3}$$

Тунельний струм через ділянку S поверхні зразка дорівнює $I(S) = \int_S j dS$.

Визначимо величину R наступним чином:

$$I(z \le r \le R)/I(z \le r < \infty) = 0.9\,. \tag{4}$$

Обчислення з використанням формули (3) приводять до співвідношення

$$\frac{R}{z}\exp(\kappa(R-z)) = \sqrt{10}\,. \tag{5}$$

Користуючись рівнянням (5), можна знайти R. В першому наближенні в цьому рівнянні можна прийняти $R/z = 1$. Тоді маємо

$$R - z \approx 1.2/\kappa\,. \tag{6}$$

Підставляючи типові значення $\kappa = 1.2$ 1/Å, $z = 3$ Å, отримуємо $R = 4$ Å.

Як випливає з визначення (4) величини R, мікроскоп усереднює деталі поверхні зразка в області радіусу $x = \sqrt{R^2 - z^2}$, тому ця величина може слугувати оцінкою роздільної здатності мікроскопа в площині поверхні зразка. Користуючись отриманим значенням R, знаходимо, що $x \approx 3$ Å.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Тузяк, О.Я. Основи електронної та зондової мікроскопії [Текст] / О.Я. Тузяк, В.Ю. Курляк. – Львів: ЛНУ імені Івана Франка, 2012. – 296 с.

2. Курбацький, В. П. Граничні характеристики сканувального тунельного мікроскопа [Текст] / В. П. Курбацький, А. В. Коротун, В. В. Погосов // VI Міжнародна науково-технічна конференція з нагоди 90-річчя УДХТУ «Комп'ютерне моделювання та оптимізація складних систем» (КМОСС-2020) (Листопад, 4-6, 2020). – Дніпро, ДВНЗ УДХТУ, Україна. – С. 192–193.

СЕКЦІЯ «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЕЛЕКТРОННИХ ЗАСОБІВ»

УДК 621.396.6.017:004.942
Дейдей В.С.[1],Шило Г.М.[2], Куляба-Харитонова Т.І.[3], Чернишев В.А.[4]
[1] бібліотекар ВСП «ЗФККТ НУ «Запорізька політехніка»
[2] д-р техн. наук, проректор НПР та ППРУ НУ «Запорізька політехніка»
[3] старш. викл. НУ «Запорізька політехніка»
[4] студ. гр.РТ-510 НУ «Запорізька політехніка»

МОДЕЛЮВАННЯ ТЕПЛОВИХ РЕЖИМІВ РАДІОЕЛЕКТРОННИХ ПРИСТРОЇВ В FUSION 360

Хмарні технології і обчислення надають можливість спільного користування ресурсами, інформацією та програмним забезпеченням через підключення до Інтернету. Інформація та дані зберігаються на віртуальних чи фізичних серверах, котрі контролюються і підтримуються постачальником хмарних обчислень. Такий підхід зараз впроваджується в CAD/CAM/CAE-системах.

Особливо актуально використання хмарних САПР в навчанні студентів. Компанії, що розробляють такі системи, надають можливість використання безкоштовної версії для університетів. Перевагами Fusion 360 над іншими хмарними САПР є можливість проведення базового моделювання теплових режимів без встановлення додаткових модулів.

В основі теплових розрахунків у Fusion 360 лежить Autodesk Nastran In-CAD – вбудована система, що базується на методі кінцевих елементів. Генератор розрахункової сітки у Fusion 360 за замовченням генерує сітку кінцевих елементів у автоматичному режимі, також є можливість самостійно настроїти параметри сітки та вручну виділити окремі зони, де необхідно задати особливі параметри. При формуванні сіток у великих габаритах обчислювального простору система застосовує адаптивні сітки, де розмір комірок зменшено для дрібних об'єктів або відбувається зміна форми чи напрямку потоку.

Основні етапи методики моделювання теплових режимів у хмарній Fusion 360 в середовищі SIMULATION.

Крок 1. Створення 3D-моделі або імпорт вже існуючої моделі з інших САПР – створення тривимірної геометрії пристрою або відкриття вже існуючої.

Крок 2. Створення проєкту у середовищі «Simulation Workspace» – вибір задачі, із урахуванням теплопередачі у пристрої.

Крок 3. Завдання параметрів оточуючого середовища та матеріалів пристрою.

Крок 4. Завдання температурних умов роботи пристрою – потужності джерела тепла, температури оточуючого середовища.

Крок 5. Завдання базової розрахункової сітки.

Крок 6. Адаптація базової розрахункової сітки для проведення найбільш точних розрахунків.

Крок 7. Запуск процесу симуляції.

Крок 8. Аналіз результатів симуляції – визначення координат, значень максимальної температури нагріву друкованих плат у пристрої та перепад температури на платі та у середині корпусу.

Застосування алгоритму розглянуто на моделі блоку етажерочної конструкції (рис.1).

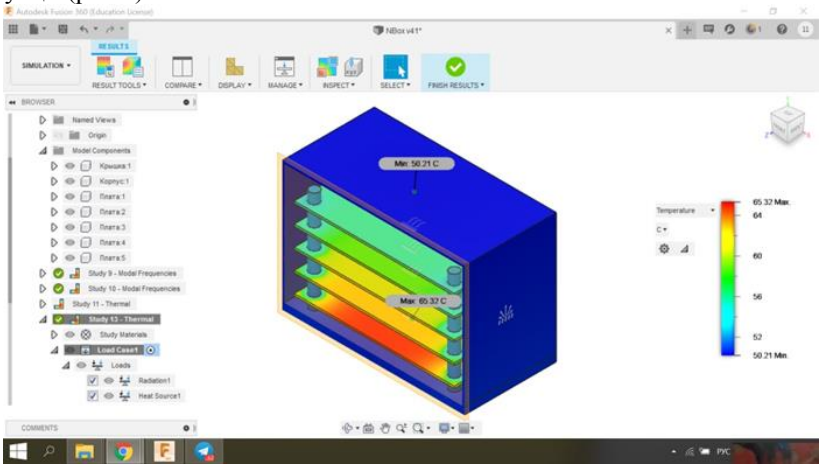


Рисунок 1 - Розподіл температур всередині блока

Таким чином, Під час дослідження теплових режимів в Fusion 360 проводився аналіз максимальної температури плат. В результаті встановлено, що максимальне значення температури плат залежить від потужності розсіювання та розміщення плат. Теплопередача від верхньої поверхні плати відбувається конвекцією та випромінюванням до поверхні корпусу із значно меншою температурою, що покращує тепловідвід та, як наслідок, зниження температури верхньої плати. Тепловідвід конвекцією та випромінюванням від внутрішньої поверхі плат здійснюється у просторі з більш високою температурою, що обумовлює підвищення температури цих плат. В процесі дослідження також з'ясовано, що температури корпусу практично однакові. Тому при оптимізації розміщення плат у блоці доцільно враховувати лише перепад температури у блоці, котрий визначається різницею максимальної температури у блоці та температурою основи корпусу.

УДК 004.942:669-1
Шило Г.М.[1], Шевченко О.С.[2]
[1] д-р техн. наук, проректор з НПР та ППРУ НУ «Запорізька політехніка»
[2] старш. викл. каф. ІТЕЗ НУ «Запорізька політехніка»

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ПРОЦЕСУ МІКРОПЛАВОК В ІНДУКЦІЙНІЙ ПЕЧІ

Мікрометалургійні плавки мають свої особливості та потребують додаткових досліджень для визначення оптимальних параметрів роботи печі. Через складність таких досліджень на реальних об’єктах та необхідність проведення великої кількості експериментів, доцільно використовувати попередні дослідження з допомогою віртуальних комп’ютерних моделей металургійних печей, що створюються на базі CAE-системи. Тому комп’ютерне моделювання індукційної печі є актуальною задачею для дослідження металургійних процесів.

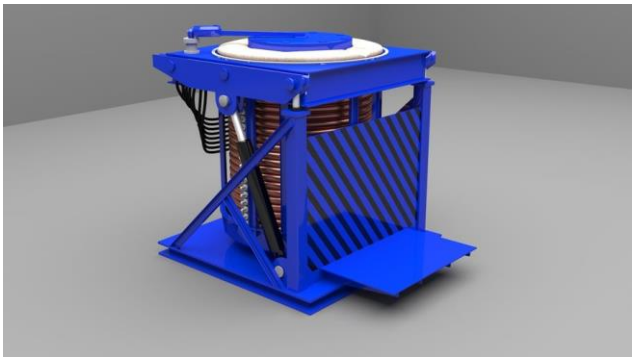


Рисунок 1 – Тривимірна модель вакуумної індукційної печі для мікроплавок

Метою роботи є розробка віртуальної моделі вакуумної індукційної плавильної печі для мікрометалургійних досліджень.

Під процесом мікрометалургії розуміють плавку невеликих об’ємів металу з вагою від 80 до 300 грам для отримання зразків для досліджень. Для проведення мікрометалургійних досліджень створено вакуумну індукційну піч, яка має досить невеликі розміри – робоча камера 220х220х280 мм, індуктор - діаметр 100 мм та висота 130 мм. В камері є можливість створити глибину вакууму 15 мікрон. Споживана потужність індуктора становить 1500 Вт. Тривимірну модель печі наведено на рис. 1.

Для проведення розрахунків було створено спрощену геометричну модель індуктор-тигель, яка містить в собі лише керамічний тигель та мідний

індуктор (рис. 2), де 1 – тигель, 2 – мідний індуктор. На цій моделі проводиться розрахунок часу переходу стопів з твердої у рідку фазу. Для цього задаються параметри потужності та частоти індуктора. Розроблена віртуальна модель не враховує глибину вакууму робочого середовища печі, теплопередачі від індуктора до кожуха печі. Однак, таке спрощення значно не вплине на реальний час проведення плавки.

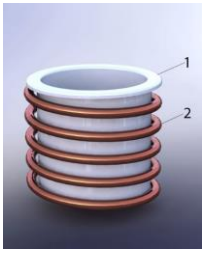


Рис. 2 – Тривимірна модель індуктор-тигель для проведення розрахунку режиму плавлення

Для проведення попередніх розрахунків режимів нагрівання використовувалась CAE-система COMSOL Multiphysics [1].

Для дослідження процесу плавки враховуються параметри: атмосфера середовища (тиск граничного вакууму, або інше середовище), частота та напруга індуктора, потужність конденсаторної батареї, контроль температури середовища, тигля, охолоджуючої рідини індуктора. Контроль та керування цими параметрами дозволить біль точно розрахувати режим роботи обладнання. В умовах проведення сучасних досліджень нових сплавів печі повинні відповідати параметрам високої ефективності, надійності та гнучкості своїх процесів. Оскільки індукційній печі необхідна велика потужність для досягнення температури, необхідної для нагріву та плавлення, низка досліджень направлена на енергоефективність та точність розрахунку спожитої електричної енергії. Енергетична оптимізація передбачає покращення економічних показників, екологічності та як наслідок зменшення витрат на розробку та дослідження нових сплавів [2].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Vincent Bruyere «Tips and Tricks for Modeling Induction Furnaces» COMSOL Blog, 4 march 2015 [Електронний ресурс]. – Режим доступу: https://www.comsol.eu/blogs/tips-and-tricks-for-modeling-induction-furnaces/?setlang=1

2. Antolin-Urbaneja, Juan & González, Asier & Lopez-Guede, Jose & Ipiña, J. (2018). Digital industrial furnaces: Challenges for energy efficiency under VULKANO project. Journal of Energy Systems. 204-217. 10.30521/jes.474499.

УДК 378.147
Фурманова Н.І.[1], Фарафонов О.Ю.[1], Малий О.Ю.[2]
[1] канд. техн. наук, доц., доцент каф. ІТЕЗ НУ «Запорізька політехніка»
[2] канд. техн. наук, доцент каф. ІТЕЗ НУ «Запорізька політехніка»

ВИКОРИСТАННЯ МОДЕЛІ «ПЕРЕВЕРНУТОГО КЛАСУ» ДЛЯ НАВЧАННЯ ЗА СПЕЦІАЛЬНОСТЯМИ 172 ТА 151

Використання традиційних підходів до організації навчального процесу має свої переваги та недоліки. З одного боку, відпрацьовані за багато років методики є зрозумілими та звичними для викладачів та студентів. З іншого боку, існує ряд причин, з яких застосування моделі «перевернутого класу» може розглядатися як прийнятний варіант навчання:

- рекомендоване співвідношення годин аудиторної роботи і годин самостійної складає близько 40:60;

- навчання має формувати у здобувача різні компетентності, пов'язані із самоосвітою (151 спеціальність: здатність до пошуку, опрацювання та аналізу інформації з різних джерел [1]; 172 спеціальність: здатність до абстрактного мислення, аналізу та синтезу; здатність планувати та управляти часом; здатність вчитися і оволодівати сучасними знаннями; вміння виявляти, ставити та вирішувати проблеми [2]).

Сьогодення вносить додаткову причину для застосування моделі «перевернутого класу»: у форматі змішаного навчання, коли кількість аудиторних занять обмежена, така модель є найбільш відповідною для отримання та закріплення знань.

«Перевернутий клас» - це модель освіти, яка передбачає отримання теоретичних знань здобувачем самостійно, під час опрацювання лекційних матеріалів, а аудиторні заняття складаються із обговорення вивченого матеріалу, внесення роз'яснень, презентації проєктів, виконання практичних занять тощо. При цьому теоретичний матеріал може надаватися як у вигляді попередньо записаних відеолекцій, доступних здобувачу у будь-який час, так і у вигляді текстових матеріалів, наданих здобувачам освіти.

Завдання для самостійного опрацювання можуть містити не лише лекційний матеріал, але і роботу в команді для виконання групових проєктів, що потім презентуються під час аудиторних або онлайн-занять з викладачем.

Такий підхід було застосовано на кафедрі ІТЕЗ, зокрема, під час викладання дисципліни «Основи технології електронних апаратів». Здобувачі

отримували всі необхідні матеріали для самостійного опрацювання (лекції, статті, відеофайли тощо), які під час занять із викладачем аналізувались, обговорювались, уточнювались. Викладання дисципліни «Обчислювальна техніка та мікропроцесори» також містило виконання завдань із написання програм для мікроконтролерів, які в подальшому розглядалися під час занять.

Переваги моделі «перевернутого класу» наступні:

- студент отримує знання не пасивно, під час прослуховування лекцій, а активно, що сприяє більшій залученості до освітнього процесу та отримання знань;

- здобувач несе відповідальність за власне навчання [3];

- розв'язання практичних задач самостійно стимулює пізнавальну діяльність, знання здобуваються із зануренням у проблематику.

Хоча дана модель навчання може бути складною для як для викладача, оскільки вимагає більшого часу для підготовки занять, так і для здобувача, що не мав досвіду навчання у такому форматі, на нашу думку, такий підхід є актуальним і найбільш відповідним вимогам часу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стандарт вищої освіти бакалавра за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології» галузі знань 15 Автоматизація та приладобудування» [Електронний ресурс]. – Режим доступу: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/151-avtomatizatsiya-ta-kompyuterno-integrovani-tekhnologii-bakalavr.pdf

2. Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 17 «Електроніка та телекомунікації», спеціальність 172 «Телекомунікації та радіотехніка» [Електронний ресурс]. – Режим доступу: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/172-telekomunikatsii-ta-radiotekhnika-bakalavr.pdf

3. Приходькіна Н.О. Використання технології «перевернеого» навчання у професійній діяльності викладачів вищої школи / Н.О. Приходькіна [Електронний ресурс]. – Режим доступу: http://qoo.by/2Bk

УДК 681.51
Фарафонов А.Ю.[1], Малий О.Ю.[2], Піроженко О.О.[3]
[1] канд. техн. наук, доц., доцент каф. ІТЕЗ НУ «Запорізька політехніка»
[2] канд. техн. наук, доцент каф. ІТЕЗ НУ «Запорізька політехніка»
[3] аспірант каф. ІТЕЗ НУ «Запорізька політехніка»

ПРОЕКТУВАННЯ РОБОТА ДЛЯ ДОСЛІДЖЕННЯ ГРУПОВОЇ ПОВЕДІНКИ

Для дослідження групової поведінки з 2012 року використовуються рішення у вигляді малогабаритних автономних роботів під назвою Kilobot [1], або більш конструктивне складного рішення 2015 року 3D M-Block [2], або рішення Tribots [3], а також так звані роботи з «ройовим» інтелектом, які направленні на оптимізацію зв'язку та взаємодії один з одним: SwarmBot [4], Swarmanoid [5], I-SWARM [6]. Ці рішення повинні реалізовувати наступний функціонал:

- рух вперед;
- обертання;
- зв'язок з сусідами;
- вимірювання відстані;
- масштабування кількості роботів.

У якості елементів зв'язку використовують інфрачервоні або світлодіоди. Але у Kilobot використання інфрачервоного діоду дозволяє отримувати інформацію о найближчих сусідах та не дає змогу визначити напрямок на сусіда. У Robocube взагалі діоди видимого кольору подають усього дві команди: на паркування або продовжити рух.

Масштабування кількості роботів у групі є найскладнішою задачею. Це пов'язано з неможливістю точно визначити кількість роботів, необхідних для виконання конкретної задачі. Технологія S-DASH (масштабоване розподілене самостійне збирання та самовідновлення) дозволяє не тільки масштабувати кількість роботів в групі для відтворення зображення, а й масштабувати саме зображення виходячи з кількості роботів в групі [7]. Таким чином, кількість роботів в групі може обмежуватися лише площею для виконання поставленої задачі.

Використання Kilobot потребує заказ друкованих плат та складне мініатюрне складання та значні витрати коштів на живлення. Конструкція Robocube та Tribots досить складна для відтворення. Конструкції типу роботів-термітів недостатньо описані [8]. Тому пропонується конструкція робота для дослідження групової поведінки з використанням ESP-32. Використання мережі Wi-Fi дозволить проводити керування роботом за допомогою отриманого роботом IP адреса, що значно спрощує доступ та програмну реалізацію загального керування та ідентифікації.

До складу робота входить:

- компас для орієнтації робота;
- лазерний датчик відстані з діапазоном до 2 метрів для визначення сусідніх роботів та перешкод;
- ІЧ приймач для ідентифікації присутності інших роботів поряд;
- аналоговий датчик освітлення для ідентифікації робота від перешкоди та визначення точного напрямку на робота;
- світло та інфрачервоний діоди ідентифікації та світлодіоди індикації стану;
- рухома платформа.

Аналоговий датчик освітлення має додаткові елементи для формування вузької діаграми направленості що і дозволяє ідентифікувати напрямок на робота та підтвердити показами лазерного датчика відстані. Окрім цього аналоговий датчик освітлення за допомогою відповідної схеми перетворюється у приймач інтерфейсу UART – що одночасно дозволяє провести не тільки ідентифікацію робота, але і трансляцію однонаправленого повідомлення за допомогою світлодіоду.

Таким чином, конструкція робота дозволяє імітувати таки елементи групової взаємодії:

1. Орієнтування індивіду у просторі.
2. Почуття присутності інших у зоні дотику.
3. Ідентифікація перешкод та сусідів.
4. Віддалена однонаправлена комунікація у вигляді повідомлення іншим (декларація намірів).

Ця конструкція є базовою та не включає елементи спрямованого двонаправленого зв’язку між сусідніми роботами, що моделює ситуацію взаємодії індивідів на значної відстані.

Якщо необхідно реалізувати двонаправлену передачу даних це можна зробити програмно при ідентифікації одного робота іншим за допомогою Wi-Fi мережі.

Розроблена конструкція є габаритною у порівнянні з аналогами але не потребує оригінальних комплектуючих та складної реалізації живлення та підзарядки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Rubenstein, M., Shen, W-M. Scalable self-assembly and self-repair In A Collective Of Robots // 2009 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). — 2009-12-11. — С. 1484-1489.

2. Прыгающие робокубы научились узнавать друг друга и самоорганизовываться [Електронний ресурс]. – Режим доступу: https://nplus1.ru/news/2019/10/31/m-blocks.

3. Распределение обязанностей помогло роботам точно передвинуть груз [Електронний ресурс]. – Режим доступу: https://nplus1.ru/news/2019/07/11/tribots.

4. Mondada, F., Pettinaro, G.C., Guignard, A. et al. Swarm-Bot: A New Distributed Robotic Concept // Autonomous Robots 17. — 2004. — С. 193–221.

5. M. Dorigo et al. Swarmanoid: A Novel Concept for the Study of Heterogeneous Robotic Swarms // IEEE Robotics & Automation Magazine, vol. 20, no. 4. — Dec. 2013. — С. 60-71.

6. H. Woern, M. Szymanski and J. Seyfried. The I-SWARM project // ROMAN 2006 - The 15th IEEE International Symposium on Robot and Human Interactive Communication, Hatfield, UK — 2006. — С. 492-496.

7. M. Rubenstein, Wei-Min Shen. Automatic scalable size selection for the shape of a distributed robotic collective // 2010 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). — 2010-10-01. — С. 508-513.

8. A multirobot construction system [Електронний ресурс]. – Режим доступу: https://science.sciencemag.org/content/343/6172.cover-expansion.

УДК 622.2.33.36

Котляров В.А.[1], Фарафонов О.Ю.[2]
[1] студ. гр. РТ-118 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц., доц. каф. ІТЕЗ НУ «Запорізька політехніка»

ВИКОРИСТАННЯ ПРОТОКОЛУ I2C НА ПРИКЛАДІ ЛАЗЕРНИХ ДАТЧИКІВ ВІДСТАНІ

При використанні лазерних датчиків відстані передача даних відбувається через протокол I2C. Цей протокол реалізовано на датчиках відстані виводами scl та sda, які генеруюсь логічні сигнали. Scl шина відповідає за генерацію сигналів, а sda шина – за передачу даних (дивіться рис.3).

Один такий сигнал відповідає одному біту. Пін xShut дозволяє звертатися до датчика та змінювати його адресу.

Знявши дані з scl та sda шин логічним аналізатором, отримано результати у вигляді графіку. На sda шині з'явилося багато пакетів даних, але зараз нас цікавлять перші три. В них здійснюється присвоєння адрес трьом датчикам, що і відбувається у процесі виконання програми (рис.1), яка закладена у платформу ардуіно.

Знявши логічним аналізатором дані з виводів xShut, кожного з датчиків бачимо почергове звернення до них (рис.2).

```
pinMode(XSHUT_pin1, OUTPUT);
pinMode(XSHUT_pin2, OUTPUT);
pinMode(XSHUT_pin3, OUTPUT);

delay(1000);

Wire.begin();

sensor3.setAddress(sensor3_newAddress);
pinMode(XSHUT_pin3, INPUT);
delay(10);
sensor2.setAddress(sensor2_newAddress);
pinMode(XSHUT_pin2, INPUT);
delay(10);
sensor1.setAddress(sensor_newAddress);
pinMode(XSHUT_pin1, INPUT);
delay(10);
```

Рисунок 1 – Розглянута частина програми.

У програмі в цей час йде змінення характеристик пінів ардуіно, до яких підключено ці виводи, з вихідних на вхідні.

Рисунок 2 – Звернення до датчиків.

На графіку, що побудований логічним аналізатором, це виглядає як змінення низького рівня сигналу на високий.

В цей же час на шині sda отримано пакети даних, які відповідають за присвоєння датчикам їх адрес (рис.3).

Спочатку йде ініціалізація датчика зі стандартною адресою, після чого присвоєння індивідуального адресу.

В наступних пакетах даних в шині sda бачимо отримання значень відстані, які відправляють датчики почергово(рис.4). У подальшому на пінах xShut не відбувається жодних змін.

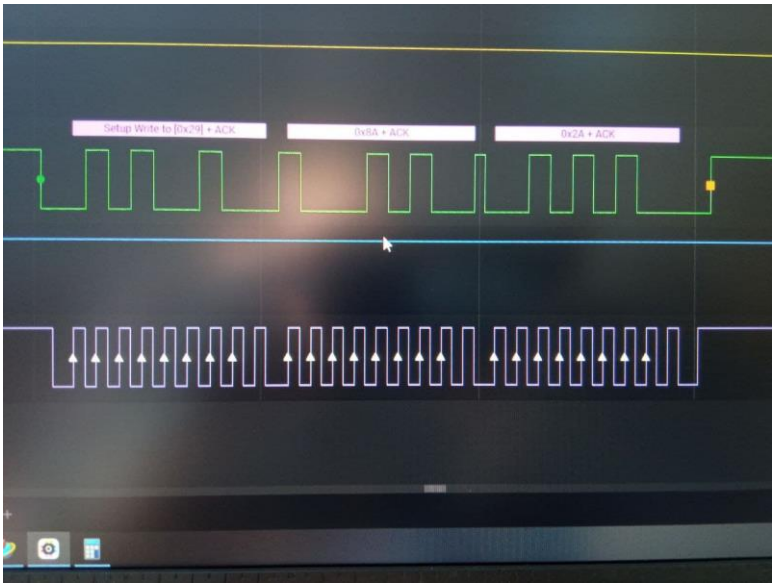


Рисунок 3 – Присвоєння датчику адреси 42.

