МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ
ДЕРЖАВНОГО УНІВЕРСИТЕТУ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ»

Одинадцята студентська науково-технічна конференція, присвячена 100-річчю коледжу

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

22 травня 2021 року

Збірка тез

Одеса, 2021

Телекомунікаційні, інформаційні та комп'ютерні мережі і системи: теперішнє та майбутнє: матеріали одинадцятої студентської науково-технічної конференції, присвяченої 100-річчю коледжу, м. Одеса, 22 травня 2021 року – Одеса, ВСП «ФКЗІ ДУІТЗ», 2021 – 42 с.

Дана збірка містить тези матеріалів, що представлені на одинадцятій студентській науково-технічній конференції «**Телекомунікаційні, інформаційні та комп'ютерні мережі і системи: теперішнє та майбутнє»**, присвяченої 100-річчю коледжу, що проводиться 22.05.2021 р. у відокремленому структурному підрозділі «Фаховий коледж зв'язку та інформатизації Державного університету інтелектуальних технологій і зв'язку».

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 ВСП «Фаховий коледж зв'язку та інформатизації ДУІТЗ»

ЗАСТУПНИК ГОЛОВИ ОРГКОМІТЕТУ:

Горлінська О. Ю. – заступник директора з навчальної роботи

СЕКРЕТАР ОРГКОМІТЕТУ:

Гуменна О. А. – завідувач навчально-методичного кабінету

ЧЛЕНИ ОРГКОМІТЕТУ:

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

Владова Т. С. – завідувач денного відділення

Гуменна О. А. – завідувач навчально-методичного кабінету, секретар оргкомітету

Кокорєва З. Р. – голова циклової комісії інтелектуальних технологій та зв'язку

Орлова Л. Б. викладач циклової комісії інтелектуальних технологій та зв'язку

Малюта С. О. – викладач циклової комісії інтелектуальних технологій та зв'язку

Д'яченко А. І. – голова ради студентського самоврядування, студентка групи З-41

ЖУРІ КОНФЕРЕНЦІЇ

ГОЛОВА ЖУРІ:

Стерлковська І. В. – д.т.н, професор, директор ННІ інфокомунікацій та програмної інженерії ДУІТЗ

ЧЛЕНИ ЖУРІ:

секція автоматизації, телекомунікацій та радіотехніки

Баляр В. Б. – к.т.н., старший викладач кафедри телебачення та радіомовлення ДУІТЗ

Пилявський . В. – к.т.н., доцент кафедри телебачення та радіомовлення ДУІТЗ

секція інформаційних технологій

Кумиш В. Ю. – к.т.н, начальник НДЧ ДУІТЗ

Царьов Р. Ю. – старший викладач кафедри мереж зв'язку ДУІТЗ

секція комп'ютерних технологій та захисту інформації

Стайкуца С. О. – к.філос.н., доцент кафедри кібербезпеки та технічного захисту інформацій ДУІТЗ

Басов В. Є. – к.т.н., доцент кафедри кібербезпеки та технічного захисту інформацій ДУІТЗ

ЗМІСТ

Секція автоматизації, телекомунікацій та радіотехніки

1. Москаленко Т. Д., Литвиненко В. С. Порівняльний аналіз систем оптичної передачі інформації по GPON та EPON 5

2. Широков Л. І. Дослідження підсилювачів частот у гітарному обладнанні 8

3. Поліщук А. В. Порівняльний аналіз сигнальних конструкцій 5G 11

4. Случик М. В., Бартков Б. Л. Розробка макету метеостанції на основі Adruino nano 15

5. Івашковська К. Ю. Аналіз випливу електромагнітних хвиль 5G на організм людини 17

Секція інформаційних технологій

1. Побережний М. В., Загребельний А. Ю. Розробка аудіо-додатку у програмному середовищі JUCE 20

2. Галабурда В. Г. Система контролю облікових записів пацієнтів кінезіоцентру 23

3. Яценко О. К. Інформаційне та програмне забезпечення системи автоматизованого моніторингу відвідуваності занять 25

4. Салабай М. О. Перспективи застосування графічних калькуляторів у сучасній освіті 27

5. Шевченко Л. В. Розробка сайтів для створення чат-ботів 30

Секція комп'ютерних технологій та захисту інформації

1. Петін М. В., Букач В. М. Розробка програмного забезпечення гри на основі платформи UNITY 2D 32

2. Тишкул М. В. Квантовий розподіл ключів – нова технологія криптографічного захисту інформації 34

3. Дроздовський М. Д. Аналіз методів захисту від атак типу «розподілена відмова в обслуговуванні» (DDoS) 36

4. Яроцька Д. С. Електронний цифровий запис. Особливості використання в Україні 38

ПОРІВНЯЛЬНИЙ АНАЛІЗ СИСТЕМ ОПТИЧНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ ПО GPON ТА EPON

Москаленко Т. Д., Литвиненко В. С, студенти 4-го курсу, групи Тр-41, спеціальність 172 Телекомунікації та радіотехніка.

Науковий керівник – Бєльдюгіна С. С., викладач циклової комісії інтелектуальних технологій та зв'язку ВСП «Фаховий коледж зв'язку та інформатизації ДУІТЗ»

Анотація. *У роботі запропоновано методику розрахунку загасання сигналу для GPON і EPON та проведено розрахунки втрат сигналу у лінії між OLT та ONU.*

Головна мета – порівняльний аналіз двох систем оптичного передавання інформації GPON і EPON та визначення величини похибки між виміряними та розрахованими значеннями сигналу.

В даній роботі розглянуто системи оптичного передавання сигналу по GPON та EPON, приведені відмінності систем GPON та EPON, зроблено детальний опис абонентського терміналу. Є необхідність враховувати всі особливості кожної з технологій, щоб віддати перевагу, вибираючи між технологіями - у кожної з них є свої плюси і мінуси, від яких залежить майбутній бюджет проекту. Для обох технологій використовується метод шифрування з використанням ключа довжиною в 128-біт. EPON і GPON працюють на однакових частотних планах: downstream йде в діапазоні 1480 ~ 1500 нм, upstream розрахований на довжини в рамках 1260-1360 нм, довжина хвилі наближена до значення 1550 нм зазвичай зарезервована для ТВ-сигналу або інших застосувань. GPON і EPON ідентичні за винятком швидкості і створені за одним стандартом IEEE 802.3 ah, а GPON - принципово інша технологія на основі стандарту ITU-T G.984. Окрім того, проаналізовано тип обладнання, яке використовувалось в роботі, запропоновано методику розрахунку загасання сигналу для GPON та EPON. Проведено аналіз отриманих даних та визначено похибку між розрахованими та експериментальними даними. На основі отриманих результатів аналізу сформовано рекомендації щодо використання GPON та EPON.

Значення розрахованих і виміряних значень сигналу зведено до таблиці 1.

Таблиця 1 – Значення розрахованих і виміряних значень сигналу

	При-хід сигна лу	$N_р$	$A_р$, дБ	$N_з$	$A_з$, дБ	$A_{роз_1}$ дБ	$A_{роз_2}$ дБ	a	A, дБ	$A_{розрах.}$	$A_{виміряне}$
GPON	+3дБ	1	0,05	5	0,05	13,9	10,7	0,22	26,61	-23,61	-23,68
EPON		1	0,05	5	0,05	13,9	10,7	0,22	24,94	-21,94	-21,74

Експериментально виявлено, що застосування вказаної методики та обладнання дає середню похибку між розрахунковими та реальними значеннями сигналу при GPON на рівні 0,2 дБ, а при EPON така похибка складатиме 0,07дБ. У GPON рівень сигналу гірший ніж у EPON з урахуванням того, що кількість абонентів відрізняється і, відповідно, середнє загасання сигналу виходить більше ніж у EPON.

Висновки

За результатами роботи можна зробити такі висновки:

– детально проаналізовано системи EPON та GPON;

– проведені розрахунки втрати сигналу між OLT та ONU;

– запропоновано та детально проаналізовано тип обладнання для оптичних мереж;

– проведено порівняння розрахованих та виміряних сигналів;

– на основі результатів досліджень сформовано наступні рекомендації:

– систему оптичного передавання інформації GPON вигідніше використовувати ніж EPON, тому що за рахунок більшої кількості абонентів більше компенсуються витрати.

Перелік посилань

1. https://www.ua5.org/lan/136-merezh-ethernet-jj-fast-ethernet.html - Мережі Ethernet й Fast Ethernet.

2. https://deps.ua/katalog/opticheskie-muftyi/ru-myfta-opticheskaya-crosver-fosc-spm.html - Муфта оптическая Crosver FOSC-SPM.

3.https://yunc.org/%D0%AD%D0%9B%D0%95%D0%9A%D0%A2%D0%A7%D0%95%D0%A1%D0%9A%9B%D0%AC#:~:text=%D0%9F%D1%80%%BB%D1%8F.&text=%D0%92%20%D1%82%D0%B0%D0%BA%D0%BE%D0%BC%20%.

4. https://m.eltexsl.ru/gpon-vs-bdcom – Eltex Solutions. Официальный дилер завода. GPON или EPON? Eltex или BDCOM?

5. http://sysadm.pp.ua/internet/standarty-ethernet.html - Стандарты Ethernet.

6. https://habr.com/ru/post/208202 – Шпаргалка по типам и стандартам Ethernet 802.3.

ДОСЛІДЖЕННЯ ПІДСИЛЮВАЧІВ ЧАСТОТ У ГІТАРНОМУ ОБЛАДНАННІ

Широков Л. І. студент 3-го курсу, групи Тр-31, спеціальність 172 Телекомунікації та радіотехніка

Науковий керівник – Бєльдюгіна С. С., викладач циклової комісії інтелектуальних технологій та зв'язку ВСП «Фаховий коледж зв'язку та інформатизації ДУІТЗ»

Анотація. *В даному дослідженні ми зануримося у специфіку підсилювального гітарного обладнання, порівняємо різні типи ПНЧ в цій сфері та дізнаємося, чи зможуть цифрові технології замінити аналогове гітарне обладнання.*

Головна мета – дослідження принципів роботи різних типів гітарних підсилювачів та їх порівняння між собою.

