НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ МОЛОДИХ УЧЕНИХ

Актуальні проблеми інформаційних технологій

APIT

20 грудня 2019 року

МІНІСТЕРСТВО ОСВІТИ І НАКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ МОЛОДИХ УЧЕНИХ

«Актуальні проблеми інформаційних технологій»

20 грудня 2019 року

Матеріали доповідей

Київ 2019

ЗМІСТ

ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ

УДК 004.735
[1] **А.С. Дуднік**
Доктор технічних наук, доцент, доцент кафедри мережевих та інтернет технологій
[2] **І.К. Кобернюк**
Магістрант
[1] Київський національний університет імені Тараса Шевченка, м. Київ
[2] Міжрегіональна академія управління персоналом, м.Київ

РОЗРОБКА РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНО-НАВІГАЦІЙНОЇ СИСТЕМИ ДЛЯ ДИСПЕТЧЕРСЬКОГО ЦЕНТРУ АВТОТРАНСПОРТНОГО ПІДПРИЄМСТВА

У даному дипломному проекті представлені результати розробки розподіленої інформаційно-навігаційної системи (далі по тексту AVL системи) диспетчерського центру автотранспортного підприємства, що виконує збір, обробку, відображення та збереження даних, отриманих від апаратури автотранспортних засобів, а також забезпечує підвищену точність визначення координат автотранспортних засобів. Перший розділ присвячений аналізу застосування навігаційних технології у сучасних AVL системах, а також розгляду представлених на українському ринку розробок таких систем з метою оцінки їх функціональних можливостей, переваг і недоліків.

У другому розділі проведений аналіз існуючих технологій місцевизначення рухомих об’єктів, зокрема з використанням супутникових навігаційних систем (СНС), описані фактори, що впливають на точність місцевизначення об’єктів, а також наведені рекомендації щодо реалізації в AVL системах відносно-диференційного методу для забезпечення достатньо високої точності визначення координат об’єктів у складних експлуатаційних умовах.

У третьому розділі було проведено проектування і розробку програмного забезпечення AVL систем, зокрема обґрунтовано структуру системи і вимоги до апаратного забезпечення, розроблені алгоритми функціонування окремих програмних модулів, обрано мову програмування і СУБД, з використанням яких створено тестовий варіант програмного забезпечення для АРМ диспетчера AVL системи.

У четвертому розділі наведені розрахунки щодо економічної ефективності розробки і комерційної експлуатації даної AVL системи.

Список використаних джерел

1. Баранов Г.Л. Диспетчерські системи класу AVL по управлінню перевезеннями із застосуванням супутникових технологій // Системні методи керування, технологія та організація виробництва, ремонту і експлуатації автомобілів. Застосування супутникових технологій у транспортній галузі. - К.: НТУ, ТАУ. - 2012. - С.18 - 23.

УДК 004.728.3.057.4
[1] **А.С. Дуднік**
Доктор технічних наук, доцент, доцент кафедри мережевих та інтернет технологій
[2] **М.В. Мельниченко**
Магістрант
[1] *Київський національний університет імені Тараса Шевченка, м. Київ*
[2] *Міжрегіональна академія управління персоналом, м.Київ*

ОСОБЛИВОСТІ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ УПРАВЛІННЯ КОМП'ЮТЕРНОЮ МЕРЕЖЕЮ НА КАНАЛЬНОМУ РІВНІ ЕТАЛОННОЇ МОДЕЛІ OSI

Не можливо уявити майбутнє без застосування нових і вже існуючих мережних і телекомунікаційних технологій. Глибокі зміни в техніці зв’язку та обчислювальній техніці підводять нас до нової епохи - інформатизації суспільства й створення глобальної інформаційної інфраструктури (ГІІ). Ця інфраструктура дає змогу надавати користувачам набір комунікаційних послуг, які забезпечують відкриту множину допоміжних програмних продуктів, що охоплюють усі види інформації й можливість її одержання у будь-який час, в будь якому місці, за прийнятною ціною і з високою якістю.

Кінцевою метою ГІІ є гарантія доступу кожному громадянину до інформаційного співтовариства. Основою ГІІ є інформаційна мережа, що з’явилася внаслідок інтеграції мереж зв’язку та мереж ЕОМ. На базі цієї інтеграції розроблено концепцію інтелектуальної мережі (ІМ).

Кінцеві пристрої візуального відображення даних є придатними для більш ніж одного виду інформації. І, нарешті, мережа зв'язку дає змогу передавати мовну, текстову інформацію, дані і зображення через те саме з'єднання: користувач одержить доступ до цієї мережі незалежно від виду служби через «штепсельну розетку зв'язку». За допомогою цих засобів були значно збільшені продуктивність праці та економічна ефективність як окремих людей, так і цілих організацій. Можна зробити висновок, що об'єднання зусиль трьох галузей промисловості - комп'ютерної індустрії, побутової радіоелектроніки і електрозв'язку - наблизило досягнення основної мети - створення глобальної інформаційної інфраструктури (ГІІ) .

Список використаних джерел

1. Стеклов В.К., Беркман Л.Н. Проектування телекомунікаційних мереж: Підручник для студентів вищ. навч. закладів за напрямком „ Телекомунікації” /за ред. В.К.Стеклова.-К.: Техніка, 2012.-792 с.

2. Калита Д. М. Комп`ютерні мережі. Апаратні засоби та протоколи передачі даних. - К.: Видовничо-поліграфічний центр „Київський Університет”, 2013. - 327 с.

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

УДК 004.51

[1] **С.В.Поперешняк**
Доцент, кандидат фізико-математичних наук кафедри програмних систем і технологій факультету інформаційних технологій
[1] **Д.С.Коротін**
Студент 4 курсу кафедри програмних систем і технологій факультету інформаційних технологій
[1] *Київський національний університет імені Тараса Шевченка*
м. Київ, Україна

СУЧАСНІ ПІДХОДИ ЩОДО МОДЕЛЮВАННЯ ЗАСТОСУВАННЯ ОБ'ЄКТНОЇ МОДЕЛІ ВЗАЄМОДІЇ DSP-SSP СИСТЕМ ЧЕРЕЗ AD EXCHANGE

У дослідженні проведено аналіз взаємодії DSP-SSP систем через Ad Exchange [1]. За результатами проведеного аналізу сформовано мету наукового дослідження, яка полягає в тому, що на основі удосконаленої методики застосування об'єктної моделі взаємодії систем DSP-SSP провести моделювання та обґрунтувати доцільність використання реалізованих платформ для автоматизації купівлі та продажу медіа контенту на світовому ринку [2].

Для досягнення поставленої мети було з'ясовано, що Ad Exchange є посередником між DSP та SSP платформами і реалізує модуль один до багатьох [1]. Визначено, що така система дає можливість працювати на цифровому ринку, де видавці та рекламодавці збираються разом для торгівлі цифровими рекламними ресурсами [3].

Зроблено висновок, що Ad Exchange – автономна платформа, яка полегшує і спрощує програмну покупку оголошень.

Авторами представлено модель роботи системи Ad Exchange, вказані її переваги та недоліки. Запропоновано удосконалену методику використання об'єктної моделі взаємодії DSP-SSP систем через Ad Exchange. Визначено, що важливою складовою для реалізації даної методики є Аналітика, яка була реалізована на DSP платформі, де клієнт може слідкувати за важливими коефіцієнтами виграшу, кліків тощо [2, 4]. Ad Exchange є інструментом для автоматизації процесу купівлі та продажу Інтернет контенту з можливістю отримувати більший заробіток та економити час на здійснення операцій [2, 3]. Розроблені авторами рекомендації відстежують неякісні пропозиції і борються з ризиками.

За рахунок включення блоку Validator удосконалено відомий алгоритм роботи DSP, SSP. На основі представленої моделі здійснено моделювання, де реалізовано блок Validator, рис.1 [5-7].