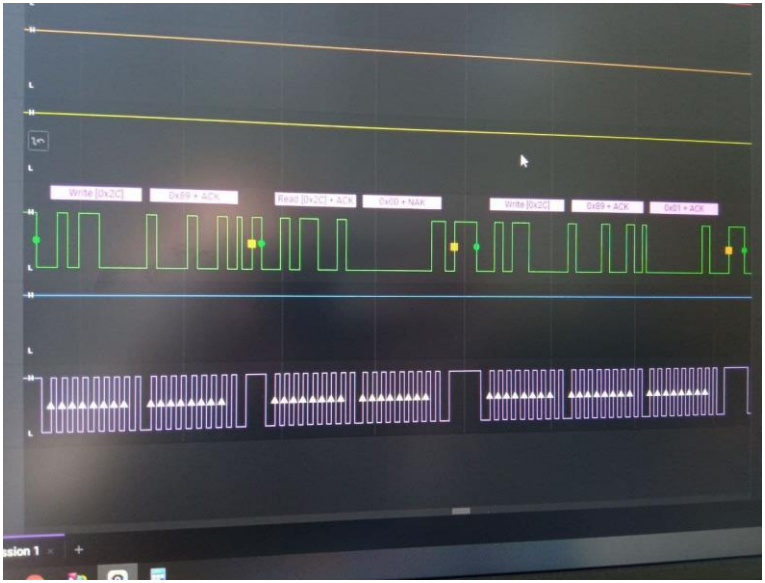


Рисунок 4 – Пакети даних з датчиків.

Отже, замість послідовного звертання до датчиків через xShut, можна просто їх послідовно увімкнути один раз, наприклад за допомогою транзисторів з різними конденсаторами в обв'язці, а потім вимкнути струм на цих виводах. Таким чином можна звільнити піни на ардуіно та скоротити програму, не звертаючись до датчиків окремо в її сетапі.

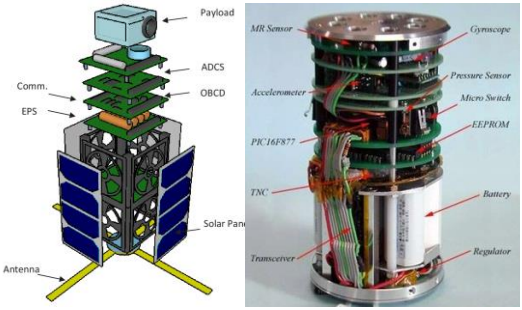
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Интерфейс I2C [Електронний ресурс]. – Режим доступу: www/URL: http://robocraft.ru/blog/communication/780.html - 05.04.2021.

УДК 629.783
Шевченко О.С.
старш. викл. каф. ІТЕЗ НУ «Запорізька політехніка»

ВИКОРИСТАННЯ ПРОТОТИПІВ СУПУТНИКІВ CANSAT ТА CUBESAT В ОСВІТНЬОМУ ПРОЦЕСІ

Вивчення технології конструювання та виготовлення сучасних супутників досить коштовний процес і не кожен навчальний заклад має змогу надати студентам таку можливість. З розвитком сучасних технологій, а саме електроніки, мікропроцесорної техніки та адитивних технологій ця тематика стає ще більш доступною для студентства та науковців.



а б

Рисунок 1 – Структура супутників типу CubeSAT (а) та CanSAT(б)

За допомогою сучасних CAD/CAE-систем можна проєктувати конструкції супутників, а також виконувати розрахунки та симуляції.

Моделі супутників CanSAT та CubeSAT (рис. 1) надають можливість студентам та школярам для проведення досліджень не лише на віртуальних моделях, а навіть і у реальних умовах.

Супутники типу CubeSAT мають габаритні розміри 100x100x100 мм та вагу не більше 1,33 кг і декілька апаратів можуть об'єднуватись в один [1]. В свою чергу, концепція навчальних супутників типу CanSAT побудова на мініатюризації, тобто конструкція не перевищує об'єм жерстяної банки з-під напоїв об'ємом 330 мл. Такі супутники мають наступні габаритні розміри: діаметр – 66 мм, висота – 115 мм, вага – 350 г. Дещо відрізняються такі супутники і по вартості виготовлення, робочій висоті, цілям застосування.

Супутники типу CubeSAT використовують на низькій опорній орбіті на висоті від Землі 193-220 км. Зазвичай такий супутник має в своєму складі один (рідше два) експеримент, засоби зв'язку та телеметрії. Для створення супутників даного типу використовуються готові електронні модулі та програмне забезпечення для них, дуже рідко виготовляють модулі самостійно. Сукупність вищевказаних факторів дозволяє створювати та запускати дані супутники в діапазоні вартості від 60 до 85 тис. доларів і кожен рік цей показник знижується.

Цей сегмент надає доступ і можливість створювати справжні прототипи студентських дослідних супутників і прикладом цього є два українських студентських супутника PolyITAN-1 та PolyITAN-2.

Інший, більш доступний для університетів та навіть шкіл тип супутників CanSAT не має можливості виходу на орбіту Землі, але такий тип супутника має низку переваг. Дуже популярні у всьому світі проведення змагань і хакатонів серед студентської молоді саме з конструювання та виготовлення супутників типу CanSAT. Частіше супутники типу CanSAT використовуються для відпрацювання двох основних задач: визначення температури та тиску атмосфери. Випробування супутника відбувається у наступних етапах: відділення від ракети-носія, включення телеметрії та посадка. Зазвичай висота відділення від носія становить від 1 до 4 км (інколи може становити і 250-750 м) [2] і носієм може бути як ракета так і квадрокоптер. Безперечною перевагою цих супутників є низька вартість – до 500$, яку зазвичай встановлюють організатори змагань.

В теперішній час досить популярною стає космічна тематика і все більше студентів цікавиться напрямком конструювання та використання космічних апаратів дослідницького типу. Тому можна зробити деяке розмежування щодо використання цих двох типів супутників. Супутники типу CanSAT слід використовувати для максимальної популяризації і надання базових знань щодо космічного проєктування, а супутники типу CubeSAT доцільно використовувати для проведення більш глибоких наукових

досліджень і розвитку конструкторських навичок у студентів у напрямку космічної техніки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. CubeSat Design Specification Rev.12. The CubeSat Program, Cal Poly SLO. 21.07.2013. Showing WebCite for URL: http://www.cubesat.org/images/developers/cds_rev12.pdf

2. R. P. Ramadhan, A. R. Ramadhan, S. A. Putri, M. I. C. Latukolan, Edwar and Kusmadi, "Prototype of CanSat with Auto-gyro Payload for Small Satellite Education," 2019 IEEE 13th International Conference on Telecommunication Systems, Services, and Applications (TSSA), Bali, Indonesia, 2019, pp. 243-248, doi: 10.1109/TSSA48701.2019.8985514.

UDC 621.3:378.14

Bielinska I.[1], Furmanova N.[2]
[1]student of RT-517 Zaporizhzhia Polytechnic National University
[2] PhD, Docent of ITED department, Zaporizhzhia Polytechnic National University

«ARTS AND MINDFULNESS IN EDUCATION» PROJECT

Together with the team we are working on the Arts & Mindfulness in Education project.

Every Monday there is a training with coaches and a sponsor, where we meditate, explore our body and mind. Irma Smegen, one of the sponsors of the project gave us a book she wrote herself. It tells about methods of improving education through exercises related to meditation.

To get rid of unnecessary emotions, clear your mind and focus on what is necessary, feel the breath, your body. In today's world, when the pace of life is fast enough, it is very difficult to focus on consciousness and your body.

We meditated with food, ate slowly, tried the texture of chocolate with one finger, sniffed, listened to it. For many it was very funny and surprised. We were asked to wear comfortable clothes for classes and take off shoes in a special room where there are mattresses and you can lie down. We lay for about an hour, I was not very comfortable because I came in dressed in a business style and was impressed. It feels like hypnosis.

From a technical point of view, the project is to create a web application music calendar with a specially selected melody for children of different ages to perform similar exercises. Thereby improving the educational process. We use

Javascript-based libraries, frameworks and develop a database using Postgresql, node.js and more. Defined a technology stack for frontend & backend parts.

We created a working group of 3 people, 2 programmers and 1 designer. Other team members work on site content, collect information about composers, etc. At the beginning of the project, we conducted a Belbin test to distribute roles. We also wrote a project plan and determined deadlines.

We do not have teachers, lectures, laboratory works. But we can ask for help from the teacher or other team.

Related subjects, such as corporate communication and entrepreneurship, cross media design, English, are aimed at enabling us to develop our project. We learned to create logos, study business models and prescribe the target audience, in English we will train presentation skills, facial expressions, gestures and pronunciation.

We are very surprised by the education system in Belgium. Absolutely different approach. There are no requirements, all responsibility is placed on students and only at personal desire, teamwork it is possible to carry out the project moment and in any situation, ready to meet. And very comfortable working conditions on campus.

УДК 004.946
Шило А.П.[1], Пархоменко А.В.[2], Шило Г.М.[3], Огренич Є.В.[4]
[1] студ. гр.РТ-619 НУ «Запорізька політехніка»
[2] студ. гр.РТ-619 НУ «Запорізька політехніка»
[3] проректор НПР та ППРУ НУ «Запорізька політехніка»
[4] в.о.зав.каф.ІТЕЗ НУ «Запорізька політехніка»

АНІМАЦІЯ 3D-МОДЕЛЕЙ В BLENDER

3D-моделювання та анімація на даний момент використовується у багатьох сферах життя, зокрема при створенні медійних продуктів. Серед них можна виділити: кіно, мультфільми, відеоігри, та навіть навчальні відеоролики, що містять в собі корисні матеріали. З появою комп'ютерної графіки створення анімації стало легшим, а також з'явились нові шляхи її реалізації. Впровадження сучасних технологій доповненої та віртуальної реальності не тільки у сферу розваг, а й у промисловість для створення навчальних симуляторів, експлуатаційної документації, потребують формування компетенцій зі створення 3D-моделей та їх анімації у здобувачів на всіх освітніх програмах напряму інформаційних технологій та автоматизації. Сьогодні існує 2 типи анімації: 2D та 3D анімація. У 2D анімації, художнику-мультипликатору доводиться промальовувати кожен кадр його творіння, щоб об'єкт «рухався» на екрані. Анімація у тривимірній

комп'ютерній графіці - це процес зміни властивостей (параметрів) тривимірного об'єкту з плином часу.

За допомогою програми Blender можна реалізувати 3D анімацію декількома шляхами:ключові кадри; анімація за траєкторією; створення анімації при динамічних симуляції; анімація, отримана шляхом захоплення руху (motion capture).

Створення анімації з ключовими кадрами - один з найбільш простих способів створення 3D анімації персонажів. Суть методу полягає у наступному: на шкалі часу задається кілька головних точок, в яких становище або форма об'єкта змінюється. Аніматор задає потрібні параметри моделі в зазначених точках, а «проміжні» кадри програма розраховує автоматично.

Анімація за траєкторією вимагає задати шлях руху об’єкта. Даний спосіб часто підходить для анімації рухомих технічних об'єктів, анімації камер і анімації технічних процесів.

У разі, коли потрібна анімація персонажа у середовищі, доречним стає використання шляху створення анімації при динамічних симуляціях. Такий спосіб є відображенням взаємодії 3D-моделі з навколишнім середовищем. Найпростішим прикладом такого впливу є коливання волосся та одягу моделі від переміщення повітряних мас.

Сьогодні також популярним способом анімації є технологія захоплення рухів. Як правило для отримання анімації даним способом необхідне спеціальне обладнання для захоплення руху, актор, з якого анімація буде захоплюватися, а також спеціальне програмне забезпечення. “Motion capture” використовується практично у всіх фантастичних фільмах та при створенні відеоігор. В результаті такої анімації рухи героя виходять реалістичними та переконливими.

Метод анімації за траєкторією використовується при навчання як ознайомлення з 3D-анімацією. Етапи реалізації “Анімація за траєкторією” у Blender:

Крок 1. Створення 3D-моделі або імпорт вже існуючої моделі з інших програм.

Крок 2. Використовуючи криву “Path”, створити траєкторію переміщення об’єкту.

Крок 3. Розмістити об’єкт на стартову точку анімації.

Крок 4. Закріпити об’єкт на траєкторії.

Крок 5. Редагуємо швидкість переміщення об’єкту по траєкторії. Налаштовуємо тривалість анімації та кількість кадрів на секунду.

Крок 6. За необхідності додаємо на траєкторію ключові точки, в яких деякі параметри 3D-об’єкту повинні змінитися.

Крок 7. Для динамічності анімації можна додати траєкторію камери.

Крок 8. Здійснюємо рендер готових кадрів.
Крок 9. Об'єднуємо кадри в анімацію об'єкта.

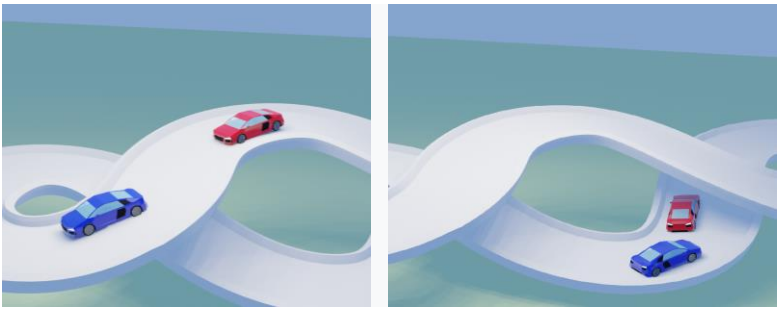


Рисунок 1 - Кадри анімації

Таким чином, була створена анімація руху автомобілів по треку. Був використаний метод "Анімація по траєкторії". Особливістю даного способу реалізації анімації є застосування завдання шляху руху на камеру, що пересувається паралельно із основними 3D-моделями. А також, з цим способом надання анімації циклічності є легшим. Даний метод анімації являється не надто складним у реалізації, що дає змогу його використовувати при навчання як ознайомлення з 3D-анімацією загалом.

УДК 004.94
Бучко І.В.[1], Фурманова Н.І.[2]
[1] студ. гр.РТ-518сп НУ «Запорізька політехніка»
2 канд. техн. наук, доц., доц. каф. ІТЕЗ НУ «Запорізька політехніка»

ГРАФІЧНА ВІЗУАЛІЗАЦІЯ СКЛАДАЛЬНОГО ПРОЦЕСУ РАДІОЕЛЕКТРОННИХ ПРИСТРОЇВ У САПР

З розвитком інформаційних технологій, кожне передове підприємство піклується про впровадження та забезпечення на виробництві, новітніх методів пришвидшення та автоматизації процесів випуску продукції. Сучасні CAD/CAM/CAE-системи пропонують широкий перелік інструментарію для задоволення цього запиту.

Комплект конструкторської містить один з найважливіших документів для виробництва – це складальне креслення виробу. З підвищенням складності виробу в свою чергу ускладнюється складальне креслення та збільшується його об'єм. Це призводить до збільшення необхідних робітників на етапі складання. Також цей факт впливає на навчання нових

кадрів, коли старший робітник вимушений приділяти увагу та час для пояснення особливостей складання того чи іншого приладу.

Графічна візуалізація вирішує низку проблем при організації процесу складання: зниження кількості необхідних робітників на один виріб; знижує поріг входу при навчанні нових спеціалістів; пришвидшує опанування кожного наступного нового приладу.

Метою запропонованого проєкту є створення виконавчого файлу з графічною візуалізацією процесу складання в системі САПР верхнього рівня Siemens NX та доповнення або часткова заміна певної документації в чинному комплекті.

До складу конструкторських програм Siemens NX входять інструменти для проєктування деталей та агрегатів, створення користувацьких конструктивних елементів, проєктування листових тіл, створення простих і складних поверхонь, трубопроводів, електричних джгутів, засоби моделювання людини, проєктування друкованих плат, розробки пресформ і штампів.

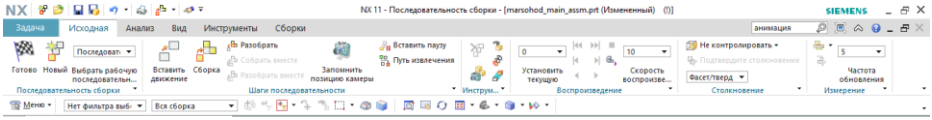


Рисунок 1 – Панель інструменту «Послідовність» в Siemens NX

Процес створення візуалізації не потребує багато часу, адже конструктор під час первинного моделювання виробу накладає усі необхідні “залежності”, які в подальшому буду використанні інструментом «Послідовність. Виконавчий файл з графічною візуалізацією може бути відкритий у самій програмі Siemens NX, так і експортований у відео формат.

Гнучкість формату дозволяє: заощадити кошти на обладнання робочого місця комп’ютерами, так як працівнику достатньо планшету для відтворення процесу складання; швидко вносити зміни в процес складання; підвищує зручність електронного документообігу між робітниками конструкторського бюро та цеху складання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Siemens NX [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Siemens_NX

2. САПР технологічних ліній та комплексів [Електронний ресурс] – Режим доступу: https://elearning.sumdu.edu.ua/free_content/lectured:c63606a1c882cab8eea0d192228761c1ba46c202/latest/259768/index.html

УДК 004.94
Булатов В.В.[1], Фурманова Н.І.[2]
[1] студ. гр.РТ-518сп НУ «Запорізька політехніка»
2 канд. техн. наук, доц., доц. каф. ІТЕЗ НУ «Запорізька політехніка»

СТВОРЕННЯ ВІРТУАЛЬНОГО СЕРЕДОВИЩА НАВЧАЛЬНОЇ ЛАБОРАТОРІЇ В UNITY

Тривимірна графіка, або 3D — розділ комп'ютерної графіки, сукупність прийомів та інструментів, призначених для зображення об'ємних об'єктів.

Тривимірне зображення на площині відрізняється від двовимірного тим, що включає побудову геометричної проекції тривимірної моделі на площину (наприклад, екран комп'ютера) за допомогою спеціалізованих програм. При цьому модель може як відповідати об'єктам з реального світу, так і бути повністю абстрактною.

У сучасних реаліях неможливо уявити свій світогляд без втручання тривимірної графіки.

З кожним роком вона охоплюю все більше і більше сфер діяльності людини. Під час перегляду кінематографії, комп'ютерних іграх, промисловості, міському плануванні, медицині.

Кожній людині потрібен відпочинок, і якщо порівняти рівень розваг і їх реальність 20 років тому і зараз, ми побачимо суттєві зміни в якості реалізації кінематографії та комп'ютерних ігр. Хоч це і не головна первага тривимірної графіки, але це допомагає людині у повній мірі перенестись і відчути весь спектр емоції.

Тривимірна графіка незамінна у презентації майбутнього виробу. Для того, щоб розпочати виробництво необхідно намалювати, а потім створити 3D-модель об'єкту. А вже на основі 3D-моделі, за допомогою технологій швидкого прототипування, складається реалістичний прототип майбутнього виробу.

Після візуалізації, отримане зображення можна використовувати у розробці дизайну упаковки або для створення зовнішньої реклами, POS-матеріалів і дизайну виставкових стендів.

Ми розглянули направлення котрі широко використовується і з якими стикається людина кожен день, а тепер перейдемо до більш важливих на мою думку діяльностей, котрі не тільки полегшують але й зберігають здоров'я і життя людини, а саме: сфера медицини та промислова.

Існують важкі хвороби, лікування котрих потребує високий рівень кваліфікації лікаря, але й цього не завжди достатньо. Трапляються хвороби зв'язані з мозком людини, коли виникає потреба спочатку розробити прототип і на ньому перевірити можливість проведення операції.

На сьогоднішній день це допомогло і врятувало життя не одній тисячі людей.

3D-принтер для стоматологів дозволяє випускати довговічні і якісні моделі коронок, мостів, вінірів та ін. Це істотно полегшує і прискорює роботу зуботехнічної лабораторії, широкий асортимент матеріалів дозволяє в короткі терміни вирішити практично будь-яке завдання. За допомогою стоматологічного 3D-принтера можна моделювати значна кількість необхідних примірників за одну сесію. Всі проекти зберігаються в файлах, тому в майбутньому можна повторно виготовити таку ж модель при необхідності.

В промисловості існують ділянки підвищеної небезпеки, задля цих задач, були розроблені роботи котрі повторюють всі рухи людини, котра в цей момент використовує установку доповненої або віртуальної реальності.

Також і сфера освіти перейняла цю ідею і почала навчати майбутніх працівників не у реальних умовах, в котрих студент може завдати собі і навколишнім шкоду, а у віртуальній реальності, котра відповідає всім стандартам і нормативам виробництва.

Наприкінці свого докладу я приділлю увагу саме тій сфері, котра мені більш до вподоби, а саме 3D—візуалізація.

Технологія 3D-моделювання в архітектурі давно показали себе з найкращого боку. Сьогодні створення тривимірної моделі будівлі є незамінним атрибутом проектування. На підставі 3D-моделі можна створити прототип будівлі. Прототип може повторювати лише загальні обриси будівлі, або бути деталізованою збірною моделлю майбутньої будови.

Що ж стосується дизайну інтер'єрів, то, за допомогою технології 3D-моделювання, замовник може побачити, як виглядатиме його житло або офісне приміщення після проведення ремонту.

Наша кафедра радіоелектроніки та телекомунікації йде в ногу з наукою, тому студенту вже не перший рік набувають та вдосконалюють свої знання у цій сфері.

У своїй дипломній роботі я поєднав візуалізацію інтер’єру з освітньо-пізнавальною функцією. Для цього створюється ідентична копія лабораторії кіберфізичних знань у тривимірному середовищі, після чого вона буде перенесена у програму Unity, в якій буде можливість відобразити нашу лабораторію, та внести функцію пересування по цій кімнаті.

Це стане наглядним прикладом освітнього процесу, котрий абітурієнти зможуть здобути у стінах нашого університету, та екскурсія по лабораторії.

Аби пройти таку екскурсію, або будь яку схожу, у вас є два варіанти:

-перший, коли у вас є установка віртуальної реальності з датчиками та контролерами. Завантаживши необхідний файл у вас буде змога переміститися у стіни лабораторії та ознайомитись з нею, та обладнанням з

яким у вас буде змога працювати, відкриваючи усі шухляди та перемикаючи різні вимикачі.

-другий варіант, більш доступний, але він має менший функціонал, це окуляри віртуальної реальності.

В них вставляється звичайний телефон, запускається таж сама програма, і ви маєте змогу пересуватися так само по лабораторії, але за відсутності контролерів та датчиків, ви не маєте змоги виконувати будь які дії з предметами.

У своєму докладі я приділив увагу як на мене головним перевагам та функціям тривимірної графіки.

УДК 004.94
Поспеєва І.Є.[1], Потапенко А.Р. 2, Соколік І.П.[2]
[1] старш. викл. каф. ІТЕЗ НУ «Запорізька політехніка»
[2] студ. гр. РТ-118сп НУ «Запорізька політехніка»

ОСОБЛИВОСТІ 3D-МОДЕЛЮВАННЯ НЕСУЧИХ КОНСТРУКЦІЙ РАДІОЕЛЕКТРОННИХ, МЕХАТРОННИХ, РОБОТОТЕХНІЧНИХ ПРИСТРОЇВ З ВИКОРИСТАННЯМ САПР INVENTOR

Зараз в усьому світі відбувається загальна комп'ютеризація. Обчислювальна техніка впроваджується в усі галузі людської діяльності – від виконання найскладніших робіт, що потребують одночасної обробки величезної кількості інформації за дуже короткий час, до галузей ігор та розваг.

Останнім часом у інженерній діяльності все ширше застосовуються системи автоматизованого проектування (САПР), які дозволяють виконувати практично усі види проектних робіт. Ці системи постійно розвиваються, ускладнюються, удосконалюються. Якщо перші САПР дозволяли виконувати тільки деякі окремі дії, пов'язані, наприклад, з проведенням розрахунків, моделюванням окремих елементів конструкцій, виконанням креслень, то сучасні САПР – це цілі комплекси, які ув'язують не тільки увесь процес розробки виробів у цілому, а й технологічну підготовку виробництва, документообіг, питання менеджменту у єдине ціле.

Однією з розробок Autodesk є сучасна система Autodesk Inventor, яка дозволяє використовувати нові принципи проектування виробів, засновані на тривимірному (3D) моделюванні, для створення конструкцій будь-якого рівня складності, в тому числі і в галузі радіоелектроніки, мехатроніки, робототехніки, коли вироби містять десятки, а то й сотні електрорадіоелементів, деталей, складових одиниць тощо.

Переваги 3D-моделювання незаперечні. Основний недолік плоского проектування полягає в тому, що за 2D-кресленнями важко уявити, як виріб виглядає в просторі, тому їх доводиться супроводжувати реальними прототипами, в ролі яких виступає перший випущений виріб або перша партія. Помилки в кресленнях доводиться виправляти на вже створеному виробі, що уповільнює випуск продукції і призводить до додаткових витрат. 3D-системи, навпаки, дозволяють змоделювати виріб до створення креслень або дослідних зразків.

3D-технологія дозволяє проводити тестування майбутнього виробу віртуальними методами. Моделі можна передавати в системи інженерних розрахунків, призначені для всебічного аналізу виробів: на функціональність, міцність, довговічність, стійкість до вібрації, керованість, безпеку, ремонтопридатність, технологічність і т. ін., що дозволяє оптимізувати конструкцію з урахуванням різних фізичних властивостей.

Ще однією перевагою 3D-моделей є можливість передавати їх в системи підготовки виробництва, які автоматично створюють програми для верстатів з ЧПК.

Серйозною перевагою 3D-моделювання є також властивість асоціативності. Якщо змінити розмір однієї деталі в збірці, то відповідним чином зміняться розміри пов'язаних з нею елементів, причому ці зміни будуть відображені і усіх кресленнях і специфікаціях.

