

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВ'ЯЗКУ ІМ. О. С. ПОПОВА
КОЛЕДЖ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ**

Дев'ята студентська науково-технічна конференція

**ТЕЛЕКОМУНІКАЦІЙНІ, ІНФОРМАЦІЙНІ
ТА КОМП'ЮТЕРНІ МЕРЕЖІ І СИСТЕМИ:
ТЕПЕРІШНЄ ТА МАЙБУТНЄ**

30 березня 2019 року

Збірка тез

Одеса, 2019

Телекомунікаційні, інформаційні та комп'ютерні мережі і системи: теперішнє та майбутнє: матеріали дев'ятої студентської науково-технічної конференції, м. Одеса, 30 березня 2019 року – Одеса, КЗІ ОНАЗ ім. О.С. Попова, 2019 – 32 с.

Дана збірка містить тези матеріалів, що представлені на дев'ятій студентській науково-технічній конференції «**Телекомунікаційні, інформаційні та комп'ютерні мережі і системи: теперішнє та майбутнє**», що проводиться 30.03.2019 р. в коледжі зв'язку та інформатизації Одеської національної академії зв'язку ім. О.С. Попова.

До збірки включені тези доповідей за секціями:

- автоматизації, телекомунікацій та радіотехніки;
- інформаційних технологій;
- комп'ютерних технологій та захисту інформації.

Робочі мови конференції – українська, англійська.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

ГОЛОВА ОРГКОМІТЕТУ:

Петрусенко С. Ю. – к.п.н., директор коледжу зв'язку та інформатизації
ОНАЗ ім. О. С. Попова

ЗАСТУПНИК ГОЛОВИ ОРГКОМІТЕТУ:

Горлінська О. Ю. – заступник директора з навчальної роботи

СЕКРЕТАР ОРГКОМІТЕТУ:

Орлова Л. Б. – викладач циклової комісії інформатики та обчислювальної техніки

ЧЛЕНИ ОРГКОМІТЕТУ:

Ящишина І. Я. – заступник директора з навчально-виховної роботи

Трофименко Ю.В. – завідувач денного відділення, викладач циклової комісії телекомунікацій та радіотехніки;

Осадчук Т. В. – методист

Кокорєва З. Р. – голова циклової комісії телекомунікацій та радіотехніки

Кокорєв О. В. – к.філ.наук, голова циклової комісії інформатики та обчислювальної техніки

Малюта С. О. – викладач циклової комісії інформатики та обчислювальної техніки

Тарашкевич В. О. – голова ради студентського самоврядування, студентка групи Р-41

ЖУРИ КОНФЕРЕНЦІЇ

ГОЛОВА ЖУРИ:

Каптур В. А. – к.т.н, с.н.с., проректор з наукової роботи
ОНАЗ ім. О. С. Попова

ЧЛЕНИ ЖУРИ:

секція автоматизації, телекомунікацій та радіотехніки

Тіхонов В. І. – лауреат Державної премії України в галузі науки і
техніки, доктор технічних наук, професор кафедри
мереж зв'язку ОНАЗ ім. О. С. Попова

Баляр В. Б. – к.т.н., старший викладач кафедри телебачення та
радіомовлення ОНАЗ ім. О. С. Попова

секція інформаційних технологій

Кумиш В. Ю. – к.т.н, начальник НДЧ ОНАЗ ім. О. С. Попова

Царьов Р. Ю. – старший викладач кафедри мереж зв'язку
ОНАЗ ім. О. С. Попова

секція комп'ютерних технологій та захисту інформації

Васіліу Є. В. – д.т.н., професор, директор ННІ РТ та ІБ
ОНАЗ ім. О. С. Попова

Севастєєв Є. О. – старший викладач кафедри інформаційної безпеки та
передачі даних ОНАЗ ім. О. С. Попова

ЗМІСТ

Секція автоматизації, телекомунікацій та радіотехніки

1. **Тарашкевич В. О.** Методи просторового аналізу для оцінки паралаксу 6
2. **Тростянецький Д. К., Венжик В. С.** Сучасні бездротові технології. Розробка власного приладу з їх використанням 10
3. **Васильєв П. С.** Теоретичні аспекти SDN & NFV технологій та приклади їх використання 12

Секція інформаційних технологій

1. **Максимишин О. І.** Порівняльний аналіз сучасних фреймворків для мікроконтролерів та засобів розробки 16
2. **Мерецький К. А., Тиховський С. Л.** Порівняльний аналіз технологій при використанні Javascript та WebAssembly 18
3. **Д'яченко А. І.** Порівняльний аналіз hash-функцій 20

Секція комп'ютерних технологій та захисту інформації

1. **Філіппова М. В.** Аналіз використання Darknet інтернет-користувачами 23
2. **Червоненко Б. М., Харламов А. А.** Наукова актуальність кіберспорту та його майбутнє як частини традиційних видів спорту/ Esports science and its future as a part of traditional sports 24
3. **Белолиця Ю. О.** Порівняльний аналіз VPN сервісів 27

МЕТОДИ ПРОСТОРОВОГО АНАЛІЗУ ДЛЯ ОЦІНКИ ПАРАЛАКСУ

Тарашкевич В. О., студентка 4-го курсу, групи Р-41, галузь знань 17 Електроніка та телекомунікації, спеціальність 172 Телекомунікації та радіотехніка .

Науковий керівник – викладач **Борисенко В. С.**

Коледж зв'язку та інформатизації ОНАЗ ім. О. С. Попова

***Анотація.** Вектор паралакса може бути визначений як для окремих елементів зображення, так і для групи елементів або об'єктів, що становлять стереоскопічне зображення (випадок об'єктно-орієнтованого кодування), тобто оцінка паралаксу може бути здійснена співставленням точок, фрагментів або об'єктів лівого і правого зображень. Процедура знаходження паралакса вимагає значних обчислювальних витрат, тому основною вимогою при її здійсненні є швидкодія, що супроводжується точним виявленням паралактичних зсувів об'єктів сцени. Швидкодію можна забезпечити, застосовуючи метод фазової кореляції для оцінки паралакса.*

Одним з основних напрямків розвитку в області виробництва, обробки, поширення і відображення інформації є цифрове телерадіомовлення. Розвиток телевізійних технологій нерозривно пов'язаний зі створенням об'ємного телебачення. У порівнянні зі звичайним телебаченням, об'ємне володіє інтерактивністю і об'ємністю, що дозволяє очам людини працювати в природному режимі. Велика частина існуючих сьогодні методів формування об'ємного зображення використовують фізіологічні особливості зору.