Електрогітара – музичний інструмент, що використовує явище електромагнітної індукції для перетворення енергії механічного коливання металевих струн в електричний сигнал. Звісно, електричний струм, наведений в обмотці катушки коливанням струн є дуже слабким. Для оптимального використання його необхідно підсилити. Проте функції підсилювача низьких частот в даному випадку не обмежуються тільки задачею підсилення сигналу. ПНЧ формує базовий гітарний звук, який потім підлягає різноманітним обробкам, при чому роль ПНЧ в цьому процесі не менша, ніж в самої електрогітари. Тож підсилювач є невід'ємною ланкою в ланцюзі формування електрогітарного звуку та його подальшому використанні.

В гітарному обладнанні для формування та підсилення сигналу використовувалися в основному аналогові схеми на електронних лампах (вакуумні) та транзисторах (твердотільні). Наразі набирає популярності програмна емуляція гітарного підсилювача.

На запитання: "який тип гітарних підсилювачів є найкращим?", є однозначна відповідь – лампові. Лампові гітарні підсилювачі створюють класичне електрогітарне звучання, улюблене музикантами, проте в них є ряд техніко-експлуатаційних недоліків. Найвагоміші: професійне лампове обладнання має високу ціну для середнього споживача ринку, таке обладнання часто масивне та занадто чутливе до механічних навантажень.

Тож задача будь-якого іншого типу гітарного підсилювача – апроксимація, максимальне наближення до характеристик лампового звуку без самих радіоламп, поєднання якості, невисокої вартості та малих габаритів.

Основні відмінності впливу транзисторних і лампових підсилювачів на сигнал: на лінійній ділянці роботи вакумні підсилювачі вносять більше спотворень, ніж твердотільні, з переважаючою другою гармонікою, рівень спотворень нарощується плавно зі збільшенням рівня сигналу (динамічне спотворення), відбувається його компресія, перехід на нелінійну ділянку поступовий; в твердотільних підсилювачах на лінійній ділянці амплітудної характеристики вноситься менший рівень нелінійних спотворень, які не залежать від рівня сигналу, а на нелінійній ділянці сигнал жорстко кліпується, перехід на нелінійну ділянку різкий, в спектрі гармонік за з'являється багато високочастотних компонент.

Під цифровими гітарними підсилювачами розуміють емуляцію (імітацію) роботи аналогового підсилювального тракту, його впливу на звуковий сигнал за допомогою спеціальних алгоритмів програмування на цифрових пристроях. Цифрова обробка сигналу дуже корисна тим, що за її допомогою можна змінювати та перетворювати сигнал практично будь-яким чином. Тобто, в теорії, для нашого випадку можна імітувати будь-яке звучання, чи лампових, чи транзисторних підсилювачів.

З часом, на мою думку, цифрова емуляція буде все більше витісняти аналогове обладнання на професійній арені, особливо в студіях звукозапису, а в домашньому використанні вона вже зараз є найкращим рішенням для споживача ринку гітарного обладнання.

Висновки

За результатами роботи можна зробити такі висновки:

– досліджено основні принципи роботи лампових, транзисторних та цифрових гітарних підсилювачів;

– розглянуто явище нелінійних спотворень підсилювачів та його вплив на сигнал електрогітари;

– порівняно недоліки та переваги різних типів гітарних підсилювачів;

– на основі результатів дослідження сформовано наступні висновки:

– для домашнього використання цифрові гітарні підсилювачі є найкращим рішенням. В подальшому вони будуть витісняти аналогове гітарне обладнання і в професійній (концертній та студійній) сфері.

Перелік посилань

1. http://www.muzoborudovanie.ru/equip/instr/combo/amps/amps.php - Использование гитарных усилителей Владимир Севостьянов.

2. https://electroclub.info/articles/stati-punkt-1/tubes-and-hybrids - Лампы или транзисторы?

3. https://www.kenrockwell.com/audio/why-tubes-sound-better.htm - Why Tubes Sound Better.

4.https://nssound.ru/svedenie-i-mastering/iskazhenie-signalov-distortion/distortion-distorshn-distoshn - Что такое эффект — distortion? Принцип действия эффекта, применение в проектах, известные исполнители, использующие данный эффект, цифровые и аналоговые устройства с примерами.

5. http://jablog.ru/blog/workshop/3647.html - Лампы для гитарного усилителя: в чем различия?

6. http://www.n-audio.com/articles/acu9.htm - О заметности искажений.

7. https://gigabaza.ru/doc/47426.html - Усилитель мощности с улучшенным спектром гармоник и вопросы оценки нелинейных искажений.

8.http://wikisound.org/%D0%94%D0%B8%D1%81%D1%82%D0%BE%D1%80%D1%88%D0%BD – Сведение и мастеринг.

9. http://electrovoice.com.ua/articles.php?id=10 – Ирина Алдошина. Субъективная оценка нелинейных искажений.

10.https://guitargearfinder.com/guides/ultimate-guide-to-impulse-responses-for-guitarists - Ultimate Guide to Impulse Responses for Guitarists.

11.https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%B3%D1%96%D1%82%D0%B0%D1%80%D0%B0 – Електрогитара.

ПОРІВНЯЛЬНИЙ АНАЛІЗ СИГНАЛЬНИХ КОНСТРУКЦІЙ 5G

Поліщук А.В., студентка 4 курсу, група Тр-41, спеціальність 172 «Телекомунікації та радіотехніка»

Науковий керівник – Орябінська О.О., викладач кафедри телекомунікаційних систем ДУІТЗ

Анотація. *В роботі розглянуті основні сигнальні конструкції OFDM, GFDM, UFMC, f-OFDM і FBMC, рекомендовані до застосування в системах 5G. Ефективність сигнальних конструкцій оцінювалася за трьома критеріями: спектральна густина потужності, частотно-часова ефективність та обчислювальна складність.*

Останнім часом мережі п'ятого покоління (5G) привертають більше уваги промислових і академічних дослідників через швидке зростання ринку зв'язку. У 5G було введено кілька додатків для задоволення нових вимог цього ринку, наприклад, зв'язок між машинами (M2M), інтернет речей (IoT) і зв'язок між транспортними засобами (V2V). Це вимагає використання нової системи на фізичному рівні (PHY) та виконання вимог нових додатків. Сигнальні конструкції є однією з основних складових фізичного рівня системи, а отже проведення порівняльного аналізу сигнальних конструкцій, що рекомендуються для систем 5G є своєчасним завданням.

Головним недоліком систем 4G є неможливість досягти максимальних користувальницьких швидкостей передачі даних при одночасному обслуговуванні декількох абонентів, а в контексті нових вимог для 5G він стає особливо істотним. Крім того, розподіл ортогонального ресурсу вимагає суворої синхронізації, що пов'язане з додатковими часовими затримками в радіоінтерфейсі, неприйнятними у випадках численних з'єднань в реальному масштабі часу.

Фокус дослідних робіт в рамках 5G зосереджений саме на пошуку нових методів множинного доступу, бо ця область реально містить потенціал для усунення зазначених недоліків за рахунок різних схем виділення декільком користувачам одного і того ж ресурсу (неортогонального призначення ресурсу як у часовому, так і в частотному доменах).

Ці методи поки не систематизовані і в деяких випадках дублюють один одного, маючи різні назви.

Задачею дослідження є систематизація відомостей про сигнальні конструкції 5G та порівняння їх за певними критеріями.

Основні параметри, за якими порівнювалися сигнальні конструкції:

1. частотно-часова ефективність;

2. спектральна густина потужності, а саме рівень поза смугового випромінювання;

3. обчислювальна складність визначається кількістю дійсних множень на пакет.

Частотно-часова ефективність

Частотно-часова ефективність залежить від форми сигнальної конструкції і є важливим параметром для порівняння характеристик різних сигналів. В часовій області ефективність визначається відношенням частки часу в пакеті витраченого на передавання інформації до загальної тривалості пакету, включаючи циклічні префікси та "хвости" символів через розтягнення за рахунок фільтрації. Ефективність в частотній області визначається відношенням кількості під несучих, на яких передаються дані до загальної кількості піднесучих, включаючи захисні інтервали частот, так звані нульові піднесучі.

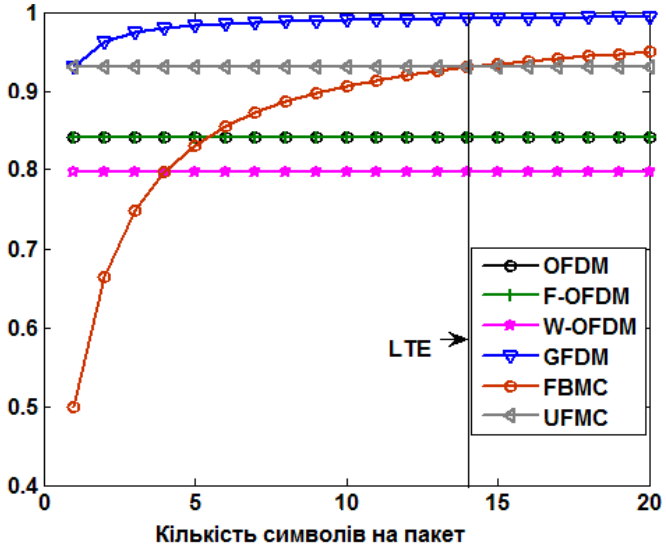

Рисунок 1 – Частотно-часова ефективність в залежності від розміру пакета

Припускаючи, що один користувач займає всю смугу пропускання, рисунок 1 демонструє порівняння частотно-часової ефективності різних сигнальних конструкцій в залежності від кількості символів в пакеті .