І нарешті, дуже важлива перевага 3D-моделювання полягає в можливості багаторазового використання спроектованої деталі або вузла для створення цілого сімейства аналогічних об'єктів.

У Autodesk Inventor створення виробу можна починати на будь-якому етапі процесу проектування. Якщо проектування починається з „чистого листа”, то спочатку створюється порожня збірка, яка послідовно заповнюється деталями. Якщо допрацьовується вже наявна збірка, нові деталі створюються „за місцем” - так, щоб вони були добре сполучені з вже наявними деталями. Ця методологія проектування дозволяє застосовувати будь-які стратегії проектування: знизу вгору, зверху вниз і вгору-вниз від середини.

У Autodesk Inventor також є можливість створення проектів. Проект представляє собою логічно організовану структуру даних про проектованої конструкції. До нього включаються файли моделі, креслення, схеми та примітки. Інформація про проект зберігається в файлах XML з розширенням .ipj.

Можна створити два типи проектів: для одного проект і проект сховища, якщо встановлена програма Autodesk ® Vault. Перші проекти призначені для роботи одного конструктора. Якщо на комп'ютері встановлений Autodesk Vault, Vault-проекти дозволяють організувати спільну

роботу декількох конструкторів над одним проектом. Система доповнюється дуже розширеною бібліотекою компонентів, яка включає стандартні деталі, елементи конструкцій деталей та складальних одиниць.

Розглянута САПР є однією з перспективних сучасних систем, містить дуже важливі можливості для зручної швидкої та якісної роботи конструкторів в галузі радіоелектроніки, мехатроніки, робототехніки, дозволяє уникнути грубих помилок у процесі проектування. Її впровадження у навчальний процес та застосування при виконанні конструкторських та технологічних курсових та дипломних проектів дозволить підвищити рівень підготовки майбутніх спеціалістів.

УДК 004.94
Фурманова Н.І.[1], Овчіннікова Н.І.[2], Романченко О.О.[3]
[1] канд. техн. наук, доц., доц. каф. ІТЕЗ НУ «Запорізька політехніка»
[2] голова ПЦК «Електроніка» ЗЕФК НУ «Запорізька політехніка»
[3] студ. гр. МЕТ 18 1/9 ЗЕФК НУ «Запорізька політехніка»

РОЗРОБКА СПРОЩЕНОЇ МОДЕЛІ АНІМОВАНОГО ОБ'ЄКТА ІЗ ЗАВДАННЯМ ТЕКСТУР

Історія 3D графіки починає свій шлях ще з 1960 року, коли в університеті Юти першу кафедру комп'ютерної графіки відкрили Айван Сазерленд і Девід Еванс. Сазерленд створив програму, яка була прообразом усіх сучасних 3D-редакторів.

У сучасних проектах для створення анімованих 3D моделей є певний пайплайн – це послідовність дій для створення моделей.

Робочий процес містить наступні кроки: створення базової геометрії, ретопологія, UV-розгортка, запікання нормалей, накладання текстур, ріггінг, анімація.

Створення моделі починається з етапу моделювання або скульптингу. Під час цього процесу дуже важливо дотримуватися певних правил, порушення яких у майбутньому може суттєво збільшити час виконання проекту. Наприклад, не повинно бути накладання геометрій, порушень топології тощо.

Наступний етап – ретопологія. Він потрубен для зменшення кількості полігонів на моделі для оптимізації її під ігровий движок. Також він робиться у випадку коли потрібно переробити топологію об'єкту – зробити її більш акуратною. Цей етап можна пропустити, якщо модель проста або якщо вона тільки для рендеру.

Після етапу ретопології йде етап UV-розгортки. Це необхідно для правильного накладання текстур на модель. Якщо модель проста – то можна обійтись і без неї, накладаючи текстури одразу на полігони.

Світло у комп'ютерній графіці - поняття цікаве, воно працює не зовсім за тими правилами, за якими працює в житті. Запікання – це процес переносу нормалей з highpoly моделі на lowpoly, після якої LP модель буде мати такий же вигляд, як и HP, але полігонів на ній буде значно менше.

Просто на сірого персонажа буде не дуже цікаво дивитись, тому його потрібно "розмалювати". Як вже зазначалося вище – для простої моделі текстури можна накладати одразу на полігони, але для складних моделей текстури накладаються на UV-розгортку. В залежності від обраного шейдеру світло буде по різному відображатись від матеріалів. Саме від шейдеру та його правильно налаштування залежить буде матеріал металом або шкірою.

Передостанній етап створення анімованої моделі – ріггінг. Від потрібен для об'єднання моделі і скелета, завдяки якому її буде можливо анімувати. Є два основних способи ріггінгу – якірний, під час якого певні частини моделі намертво прив'язують до певної кістки, і ваговий – прив'язка усієї моделі до усього скелету і визначення сили дії кожної окремої кістки на кожний окремий полігон.

Анімація - це останній етап. Якщо ріггінг був зроблений правильно – то анімація, як правило, проблем не викликає. Основним і найпопулярнішим способом анімації є анімація по кейфреймам – спеціальним точкам, між якими програма сама розраховує усі дії об'єкту.

Практично всі наведені етапи були використані для створення цієї моделі і її анімації.

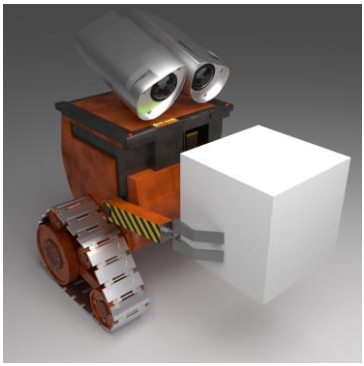


Рисунок 1 – Модель робота

Оскільки представлена модель досить проста, то для більшої її частини використовувався простий спосіб накладання текстур, але розгортку корпусу все ж довелося зробити для накладання на неї напису і індикатору заряду.

Анімація моделі також не зайняла багато часу, оскільки сам скелет був зроблений правильно і він доволі простий.

Дотримуючись цього пайплайну студії зі світовим ім'ям роблять величезні проекти. Це довгий, доволі клопітливий і строгий процес, але результат того коштує.

УДК 004.9
Палівода Д.С.[1], Фарафонов О.Ю.[2]
[1] студ. гр. РТ-618сп НУ «Запорізька політехніка»
[2] канд. техн. наук, доц., доц. каф. ІТЕЗ НУ «Запорізька політехніка»

МОДЕЛЮВАННЯ ВИПРОБУВАНЬ КВАДРОКОПТЕРІВ В СИСТЕМАХ CAD

Технології розвиваються досить швидко, і дозволяють побачити давно відомі речі під іншим кутом. Розвиток комп'ютерних технологій значно спростив процес розрахунків та проектування приладів та систем. За допомогою систем симуляції реальних об'єктів можна наглядно оцінити та побачити роботу того чи іншого приладу.

Задачею роботи було провести симуляцію випробувань тривимірної моделі безпілотного літаючого апарату типу квадрокоптер, використовуючи CAD-системи із графічним.

Для розробки був обраний Fusion 360. Рішення Fusion 360 полягає в використанні багатокомпонентної системи деталей, в якій компоненти збірки побудовані і зібрані в єдиний файл. На відміну від Solidworks, Fusion 360 не потрібно посилатися на кілька файлів при будівництві збірки.

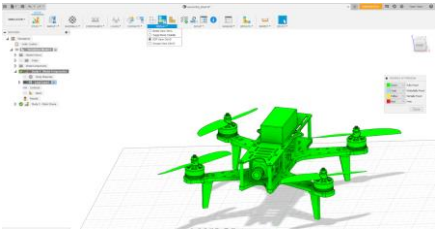


Рисунок 1 – Збірка квадракоптеру у Fusion 360

Fusion 360 пропонує безліч простих у використанні аналітичних пакетів, щоб зрозуміти, як деталь буде реагувати на зовнішні впливи. Ці пакети включають в себе: аналіз статичних напружень, термічний аналіз, вигин і оптимізацію форми. Таким чином, Fusion 360 відмінно підходить для базових і простих у використанні симуляцій, але в ньому відсутні деякі більш просунуті функції.

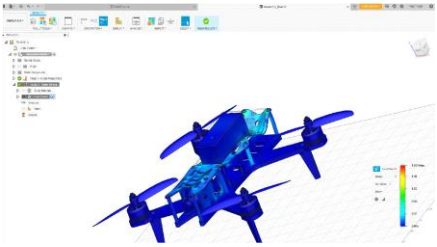


Рисунок 2 – Результат аналізу статичних напружень

У роботі були проведені аналіз статичних напружень та частотний аналіз. Перед початком будь-яких випробувань треба обирати закріплені площини у моделі. Для проведення статистичних напружень треба ще увімкнути режим гравітації та обрати поверхні на які прикладається саме навантаження і який саме тип навантаження. За результатами цього випробування видно, що є мінімальне навантаження на верхній частині корпусу та на центральних стійках між пластинами корпусу. Однак навіть така деформація не спричинить якісь критичні наслідки та закладена у норму.

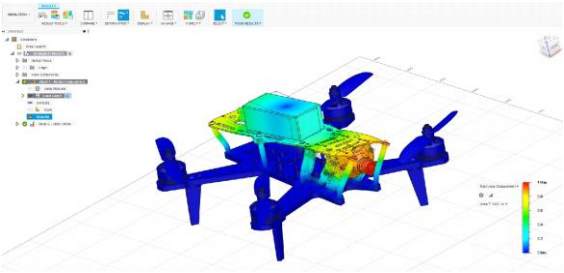


Рисунок 3 – Результат частотного аналізу

За результатами частотного аналізу визначив що під час коливань значні навантаження йдуть знов на верхню частину корпусу та на усі стійки. Максимум вібрацій припадає на камеру.

Висновками з обох симуляцій є те що усе навантаження припадає на верх квадрокоптеру та нерівномірно розподіляється по усьому корпусу.

Цього можна уникнути переробивши кріплення між частинами корпусу замінивши стійки. Для уникнення вібрацій на камері треба використовувати демпфер підвіску.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ГОСТ 23501.101-87 Системы автоматизированного проектирования. Основные положения [Текст]. – Введ. 01.07.1988. – М.: Издательство стандартов, 1988. – 10 с.

2. ГОСТ 2.052-2006. Единая система конструкторской документации. Электронная модель изделия. Общие положення [Текст]. – Введ. 01.09.2006. – М.: «Стандартинформ», 2007. – 12 с.

СЕКЦІЯ «ЗАХИСТ ІНФОРМАЦІЇ»

УДК 004.056
Лізунов С.І.[1], Філобок Є.В.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. РТ-810м НУ «Запорізька політехніка»

ВИКОРИСТАННЯ СИСТЕМ АКТИВНОГО ЗВУКОПРИДУШЕННЯ ДЛЯ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ

Однією з актуальних проблем захисту інформації є захист акустичної (мовної) інформації. Коливання, які виникають у огороджувальних конструкціях (стіни, вікна, перекриття, двері) при веденні розмови, являють собою акустичний канал витоку інформації. Задля усунення витоку інформації, застосовують або звукоізоляцію (пасивний метод захисту), або генератори акустичного шуму (активний метод).

У сфері захисту інформації задля запобігання розповсюдження мовної інформації у приміщеннях, тобто створення акустичної захищеності, можна використовувати технологію активного звукопридушення (шумопридушення). Така система складається з: електронного блоку управління, мікрофонів і аудіосистеми з динаміками (рис. 1).

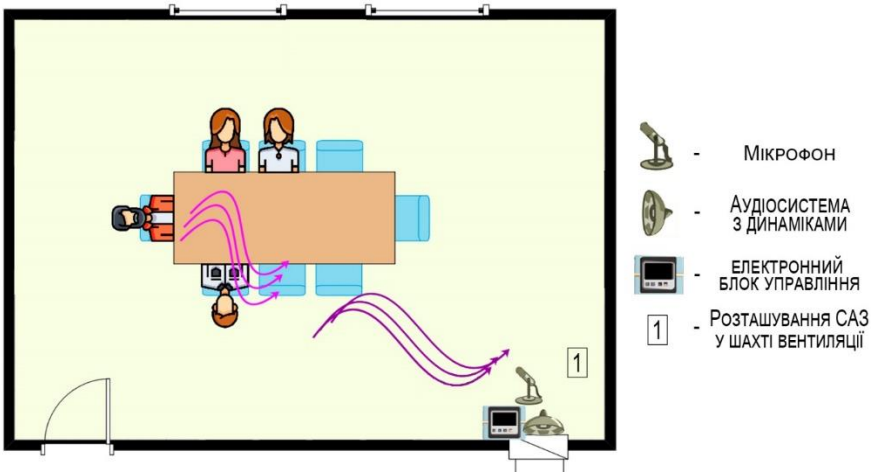


Рисунок 1 – Застосування системи активного звукопридушення під час переговорів

Сутність її полягає у аналізі вхідних звукових сигналів та генеруванні таких самих сигналів зі збереженням амплітуди, але зміною фази на 180

градусів. У процесі такої інтерференції хвиль, відбувається взаємне зменшення результуючої амплітуди, іншими словами, хвилі гасять одна одну [1]. Але такі системи не є ідеальними, тому що блоку обробки потрібен час для формування і генерації сигнала придушення. За рахунок цього будуть виникати затримки, які призведуть до того, що сигнали вже не будуть строго протифазними, що порушує принцип активного звукопридушення [2]. Як правило, такі системи ефективно працюють з частотами сигналу до 1 кГц, що замало для повного придушення мовної інформації [3].

Задля часткового вирішення цієї проблеми пропонується установка додаткового мікрофона (мікрофонів), безпосередньо біля джерел звуку. Їх підключення відбувається за допомогою екранованого кабелю, для того, щоб унеможливити можливість витоку інформації (рис. 2).

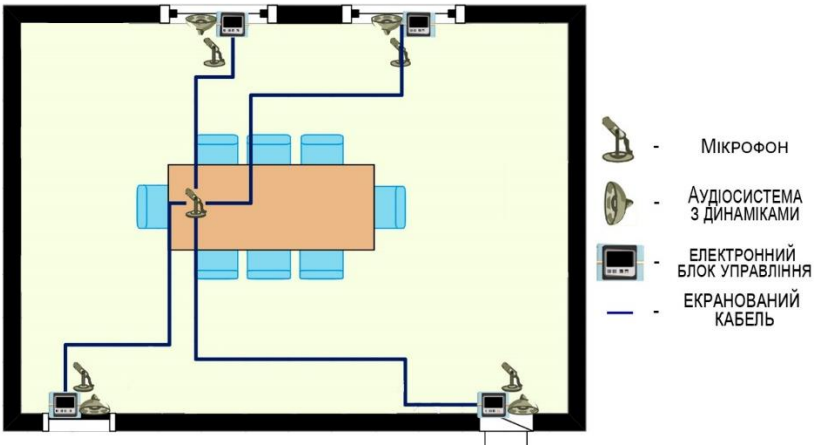


Рисунок 2 – Схема системи активного звукопридушення з підвищеною синхронізацією

Швидкість поширення звукових хвиль у просторі набагато менше, ніж швидкість електричного сигналу, переданого від мікрофона до електронного блоку. Тобто виходить, що система працює на «випередження». Електронний блок заздалегідь отримує сигнал від мікрофона і має додатковий час на створення образу сигналу у протифазі, а після надходження звуку на мікрофон, який стоїть біля вразливого місця, система починає створювати кінцевий сигнал порівнюючи обидва отриманих сигнали. При цьому буде суттєво зменшена затримка в обробці сигналу, тому що система вже «знає» більшу частину відомостей про сигнал, їй залишається лише порівняти з другим сигналом і упевниться, що вони ідентичні. У більшості випадків цього достатньо для того, щоб на виході блоку ми завжди отримували

потрібний сигнал придушення. При такому рішенні цієї задачі значно підвищується швидкодія системи. Вона здатна пригнічувати сигнали з частотами до 4 кГц, що в більшості випадків цілком задовільно.

Використання на практиці розробленої системи, може суттєво допомогти у проведенні безпечних переговорів та приховати сам факт перемовин в даному місці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Как работает система шумоподавления в современных наушниках. [Електронний ресурс]. – Режим доступу: https://www.iphones.ru/iNotes/697768

2. Основы ЦОС. Активное шумоподавление. [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=2JgoeuM7iVM

3. Активная система шумоподавления для «чайников» [Електронний ресурс]. – Режим доступу: http://android.mobile-review.com/articles/50408/

УДК 004.056.55

Антонюк М.А.[1], Неласа Г.В.[2]
[1] асп. НУ «Запорізька політехніка»
[2] канд. техн. наук, проф. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ РЕАЛІЗАЦІЇ МАЛОРЕСУРСНОЇ КРИПТОГРАФІЇ

Актуальні питання світу із впровадження технологій, що допоможуть людству постають дуже гостро у час карантинних заходів. Створюється величезна купа пристроїв для виявлення та діагностування стану людей, для моніторингу поточного стану.

Сучасний світ крокує до повної діджиталізації. Цифрові пристрої займають місце цифрового помічника людини полегшуючи та покращуючи його життя. Загалом покращення виникають у момент об’єднання великої кількості розумних пристроїв у єдину систему. На жаль, «інтернет речей» це не лише красива назва, а й повноцінна мережа, де пристрої обмінюються службовою та досить конфіденційною інформацією. «Інтернет речей» диктує свої правила розвитку та поширення пристроїв [1]. Критично важливі дані необхідно захищати, так як це загроза кіберпростору. На жаль, наразі, у більшості пристроїв такої категорії не впроваджено жодного захисту. Зазвичай, всі данні передаються у відкритій формі і єдиний захист, який ці пристрої можуть використовувати – закладений у протоколах передачі даних. На жаль, цього недостатньо. Захист кіберпростору не обмежується лише захистом конфіденційності інформації.

Натомість не важливо від яких типів атак захищатися: починаючи зі збереження конфіденційності, цілісності інформації і закінчуючи порушенням доступу до інформаційних ресурсів. Останній тип нападу може виникати частіше, через поширеність та доступність смарт-пристроїв, так як на них можуть перекладатися деякі функції по ідентифікації користувачів. Наприклад, NFC-чіп у смарт-годиннику, як ключ до дверей з NFC-зчитувачем.

Більшість смарт-пристроїв незалежно від їх розміру мають власний захист, але це не відноситься до більшості гаджетів, які входять в категорію "Інтернет речей" (як вже було вказану у прикладі, смарт-годинник), адже у більшості випадків навіть не виникає думки, що якусь шкоду можливо завдати реалізуючи атаку на ці пристрої, або використовувати ці пристрої для обхідної атаки на пристрої с захистом.

Рішення – використовувати криптографію. "Хмари", сервера, що їх підтримують, мережі, персональні комп'ютери, кишенькові смарт-пристрої – це такі гіганти, на яких вже реалізовані і використовуються алгоритми криптографічного захисту. Оскільки обчислювальна потужність з роками зростала, технологія шифрування стала лише вдосконаленою та безпечнішою. Однак цей прогрес у технології також виявив потенційні обмеження малоресурсних сучасних методів шифрування.

Довжина ключа шифрування є показником сили методу шифрування. Наприклад, оригінальний ключ шифрування DES (Data Encryption Standard) складав 56 біт, тобто він мав 2^56 можливостей комбінування. Завдяки сучасній обчислювальній потужності 56-розрядний ключ перестав бути захищеним, оскільки він вразливий до злому атакою грубої сили. Сьогодні стандарт сучасних ключів шифрування становить до 4096 бітів у системі RSA. Дешифрування 4096-бітового ключа шифрування практично неможливо з огляду на кількість можливих комбінацій. Однак квантові обчислення загрожують змінити цю безпечну природу.

Квантові обчислення використовують властивості квантової механіки для одночасної обробки великих обсягів даних. Встановлено, що квантові обчислення досягають обчислювальної швидкості в тисячі разів швидше, ніж сучасні суперкомп'ютери. Ця обчислювальна потужність є викликом сучасній технології шифрування. Наприклад, шифрування RSA використовує множення дуже великих простих чисел, щоб створити просте число для його відкритого ключа. Для декодування цього ключа без його приватного ключа потрібно врахувати це просте число, що може зайняти дуже багато часу на сучасних комп'ютерах. Суперкомп'ютеру знадобиться десь від тижня до місяця, щоб врахувати цей ключ.

Звичайно, варто враховувати обмеження, які накладаються від можливостей апаратного та програмного забезпечення смарт пристроїв.

Згідно з результатами досліджень, які проводив NIST (National Institute of Standards and Technology), з порівняння розмірів ключів RSA і ECC, необхідних для отримання однакового рівня захисту, еліптична криптографія може використовувати ключи довжиною у 160 біт аби забезпечити стійкість в 2048 біт RSA або 521 біт щоб забезпечити стійкість в 4096 біт RSA.

Останнім часом набирають популярності квантові комп'ютери. Квантові обчислення можуть використовувати квантові алгоритми для факторизації простого числа RSA за той самий проміжок часу, який потрібен звичайним комп'ютерам для його генерації. Це зробить усі дані, захищені поточним шифруванням із відкритим ключем, вразливими до атак квантових обчислень.

Інші методи шифрування так само вразливі для квантових обчислень. Хоча такі обчислення можуть загрожувати безпеці шифрування в майбутньому, вони у тому вигляді, як зараз існують, все ще дуже обмежені. На даний момент квантові обчислення не є комерційно доступними, не можуть обробляти великі обсяги коду і існують лише як обчислювальні пристрої, а не як комп'ютери. Крім того, квантові обчислення можна буде використовувати на користь шифрування. Так готуються стандарти пост-квантового шифрування на майбутнє.

Саме тому ще є певні причини зі створення можливостей, які дозволять прискорювати виконання вже існуючих алгоритмів. Не лише самі алгоритми можна оптимізувати, але й також оптимізувати виконання необхідної арифметики. Для більш наглядного прикладу необхідно виконувати дослідження на достатньо низькому рівні. А тому мета роботи - дослідити можливості еліптичної криптографії на пристроях з обмеженим об'ємом пам'яті.

Для реалізації авторами було обрано мікроконтролер Arduino. Arduino виступає у ролі найпростішого скалярного процесу, що обробляє один елемент даних за одну інструкцію. На мікроконтролері було реалізовано арифметику еліптичних кривих над простим полем Галуа: додавання точок і множення точки на число. Ця арифметика є базовою для генерації ключів, формування та верифікації електронного цифрового підпису. Мікроконтролер використовується для дослідження швидкості різних типів систем координат: афінна, стандартна проективна, система Якобі, система Чудновського-Якобі та змішанні системі Якобі.

Дослідження, що проводяться авторами, в змозі дати відповідь на питання, яка система найшвидша і має більший потенціал з впровадження в системи захисту для смарт-пристроїв. Економія апаратного часу з розрахунку базової арифметики дає зріст швидкодії смарт-пристрою із захистом і буде корисна не лише для пристроїв "Інтернету речей".

Авторами проведено аналіз математичних основ теорії скінченних полів та реалізація логіки мікроконтролеру на основі розглянутих алгоритмів з використанням мови програмування Arduino.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Жуков А. Е. Легковесная криптография [Текст] /А. Е. Жуков // Вопросы кибербезопасности. – 2015. – №1(9). – С. 26–43.

УДК 004.77
Семерюк Т.М.[1], Неласа Г.В.[2]
[1] асп. НУ «Запорізька політехніка»
[2] канд. техн. наук, проф. НУ «Запорізька політехніка»

УПРАВЛІННЯ РИЗИК-ОБ'ЄКТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Темпи розвитку сфери інформаційних технологій зумовлюють необхідність прояву пильної уваги до питань забезпечення інформаційної безпеки, а також відповідності її стану швидких змін в технологіях, зменшення вірогідності реалізації ризиків, пов'язаних з інформаційними загрозами. Метою управління ризиками інформаційної безпеки є підтримування їх на прийнятному для організації рівні. Для вирішення поставленої задачі створюються комплексні системи інформаційної безпеки. При створенні таких систем постає питання вибору засобів захисту, які забезпечують зниження, виявлених в процесі аналізу, ризиків інформаційної безпеки без надмірних витрат на впровадження і підтримку цих засобів. Аналіз ризиків інформаційної безпеки дозволяє визначити необхідну і достатню сукупність засобів захисту інформації, а також організаційних заходів, спрямованих на зниження ризиків інформаційної безпеки, і розробити архітектуру системи інформаційної безпеки організації, яка буде максимально ефективна для її діяльності і спрямована на зниження її ризиків інформаційної безпеки.

Ризик інформаційної безпеки є потенційна можливість використання вразливостей засобів конкретної загрози для заподіяння шкоди об'єкту.

Існує також умовна класифікація ризиків: за джерелом ризику (наприклад: хакерські атаки, фінансові помилки, вплив державних регуляторів, юридичні претензії контрагентів, негативний інформаційний вплив конкурентів); по цілі (інформаційні засоби, матеріальні ресурси, репутація); за тривалістю впливу (операційні, тактичні, стратегічні).

Методики і рекомендації базуються на двох основних підходах до подання оцінок інформаційних ризиків: якісному і кількісному. Завданням

якісної оцінки є визначення можливих видів ризиків, оцінка принципового рівня серйозності загроз, а також виділення факторів, що впливають на рівень обґрунтування різних можливих контрзаходів.