Сьогодні 3D-технології є одним з перспективних напрямків розвитку телевізійних систем. При цьому важливим питанням, крім зйомки і відтворення об'ємних зображень, є методи їх кодування для зберігання і передачі по каналу зв'язку. При створенні 3D потрібно змістити зображення одне щодо іншого для розносу об'єктів по глибині, але не можна сильно розносити зображення відносно один одного, тому що мозок перестане сприймати їх як одне ціле, а буде сприймати як різні зображення. Регулюючи в телевізорі глибину 3D програмно задається, наскільки зрушити зображення відносно один одного. Завдяки ефекту паралакса - зміни видимого положення об'єкту відносно віддаленого фону в залежності від положення спостерігача.

Формування просторового образу у свідомості спостерігача визначають більшою мірою яскравості перепади. Колірна складова зображення при цьому

відіграє другорядну роль і підвищує якісний рівень зображення. При утворенні сигналом паралактичних різниць (СПР) інформація про просторове розташування об'єктів укладена в складову яскравості. Проте, кольорорізницеві дані також повинні бути присутніми в СПР. Це дозволяє на приймальній стороні синтезувати другий кадр в кольорі і виключити зменшення насиченості об'ємної моделі сцени.

Телевізійні сигнали мають значну надмірність. Це поширюється і на стереоскопічні зображення. В результаті, СПР містить контури предметів і різниці тих елементів, яких немає в обох кадрах стереопари. Товщина контурів об'єктів змінюється в залежності від величини паралакса. Різницеве зображення має просторову надмірність. Передача динамічних стереоскопічних ТБ зображень призводить також і до тимчасової надмірності.

Іншим варіантом передачі стереоскопічних зображень є метод з оцінкою і компенсацією паралаксу. Найближча аналогія між зображеннями двовимірному телебачення, що відрізняються тимчасовим інтервалом, в яких зміна змісту визначається як рухом камери, так і рухом об'єктів, і зображеннями, складовими стереопару. Цей факт дозволяє поширити ідею усунення тимчасової надмірності, яка здійснюється на основі диференціальної імпульсно-кодової модуляції (ДІКМ) з компенсацією руху на стереоскопічні зображення, для усунення бінокулярної надмірності. У цьому випадку мова йде вже про ДІКМ з компенсацією паралаксу.

Велике значення має і розмір області привласнення знайдених векторів паралаксу. Величина зони аналізу залежить від розміру області присвоєння. Після знаходження вектора паралаксу необхідно його привласнити певній області фотографії. Це означає, що всі елементи цієї області мають одне і те ж значення паралаксу. Однак при стисканні стереоскопічних зображень не потрібно точне знаходження величини паралаксу. Крім того, присвоєння області тільки одного вектора зменшує кількість переданих даних. Зменшення розміру блоку викликає підвищення кількості векторів і - як результат - підвищення швидкості цифрового потоку. В якості області присвоєння векторів паралаксу може бути обраний блок розміром $8 * 8$ відліків. Визначивши розмір області привласнення, необхідно знайти і розміри зони аналізу, приймаючи її форму прямокутної.

Перетворені в цифрову форму зображення (вихідна стереопара) фільтруються і проріджуються по діагоналі, що призводить до утворення шахового малюнка, що складається з клітин лівого і правого уявлень в стандартному ортогональному дискретизованому форматі, які потім накладаються один на одного і виходить комбіноване чергування пікселів «лівих» і «правих» зображень. Описаний формат, на відміну від інших затворів технологій, зберігає і горизонтальний, і вертикальний дозволи зображення, забезпечуючи тим самим високу якість зображення.

Стереозображення на екрані - це накладені один на одного зображення правого і лівого ракурсів просторового об'єкту. В такому сумарному зображенні однойменні точки об'єкта мають горизонтальний зсув. Цей зсув, іменований горизонтальним паралаксом, є наслідком реєстрації об'єкта з двох ракурсів. Горизонтальні паралакси є причиною конвергенції зорових осей при спостереженні зображення на екрані, що викликає відчуття, подібних до тих, що виникають при бінокулярному сприйнятті. На відміну від "корисних" - горизонтальних паралаксів, розрізняють "шкідливі" - вертикальні паралакси, які виникають в результаті неправильного юстирування знімальної техніки, коли головні оптичні осі лівого і правого об'єктивів не лежать в одній горизонтальній площині. Наявність вертикального зсуву лівого зображення щодо правого призводить до зрушення зорових осей по вертикалі, невластиве нашому зору, і є однією з причин стомлюваності при сприйнятті стереофільмів.

Горизонтальні паралакси можуть мати як "позитивне", так і "негативне" значення. Якщо точка лівого зображення на екрані розташована лівіше однойменної точки правого зображення, то такий паралакс буде позитивним. Якщо ж точка лівого зображення розташована правіше однойменної точки правого зображення - такий паралакс буде негативним.

Для стереоскопічних зображень, через наявність тільки горизонтального паралаксу, використання квадратних ділянок може призвести до помилкового присвоювання векторів паралаксу. Для виключення цього форма ділянки перетворення або зони аналізу повинна бути прямокутною. Зі зменшенням розміру блоку передбачення поліпшується, тому що ймовірність, що ліве і праве зображення мають аналогічні великі блоки, мала. З іншого боку, зменшення розміру блоку викликає підвищення кількості векторів і в результаті - підвищення швидкості цифрового потоку. Оскільки в фазовій кореляції використовується перетворення Фур'є, то збільшення розміру блоку вимагатиме збільшення розміру зони аналізу, що в результаті призведе до підвищення кількості виконуваних арифметичних операцій, тобто до зниження швидкодії. Тому з цього боку вибирати відносно великий блок недоцільно.

Поділ зображень стереопари на зони може супроводжуватися тим, що в відповідні зони аналізу, мають ідентичні координати як в лівому, так і в правому зображеннях, можуть не потрапити досліджувані на паралактичному зміщенні об'єкти. Для усунення цього зони роблять з перекриттям, оцінки паралаксу на основі фазової кореляції. Підхід до оцінки паралаксу на основі фазової кореляції дозволяє скоротити час виконання аналізу і, як наслідок, послабити апаратні вимоги при створенні кодуєчих пристроїв. Разом з цим, використання фазової кореляції забезпечує нечутливість до яркісних змін, які характерні для стереоскопічних

зображень, і зменшення кількості помилок у разі періодичних структур. Стереоскопічні зображення можуть бути також представлені у вигляді одного з кадрів стереопари і карти глибини.

При кодуванні багато ракурсів зображень передбачається використання кореляції, як між зображеннями різних (сусідніх) ракурсів, так і між зображеннями одного ракурсу.

Формат представлення аудіовізуальних сцен не повинен залежати від методу доставки медіа-об'єктів. Повинно бути забезпечено незалежне уявлення об'єктів різних типів в сцені, незалежний доступ до об'єктів для обробки, маніпуляцій і повторного використання. Стандарт повинен також визначати способи забезпечення перешкодозахищеності від помилок, що виникають в каналах з важкими умовами передачі даних (наприклад, в мобільному зв'язку). Необхідно визначити способи компонування аудіовізуальних сцен з об'єктів різних типів. Треба створити систему опису об'єктів і подій в сцені, а також забезпечити гіперзв'язку і інтерактивність.