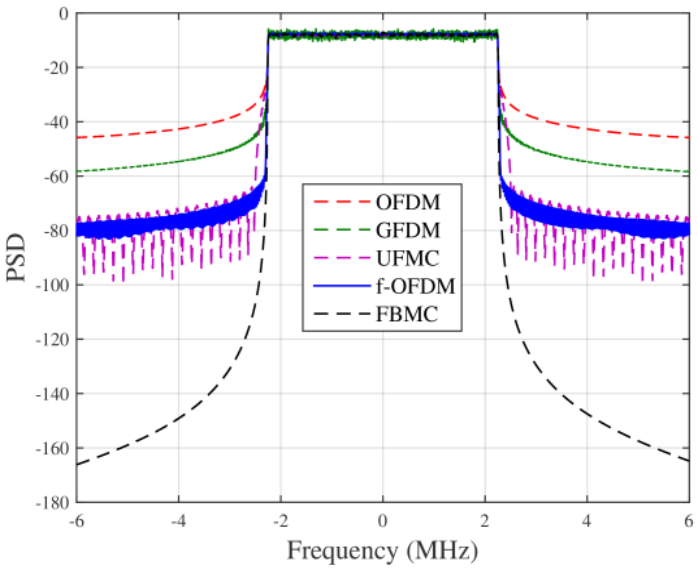

Рисунок 2 – Типові графіки спектральної густини потужності при однаковій кількості службових даних

Частотно-часова ефективність усіх сигнальних конструкцій крім GFDM та FBMC не залежить від розміру пакета. Частотно-часова ефективність FBMC наближається до ефективності OFDM, коли розмір пакета наближається до 5, і він показує більшу ефективність для розмірів пакета, що перевищує 5 символів. Ґрунтуючись на цих аналітичних результатах, можна зробити висновок, що і UFMC, і GFDM більше підходять для передачі короткими пакетами в порівнянні з іншими сигнальними конструкціями. FBMC більше підходить для передачі довгих пакетів і неефективний для передачі коротких пакетів.

Спектральна густина потужності

Як бачимо з графіків найнижчий рівень позасмугового випромінювання в FBMC. В UFMC та f-OFDM рівні позасмугового випромінювання співрозмірні та у порівнянні з FBMC значно більші. Порівняно з UFMC та f-OFDM у GFDM рівень позасмугового випромінювання більший приблизно на 20 дБ. За величиною позасмугового випромінювання найбільшу перевагу має FBMC.

Обчислювальна складність

Обчислювальна складність сигнальних конструкцій 5G розглядалася з точки зору загальної кількості необхідних реальних множень на пакет, що складається з M символів з декількома несучими (кожен символ складається з N піднесучих) [2]. При

обчисленні складності UFMC і GFDM передбачається, що кожне комплексне множення може бути виконано з використанням трьох дійсних множень.

В порівнянні з OFDM, WOFDM має найнижчу складність. F-OFDM і FBMC приблизно в п'ять і шість разів складніше OFDM, а GFDM майже в 12 разів складніше в порівнянні з OFDM. Найвищу складність демонструє UFMC. Складність UFMC прямо пропорційна кількості піддіапазонів, які, в свою чергу, залежить від розміру піддіапазону. Слід зазначити, що більш ефективні способи реалізації, наприклад багатофазна реалізація, можуть знизити складність UFMC майже в 4,5 рази [2]. Використання меншого розміру ШПФ на піддіапазон в UFMC також може значно знизити складність [2].

Висновки

Однозначного рішення щодо найкращої сигнальної конструкції для систем 5G немає. В залежності від особливостей передавання сигналу (короткі пакети або довгі) та бажаної складності обладнання, яка суттєво впливає на вартість обладнання та час затримки при обробці, оптимальними будуть різні рішення щодо вибору сигнальної конструкції.

Перелік посилань

1. Al-Jawhar, Y.A., Ramli, K.N., Taher, M.A., Shah, N.S.M., Mostafa, S.A. and Khalaf, B.A. (2021), Improving PAPR performance of filtered OFDM for 5G communications using PTS. ETRI Journal. https://doi.org/10.4218/etrij.2019-0358.

2. Ayesha Ijaz, Lei Zhang, Pei Xiao and Rahim Tafazolli (December 14th 2016). Analysis of Candidate Waveforms for 5G Cellular Systems, Towards 5G Wireless Networks - A Physical Layer Perspective, Hossein Khaleghi Bizaki, IntechOpen, DOI: 10.5772/66051. Available from: https://www.intechopen.com/books/towards-5g-wireless-networks-a-physical-layer-perspective/analysis-of-candidate-waveforms-for-5g-cellular-systems#B15.

3. Xi Zhang1, Ming Jia2, Lei Chen1, Jianglei Ma2, Jing Qiu1 1Chengdu Research & Development Centre, Huawei Technologies Co., Ltd., People’s Republic of China 2Ottawa Research & Development Centre, Huawei Technologies Canada Co., Ltd., Canada Filtered-OFDM — Enabler for Flexible Waveform in The 5th Generation Cellular Networks. Available from: https://www.groundai.com/project/filtered-ofdm-enabler-for-flexible-waveform-in-the-5th-generation-cellular-networks/1.

4. Van Eeckhaute, M., Bourdoux, A., De Doncker, P. et al. Performance of emerging multi-carrier waveforms for 5G asynchronous communications. J Wireless Com Network 2017, 29 (2017). https://doi.org/10.1186/s13638-017-0812-8.

РОЗРОБКА МАКЕТУ МЕТЕОСТАНЦІЇ НА ОСНОВІ ADRUINO NANO

Случик М.В., студентка 3-го курсу, група К-31, 122 «Комп'ютерні науки» спеціальність, Бартков Б.Л., студент 3-го курсу, група То-31, спеціальність 172 «Телекомунікації та радіотехніка».

Науковий керівник – Кокорєв О. В., викладач циклової комісії інтелектуальних технологій та зв'язку ВСП «Фаховий коледж зв'язку та інформатизації ДУІТЗ»

Анотація. *Розглянуто принцип роботи Adruino nano та датчики MQ-4, AM2302. Зображено принцип побудови метеостанції на базі Adruino nano та мову програмування C/C++*

На сьогоднішній час є безліч різних домашніх метеостанцій, але нашою метою є акцентувати як важливо на даний час в будинку контролювати такі показники як; температуру, вологість, та рівень CO2..

В основу проекту закладено виміри в кімнаті в майбутньому макет буде вдосконалюватись та будемо збільшувати програмні та фізичні показники тобто навчити вимірювати не тільки вуглекислий газ але й природний і зріджений гази та інші які можуть нашкодити людині.

Використовуючи мікроконтролер та ці всі датчики потрібно дотримуватись алгоритму побудови пристрою:

1. Намалювати принципову схему пристрою
2. Створити макетну плату та розпаяти датчики та модулі
3. Тестування кожного датчика та модуля
4. Створення ПО
5. Тестування ПО
6. Отримання результатів показників

Ми акцентуємо увагу на створення ПО.

Для створення програмного забезпечення для Arduino ми використали Arduino IDE та такі бібліотеки:

1. U8glib.h (Бібліотека для роботи з OLED екраном SSD1306)
2. stDHT.h (Бібліотека для роботи з DHT22 AM2302)

Розберемо частину коду, а саме вивід інформації на OLED екран.

```
#include "U8glib.h"  //Інстлаляція бібліотеки

U8GLIB_SH1106_128X64 u8g(U8G_I2C_OPT_NONE); // підключеня OLED екрану по I2C / TWI

void draw(void) {

  u8g.setFont(u8g_font_unifont); // Шрифи
  u8g.setPrintPos(0, 20); //розміщення строки
    u8g.print("weather station"); //відображення інформації
}
void setup(void) {

}
void loop(void) {  //
  u8g.firstPage();
  do { // функція друку
    draw();
  } while( u8g.nextPage() );

  delay(500); // Відновлення картинки
}
```

Висновки

В результаті виконаної роботи було створено метеостанцію. Також було додане самостійне живлення від батарейок. Експериментальним методом в різних місцях Одеси було виведено, що усі дані зчитуються правильно, з можливістю похибки у 0,02%. Ми навчилися працювати у парі, познайомилися з Adruino nano/

Перелік посилань

1.https://catcatcat.d-lan.dp.ua/shemotehnika/oled-displei/drayver-oled-ssd1306/#:~:text=SSD1306%20%D1%8F%D0%B2%D0%BB%D1%8F%D0%B5%D1%82%D1%81%D1%8F%20%D0%BE%D0%B4%D0%BD%D0%BE%D0%BA%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9%20%D0%9A%D0%9C%D0%9E%D0%9F%20OLED,%D0%B2%D0%BD%D0%B5%D1%88%D0%BD%D0%B8%D1%85%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%BE%D0%BD%D0%B5%D0%BD%D1%82%D0%BE%D0%B2%20%D0%B8%20%D0%BF%D0%BE%D1%82%D1%80%D0%B5%D0%B1%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D1%8D%D0%BD%D0%B5%D1%80%D0%B3%D0%B8%D0%B8 - Драйвер OLED SSD1306.

2.https://all-spares.ua/ru/technical-articles/what-does-18650-battery-mean.html#:~:text=%D0%90%D0%BA%D0%BA%D1%83%D0%BC%D1%83%D0%BB%D1%8F%D1%82%D0%BE%D1%80%2018650%20%E2%80%93%20%D1%8D%D1%82%D0%BE%20%D0%BB%D0%B8%D1%82%D0%B8%D0%B9%2D%D0%B8%D0%B

E%D0%BD%D0%BD%D0%B0%D1%8F,%D0%BE%D1%82%201600%20%D0%B4%D0%BE%203600%20%D0%BC%D0%90%D1%87.&text=%D0%9D%D0%B0%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D1%80%2C%20%D1%81%D0%B2%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%BE%D0%B4%D0%BD%D1%8B%D0%B5%20%D1%84%D0%BE%D0%BD%D0%B0%D1%80%D0%B8%2C%20%D0%B1%D0%B0%D1%82%D0%B0%D1%80%D0%B5%D0%B8%20%D0%B2,%D0%BD%D0%BE%D1%83%D1%82%D0%B1%D1%83%D0%BA%D0%B0%D1%85%2C%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%B2%D0%B5%D0%BB%D0%BE%D1%81%D0%B8%D0%BF%D0%B5%D0%B4%D1%8B%20%D0%B8%D0%BB%D0%B8%20Power%20Bank - Что такое аккумулятор 18650?

3. https://blog-programmista.ru/post/80-arduino-ide-cto-eto-za-programma.html - Arduino IDE что это за программа?

4.https://radioprog.ru/shop/merch/10 - Arduino Nano.

5.https://habr.com/ru/post/313490 - Подключение oled дисплея с контроллером SSD1306 к STM32 по I2C

6.https://arduinomaster.ru/datchiki-arduino/datchiki-temperatury-i-vlazhnosti-dht11-dht22 - Подключение датчика DHT11 или DHT22 к Ардуино.

АНАЛІЗ ВПЛИВУ ЕЛЕКТРОМАГНІТНИХ ХВИЛЬ 5G НА ОРГАНІЗМ ЛЮДИНИ

Івашковська К. Ю., студентка 2-го курсу, група То-21, спеціальність 172 «Телекомунікації та радіотехніка».