Кількісні методики надають реальні і осмислені чисельні значення всім елементам процесу аналізу ризиків. Кількісний аналіз дозволяє отримати конкретне значення ймовірності реалізації загрози. Кожен елемент в процесі аналізу вводиться в кількісному вигляді в рівняння для визначення загального і залишкового ризику. Якщо застосовуються якісні методи, можливі ризики порушення інформаційної безпеки повинні бути впорядковані за ступенем їх небезпеки з урахуванням факторів, як рівень загрози і вразливості. Ризики можуть бути оцінені за допомогою кількісних шкал. Це дасть можливість спростити аналіз існуючих загроз в інформаційних системах і вибір заходів захисту. Однак в цьому випадку пред'являються більш високі вимоги до шкал вимірювання вихідних даних. Наявність декількох загроз (вразливостей) характеризується відповідними частковими ризиками, сукупний вплив яких описується певним інтегральним ризиком, оцінювання якого в загальному випадку може бути досить складним [1]. Методики управління ризиками, розроблені за рекомендаціями стандартів, найчастіше спираються на перебірний підхід: розглядається кілька можливих варіантів побудови засобів захисту інформації, в яких рівні ризиків (інтегрального ризику) зменшуються до прийнятних значень. Перевагою якісного підходу є його простота, мінімізація термінів і трудовитрат на проведення оцінки ризиків. Перевагою кількісного підходу є точність оцінки ризиків, наочність результатів, недоліками - складність, висока трудомісткість і тривалість виконання.

Конкретні вимоги до заходів об'єктового захисту визначаються за результатами спеціальних досліджень технічних засобів з урахуванням встановленої категорії об'єкта, що захищається, в залежності від ступеня конфіденційності оброблюваної інформації і умов розміщення. Різні атаки вимагають різних технологічних рішень по забезпеченню інформаційної безпеки об'єктів атак. Оскільки кількість атак і їх модифікацій обчислюється більш, ніж п'ятизначним числом, то розробляються різні класифікації підходів забезпечення інформаційної безпеки, що охоплюють групи атак. При захисті конкретного об'єкта атаки від ризику кожна з функцій безпеки може бути модифікована. Наприклад, можна змінити алгоритм шифрування, змінити налаштування брандмауера, застосувати новий правовий акт і т.і.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Nazarov A.N., Nguyen Xuan Tien, Tran Minh Hai. Modeling of information attacks, and security risk assessment facilities. T-Comm. 2016.Vol. 10. No.8, pp. 69-78.

УДК 621.391.63
Карпуков Л.М.[1], Щекотихін О.В.[2]
[1]д-р техн. наук, проф. НУ «Запорізька політехніка»
[2]канд. техн. наук, доц. НУ «Запорізька політехніка»

ВТРАТИ ПОТУЖНОСТІ НА СТИКУ ОПТОВОЛОКОН З РАДІАЛЬНИМ ЗСУВОМ

Розглядаються втрати оптичної потужності на неоднорідності (див. рис. 1), що виникає при радіальному зміщенні оптичних оптоволокон, які з'єднаються.

Нехай в перетині $z = 0$ на торець слабконаправляючого оптоволокна 2 уздовж його осі падає потік потужності з волокна 1. Радіуси оптоволокон однакові і рівні a, їх центри зміщені уздовж осі x на величину d.

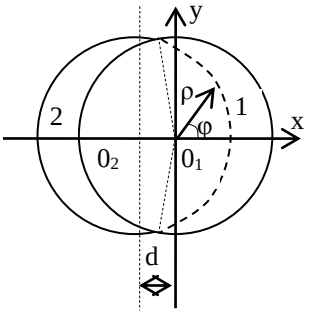


Рисунок 1 – Стик оптоволокон з радіальним зсувом

В полярній системі координат площа загальної поверхні S_2 між волокнами:

$$S_2 = \pi a^2 - \int\limits_{-\frac{\pi}{2}-\varphi_0}^{\frac{\pi}{2}+\varphi_0} \int\limits_{\rho(\varphi,d)}^{a} \rho d\rho d\varphi = a^2 \left(\pi - 2\varphi_0 - \frac{d}{2a}\sqrt{1-\left(\frac{d}{2a}\right)^2} \right), \qquad (1)$$

де $\varphi_0 = \arcsin\left(\frac{d}{2a}\right)$, $\rho(\varphi,d) = a\left(\sqrt{1-\left(\frac{d}{a}\sin\varphi\right)^2} - \frac{d}{a}\cos\varphi\right)$, $\varphi_0 = \arcsin\left(\frac{d}{2a}\right)$.

У наближенні Френеля [1] втрати потужності будуть визначатися відношенням площ S_2 и $S_1 = \pi a^2$:

$$\alpha_f = -10\lg\left[1-\frac{2}{\pi}\left(\arcsin\frac{d}{2a}+\frac{d}{2a}\sqrt{1-\left(\frac{d}{2a}\right)^2}\right)\right]. \qquad (2)$$

Більш суворий аналіз процесів на неоднорідностях забезпечує загальна теорія збудження мод [2].

Будемо вважати, що оптоволокно збуджується тільки тією частиною однорідного пучка світла потужністю $P_s = n_1\pi a^2/(2Z_0)$, яка безпосередньо потрапляє на торець серцевини оптоволокна 2. У цьому наближенні втрати потужності основної моди, що збуджується, буде визначатися таким чином:

$$\alpha_v = -10\lg\left[\frac{1}{\pi^2 a^4}\frac{\left(S_0 - S_1(d)\right)^2}{D}\right], \qquad (3)$$

де $D = \frac{J_1(\bar{\chi}_1)^2}{J_0(\bar{\chi}_1)^2}+\frac{K_1(\bar{\chi}_2)^2}{K_0(\bar{\chi}_2)^2}$, $S_\rho(d) = 2\int_0^{\varphi_0}\int_{\rho(\varphi,d)}^{a}\frac{J_0(\bar{\chi}_1\rho/a)}{J_0(\bar{\chi}_1)}\rho d\rho d\varphi$,

$$S_0 = \int_0^{2\pi}\int_0^{a}\frac{J_0(\bar{\chi}_1\rho/a)}{J_0(\bar{\chi}_1)}\rho d\rho d\varphi = 2\pi a\frac{J_1(\bar{\chi}_1)}{\bar{\chi}_1 J_0(\bar{\chi}_1)}.$$

$\bar{\chi}_1$ - характеристичний параметр серцевини волокна, $\bar{\chi}_2$ - характеристичний параметр оболонки світловоду, J_m - функція Бесселя m-го порядку, K_m - функція Кельвіна m-го порядку.

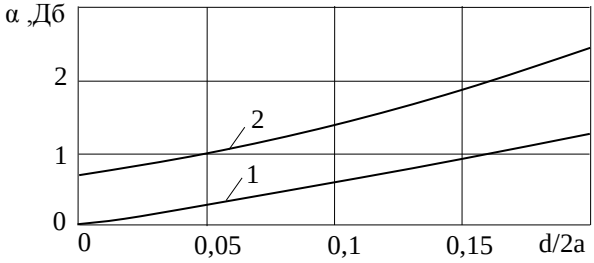


Рисунок 2 - Втрати потужності на неоднорідності

На рисунку 2 приведені графіки втрат α_f (крива 1) і α_v (крива 2). У α_v враховані додаткові втрати, які пов'язані з збудженням основної моди однорідним пучком світла.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гладких В.А. Френелевские потери энергии в волоконно-оптических линиях связи /В.А. Гладких, И.А. Кривошеев, Т.В. Кожевникова // Вестник ТСГУ «Машиностроение и приборостроение» - 2011, №4 (23), с.89-96.

2. Снайдер А. Теория оптических волноводов: Пер. с англ. Под ред. Е.М. Дианова, В.В. Шевченко. / Снайдер А., Лав Дж. // – М.: Радио и связь, 1987. – 656 с.

УДК 330.47

Каткова Т.І.[1], Карпуков Л.М.[2], Воскобойник В.О.[3]

[1] студ. гр. РТз-810м НУ «Запорізька політехніка»

[2] д-р техн. наук, проф. НУ «Запорізька політехніка»

[3] канд. техн. наук, проф. НУ «Запорізька політехніка»

ЕКОНОМІЧНА БЕЗПЕКА ЯК СКЛАДОВА КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Для сьогоднішнього стану економіки України як самостійної незалежної держави, утвердження її як суб'єкта світового співтовариства найбільше актуальними є проблеми забезпечення стійкого соціально-економічного розвитку, формування механізму протидії внутрішнім та зовнішнім загрозам, розвитку системи міжнародної економічної взаємозалежності. Сукупність цих проблем та послідовність їх вирішення тісно пов'язані з категорією «безпека», а отже і з національною безпекою держави загалом.

На сьогодні сучасними науковцями досліджено та законодавством запроваджено поняття «національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [1].

Українське законодавство розглядає національну безпеку, як захищеність життєве важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у політичній, економічній, соціальній, екологічній, науково – технологічній, інформаційній, воєнній сфері та інших сферах при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам [2, с. 130 – 131].

Постійні зміни внутрішніх та зовнішніх чинників розвитку національної економіки актуалізує дослідження питання забезпечення економічної безпеки держави.

В своїх дослідженнях В.М. Малишкона наголошує, що у системі національної безпеки економічна безпека здійснює визначені функції, тобто несе суттєве функціональне навантаження. Її суть полягає у тому, що вона є матеріальним підґрунтям національної суверенності, що формулює реальні можливості в забезпеченні інших видів безпеки. Тобто економічна безпека – це основа для функціонування всіх інших її елементів, що входять у цю систему [1].

У зарубіжній та вітчизняній літературі існує багато підходів до тлумачення поняття економічної безпеки держави за допомогою таких характеристик [4, с. 40 - 41]:

• стійкість та стабільність, протидія внутрішнім і зовнішнім загрозам, під якими розуміємо міцність і надійність зв'язків між усіма елементами економічної системи, стабільність економічного розвитку держави, стійкість до стримування та знешкодження дестабілізуючих загроз факторів;

• економічна незалежність, що характеризує насамперед можливість для будь-якого суб'єкта економічної безпеки самостійно приймати і реалізовувати стратегічні економічні та політичні рішення для розвитку, можливість використовувати національні конкурентні переваги для забезпечення стабільності та розвитку;

• самовідтворення та саморозвиток. Ця характеристика передбачає створення необхідних умов для ведення ефективної економічної політики та розширеного самовідтворення, забезпечення конкурентоспроможності національної економіки на світовій арені;

• національні інтереси. Ця характеристика визначає спроможність національної економіки захищати національні економічні інтереси.

Національні економічні інтереси лягають в основу економічної політики, що проводиться державою, важливою складовою частиною якої є забезпечення економічної безпеки, однієї з найважливіших функцій держави. Це гарантія незалежності країни, умова стабільності й ефективної життєдіяльності суспільства.

Тому, враховуючи дослідження науковців можна зробити висновок, що національної безпеки буде неповною без всебічної оцінки економіки, її міцності, надійності враховуючи наявність реальних і потенційних зовнішніх та внутрішніх загроз. А отже, економіка є однією з життєве вагомих напрямів діяльності особистості, суспільства і держави, а забезпечення економічної безпеки припадає до найважливіших національних пріоритетів у боротьбі з правопорушеннями.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про національну безпеку України» 2469-VIII від 21.06.2018 р.

2. Малишко В.М. Актуальні проблеми економічної безпеки в системі національної безпеки України. Юридичний вісник. Повітряне і космічне право. 2015. № 4. с. 129 - 133.

3. Про основи національної безпеки Закон України - режим доступу: http:// zakon2.rada.gov.ua/laws/ show/96415.

4. Скорук О.В. Економічна безпека держави: сутність, складові елементита проблеми забезпечення. Науковий вісник Ужгородського національного університету: Сер.: Міжнародні економічні відносини та світове господарство. Ужгород. 2016. Вип. 6. Ч. 3. с. 39 - 42.

УДК 004.056.53

Савченко Ю.В.[1], Стелюк Б.Б.[1], Воскобойник В.О.[2]

[1] студ. гр. РТз-810м НУ «Запорізька політехніка»

[2] канд. техн. наук, проф. НУ «Запорізька політехніка»

ФІНАНСОВІ ПИТАННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ СВІТОВОЇ ЕКОНОМІКИ

Інвестиційний інтерес до криптовалют залишається ще недостатньо високим, щоб зробити значимий вплив на світову економіку, але у майбутньому ситуація може змінитися, і криптоекономіка зробить свій внесок у розвиток глобальної економіки. Технологія блокчейн може зіграти важливу роль у процесі підвищення відкритості та результативності світової фінансової системи і економіки загалом.

Криптовалюта (від англ. Cryptocurrency) – вид цифрової валюти, емісія та облік якої засновані на асиметричному шифруванні і застосуванні різних криптографічних методів захисту, таких як Proof-of-work та/або Proof-of-stake. Функціонування системи відбувається децентралізовано в розподіленій комп'ютерній мережі [1].

До липня 2013 року програмне забезпечення всіх криптовалют, крім XRP (Ripple), базувалося на відкритому вихідному коді системи Bitcoin. З липня 2013 року стали випускатися самостійно розроблені платформи, які крім криптовалюти підтримують різну крипто-інфраструктуру — біржову торгівлю, магазини, месенджери та інше. До таких криптоплатформ відносяться: BitShares, Mastercoin, Nxt; анонсуються й інші платформи. У криптовалюти за замовчуванням не передбачено примусове повернення платежів, однак є можливості угод за участю посередника, коли для

завершення або скасування угоди потрібна згода всіх трьох або довільних двох сторін, кошти не можуть бути примусово заморожені або вилучені без доступу до приватного ключа власника, однак учасники угоди можуть добровільно тимчасово взаємно блокувати свої кошти як заставу. Як правило, є верхня межа загального обсягу емісії. Однак у деяких криптовалют, таких як PPCoin, Novacoin, Sifcoin та інших відсутня фіксована верхня межа загального обсягу емісії і можлива як емісія за рахунок наявних накопичень, так і демісія шляхом обов'язкового знищення невеликої фіксованої суми в кожній транзакції. Всі існуючі на даний момент криптовалюти використовуються псевдонімне — всі транзакції публічні, але прив'язки до конкретної людини за замовчуванням немає, проте особу користувача може бути встановлено, якщо відома необхідна додаткова інформація[2]. Ведеться розробка Zerocoin, де планується замінити псевдоанонімність на анонімність [3].

Криптовалюти, як новітні електронні засоби платежу, на сьогодні не мають свого законодавчого закріплення в Україні, а відтак – і нормативного визначення [4, 5]. Є загальне розуміння, що криптовалюти являють собою одиниці вартості, які зберігаються на електронних пристроях, використовуються як засоби платежу, а транзакції здійснюються за допомогою криптографії. У Верховній Раді України зареєстровано кілька законопроектів щодо обігу криптовалют, які демонструють різні підходи до правової кваліфікації цього інституту. Проект Закону України № 7183 «Про обіг криптовалюти в Україні» (далі – законопроект 7183) визначає криптовалюту як програмний код (набір символів, цифр та букв), що є об’єктом права власності, може виступати засобом міни, відомості про який вносяться та зберігаються у системі блокчейн в якості облікових одиниць поточної системи блокчейн у вигляді даних (програмного коду) [6]. Визначення криптовалюти у такий спосіб видається не дуже вдалим через зосередження на технічному аспекті, що відсуває на другий план економіко-правовий зміст поняття (з технічної точки зору категорія «програмний код» охоплює досить широке коло об’єктів, більшість з яких взагалі не пов’язані з криптовалютами, включаючи комп’ютерні програми, інформаційні бази даних тощо).

Альтернативний проект Закону України № 7183-1 «Про стимулювання ринку криптовалют та їх похідних в Україні» (далі – законопроект 7183-1) пропонує визначити криптовалюту як децентралізований цифровий вимір вартості, що може бути виражений у цифровому вигляді та функціонує як засіб обміну, збереження вартості або одиниця обліку, що заснований на математичних обчисленнях, є їх результатом та має криптографічний захист обліку.

Не вщухає дискусія серед науковців щодо правової природи криптовалют: їх визначають і як гроші, і як засоби обміну або розрахунку, відмінні від грошей, і як грошові сурогати, і навіть як товари. Дослідження питання, чи правомірне вважати криптовалюти різновидом грошей, видається доцільним почати з аналізу існуючих на даний час дефініцій грошей. Стаття 192 Цивільного кодексу (ЦК) України, хоч і називається «Гроші (грошові кошти)», жодних визначень не містить, зазначаючи лише, що законним платіжним засобом на території України є гривня, а іноземна валюта використовується у випадках і в порядку, встановлених законом. Згідно з Національним положенням (стандартом) бухгалтерського обліку «Загальні вимоги до фінансової звітності», затвердженим наказом Міністерства фінансів України від 07.02.2013 № 73 грошові кошти (гроші) – готівка, кошти на рахунках у банках та депозити до запитання. Але змісту поняття «гроші» ці норми не розкривають. Інші законодавчі акти також не містять визначення цього поняття, тож заповнювати прогалину.

Гроші є мірою вартості, загальним еквівалентом, універсальним засобом обміну. Ці характеристики чітко кореспондуються з функціями грошей. За теорією К. Маркса їх можна виділити п’ять [7]:

– міра вартості;
– обмін (обіг);
– засіб накопичення (утворення багатства);
– засіб платежу;
– світові гроші.

Сучасні економісти до зазначеного переліку додають інші функції: забезпечення функціонування держави; регулятора споживання; стимуляції науково-технічного прогресу тощо. Але те, що є характерним для сучасного суспільства, може бути абсолютно неприродним для суспільства стародавнього світу чи періоду середньовіччя. Тобто, певні функції грошей починають себе проявляти лише за певних умов, на певному етапі суспільного розвитку. На сучасному етапі гроші існують у матеріальній або нематеріальній формі.

Криптовалюти на сьогодні – не лише об’єктивна реальність, а й суттєвий економічний фактор. Як уже зазначалося, і в наукових колах, і на рівні урядів різних держав немає єдності щодо того, до якої категорії слід віднести криптовалюти.

Учасники саміту Великої двадцятки, який проходив у Буенос-Айресі 19–20 березня 2018 р., свідомо відійшли у своєму комюніке від використання терміну криптовалюта (crypto-currency), замінивши його на криптоактиви (crypto-assets), де прямо підкреслено: криптоактиви не мають ключових атрибутів суверенних валют. На думку учасників саміту, криптовалюта – це не валюта, а актив, тому вони використовують термін «криптоактив» як

більш коректний. Така позиція не є загальноприйнятою навіть усередині самих країн учасників двадцятки.

На урядовому рівні країни демонструють різні підходи до правової кваліфікації криптовалют. Усередині цих країн не припиняються дискусії, які часто призводять до різних тлумачень цього інституту відомствами однієї країни. У Сполучених Штатах Америки криптовалюти розглядаються одночасно як аналог грошей, як власність і як біржові товари, залежно від позиції тієї чи іншої інституції. Особливість США – прецедентна система права, яка дозволяє судам активно брати участь у законодавчому врегулюванні різних питань, не виключаючи й криптовалюти.

Проблему Bitcoin не обійшли увагою федеральні органи США. Голова Федеральної резервної системи (ФРС) США Джанет Йеллен озвучила офіційну позицію ФРС щодо криптовалют, заявивши, що криптовалюта жодним чином не пересікається з банківською сферою, а тому ФРС не має повноважень з її регулюванню. Федеральне бюро розслідувань у своїх офіційних звітах розглядає Bitcoin як віртуальну валюту. Подібна ж позиція й у Комісії з фінансових злочинів при Міністерстві фінансів США. Американська державна комісія, що завідує біржовими ф'ючерсами, прирівняла криптовалюти до біржових товарів. У грудні 2017 р. ця комісія офіційно дозволила розпочати торгівлю ф'ючерсами на Bitcoin. Голова комісії Крістофер Джанкарло зауважив, що Bitcoin є віртуальною валютою, товаром, з яким комісія ще жодного разу не стикалася.

В Європі підходи до криптовалют також не є чимось усталеним чи уніфікованим. Європейський центральний банк (ЄЦБ) використовує термін «віртуальні валюти», до яких відносить і Bitcoin. Віртуальну валюту ЄЦБ визначив як тип нерегульованих цифрових грошей, який видається і зазвичай контролюється його розробниками, використовується і приймається серед членів певного віртуального співтовариства.

Справжній прорив щодо офіційного визначення статусу криптовалют зробила Республіка Білорусь, президент якої 21 грудня 2017 р. підписав Декрет № 8 «Про розвиток цифрової економіки», яким легалізував обіг криптовалют на території країни. Згідно з пунктом 4 додатку № 1 до вказаного Декрету криптовалюта визначається як біткоін або інший цифровий знак (токен), що використовується у міжнародному обороті в якості універсального засобу обміну.

З викладеного випливає, що існує досить широкий спектр тлумачень поняття «криптовалюта» офіційними органами різних країн. В цій різноманітності вбачається певна закономірність: в тій чи іншій формі, але криптовалюти все ж таки визнаються засобами обміну, а у деяких випадках – навіть засобами платежу.

Поява криптовалюти стала можливою завдяки криптографії і принцип обігу криптовалют заснований на технології блокчейн, проте зазначені аспекти – технічна сторона питання. Криптографія – лише механізм, але не суть; механізм, який не має жодного відношення ані до правової природи, ані до юридичного статусу криптовалют. Криптографія досить давно почала використовуватися для шифрування інформації, і криптовалюти в цьому питанні лише побічний продукт. Та ж сама технологія блокчейн застосовується у багатьох інших сферах, наприклад, у державних реєстрах, приклад чого – Державний земельний кадастр України. Більше того, НБУ заявив про можливість емісії е-гривні, в основу якої буде покладена технологія блокчейн, причому цілком зрозуміло, що за термінологією обох вищеназваних законопроектів е-гривня не підпадатиме під ознаки криптовалюти, хоча б при її створенні і використовувалися криптографія та технологія блокчейн, оскільки однією з основних ознак криптовалют зразка Bitcoin є децентралізованість і відсутність єдиного емітента.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Карчева Г.Т. Віртуальні інноваційні валюти як валюти майбутнього / Г.Т. Карчева, С. М. Нікітчук. // Фінансовий простір. 2015. С. 24–30.

2. Вплив криптовалют на економіку. Pingblockchain.com Все про ринок криптовалюти, біт-койн, блокчейн, майнінг, торгівлю. URL: https://pingblockchain.com/vpliv-kriptovaljut-na-ekonomiku/

3. Melanie Swan. Blockchain: Blueprint for a New Economy. — 2015. — 152 p. — ISBN 978-1-4919-2047-3.

4. Проценко А. Т. Правове регулювання обігу електронних грошей в Україні: дис. канд. юрид. наук; 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право; Міжрегіональна акад. упр. персоналом. Київ, 2016. 202 с.

5. Про стимулювання ринку криптовалют та їх похідних в Україні : Проект Закону України від 10.10.2017 №7183-1.URL: http://w1.c1.rada.gov.ua/pls/zweb2/ webproc4_1?pf3511=62710.

6. Про обіг криптовалюти в Україні: Проект Закону України від 06.10.2017 № 7183. URL: http://w1.c1.rada.gov.ua/pls/zweb2/ webproc4_1?pf3511=62684.

7. Маркс К. Капітал. М.: Изд-во полит. лит., 1969. 907 с.

УДК 65.01:519.8:621
Паршина О.А.[1], Карпуков Л.М.[2,] Воскобойник В.О.[3]
[1] студ. гр. РТз-810м НУ «Запорізька політехніка»
[2] д-р техн. наук, проф. НУ «Запорізька політехніка»
[3] канд. техн. наук, проф. НУ «Запорізька політехніка»

ВИКОРИСТАННЯ НЕЙРОМЕРЕЖЕВИХ ТЕХНОЛОГІЙ ДЛЯ МОДЕЛЮВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

В сучасних умовах діджиталізації питання забезпечення інформаційної безпеки держави набувають суттєвої актуальності. З метою забезпечення надійного захисту та збереження інформаційних ресурсів, як на рівні підприємств, організації, так і на рівні окремих підрозділів використовуються комплексні системи захисту інформації.

Комплексна система захисту інформації поєднує сукупність органів та виконавців з використанням техніки та об'єктів захисту інформації, які функціонують у відповідності до встановлених правових, організаційно-розпорядчих і нормативних документів по захисту інформації. Враховуючи складність таких систем, вважаємо, що вирішення цілого комплексу завдань з напрямку забезпечення інформаційної безпеки потребують проведення досліджень структур та показників надійності захисту інформації.

Результати проведених досліджень дозволяють зазначити що, для ефективного вирішення теоретичних та практичних аспектів проблеми забезпечення високого рівня експлуатаційної надійності комплексних систем захисту інформації, необхідно проводити моніторинг та досліджувати складний процес їх функціонування. Можливим варіантом вирішення комплексу задач є побудова інформаційної моделі комплексної системи захисту інформації на основі синтезу її елементів. Відзначимо, що зручним базисом для представлення таких моделей вважаються штучні нейронні мережі [1, 2], які дозволяють сформувати високоефективну комплексну систему з паралельною обробкою інформації.

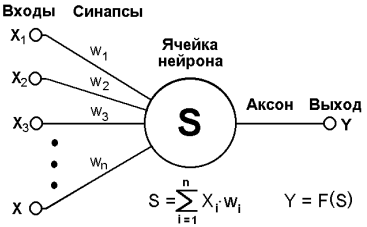


Рисунок 1 – Математична модель нейрону моделі системи захисту інформації

Нейронну мережу для моделювання комплексної системи захисту інформації формально визначимо, як сукупність простих процесорних елементів (нейронів), що володіють повністю локальним функціонуванням та які об'єднані зв'язками (синапсами) в одному напрямку.