Основна відмінність MPEG-4 від всіх інших стандартів - об'єктно-орієнтоване уявлення аудіовізуальних сцен, які утворюються з використанням окремих об'єктів, розташованих певним чином в просторі і часі. Це дає ряд переваг. Різні об'єкти можуть мати різні і найбільш підходящі типи кодового уявлення. Дані різних типів можуть об'єднуватися в одній сцені, коли, наприклад, анімаційні персонажі поміщаються в зображення реального світу, а реальний персонаж занурюється у віртуальне середовище. Стає можливим інтерактивне взаємодія з окремими об'єктами сцени на основі використання гіперзв'язків. В MPEG-4 вводиться спеціальна мова BIFS, що дозволяє задавати положення об'єктів в сцені, компонувати, змінювати, додавати нові об'єкти. BIFS заснований на мові моделювання віртуальної реальності VRML. У мові BIFS додано оновлення в реальному часі. Команди BIFS роблять доступним зміна властивостей об'єктів і завдання їх поведінки. Інтерактивність - одна з найбільш багатообіцяючих функціональних можливостей MPEG-4. Вона підтримується об'єктно-орієнтованим кодуванням, управлінням поведінкою об'єктів за допомогою засобів BIFS, гіперзв'язків.

Стрімкий прогрес технологій оброблення зображення буде весь час призводити до зміни технологій, направленої на подальше вдосконалення інфокомунікаційних систем.

Висновки:

1) Для отримання об'ємного зображення необхідно передавати два сигнали: один сигнал лівого кадру стереопари, а інший - правого.

2) Однією з основних завдань в стереоскопічному телебаченні є вибір способу кодування і передачі об'ємних зображень, що дозволяє задовольнити дві суперечливі вимоги: компактність переданих даних і збереження високої якості відновлених на приймальній стороні зображень.

3) Одним з варіантів передачі стереоскопічних зображень є метод з оцінкою і компенсацією паралаксу.

4) Вектор паралаксу може бути визначений як для окремих елементів зображення, так і для групи елементів або об'єктів, що становлять стереоскопічне зображення (випадок об'єктно-орієнтованого кодування).

5) Для швидкодії процедури знаходження паралаксу, що супроводжується точним виявленням паралактичних зсувів об'єктів сцени, застосовують метод фазової кореляції для оцінки паралаксу.

7) Основна відмінність MPEG-4 від всіх інших стандартів - об'єктно-орієнтоване уявлення аудіовізуальних сцен, які утворюються з використанням окремих об'єктів, розташованих певним чином в просторі і часі.

Перелік посилань:

1. <https://www.youtube.com/watch> Що таке паралакс ефект.
2. <http://embodiedmedia.org/project> Пристрій екрану ТБ
3. <http://lib.broadcasting>. Об'ємне ТВ символ 21 століття
4. <http://ru.okno-tv.ru/> 3D: кодування і передача сигналів об'ємного телебачення.
5. <http://polit.ru/> Механізми бінокулярного зору людини і сприйняття фільмів 3D формату /
6. <https://studfiles.net/> Об'ємне телебачення, Стереотелебачення.
7. <http://iitp.ru/upload/c>Стереозір: основні поняття і показники функціонування механізмів стереосприйняття людини.

СУЧАСНІ БЕЗДРОТОВІ ТЕХНОЛОГІЇ. РОЗРОБКА ВЛАСНОГО ПРИЛАДУ З ЇХ ВИКОРИСТАННЯМ

Гростянецький Д. К. студент 4-го курсу, група О-41, спеціальність 5.05090302 «Технічне обслуговування і ремонт апаратури зв'язку та оргтехніки».

Венжик В. С. студент 4-го курсу, група О-41, спеціальність 5.05090302 «Технічне обслуговування і ремонт апаратури зв'язку та оргтехніки».

Науковий керівник – к.філос.наук **Кокорев О.В.**

Коледж зв'язку та інформатизації ОНАЗ ім. О. С. Попова

***Анотація.** У роботі розглянута історія та розвиток технології бездротової передачі енергії, її користь, зручність та доцільність у повсякденному житті.*

Головна мета – виявити усі плюси та мінуси ,звернутися до розвитку даної технології в цілому та продемонструвати власний робочий прилад, що ілюструє свіжий погляд у бездротове майбутнє.

Сучасний світ дає поштовх людям шукати способи поліпшення та вдосконалення свого життя. Ми повинні постійно вирішувати чимало питань, робити багато задач у повсякденні та побуті. Але чимало з нас навіть не замислюється над тим, що достатня частина буденних обов'язків так чи інакше пов'язана з використанням дротів. Саме тому бездротові технології покликанні неабияк спростити наші щоденні справи.

Головні переваги бездротових технологій передачі енергії – це дуже висока зручність, універсальність, приваблива економічність при тривалій експлуатації та безумовна практичність. Усе це покликано створити приємні для користувача умови використання, а також спростити його повсякденну взаємодію з різними приладами.

Хоча технології активно розвиваються вже понад тридцять років, вони все одно не зупиняють свій рух вперед і мають доволі перспективне майбутнє. З кожним роком нові розробки надають нам все більше можливостей в роботі, житті, дослідженнях тощо. На нашу думку, все через те, що це приносить неабияку користь людині. Завдяки цьому зберігається багато часу, який на даний момент є дуже цінним. Саме ця ідея передбачена людством та розробниками цього напрямку - не витратити багато часу на речі, де не потрібно багато уваги. З точки зору використання, весь процес базується на використанні ближнього електромагнітного поля на відстанях близько однієї шостої довжини хвилі. Завдяки електродинамічній індукції, змінний електричний струм, що протікає через первинну обмотку, створює змінне магнітне поле, яке діє на вторинну обмотку, індукуючи в ній електричний струм.

У результаті проведення наукової роботи розробили наочний приклад бездротової передачі енергії і тим самим показати більш свіжий підхід. А також на основі вивчених матеріалів зробити висновки щодо цієї технології. По-перше знайшли плюси та недоліки, по-друге оцінили розвиток і перспективи галузі, які впродовж років демонструють імениті компанії.

Висновки

Поява бездротових технологій у світі надало людям багато можливостей, які спростили їх життя. Люди породжують потребу пошуку ефективних альтернатив, які мають змогу підняти рівень технологічності, що безумовно приведе нас до високотехнологічного майбутнього. Крім того ця технологія вже зараз є найбільш

перспективною та привабливою для більшості людей не тільки з точки зору зручності у повсякденному використанні, а й з точки зору екології. Темпи розвитку, нові втілення та свіжі ідеї в цьому напрямку дають поштовх вірити у справжнє бездротове майбутнє.