Науковий керівник – Сідень С. В., к.т.н., викладач кафедри технічної електродинаміки та систем радіозв’язку ДУІТЗ.

Анотація. *Проводиться аналіз, мета якого – підтвердити або спростувати чутки про небезпечний вплив 5G на організм людини.*

Одразу після появи інформації про 5G суспільство зацікавилося поглибленим вивченням нової технології, зовсім не схожої на те, чим ми користувалися по сьогодення. Мережі мобільного зв'язку пройшли великий шлях розвитку; з'явилися нові типи користувача пристроїв - смартфони і планшети. Можливості, які відкривають мобільні технології сього-дні, вже давно вийшли за рамки голосових послуг, створюючи нові способи спілкування, обміну даними та бізнес-моделі, тому прогрес в цій галузі нам критично необхідний. Мобільні системи 5G зараз розробляються для задоволення вимог з точки зору швидкості передачі даних, затримки, надійності та з низькою вартістю.

Сучасні люди проводять величезну кількість часу спілкуючись за допомогою мобільних телефонів, але лише деякі розуміють, як саме вони працюють і як впливають на наш організм. Страхи та хвилювання про те, що робота п'ятого покоління мобільного зв'язку та можливі наслідки його впливу та шкоди на організм людини зростають. І як завжди люди поділилися на дві групи: ті, хто чекає на нові пристрої зв'язку та ті, хто бояться.

Всі побоювання спричинені в основному використанням високих радіочастот, які дозволяють домогтися високих швидкостей передачі даних. Суть у тому, що на великих відстанях вони менш надійні, ніж звичні та низькі частоти. Для того щоб забезпечити покриття, провайдерам доведеться побудувати більше невеликих точок доступу.

5G працює на вкрай високих частотах. Це випромінювання є неіонізуючим тому, що енергія фотонів не є достатньою для видалення електрона від атома або молекули. Посилення досліджень застосувань та нових технологій стимулювало інтерес, а також занепокоєння щодо біологічної безпеки при таких частотах. Потрібне біологічне дослідження, щоб забезпечити безпеку та покращити наші основні розуміння взаємодії системи вкрай високих частот з людським тілом. Більше того, з точки зору технічної безпеки, це дослідження також необхідне для точної оцінки потенційних небезпек для здоров'я, пов'язаних з опроміненням. Також для розробки та оновлення стандартів безпеки для такого режиму

Для дослідження впливу електромагнітних хвиль було зроблено експериментальну модель голови людини, яка складається зі шкіри та мозку. Аналіз проводився у середовищі електродинамічного моделювання FEKO. Одним з варіантів використання такого програмного продукту є аналіз впливу електромагнітних хвиль на живі організми. В основному вплив ЕМ хвиль аналізується на основі питомого коефіцієнта поглинання електромагнітної енергії (Specific absorption rate, SAR) – показник, що визначає енергію електромагнітного поля, що виділяється в тканинах тіла людини за одну секунду.

$$\mathrm{SAR} = \frac{P_{\mathrm{diss}}}{m} = \frac{\sigma |E|^2}{\rho},$$

Спочатку була побудована модель голови людини, виконана у формі шару з електрофізичними параметрами. Після цього було вирішено порівняти рівні питомого коефіцієнт поглинання електромагнітної енергії для різних варіантів:

- для існуючих мереж мобільного зв'язку (2G, 900 МГц),
- та для новітніх мереж 5G (субміліметровий діапазон – 6 ГГц).

У якості антени було обрано простий та ефективний випромінювач – напівхвильовий диполь з розмірами 0,15 м для частоти 900 МГц та 0,025 м для частоти 6 ГГц.

Проаналізувавши всі дослідження, які проводилися до цього часу і з власних міркувань можна сказати, що негативного впливу 5G на організм людини не виявили

Висновки

Боятися 5G не варто. Радіохвилі, видиме світло і ультрафіолетові хвилі – теж частина цього електромагнітного спектру. Дійсно небезпечні лише найвищі частини цього спектру, зокрема, рентгенівське випромінювання і гамма-випромінювання. Міліметрове ж є неіонізуючим, тобто не руйнує молекулярних зв'язків, а відтак не спричиняє негативного впливу на людський організм.

Єдине, чого варто побоюватися у випадку з неіонізуючим випромінюванням, це тепло, яке можуть генерувати радіохвилі.

Перелік посилань

1. Степанова Л.І. Енергетичні характеристики електромагнітного поля ан-тен засобів мобільного зв’язку. 2017 – 168 с.

2. T. S. Rappaport and C. M. Collins. Safe for Generations to Come: Considerations of Safety for Millimeter Waves in Wireless Communications. 2015 – 21с.

3. Sahar Aqeel Abdulrazzaq - SAR Simulation in Human Head Exposed to RF Signals and Safety Precautions. 2013 – 8с.

4. Полуденко Д. С. Реферат – ТЕХНОЛОГІЇ МОБІЛЬНОГО ЗВ'ЯЗКУ П'ЯТОГО ПОКОЛІННЯ (5G). 2015 – 19 с.

5. FEKO: Електромагнітний та тепловий аналіз моделі людського тіла з імплантатом при МРТ.

СЕКЦІЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

РОЗРОБКА АУДІО-ДОДАТКУ У ПРОГРАМНОМУ СЕРЕДОВИЩІ JUCE

Побережний М. В., Загребельний А. Ю. студенти 3-го курсу, група З-31, спеціальність 121 «Інженерія програмного забезпечення».

Науковий керівник – Пилявський В. В., к.т.н., доцент кафедри телебачення та радіомовлення ДУІТЗ

Анотація. *Розглянуто принцип розробки аудіо-плаґінів. Зображено процес розробки аудіо-плаґіну на базі мови програмування C++ за допомогою бібліотеки JUCE.*

Сьогодні аудіо-плаґіни використовують як альтернативу всім існуючим фізичним синтезаторам для написання музики, обробки її, а також для зведення вокалу з мелодією. Плаґін – додаток, незалежно скомпільований програмний модуль, що динамічно підключається до основної програми, призначений для розширення або використання її можливостей. Належить до загального програмного класу додатків. Плаґіни, зазвичай, виконуються у вигляді динамічних бібліотек. Virtual Studio Technology – стандарт плагінів звукових ефектів та програмних синтезаторів, запроваджений в 1996 р. фірмою Steinberg. У сучасній реальності практично у всьому, що стосується написання музики, використовують VST плагіни.

Питання успіху VST лежить глибоко в історії написання музики. До моменту появи технології люди використовували фізичні аудіо-ефекти та синтезатори, але через велику вартість мало хто мав змогу хоча б трохи поринути у світ музики. Саме тому в 1996 р., компанія Steinberg запровадила новітню, на той час, технологію, на якій базується робота більшості сучасних програмних синтезаторів.

Існує 3 типи VST плаґінів:

VST інструменти – VST-плаґіни, що генерують звук. Звичайно це віртуальні синтезатори або семплери. Одним із перших VST-інструментів був Neon VSTi, що був включений у Steinberg's Cubase. На сьогоднішній день існує багато VST-інструментів як вільних, так і комерційних. Деякі, як наприклад Native Instruments' Pro-53, відтворюють зовнішній вигляд та звук синтезаторів минулого (в даному разі Prophet-5).

VST ефекти – VST-плаґіни, що здійснюють обробку звукового сигналу, наприклад ефекти реверберації. Інші плаґіни використовуються для візуального спостереження властивостей звукового сигналу без його редагування. Більшість плаґінів дозволяють поєднувати декілька ефектів у певний ланцюг. На сьогоднішній день існує багато VST-ефектів як вільних, так і комерційних.

VST MIDI ефекти – VST-плаґіни, що обробляють MIDI-повідомлення перед тим, як MIDI-дані потрапляють на інші VST інструменти або апаратні пристрої; вони дозволяють. наприклад транспонувати музику або генерувати арпеджіо.

MIDI (цифровий інтерфейс музичних інструментів) – стандарт передачі інформації між електронними музичними інструментами, розроблений 1983 року, що дає можливість електронним музичним інструментам взаємодіяти між собою чи комп'ютером та іншим MIDI-сумісним обладнанням, здійснювати з одного інструменту управління іншими. MIDI не передає та не генерує звук — натомість MIDI передає «повідомлення», такі як нота-вкл./нота-викл., висота (pitch) та динаміка взятої ноти на інструменті; контрольні сигнали для таких параметрів як гучність, панорама, сигнали відліку часу для синхронізації темпу, тощо. Музичний інструмент приймає такі повідомлення і генерує звук. Інструментом може бути як реальний пристрій, наприклад, синтезатор, так і віртуальний – програма на комп'ютері. Як електронний протокол, MIDI відзначається надзвичайно широким поширенням.

DAW в термінології музичних продюсерів – електронна система, призначена для запису і редагування цифрового аудіо. Основна властивість робочих станцій – можливість вільно маніпулювати із записаним звуком, більшість робочих станцій також підтримують технологію MIDI.

JUCE – це всеохоплююча бібліотека класів C++ для розробки кросплатформеного програмного забезпечення. Він містить практично всі що вам може знадобитися для створення більшості додатків. Особливо добре підходить для побудови складних GUI, обробки графіки та аудіо.

Детальний опис частин коду:

```
void SynthVoice::startNote(int midiNoteNumber, float velocity, juce::SynthesiserSound* sound, int currentPitchWheelPosition)
{
   osc.setFrequency(juce::MidiMessage::getMidiNoteInHertz(midiNoteNumber));
   adsr.noteOn();
}
```

Викликається для старту нової ноти, за рахунок отримання даних з міді-клавіатури і встановлення їх в якості частоти осцилятора в герцах.

```
class SynthVoice :public juce::SynthesiserVoice
{
private:
 juce::dsp::Oscillator<float> osc{ [](float x) {return std::sin(x); } };
};
```

Визначає вид хвилі для осцилятора. За допомогою зміни значення, що повертається можна домогтися різних хвиль: синуса, пили, квадрата.

```
//return std::sin (x);
//return x/MathConstants<float>::pi;
//return x<0.0f? -1.0f ^1.0f
```

Види хвилі для осцилятора.

```
void GaloreAudioProcessor::prepareToPlay (double sampleRate, int samplesPerBlock)
{
   synth.setCurrentPlaybackSampleRate(sampleRate);
   for (int i = 0; i < synth.getNumVoices(); i++)
   {
      if (auto voice = dynamic_cast<SynthVoice*>(synth.getVoice(i)))
      {
         voice->prepareToPlay(sampleRate, samplesPerBlock, getTotalNumOutputChannels());
      }
   }
}
```

Повідомляє базового класу об'єктів AudioSource, для відтворення аудіопотоків, про приготування до відтворення звуку. AudioSource має два стани:

"Готовий" ("prepared") і "не готовий" ("unprepared").