Сформована в такий засіб нейронна мережа дозволить здійснити моделювання шляхом сприймання деякого вхідного сигналу із зовнішнього середовища з покроковим перетвореннями в кожному процесорному елементі. При цьому під сигналом у широкому значенні будемо розуміти вектор станів входів нейронної мережі.

У процесі проходження сигналу по зв'язкам мережі відбувається його обробка, результатом якої є певний вихідний сигнал. В укрупненому вигляді штучна нейрона мережа виконує функціональну відповідність між входом і виходом, і може служити інформаційною моделлю комплексної системи захисту інформації.

Представимо математичну модель нейрону системи захисту інформації. На рис. 1 у графічному вигляді показаний нейрон, який перетворює вхідні сигнали у вихідний сигнал.

Сигнали сили $x_1, x_2, ..., x_n$, які поступають до синапсів,

перетворюються лінійним чином, таким чином до тіла нейрону поступають сигнали сили $w_1*x_1, w_2*x_2, ..., w_n*x_n$ (де w_i – вага відповідних синапсів). В наслідок цього у тілі нейрону відбувається підсумовування сигналів:

$$S = \sum_{i=0}^{n} w_i * x_i \,, \tag{1}$$

де x_i – компонента вхідного вектора (вхідний сигнал); w_i – вага синапсу, $i = 1 \ldots n$; s – результат підсумовування.

Потім використовуємо до суми активаційну функцію, що дозволяє сформувати на виході сигнал сили:

$$Y = f(S). \tag{2}$$

де f – нелінійне перетворення (активаційна функція); Y – вихідний сигнал нейрона.

В якості активаційної функції було обрано одну з найпоширеніших функцій – нелінійну функцію активації з насиченням, так звану й відому логістичну функцію [2]:

$$f(s) = \frac{1}{1+e^{-s}} \cdot \tag{3}$$

За допомогою цієї функції здійснено стиснення вхідного параметра в діапазоні від 0 до 1.

Запропоновано структуру нейронної мережі для моделювання комплексної системи захисту інформації. Особистою рисою запропонованої

структури нейронної мережі є глобальність зв'язків, тому що її базові елементи спочатку націлені на роботу з широкосмуговою інформацією та кожний нейрон мережі пов'язаний з усіма нейронами попереднього шару обробки даних. Проведення досліджень з використанням нейромережевих технологій дозволяє сформувати підґрунтя для прийняття рішень із забезпечення відповідного рівня надійності комплексної системи захисту інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Галушкин А.И. Теория нейронных сетей. Кн.1: Учеб. пособие для вузов / Общая ред. А.И. Галушкина. М.: ИПРЖР, 2000. 416 с.

2. Круглов В.В., Борисов В.В. Искусственные нейронные сети. Теория и практика. 2-е изд., стереотип. М.: Горячая линия – Телеком, 2002. 382 с.

УДК 004.9

Воскобойник В.О.[1], Бєдняк О.Г.[2]
[1] канд. техн. наук, проф. НУ «Запорізька політехніка»
[2] старш. викл. НУ«Запорізька політехніка»

ТЕХНОЛОГІЇ 5G ТА ПИТАННЯ ЇХ ТЕСТУВАННЯ

Поява стільникових мереж четвертого покоління 4G LTE стало більшим стрибком уперед для миру мобільних даних завдяки підтримці передачі даних з високою пропускною здатністю, що забезпечує для користувачів повнофункціональний доступ в Інтернет на ходу.

У даний момент мережі 4G підтримують смугу пропущення до 20 МГц, а теоретична швидкість передачі даних технології LTE advanced може досягати одиниць Гбіт/сек.

Для підвищення пропускної здатності можуть застосовуватися різні нові технології, такі як модуляція за схемою 256 QAM, 4x4 MIMO з 10 просторовими потоками з використанням двох високочастотних несучих з 4 рівнями для кожної й 1 низькочастотної несучої з 2 рівнями; а також застосування агрегації декількох несучих або об'єднання декількох каналів зі смугою 20 Мгц.

На додаток до нових завдань тестування пропонується два шляхи розвитку нової технології 5G. Перший шлях – NR-5G (де NR позначає NewRadio). Цей шлях не буде мати зворотної сумісності.

Другий шлях – LTE-5G. Даний шлях має на увазі використання існуючої інфраструктури 4G у комбінації з додатковими поліпшенням технології LTE з метою підтримки майбутніх послуг мережі 5G. LTE-5G –

найбільш імовірний шлях, який буде обраний операторами, оскільки багато хто з них уже зробили значні інвестиції в побудову мереж четвертого покоління.

Ключовою вимогою для розгортання мереж 5G є доступність спектра, тому розглядаються як більш високі, так і низькі частоти, і багато операторів проводять активне тестування в цих діапазонах.

Пропоновані смуги частот 5G перебувають у смузі до 6 ГГц, а також у більш високому діапазоні частот до 100 ГГц. Ці смуги можуть становити особливий інтерес як для звичайних, так і для нових нетрадиційних завдань і є ключовими для забезпечення необхідного широкосмугового покриття мереж 5G для таких областей застосування, як Інтернет речей (Iot), промислової автоматизації й критично важливих бізнес-завдань.

Є проблеми втрат з розповсюдженням радіохвиль. Наявність операторів по усьому світу зараз проводять тестування в діапазонах частот із центральними частотами близько 28 ГГц і 39 ГГц. Використання даного СВЧ спектра пов'язане з новими специфічними проблемами, а саме, застосування СВЧ сигналів має на увазі вживання спеціальних заходів щодо мінімізації витрат в каналах передачі. Загасання вільного розповсюдження на відстані 5 метрів на частоті 28 ГГц становить 75 дБ, 78 дБ на частоті 39 ГГц і 82 дБ на частоті 60 ГГц.

Однією з складових каналів передачі та приймання інформації є час затримки. Новітні технології спрямовані на підвищення надійності в таких сферах. Це стосується питань забезпечення зв'язків системах для передачі особливо важливої інформації для поліції, пожежних, швидкої допомоги й інших служб оперативного реагування.

Зв'язок транспортного засобу з навколишнім середовищем (V2X) – ще одне завдання, яке вимагає надзвичайно надійної роботи мережі. Швидше за все безпілотні автомобілі стануть дійсно життєздатними на комерційній основі тільки, коли буде розгорнута інфраструктура мережі 5G.

Таким чином, слід зазначити, що захоплення та впровадження широкосмугових високочастотних сигналів систем зв'язку5G зі складними схемами формування діаграми спрямованості й поляризації потребують подальше вдосконалення.

Одним з питань вирішення цього є впровадження й застосування нового тестового обладнання. Не можливо вирішити ці проблеми без відповідної підготовки фахівців в цьому напрямку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Олейникова А.В. Перспективы развития связи 5G / Олейникова А.В., Нуртай М.Д., Шманов Н.М. // Современные материалы, техника и технологии. – 2015. –№ 2 (2). – С. 233- 235.

УДК 004.75:339.722
Ситник А.А.[1], Козіна Г.Л.[2]
[1] студ. гр. РТ-810м НУ «Запорізька політехніка»
[2] канд. фіз-мат. наук, доц. НУ «Запорізька політехніка»

СИСТЕМИ ЗАХИСТУ У КРИПТОВАЛЮТАХ СВІТУ

На сьогодні фінансовий ринок має багато різних криптовалют. Найпопулярнішими криптовалютами є Bitcoin, Ethereum, Litecoin, Monero, Dash. До цього списку можна занести першу криптовату, що була створена в Україні, це – Карбованець (Електронний карбованець). Електронний карбованець (Karbowanec – KRB) – криптовалюта, орієнтована на українського користувача. Вона була започаткована 30 травня 2016 року, оголошення про запуск проекту і початок майнінгу було розміщене на форумі Bitcointalk. Публічної інформації про розробників немає. Працює на технології CryptoNote.

Однією з технологій, що використається в криптовалютах, є блокчейн. Блокчейн (ланцюжок блоків) – розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків), що постійно довшає. Ці дані мають бути захищені від підробки та спотворення: кожен блок містить часову позначку, хеш попереднього блока та дані транзакцій, подані як хеш-дерево.

Існують різні механізми захисту криптовалют. Розглянемо деякі з них, що описані в [1-4].

Протокол доказу з нульовим розголошенням. Він дозволяє захистити інформацію про те, скільки грошей знаходиться на конкретному обліковому записі, блоці розподіленої бази даних. Щоб підтвердити, що транзакція обробляється правильно, необхідне лише повідомити про основні властивості записів, не називаючи конкретних цифр (протокол підтверджує наявність інформації, не розкриваючи її змісту). Так працює доказ з нульовим розголошенням. Використовується з 2014-2015 років.

Доказ виконання роботи. Доказ виконання роботи – Proof-of-work (PoW) є принципом захисту систем від зловживання послугами (наприклад, DoS-атак або розсилок спаму), заснованим на необхідності виконання стороною, яка робить запит (клієнтом), деякої досить складної тривалої роботи (POW-завдання, одностороння функція), результат якої легко і швидко перевіряється стороною, що обробляє запит (сервером). Головна особливість цих схем полягає в асиметрії витрат часу — тривалість для ініціатора запиту і висока швидкість для відповіді.

Підтвердження частки. Підтвердження частки – Proof-of-stake (PoS) є методом захисту в криптовалютах, заснованим на необхідності доказу зберігання певної кількості коштів на рахунку. При використанні цього

методу алгоритм криптовалюти з більшою ймовірністю вибере для підтвердження чергового блоку в ланцюжку обліковий запис з великою кількістю коштів на рахунку. Метод використовують як альтернативу методу Proof-of-work, в якому більшу ймовірність підтвердження блоку має обліковий запис з великими обчислювальними потужностями. Метод був запропонований в 2011.

Криптографічні цифрові підписи. Хоча криптовалютний фінансовий потік не передбачає контролю з боку центрального банку, транзакції теж потрібно підтверджувати цифровим підписом.

Криптографічні хеш-функції. Хеш-функція – це функція, що перетворює вхідні дані будь-якого (як правило великого) розміру в дані фіксованого розміру. У різних валютах використовуються різні хеш-функції (таблиці 1).

Таблиця 1 – Хеш-функції та методи захисту, що використовуються у криптовалютах

криптовалюта	хеш-функція	метод захисту
Bitcoin	SHA-256d	PoW
Litecoin	Scrypt	PoW
Monero	CryptoNight	PoW
Ethereum	Ethash	PoW

Гомоморфне шифрування. Для збереження анонімності можна застосовувати гомоморфне шифрування. Воно дозволяє виконувати з зашифрованими даними математичні операції, які відповідають результатам обчислень з оригінальними даними. Головне у всіх методах - забезпечити правильну синхронізацію інформації елементів системи. Інакше є ризик заплутатися: деякі комп'ютери будуть вважати, що у вас є певна сума криптовалюти, а інші не побачать грошей на рахунку.

Роботу технології розподілених реєстрів(блокчейну) підтримують майнери. Вони займаються підтвердженням транзакцій, генерацією нових блоків і додаванням їх в блокчейн. У мережах, заснованих на алгоритмі консенсусу PoW, для додавання нового блоку майнеру потрібно проводити складні обчислення, щоб довести виконання роботи.

Така важливість обчислювальних потужностей робить можливим проведенням атаки 51%. [5].

Її суть полягає в тому, що кілька майнерів зі значними обчислювальними потужностями (хешрейтом), можуть отримати «контрольний пакет» в мережі, тобто в них у наявності більше всього хешрейту. В результаті вони можуть створювати блоки на свій розсуд,

маніпулювати двосторонніми операціями, не підтверджувати транзакції - це відкриває можливість для багаторазових витрат одних і тих же грошей («подвійні витрати»).

У 2018 році жертвами такої атаки стали шість відомих криптовалютних проектів.

Проект Electroneum піддався атаці в квітні 2018 року. Цей альткоін був запущений на базі алгоритму CryptoNight. Після атаки розробникам вдалося підвищити рівень безпеки проекту.

Монета Bitcoin Gold була атакована двічі - в перший раз 16 травня 2018 року, а потім три дні потому. В результаті збиток перевищив $ 18 млн, а криптовалютні біржі почали виключати Bitcoin Gold з лістингу.

В кінці травня 2018 року під атакою виявилася мережа монети Litecoin Cash. При цьому розробникам вдалося досить швидко впоратися з цим завданням, що запобігло масштабні втрати.

На початку червня 2018 року жертвою атаки «51 відсоток» стала мережа ZenCash. Зловмиснику вдалося захопити контроль над мережею на кілька годин. В результаті йому вдалося двічі витратити криптовалюту на суму $ 30 000.

Зломщикам вдалося використати алгоритм Lyra2Re для атаки на мережу криптовалюти Verge. В результаті було викрадено близько $ 1,4 млн.

Популярна в Японії криптовалюта Monacoin була атакована в травні 2017 року. На момент атаки проект використовував алгоритм Lyra2Rev2. Зловмисникам вдалося його зламати, збиток від їх дій був оцінений в $ 90 000.

Хоча багато вдалих атак було проведено на різні криптовалюти, вони не втрачають свого попиту і залишаються популярними, як от біткойн.

Розглянемо безпеку цей найпопулярнішої криптовалюти світу [6].

Біткойн дозволяє досягти безпрецедентного рівня безпеки. Мережа захищає користувачів від найбільш поширених шахрайств, таких як повернення платежів або неавторизовані списання коштів, а біткойни неможливо підробити. Користувачі можуть створити резервну копію або зашифрувати свої гаманці, а пристрої для зберігання біткойнів можуть в майбутньому зробити крадіжку дуже малоймовірною.

Блокчейн (біткоіну) - це публічний запис всіх біткойн-транзакцій в хронологічному порядку. Ланцюжок блоків єдиний для всіх користувачів біткойнів. Блокчейн застосовує певний набір правил, для генерації нових блоків. Одне з правил полягає в тому, що здатність створювати блок, повинна бути пропорційна загальній обчислювальній потужності механізму PoW. Це означає, що вам фактично необхідно володіти своєю комп'ютерною потужністю, необхідною для створення нового блоку, що робить процес злому дуже складним і дорогим для зловмисника.

У квітні 2014 року Лабораторія Касперського повідомила про зростання вірусних атак, спрямованих на крадіжки біткойнів, в тому числі через крадіжку файлів з ключами (wallet.dat).

Для захисту від збоїв рекомендовано використовувати паперові та / або цифрові бекапи (з можливістю їх зашифрувати і / або зберігати кілька частин в різних місцях).

Для захисту від крадіжки рекомендовано «холодне зберігання» або апаратні засоби захисту. При цьому шифрування гаманця саме по собі не є надійним захистом від троянських програм, оскільки пароль може бути прочитаний через кейлоггер. Холодне зберігання полягає в зберіганні приватного ключа на комп'ютері, що не є підключеним до інтернету, і з можливістю здійснення операцій на комп'ютері, який має підключення до інтернету. Даний метод реалізований, наприклад в Bitcoin-клієнті *Armory*.

Отже, найпопулярнішою валютою вважається біткойн через постійну увагу та цікавість все більшої кількості людей. Система безпеки біткойн постійно оновлюється та вдосконалюється.

Однак гарантувати стовідсотковий захист навіть у біткоїні не можливо, в нього як і в інших криптовалютах, атакуючі знаходять слабкі місця, які можуть бути використані для атаки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Безопасность криптовалют [Електронний ресурс]. – Режим доступу: https://postnauka.ru/talks/81984

2. Доказ виконаної роботи [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Доказ_виконаної_роботи

3. Proof-of-stake [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Proof-of-stake

4. Список криптовалют [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Список_криптовалют

5. Как взламывают блокчейн и криптовалюты: 6 успешных атак «51 процента» [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/blog/company/pt/344915.php

6. Биткойн#Безопасность [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Биткойн#Безопасность

УДК 004.415.24:004.056.57
Бондаренко О.О.[1], Козіна Г.Л.[2]
[1] студ. гр. РТ-810м НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

ВИКОРИСТАННЯ СТЕГАНОГРАФІЇ В КІБЕРАТАКАХ

Стеганографія це спосіб передачі або зберігання інформації з урахуванням збереження в таємниці самого факту такої передачі. У даній роботі буде розглянуто використання стеганографії в зображенні. Тому варто також сказати, що стеганографія зображень – це приховування коду, можливо шкідливого, у звичайному зображенні.

Вперше поняття стеганографії було введено в 1499 році, але приховування інформації використовувалось ще до нашої ери. Наприклад в 240 році до нашої ери, китайський імператор Цин Шихуанді дуже полюбляв писати секретні листа [1]. Використовував він, для цього, густий рисовий відвар, який після висихання не залишав ніяких видимих слідів. Далі цей лист потрапляв в потрібні руки, і після змочування слабким спиртовим розчином йоду починали з'являтися написані раніше ієрогліфи.

Кібератака – це несанкціонована, шкідлива спроба людини або будь-якої нечесно налаштованої організації проникнути в інформаційну систему іншої людини або організації. Тобто кібератака – це масове зараження комп'ютерів вірусами. Як правило, зловмисники прагнуть отримати з цього вигоду. Яскравий приклад кібератаки стався у 2017 році, атака була націлена на Україну. Але через кілька годин вірус вирвався за її межі. Іменував він себе NotPetya. Потрапивши на один комп'ютер через оновлення M.E.Doc (українське програмне забезпечення для подання звітності до контролюючих органів), вірус отримував логін і пароль адміністратора і поширювався далі по локальній мережі. Можна сказати, що цей вірус покращив Україну в сфері кібербезпеки. Адже вже минуло більше трьох років, а нові, масштабні віруси більше не з'являлись. Але той факт, що з часів NotPetya в Україні не було жодної гучної атаки, не свідчить про те, що зловмисники припинили свою активність.

На сьогодні існує велика кількість різних алгоритмів і методів стеганографії. Основні з них це методи LSB та квантування; алгоритм Коха-Жао; метод, заснований на приховуванні даних в коефіцієнтах дискретного косинусного перетворення та метод приховування інформації в службових полях формату. Ці методи розглянуті у [2].

За останні 10 років стеганографія стала дуже часто використовуватися в різних шкідливих програмах і засобах кібершпіонажу. Нижче приведено список, який складається з десяти найбільш популярних вірусів, які в своїх неблагих цілях використовували стеганографію:

1) Duqu (2011);
2) KinS (2011);
3) Stegoloader (2012);
4) ZeusVM (2014);
5) Gatak (2015);
6) TeslaCrypt (2015);
7) NetTraveler (2016);
8) Cerber (2017);
9) Triton (Fibbit) (2017);
10) Microcin (SixLittleMonkeys) (2020).

Як ми бачимо віруси, які використовували стеганографію в поганих цілях, з'являлися майже щороку і це тільки популярні з них.

У даній роботі буде розказано про найперший вірус, який шифрував дані і приховував їх усередині графічних файлів "JPEG", які пізніше відправлялися на сервер управління. Даний вірус був спрямований на найбільші світові компанії. Його прозвали ім'ям Duqu. Про нього стало відомо 1 вересня 2011 року. Свого часу він торкнувся великої кількості країн (рисунок 1, [3]). Він містив дуже багато складних функцій, які могли бути розроблені тільки групою висококваліфікованих програмістів. Як вже було сказано раніше, ці функції включали стенографічні процеси, які шифрували вкрадені дані і вставляли їх в зображення перед тим, як відправити на сервери, контрольовані зловмисниками.

A – Франція, Нідерланди, Швейцарія, Україна; B – Індія; C – Іран; D – Іран; E – Судан; F – В'єтнам

Рисунок 1 – Географічне поширення

Щоб не вдаватися в подробиці його змісту, а там дуже багато інформації, яка не пов'язана з цією роботою, перейдемо відразу до використання стеганографії у вірусі Duqu. В даному вірусі є файл Infostealer

[3]. Цей автономний виконуваний файл був завантажений вірусом Duqu. Його основні функції виконуються бібліотекою DLL, що міститься у виконуваному файлі. Крім того DLL зберігається у вигляді зашифрованих даних у файлі JPEG. JPG – це перші 8192 байт зображення Хаббла (рисунок 2, [3]).

Існування цього зображення змусило деяких припустити, що Duqu може бути загрозою «зірок», оголошеної іранськими офіційними особами в квітні 2011 року, але здається, що розробникам даного вірусного програмного забезпечення просто подобалася астрономія.

При виконанні файл витягував зашифровану DLL зі збереженого в ній JPEG, а потім виконував експорт DLL. DLL крав дані і зберігав їх у файлі з довільним номером в папці %Temp% користувача, додаючи до файлів журналу ~ DQ (наприклад, ~ DQ7.tmp).

Цей DLL міг вкрасти: списки запущених процесів; дані облікового запису; назву дисків; скріншоти; мережеву інформацію; натискання клавіш; назви відкритих вікон. Також він міг переглядати файли на всіх дисках, включаючи знімні. Детальніше про DLL розписано у [3].

Рисунок 2 – Зображення Хаббла

Як бачимо все це було зроблено за допомогою однієї маленької картинки про космос. Існує три головних причини використання стеганографії авторами шкідливого програмного забезпечення в своїх розробках [2]:

стеганографія дозволяє приховати сам факт завантаження/вивантаження даних, а не тільки самі дані;

стеганографія допомагає обійти DPI-системи, що актуально в корпоративних мережах;

використання стеганографії може дозволити обійти перевірку в AntiAPT-продуктах, оскільки останні не можуть обробляти всі графічні файли.

Отже, після розгляду даної роботи можна зробити висновок, що використання стеганографії сьогодні дуже популярна ідея серед авторів шкідливого програмного забезпечення, тому потрібно обов'язково вміти з цим боротися.

Для цього існує безліч різних шляхів вирішення даної проблеми. Основне з них це постійне оновлення антивірусних програм. Хоч антивіруси і не врятують від вразливості нульового дня, але подальший стабільний захист комп'ютера вони забезпечити зможуть. Більш докладне рішення даної проблеми буде розглянуто авторами пізніше.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стеганография. История тайнописи [Електронний ресурс]. – Режим доступу: http://maxima-library.org/knigi/genre/b/451565?format=read

2. Стеганография в современных кибератаках [Електронний ресурс]. – Режим доступу: https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/

3. W32.Duqu. The precursor to the next Stuxnet. [Електронний ресурс]. – Режим доступу: https://scadahacker.com/files/duqu/w32_duqu-the-next-precursor-to_the_next_stuxnet_v1.4.pdf

УДК 004.9

Бондаренко О.О.[1], Філобок Є.В.[1], Неласа Г. В.[2]
[1] студ. гр. РТ-810м НУ «Запорізька політехніка»
[2] канд. техн. наук, проф. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ КВАНТОВИХ ОБЧИСЛЕНЬ НА ПРИКЛАДІ СЕРВІСІВ IBM QUANTUM EXPERIENCE ТА GOOGLE QUANTUM PLAYGROUND

Квантовий комп'ютер — обчислювальний пристрій, який використовує явища квантової суперпозиції і квантової заплутаності для передачі і обробки даних [1]. Його швидкодія у рази більше, ніж у звичайних комп'ютерів. Він використовує замість звичайних бітів – кубіти.

Цей напрям зараз є дуже популярним, тому багато компаній працюють над створенням своїх власних квантових комп'ютерів. У цій роботі піде розмова про квантові інструменти від Google та IBM.

Компанії IBM вдалося розробити 50-кубітовий комп'ютер. Задля популяризації теми квантових обчислень IBM розробила онлайн платформу-

симулятор IBM Quantum Experience[2,3], яка надає користувачам доступ до набору прототипів квантових процесорів IBM через хмару.

Симулятор IBM Quantum Experience (рис.1) представляє собою сайт, який містить три розділи: задачі, розділ для створення схем алгоритмів та розділ квантової лабораторії, що є середою для програмування на мові Qiskit. Завдяки розділу зі схемами, можливо вирішувати квантові задачі або тестувати алгоритми. На сайті можливо самостійно вибрати будь-яку потужність квантового комп'ютеру, з представлених. Після виконання задачі на екран виводиться ретельний звіт з виконаної роботи.

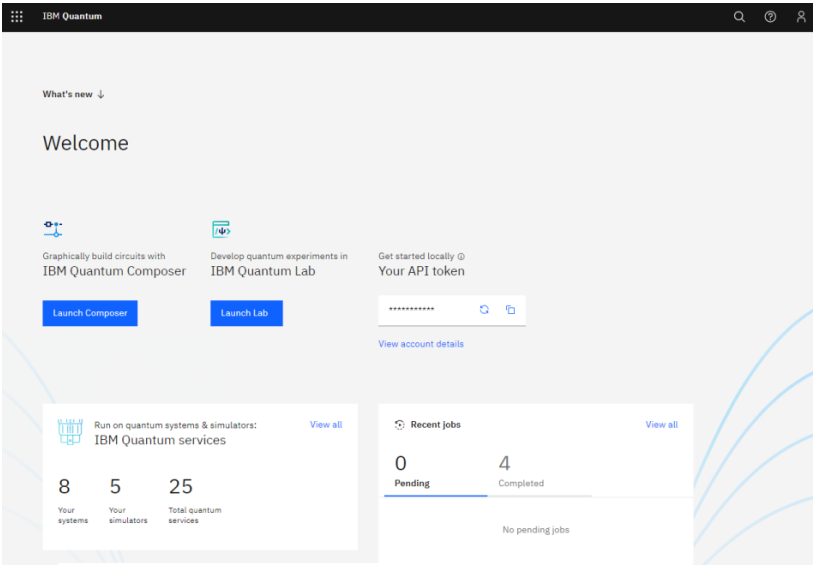


Рисунок 1 – Головна сторінка сайту IBM Quantum Experience

Далі піде розмова про популярну квантову пісочницю від Google під назвою Quantum Computing Playground[4,5]. На даний момент нереально просто купити собі квантовий комп'ютер. Але завдяки Google кожен користувач може перетворити свою "машину" в квантову. Мається на увазі лише моделювання роботи квантового комп'ютера на його молодшому побратимові, шляхом запуску веб-додатку для браузера.