Перелік посилань:

1. Все про бездротову передачу енергії:
https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D1%81%D0%BF%D1%80%D0%BE%D0%B2%D0%BE%D0%B4%D0%BD%D0%B0%D1%8F_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B0_%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%B0
2. https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BC%D0%B0%D0%B3%D0%BD%D0%B8%D1%82%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D0%B4%D1%83%D0%BA%D1%86%D0%B8%D1%8F
3. Історія:
<https://electrosam.ru/glavnaja/jelektrooborudovanie/jelektropitanie/besprovodnoe-elektrichestvo/> <http://kakizobreli.ru/izobreteniya-nikoly-tesly/>
4. Стандарт Qi:
[https://ru.wikipedia.org/wiki/Qi_\(%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82_%D0%BF%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D1%8F\)](https://ru.wikipedia.org/wiki/Qi_(%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82_%D0%BF%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D1%8F))
5. Сучасні бездротові зарядні пристрої: <http://2a3a.ru/qi/>
6. Майбутнє технології: <https://www.dailytechinfo.org/mobile/9558-wi-charge-technologiya-kotoraya-prevratit-vse-pomeschenie-v-odnu-bolshuyu-zaryadku-dlya-mobilnyh-ustroystv.html>.
7. <https://ecotechnica.com.ua/technology/3815-sozdana-besprovodnaya-zaryadka-kotoruyu-mozhno-obrezat-po-razmeru-gadzheta.html>
8. Переваги та недоліки: <https://wd-x.ru/plyusy-i-minusy-besprovodnoj-zaryadki/>

ТЕОРЕТИЧНІ АСПЕКТИ SDN & NFV ТЕХНОЛОГІЙ ТА ПРИКЛАДИ ЇХ ВИКОРИСТАННЯ

Васильєв П.С., студент 4-го курсу, група О-41, спеціальність «Монтаж, ремонт та обслуговування апаратури зв'язку та оргтехніки»

Науковий керівник – викладач **Малюта С.О.**

Коледж зв'язку та інформатизації ОНАЗ ім. О. С. Попова

Анотація. Розглядаються теоретичні аспекти SDN & NFV технологій та реальні приклади використання цих технологій у бізнес рішеннях та причини того, чому деякі компанії впроваджують ці технології, а інші утримуються від їх використання.

Ключові принципи програмно-конфігурованих мереж – поділ процесів передачі та управління даними, централізація управління мережею за допомогою уніфікованих програмних засобів, віртуалізація фізичних мережевих ресурсів. Протокол OpenFlow, який реалізує незалежний від виробника інтерфейс між логічним контролером мережі і мережевим транспортом, є однією з реалізацій концепції програмно-конфігурованих мереж і вважається рушійною силою її поширення і популяризації.

Основна суть SDN полягає в фізичному поділі рівня управління мережею (network control plane) від рівня передачі даних (forwarding functions) за рахунок перенесення функцій управління (маршрутизаторами, комутаторами і тощо) в програми, що працюють на окремому сервері (контролері).

У результаті повинна вийти гнучка, керована, адаптивна та економічна архітектура, яка здатна ефективно адаптуватися під передачу великих потоків різних видів трафіку.

Таким чином, SDN намагається розділити дві площини - управління мережею і транспорт, і в підсумку забезпечити централізацію управління розподіленої мережі з метою більш ефективного використання ресурсів і автоматизації управління мережевими сервісами. NFV же зосереджена на оптимізації мережевих сервісів всередині мережі за рахунок поділу втратити зв'язок із мережею (наприклад, DNS, кешування та ін.), від власне реалізації апаратного забезпечення. Вважається, що NFV дозволяє універсалізувати програмне забезпечення, прискорити впровадження нових функцій мережі і служб і при цьому не вимагає відмови від уже розгорнутої мережевої інфраструктури.

SDN та NFV дозволяють спростити конфігурацію мереж, масштабувати мережі і сервіси за запитом, автоматизувати управління мережею, збільшити потужність фізичної інфраструктури за рахунок накладення віртуальної, знизити CAPEX і OPEX, а в перспективі – швидко реконфігурувати бізнес під поточні завдання.

Висновки:

В результаті виконаної роботи було розглянуто теоретичні аспекти SDN & NFV технологій та реальні приклади використання цих технологій у бізнес-рішеннях.

Практичний ефект від впровадження NFV / SDN для B2B клієнта:

- Управління послугами з Особистого Кабінету.

- Отримання мережевих функцій як послуг з чітким SLA.
- Зниження витрат на обслуговування власних мережевих функцій та ІТ систем за рахунок їх перенесення на «сторону» оператора.
- Отримання доступу до послуг в режимі 24/7 навіть при зміні фізичного місця перебування офісу.
- Отримання доступу до послуг за мінімальний час при підключенні додаткового офісу.
- Можливість тестової експлуатації послуги без необхідності її реалізації.

Практичний ефект від впровадження NFV / SDN для провайдера:

- ✓ Зниження вартості підключення - послуги віртуалізуються і не вимагають виділеного обладнання.
- ✓ Використання COTS обладнання (стандартне обладнання x86 архітектури)
- ✓ Скорочення або повна відміна виїздів до клієнта для підключення додаткових послуг.
- ✓ Доступ до послуг в режимі 24/7 навіть при переїзді клієнта.
- ✓ Зниження часу як на підключення нового клієнта, так і на додавання нових послуг.
- ✓ Зниження вартості експлуатації.
- ✓ Швидке і еластичне масштабування послуг в залежності від потреб.
- ✓ Уніфіковані вклучення на мережі - зниження кількості різнотипного кінцевого обладнання.

Таким чином, запровадження цих технологій позитивно вплине на рішення деяких проблем у різних компаній та сприяє зниженню CAPEX та OPEX.

Перелік посилань:

1. <http://www.tadviser.ru/index.php/%D0%92%D0%B8%D1%80%D1%82%D1%83%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F>
2. [http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE-%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%8F%D0%B5%D0%BC%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_\(Software-Defined_Network,_SDN\)_%D0%B8_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE-%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%8F%D0%B5%D0%BC%D1%8B%D0%B5_%D0%A6%D0%9E%D0%94_\(Software-](http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE-%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%8F%D0%B5%D0%BC%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8_(Software-Defined_Network,_SDN)_%D0%B8_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE-%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%8F%D0%B5%D0%BC%D1%8B%D0%B5_%D0%A6%D0%9E%D0%94_(Software-)

Defined_Data_Center,_SDDC)#.D0.9F.D1.80.D0.B5.D0.B4.D0.BF.D0.BE.D1.81.D1.8B.D
0.BB.D0.BA.D0.B8_.D0.B4.D0.BB.D1.8F_.D0.BF.D0.BE.D1.8F.D0.B2.D0.BB.D0.B5.D0
.BD.D0.B8.D1.8F_SDN_.D0.B8_NFV

3. [http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:SD-WAN_\(Software_Defined\)](http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:SD-WAN_(Software_Defined))

4. <https://helpiks.org/3-15269.html>

СЕКЦІЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ ФРЕЙМВОРКІВ ДЛЯ МІКРОКОНТРОЛЕРІВ ТА ЗАСОБІВ РОЗРОБКИ

Максимишин О.І., студент 4-го курсу, група 3-41, спеціальність «Розробка програмного забезпечення».