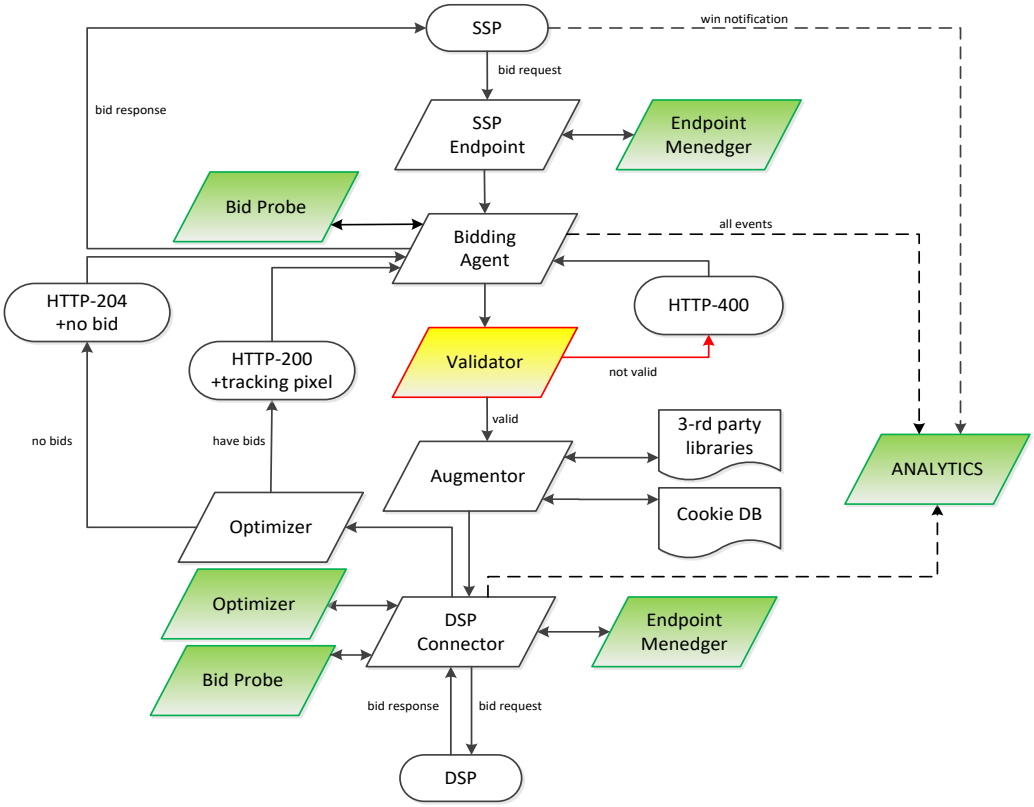


Рис. 1 – Модель роботи системи Ad Exchange

Зроблено висновок, що найважливішою складовою цієї моделі є вперше запропонований авторами блок Validator, який виставляє рекламу лише для встановленого певного контингенту людей. Реалізований в моделі Validator є основною перевагою представленої системи над іншими.

Список використаних джерел

1. DSP, SSP и Ad exchange – что это такое и как они все дружат? [Електронний ресурс]. – Реклама: культурный контекст / Ред. Т.Э. Гринберг, М.В. Петрушко. – М.: РИП-Холдинг, 2004. – 186 с.

2. Ad Exchange: краткое руководство и что нужно знать издателям. [Електронний ресурс] – Ресурс доступу: http://programmatic.com.ua /2017/09/ad-exchange-kratkoe-rukovodstvo-chto-nyzhno-znat-publisher/.

3. Сервер Ad Exchange – не как у других. [Електронний ресурс]. – Ресурс доступу: https://habr.com/ru/company/maxilect/blog/421471/.

4. Deep Reinforcement Learning for Sponsored Search Real-time Bidding. [Електронний ресурс] – Ресурс доступу: https://arxiv. org/pdf/1803.00259. pdf.

5. Budget Constrained Bidding by Model-free Reinforcement Learning in Display Advertising. [Електронний ресурс] – Ресурс доступу: https://arxiv.org/pdf/1802.08365.pdf.

6. Real-Time Bidding with Multi-Agent Reinforcement Learning in Display ресурс] – Ресурс доступу: https://arxiv.org/pdf/1802.09756.pdf.

7. Targeted advertising. [Електронний ресурс] – Ресурс доступу: https://en.wikipedia.org /wiki/Targeted_advertising.

УДК 005.8:005.41
[1] **І.І.Ізотов**
Студент 4 курсу кафедри мережевих та інтернет технологій факультету інформаційних технологій
[1] **А.В.Демченко**
Студент 4 курсу кафедри мережевих та інтернет технологій факультету інформаційних технологій
[1] *Київський національний університет імені Тараса Шевченка, м.Київ*

ГІПЕРКОНВЕРГЕНТНІ СИСТЕМИ

Що таке гіперконвертована інфраструктура? Гіперконвертована інфраструктура (HCI) поєднує загальне обладнання для обробки даних, використовуючи місцеві ресурси зберігання, та інтелектуальне програмне забезпечення для створення гнучких будівельних блоків, які замінюють застарілу інфраструктуру, що складається з окремих серверів, мереж зберігання даних та масивів зберігання даних. Переваги включають нижчий рівень TCO, підвищення продуктивності та підвищення продуктивності роботи в IT-командах.

Народження гіперконвертованої інфраструктури.

З веб-вибухом 90-х років було введено інфраструктуру з серверною мережею SAN та мережами зберігання даних, яка містить незалежні модулі, які можна оновлювати чи змінювати, не впливаючи на інші шари. Ця інфраструктура революціонізувала IT-відділи і застосовується з тих пір.

Але зараз, в епоху гібридної хмари, 3-х рівневий вже не може йти в ногу з потребами в IT. Це складний, непростий, не дає міцної основи для DevOps і не може масштабуватись з величиною, якою раніше був.

Сьогодні HCI - це інфраструктура вибору для компаній, які хочуть залишатися конкурентоспроможними та забезпечити, щоб їх центри обробки даних були готовими до хмар.

Як працює гіперконвертована інфраструктура? HCI конвертує весь стек центру обробки даних, включаючи обчислення, зберігання, мережу зберігання даних і віртуалізацію. Складна і дорога застаріла інфраструктура замінюється платформою, що працює під ключ, на стандартних галузевих серверах, які дозволяють підприємствам запускати та масштабувати один вузол за раз. Програмне забезпечення, що працює на кожному вузлі сервера, поширює всі операційні функції по кластеру для кращої продуктивності та стійкості. Компоненти гіперконвертованої інфраструктури. HCI складається з двох основних компонентів, розподіленої площини та площини управління. Розподілена площина пролягає через кластер вузлів, що надають послуги зберігання, віртуалізації та мереж для гостьових додатків - будь то VM або контейнерні програми. Площина управління дозволяє вам легко адмініструвати ресурси HCI з одного місця та з одного виду і виключає потребу в окремих рішеннях для управління серверами, мережами зберігання даних та віртуалізацією [2].

Практично всі сучасні гіперконвертовані інфраструктурні рішення визначені на 100% програмним забезпеченням, не залежно від власного обладнання. Кожен вузол HCI в кластері працює гіпервізором (Nutanix AHV, VMware ESXi або Microsoft Hyper-V), а функції управління HCI працюють як окрема віртуальна машина на кожному вузлі, утворюючи повністю розподілену тканину, яка може масштабувати ресурси за допомогою додатка нових вузлів [3].

Переваги гіперконвертованої інфраструктури.