Метод повинен бути викликаний, як мінімум, один раз для не готової AudioSource, щоб перевести його в стан "готовий", перш ніж будь-які виклики getNextAudioBlock () будуть проведені. Даний метод дозволяє синтезатору формувати будь-які з ресурсів, необхідних в процесі програвання.

setCurrentPlaybackSampleRate – повідомляє синтезатору, яка частота дискретизації звуку, який він буде використовувати для рендеринга звуку. Це значення повідомляється голосам (voices), щоб вони могли використовувати його для відтворення правильної висоти тону. Коли відтворення закінчено – метод releaseResources () викликається для приведення потоку назад в стан "не готовий".

Висновки

Роль сучасних інформаційних і комунікаційних технологій в удосконаленні та модернізації комп’ютерного простору залишається важливою протягом багатьох

років. У представленій роботі проведено аналіз основних понять і термінів створення VST-плаґіну та розглянуто приклад створення VST-плаґіну в інтерфейсі C++.

Перелік посилань

1. https://uk.wikipedia.org/wiki/Плагін
2. https://uk.wikipedia.org/wiki/Virtual_Studio_Technology
3. https://uk.wikipedia.org/wiki/Секвенсер_(музика)
4. https://uk.wikipedia.org/wiki/Цифрова_звукова_робоча_станція
5. https://uk.wikipedia.org/wiki/MIDI
6. https://uk.wikipedia.org/wiki/Steinberg
7. https://uk.wikipedia.org/wiki/Juce
8. https://habr.com/ru/post/209956/

СИСТЕМА КОНТРОЛЮ ОБЛІКОВИХ ЗАПИСІВ ПАЦІЄНТІВ КІНЕЗІОЦЕНТРУ

Галабурда В.Г., студент 2-го курсу, група З-21, спеціальність 121 «Інженерія програмного забезпечення»

Науковий керівник – Малюта С.А., викладач циклової комісії інтелектуальних технологій і зв’язку ВСП «Фаховий коледж зв’язку та інформатизації ДУІТЗ»

Анотація. *Даний сервіс розробляється для компанії, яка надає медичні послуги в Одесі, але, у подальшому даний проект буде розроблений як універсальна CRM система для компаній медичних послуг.*

Кінезіотерапія – напрямок фізичної терапії, який передбачає виконання активних і пасивних рухів, певних вправ лікувальної гімнастики та роботи на тренажерах для досягнення конкретного терапевтичного результату. Тобто, це лікування «рухом». Саме за таким принципом працює компанія даної системи керування.

CRM система – це система керування взаємовідносин клієнтів будь-якого бізнесу. Тобто, бізнес у даному випадку – це кінезіоцентр, а пацієнти – клієнти. Така система потрібна для підвищення ефективності обслуговування клієнтів та більш легшої праці з даними про пацієнтів.

У будь-яких медичних закладах, будь-то державні чи приватні, є система медичних карток пацієнта, прийом до лікаря, прописування курсу лікування, медикаментів тощо. На даний час це все є лише у паперовому вигляді, що незручно. Отже моя система полегшить взаємодію медичного закладу і клієнтів. У майбутньому

у проекті буде багато статистичних даних, на базі яких можна буде і автоматизувати деякі процеси, але не більшість, тому що справа йде про здоров'я людини.

Вище визначено, що таке кінезіотерапія, також зазначено що, проект буде розроблений як унікальна система. Так, у подальшому у систему буде добавлено система виписування направлень, аналізів тощо, що зробить даний систему універсальною. На даний час вже розроблено систему призначення медикаментів.

На даний час такого роду сервіси вже є, наприклад, pb4.com.ua (Поліклініка без черг), тому постає питання: «До чого ж розробляти дану систему?».

Я почав розробку цієї системи/сервісу для компанії на замовлення і хочу скористатися доступними для мене даними. З цих даних можна робити дуже точну статистику захворюваності, вилікування, досліджувати дійсність медичних препаратів при певному діагнозі. Це якщо говорити вже про універсальну систему контролю облікових записів. Але всі алгоритми складання статистики будуть перевіренні лікарями.

В розробленій системі є:

– Медичні картки. До медичних карток входять сукупність даних, які потрібні лікарю та пацієнту для подальшого їх використання в інших медичних закладах, звісно, якщо система, що розробляється буде актуальною. На даний час, це список тренувань (оскільки мова йде про кінезіоцентр), діагноз, список медикаментів з дозуванням та терміном вживання, призначених лікарем, у подальшому буде дороблена система виписування направлень на аналізи та медичні дослідження, результатів аналізів, короткої історії лікування. Ще не все на даний час є, тому що зараз система розробляється для кінезіоцентру.

– Запис до лікарів

Розроблена система подібна до існуючої pb4.com.ua, але є більш зручною. У кожного лікаря буде встановлено розклад прийому пацієнтів та приблизний час прийому одного пацієнта залежно від мети візиту.

Висновки

Була розроблена система регулювання взаємовідносин пацієнтів та лікарів, яка буде в подальшому доповнюватися універсальним функціоналом. У системі однією із головних ідей є збір статистичних даних та їх аналіз. Проект є ком комерційно вигідною розробкою. Головними перевагам розробки є:

Зручність для кінцевого споживача;

Проект має можливості для розвитку та підлаштування до різних потреб та умов використання.

Перелік посилань

1. https://uk.wikipedia.org/wiki/Кінезітерапія
2. https://pb4.com.ua
3. https://global.newmedicine.com.ua

ІНФОРМАЦІЙНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ АВТОМАТИЗОВАНОГО МОНІТОРИНГУ ВІДВІДУВАНОСТІ ЗАНЯТЬ

Яценко О. К., студент 2-го курсу, група З-21, спеціальність 121 «Інженерія програмного забезпечення»

Науковий керівник – Косирева Л. А., старший викладач кафедри інформаційних технологій УІТЗ

Анотація. *В роботі розроблена логіка і дизайн інтерфейсу для створення додатка, що представляє інформаційну панель з інформацією про хід навчального процесу групи. Ця програма спростить отримання даної інформації і забезпечить швидке взаємодія куратора зі студентами.*

Ця робота має вигляд інформаційної панелі – дашборда і розроблена за допомогою програмного інструменту Figma.

Візуалізація даних відіграє важливу роль в будь-якому бізнесі. Використовуються різні способи їх відображення – таблиці, графіки, звіти і багато інших.

Інформації навколо дуже багато. І найчастіше розібратися в цьому океані неймовірно важко. Щоб допомогти бізнесам розібратися в даних, зібрати їх на одному екрані і постійно оновлювати їх, існують дашборди – інтерфейси візуалізації, призначені для користувача.

Дашборд – це сучасний формат збору і візуального представлення даних, згрупованих за змістом на одному екрані для більш легкого візуального сприйняття інформації. Це аналітична панель із зрозумілим інтерфейсом для інтерактивної взаємодії з величезною кількістю показників, що постійно змінюються і які отримані в ході узагальнення даних. Їх звіти показують актуальну і об'єктивну інформацію з тих чи інших відомостей. З його допомогою в одну систему підтягують показники з систем аналітики, таблиць, CRM, соціальних мереж і баз даних.

Цим інструментом здебільше користуються аналітики, які за службовим обов'язком кожен день працюють з великими масивами даних. Дашборд стає зручним інтерфейсом між аналітичним двигуном і користувачем, і тому повинен бути інтуїтивно зрозумілим і таким, який можна налаштувати під себе.

Одним з доступних середовищ для розробки дашборда є безкоштовна хмарна платформа Google Data Studio. Вона корисна для маркетингу, так як можна використовувати такі джерела, як Google Analytics і Google AdWords. Заслуговує на повагу платформа Tableau - велика платформа з потужними і багатофункціональними інструментами, яка дозволяє проводити глибокий і різнобічний аналіз інформації з великими масивами даних, а потім представляти результат в інтерактивній формі.

Існують програми-інструменти для створення інтерфейсів і логіки при розробці дашборда. Одним з таких інструментів є крос-платформний онлайн-сервіс для дизайнерів інтерфейсів і веб-розробників.

Існує цілий ряд рекомендацій по розробці дашборда. Основними модулями дашборда є графіки, діаграми, таблиці, карти. Вибір неправильного типу діаграми або візуалізації даних за замовчуванням може заплутати користувачів або привести до невірного тлумачення даних. Коли все має узгоджену структуру, користувачеві легше працювати з інтерфейсом, він все легко знаходить. Оскільки головна мета дашборду – надати інформацію, кожна дрібниця має значення. Тому при створенні дашборду дуже важливо розробити чітку структуру дизайну і інтерфейсу і забезпечити узгодженість даних.

У моїй роботі розроблений дизайн та інтерфейс для багатосторінкового веб-документу, який складається з декількох розділів. Розроблено логіку функціональності цього веб-додатка. В якості інструмент розробки я вибрав онлайн-середовище Figma.

Мною розроблений дизайн і інтерфейс для створення дашборда, що представляє інформаційну панель з інформацією про хід навчального процесу групи. Додаток призначений для куратора групи з метою контролю відвідування та успішності студентів.

В роботі розроблені прототипи наступних сторінок: Головна сторінка, Список студентів групи, Профіль, Відвідуваність, Успішність.

Головна сторінка містить основну інформацію про всі сторінки системи. На сторінці Відвідуваність розміщено таблицю поточного дня зі списком студентів та предметами за розкладом. Дані на сторінці підтягуються з гугл-таблиць викладача по кожному предмету і можуть бути переглянуті куратором групи в будь-який час. На сторінці присутні іконки кнопок, за якими куратор має змогу зв’язатися з даним студентом або групою студентів та відправити їм деяке повідомлення. На сторінці присутня кнопка Показати календар, яка дозволяє користувачеві перегортати сторінки з потрібних його датам.