Науковий керівник – викладач **Петровський Р.І.**

Коледж зв'язку та інформатизації ОНАЗ ім. О. С. Попова

***Анотація.** Проводиться аналіз, мета якого – порівняти сучасні фреймворки, які використовуються для розробки програмного забезпечення для мікроконтролерів та апаратні засоби розробки.*

В останні роки активно розвивається ідея ІОТ та різних дистанційно керованих пристроїв. Переважно в цих галузях не можливо використання звичайних комп'ютерів за через низьку причин: габарити, значне енергоспоживання та ціна. Але головною причиною є те, що сучасні комп'ютери та операційні системи не можуть забезпечити відповідний рівень відклику на зовнішні події. Це дуже важливо в критичних галузях, наприклад в машинобудуванні, коли ціна помилки автоматики дуже висока. Для рішення цих проблем було створено мікроконтролери – зменшені копії процесорів з вбудованою пам'яттю та периферією. Замість операційних систем загального призначення було розроблено операційні системи реального часу, які мають гарантований час реакції на зовнішні події.

Історично склалося, що основною мовою програмування мікроконтролерів довго залишався асемблер. Це накладало значні обмеження на складність розроблювальних програм та потребувало значної кваліфікації програмістів. Це було викликано низькою кількістю доступної пам'яті та недостатнім розвитком компіляторів, які створювали не достатньо ефективний код для систем жорсткого реального часу. З розвитком та покращенням компіляторів до інструментів розробки додалася мова С. Вона є досить близькою до апаратного забезпечення, швидка у виконанні та не використовує додаткові ресурси. В цей час з'являються компілятори Basic для мікроконтролерів, але вони програвали С в швидкості та структурованості коду.

Наступним кроком стала поява C++/11, яка принесла шаблони та метапрограмування. Це дозволяє уникнути повторювання коду та створювати гнучкі конструкції, наприклад програмний клас віртуальних портів вводу-виведення, які дозволяють об'єднувати довільні фізичні виводи в логічні порти. Також в цій галузі знайшло місце об'єктно-орієнтоване програмування, яке може бути реалізовано з

використанням шаблонів та статичного поліморфізму. Ще одним нововведенням C++/11-14 стала поява конструкції `constexpr`, яка може бути використана для розрахунків під час компіляції. Це дозволило рахувати параметри реєстрів периферії на етапі компіляції, що дозволяє перевірити коректність параметрів ще до завантаження та зменшити час ініціалізації. Але попри значні переваги дані методики тільки почали розповсюдження в галузі мікроконтролерів, першим масштабним фреймворком, який використовує дані технології став `Modm`.

С розвитком ІОТ з'явилася потреба в засобах для праці з мережевими функціями, котрі повинні буду простими та безпечними при праці в мережі. Для цього були спроби перенесення мов Java та C#, для яких були створені відповідні проекти Java ME embedded та .NET Micro Framework. Проте дані проекти не отримали значного поширення та були припинені. Опосередковано це можливо зв'язати з використанням дорогих плат для розробки з досить потужними мікроконтролерами, в яких значну частину ресурсів займала середовище виконання. Паралельно з цими комерційними проектами розвивалися два аналогічних відкритих проекти Espruino та MicroPython – реалізації JavaScript та Python відповідно. Вони потребують значно менше ресурсів та використовують більш доступні мікроконтролери.

Середовища розробки для мікроконтролерів майже не відрізняються від звичних IDE. Більшість з них являє собою модифіковані версії IDE Eclipse чи Visual Studio, які використовують зовнішній дебагер GDB в купі з сервером відлагодження OpenOCD та сумісні апаратні дебагери.

Актуальність роботи полягає в необхідності використання засобів розробки, що полегшують написання, відлагодження та перенесення програмного забезпечення на різні апаратні платформи.

В ході роботи було розглянуто сучасні інструменти розробки програмного забезпечення для мікроконтролерів. Проведено порівняння апаратних дебагерів, плат для розробки та сучасних фреймворків.

Висновки

За результатами роботи можна зробити наступні висновки:

1) Фреймворк Arduino морально застарів, відсутність засобів відлагодження коду та концепція «скетчів» не дозволяють створювати складні та об'ємні проекти.

2) Фреймворк Modm знаходиться в стані активного розвитку, має модульну структуру та перевірку параметрів периферії під час компіляції, але відсутність мережевого стеку та драйверів мережевих пристроїв робить її мало придатною для використання в ІОТ.

3) Фреймворк RIOT є потужним засобом для організації мережі IOT пристроїв, має зручні засоби відладки (віртуалізація в POSIX середовищі, вбудований термінал), низькі вимоги до апаратної частини, у купі з наявністю багатьох мережевих протоколів.

4) Головним недоліком фреймворку Espruino є підвищені вимоги до продуктивності і обсягу пам'яті пристрою, проте це компенсується тим, що для розробки програмного забезпечення не потрібні IDE та компілятори, бо сумісна плата має власний інтерпретатор JavaScript та інтерактивну консоль.

5) Дебагер Black Magic Probe проявив себе як перспективне та конкурентне рішення в порівнянні з комерційними приладами. Відкритість коду та електронних схем, підтримка спілки та можливість самостійного збирання вкупі з вбудованим сервером відлагодження робить його одним з кращих доступних дебагерів.

Перелік посилань:

1. <https://www.flocman.ru/review/article.html?di=500219> “Почему не стоит использовать Arduino для обучения программированию”
2. <https://habr.com/ru/company/amparka/blog/392399/> “Espruino: JavaScript в микроконтроллере”
3. <https://www.espruino.com/FAQ> “What is Espruino?”
4. <https://microcontrollerelectronics.com/how-to-convert-an-stm32f103c8t6-into-a-black-magic-probe/> “How to convert an STM32F103C8T6 into a Black Magic Probe”
5. <https://modm.io/how-modm-works/> “How modm works”
6. https://www.researchgate.net/publication/320000233_A_Comparative_Study_between_Operating_Systems_Os_for_the_Internet_of_Things_IoT “A Comparative Study between Operating Systems (Os) for the Internet of Things (IoT)”

ПОРІВНЯЛЬНИЙ АНАЛІЗ ТЕХНОЛОГІЙ ПРИ ВИКОРИСТАННІ JAVASCRIPT ТА WEBASSEMBLY

Мерецький К. А., Тиховський С. Л., студенти 3-го курсу, група 3-31, спеціальність 121 «Інженерія програмного забезпечення»

Науковий керівник – викладач **Петровський Р.І.**

Коледж зв'язку та інформатизації ОНАЗ ім. О. С. Попова

Анотація.