Переваги переходу від складної застарілої інфраструктури до простоти гіперконвергенції багато, але серед основних причин, за якими організації перемикаються, - це нижчі витрати, поліпшення, стабільна продуктивність, менший набір центрів обробки даних, більша ефективність та продуктивність в IT-командах та максимальна інфраструктура ROI. Інфраструктура під ключ. Інтегровані ресурси сервера, зберігання, мереж та віртуалізації, а також можливості управління системою та управління операціями. Швидке розгортання. Розгортайте інфраструктуру за лічені хвилини, щоб IT-команди могли зосередити свою увагу на додатках та послугах, що живлять бізнес. 100% програмне забезпечення. Підтримує широкий спектр різних апаратних платформ - включаючи три з чотирьох найпопулярніших серверних платформ у світі. Платформа світового класу [4]. Кожен гіперконвертований сервер (вузол) включає в себе апаратне забезпечення x86, що працює на базі флеш-накопичувачів та традиційні жорсткі диски, а також програмне забезпечення Nutanix. Чудова продуктивність та стійкість. Гіперконвергентне програмне забезпечення Nutanix, що працює на кожному вузлі, розподіляє всі операційні функції по кластеру. Безпрецедентна гнучкість. Один кластер може мати необмежену кількість вузлів, причому типи вузлів мають різну кількість пам’яті, процесора та пам’яті, тому ви можете запускати кілька робочих навантажень з максимальною ефективністю [1].

Список використаних джерел

1. What is hyperconverged infrastructure? – Ресурс доступу: https://www.nutanix.com/hyperconverged-infrastructure

2. What is hyperconvergence? – Ресурс доступу: https://www.networkworld.com/article/3207567/what-is-hyperconvergence.html

3. What is Hyperconverged Infrastructure? – Ресурс доступу: https://www.vmware.com/products/hyper-converged-infrastructure.html

4. Hyperconverged Infrastructure – Ресурс доступу: https://www.datacore.com/hyperconverged-infrastructure/

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ В ОСВІТІ, ЕКОНОМІЦІ ТА ОБОРОНІ

УДК 629.73:623.55.028
[1] О.І. Тимочко
доктор технічних наук, професор, професор кафедри повітряної навігації та бойового управління авіацією
[1] О.О. Арословкін
ад'юнкт
[1] А.В. Самокіш
ад'юнкт
[1]Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків

УДОСКОНАЛЕННЯ ПРОЦЕСУ НАВЕДЕННЯ НА НАЗЕМНІ (МОРСЬКІ) ЦІЛІ ПО МАЛОІНФОРМАТИВНИМ ОРІЄНТИРАМ

При візуальному виводі літальних апаратів (ЛА) передовим авіанавідником на цілі в умовах підстилаючої поверхні з однорідними текстурами (ліс, пустеля, водна поверхня), можна виділити ряд факторів, що необхідно врахувати в процесі управління:

1. Зміна спостережуваних характеристик орієнтирів при зміні умов спостереження (день-вечір, освітленість підстилаючої поверхні та т.п.), Що призводить до збільшення помилок виявлення орієнтирів.

2. Функціонування в умовах малоінформативного поля, зокрема, коли ЛА може опинитися поза областю спостереження досить інформативного орієнтира.

Наявність зазначених проблем істотно зменшує ефективність наведення авіації. Спроби вирішення цього завдання тільки візуальними методами наведення, коли в межах досяжності екіпажу ЛА не має достатньо інформативних орієнтирів, фізично не реалізоване.

Розглянемо деякі ситуації, пов'язані з невиявленням орієнтира:

- відсутність орієнтира на спостерігаючій поверхні;
- помилка його виявлення (пропуск цілі).

Для вирішення завдань наведення в кожній із зазначених ситуацій можуть застосовуватися різні підходи:

1. Продовження пошуку з розширенням (зміною) області пошуку.

2. Заміна об'єкта пошуку-перехід до пошуку інших орієнтирів.

3. Пошук шуканого орієнтира зі зміною умов спостереження, наприклад, зі зміною висоти польоту або ракурсу спостереження.

4. Пошук шуканого орієнтира за допомогою нового (наприклад, доповненого) робочого словника ознак (альтернативний набір ознак).

Вибір орієнтирів для вирішення поставлених завдань ґрунтується на оцінці його інформативності.

Для оцінки інформативності орієнтирів і їх ознак взято за основу прийняту міру інформації за Шенноном:

$$I = I(X|Y) = H(X) - H(X|Y), \quad (1)$$

де: $I(X|Y)$-кількість інформації, що міститься в повідомленні Y про подію X ;

$H(X)$-ентропія події X;

$H(X|Y)$-умовна ентропія X при отриманні повідомлення Y.

Оцінка інформативності орієнтирів дозволяє враховувати їх унікальність, а також ймовірність виявлення орієнтира і ймовірність виходу екіпажу ЛА в область, яка містить орієнтир.

Якщо зазначені способи управлінь не призводять до успішного вирішення поставленого завдання наведення, то пропонується перейти до наведення за малоінформативними орієнтирами. Під аналізом ситуацій будемо розуміти формування опису спостерігаючої поверхні, зокрема малоінформативних орієнтирів, і відносин між ними. Подібні описи дозволять розширити коло вирішуваних завдань наведення екіпажів ЛА, підвищити ефективність спостережень в складних, невизначених і змінюваних умовах.

Ймовірність рішення завдання в такому випадку прийме такий вигляд (з урахуванням умови $P(X_{вияв})=1$).

$$P(X_{нав})=1-\Pi_{n=1}^{N}(1-P(X_{нав}|X_{вп}))*(1-P(X_{нав}|X_{відн})), \quad (2)$$

де: $P(X_{нав}|X_{вп})$-ймовірність визначення положення із заданою точністю при виявленні орієнтира $X_{вп}$, $n \in N$;

N –кількість малоінформативних орієнтирів на ділянці місцевості;

$P(X_{нав}|X_{відн})$-ймовірність визначення положення із заданою точністю за умови опису відносин між орієнтирами.

Очевидно, що зі збільшенням кількості спостережуваних малоінформативних орієнтирів ймовірність $P(X_{нав})$ буде зростати.

У роботі розглянута робота передового авіанавідника при наведенні авіації на наземні (морські) цілі та вибір орієнтирів в умовах малоінформативної поля. Результати роботи показали, що для ведення бойових дій в умовах малоінформативного поля необхідно удосконалювати процес підготовки авіанавідника по розпізнаванню ознак інформативності. На теперішній час це можна зробити шляхом автоматизації процесу підготовки авіанавідника використовуючи нечіткі множини 2-го типу для методу та алгоритму описів спостерігаючої поверхні на малоінформативній місцевості, що дозволить уникнути недоліки хибного виявлення орієнтирів або їх невиявлення.

Список використаних джерел

1. Наведення літаків на повітряні та наземні цілі: навч. пособ. / В.Г. Чернов, В.А. Волобуєв, О.К. Желем. – ХУПС, 2004. – 131 с.

3. Петрушенко Н.Н. Особенности измерения дальности целей, лоцируемых под малыми углами места над морем / Н.Н. Петрушенко, О.Б. Котов, В.Д. Карлов, Е.А. Меленти // Тези доп. Восьмої наук. конф. ХУПС – Х.: ХУПС, 2012. – С. 293.

УДК 005.8:005.41
[1] **О.Ю. Герасименко**
Асистент кафедри мережевих та інтернет технологій
[1] **В.Р. Бокань,**
Студент
[1] **О.В. Федорчук**
Студент
[1] Київський національний університет імені Тараса Шевченка, м.Київ

ПЕРСПЕКТИВИ РОЗВИТКУ ТА ВИКОРИСТАННЯ МОБІЛЬНИХ ПЛАТЕЖІВ НА ОСНОВІ БЛОКЧЕЙН

Завдання полягає у вивченні перспективи використання мобільних платежів із суміжною технологією блокчейн на основі розподіленої платіжної системи Ripple.

Актуальність даної роботи полягає у вивченні ефективного способу рішення цілого ряду проблем проведення традиційної операції мобільних платежів, а саме проблеми безпеки мобільних платежів, онлайн-покупок, подвійні витрати, шахрайство, ціноутворення та інші.

Метою роботи полягає здійснення аналізу використання технології блокчейн у мобільних платежах та узагальнення на основі цього перспектив її розвитку та використання у сучасних системах.

Завдання, поставлені в ході дослідження:

1. Провести аналіз традиційних систем здійснення мобільних платежів без використання блокчейн та Ripple.
2. Вивчити принцип роботи технології блокчейн та з’ясувати можливі застосування у Ripple.
3. Дослідити як впровадження блокчейну впливає на роботу системи проведення платежів.
4. Виявити перспективи розвитку та використання блокчейну у мобільних платежах.