Дизайн сторінки “Успішність” подібний описаній вище сторінці і містить додатковий стовпчик з середньою оцінкою по предмету.

На сторінці “Список студентів” розташовуються картки з ім'ям і фотографією конкретного студента. При клацанні миші на картку користувач потрапляє на окрему сторінку, яка представляє собою профіль даного студента. На сторінці Профіль студента присутні всі особисті дані конкретного студента: прізвище, ім'я, адреса електронної пошти, дата народження студента, його контактний телефон та посилання на вайбер або телеграм. Дані можна переглядати. Якщо у користувача є відповідні права, дані можна і редагувати.

На кожній сторінці також присутній функціонал швидкого зв'язку із студентами.

При розробці всіх сторінок враховані рекомендації щодо створення дашборду, встановлені пріоритети в розстановці інформаційних блоків та створені взаємозв'язки між сторінками, що допомагають отримати додаткову інформацію.

Висновки

У процесі роботи створено макет інформаційної панелі, що спростить отримання інформації про хід навчального процесу групи і забезпечить швидку взаємодію куратора зі студентами. В макеті реалізована побудова логіки і дизайну візуалізації інформації у вигляді декількох блоків або карток для панелі дашборд. Розробка макету проведена в середовищі онлайн-додатка Figma.

Перелік посилань

1. Що таке дашборд. Електронний ресурс: https://www.octoboard.com/что-такое-дашборд
2. https://habr.com/ru/company/devexpress/blog/341972/
3. Дашборд як інтерактивна альтернатива табличних звітів. Електронний ресурс: https://sendpulse.com/ru/blog/dashboard
4. Dashboard. Електронний ресурс: https://terralink-xde.readthedocs.io /ru/latest/developer /Architecture/Dashboard/Architecture-Dashboard.html

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ГРАФІЧНИХ КАЛЬКУЛЯТОРІВ У СУЧАСНІЙ ОСВІТІ

Салабай М.О., студент 2-го курсу, групи З-21, спеціальність 121 «Інженерія програмного забезпечення».

Науковий керівник – Басов В.Є., к.т.н., доцент кафедри інформаційної безпеки та передачі даних ДУІТЗ

Анотація. *У роботі представлені можливості графічного калькулятора та перспективи його використання на прикладі розроблених програм*

Зараз більшість калькуляторів виконують лінійні прості обчислення, а якщо є будь-які специфічні завдання які є непростими лінійними обчисленнями, а складними структурами тоді розв'язання таких задач займає дуже багато часу і зовсім не ефективно.

Приблизно так зараз працюють більшість навчальних закладів України або ти тримаєш все в голові, і навіть, якщо отримав результат, ти перевірити його не можеш або йти шляхом знаходження в інтернеті.

Який з цього вихід? Вихід є і полягає він у використанні графічних калькуляторів.

Зараз використання графічних калькуляторів не те що можливо, а й заохочується. А ось у нас більшість вчителів не використовують їх в процесі проведення своїх занять. Чому так? Річ у тім що зараз у нас графічні калькулятори не використовують повсюдно, а замість них використовують смартфони що накладає свої проблеми, а саме можливості для учнів доступу в інтернет, спілкування між собою в соціальних мережах що дає можливості списати.

Що це взагалі таке і що він може дати?

Графічний калькулятор це «старший брат» інженерного калькулятора. Всі функції інженерного у нього є на додаток обчислювальна потужність порівнянна з сучасним смартфоном, при цьому зручність використання вище, можливість вирішення складних рівнянь, а саме цікаве так це можливість запуску і роботи з власне розробленими програмним забезпеченням для вирішення специфічних завдань.

Слід вказати, що в сучасних умовах калькулятор, особливо з вбудованою СКМ здатний допомогти не лише студенту, а і науковцю. Цей пристрій має вже від виробника велику кількість готових програм та можливість розробки науковцем – дослідником власних програм, що дає можливість в процесі досліджень одержати науковий результат швидше, ніж на комп’ютері.

Висновки

У результаті виконання роботи було представлені можливості графічного калькулятора та перспективи його використання на прикладі розроблених програм для розрахунку опору випромінювання антени симетричного вібратора на основі:

$$R_\Sigma = \frac{2P_\Sigma}{I_\Pi^2} = \frac{1}{\sqrt{\frac{\mu}{\varepsilon}}\, I_\Pi^2} \int_0^{2\pi} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} E_{\theta_m}^2 r_0^2 \, d\phi \, d\theta$$

Була одержано:

$$\begin{aligned} R_\Sigma = 30(&2(C + \ln 2kl - \mathrm{ci}\, 2kl) \\ &+ \cos 2kl(C + \ln kl + \mathrm{ci}\, 4kl - 2\,\mathrm{ci}\, 2kl) \\ &+ \sin 2kl(\mathrm{si}\, 4kl - 2\mathrm{si}\, 2kl)) \end{aligned}$$

де C ≈ 0,577… постійна Ейлера;

$\mathrm{si}\, x = \int_0^x \frac{\sin U}{U} dU$ - інтегральний синус;

$\mathrm{ci}\, x = -\int_0^x \frac{\cos U}{U} dU$ - інтегральний косинус.

та складена програма для розрахунку в залежності від довжини антени.

Також виконано численне інтегрування по області на двовимірній поверхні:

$$\begin{aligned} F(x_1, x_2, m_1, m_2, \sigma) \\ &= \frac{1}{2\pi\sigma^2} \iint_S e^{-\frac{x_1 - m_1}{2\sigma^2}} e^{-\frac{x_2 - m_2}{2\sigma^2}} dx_1 dx_2 \\ &= \frac{1}{2\pi\sigma^2} \int_{x_1} \left(\int_{x_2} e^{-\frac{x_1 - m_1}{2\sigma^2}} e^{-\frac{x_2 - m_2}{2\sigma^2}} dx_2 \right) dx_1 \end{aligned}$$

розрахунки, якого були проведенні виключно на графічному калькуляторі.

Перелік посилань

1. http://tdo.at.ua/voronkin/stattja_kalkuljatory.pdf. Стаття «Потенціал використання графічних калькуляторів у навчанні математики в закладах загальної середньої освіти україни» О. Воронкін.

2. https://calculators-online.ru/novosti/programmiruemye-kalkulyatory-osnova-shkolnogo-obrazovaniya.html. Стаття «Програмований калькулятор - ОСНОВА ШКІЛЬНОГО ОСВІТИ»

3. https://cyberleninka.ru/article/n/informatsionnye-tehnologii-obucheniya-matematike-v-shkolah-ssha/viewer. Стаття «Інформаційні технології навчання математики в США»

4. https://cyberleninka.ru/article/n/organizatsiya-uchebnoy-deyatelnosti-studentov-po-matematike-s-ispolzovaniem-malyh-sredstv-informatizatsii/viewer. Стаття «Організація навчальної діяльності студентів з математики з використанням малих засобів інформатизації»

РОЗРОБКА САЙТУ ДЛЯ СТВОРЕННЯ ЧАТ-БОТІВ

Шевченко Л. В., студент 3-го курсу, група З-31, спеціальність 121 «Інженерія програмного забезпечення».

Науковий керівник – Орлова Л. Б., викладач циклової комісії інтелектуальних технологій та зв’язку ВСП «Фаховий коледж зв’язку та інформатизації ДУІТЗ

Анотація. *Розроблено сайт для спрощення розробки ботів у месенджерах. Зображено архітектуру сайту, технології на яких вона працює.*

За останні кілька років месенджери стали одним з основних способів спілкування в інтернеті. У зв'язку з цим все більше компаній потребують власних ботів. Так як чат з ботом нічим не відрізняються від звичайного чату з людиною, людям простіше взаємодіяти з компанією.

В началі розвитку інтернету, багато людей хотіли зробити собі сайт але не вміли цього робити, тому почали з'являтися конструктори сайтів такі, як WordPress, які дозволяли зробити сайт будь-якій людині без навичок програмування, через те що чат-боти починають собою привичні сайти, я вирішив зробити такий сайт, який дозволяв би кожному хто потребує чат-бота для свого бізнесу, зробити його самостійно, без навичок програмування, так сама як це дозволяють робити конструктори сайтів.

Для розробки було використано мову програмування Python, веб-фреймворки: Flask та Django, бібліотеки: ZeroMQ, python-telegram-bot, React JS та SemanticUI-React.

Програми зроблені за допомогою цих бібліотек, можуть працювати на будь-яких платформах: Linux, Windows та Mac OS.

Використовуючи фреймворк Django, треба дотримуватися загального алгоритму створення веб-сайтів:

Створення нового додатку;

Реєстрація додатку у файлі конфігурації;

Створення необхідних моделей в базі даних;

Створення функцій, що мають відповідати на вхідні запити;

Зробити міграцію бази даних.

Детальне пояснення наведеного алгоритму створення нейронної мережі:

Створення нового додатку:

Створюємо додаток з назвою “bots” за допомогою команди “python manage.py startapp bots”;

Реєстрація додатку у файлі конфігурації:

Для цього змінюємо поле INSTALLED_APPS у файлі settings.py, додаючи туди назву нового додатку “bots”.

Створення необхідних моделей в базі даних:

Нам потрібно створити такі моделі: Bot, Command, InlineKeyboardButton, CallbackHandler та Message;

Для цього додаємо їх до файлу models.py згідно з офіційною документацією.

Створення функцій що мають відповідати на вхідні запити:

Далі додамо функції у файл такі як, “start_bot”, “stop_bot”, “bot_list” та ін. до файлу views.py.

Зробити міграцію бази даних:

Щоб новий додаток запрацював, треба виконати дві команди:

“python manage.py makemigrations” та “python manage.py runserver”.

Висновки

Роль месенджерів у житті сучасних людей значно поширюється, зараз це один з головних засобів зв'язку. У представленій роботі розроблено сайт що робить розробку чат-ботів значно легшою, роблячи вхідний поріг набагато нижче.

Перелік посилань

1. https://docs.djangoproject.com/en/3.1/ Офіційна документація фреймворку Django.
2. https://core.telegram.org/bots/api Офіційна документація до Telegram API.
3. https://developers.viber.com/docs/api/python-bot-api/ Офіційна документація Viber.
4. https://developers.facebook.com/docs/messenger-platform/
5. Офіційна документація Facebook Messanger.
6. https://zeromq.org/languages/python/ Офіційна документація ZeroMQ.