Проводиться аналіз, мета якого – порівняти дві сучасні технології, які використовуються для розробки клієнтської частини веб-додатків.

В останні роки навантаження на клієнтську частину браузера помітно зросло: з появою специфікації ES5 мови Javascript, яка привнесла технологію AJAX, з'явилася можливість перекласти велику кількість запитів на користувача веб-сайту, через що використання на веб-сайтах Javascript-коду швидко піднялося. Javascript відкрив для розробників програмного забезпечення багато можливостей.

Після цього, з кожним роком потреби бізнесу щодо веб-додатків зростали: браузерні ігри, різноманітні професійні інструменти, які мали можливість працювати незалежно від платформи через те, що не було необхідності їх встановлювати та запускати. Також це робило їх кросплатформеними — найважливіша вимога до них була виконуватися рушієм браузера.

Але Javascript з самого початку розроблявся як нескладна мова для веб-дизайнерів та людей, далеких до написання коду. Через це він потребував великих потужностей для свого виконання, що робило його повільнішим за низькорівневі мови програмування.

Використання інструменту Emscripten для компіляції коду алгоритмів “Послідовність Фібоначчі”, “Сортування бульбашкою”, “Швидке сортування” на мові програмування C. Розгляд можливостей, переваг, майбутніх впроваджень технології WebAssembly та її взаємодія з браузером. Розробка невеликого веб-додатка, який демонструє роботу алгоритмів та порівнює швидкість виконання програм на Javascript та WebAssembly.

Висновок

За результатами роботи можна зробити висновок, що програми алгоритмів та роботи с числами на WebAssembly виконуються швидше ніж на JavaScript

Перелік посилань:

1. <https://ru.wikipedia.org/wiki/Asm.js>
2. <https://habr.com/ru/post/193642/>
3. http://kripken.github.io/mloc_emscripten_talk
4. <https://ru.wikipedia.org/wiki/WebAssembly>
5. <https://habr.com/ru/post/342180/>
6. <https://webassembly.org/>

ПОРІВНЯЛЬНИЙ АНАЛІЗ HASH-ФУНКЦІЙ

Д'яченко А. І., студентка 2-го курсу, група 3-21, спеціальність 121
«Інженерія програмного забезпечення»

Науковий керівник – к.ф.-м.н. Козловська В.П.

Одеський державний екологічний університет

Анотація. *Кількість інформації, що передається в мережі Інтернет постійно зростає. На даний момент комп'ютери обмінюються тисячами терабайтів даних щодня, з яких вагома частина повинна залишатися секретною. Пропорційно збільшенню об'ємів інформації збільшуються випадки її навмисного або випадкового пошкодження, а також спроби вкрасти або підробити її. Вирішенням подібних проблем є одностороннє криптографічне перетворення, за допомогою якого можливо створити “відображення” оригінальної інформації. Важливим моментом є те, що неможливо отримати оригінал використовуючи “відображення”. Таким перетворенням є хешування. Хешування інформації використовується для перевірки цілісності даних, електронно-цифрового підпису, зберігання та передачі паролів, а також індексування баз даних. Метою цієї роботи є аналіз та порівняльна характеристика найрозповсюдженіших hash-функцій.*

Hash-функція – алгоритм, що призначений для перетворення вхідного інформаційного потоку необмеженого обсягу в послідовність біт фіксованого розміру.

Хешування – процес обробки вхідних даних hash-функцією для отримання hash-суми.

Hash-сума – послідовність біт, що є результатом обробки даних hash-функцією, має фіксований розмір.

Але хешування не є ідеальним вирішенням проблеми, фіксований розмір має свої недоліки - обмежена кількість hash-сум. Наслідком цього є однакові hash-суми для різних вхідних даних. Таке явище має назву - колізія. Відмінною рисою криптографічно стійких hash-функцій - є мінімальна кількість колізій.

Hash-функції поділяють на криптографічні та не криптографічні. Ідеальна криптографічна hash-функція має чотири основні властивості:

1. легкість обчислення hash-суми для будь-якого повідомлення
2. неможливо утворити повідомлення для заданої hash-суми
3. неможливо змінити повідомлення без зміни hash-суми
4. неможливо знайти два різних повідомлення з однаковою hash-сумою

Для проведення порівняльного аналізу hash-функцій було обрано та реалізовано наступні алгоритми:

MD6 (512 біт) - алгоритм хешування змінної розрядності, призначений для створення hash-сум довільної довжини. Використовується для перевірки цілісності і, у деякому сенсі, достовірності опублікованих повідомлень, шляхом порівняння hash-сум повідомлення з опублікованими.

SHA3 (512 біт) - односпрямована hash-функція для створення hash-сум змінної розрядності. Активно використовується в блокчейн-технологіях та електронно-цифрових підписах.

CRC (32 біт) - алгоритм знаходження hash-сум, заснований на певних математичних властивостях циклічного коду. Призначений для перевірки цілісності даних, яка використовується в ZIP, OpenPGP та інших стандартах.

MurmurHash (32 біт) – проста та швидка hash-функція загального призначення, придатних для некриптографічного використання.

BLAKE (512 біт) - криптографічна hash-функція, яка також використовується в блокчейн-технологіях.

CityHash (32 біт) - не криптографічна hash-функції розроблених компанією Google. Використовуються для обчислення hash-сум та зберігання даних у hash-таблицях.

Висновок. Завдяки порівняльному аналізу найрозповсюдженіших hash-функцій було зроблено наступні висновки. Серед криптографічних hash-функцій (MD6, SHA3, BLAKE), що мають майже однакові криптографічні характеристики, треба звертати увагу на розподіленість, яка впливає на можливу кількість колізій, та швидкість, яка залежить від довжини вхідного повідомлення. На невеликих об'ємах даних, наприклад паролі розміром приблизно 20 символів, найшвидшим виявився – SHA3 (~16 мікросекунд), але на великих об'ємах, художній твір, або бінарний файл розміром близько 337 000 байт, – BLAKE (~13771 мікросекунд). При порівнянні не криптографічних hash-функцій (CRC, MurmurHash, CityHash) пріоритетним параметром є швидкість. CityHash може обробити невелике повідомлення за ~4,4 мікросекунди, на що, CRC та MurmurHash, в свою чергу, знадобиться лише ~0,4 мікросекунди. З великою кількістю інформації найшвидше упорається MurmurHash, йому знадобиться лише ~411 мікросекунд. Але слід враховувати, що не криптографічні функції мають порівняно великий коефіцієнт колізій.