У даній роботі був використаний теоретичний метод дослідження, а саме вивчення, аналіз наукової роботи та методичної літератури по цій темі.

Представлені результати містять значний обсяг змістовної інформації та ґрунтовні підвалини для розробки й упровадження практичних дій як на національному рівні, так і на рівні окремих регіонів та конкретних підприємств.

Ми з'ясували, що хоч і новотехнологічні мобільні платіжні системи більш безпечніші ніж традиційні, але вони також мають проблеми з безпекою. Але використання платіжних систем на основі технології блокчейн підвищує безпеку транзакцій та підтвердження їх дійсності.

Результатом проекту є висновок, що прийняття розподілених мереж, таких як Ripple, може допомогти банківській галузі реалізувати більш швидку обробку

платежів, а також підвищити ефективність глобальних платежів і кореспондентських банківських послуг. Хоча цей метод вважається менш безпечним від технології блокчейн, але має свої переваги у швидкості транзакцій.

Список використаних джерел

1. Global Payments Should Be Easy [Електронний ресурс] — Режим доступу: https://www.ripple.com/
2. Mobile Payment [Електронний ресурс] — Режим доступу: https://www.investopedia.com/terms/m/mobile-payment.asp
3. Mobile Payments And Why Blockchain Is Changing The World [Електронний ресурс] — Режим доступу: https://blog.goodaudience.com/mobile-payments-and-why-blockchain-is-changing-the-world-c3c58dc19211
4. What in the world is blockchain? [Електронний ресурс] — Режим доступу: https://www.mobilepaymentstoday.com/articles/what-in-the-world-is-blockchain/
5. Mobile wallets need blockchain for the next stage [Електронний ресурс] — Режим доступу: https://www.paymentssource.com/opinion/mobile-wallets-need-blockchain-for-the-next-stage
6. What Is Ripple. Everything You Need To Know [Електронний ресурс] — Режим доступу: https://cointelegraph.com/ripple-101/what-is-ripple

УДК 005.8:005.41
[1] **Ю.В.Кравченко**
Доктор технічних наук, професор, професор кафедри мережевих та інтернет технологій
[1] **А.Ю.Толстокорова**
Студентка
[1] **Я.С.Кірєєв**
Студент
[1] Київський національний університет імені Тараса Шевченка, м.Київ

ПЕРСПЕКТИВИ РОЗВИТКУ ОСВІТИ ЗА ДОПОМОГОЮ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

Зі збільшенням знань та технологічного прогресу суспільства, наша країна вимагає навичок навчання, які могли б допомогти їй йти в ногу з розвитком науки і техніки. Освіта в двадцять першому столітті - це центр, з якого виникають усі зміни та події. Інформаційні технології в освіті потребують культури. Цю культуру потрібно вивчити разом із використанням апаратних ресурсів. Що таке інформаційні технології [1]. Важливість та роль інформаційних технологій у навчанні [2] [3]. Роль інформаційних технологій в освіті малорозвинених країн [4]. Використання сучасних інформаційних технологій в освіті України [5]. ІТ та необхідність зміни освіти [6]. Сучасні, помірні та прості технології сучасної світової освіти.

Список використаних джерел

1. Дж. Генсон та Р. Румана Нові технології зв'язку в країнах, що розвиваються [Видавництво: Lawrence Erlbaum Associates] / Місце видання: Hillsdale, NJ. - 1990 рік.

2. Т. Нельсон і Г. Кух Студентський досвід з інформаційними технологіями та їх зв'язок з іншими аспектами залучення студентів [Документ, представлений на щорічному засіданні асоціації з інституційних досліджень] / 30 травня, червень 32004; Бостон. MA, - 2004.

3. Г.Бошамп та Дж. Паркінсон Ставлення Публіса до шкільної науки, коли вони переходять із багатої ІКТ початкової школи до середньої школи з меншою кількістю ресурсів ІКТ: Чи важливі ІКТ? [Електронний ресурс] // 3 січня 2008 року # Springer science + Бізнес-медіа, LLc 2007.

4. W.J.Stover. Інформаційні технології в третьому світі // Боулдер, штат Колорадо, - 1984 рік

5. Хомішин І. Ю. Сучасні інформаційні технології в освіті. ІТ-право: проблеми та перспективи розвитку в Україні: [збірник науково-практичних конференцій] (Львів, 18 листопада 2016 р.). Львів: НУ «Львівська політехніка», 2016. С. 151–153.

6. А. Кірквуд і Л. Ціна. Учні та навчання в двадцять першому столітті. Вища освіта т., 30.НО, 3. червня 2005 р., с.257-274.2005. F. Hamidi та ін. / Procedia Computer Science 3 (2011) 369–373 373

СИСТЕМИ ТА МЕТОДИ ЗАХИСТУ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

УДК 005.8:005.41
[1] **Ю.В.Кравченко**
Професор
[1] О.А.Перцюх
Студент
[1] В.А.Цикун
Студент
[1] М.Д.Рогачов
Студент
[1] П.С.Грищук
Студент
[1] Київський національний університет імені Тараса Шевченка, м.Київ

ОРГАНІЗАЦІЙНІ ЗАСАДИ УПРАВЛІННЯ ПРОГРАМАМИ ІНФОРМАТИЗАЦІЇ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

Сумна статистика наглядно демонструє, що абсолютна більшість компаній та установ, в тому числі державних, мають критичні уразливості в своїй мережевій інфраструктурі, що є неприйнятним фактом для сучасної структури, та не рідко виливається в серйозні, а іноді, катастрофічні наслідки, причому не тільки для власників структур, а і для їх клієнтів та сторонніх осіб[1].

Вічна боротьба систем захисту та систем взлому ще ніколи в історії не була настільки комплексною, інтелектуальною та багатофакторною. Світові тенденції в сфері кібербезпеки диктують життєву необхідність у перманентній готовності до атак, що є неможливим без постійної актуалізації своїх знать, навичок та методів боротьби. Тут виникає ще один нюанс — неможливо будувати захист спираючись лише на теорію, потрібно перевіряти інфраструктуру на практиці. Адекватним методом таких перевірок і є аудити, спираючись на які я буду розписувати сучасні системи захисту з їх уразливостями та перспективами розвитку.[2]

Хотілося б окремо звернути увагу на ту частину систем безпеки, якою, як правило, нехтують: соціальна сторона проблеми. Як кажуть профільні фахівці, 90% уразливостей ліквідуються 10% необхідних зусиль, і левову долю в цих 90% уразливостей складає саме людський фактор. Банальне незнання азів кібербезпеки призводить до того, що навіть інфраструктури, в яких відсутні серйозні типи уразливостей, роблять фатальні проблеми самостійно, зсередини структури.[3]

Список використаних джерел

1. 1.Raef Meeuwisse: Cybersecurity for beginners - / Raef Meeuwisse// Cybersecurity general course - 2015. - Вид.2. - С. 46-82.

2. Cisco netacad courses: CyberOps Chapter 3. [Електронний ресурс] - 2019. Chapter 3

3. Helen Wong: Cyber Security: Law and Guidance - / Helen Wong// Cybersecurity course - 2016. - Вид.1. - С. 31-69.

УДК 681.324
[1] Труш О.В..,
к.т.н., доцент
[2] Хмара Б.О.,
магістрант
[2] Личко Ю.В.
магістрант
[1]Київський національний університет імені Тараса Шевченка
[2]Одеська національна академія зв'язку імені О. Попова

ТЕХНОЛОГІЯ ОЦІНЮВАННЯ СТАНУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ WEB -САЙТІВ В УМОВАХ ВПЛИВУ АКТУАЛЬНИХ ЗАГРОЗ І УРАЗЛИВОСТЕЙ

Рівень інформатизації та розвитку інформаційних технологій, а також та сучасні вимоги правових актів, нормативних документів (НД) в галузі захисту інформації та правил щодо захисту інформації, яка є власністю держави, вимагають забезпечення організаційно-технічних заходів щодо захисту державної інформації, яка публікується в глобальних мережах (в т.ч. Інтернет), а саме створення комплексної системи захисту інформації (КСЗІ) в автоматизованих системах призначених для розміщення та публікації контенту WEB-сторінки державної установи.