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ГРИ НА ОСНОВІ ПЛАТФОРМИ UNITY 2D

Петін М. В., Букач В. М., студенти 2-го курсу, група Кн-21, спеціальність 121 «Інженерія програмного забезпечення»

Науковий керівник – Корчинсьткий В. В., д.т.н, доцент кафедри інформаційної безпеки та передачі даних ДУІТЗ

Анотація. *Проводиться робота, мета якої – показати процеси та етапи розробки платформера на ігровому рушії Unity.*

Ігровий рушій - програмний рушій, центральна програмна частина будь-якої відеогри, яка відповідає за всю її технічну сторону, дозволяє полегшити розробку гри шляхом уніфікації та систематизації її внутрішньої структури. Важливим значенням рушія є можливість створення багатоплатформових ігор.

Редактор Unity має простий Drag & Drop інтерфейс, який легко налаштовувати, що складається з різних вікон, завдяки чому можна проводити налагодження гри прямо в редакторі. Рушій підтримує дві сценарні мови: C #, JavaScript (модифікація). Проект в Unity ділиться на сцени (рівні) – окремі файли, що містять свої ігрові простори зі своїм набором об'єктів, сценаріїв, і налаштувань. Сцени можуть містити в собі як об'єкти (моделі), так і порожні ігрові об'єкти. Об'єкти, в свою чергу містять набори компонентів, з якими взаємодіють скрипти. Вони мають назву (в Unity допускається наявність двох і більше об'єктів з однаковими назвами), можуть мати тег (мітку) і зображення, на якому об'єкт повинен відображатися. Так, у будь-якого предмета на сцені обов'язково присутній компонент Transform — він зберігає в собі координати місця розташування, повороту і розмірів по всім трьом осям. У об'єктів з видимою геометрією також за умовчанням присутній компонент Mesh Renderer, що робить модель видимою.

Unity підтримує фізику твердих тіл і тканини, фізику типу Ragdoll. У редакторі є система успадкування об'єктів; дочірні об'єкти будуть повторювати всі зміни позиції, повороту і масштабу батьківського об'єкта. Скрипти в редакторі прикріплюються до об'єктів у вигляді окремих компонентів. При імпортуванні текстури в рушій можна згенерувати alpha-канал, mip-рівні, normal-map, light-map, карту відображень, проте безпосередньо на модель текстуру прикріпити не можна – буде створено матеріал, з яким буде призначений шейдер, і потім матеріал прикріпиться до моделі. Редактор Unity підтримує написання і редагування шейдерів. Крім того він містить компонент для створення анімації, яку також можна створити

попередньо в 3D-редакторі та імпортувати разом з моделлю, а потім розбити на файли.

Як правило, ігровий рушій надає безліч функціональних можливостей, що дозволяють їх задіяти в різних іграх, в які входять моделювання фізичних середовищ, карти, динамічні тіні і багато іншого. На відміну від багатьох інших рушіїв, у Unity є дві основні переваги: наявність візуальної середовища розробки та міжплатформова підтримка. Перший фактор включає не тільки інструментарій візуального моделювання, а й інтегроване середовище, ланцюжок складання, що направлено на підвищення продуктивності розробників, зокрема, етапів створення прототипів і тестування. Під міжплатформовою підтримкою мається на увазі не тільки місця розгортання (установка на персональному комп'ютері, на мобільному пристрої, консолі і тощо), але і наявність інструментарію розробки (інтегроване середовище може використовуватися під Windows і Mac OS). Третьою перевагою є модульна система компонентів Unity, за допомогою якої відбувається конструювання ігрових об'єктів, коли останні є комбіновані скриньки функціональних елементів. На відміну від механізмів успадкування, об'єкти в Unity створюються за допомогою об'єднання функціональних блоків, а не приміщення в вузли дерева успадкування. Такий підхід полегшує створення прототипів, що актуально при розробці ігор.

Недоліками виступають обмеження візуального редактора при роботі з багатокомпонентними схемами, коли в складних сценах візуальна робота ускладнюється. Другим недоліком називається відсутність підтримки Unity на посилання із зовнішньої бібліотеки, роботу з якими програмістам доводиться налаштовувати самостійно, і це також ускладнює командну роботу. Ще один недолік пов'язаний з використанням шаблонів. З одного боку, ця концепція Unity пропонує гнучкий підхід візуального редагування об'єктів, але з іншого боку, редагування таких шаблонів є складним. Також, WebGL-версія рушія, в силу специфіки своєї архітектури (трансляція коду з C # в C ++ і далі в JavaScript), має ряд невирішених проблем з продуктивністю, споживанням пам'яті і працездатністю на мобільних пристроях.

Висновки

За результатами роботи можна зробити наступні висновки:

1. Unity є одним за найкращих ігрових рушіїв для створення однією людиною, або невеликою командою, інді-ігор.
2. Unity дозволяє створювати ігри для більш ніж для 25 платформ, що робить її дуже функціональною та пластичною.
3. Ігровий рушій має сучасний рівень графіки, що дозволяє створювати ігри високого рівня без складних навичок програмування.

Перелік посилань

1. https://itproger.com/news/69. «Обзор и изучение игрового движка Unity»
2. https://itkeys.org/about-unity/ «О Unity: обзор движка»
3. https://uk.wikipedia.org/wiki/Ігровий_рушій. «Ігровий рушій»
4. https:// uk.wikipedia.org/wiki/Unity_(рушій_гри) «Unity(ігровий рушій)»
5. https://vc.ru/pixonic/47088-2d-courses-tutorials(Основи створення ігор)

КВАНТОВИЙ РОЗПОДІЛ КЛЮЧІВ – НОВА ТЕХНОЛОГІЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Тишкул М. В., студент 2-го курсу, група Кн-21, спеціальність 122 «Комп'ютерні науки».

Науковий керівник – Васіліу Є. В., д.т.н., професор, директор ННІ радіо, телебачення та інформаційної безпеки ДУІТЗ

Анотація. *На основі наявних в літературі результатів досліджень стійкості квантових протоколів розподілу ключів до різних атак підслуховування агента проведено аналіз надійності двох протоколів. З'ясовано, що протокол з шістьма станами є незначно більш стійким, ніж протокол BB84. Однак протокол з шістьма станами має значно меншу ефективність ніж BB84. Таким чином, для практичного використання протокол BB84 є більш переважним.*

Квантова криптографія - рішення задач криптографічного захисту інформації з використанням квантових властивостей окремих фотонів (носіїв інформації в квантової криптографії).

Принципи квантової криптографії були закладені Стівеном Візнером з Колумбійського університету в Нью-Йорку, який на початку 1970-х років запропонував ідею квантового спряженого кодування. У його роботі було показано, як зберігати та передавати два повідомлення шляхом їх представлення у вигляді двох «спряжених спостережуваних», наприклад, лінійної та циклічної поляризацій світла, таким чином, що одна з них (але не обидві), може бути прийнята і розшифрована. Візнер проілюстрував свою ідею концепцією гіпотетичних квантових грошей, які неможливо підробити.

Сучасна квантова криптографія заснована на передачі бітів окремими фотонами, многофотонні імпульси повинні бути виключені для забезпечення секретності передачі. В результаті досягти високої швидкості передачі в квантовому каналі поки не можливо – в даний час максимальна швидкість становить декілька сотень кбіт/с. Отже, практично квантову криптографію поки можна застосовувати в основному для розподілу ключів, які потім будуть використовуватися для

шифрування високошвидкісних потоків даних, переданих по звичайним, в тому числі і відкритим каналам зв'язку. Цим обумовлений пріоритет одного з напрямків квантової криптографії - квантових протоколів розподілу ключів (КПРС). Більшість теоретичних і експериментальних досліджень нині присвячено розробці і вдосконаленню КПРС, а також аналізу ступеня їх захищеності від можливих атак.

Найвідоміший та найкраще розроблений метод квантової криптографії — це квантовий розподіл ключа, який описує процес застосування квантової комунікації для створення та обміну секретним ключем між двома користувачами (яких традиційно називають Алісою і Бобом) без можливості втручання третьої сторони (Єви), що прагне перехопити інформацію про ключ.

Можливі області застосування КРК:

– Області, де потрібен високий рівень безпеки, наприклад, там, де до теперішнього часу ключі розподілялися за допомогою довірених кур'єрів.

– Альтернатива схемам розподілу сеансових ключів в симетричних криптосистемах, які засновані на методах криптографії з відкритим ключем (наприклад, альтернатива схемі Діффі - Хеллмана).

Протокол BB84

Протокол використовує 4 квантових стани, що утворюють 2 базиси, наприклад поляризаційні стани світла. Стани всередині одного базису ортогональні, але стани з різних базисів - попарно неортогональної. Ця особливість протоколу дозволяє виявити можливі спроби нелегітимного знімання інформації.

Носіями інформації в протоколі є фотони, поляризовані під кутами 0°, 45°, 90°, 135°. За допомогою вимірювання можна розрізнити лише 2 ортогональних стану:

– фотон поляризований вертикально або горизонтально;

– фотон поляризований під кутами 45° або 135°.

Достовірно відрізнити за одне вимірювання, наприклад, горизонтальний фотон від фотона, поляризованого під кутом 135°, неможливо.

Для кодування інформації в протоколі використовуються чотири стани поляризації, що утворюють два неортогональних один одному базису: прямокутний та діагональний.

Протокол Six-State

Протокол з шістьма станами, інакше відомий як three base cryptographic method, є розширенням протоколу BB84 на використання трьох базисів замість двох. Це означає, що Єві доведеться вибрати правильний базис серед 3 можливих. Цей протокол має підвищену імовірність виявлення перехоплення за рахунок зменшення довжини просіяного ключа (приблизно дві третини виявлених бітів будуть в неправильному базисі), таким чином, можна запропонувати підвищену безпеку.