Перелік посилань:

1. <https://cryptoperson.ru/cryptography/что-такое-hjesh-kod-i-hjesh-funkcija-prakticheskoe-primenenie-obzor-populjarnyh-algoritmov>
2. <https://bits.media/khesh-funktsiya-sha-3-budushchee-blokcheyna-dlya-rynkov-kapitala/>

3. <https://habr.com/ru/post/178955/>
4. <https://www.securitylab.ru/blog/personal/shaurojen/22829.php>
5. <http://kriptografea.narod.ru/MD6.html>

АНАЛІЗ ВИКОРИСТАННЯ DARKNET ІНТЕРНЕТ-КОРИСТУВАЧАМИ

Філіппова М. В. студентка 2-го курсу, група 3-21, спеціальність 121 «Інженерія програмного забезпечення».

Науковий керівник – к.філос.наук **Кокорєв О.В.**

Коледж зв'язку та інформатизації ОНАЗ ім. О. С. Попова

***Анотація.** У роботі розглянута історія Darknet та його якості, актуальність його використання та безпека користувача.*

Головна мета – звернути увагу аудиторії на різкий зріст користувачів та задалегідь попередити про наслідки.

З тієї самої хвилини, коли в 2013 році Едвард Сноуден розсекретив стеження американських спецслужб, багато людей почали вести боротьбу за свою анонімність. Ніхто не хотів, щоб хтось знав його таємниці, де він знаходиться, чи відношення до дій уряду. Тому анонімність Darknet стала як ніколи доречною.

Завдяки Tor Browser (та ще цілому списку анонімних браузерів) інтернет користувачі мають можливість з легкістю використовувати необмежені знання, зібрані цілими цивілізаціями. Ми можемо “заходити” в уві нам відомі частини інтернету, але з цією владою йде велику відповідальність. Один неправильний хід може згубити життя. Немає статті в якій забороняється використання Darknet, та можливість того, що вас осудять за чужі злочини, неймовірно велика.

З кожним роком кількість користувачів зростала. Кожен прагнув зазирнути в “щілину” безмежних таємниць, схованих у глибинах інтернету. Саме тому така велика кількість сайтів та відео, метою яких є розповісти людям “як потрапити в Darknet”. Отже, треба зауважити, що перш ніж використовувати його у звичайний час – треба знати “що це?” та “як він нам допоможе?”.

Висновки

Результати опитування значної кількості людей демонструють, що досить мале їх число знає, що таке Darknet. Після пошуку великої кількості даних, які згодом допомогли мені зробити певні висновки щодо кількості користувачів цієї загадкової частини “всесвітньої павутини”, можна спокійно сказати, що питання таємності в мережі досі залишається актуальним.

Перелік посилань:

1. Darknet <https://newochem.ru/internet/darknet-o-kotorom-vy-slyshali-vsego-lish-mif/>
2. Tor Browser <https://thebestvpn.com/tor-vs-vpn/>
3. Історія інтернету
<https://www.google.com/amp/s/foreignpolicy.com/2013/12/09/the-darknet-a-short-history/amp/>
4. Bitcoin <https://coinspot.io/beginners/chto-takoe-bitcoin/>
5. Кількість отриманих коштів із Bitcoin
<https://www.statista.com/chart/amp/17128/darknet-use-of-bitcoin/>

ESPORTS SCIENCE AND ITS FUTURE AS A PART OF TRADITIONAL SPORTS

Chervonenko B. M. 3rd year student, group TR-31, course “172”

Kharlamov A. A. 3rd year student, group TO-31, course “172”

Scientific Supervisor – teacher Beldugina S. S.

College of Communication and Informatization O. S. Popov Odessa National Academy of Telecommunications

Annotation. *The main goal of this study is to prove that esports are scientifically relevant as well as to predict its future.*

ESports (also known as “electronic sports”) is a form of competition using video games. Usually, it takes the form of organized multiplayer competitions, either amongst teams of players or standalone players.

Although the mainstream culture files esports as “irrelevant”, it’s about to change. Esports is an ever growing industry with thousands of events happening worldwide and billions of dollars being invested in annually. With millions in its viewer base, eSports are projected to overcome traditional sports in popularity by 2020.

It has to be noted that there is no particular need to look at eSports as an area of disciplines that satisfy a traditional sport definition. We could just as well look at eSports as a completely separated field of study. The overrated question whether competitive gaming is a sport or not is to some extent irrelevant for the academic discussion of eSports. However, the above approach shows that there is a quite natural connection between traditional sports and eSports that goes far beyond the commonly used argument that eSports relates to the training of a proper hand-eye coordination through computer games. It

furthermore allows us to borrow academic approaches and methodologies from traditional sport and training science and to apply them to what might be called “eSports science”.

The potential of this approach lies on the fact that it does not only look at eSports as a phenomenon that deserves to be investigated purely for its influences on society and culture, for example by studying how a fastpaced FPS game such as Counter-Strike influences the use of communication and language of its players. It looks at eSports as a field of study which in return allows us to derive novel approaches and methodologies to actively advance other areas of interest that are not directly related to computer gaming.

Chart 1 – Advantages of esports when compared to traditional sports.

	eSports	Traditional sports
Accessibility	Fully accessible (w/o compromises) to anyone with a mental capacity.	Mostly inaccessible (w/o compromises) to anyone with physical disabilities.
Costs to run	All you need to compete (or run a competition for that matter) is a platform to play your game of choice.	It depends on a sport, but usually the costs are much higher.
Fairness	Usually the rules are programmed into the game, so most of the results are objective.	Most of the sports require a judge, which could influence results with subjective judgement.
Variety	There are countless amounts of genres, which are very different from each other. There are even sports games, which try to emulate most of the traditional sport disciplines.	While there is a fair variety of disciplines, they fail in comparison to the variety of eSport games.
Safety	Mostly safe, but there are minor risks of injury in regards to which peripheral you’re using.	Depends on the sport, but the risks of accidents and injuries (minor and major) are much higher.

ESports are definitely here to stay and will eventually become the cornerstone of human culture, like, for example, soccer.

Conclusion.

In this study, we made a critical analysis of esports and systematized the facts about it. We also tried to convince you to think of esports as a more accessible concept.

Based on our study, we made the following conclusion: eSports are definitely here to stay and will eventually become the cornerstone of human culture. As more people get familiar with the concept, it is probable that eSports would be both more popular and profitable than traditional sports.