КСЗІ WEB-сторінки – це сукупність організаційних і інженерно-технічних заходів, програмно – апаратних засобів, які забезпечують захист інформації WEB-сторінки у відповідності до нормативно-правових документів в галузі захисту інформації, та дозволять розміщувати та обробляти в АС.

Завдання на оцінювання стану захищеності ІР в умовах впливу загроз і уразливостей відносяться, як відомо, до класу багатокритеріальних. Для їх колегіального рішення в умовах невизначеності і конфлікту серед існуючих методів математичного моделювання, методів формування та дослідження узагальнених показників якості з використанням графоаналітичного і ним подібних підходів, експертних методів вирішення складних завдань оцінювання та вибору будь-яких об'єктів, в тому числі спеціального призначення, а також аналізу та прогнозування ситуацій з великою кількістю значимих факторів, найбільш раціональними і визначальними є саме експертні методи. Вони дають можливість більш глибоко вивчити явища, які істотно впливають на рівень захищеності як держави в цілому, так і окремих об'єктів її інформаційної та кіберінфраструктури від впливу внутрішніх і зовнішніх кібервтручань та загроз, виявити найбільш важливе та істотне у цих процесах, не опускаючи тих деталей і взаємозв'язків, без яких не може бути побудована модель досліджуваної ситуації. Підвищенню ефективності застосування експертних методів як правило сприяє:

- проведення обґрунтованого добору групи висококваліфікованих експертів, діяльність яких пов'язана з проведенням досліджень за обраними для

проведення експертизи напрямами й посади яких відповідають вимогам до таких у обраній галузі знань;
- своєчасне ознайомлення експертів з метою дослідження та пояснення їм змісту роботи, яку вони повинні виконати;
- проведення процедури анкетування експертів з урахуванням усіх особливостей конкретного завдання;
- проведення експертизи кожного заходу із забезпечення ІБ держави або окремих об‘єктів її інфраструктури відносно визначених вимог за встановленими індикаторами та відповідними їм показниками.

Враховуючи значне поширення відомих методів експертного оцінювання, що дозволяють безпосередньо використовувати судження та інтуїцію експертів у будь-якій формалізованій структурі для вирішення завдань ми отримали метод анкетування. Як вихідні дані будемо використовувати сформовану за еталонною вибіркою актуальних загроз множину пар — загроза - уразливість та множину показників (критеріїв) існуючих загроз, що характеризують можливість порушення конфіденційності, цілісності, доступності та спостережності інформації. Рішення даної задачі зводиться до визначення індексу захищеності інформаційних ресурсів та обчислення комплексного показника, що характеризує стан їх захищеності. Індекс захищеності ІР вважатимемо динамічною кількісно-якісною характеристикою, яка вказує на здатність організації забезпечити власну ІБ та підтримувати безпечне функціонування об‘єктів їх інформаційної структури в умовах існуючих загроз інформаційним ресурсам. Його визначення здійснюється на підставі виявлення відхилень від штатного режиму функціонування ІР, ІТ систем і мереж, а також програмних і апаратних засобів шляхом аналізу чотирьох основних категорій, а саме:

- впливу на цілісність;
- впливу на конфіденційність;
- впливу на доступність;
- впливу на спостережність.

Кожна з цих категорій підпадає під вплив пар загроза / уразливість (ZY), сформованих за еталонною вибіркою актуальних загроз інформаційній безпеці. Такими парами можуть бути пари:

Отримання несанкціонованого логічного доступу до інформації зовнішніми зловмисниками / відсутність політики використання послуг мережі (ZY1);

Відсутність можливості відновлення роботи / відсутність резервного копіювання інформації (ZY2);

Розкриття, продаж, шахрайське копіювання інформації / відсутність процедури поводження з інформацією (ZY3);

Порушення персоналом організаційних заходів щодо забезпечення ІБ / відсутність політики інформаційної безпеки (ZY4);

Неконтрольована модифікація інформаційного ресурсу / відсутність криптографічних заходів захисту (ZY5).

На основі наведених вище індикаторів, що характеризують здатність організації забезпечити ІБ і підтримувати безпечне функціонування власних

об‘єктів інформаційної структури можна зробити оцінювання стану захищеності інформаційних ресурсів в умовах впливу актуальних загроз і уразливостей.

Список використаних джерел:

1. Низамутдинов М.Ф. Тактика защиты и нападения на Web-приложени. - СПб.: БХВ- Петербург, 2005. – 432 с.: ил.
2. Невойт Я. Аналіз методів та засобів оцінки стану захищеності інформаційних ресурсів від впливу актуальних загроз і уразливостей. – Київ. 2016.- 170с.
3. Облачные вычисления: обзор и рекомендации. Общая среда облачных вычислений - Рекомендации Национального Института Стандартов и Технологий (США), NIST, USA, 2007
4. SoCC '10: Proceedings of the 1st ACM symposium on Cloud computing / Hellerstein, Joseph M. — N. Y.: ACM, 2017. — ISBN 978-1-4503-0036-0.

УДК 004.932.2
[1] Труш О.В.
к.т.н., доцент
[2] Радзівілов Г.Д.
к.т.н., доцент
[3] Лук'янюк О.О.
магістрант
[1]Київський національний університет імені Тараса Шевченка
[2]Військовий інститут телекомунікацій та інформатизації
[3]Одеська національна академія зв'язку імені О. Попова

ВИКОРИСТАННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ІДЕНТИФІКАЦІЇ ОСІБ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

***Анотація**. Розглядаються можливості систем відеоспостереження з функцією "розпізнавання осіб" на об'єктах охорони, охороні громадського порядку та інших місцях.*

Система відеоспостереження стає популярною серед власників приватних будинків в Україні, так як дозволяє в безперервному режимі контролювати ситуацію у власній оселі. Залежно від індивідуальних потреб встановлюють традиційні відеокамери, які видно кожній людині, або мініатюрні приховані камери, надійно заховані від сторонніх очей в потрібному місці. Кожен з представлених варіантів стеження має свої переваги і недоліки.

Система відеоспостереження з функцією "розпізнавання осіб" працює за принципом порівняння отриманого зображення з наявним у базі. Середньостатистичний комплекс уміє ідентифікувати людську особу що на відстані не перевищує десяти метрів відеокамери. При цьому відвідувач буде упізнаний навіть з урахуванням наявності змін фізичних параметрів особи :зміна зачіски, борода, наявність окулярів і т. д. Аналіз ґрунтується на порівнянні біометричних параметрів будови голови, індивідуальних для кожної людини. При цьому сканування відбувається на ходу, відвідувачеві досить повернути лице до сканера під час руху. Система відеоспостереження може бути пов'язана з турнікетами і іншими облаштуваннями авторизованого входу і працювати автоматично. Непізнані відвідувачі не отримають доступу на територію, що охороняється, а їх фото буде збережено у базі для обробки службою охорони.

Зазвичай такі системи встановлюються у великих корпораціях, де від безпеки залежить майбутній успіх компанії, наприклад, компанії по розробці нових типів озброєння або мікросхем, біологічна лабораторія. Система автоматично розпізнає усіх співробітників і порівнює з базою даних. У разі невідповідності або відсутності людини в системі, вона активізує протоколи безпеки, в кімнаті охорони спалахує тривожний сигнал і червона світлова індикація. Місце виявлення порушника точно вказується на електронній карті об'єкту і охорона за лічені секунди знаходить порушника.