На закінчення зазначимо таке. Як показує аналіз літературних джерел, стійкість протоколу BB84 до всіх видів атак незначно менше стійкості протоколу з шістьма станами. Однак швидкість передачі ключа по протоколу BB84 істотно вище, так як його середня ефективність дорівнює 1/2, а протоколу з шістьма станами – 1/3. Таким чином, для передачі довгих ключів слід віддати перевагу протоколу з шістьма станами. Якщо ж агент, що підслуховує, має можливість застосувати атаку поділу числа фотонів на протокол BB84, то, використовуючи джерело із середнім числом фотонів в імпульсі не більше 0,1, а також квантовий канал з малими втратами ($\boldsymbol{\eta}$ = 0,9 – 1) законні користувачі зможуть встановити секретний ключ, коли рівень помилок при передачі не перевищує ~ 14%. Однак платою за секретність в цьому випадку буде низька швидкість передачі ключа.

Висновки

При роботі з даною темою ми проаналізували сучасний стан квантової криптографії та квантового розподілу ключів, а також розглянули два протоколи та порівняли їх стійкість та ефективність та з'ясували, що при передачі інформації краще застосовувати протокол BB84.

Перелік посилань

1. https://ela.kpi.ua/bitstream/123456789/26803/1/Khorunzhyy_magistr.pdf. «Аналіз видів та способів генерації квантових та мних ключів.
2. https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F
3. https://ru.qaz.wiki/wiki/BB84. Квантовая криптография.
4. https://ocw.tudelft.nl/course-lectures/6-3-1-bb84-states-six-state-protocol. 6.3.1 BB84 states and the six state protocol

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІД АТАК ТИПУ «РОЗПОДІЛЕНА ВІДМОВА В ОБСЛУГОВУВАННІ» (DDOS)

Дроздовський М. Д., студент 2-го курсу, група Кн-21, спеціальність 122 «Комп'ютерні науки»

Науковий керівник – Кільдішев В.Й., к.т.н., доцент кафедри інформаційної безпеки ДУІТЗ

Анотація. *В даному дослідженні ми з'ясуємо що таке ddos атаки, які бувають їх види, принцип дії і методи захисту від них*

DDoS-атака (Distributed Denial of Service) - розподілений напад на IT-систему організації з метою довести її до відмови. На систему направляється величезна кількість запитів, через які її продуктивність знижується аж до повного «зависання». Уразливі елементи - інтернет-канали, сервери, міжмережеві екрани. Зазвичай для атаки використовуються скомпрометовані системи.

Завдання атакуючих - вивести сайт з ладу або «під шумок» вкрасти дані. Часто DDoS-атаки чергуються зі спробами злому сайтів.

Переважна більшість атак розвиваються в такій послідовності:

1) збір даних про жертви і їх аналіз з метою виявлення явних і потенційних вразливостей, вибір методу атаки;

2) підготовка до атаки шляхом розгортання шкідливого коду на комп'ютерах і підключених до Інтернету пристроях, управління якими вдалося перехопити;

3) генерація потоку шкідливих запитів з безлічі пристроїв, що знаходяться під управлінням зловмисника;

4) аналіз результативності атаки: якщо цілей атаки домогтися не вдалося, зловмисник може провести більш ретельний аналіз даних і здійснити новий пошук методів атаки (перехід до п.1).

Найбільш часто вживаний спосіб класифікації атак - за рівнем OSI, на якому вони були здійснені. Перерахую найбільш поширені види атак:

Мережевий рівень (L3): DDoS-атаки цього рівня «працюють» по протоколах IP, DVMRP, ICMP, IGMP, PIM-SM і ін.Цілями атак є в першу чергу мережеві пристрої - комутатори (свічі) і маршрутизатори (роутери).

Транспортний рівень (L4): вплив здійснюється за протоколами TCP і UDP, а також по підпротоколам DCCP, RUDP, SCTP, UDP Lite. Цілями атак цього рівня зазвичай стають сервери і деякі інтернет-сервіси, наприклад ігрові.

Рівень додатків (L7): атака здійснюється на рівні протоколів додатків. Найчастіше зловмисники використовують HTTP, HTTPS і DNS. Атаки цього рівня націлені як на популярні мережеві сервіси, так і на різні веб-сайти і веб-додатки.

Брандмауери та системи запобігання вторгнень на сервери самі по собі уразливі і розраховувати тільки на їх надійність не варто.

Висновки

Для TCP-трафіку рекомендується використовувати хмарні сервіси для фільтрації підозрілих запитів. Також рекомендується:

– проводити моніторинг DNS: підозрілу мережеву активність можна відстежити. Для цього рекомендується використовувати комерційні DNS-рішення,

або Open-source продукти (наприклад, BIND). Ви зможете в режимі реального часу відслідковувати мережевий трафік і запити до DNS. Для економії часу також рекомендується будувати базовий профіль мережевої інфраструктури і оновлювати його в міру масштабування бізнесу;

– розширювати апаратні ресурси DNS: компромісне рішення, що дозволяє захистити інфраструктуру від дрібномасштабних атак. Закупівля додаткових потужностей також пов'язана і з вкладенням;

– будувати конфігурації високої доступності: DNS служба розгортається на HA-сервері, що дозволяє відновити роботу сервісу на резервної машині, в разі якщо основна виявиться недоступною

Перелік посилань

1. https://stormwall.pro/knowledge-base/termin/ddos-protection. DDoS-protection.

2. https://www.iksmedia.ru/articles/5491543-DDoS-celi-metody-sredstva-zashhity.html. DDoS: цели, методы, средства защиты.

ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС. ОСОБЛИВОСТІ ВИКОРИСТАННЯ В УКРАЇНІ

Яроцька Д. С., студентка 1-го курсу, група Кб-11, спеціальність 122 «Комп’ютерні науки».

Науковий керівник – Тінгаєв О. А., к.фіз-мат.н., доцент, викладач циклової комісії інтелектуальних технологій та зв’язку ВСП «Фаховий коледж зв’язку та інформатизації ДУІТЗ

Анотація. *Розглянуто принципи створення і застосування ЕЦП. Описаний криптографічний алгоритм RSA. Наведені юридичні основи використання ЕЦП в Україні та алгоритм його отримання.*

Електронний цифровий підпис (ЕЦП) — реквізит електронного документа, призначений для захисту даного документа від підробки, отриманий в результаті криптографічного перетворення інформації з використанням закритого ключа ЕЦП і що дозволяє ідентифікувати власника сертифіката ключа підпису, а також встановити відсутність спотворення інформації в електронному документі.

Електронний цифровий підпис знадобиться тим, хто збирається використовувати в роботі електронні документи, здавати звітність та отримувати послуги в інтернеті.

Паперовий документ може бути підписаний простим розчерком пера. Для того щоб забезпечити можливість підписання електронних документів, були розроблені спеціальні технології, названі за аналогією ЕЦП. Специфічність електронного підпису, її відмінність від власноручного зумовили необхідність розробки і прийняття спеціального законодавства, що регулює порядок використання новітніх програмних засобів ідентифікації електронних документів в цивільному обороті.

Спеціальним законом, що встановив «правовий статус ЕЦП та врегулював відносини, що виникають при використанні ЕЦП», став Закон України «Про електронний цифровий підпис» від 22 травня 2003 року.

В основі електронного підпису лежить криптографія відкритого ключа. З її допомогою формується спеціальний сертифікат користувача. Він містить дані про користувача, відкритий ключ і електронний підпис сертифіката, її можна перевірити за допомогою відкритого ключа кваліфікованого провайдера. Алгоритм гарантує, що зробити генерацію підпису може тільки кваліфікований провайдер, який має секретний ключ шифрування, і довіра до якого є основою для роботи всієї системи ЕЦП.

При створенні цифрового підпису за класичною схемою відправник:

– застосовує до вихідного повідомлення T хеш-функцію h(T) (хеш-функція – легко обчислювана функція, яка перетворює вихідне повідомлення довільній довжини в повідомлення, фіксоване довжини (хеш-образ), для якої не існує ефективного алгоритму пошуку колізій) і отримує хеш-образ r повідомлення;

– обчислює цифровий підпис s по хеш-образу r з використанням свого закритого ключа;

– посилає повідомлення T разом з цифровим підписом s одержувачу.

Одержувач, відокремивши цифровий підпис від повідомлення, виконує наступні дії:

– застосовує до отриманого повідомленням T хеш-функцію h(T) і отримує хеш-образ r;

– розшифровує хеш-образ r' з цифрового підпису s з використанням відкритого ключа відправника;

– перевіряє відповідність хеш-образів r і r' і якщо вони збігаються, то відправник дійсно є тим, за кого себе видає, і повідомлення при передачі не піддалося спотворенню.

Алгоритм RSA

1. Вироблення ключів (виконує відправник A).

2. Відправлення повідомлення та ЕЦП (виконує відправник A).

Таблиця 1. Відправлення повідомлення та ЕЦП на базі алгоритму RSA

№	Опис операції	Приклад
1	Обчислення хеш-образу h = h(T), де T – вихідне повідомлення, h(T) – хеш-функція (для MD5 довжина хеш-образу 128 біт).	h = 7
2	Вироблення цифрового підпису s = hd mod n, де d – закритий ключ відправника A, n – частина відкритого ключа відправника A.	s = 729 mod 91 = 63
3	Відправка одержувачу B вихідного повідомлення T і цифрового підпису s.	

3. Отримання повідомлення і перевірка електронного підпису (виконує одержувач B).

Висновки

1. Треба як можна швидше опанування ЕЦП всім дієспроможним населенням країни, а не тільки адміністраціями та фахівцями державних установ та керівництвом комерційних підприємств, як воно є зараз;

2. Бурний розвиток квантових комп’ютерних технологій призведе найближчим часом до того, що криптографічна основа ЕЦП у вигляді алгоритму RSA та подібних йому не буде давати надійний захист документу. Одним з варіантів розвитку ЕЦП є застосування алгоритмів, які базуються на точках еліптичних кривих

Перелік посилань

1. https://uk.wikipedia.org/wiki/Електронний цифровий підпис.
2. http://www.ucrf.gov.ua/uk/doc/laws/1149760377/ – Закон України "Про ЕЦП".
3. https://web.archive.org/web/20100301080922. Subscription Service.
4. http://bezpeka.com/ru/lib/spec/cript.html.
5. https://thedigital.gov.ua/news/yak-oformiti-elektronniy-pidpis. Як оформити електронний підпис?

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

Здано в набір 29.03.2021 р. Підписано до друку 02.04.2021 р.
Тираж 20 прим. обсяг 0,2 друк. арк.
Віддруковано в ВСП «Фаховий коледж зв'язку та інформатизації ДУІТЗ»
© ВСП «ФКЗІ ДУІТЗ», 2021