References

1. J. Fromme, "Computer Games as Part of Children's Culture", *The International Journal of Computer Game Research*, 2003 [Online] Available at: <http://www.gamestudies.org/0301/fromme/>
2. J. Goldstein, "Violent Video Games" in *Handbook of Computer Game Studies*, eds. Raessens, J. & Goldstein J., MIT Press, Cambridge, 2005.
3. J. Katzenbach and D. Smith, *The Wisdom of Teams: Creating the High-Performance Organization*, HarperBusiness, 1994.
4. M. Kim, "Spiele-Boom in Korea", *Game-Face*, 2005, [Online] Available at: http://www.game-face.de/article.php3?id_article=162
5. M. Knox, "The Sport of Computer Gaming", *3DActionPlanet*, 1999 [Online]: <http://www.3dactionplanet.com/features/editorials/sport/>
6. D. Kushner, *Masters of Doom: How Two Guys Created an Empire and Transformed Pop Culture*, Random House Trade Paperbacks, 2004.
7. C. Tiedemann, "Sport (and culture of physical motion) for historians, an approach to precise the central terms", IX. International CESH-Congress, Crotone, Italy, 2004.
8. *The Frag Diary* 1997, [Online] Available at: <http://bluesnews.com/articles/thefrag.html>
9. *The OGA* 1999, [Online] Available at: http://www.eurogamer.net/article.php?article_id=105
10. T. Welch, "The History of the CPL", *Cyberathlete Professional League 2002* [Online] Available at: <http://www.thecpl.com/league/?p=history>
11. T. Wright, E. Boria and P. Breidenbach, "Creative Player Actions in FPS Online Video Games: Playing Counter-Strike", *The International Journal of Computer Game Research*, 2002, [Online] Available at: <http://www.gamestudies.org/0202/wright/>
12. M. Vansteenkiste and E. Deci, E. "Competitively contingent rewards and intrinsic motivation: Can losers remain motivated?", *Motivation and Emotion*, vol. 27, pp. 273-299, 2003.

ПОРІВНЯЛЬНИЙ АНАЛІЗ VPN СЕРВІСІВ

Белоциця Ю.О., студент 4-го курсу, група К-41, спеціальність 5.05010101
«Обслуговування програмних систем та комплексів»

Науковий керівник – викладач **Орлова Л.Б.**

Коледж зв'язку та інформатизації ОНАЗ ім. О. С. Попова

Анотація. У мережі Інтернет нас чекає багато небезпек, як наприклад: підміна DNS-серверу. Завдяки чому зловмисник може перехопити наші особисті дані, а далі продати їх. Завдяки VPN, ми можемо зашифрувати увесь трафік та передавати його через DNS сервер VPN провайдеру. Але не всі VPN-сервери безпечні, у цій роботі було проаналізовано основні VPN протоколи ринку.

Зараз на ринку є чотири основних протоколу тунельовання(ПТ): OpenVPN, PPTP, L2TP, IPsec IKEv2. Було проаналізовано алгоритми шифрування, порти з'єднання, автентифікацію даних, тощо.

PPTP – стандартний ПТ Windows має слабкий алгоритм шифрування і може бути зламаний, але його досі використовують, тому що простий у налаштуванні і використанні. Також має змінну IP-адрес. Але може бути зламаний завдяки ARP spoofing та використанню chap2asleap.

L2TP має більше мінусів ніж плюсів, перший як мінус так і плюс цього протоколу – подвійне інкапсулювання: спочатку створюється тунель IPsec, а потім вже через нього проходять дані L2TP, з одного боку це підвищує безпеку, з іншого дуже уповільнює швидкість роботи. Також використовує стандартний порт UDP(500), тому може бути заблокований. Працює з шифрами 3DES та AES. Перший може бути зламано за допомогою атаки meat in the middle, або атаки типу sweat32. Ще одним мінусом є те, що він використовує PSK(pre-shared keys), завдяки чому зловмисник може видати себе за VPN сервер та прослуховувати трафік. Але є й плюс, ОС мають підтримку цього ПТ, не має інформації про можливість розшифрувати данні, які було зашифровано за допомогою AES.

IPsec IKEv2 – це авторизація через сертифікат, тому має підтримку не на всіх ОС(хоча, сам IPsec має підтримку на всіх ОС). Ipsec IKEv2 працює значно швидше, ніж L2TP/IPsec, але повільніше ніж PPTP, але він працює на мережевому рівні моделі OSI, тому може шифрувати початковий пакет цілком, або від транспортного рівня і вище. Також має механізми обходу NAT. Через все це, складний, як у налаштуванні, так і у використанні, не має стандартизованих термінологій і інструментів конфігурації. Також він пропонує використовувати сильні алгоритми шифрування, але використання сильних алгоритмів шифрування вимагає хороші обчислювальні

потужності. Також легко може бути виявлено за допомогою DPI(Deep packet inspection).

OpenVPN – opensource проект, який більшість спеціалістів на сьогоднішній день вважає найбільш безпечним варіантом побудови VPN. На мій погляд так вважають завдяки його налаштованості, наприклад його можливо налаштувати для роботи через порт 443, що маскує його під HTTPS, тим самим ускладнює його блокування. Також він використовує бібліотеку OpenSSL, яка підтримує багато криптоалгоритмів – 3DES, CAST-128, Camelia, AES, Blowfish.

Висновок.

Завдяки аналізу рішень, що є зараз основними на ринку, було виявлено, що найбезпечнішим з них є OpenVPN, завдяки тому що має багато можливостей для налаштування, на друге місце був поставлений IPsec IKEv2, через те, що використовує новий стандарт протоколу обміну ключами, та може також бути замаскований, але для того, щоб використовувати його безпечно, треба мати навички мережевого інженера, та хороші обчислювальні потужності, крім того він може бути знайдений за допомогою DPI. На третьому місці стоїть L2TP/IPsec, завдяки тому, що має можливість безпечного налаштування, завдяки AES, але використовує стандартний порт, та може бути зламаний через підміну PSK. І на останньому місці стоїть PPTP, через те, що не має можливості налаштування, може бути заблокований, та зламаний за допомогою атаки через ASLEAP.

Перелік посилань:

1. <https://openvpn.net/vpn-server-resources/>
2. <https://www.infoworld.com/article/3112324/new-collision-attacks-against-triple-des-blowfish-break-https-sessions.html>
3. RFC 7296 – Internet Key Exchange Protocol Version 2 (IKEv2)
4. RFC 3193 – Защищая L2TP використовуючи IPsec
5. RFC 2637 – Point-to-Point Tunneling Protocol (PPTP)
6. Zhu, Bo; Guang Gong (2011). “MD-MITM Attack and Its Applications to GOST, KTANTAN and Hummingbird-2”
7. Andrew Mason. IPSec Overview

Технічний редактор – *Горлінська О. Ю.*, заступник директора з НР
Комп’ютерне макетування – *Орлова Л. Б.*, викладач

Здано в набір 26.03.2019 р. Підписано до друку 27.03.2019 р.

Тираж 20 прим. обсяг 0,1 друк. арк.

Віддруковано в коледжі зв’язку та інформатизації ОНАЗ ім. О.С. Попова

© КЗІ ОНАЗ, 2019.