Функціональність системи:

- виявлення (Камера від 1 Мп, фокус на відстань від 1 мм). Дія цієї охоронної системи спрямована на фіксацію проникнень на підконтрольні об'єкти. Сканер в змозі відрізнити людину від кішки або білки, але не зможе ідентифікувати його;

- розпізнавання (Камера від 2 Мп, фокус на відстань від 6 мм). В даному випадку основною функцією сканера є розпізнавання осіб відвідувачів за принципом "свої-чужі". При перегляді відео ряд у зображення буде досить змащеним, Ви дізнаєтеся на нім знайомі обличчя, але у випадку якщо на об'єкт проник злодій, знайти його по цих кадрах буде дуже скрутно;

- ідентифікація (Камера більше 2 Мп, фокус на відстань від 8 мм) Ці системи можуть виконувати усі функції попередніх типів, при цьому якість отримуваного зображення буде цілком досить щоб пізнати зловмисника. Таке фото цілком можна передати у судові органи і органи правопорядку.

В якості приклада можна навести обладнання компанії ZKTeco, яка в Україні використовує біометричні системи обліку роботи персоналу та контролю доступу в приміщення, які використовують ідентифікацію 3D-геометрії обличчя. Інженери цієї компанії розробили систему ідентифікації особи за стереозображенням обличчя з двох камер одночасно, одна з яких інфрачервона.

Рис. 1. Термінал компанії ZKTeco для контролю доступу за геометрією обличчя в 3D.

Це дозволяє врахувати не лише риси обличчя, але і об’єм елементів обличчя незалежно від освітлення, та захищає систему від неправомірного доступу за допомогою фотографії особи. Отже, як ми бачимо, є значний розвиток систем відеоспостереження з використанням біометричної технології розпізнавання за обличчям і використання таких систем.

Місця застосування

- організувати прохідну на підприємстві або інших закритих від сторонніх людей об'єктах. Відеоспостереження можна зв'язати з турнікетами і організувати автоматичний пункт пропуску за принципом "свої-чужі";

- організувати систему протидії розкраданням в торгових точках і інших приватних володіннях. Будь-які магазини, особливо великі, стикаються з проблемою пристрасті деяких відвідувачів до крадіжці. Частенько одні і ті ж люди, схильні здійснювати крадіжки в одних і тих же торгових точках. Встановивши камери з системою розпізнавання осіб, можна ретельніше

придивлятися до дій людини, що вже попалася на крадіжці. Сканер повідомить на пульт охорони як тільки він зайде в магазин;

- організувати систему протидії проникненню на територію домоволодіння і інші закриті об'єкти. Іноді людині складно на моніторі відрізнити зловмисника, що зачаївся, від куща, або іншого предмета, тим більше якщо камери встановлені на слабоосвітленій ділянці місцевості. Але ж то що недоступне людині, цілком може зробити комп'ютерний модуль;
- фейс-контроль в нічних клубах - 100% захист від непрошених гостей.

Висновки. Враховуючи широке застосування систем відеоспостереження для охорони об’єктів інформаційної діяльності з використанням біометричної технології розпізнавання особи за геометрією обличчя, можна зробити висновок про доцільність запровадження таких систем в системах охорони об’єктів та в правоохоронній діяльності в Україні.

Список використаних джерел:

1. Системы биометрической идентификации по геометрии лица. [Електронний ресурс]. — Режим доступу: http://zkstore.com.ua/a101064-sistemybiometricheskoj-identifikatsii.html
2. http://kaschtan.com.ua/shop/category-23-.Videonablyudenie.html- Відео-спостереження, спеціалізована відео техніка.
3. http://www.bastion.kiev.ua/Main/Videonablyudenie - Системи відеоспостереження.
4. http://videokamera.in.ua - Все о відеокамерах в Україні.

ТЕОРЕТИЧНІ АСПЕКТИ КОМП'ЮТЕРНИХ НАУК

[1] **Ю.В.Кравченко**
Професор
[1] **А.В.Іванова**
Студент
[1] *Київський національний університет імені Тараса Шевченка, м.Київ*

УПРАВЛІННЯ ІТ ПРОЕКТАМИ В МІЖНАРОДНИХ КОРПОРАЦІЯХ

Актуальність роботи полягає в тому, що управління проектами — одне із самих древніх і шановних досягнень людства. Аналізуючи проектний менеджмент з позиції його історичного розвитку, слід зазначити, що проектний підхід набув особливої популярності саме в останні десятиліття. Він використовується не лише в стратегічно важливих галузях економіки, як от будівництво, інженерія та оборонна індустрія, де саме і були розроблені основні методи з проектного менеджменту, але й набув своєї популярності і в інших сферах народного господарства та в приватному житті окремих громадян. Вивченням специфіки управління саме ІТ-проектів буде метою данної роботи.

Управління проектом - це діяльність, спрямована на реалізацію проекту з максимально можливою ефективністю при заданих обмеженнях за часом, ресурсами, а також якості кінцевих результатів проекту (документованих, наприклад, у технічному завданні). Для того, щоб ефективно управляти обмеженнями проекту використовуються методи побудови і контролю календарних графіків робіт.

Методи керування проектами включають такі, як: сіткове планування й керування, календарне планування, логістику, стандартне планування, структурне планування, ресурсне планування, імітаційне моделювання на ЕОМ і інші.

Сьогодні основні методи управління підприємствами тісно переплітаються з методами проектного менеджменту, а саме: сіткове моделювання, графік Ганта, метод критичного шляху, PERT - метод, робоча структура проекту, матрична та проектна організаційні структури управління тощо. Їх застосування значно зменшує трудомісткість робіт, підвищує якість управлінської діяльності, контроль за виконанням спланованих завдань та вчасне введення коректив при виявленні відхилень. Однак не всі керівники організацій ознайомлені з сучасним інструментарієм проектного менеджменту та з іншими науковими досягненнями у цій сфері діяльності, тому і не готові використовувати проектних підхід в себе на підприємствах, оскільки вважають, що він притаманний лише проектним організаціям. Це пов’язано, насамперед, з нерозумінням сутності самого терміна «проект» та, відповідно, з незнанням загальних характеристик проектів.

Розуміння сутності проектів дасть змогу керівникам компаній частіше використовувати в своїй діяльності проектний підхід, який значно підвищить рівень ефективності їх виробничо-господарської та управлінської діяльності. Сьогодні низка міжнародних та національних організацій займається саме питаннями синтезу проектного підходу у діяльність компаній різних галузей.

Теми до розгляду:

- Теоретичні основи управління проектами.
- Сутність проектів.
- Класифікація проектів.
- Сутність системи управління проектами.
- Життєвий циел проекту.
- Учасники проекту.
- Ціль і стратегії проекту.
- Формування бюджету проекту.
- Аналіз системи управління проектами на прикладі ІТ корпорації
- Організаційні структури управління проектами.
- Сучасні методи управління проектами. РОЗДІЛ IV. Шлях вдосконалення проектних робіт
- Автоматизація проектних робіт.

Список використаних джерел

1. «Управління апроектами», підручник [Електронний ресурс] — Режим доступу: https://buklib.net/books/22265/

2. Управлінни проектами - підручник, Київ “Каравела” 2009 – Тарасюк М.В.

3. Сутність проектів та їх загальна характеристика - Х.С. Передало, Ю.В. Огерчук, О.О. Пшик-Ковальська / Національний університет “Львівська політехніка”

4. Економіка підприємства Ч.1 - [Електронний ресурс] — https:// pidruchniki.com/74431/ekonomika/rozrobka_byudzhetu_proektu

5. Управління спецпроектами (конспект лекцій НУДПСУ) - [Електронний ресурс] — http://studentbooks.com.ua/content/view/1310/42/1/3/

6. «Проектний аналізи», підручник [Електронний ресурс] — https://buklib.net/
books/34105/

7. "Старченко Г. В. Управління проектами: теорія та практика : навч. посіб. / Г. В. Старченко. – Чернігів : видавець Брагинець О. В., 2018. – 306 с.