Quantum Computing Playground (рис.2) — це веб-додаток Chrome, який використовує WebGL для імітації до 22 кубітів на графічному процесорі. Як ми бачимо комп'ютер від Google може моделювати квантові регістри тільки до 22 кубітів (на відміну від IBM Quantum Experience). Також за допомогою Quantum Computing Playground можна писати, компілювати і виконувати код.

Але найцікавіше це те, що він може візуалізувати квантові стани в 2D і 3D вигляді. Програми пишуться мовою QScript, яка схожа на будь-яку іншу просту Bash-подібну мову.

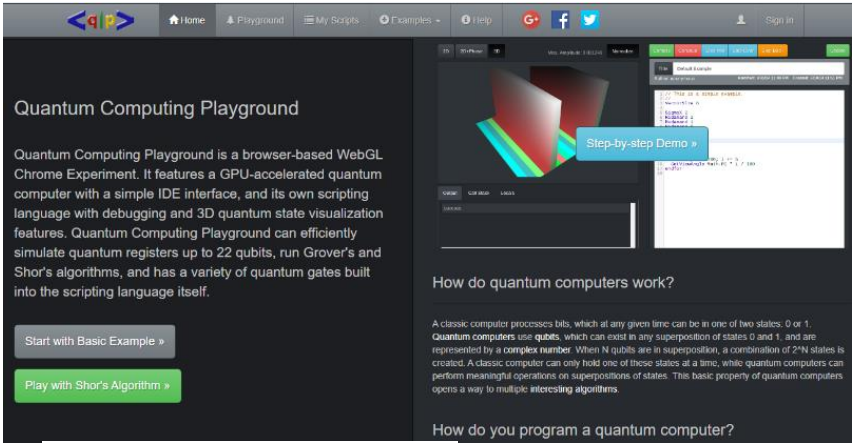


Рисунок 2 – Головна сторінка сайту Quantum Computing Playground

У даній квантовій пісочниці реалізовано безліч квантових гейтів. Нижче будуть представлені тільки основні з них:

1) Оператор Адамара;
2) Сігма X (квантовий еквівалент бітового заперечення);
3) Квантове перетворення Фур'є;
4) Тоффолі-гейт;
5) Фазовий поворот.

Отже, ми розглянули два популярних сайту пов'язаних з квантовими комп'ютерами IBM Quantum Experience і Quantum Computing Playground. З їх допомогою можна реалізовувати квантові алгоритми, досліджувати приклади програм, компілювати їх, налагоджувати і запускати в звичайних браузерах. Використання даних сайтів на практиці допоможе краще пізнати принципи роботи квантових комп'ютерів.

На наш погляд, головним недоліком цих середовищ є відсутність докладного документування мов програмування Qiskit і QScript відповідно. Дуже складно знайти онлайн-посібники, які допоможуть зрозуміти ці мови, але з базовими знаннями о програмуванні розібратися в цьому не складе великих труднощів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Квантовые компьютеры как будущее вычислительных технологий. [Електронний ресурс]. – Режим доступу: https://sk.ru/news/kvantovye-kompyutery-kak-buduschee-vychislitelnyh-tehnologiy/
2. Quantum Computing – IBM. [Електронний ресурс]. – Режим доступу: https://www.ibm.com/quantum-computing/
3. Глобальный международный проект свободного доступа к квантовым компьютерам IBM Quantum Experience. [Електронний ресурс]. – Режим доступу: https://controleng.ru/innovatsii/ibm-quantum-experience/
4. Quantum Computing Playground [Електронний ресурс]. – Режим доступу: http://www.quantumplayground.net
5. Квантовая онлайн-песочница от Google [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/246483/

УДК 004.056.5:342

Орловський Д.І.[1], Куцак С.В.[2]
[1]студ. гр. РТ-818 НУ «Запорізька політехніка»
[2]старш. викл. НУ «Запорізька політехніка»

СТАН НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Серед методів захисту інформації від несанкціонованого доступу стеганографія виділяється своєю особливістю, забезпечуючи конфіденційність не шляхом приховування змісту повідомлення, а через збереження в таємниці самого факту його існування.

Базові поняття стеганографії були погоджені в 1996 році на 1-й Міжнародній конференції з приховування інформації – Information Workshop on Information Hiding'96. Проте імплементація напрацювань науковців, що передбачає підготовку відповідних нормативно-правових актів (НПА) і нормативних документів з технічного захисту інформації (НД ТЗІ), відбувається повільно і через це не дає можливості забезпечити належне правове, понятійне та технологічне взаємоузгодження у використанні методів стеганографічного захисту інформації.

В даній роботі проводиться аналіз вітчизняного нормативно-правового забезпечення стеганографічного захисту інформації та (з урахуванням положень Доктрини інформаційної безпеки України і Стратегії національної безпеки України) Сполучених Штатів Америки (США) як стратегічного партнера і Російської Федерації (РФ) як джерела довгострокових системних загроз національній безпеці України.

Дослідження показало, що у вітчизняних НПА відсутні будь-які норми-дефініції щодо стеганографії. Єдина згадка про стеганографію є лише в НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу» як синоніму «принципу забезпечення конфіденційності шляхом організації прихованого каналу передачі всередині іншого відкритого каналу».

Не менш «обмеженою» (але більш предметною) щодо стеганографії є нормативно-правова база РФ, де це поняття зустрічається у декількох методичних документах з інформаційної безпеки та детально розглядається в наказі Федеральної податкової служби «Про забезпечення безпеки персональних даних при їх обробці в автоматизованих інформаційних системах податкових органів», де стеганографічному захисту відведений окремий розділ: «Загальна характеристика нетрадиційних інформаційних каналів» [1]. У цьому наказі стеганографія визначається як «мистецтво приховувати інформацію серед іншої інформації», а методи комп'ютерної стеганографії - це методи, що «призначені для приховування факту передачі повідомлення шляхом вбудовування прихованої інформації в зовнішньо нешкідливі дані (текстові, графічні, аудіо- або відеофайли). Також у цьому документі наводяться пояснення щодо можливих каналів реалізації стенографічних методів у інформаційних системах передачі даних.

В США питаннями стеганографічного захисту займаються декілька державних інституцій. Так, Федеральним Бюро Розслідувань ще у 2004 році опублікувало статтю «Огляд стеганографії для експерта з комп'ютерної криміналістики» [2], в якій детально розглянуті базові поняття стеганографії. Національний інститут стандартів і технологій (National Institute of Standards and Technology, NIST) дає визначення стеганографії як «мистецтва та науки спілкування таким чином, що прихованим є сам факт існування спілкування» [3] та «вбудовування даних у інші дані з метою їх приховування» [4].

В інструкціях Комітету із систем національної безпеки Міністерства оборони США (Committee on National Security Systems (CNSS) Instruction) стеганографія визначена як «мистецтво, наука та практика спілкування таким чином, щоб приховати існування спілкування». Крім цього, термін «стеганографія» широко використовується галузевих статтях Міністерства юстиції США, де питання стеганографії вивчається в контексті нової можливої кіберзагрози [5].

Таким чином, порівняльний аналіз понятійної бази стеганографії в різних країнах показав, що США мають найбільш повну та інформативну термінологію в галузі стеганографії. В РФ та Україні практично відсутнє нормативно-правове регулювання методів та засобів стеганографії.

На нашу думку, відсутність належного вітчизняного нормативного-правового забезпечення в сфері стеганографічного захисту інформації,

можливо, є недопрацюванням суб'єктів нормотворення або ж таке забезпечення існує, але з грифом обмеженого доступу (грифом секретності), і не може бути досліджено в рамках відкритих літературних джерел.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Приказ Федеральной налоговой службы от 21 декабря 2011 г. N ММВ-7-4/959@ [Електронний ресурс]. – Режим доступу: https://www .garant.ru/products/ipo/prime/doc/70012476/

2. Kessler G.C. An Overview of Steganography for the Computer Forensics Examiner [Електронний ресурс]. – Режим доступу: https://bit.ly/3rA9F0W

3. NIST Special Publication 800-101. Revision 1 [Електронний ресурс]. – Режим доступу: https://bit.ly/2PDobI2

4. NIST Special Publication 800-86 [Електронний ресурс]. – Режим доступу: https://bit.ly/3rzlgxn

5. Wingate J.E. Digital Steganography: Threat or Hype? [Електронний ресурс]. – Режим доступу: https://bit.ly/3cu83S6

УДК 004.056.53

Ребриков М.М.[1], Куцак С.В.[2]
[1]студ. гр. РТ-818 НУ «Запорізька політехніка»
[2]старш. викл. НУ «Запорізька політехніка»

БЕЗПЕЧНЕ ЗБЕРІГАННЯ ТОКЕНА АВТОРИЗАЦІЇ (JWT) НА КЛІЄНТСЬКІЙ СТОРОНІ ВЕБДОДАТКУ

Зі стрімким зростанням кількості мережевих сервісів, таких як соціальні мережі, онлайн-банкінг, сервіси, що забезпечують хмарне зберігання інформації та кругообіг документів у електронному форматі, питання авторизації виникає практично в кожному з них. Для авторизації в сучасних вебдодатках часто використовують JSON Web Token [1] (далі JWT), який офіційно з'явився та широко використовується з 2015 року.

JWT - це відкритий стандарт (RFC 7519 [2]) для створення токенів доступу, які, як правило, використовуються для передачі даних аутентифікації в клієнт-серверних додатках. Токени створюються сервером, підписуються алгоритмом HMAC (з використанням секретного ключа) або алгоритмами шифрування, такими як RSA або ECDSA (з використанням пари відкритого і закритого ключів) і передаються на клієнтську сторону додатку. В подальшому користувач використовує даний токен для підтвердження своєї особи.

В даній роботі розглядається питання безпечного зберігання JWT на клієнтській стороні додатку. Існує два основні методи зберігання токенів в пам'яті браузера: в локальному сховищі і в файлах cookie [3]. Також є третій спосіб (зберігання токена в змінній JavaScript), але він практично не використовується, так як зловмисник може без труднощів звернутися до цієї змінної з використанням JavaScript і заволодіти токеном. Також, використовуючи цей метод, не є можливим передавати токен між двома або більше відкритими вкладками браузера. Тому в даній роботі розглядаються тільки двох перших методів зберігання токена, а саме: в локальному сховищі браузера і в файлах cookie.

Переваги зберігання JSON Web токена в локальному сховищі браузера:

• якщо в API (програмний інтерфейс додатку) є необхідність передавати токен авторизації саме в заголовку запиту, то зручно використовувати локальне сховище, тому що ним можна керувати за допомогою JavaScript;

• якщо в API, який використовується в додатку, немає можливості додати функціонал встановлення cookie файлів, то єдиним місцем зберігання токена є локальне сховище.

Недоліки зберігання JSON Web токена в локальному сховищі браузера:

• локальне сховище браузера вразливе до атак типу "Впровадження коду", а саме "XSS-атака" (Cross-Site Scripting). Джерелом такої атаки може бути скрипт сторонньої JavaScript бібліотеки, підключеної до вашого вебдодатку.

Переваги зберігання JSON Web токена в файлах cookie:

• при кожному запиті клієнтської сторони додатку до сервера, cookie будуть відправлятися автоматично. Це є перевагою лише в тому випадку, якщо API додатку не вимагає знаходження токена авторизації в заголовку запиту. В іншому випадку неможливо зберігати токен авторизації в файлах cookie;

• якщо при встановленні cookie файлів вказати прапор "HttpOnly", то зловмисник не зможе отримати доступ до токену авторизації використовуючи JavaScript.

Недоліки зберігання JSON Web токену в файлах cookie:

• не є можливим зберігати багато даних в токені авторизації, так як розмір файлу cookie обмежений 4Кб.

• файли cookie схильні до атак типу "Міжсайтова підробка запиту" (CSRF-атака), але існує спосіб знизити можливість реалізації такої атаки.

Для реалізації захищеного зберігання токена авторизації в файлах cookie необхідно пам'ятати про наступні правила:

• на сайті повинен бути встановлений SSL (Secure Sockets Layer) – захищений сертифікат;

• файли cookie повинні мати прапор "HttpOnly = true". Це унеможливлює "XSS-атаку";

• файли cookie повинні мати прапор "SameSite = Strict". Це унеможливлює "CSRF-атаку";

• файли cookie повинні мати прапор "Secure = true". При наявності цього прапора, файли cookie будуть передаватися тільки по захищеному каналу зв'язку HTTPS.

Використання JWT (токена авторизації) у файлах cookie на даний момент вважається найбезпечнішим способом зберігання даних на стороні клієнта вебдодатку. Цей спосіб найбільш захищений від можливої реалізації атак зловмисника на дані користувача, але має і недоліки, які потрібно враховувати під час реалізації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties [Електронний ресурс]. – Режим доступу: https://jwt.io/

2. RFC 7519 (JSON Web Token) [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc7519

3. Using HTTP cookies [Електронний ресурс]. – Режим доступу: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

УДК 003.26

Ponomarenko Ye.[1], Nelasa H.[2]
[1]student of group RT-810m NU "Zaporizhzhia Polytechnic"
[2]PhD (Information protection systems), professor NU "Zaporizhzhia Polytechnic"

USING OF ELLIPTIC CURVES ISOGENIES IN CRYPTOGRAPHIC PROTOCOLS

Existing public-key cryptography is based on the difficulty of factoring and the difficulty of calculating elliptic curve discrete logarithms. Because these two problems can be easily and effectively solved by a sufficiently large-scale quantum computer, now in development are approaches that appear to be resistant to the hacker attack within the access to a quantum computer. Even if such a quantum computer does not exist today, the prospect of its creation in the near future makes it necessary to prepare a cryptographic infrastructure and protect our data now.

Cryptosystems are being developed which security is based on various hard mathematical problems that cannot be solved by a large-scale quantum computer.

In cryptography, isogeny is the rational mapping of points from one curve to another. The algorithm developed by J. Velu [2], implemented in the work, allows to calculate the function for such mapping.

The features of the use of elliptic curves isogenies in cryptographic protocols are studied. Cryptosystems based on isogenies allow us not only to improve already used, but also to implement fundamentally new cryptographic protocols. Such cryptosystems are resistant to quantum attacks.

The reviewed Diffie-Hellman protocol using supersingular curve isogenies (SIDH), which is similar in structure to the standard algorithm, but uses supersingular elliptic curves and isogenies between them as a mathematical basis. This algorithm was proposed by Jao and DeFeo in [3]. Despite the use of elliptic curves, the security of the algorithm is provided not by the hardness of the elliptic curve discrete logarithm problem, but by the hardness of computing large-scale isogenies between two elliptic curves.

REFERENCES

1. Rostovtsev A., Stolbunov A. Public-Key Cryptosystem Based on Isogenies, Saint Petersburg, 19 p. (2006).

2. J. V´elu, Isog´enies entre courbes elliptiques, C.R. Acad. Sc. Paris, S´erie A., 273 pp. 238-241 (1971).

3. David Jao, Luca De Feo, Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies, Canada, 15 p. (2011).

УДК 004.042

Зайцева А.О.[1], Воскобойник В.О.[2]
1 студ. гр. РТ-819, НУ «Запорізька політехніка»
2 канд. техн. наук, проф. НУ «Запорізька політехніка»

ГІБРИДНИЙ АЛГОРИТМ В СУЧАСНИХ КРИПТОСИСТЕМАХ

У наш час є багато методів захисту інформації. Одним х таких методів є шифрування інформації. Шифрування — у системах обробки інформації – алгоритмічне (криптографічне) перетворення даних, яке виконується у посимвольній послідовності з метою одержання шифрованого тексту. Процес шифрування стає можливим завдяки криптографічним ключам в поєднанні з різними математичними алгоритмами. Э два основних методи шифрування - симетричне та асиметричне.

На практиці, використання асиметричного шифрування призводить до істотного збільшення розміру зашифрованого тексту в порівнянні з відкритим текстом. З іншого боку, використання відкритих і секретних ключів, унікальних для кожного абонента, є затребуваним у багатьох криптографічних додатках, наприклад при реалізації конфіденційної електронної пошти.

Постає питання: що треба зробити, щоб вирішити ситуацію з недоліками методів шифрування та вимогами до захисту інформації?

Все це призводить до виникнення так званої гібридної схеми шифрування. Гібридна (або комбінована) криптосистема - це система шифрування, що поєднує переваги криптосистеми з відкритим ключем з продуктивністю симетричних криптосистем. Симетричний ключ використовується для шифрування даних, а асиметричний для шифрування самого симетричного ключа, інакше це називається числовою упаковкою.

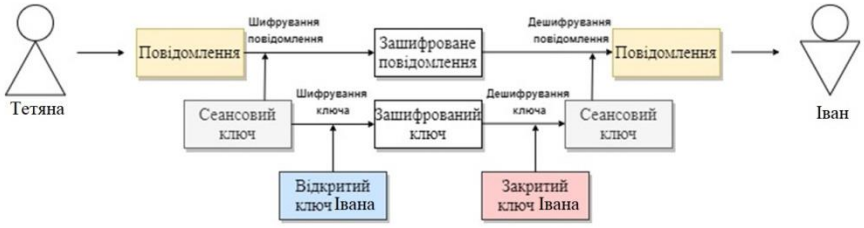


Рисунок 1 – Приклад гібридного алгоритму шифрування

Гібридні криптосистеми використовують переваги двох основних криптосистем: симетричної і асиметричної криптографії. На цьому принципі побудовані такі протоколи, як PGP і TLS.

Основний недолік асиметричної криптографії полягає в низькій швидкості через складні обчислення, необхідні її алгоритмами, в той час як симетрична криптографія традиційно показує високу швидкість роботи. Однак симетричні криптосистеми мають один істотний недолік - їх використання передбачає наявність захищеного каналу для передачі ключів. Для подолання цього недоліку вдаються до асиметричних криптосистем, які використовують пару ключів: відкритий і закритий.

Прикладом може служити надана схема спілкування (рис. 1)

На етапі відправки ми бачимо такі дії. Спочатку Тетяна генерує випадковий сеансовий ключ. Потім повідомлення Тетяни шифрується сеансовим ключем (за допомогою симетричного алгоритму). В свою чергу, сеансовий ключ шифрується відкритим ключем Івана (асиметричним

алгоритмом). В результаті Тетяна посилає Івану зашифроване повідомлення і зашифрований сеансовий ключ.

На етапі прийому. Спочатку Іван отримує зашифроване повідомлення Тетяни і зашифрований сеансовий ключ. Іван розшифровує сеансовий ключ своїм закритим ключем. За допомогою отриманого, таким чином, сеансового ключа Іван розшифровує зашифроване повідомлення Тетяни.

В наш час більшість гібридних систем працюють таким чином. Для симетричного алгоритму (3DES, AES або будь-якого іншого) генерується випадковий сеансовий ключ. Такий ключ як правило має розмір від 128 до 512 біт (в залежності від алгоритму). Потім використовується симетричний алгоритм для шифрування повідомлення. У разі блочного шифрування необхідно використовувати режим шифрування (наприклад CBC), що дозволить шифрувати повідомлення з довжиною, що перевищує довжину блоку. Що стосується самого випадкового ключа, він повинен бути зашифрований за допомогою відкритого ключа одержувача повідомлення, і саме на цьому етапі застосовується асиметричні алгоритми шифрування (RSA або алгоритм Діффі - Хеллмана). Оскільки сеансовий ключ короткий, його шифрування займає небагато часу. Шифрування набору повідомлень за допомогою асиметричного алгоритму - це завдання обчислювально більш складне, тому тут краще використовувати симетричне шифрування. Потім достатньо відправити повідомлення, зашифроване симетричним алгоритмом, а також відповідний ключ в зашифрованому вигляді. Одержувач спочатку розшифровує ключ за допомогою свого секретного ключа, а потім за допомогою отриманого ключа отримує і все повідомлення.

До речі, метод гібридного шифрування використовується в SSL / TLS сертифікатах під час послідовного зв'язку між серверами і клієнтами (веб-браузерами) в процесі, відомому як "TLS handshake". Спочатку перевіряється особистість обох сторін з використанням закритого і відкритого ключа. Після того, як обидві сторони підтвердили свою особистість, шифрування даних відбувається за допомогою симетричного шифрування з використанням ефемерного (сеансового) ключа. Це забезпечує швидку передачу великого обсягу даних, які ми відправляємо і отримуємо в Інтернеті кожну хвилину.

Отже, як бачимо з даного матеріалу, кожний метод шифрування має свої недоліки та переваги. Щоб вирішити цю проблему і вдосконалити захист інформації за допомогою шифрування була розроблена гібридна схема шифрування, яка поєднує переваги двох основних криптосистем: симетричної і асиметричної криптографії. Це призвело до більш швидкого шифрування в сполученні зі зручним розповсюдженням ключів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Иванов М. А., Ковалев А. В., Мацук Н. А., Чугунков И. В. Методы и средства защиты информации в компьютерных системах и сетях / Под ред. М.А. Иванова. – М.: КУДИЦ-ПРЕСС, 2009. 602 с.

УДК 004.75:339.722

Івлєв В.Ю.[1], Воскобойник В.О.[2]
[1]студ. гр. РТ-819 НУ «Запорізька політехніка»
[2]канд. техн. наук, проф. НУ «Запорізька політехніка»

ВРАЗЛИВІСТЬ МЕТОДІВ АУТЕНТИФІКАЦІЇ

Законодавство держави захищає своїх громадян від помилкових звинувачень відносно скоєння правопорушень. Приватні компанії, на жаль, можуть і далі продовжувати використовувати низький рівень досвідченості та розумінь систем аутентифікації в цілому.

Одним з шляхів вирішення цього питання є доцільним застосування алгоритмів розпізнавання осіб в межах комерційного використання світових брендів Microsoft, Google, Amazon і інших. Саме вони стають частиною сучасних методів інформаційної безпеки. Незалежно від платформ операційних систем чи інтерфейсу обміну інформаційними ресурсами, методи аутентифікації є і будуть важливими, а алгоритми яких постійно мають вдосконалюватися.

Аналіз показав, що досвід Японського національного інституту інформатики, який розробив окуляри з LED-лампами, які наче б то, висвітлюються з випромінюванням як білина, закриваючи обличчя від систем розпізнавання, підсвічуючи очі і ніс, скритні. Для людського ока вони майже непомітні. Розпізнавання особистості стає непомітним та не можливим на даний час.

Другим варіантом недосконалості аутентифікації з застосуванням біометрії є силіконова маска, яка надрукована на 3D-принтері. Камера, побачивши обличчя, розпізнає особу згідно даних в базі даних. Але це буде лише прообразом особи, яка не враховує приватні особливості.

Технології аутентифікації та їх застосування постійно вдосконалюються. Цьому прикладом є проект стартам Hyperface,згідно якому, винахідники вирішили виявити усереднені патерні з своїм зображенням. Вони, в завершенні своєїї ідеї, надрукували свої зображення на тканині, що привело до «обману камер спостережень».

Не слід забувати про дактилоскопію як складову аутентифікації особи. Існує декілька способів виявлення та фіксації рельєфу на пальці людини.

Найчастіше використовується оптичний: візуальний малюнок при видимому світлі або відтиск на папері (тактильність).

Наведені підходи аутентифікації та можливості протидії їм на сьогодення є умовними, оскільки розвиток сучасних технологій постійно удосконалюються. Це свідчить про те, що існує можливість обману (чи обходу) систем аутентифікації.

УДК 004.75:339.722
Книш В.В.[1], Воскобойник В.О.[2]
[1] студ. гр. РТ-719, НУ «Запорізька політехніка»
[2]канд. техн. наук, проф. НУ «Запорізька політехніка»

ЗАСОБИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА ІНФОРМАЦІЙНИХ РЕСУРСІВ

З появою цифрових даних з'явилося і питання з приводу безпеки цих даних. З того часу з'явилася велика кількість способів забезпечення безпеки.

Одним із найефективніших засобів захисту даних був і залишається захист паролем. Тут все просто: чим складніше пароль, тим складніше його буде зламати, але з цього виходять деякі проблеми: чим складніше буде пароль та чим більше додатків будуть вимагати введення пароля, тим вище ймовірність того, що користувачі будуть використовувати один і той же пароль, до того ж записуючи його, що дуже збільшує шанси на то, що захист буде зламано.

Рішень цієї проблеми має достатньо варіантів. Наприклад, була винайдена двоетапна аутентифікація. Основною перевагою такої аутентифікації є наявність фізичного ключа і PIN-коду до нього, що забезпечує додаткову стійкість до злому. Слід зазначити, що втрата апаратного ключа не тягне за собою компрометацію пароля, оскільки, крім ключа, для доступу до системи потрібен ще PIN-код до ключу.

Окремо варто розглянути системи з застосуванням разових паролів, які набувають все більшого поширення в зв'язку з широким розвитком інтернет-технологій, і системи біометричної аутентифікації. В даний час основним способом захисту інформації від несанкціонованого доступу (НСД) є впровадження так званих засобів AAA (Authentication, Authorization, Accounting - аутентифікація, авторизація, управління правами користувачів). При використанні цієї технології користувач отримує доступ до своїх даних лише після того, як успішно пройшов процедури ідентифікації і аутентифікації.