ІНТЕРНЕТ РЕЧЕЙ

[1] **Y. V. Kravchenko** – mentor
Head of the network and Internet technologies department
[2] **S. V. Ihnatiuk**
Student of the network and Internet technologies department (MIT-31)
[3] **A. O. Skvortsova**
Student of the network and Internet technologies department (MIT-41)
[4] **V. M. Bachynska**
Student of the network and Internet technologies department (MIT-41)
[5] **V. B. Moroz**
Student of the network and Internet technologies department (MIT-21)
[1, 2, 3, 4, 5] *Faculty of Information Technologies, Kyiv Taras Shevchenko National University of Kyiv*

THE IMPLEMENTATION OF INTERNET OF THINGS TECHNOLOGIES IN PARKING LOTS TO IMPROVE THE LIFE OF THE CITY

A Smart city is an urban area that uses digital technology to connect, protect, and enhance the lives of citizens. IoT sensors, video cameras, social media, and other inputs act as a nervous system, providing the city operator and citizens with constant feedback so they can make informed decisions. A smart city collects and analyzes data from IoT sensors and video cameras. In essence, it "senses" the environment so that the city operator can decide how and when to take action. Some actions can be performed automatically. For example, a public waste bin can contact the city for service when it is near capacity instead of waiting for a scheduled pickup.

The creation of special places for cars began almost simultaneously with the advent of the first cars. The number of off-road parks is limited by modern technology.

The main direction of development is the "smart" parking sensors. Transferring data to a common system. Using a network of such sensors, a parking map is created.[1]

Smart Parking systems typically receive information on available parking spaces in a specific geographic area, and a real-time process for locating vehicles in accessible locations. This includes the use of low-cost sensors, real-time data collection and mobile phone-enabled automated payment systems that allow people to pre-reserve parking or predict very accurately where they are likely to find a place.

Smart parking helps to solve one of the biggest problems when driving around the city; search for empty parking spaces and control of illegal parking.

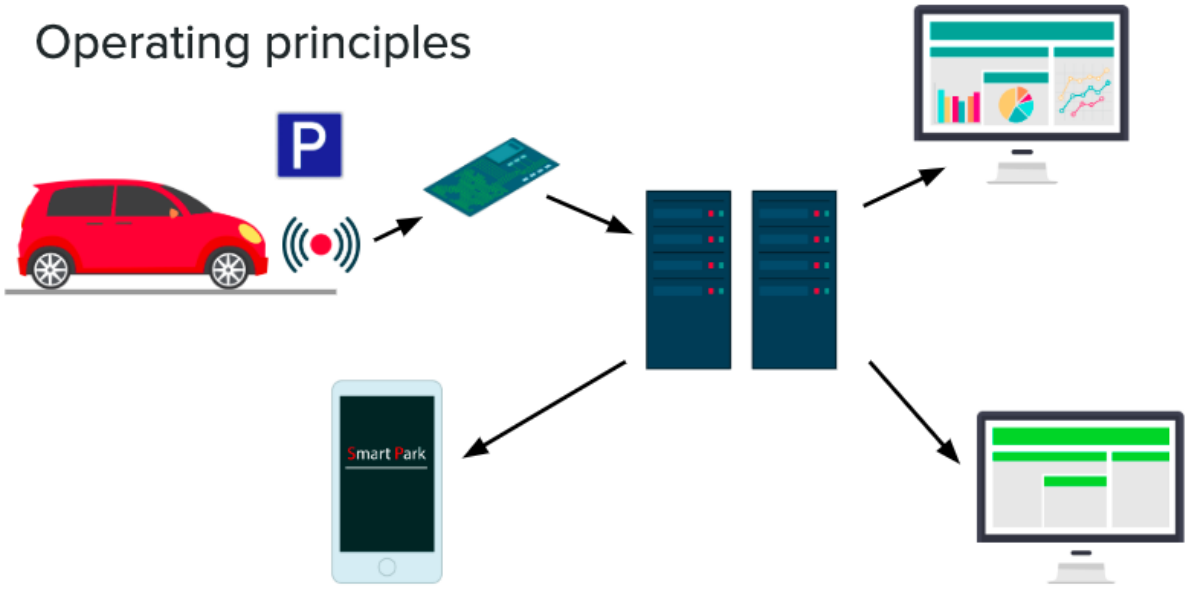
In densely populated areas as in cities, the availability of parking spaces is often less than the availability of vehicles which leads to a shortage of parking space. Studies showed that in worldwide traffic dense environment, 30 to 50 percent of the drivers look for free parking space. Based on previous studies drivers use between 3.5 and 14 minutes to find a parking space. [2,3]

Smart parking is based on the use of sensors, RFID, cameras, license plate readers, assistive devices and mobile payments to make parking smooth. Mobile IoT is critical

to covering all areas of data transmission from sensors in a centralized database. This makes it possible to install cameras and sensors in older cameras.

Wireless parking detection sensing system includes wireless parking space detector and wireless parking data collection device. The detector is used to detect available parking spots. The parking data collection device is to receive the data from sensor and relay it to application system (Fig 1.).

Figure 1



References

1. Smart Parking IoT platform to increase the efficiency of electric car recharging station: http://www.libelium.com/smart-parking-iot-platform-to-increase-the-efficiency-of-electric-car-recharging-station/

2. Shoup, D.C., Cruising for parking. Transport Policy, 2006. 13(6): p. 479-486.

3. Polycarpou, E., L. Lambrinos, and E. Protopapadakis. Smart parking solutions for urban areas. in World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a. 2013. IEEE.

УДК 004.738.5
[1] **Труш О.В.,**
к.т.н., доцент
[2] **Падаленчук А.В.,**
студент
[3] **Фекете Д.М.,**
студент
[1,2,3]*Київський національний університет імені Тараса Шевченка*

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ТУМАННИХ ОБЧИСЛЕНЬ У ІНТЕРНЕТ РЕЧАХ, ПОВ'ЯЗАНИХ З МЕДИЦИНОЮ

Оскільки пристрої стають менше, а даних стає більше, постачальники послуг мають складнощі із розробкою ефективних способів збору, аналізу, візуалізації та використання даних, які можуть помітно вплинути на догляд за пацієнтами. Дані про стан здоров'я можуть створюватися носимими пристроями, глюкометрами, домашніми вагами та іншими датчиками. Звіти Cisco передбачають, що Інтернет речей може включати до кінця десятиліття 50 мільярдів окремих пристроїв, які вироблять 507,5 зеттабайт даних.

Медичні заклади часто використовують хмарні рішення як простір для зберігання даних. В ідеалі процес обміну даними може зайняти лише кілька хвилин, але деякі пацієнти просто не можуть так довго чекати. Відповідь може лежати в туманних обчисленнях. Туманні обчислення дозволяють пристроям проводити аналітику самостійно, не потребуючи хмарного зберігання.

Туманні обчислення додають додатковий рівень обчислювальної потужності між пристроєм та хмарою, зберігаючи дані ближче до пристрою, а отже, скорочуючи час, необхідний для запиту на відповідь. Що стосується охорони здоров'я, то такі обчислення можуть бути особливо цінними для моніторингу стану пацієнтів.

Мета Інтернету речей у медицині полягає в тому, щоб полегшити пацієнтам зв'язок зі своїми лікарями, а лікарям надавати вчасну та ефективну допомогу своїм пацієнтам. Можливість сортування даних та прийняття найважливіших

рішень у власному середовищі допоможе пристрою отримати ключові дані з величезного обсягу доступних даних.

Використовуючи заздалегідь визначені протоколи авторизації та користувальницькі дані, дані про стан здоров'я пацієнта можуть бути піддані впливу будь-якого пристрою через спільний інтерфейс, але всі обчислення будуть проводитися лише там, звідки вони походять: у лікарні чи у самого лікаря, що веде облік пацієнта. Гранична екосистема може також скористатись протоколами безпеки та цілісності даних технології blockchain, щоб користувачі мали можливість перегляду та зміни певних наборів даних, а також, щоб всі пристрої отримали доступ до однієї і тієї ж актуальної інформації.

Консорціум OpenFog, заснований у листопаді 2015 року, об'єднав п'ять основних IoT організацій, включаючи ARM, Cisco, Dell, Intel, Microsoft та Лабораторію обчислювальних технологій Принстонського університету задля просування туманних обчислень. Використовуючи відкриті стандарти для створення загальноприйнятої основи для туманних обчислень на самому початку своєї популярності, консорціум, можливо, зможе уникнути деяких проблем сумісності та стандартів даних, які досі особливо дошкуляли галузі охорони здоров'я. Група також пов'язана з Інститутом інженерів електротехніки та електроніки(IEEE), Schneider Electric та GE Digital, і запустили ініціативи в Японії, в яких залучаються технічні гіганти Toshiba і Fujitsu.

На даний момент Cisco є одним з лідерів ринку технологій туманних обчислень, що тільки розвивається – саме ця компанія ввела термін "туманні обчислення"- але також є й інші компанії, такі як Amazon Web Services, IBM, Oracle та Google, які незабаром увійдуть у цю індустрію.

Але в галузі охорони здоров’я доведеться зробити багато робіт, перш ніж туманні обчислення зможуть створити повноцінний Інтернет речей.

Однак галузь охорони здоров'я та інтернет речей, як правило, дуже хвилює розробників, і туманні обчислення можуть вирішити багато проблем, які в даний час затримують ріст цієї інноваційної екосистеми. Якщо інтернет речей розквітне таким чином, як очікували провідні члени спільноти охорони здоров'я, догляд за пацієнтами може бути на межі чергової революції.

Список використаних джерел

1. Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper.

2. IEEE Spectrum. 2017. “Popular Internet of Things Forecast of 50 Billion Devices by 2020 is Outdated.”

3. International Conference on Advanced Aspects of Software Engineering, ICAASE, December, 01-02, 2018. “Cloud Edge Computing for Internet of Things Elasticity Management”

4. Shi, W., J. Cao, Q. Zhang, Y. Li, and L. Xu. 2016. “Edge Computing: Vision and Challenges.” IEEE Internet of Things Journal

5. OpenFog Reference Architecture for Fog Computing https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf

УДК 004.056
[1] В. В. Афанасьєв
Кандидат технічних наук, доцент, заступник начальника кафедри повітряної навігації та бойового управління авіацією
[1] В.М. Сургай
старший викладач кафедри повітряної навігації та бойового управління авіацією
[1] О.М. Сітков
викладач кафедри повітряної навігації та бойового управління авіацією
[2] Ю. В. Афанасьєв
студент кафедри інфокомунікаційної інженерії імені В.В. Поповського
[1]Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків
[2]Харківський національний університет радіоелектроніки, м. Харків

СИНТЕЗ МЕТОДІВ АВТЕНТИФІКАЦІЇ В РОЗПОДІЛЕНИХ СЕНСОРНИХ МЕРЕЖАХ

На даний час розвиток інфокомунікаційних технологій характеризується інтенсивним впровадженням концепції Інтернету Речей. Однією з важливих задач для забезпечення безпеки є розробка методів і засобів контролю доступу. Основною функцією для управління доступом є автентифікація. Аналіз публікацій з питань рішення задачі контролю доступу показує, що питання забезпечення безпеки доступу є актуальним [1]. Існуючі методи автентифікації не забезпечують в повній мірі захист від несанкціонованого доступу. Одним з ефективних методів забезпечення захисту інформації є застосування багатофакторної автентифікації [2].

Метою роботи є дослідження питань програмно-апаратної реалізації системи контролю та управління доступом (СКУД) для забезпечення функціонування об'єкта, який має розподілену сенсорну мережу. Ця особливість характеризується неможливістю поєднання всіх елементів в єдину інформаційну систему. Забезпечення контролю функціонування елементів системи, оновлення баз даних пропонується здійснювати з використанням безпілотних літальних апаратів (БПЛА) [3]. Таким чином в роботі розглянуто наступні задачі.

1. Програмно-апаратна реалізація СКУД з використанням однофакторного, двофакторного та багатофакторного методів автентифікації.
2. Аналіз особливостей програмно-апаратної реалізації варіантів СКУД.
3. Дослідження питань забезпечення функціонування розподіленої сенсорної мережі з використанням БПЛА.

В основу програмно-апаратної реалізації варіантів СКУД покладено застосування наступних елементів: FPM10A зчитувач відбитків пальців, мікроконтролер ESP32 з інтегрованими Wi-Fi та Bluetooth контролерами та

антенами; модуль RFID з модулем RC522; мікроконтролер ESP8266; сервер - одноплатний компьютер Raspberry Pi 3; Bluetooth-пристрій (фітнес-браслет).

Розроблено алгоритми роботи з автентифікацією по Bluetooth-пристрою, з автентифікацією по відбитку пальця та з використанням модуля RFID. Особливістю розглянутих варіантів є застосування методів, які не пов'язання між собою. Так, для радіочастотної автентифікації використовуються частоти 13,56 МГц (RFID) та частоти 2,4-2,4835 ГГц (Bluetooth).

Загальними рисами реалізованих варіантів є: необхідність наявності серверу, в якому зберігається база даних користувачів; використання мікроконтролеру ESP32 забезпечує реалізацію розглянутих методів; використання мікроконтролеру ESP8266 забезпечує реалізацію методів автентифікації без використання Bluetooth.

Для забезпечення функціонування СКУД в розподілених сенсорних мережах необхідно здійснювати синхронизацю часу в підситемах, періодично оновлювати бази даних, контролювати функціональний стан складових, виявляти факти зовнішнього впливу та несанкціонованого доступу. Ця задача, як показують дослідження, може бути реалізована за рахунок використання БПЛА. При цьому вони можуть виконувати функцію, як функціонального доповнення (мобільного шлюзу) для ретрансляції інформації при оновлені бази даних, так і в якості тимчасового сервера – мобільного серверу.

Особливістю роботи сенсорів СКУД є мала дальність дії, це обумовлено діапазоном роботи Bluetooth та Wi-Fi, що потребує забезпечення точного виходу БПЛА в задані точки. Рішення задачі синхронізації роботи системи по часу та забезпечення точного позиціонування можливе за рахунок використання апаратури GPS.

Список використаних джерел

1. Юдін О. К. Аналіз та класифікація систем контролю та управління доступом на підприємстві / О.К. Юдін, О.М. Весельська // Наукоємні технології 2018. - №2(38), С. 220-225. DOI: 10.18372/2310-5461.38.12830

2. Єсіна, М. В. Багатофакторна автентифікація: використання механізмів двофакторної автентифікації для захисту від несанкціонованого доступу / М. В. Єсіна, І. Д. Горбенко // Компьютерное моделирование в наукоемких технологиях (КМНТ-2014): Тр. науч.-техн. конф. с междунар. участием, 28-31 мая 2014 г. – Харьков: Харків. нац. ун-т им. В.Н. Каразина, 2014 – С. 159–162.

3. Афанасьєв Ю. В. Застосування безпілотних літальних апаратів, як мобільного шлюзу в концепції IoT для системи контролю і управління доступом / Ю. В. Афанасьєв, О.М. Сітков, В.В. Афанасьєв // Проблеми розвитку глобальної системи зв'язку, навігації, спостереження та організації повітряного руху CNS/ATM: тези доповідей науково-технічної конференції, м. Київ, 21-23 листопада 2018 р., Національний авіаційний університет – К.: НАУ, 2019.– С. 3.

ІМЕННИЙ ПОКАЖЧИК

Наукове видання

НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ МОЛОДИХ УЧЕНИХ «Актуальні проблеми інформаційних технологій»

20-21 листопада 2018 року

Матеріали доповідей

Формат 60x84$^{1/16}$. Ум. друк. арк. 3,3. Наклад 40. Зам. №217-8445.
Гарнітура Times New Roman. Папір офсетний. Друк офсетний.
Підписано до друку 27.12.19

Видавець і виготовлювач
ВПЦ «Київський університет»
б-р Т. Шевченка, 14, м. Київ, 01601,
(044) 239 32 22; (044) 239 31 72; тел./факс (044) 239 31 28
http:vpc.univ.kiev.ua
Свідоцтво суб'єкта видавницої справи ДК № 1103 від 31.10.02