До складу електронних систем ідентифікації і аутентифікації входять контактні і безконтактні смарт-карти і USB-ключі (USB-token).USB-ключі

працюють з USB-портом комп'ютера і виготовляються у вигляді брелків. Такі засоби, також, знайшли себе у вигляді карток-пропусків і безконтактних ключів. Безконтактні смарт-карти широко використовуються в різних додатках як для аутентифікації: режим електронного пропуску, електронний ключ до дверей, для різного роду транспортних, ідентифікаційних, розрахункових і дисконтних програм. Важливою властивістю безконтактних карт, що виділяють її з ряду інших смарт-карт, є відсутність механічного контакту з пристроєм, що обробляють дані з карти. Фактично надійність технічних елементів систем, що їх використовують, визначається надійністю мікросхем. Це призводить до істотного зниження експлуатаційних витрат на систему в порівнянні з аналогічними системами, які застосовують смарт-карти з зовнішніми контактами

Але, всі ці методи захисту не є такими надійними, як біометричні засоби. Біометрія - це ідентифікація користувача по унікальним, властивим тільки йому одному біологічними ознаками. Такі системи є найзручнішими, з точки зору самих користувачів, оскільки не потрібно нічого запам'ятовувати, а втратити біологічні характеристики вельми складно.

При біометричної ідентифікації в базі даних зберігається цифровий код, асоційований з певною людиною. Сканер або інший пристрій, що використовується для аутентифікації, зчитує конкретний біологічний параметр. Далі він обробляється за певними алгоритмами і порівнюється з кодом, що містяться в базі даних. До переваг біометричних сканерів зазвичай відносять те, що вони ніяк не залежать від користувача (наприклад, користувач може помилитися при введенні пароля) і користувач не може передати свій біологічний ідентифікатор іншій людині, на відміну від пароля.

Всі біометричні технології можна розділити на дві групи: статичні методи та динамічні. Статичні методи ґрунтуються на фізіологічної (статичної) характеристиці людини, тобто унікальній властивості, властивому йому від народження і невід'ємне, це форма долоні, відбитки пальців, райдужна оболонка, сітківка ока, форма обличчя, розташування вен на кисті руки. Динамічні методи, які ґрунтуються на поведінкової характеристиці людини - особливості, характерних для підсвідомих рухів в процесі відтворення якого-небудь дії.

Проаналізувавши різні технології апаратно-програмної та парольної аутентифікації, можна зробити висновок, що застосування паролів все менше відповідає вимогам безпеки, так як зі збільшенням складності пароля і кількості паролів для запам'ятовування буде зростати роль людського фактору. Користувачі завжди будуть вибирати найбільш прості, з їх точки зору, методи ідентифікації. Тому, враховуючи, поширення діджиталізації, повинно знаходити універсальні і зручні засоби ідентифікації користувачів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Нікифоров С.Н. Методи захисту інформації. Шифрування даних. Видавництво «Лань», 2016.–160 с.

УДК 004.75:339.722

Ковальов І.Є.[1], Воскобойник В.О.[2]
[1] студ. гр. РТ-819 НУ «Запорізька політехніка»
[2]канд. техн. наук, проф. НУ «Запорізька політехніка»

ЯК ЗМІНИТЬСЯ КРИПТОГРАФІЯ ПІСЛЯ ПОЯВИ КВАНТОВИХ КОМП'ЮТЕРІВ

Не зважаючи на те, що реально працюючого квантового комп'ютера ще створено, криптоаналітики стверджують, що квантові комп'ютери несуть дуже великий ризик навіть для найсучасніших методів криптографії. Це пояснюється тим, що квантові комп'ютери здатні збільшити свої обчислювальні потужності в експоненціальному розмірі, використовуючи квантові біти (кубіти) в якості елементної бази.

Кубіти здатні одночасно представляти різні можливі стани, проміжні між 0 і 1 - це явище називається суперпозицією, а також впливати на біти в просторі, використовуючи принцип квантової заплутаності.

За допомогою цих явищ, машина з 300 кубітами здатна представляти більше значень, ніж кількість атомів в спостережуваного Всесвіту.

Для більшого розуміння, порівняємо класичні біти з квантовими: якщо маючи 8 класичних бітів можна отримати одне з 256 значень, то 8 квантових бітів можуть представляти собою одночасно 256 значень і тому кожен новий кубіт подвоює кількість можливих значень (що добре видно на рисунку 1), саме за рахунок цього і підіймається його потужність обчислень.

І постає важливе питання: що потрібно зробити, щоб уникнути загрози витоку величезного об'єму інформації, тому що, хакери спробують використовувати квантові алгоритми в своїх цілях, оскільки вони можуть допомогти їм набагато швидше пробиватися через алгоритми шифрування.

Один з алгоритмів, опублікований Ловом Гровером з AT & T Bell Labs, допомагає квантовим комп'ютерам набагато швидше шукати варіанти вирішення рівняння. Ще один алгоритм, опублікований в 1994 році Пітером Шором, допомагає за допомогою квантових комп'ютерів неймовірно швидко знаходити прості множники цілих чисел. Це загрожує безпеці, так як більшість традиційних криптосистем спирається на факторизації цілих чисел або завдання дискретного логарифмування.

Вчені шукають алгоритми шифрування, які будуть стійкими навіть до квантових комп’ютерів.

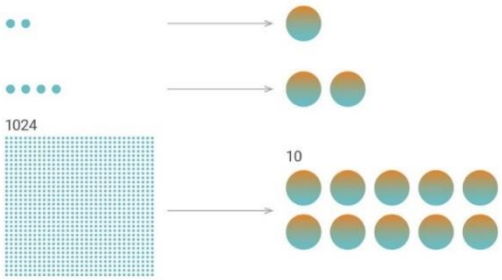


Рисунок 1 – співвідношення необхідної кількості бітів до кубітів

У останніх наукових роботах вказується, що комп'ютер з 20 млн. кубітів зможе впоратися з алгоритмом RSA всього за 8 годин, в той час як класичний комп’ютер буде це робити декілька сотень років. Прогрес квантових обчислень непередбачуваний і стрибок в створенні квантового комп’ютера може бути зроблений коли завгодно, тому важливо вже мати якісь рішення для протидії квантовим комп’ютерам.

Основна проблема на шляху створення квантових комп’ютерів – це елементна база. В якості кубіту є перспективним застосування стабілізованих фотонів як універсальних частин, спроможних використовувати своє призначення в обробці інформації. Проблема в тому, що через деякий час кубіт втрачає свої дані і цей час дуже-дуже малий. Через це, сучасні перспективні прототипи працюють при температурі - 273,13 градусів за Цельсієм (0.02 Кельвіни).

Аналіз сучасних алгоритмів шифрування показує, що методи криптографії в квантовій електроніці потребують збільшення розмірів цифрових ключів для значного збільшення кількості варіантів підтвердження дійсності користувачів. Так, просте подвоєння розміру ключа з 128 до 256 біт збільшує кількість можливих варіантів, які доведеться перебрати квантової системі, що використовує алгоритм Гровера. Тому є доцільним використовувати підхід на базі більш складних функцій з потайним входом для протидії алгоритму Шора.

Враховуючи вище сказане, слід відзначити, що важливість цього напрямку пов'язана з тим, що технології криптографії мають перспективу подальшого вдосконалення та впровадження в безліч галузей діяльності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Roger A. Grimes, Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto. Видавництво «ДМК Прес», 2020. –290 с.

УДК 004.056.52

Шестопалов О.О.[1], Воскобойник В.О.[2]
[1]студ. гр. РТ-817 НУ «Запорізька політехніка»
[2]канд. техн. наук, проф. НУ «Запорізька політехніка»

ЗАХИСТ ІНФОРМАЦІЇ ТЕХНІЧНИМИ ЗАСОБАМИ В ЦЕНТРІ ОБРОБКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У даній роботі розглянуті питання енергозабезпечення та витоку інформації по мережам електроживлення в центрах обробки інформаційних ресурсів (ЦОІР).

Більшість компаній та організацій використовує у своїй діяльності ЦОІР, або частину її складової.

Оскільки є можливість одержання інформації по лініям електроживлення, то слід виділити групу спеціальних технічних засобів: фільтри, шумогенератори.

Фільтри є достатньо універсальними пристроями, що протидіють витоку інформації. Але, головний їх недолік — відсутність захисту від спеціальних технічних засобів (СТЗ), що передають інформацію через мережу електроживлення. Фільтр захищає одиничну апаратуру, або декілька одиниць засобів технічної обробки інформації .

Інформація, яку можливо передати по лініям електроживлення, знаходиться в межах електроживлення до першого трансформатора.

Шумогенератори діють на всю мережу електроживлення до трансформатора. Усі канали можливого витоку даних по мережі 220В будуть ліквідовані. Тобто вся апаратура, підключена до мережі електроживлення в даному приміщенні, буде захищена.

Існує цілий ряд шумогенераторів таких як Соната-3, Злива-32, SI-8001, SEL SP-41/C і ін.

Вищевказані пристрої стабільні в використанні. Але, досвід їх експлуатації показав, що при виборі шумогенераторів слід звернути увагу на смугу частот генеруючого шуму та на рівень шумового сигналу.

Практика показала, що найбільш оптимальним по своїм характеристикам є шумогенератор Злива-32. Головний плюс цього

генератору — високий рівень сигналу шуму, що дозволяє бути впевненим у повному зашумленні мереж енергоживлення.

Висновок: постійний контроль ліній електромереж та контроль технічних засобів є запорукою інформаційної безпеки.

СЕКЦІЯ «ПРИКЛАДНА МАТЕМАТИКА»

УДК 539.371
Мастиновський Ю.В. [1] , Анпілогов Д.І. [2], Щербіна О.А.[3]
[1] канд. техн. наук, проф. НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»
[3] асист. НУ «Запорізька політехніка»

ПОЗДОВЖНІЙ УДАР ПО ПРУЖНОМУ ЗРІЗАНОМУ КОНУСУ

В даній роботі розглядається стрижень змінного перерізу, лінійні розміри якого малі порівняно з довжиною стрижня. Згідно з другим законом Ньютона рівняння руху можна подати у вигляді:

$$\rho F \frac{\partial^2 u}{\partial t^2} = \frac{\partial}{\partial x}\left(F\sigma_x\right), \tag{1}$$

де $F(x)$ – площа поперечного перерізу (функція, що змінюється повільно), $\sigma_x = E\frac{\partial u}{\partial x}$ – поздовжня напруга, E – модуль Юнга. Це рівняння зводиться до наступного вигляду

$$\frac{\partial^2 u}{\partial x^2} - \frac{1}{c^2}\cdot\frac{\partial^2 u}{\partial t^2} = -\frac{\partial u}{\partial x}\cdot\frac{d}{dx}\left(\ln F(x)\right). \tag{2}$$

В якості прикладу хвильового руху стрижня змінного поперечного перерізу розв'яжемо задачі про поздовжній удар по зрізаному конусу скінченної довжини (рис. 1).

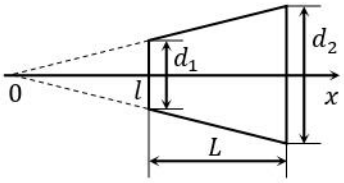


Рисунок 1 – Схема конусу.

Рівняння руху має безрозмірний вигляд

$$\frac{\partial^2 U}{\partial \xi^2} - \frac{\partial^2 U}{\partial \tau^2} = -\frac{2}{\xi}\cdot\frac{\partial U}{\partial \xi}, \tag{3}$$

де $\xi = \frac{x}{L}$, $U = \frac{u}{L}$, $\tau = \frac{ct}{L}$, $(c^2 = \frac{E}{\rho})$.

Початкові і граничні умови приймемо у вигляді

$$\tau = 0,\ \tau U = \frac{\partial U}{\partial \xi} = \frac{\partial U}{\partial \tau} = 0,\ h \le \xi \le h+1,\ h = \frac{l}{L};$$

$$\tau > 0,\ \xi = h,\ \frac{\partial U}{\partial \tau} = hV_0(\tau); \qquad \xi = h+1,\ \frac{\partial U}{\partial \xi} = 0, \tag{4}$$

Розрахунки проводились чисельно з використанням методу характеристик. Рівняння характеристик вихідного рівняння і диференціальні співвідношення на них визначаються виразами:

$$\frac{d\xi}{d\tau} = \pm 1; \qquad d\left(\frac{\partial U}{\partial \tau}\right) \mp d\left(\frac{\partial U}{\partial \xi}\right) = \pm \frac{2}{\xi} \cdot \frac{\partial U}{\partial \xi}\, d\xi. \tag{5}$$

Розрахунки проводились для $h = 1$ і $V_0(\tau) = 0{,}25\tau e^{-\tau}$. Якісні закономірності розповсюдження хвиль досліджувались шляхом порівняння результатів, отримуваних при інших вихідних даних: $h = 0{,}5$, $V_0 = const = 0{,}25$, а також з результатами випадку сталого перерізу ($d_1 = d_2$). В усіх випадках спостерігалось зменшення амплітуди хвилі аж до її відбиття.

Планується провести дослідження хвильового руху зрізаного конусу при ударі по основі більшого діаметру при аналогічних початкових і граничних умовах, а також розглянути стрижень іншого змінного перерізу.

УДК 539.3; 534.1
Левицька Т.І.[1], Пожуєва І.С.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ НАПРУЖЕНО-ДЕФОРМІВНОГО СТАНУ ОБОЛОНКИ З МАЛИМ ПОЧАТКОВИМ ПРОГИНОМ

Питання, що пов'язані з визначенням напружено-деформівного стану пружних оболонок, є актуальними задачами механіки.

У даній роботі побудована модель напружено-деформівного стану осесиметричної оболонки з малими початковими прогинами, що враховує як деформацію зсуву і інерцію обертання, так і деякі нелінійні члени. Розглядається напівнескінчена циліндрична оболонка постійної товщини *h*.

Вісь Ox спрямована уздовж твірної серединної поверхні оболонки, вісь Oy - ортогональна осі Ox, початок координат - на торці оболонки.

Вважатимемо, що оболонка має малий початковий прогин в серединній поверхні. В цьому випадку у виразах для деформацій змінюються лише складові, обумовлені переміщенням динамічного прогину, і вони приймають вид:

$$\begin{cases} e_{xx} = \dfrac{\partial \tilde{u}}{\partial x} + \dfrac{1}{2}\left(\dfrac{\partial(\tilde{v}_0 + \tilde{v}_1)}{\partial x}\right)^2 - \dfrac{1}{2}\left(\dfrac{\partial \tilde{v}_0}{\partial x}\right)^2, \\ e_{\varphi\varphi} = \dfrac{\tilde{v}_1}{R+y} + \dfrac{\tilde{v}_1^{\,2}}{2(R+y)^2}, \\ e_{xy} = \dfrac{1}{2}\left(\left(\dfrac{\partial(\tilde{v}_1 + \tilde{v}_0)}{\partial x} + \dfrac{\partial \tilde{u}}{\partial y}\right) + \dfrac{\partial(\tilde{v}_1 + \tilde{v}_0)}{\partial x} \cdot \dfrac{\partial(\tilde{v}_1 + \tilde{v}_0)}{\partial y} - \dfrac{\partial \tilde{v}_0}{\partial x} \cdot \dfrac{\partial \tilde{v}_0}{\partial y} - \dfrac{\partial \tilde{v}_0}{\partial x}\right). \end{cases} \quad (1)$$

Компоненти тензора напружень знаходились із закону Гука. Компоненти зсуву в оболонці шукалися у вигляді:

$$\begin{cases} \tilde{u}(x,y,t) = u(x,t) + (y - \dfrac{h^2}{12R})\psi(x,t), \\ \tilde{v}(x,y,t) = v(x,t) = v_1(x,t) + v_0(x,0). \end{cases} \quad (2)$$

Для виведення рівнянь руху оболонки використовувався варіаційний принцип Гамільтона-Остроградського. Розв'язок було побудовано за допомогою характеристичних рівнянь. При цьому уздовж будь-якого напрямку виконувалися умови неперервності.

Характеристики і співвідношення на них було отримано у наступному вигляді:

$$dx = \pm\beta dt\,, \quad F_3 \cdot dx \mp \beta \cdot dV_{1t} + \beta^2 dV_{1x} = 0\,;$$

$$dx = \pm dt\,, \quad -\gamma\left(F_3 dx \mp dV_{1t} + d\left(V_{1x}\right)\right) = (1-\beta^2)\left(F_1 dx \mp dU_t + dU\right)\,; \quad (3)$$

$$F_2 \cdot dt = d\psi_t \mp d\psi_x\,.$$

Початкові умови передбачалися нульовими, механічний вплив на оболонку моделювався завданням швидкості частинок на торці. Чисельні розрахунки проводилися методом характеристик. Був проведений аналіз для різних геометричних і фізичних параметрів оболонки з малим початковим прогином, а також для різних видів і тривалості торцевого навантаження.

УДК 539.371
Анпілогов Д.І.
канд. техн. наук, доц. НУ «Запорізька політехніка»

РОЗПОВСЮДЖЕННЯ НЕУСТАЛЕНИХ ПОЗДОВЖНІХ ХВИЛЬ У СТЕРЖНІ МІНДЛІНА-ГЕРМАНА

Розглядається розповсюдження неусталених поздовжніх хвиль при імпульсному збудженні у стержні змінного перерізу з урахуванням поперечних рухів і деформації зсуву. З використанням варіаційного принципу Гамільтона-Остроградського отримано формулювання відповідної крайової задачі у одно- і двохмодовій постановці (технічна теорія і рівняння Міндліна-Германа [1]). В останньому випадку одержано систему гіперболічних рівнянь і супутні їм природні крайові умови. Зауважується, що ці умови відрізняються від результатів, традиційно отримуваних із застосуванням закону Гука.

Отримані крайові задачі зведено до безрозмірного вигляду і розв'язано методом характеристик [2]. Тривалість імпульсу збудження обрано малою порівняно з часом, за який хвиля дилатації проходить відстань, рівну довжині стержня.

Аналіз отриманих результатів призводить до двох висновків. По-перше, при використанні як одномодової, так і двохмодової моделі переміщень при розповсюдженні в бік спадання площі перерізу хвилі стають нестійким (їх амплітуда зростає). По-друге, хвиля стиску-розтягу у двохмодовій моделі виявляє суттєве зменшення групової швидкості порівняно з випадком технічної теорії. Це супроводжується значним спотворенням профілю хвилі. Названі особливості стають більш помітними після відбивання хвиль.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ерофеев, В.И. Волны в стержнях. Дисперсия. Диссипация. Нелинейность [Текст] // В.И. Ерофеев, В.В. Кажаев, Н.П. Семерикова. – М. : Физматлит, 2002. – 208 с.

2. Крылов, В.И. Вычислительные методы [Текст] // В.И. Крылов, В.В. Бобков, П.И. Монастырный. – М. : Наука, 1977. – 400 с.

УДК 330.4
Калачова Д.К.[1], Шишканова Г.А. [2]
[1] студ. гр. ФЕУ-218 НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

ЗАСТОСУВАННЯ МАТЕМАТИКИ В ЛОГІСТИЦІ

При проведенні логістичного аналізу, а також для підвищення його точності і достовірності в фірмах застосовується широка ланка різноманітних математичних та економіко-математичних методів і моделей, що становлять наукову базу логістики. Серед найбільш поширених в логістичному менеджменті можна вказати: методи математичної статистики (факторний, індексний, кластерний, дисперсійний аналіз, множинні кореляційно-регресивні моделі, спектральний аналіз і ін.); функціонально-вартісний аналіз; методи статистичного імітаційного моделювання на ЕОМ; різні економетричні методи і моделі та методи експертних оцінок.

Проведення системного аналізу в логістиці будується на використанні певного інструментарію, як шляху пізнання, що спирається на певну сукупність раніше отриманих загальних знань (принципів). При проведенні системного аналізу можуть використовуватися багато різних методів.

Так, наприклад, метод сценаріїв являє собою засіб первинного впорядкування виявленої проблеми в області обслуговування споживача, отримання та збору інформації про взаємозв'язки розв'язуваної логістичної проблеми з іншими, про можливі і ймовірні напрямки майбутнього розвитку системи.

Методи експертних оцінок засновані на різних формах експертного опитування з подальшим оцінюванням і вибором за обраними критеріями найкращого варіанту. Цілями методів типу «Дельфі» є зворотний зв'язок, ознайомлення експертів з результатами попереднього етапу аналізу і облік цих результатів при оцінці значимості експертами. В основі цих методів важлива «мозкова атака». Головне призначення «мозкової атаки» полягає в пошуку нових ідей, їх широкого обговорення, конструктивної критики.

Часто в логістиці застосовуються методи типу дерева цілей. Дерево цілей є зв'язковим графом, вершини якого розглядаються як цілі логістичної системи, а ребра або дуги - як зв'язки між ними. Експертам пропонується оцінити структуру моделі досліджуваної логістичної системи в цілому і дати пропозиції щодо включення в неї неврахованих зв'язків. Важливими також є морфологічні методи. Головна ідея морфологічного підходу полягає в систематичному знаходженні всіх можливих варіантів вирішення логістичної проблеми за допомогою комбінування виділених елементів або їх ознак.

Застосування матричних форм представлення та аналізу даних не є специфічним інструментом аналізу досліджуваних логістичних систем, але

широко використовується на різних етапах аналізу логістичної системи як допоміжний засіб.

Програмно-цільовий метод являє собою розробку і виконання перспективних завдань, орієнтованих на досягнення певної мети незалежно від встановлених рамок. Він передбачає послідовну реалізацію комплексу технічних, організаційних та економічних заходів.

Метод аналізу систем використовується для оцінки альтернативних курсів дій при розподілі ресурсів відповідно до цілей логістичних підсистем. Якщо цілі встановлені, для вирішення певних завдань пропонуються різні програми. У процесі аналізу проводиться оцінка альтернативних планів.

Логістичні завдання, існуючі в практичній діяльності, вирішувати найпростішими арифметичними методами або на основі досвіду роботи неможливо. Це пов'язано з тим, що виникає безліч можливих варіантів. Так, при трьох постачальниках продукції та трьох споживачах вірогідні 90 різних варіантів рішення, а при чотирьох постачальників і чотирьох споживачах їх більш 6000 і т.д. Для того щоб відповісти на питання – який варіант більш доцільний, необхідно побудувати математичну модель – абстрактне відображення за допомогою математичної символіки реального процесу. Математична модель включає умови (обмеження) завдання і підлягає оптимізації критерій (цільову функцію).

Відшукати оптимальний варіант можна за допомогою лінійного, динамічного і стохастичного програмування. Слово «програмування» показує, що математичні методи застосовують для планування, складання програми (плану). Динамічне програмування має справу з динамічними системами, тобто системами, змінюються в часі під дією внутрішніх і зовнішніх впливів, на кожному кроці виробляється деякий вибір перетворень, залежний не тільки від часу, але і від поточного стану системи. Стохастичне програмування вивчає методи розв'язання задач управління і планування в умовах ризику і невизначеності.

Можна зробити висновок, що потреба в аналізі логістичних систем виникає при вирішенні логістичних завдань для ув'язки мети логістичної системи з безліччю засобів її досягнення, у випадках, коли елементи логістичної системи мають розгалужені зв'язки, які можуть викликати віддалені наслідки в різних ланках ланцюга поставок, і рішення по ним вимагають обліку загальних витрат по ланцюгу поставок продукції та коли мають місце важко порівнювані варіанти рішень або досягнення комплексу цілей.

УДК 330.4
Ліщина В.О.[1], Шишканова Г.А. [2]
[1] студ. гр. ФЕУ-218 НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

МЕТОДИ ЛІНІЙНОГО ПРОГРАМУВАННЯ В ЛОГІСТИЦІ

Термін «логістика» виник в збройних силах і відноситься до переміщення обладнання і матеріалів для військ в польових умовах. У сучасному світі він використовується в більш широкому сенсі для позначення процесу переміщення людей, матеріалів, інвентарю та обладнання. Головна ціль логістики це забезпечення споживача продукцією в потрібний час і потрібне місце з найменшими витратами на перевезення. Саме тому в логістиці використовують лінійне програмування щоб знайти оптимальний вид транспорту, маршрут, швидкість перевезення і звести до мінімуму псування вантажу.

Найбільш поширеним і необхідним рішенням щодо оптимізації логістики залишається транспортна задача – математична задача лінійного програмування яку використовують щоб знайти оптимальний план перевезень однорідних вантажів з пункту відправлення в пункти перевезення з мінімальними затратами. Застосовуючи розв'язок такої задачі транспортні витрати часто знижуються на 10-30 відсотків. Недоліком транспортної задачі є те що вона не враховує неоднорідність вантажу і транспортного засобу. Така проблема вирішується складанням багатоіндексних задач.

Транспортну задачу можна використати в різних випадках, наприклад, оптимізація поставок сировини і матеріалів на виробництво, оптимізація доставок товарів в роздрібні магазини зі складів, перевезення пасажирів та у багатьох інших.

Пропонується випадок молодіжного стартапу для трьох міні-пекарень, які можна позначити буквами A_1, A_2, A_3, що спеціалізуються на створенні різних солодощів. Кожна пекарня щодня може виготовляти відповідно 50, 30 та 20 тортів, які необхідно відправляти в чотири магазини B_1, B_2, B_3, B_4, з якими заключено договір. Магазини бажають отримувати торти в кількості відповідно 30, 30, 10 та 20 шт. Перевезення здійснюються на мотоциклах, одразу після виготовлення кожного з тортів. Вартість перевезення 1 торту від пекарень до магазинів наведено в таблиці 1. Потрібно визначити такий план перевезення тортів до магазинів, за якого загальні витрати кондитерського об'єднання з трьох міні пекарень будуть найменшими.

Нехай x_{ij} – кількість тортів, які перевозяться з i-ї пекарні до j-го магазину ($i = \overline{1,\ 3}$; $j = \overline{1,\ 4}$). Тоді математична модель даної задачі має вигляд

$$Z = 2x_{11} + 3x_{12} + 4x_{13} + 2x_{14} + 5x_{21} + 7x_{22} + x_{23} + \\ + 4x_{24} + 9x_{31} + 4x_{32} + 3x_{33} + 2x_{34} \to \min \quad , \tag{1}$$

за наступних обмежень

$$\begin{cases} x_{11} + x_{12} + x_{13} + x_{14} \le 50, \\ x_{21} + x_{22} + x_{23} + x_{24} \le 30, \\ x_{31} + x_{32} + x_{33} + x_{34} \le 20, \\ x_{11} + x_{21} + x_{31} + = 30, \\ x_{12} + x_{22} + x_{32} + = 30, \\ x_{13} + x_{23} + x_{33} + = 10, \\ x_{14} + x_{24} + x_{34} + = 20, \end{cases} \quad x_{ij} \ge 0, \quad i = \overline{1, 3}; \quad j = \overline{1, 4}. \tag{2}$$

Знак «≤» у перших трьох обмеженнях (2) задачі пояснюється тим, що за умовою транспортна задача є відкритою:

$$\sum_{i=1}^{3} a_i = 100; \quad \sum_{j=1}^{4} b_j = 90. \tag{3}$$

У такій ситуації, коли попит менший за пропозицію (3), частина тортів не буде виготовлена, або залишиться в пекарнях, тобто є можливість пошуку заказів від інших осіб.

Таблиця 1 – Вартість перевезень пекарня-магазин

Пекарня	Вартість перевезення 1 торту до магазинів			
	B_1	B_2	B_3	B_4
A_1	2	3	4	2
A_2	5	7	1	4
A_3	9	4	3	2

Щоб визначити оптимальний план поставленої задачі, її необхідно збалансувати, тобто звести до закритого типу. Це виконується шляхом уведення додаткового, умовного споживача B_5 із попитом $100 - 90 = 10$ тортів. Вартість перевезення одиниці продукції до умовного споживача дорівнює нулю. Після застосування методу потенціалів, одержуємо опорний план

$$X = \begin{pmatrix} 20 & 30 & 0 & 0 & 0 \\ 10 & 0 & 10 & 0 & 10 \\ 0 & 10 & 0 & 20 & 0 \end{pmatrix}, \tag{4}$$

Підставляючи (4) в (1), одержуємо, що найменші загальні транспортні витрати становитимуть 230 ум. од.

УДК 330.4
Штанько М.А.[1], Шишканова Г.А. [2]
[1] студ. гр. ФЕУ-218 НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

ВПЛИВ КАРАНТИННИХ ЗАХОДІВ У ЗВ'ЯЗКУ З COVID-19 НА ЛОГІСТИКУ УКРАЇНИ

Внаслідок пандемії коронавірусу та введених карантинних заходів падіння українського ВВП за даними Міністерства розвитку економіки, торгівлі та сільського господарства першій половині 2020 р. склало 6,5% [1]. Компанії, які ще не діджиталізувались, можуть нести збитки і надалі. Час вимагає малим підприємствам переходити на віддалений режим роботи та продовжувати більшість своєї діяльності онлайн. Якщо працювати через логістичні платформи дистанційно, то можна не лише оминути кризу, а й використати її як інструмент зростання у майбутньому.

Вочевидь, потреба в математичному аналізі теперішньої ситуації є досить актуальною. Необхідна розробка нових математичних підходів для визначення шляхів виходу з економічної кризи, в умовах невизначеності, коли потрібно обирати важко порівнювані варіанти рішень та коли елементи системи бізнесу мають розгалужені зв'язки, які можуть викликати віддалені наслідки в різних ланках ланцюга поставок, і рішення по ним вимагають обліку загальних витрат по ланцюгу поставок продукції.

В умовах запровадження карантинних заходів сфера логістичних перевезень працює в умовах необхідності дотримання вимог щодо протиепідемічної безпеки: водіїв фур та персонал вантажних потягів і суден, які перетинають кордон, перевіряють на стан здоров'я. Обмеження під час карантину Covid-19 зазнали значних змін не лише для міжнародних перевізників, а й для водіїв, що займаються перевезенням всередині країни. Зміни стосуються насамперед медичних протипоказань для водіїв та видачі їм засобів самозахисту, а саме: перед рейсом кожен водій має пройти поверхневу перевірку стану здоров'я та виміряти температуру тіла. Його мають забезпечити маскою та антисептиками, а також дезінфекторами для транспорту та рукавичками, щоб мінімізувати контакт з працівниками складу при передачі вантажу.

Логістичні перевезення на період карантину не зазнають значних збитків у порівнянні з іншими сферами діяльності, однак і тут присутній ряд проблем, пов'язаних з обмеженням руху між областями і перевірками, що

зменшують вантажопотік та впливають на втрату часу між транспортуваннями.

Закриття підприємств через коронавірус в Україні та в інших країнах вплинуло на обсяги міжнародних автомобільних перевезень. Наразі спад в автомобільній галузі у першому півріччі минулого року становить близько 20% [1], хоча в останній час спостерігається ситуація відновлення та навіть зростання автомобільних перевезень. У галузі вантажних авіаперевезень у всьому світі спостерігається зниження попиту. Водночас, скасування пасажирських рейсів вплинуло і на вартість послуг доставки вантажів, оскільки більшість із них раніше доставлялись пасажирськими літаками.

Тимчасове закриття магазинів та зменшення користування громадським транспортом призвело до збільшення попиту на онлайн-доставку товарів, тобто відчувається позитивний вплив на роботу поштових служб. Значно зросли обсяги кур'єрської доставки.

Відбувається трансформація сервісної лінійки компаній, які здійснюють доставку товарів. Наприклад, «Нова пошта» вже ввела нову функцію, яка дозволяє сплачувати доставку онлайн за третю особу - одержувача відправлення. Особливою популярністю почала користуватися доставка ліків поштою, запущена з квітня. Проте дуже важливою для таких компаній є організація належної безпеки персоналу.

У перспективі для будь-якого бізнесу пріоритетним буде адаптивність. Теперішня інноваційна ідея в логістиці (і не тільки) полягає в бімодальних ланцюжках поставок: перший традиційний модуль - ощадлива ефективність, низькі ризики, висока передбачуваність; другий модуль - швидке розпізнавання та вивчення нових можливостей, адаптивність, готовність вирішувати несподівані проблеми.

Оскільки вплив карантинних обмежень розповсюджується не тільки на один якийсь сектор, а на усі взаємопов'язані з ним, то потрібен системний підхід для виявлення наслідків, який базується на всебічному економіко-математичному аналізі. Необхідно разом визначити пріоритетні зусилля для зростання економічної системи країни в цілому. Запорукою виходу з кризи буде співпраця уряду, державних та приватних компаній.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Українська економіка впала за півроку на 6,5%. У другому кварталі - на 11% [Електронний ресурс]: Економічна правда від 6 серпня 2020 р. – Режим доступу: https://www.epravda.com.ua/news/2020/08/6/663774/

УДК 330.4
Бурда А.Ю. [1], Шишканова Г.А. [2]
[1] студ. гр. БАД-618 НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

МАТЕМАТИЧНА МОДЕЛЬ ПЛАНУВАННЯ У РЕСТОРАННОМУ БІЗНЕСІ

Ресторанний бізнес перебував у п'ятірці найпривабливіших для інвесторів. За останні часи його рейтинг дещо знизився. Але зараз ресторани відвідуються як і раніше. Ресторан надає населенню вільний доступ до послуг громадського харчування та проведення особистого і корпоративного дозвілля, організовуючи виробництво різноманітних страв у спеціально підготовленому для цього приміщенні.

Успішна робота ресторану залежить від багатьох факторів. Як і будь-яка складна система, ресторан починається з задуму його засновників та закінчується контролем функціонування закладу. Головну роль в цьому виконує практична філософія його власника або керуючого. Її розкриває підхід до ведення бізнесу, який визначає етичні та моральні цінності, що реалізуються в процесі функціонування підприємства. Одним з головних моментів в організації ресторану – це вибір категорії клієнтів з певним соціальним статусом і рівнем доходу – власної цільової аудиторії, на яку орієнтуватиметься заклад, що обумовлює всю подальшу стратегію реалізації проекту, яку повинен відображати бізнес-план ресторану.

При складанні плану, необхідно орієнтуватися скільки клієнти приблизно витрачають коштів на ресторани та кафе, для чого необхідно дослідити статистичні дані та зробити прогнозування у умовах, які постійно змінюються. Методом найменших квадратів визначено залежність між сукупними витратами в середньому за місяць у розрахунку на одне домогосподарство x, грн., та споживчими сукупними витратами на ресторани y, грн., базуючись на статистичних даних [1] за 2010-2019 роки:

$$y = 59{,}2711 + (0{,}0014 \cdot x)^2 . \qquad (1)$$

Було розглянуто лінійна та десять нелінійних моделей, обрана модель (1), яка найкраще описує статистичні дані, тому що для цієї регресії сума квадратів відхилень є найменша.

Графік залежності (1), початкові дані та довірча зона регресії наведено на рис. 1. Зроблено розрахунок прогнозного значення для x=10500 грн., відповідно одержано y = 284,28 грн.

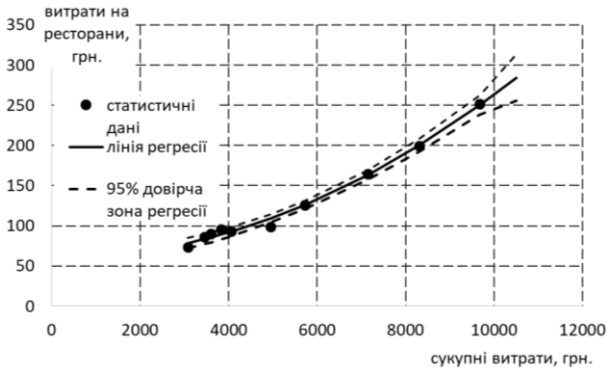


Рисунок 1 – Графік регресії та її довірчої зони.

Коефіцієнт кореляції у лінеарізованій моделі (1) r=0,9968; він близький до одиниці, тобто можна стверджувати, що між x та y існує відповідна залежність. Коефіцієнт детермінації R^2 =0,9940, що підтверджує тісний зв'язок між розглядуваними величинами. Перевірка за допомогою критерію Фішера показали, що F=3550,5 є більшим за Fкрит (0,05;1;8)=5,32, тобто модель є адекватною статистичним даним при рівні значущості $\alpha = 0{,}05$. Можна зробити висновок, що модель (1) прийнятна для економічного аналізу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Демографічна та соціальна статистика / Доходи та умови життя [Електронний ресурс]: Державна служба статистики України – Режим доступу: http://www.ukrstat.gov.ua/ operativ/operativ2020/gdvdg/ssv/arh_ssv_u.htm

УДК 519.65
Путінцева П.Д. [1], Коротунова О.В.[2]
[1] студ. гр. КНТ-220 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ДЕЯКІ ЗАСТОСУВАННЯ ВИЗНАЧЕНИХ ІНТЕГРАЛІВ

Визначені інтеграли застосовуються в техніці, геометрії, фізиці, біології, економіці та інших галузях науки. Від традиційного застосування визначених інтегралів для знаходження площин плоских фігур, площин поверхонь та об’ємів геометричних тіл до проектування космічних апаратів.

Так, наприклад, швидкість є інтеграл від прискорення. Інтегруванням прискорення за часом знаходять швидкість руху, а подальшим інтегруванням

швидкості визначається пройдений шлях. За допомогою визначеного інтеграла в фізиці також знаходяться моменти інерції, координати центру ваги, маси плоских фігур. Рух заряду в електричному полі також може описуватись за допомогою визначеного інтеграла.

В економіці за допомогою визначеного інтеграла знаходять обсяг продукції Q, що виготовлена за деякий проміжок часу $[0;T]$: $Q = \int_0^T f(t)dt$.

Функція $y = f(t)$ описує залежність продуктивності праці від часу. З використанням виробничої функції Коба-Дугласа ця залежність набуває більш складного вигляду: $Q = \int_0^T (\alpha t + \beta) e^{\gamma t} dt$.

З курсу біології відомо, що в умовах необмежених ресурсів харчування швидкість росту багатьох популяцій експоненційна, тобто $\upsilon(t) = ae^{kt}$. Такі умови можна створити, наприклад, для мікроорганізмів, якщо пересаджувати час від часу культуру, що розвивається, в нові ємності з живильним середовищем. Тоді чисельність популяції $N(t) = N(t_0) + a\int_{t_0}^T e^{kt} dt$. За подібною формулою підраховують, зокрема, чисельність культивованих цвілевих грибків, які виділяють пеніцилін.

Слід зазначити, що наведені приклади далеко не вичерпують можливі застосування визначеного інтеграла.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Курченко, О.О. Інтегральне числення функцій однієї змінної: навч. посібник [Текст] / О.О. Курченко. – К.: АСТ, 2016. – 140 с.

УДК 519.65

Похила Н.Ю. [1], Коротунова О.В.[2]
[1] студ. гр. КНТ-220 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

МЕТОД МОНТЕ-КАРЛО В ЧИСЕЛЬНОМУ ІНТЕГРУВАННІ ФУНКЦІЇ ОДНІЄЇ ЗМІННОЇ

Методом Монте-Карло називають універсальний метод статистичних випробувань. Використовується для розв’язування задач, які мають випадковий характер вихідних даних, у фізиці, математиці, економіці,

оптимізації, теорії управління тощо. Зокрема, метод Монте-Карло застосовують для наближеного обчислення інтегралів, у тому числі і кратних.

Цьому сприяє простота структури обчислювального алгоритму та цілком прийнятна похибка обчислень, яка визначається похибкою генерації псевдовипадкової послідовності чисел, що згенеровані на ЕОМ, та обсягом вибірки. Як правило, $O\left(N^{-\frac{1}{2}}\right)$, де N – число спроб.

Одна з реалізацій методу базується на геометричній інтерпретації визначеного інтегралу і геометричному визначенні ймовірності. Нехай графік функції $y = f(x)$ цілком лежить усередині прямокутника з основою (b-a) і висотою (d-c) (рис. 1).

Геометрично $\int_a^b f(x)dx$ – це площа області під кривою $y = f(x)$. Дослід, що складається в киданні навмання точок в прямокутник, замінюють формуванням N пар довільних чисел (x_i, y_i), які повинні рівномірно заповнити даний прямокутник: $a < x_i < b$, $c < y_i < d$.

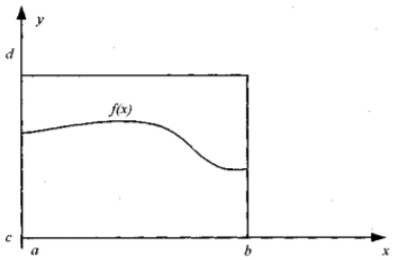


Рисунок 1 – Геометрична інтерпретація.

Тоді частина n точок (x_i, y_i), що задовольняють умову $y_i \le f(x_i)$, є оцінкою відношення інтеграла від функції $f(x)$ до площі даного прямокутника S. Значення визначеного інтеграла, згідно даного методу може бути обчислено за формулою

$$\int_a^b f(x)dx = S\frac{n}{N}. \qquad (1)$$

Значення визначеного інтеграла можна також обчислити і іншим способом, якщо розглядати його як середнє значення функції $f(x)$ на відрізку $[a;b]$

$$\int_a^b f(x)dx \approx \frac{b-a}{N}\sum_{i=1}^{N} f(x_i), \qquad (2)$$

де x_i – послідовність випадкових чисел рівномірно розподілених на відрізку $[a;b]$.

В якості прикладу методом Монте-Карло було обчислено наближене значення інтеграла $\int_1^e \sqrt[3]{x}\ln x dx$. Розрахунки було проведено для 20; 50 та 100 чисел t_i, $i=\overline{1,N}$, які згенеровано із відрізку [0;1]. Відповідні значення x_i зв'язані з t_i співвідношеннями $x_i = 1+(e-1)t_i$.

Значення функції, які обчислено із застосуванням формули (2) для кожного із значень N: 1,29569 (N=20), 1,27046 (N=50), … , 1,27679 (N=100).

Аналітичний розрахунок дає результат: $\int_1^e \sqrt[3]{x}\ln x dx \approx 1,27381$.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Мусіяка, В. Г. Основи числових методів [Текст] / В. Г. Мусіяка. – Дніпро: ЛІРА, 2017. – 256 с.

2. Самборська, О. М. Чисельні методи: навчальний посібник для студентів вищих технічних навчальних закладів [Текст] / О. М. Самборська, Б.Г.Шелестовський. – Тернопіль: ТНТУ імені Івана Пулюя, 2010. – 164 с.

УДК 378.14
Коротунова О.В.[1], Нечипоренко Н.О. [2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

ОСОБЛИВОСТІ ДИСТАНЦІЙНОГО НАВЧАННЯ В ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ В УМОВАХ РОЗПОВСЮДЖЕННЯ КОРОНОВІРУСНОЇ ІНФЕКЦІЇ

Різноманітні форми онлайн-освіти вже певний час активно впроваджуються в навчальний процес. Проте донедавна вони відігравали допоміжну роль при традиційній освіті. Одним із способів приборкання спалаху короновірусної інфекції (Covid-19) стало примусове соціальне дистанціювання. Тому дистанційне навчання в вищих навчальних закладах набуло особливого значення. Екстремальний перехід вищої освіти в дистанційний режим в умовах пандемії створив унікальну ситуацію, при якій цифрові технології виявилися єдино можливими для використання в обставинах, що склалися. Перед професорсько-викладацьким складом було поставлено надскладне завдання – забезпечити реалізацію освітніх програм в повному обсязі. Кожному викладачеві довелося її вирішувати з урахуванням специфіки своєї навчальної дисципліни.

Найбільшу популярність отримали LMS-платформи для розміщення контенту і перевірки знань студентів, вебінарні сервіси для онлайн-лекцій і консультацій, соціальні мережі і месенджери для комунікації студентів і викладачів, і розсилки по електронній пошті для доставки контенту.

Технічні аспекти використання дистанційних освітніх технологій не викликали у студентів труднощів.

Разом з тим швидкий перехід на онлайн-навчання виявив певні проблеми. Це насамперед нерівність технічних можливостей, а саме оснащеності комп'ютерною технікою і доступом в інтернет. Також екстрений перехід до навчання в дистанційному форматі продемонстрував неготовність деяких учасників освітнього процесу до впровадження і сприйняття нетрадиційних цифрових методів навчання.

Суттєво збільшилось навантаження як на студентів, так і на викладачів. Ізоляція значно зменшила можливість очних комунікацій учасників освітнього процесу і знизила прямий виховний вплив в процесі освіти.

Наслідком зазначених проблем стало певною мірою деяке «спрощення» освітнього процесу. Усе вищезазначене в підсумку може негативно відбитися на формуванні професійних компетенцій, на розвиток яких направлено освоєння певної навчальної дисципліни. Тому вважається доцільним застосовувати змішаний формат навчання.

УДК 004.912
Анпілогов Д.І.
канд. техн. наук, доц. НУ «Запорізька політехніка»

ПРО ВИПРАВЛЕННЯ ОДНІЄЇ ПОМИЛКИ В MOODLE

Сьогодення в умовах пандемії ставить задачу подальшого розвитку дистанційних технологій, зокрема, з використанням системи дистанційного навчання (СДН) Moodle [1].

Автором виконано роботу по створенню банку задач з курсу вищої математики для студентів інженерно-технічних спеціальностей з дотриманням таких вимог: тематика задач охоплює повний курс відповідно до діючої програми; завантаження додаткових графічних файлів не є потрібним; завдання розподілені між категоріями (зручно створювати тематичні тести); банк експортовано у форматі Moodle XML (обмін банком між курсами різних викладачів стає надзвичайно легким).

При створенні банку активно використовувався проект MathJax [2], який за замовчуванням підключений до курсів СДН Moodle (Керування курсом – фільтри – MathJax: Типово (Увімкнуто)). Завдяки цьому стає можливим використання відомої [3, 4] і зручної нотації TeX.

Але при верстанні оточення «matrix» вбудований редактор Moodle (Текст питання – Показати/приховати додаткові кнопки – Редактор формул – вкладка «Додаткове») здійснює макропідстановку

\(\left| \begin{matrix} a_1 & a_2 \ a_3 & a_4 \end{matrix} \right| \)

при візуалізації якої браузер видає помилку. Справа полягає в порушенні синтаксису названого оточення (невірний формат кінця рядка). Додавання ще одного прямого слешу з перетворенням формату оточення до вигляду

\(\left| \begin{matrix} a_1 & a_2 \\ a_3 & a_4 \end{matrix} \right| \)

усуває помилку і веде до коректного відображення оточення «matrix». Його тепер легко модифікувати для верстання довільних матриць і систем.

Автор сподівається, що зроблене зауваження допоможе подальшій популяризації системи TeX та проекту MathJax, і відповідно, СДН Moodle.

Висновки. Створено банк задач курсу «Вища математика» у форматі Moodle XML з використанням підтримки сервісу MathJax. Виявлено помилку редактора формул СДН Moodle і надано спосіб її усунення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Система дистанційного навчання НУ «Запорізька політехніка» [Електронний ресурс]. – Режим доступу : https://moodle.zp.edu.ua/

2. Beautiful and accessible math in all browsers [Електронний ресурс]. – Режим доступу : https://www.mathjax.org/
3. MiKTeX project [Електронний ресурс]. – Режим доступу : https://miktex.org/
4. Using TeX Notation [Електронний ресурс]. – Режим доступу : https://docs.moodle.org/310/en/Using_TeX_Notation

УДК 378.14
Коротунова О.В.[1], Нечипоренко Н.О. [2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

ПРОБЛЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ ВИЩОЇ МАТЕМАТИКИ В ТЕХНІЧНОМУ УНІВЕРСИТЕТІ

Сучасний етап розвитку вищої освіти характеризується впровадженням та розповсюдженням інформаційно-комунікаційних технологій, серед яких важливе місце займає дистанційне навчання. Математична підготовка студентів технічних спеціальностей повинна сприяти розвитку здібностей щодо застосування математичних методів для вирішення прикладних завдань. Вивчення вищої математики передбачає виконання великої кількості конкретних задач з метою вивчити основні методи та оволодіти впевненими навичками їх розв'язання.

Крім того, вивчення вищої математики вимагає досить глибоких і тривалих роздумів над основними поняттями та їх взаємозв'язками. Отже, робота з викладачем або під його безпосереднім керівництвом з вивчення фундаментальних наук залишається поки основним варіантом. Створення якісних методичних матеріалів для дистанційних курсів є досить складним і трудомістким процесом. Курс повинен бути простим і зрозумілим, щоб студенти освоїли основні ідеї та методи дослідження. Особливістю вищої математики є високий ступінь абстракції інформації, що вимагає значного напруження розумової діяльності. Слабка математична підготовка сучасних школярів ускладнює самостійну роботу деяких студентів з цієї дисципліни.

Разом з тим, використання дистанційних освітніх технологій сприяє більш гнучкому, динамічному і персоналізованому навчанню. Студенти постійно контактують з викладачем на лекціях, практичних заняттях і консультаціях. Отримують додатковий мультимедійний матеріал. Виконують завдання та проходять контроль в LMS Moodle.

Проте питання про ступінь самостійності виконання домашніх і контрольних завдань при дистанційному навчанні вищої математики залишається одним з основних. Для підтримки мотивації навчання вищої

математики слід передбачити можливість вибору студентами різного рівня підготовки відповідних за складністю та обсягом вправ і завдань. Для виконання отриманих завдань деяким студентам можливо дозволити застосування сучасних пакетів комп'ютерної математики. Добре підготовленим студентам прикладні математичні пакети слід рекомендувати для занять студентською науково-дослідною роботою по застосуванню прикладної математики в задачах своєї майбутньої спеціальності. Вони можуть модифікувати існуючі програми і алгоритми і застосовувати їх для розв'язання конкретних завдань. Отримані результати представляються у вигляді наукових робіт на студентських конференціях.

Наукове електронне видання

Можна використовувати в локальному та
мережному режимах

ТИЖДЕНЬ НАУКИ-2021. Факультет радіоелектроніки та телекомунікацій

Збірник тез доповідей щорічної
науково-практичної конференції викладачів, науковців,
молодих учених, аспірантів та студентів
19–23 квітня 2021 року

Один електронний оптичний диск (DVD-ROM);
супровідна документація.
Тираж 100 прим. Зам. № 343

Видавець і виготовлювач
Національний університет «Запорізька політехніка»
Україна, 69063, м. Запоріжжя, вул. Жуковського, 64
Тел.: (061) 769–82–96, 220–12–14

Свідоцтво суб'єкта видавничої справи 6952 від 22.10.2019
ISBN 978-617-529-263-1