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

П'ята студентська науково-технічна конференція

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

04 квітня 2015 року

Збірка тез

Одеса, 2015

Телекомунікаційні, інформаційні та комп'ютерні мережі та системи: теперішнє та майбутнє: матеріали п'ятої студентської науково-технічної конференції, м. Одеса, 04 квітня 2015 року – Одеса, КЗІ ОНАЗ, 2015. – 34 с.

Дана збірка містить тези матеріалів, що представлені на п'ятої студентську науково-технічну конференцію «**Телекомунікаційні, інформаційні та комп'ютерні мережі та системи: теперішнє та майбутнє»**, що проводиться 04 квітня 2015 р. в коледжі зв'язку та інформатизації Одеської національної академії зв'язку ім. О.С. Попова.

До збірки включені тези доповідей за секціями:
– телекомунікаційних систем та мереж;
– радіозв'язку, радіомовлення та телебачення;
– інформатики та обчислювальної техніки.

Робоча мова конференції – українська, російська.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

ГОЛОВА ОРГКОМІТЕТУ:

Петрусенко С. Ю. – 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. – голова циклової комісії інформатики та обчислювальної техніки

ЧЛЕНИ ОРГКОМІТЕТУ:

Козаченко Л. О. – голова циклової комісії систем радіозв'язку, радіомовлення та телебачення

Кокорєва З. Р. – голова циклової комісії телекомунікаційних систем та мереж

Герасимова Т. М. – завідувач навчально-методичної лабораторії

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

Махновський Д. П. – викладач циклової комісії систем радіозв'язку, радіомовлення та телебачення

Фіньковська М. С. – викладач циклової комісії телекомунікаційних систем та мереж

Воробйова О. О. – голова ради студентського самоврядування, студентка групи О-412/42

ЖУРІ КОНФЕРЕНЦІЇ

ГОЛОВА ЖУРІ:

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

ЧЛЕНИ ЖУРІ:

секція телекомунікаційних систем та мереж

Степанов Д. М. – к.т.н., доцент кафедри волоконно-оптичних ліній зв'язку ОНАЗ ім. О. С. Попова

Корчинський В. В. – д.т.н., доцент кафедри передачі даних та інформаційної безпеки ОНАЗ ім. О. С. Попова

секція систем радіозв'язку, радіомовлення та телебачення

Рожновський М. В. – к.т.н., доцент кафедри технічної електродинаміки та систем радіозв'язку ОНАЗ ім. О. С. Попова

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

секція інформатики та обчислювальної техніки

Васіліу Є. В. – д.т.н, доцент, директор навчально-наукового інституту радіо, телебачення та інформаційної безпеки ОНАЗ ім. О. С. Попова

Ніколаєнко С. В. – к.т.н., старший викладач кафедри інформаційних технологій ОНАЗ ім. О. С. Попова

ЗМІСТ

Секція телекомунікаційних систем та мереж

1. Вербецька А. М. Перспективи розвитку мережі PON в місті Одеса

2. Заболотна А. В. Несанкціонований доступ до інформації в волоконно-оптичних лініях зв'язку при втратах у волокні
3. Краєв О. В. Розробка клієнт-серверних додатків в соціальних мережах

Секція радіозв'язку, радіомовлення та телебачення

1. Лапчевський Є. В., Бондаренко В. С. Використання планшетів та смартфонів для прийому мобільного ТВ
2. Кислов Д. Ф. Дослідження можливостей глушіння мобільного зв'язку стандарту GSM-900
3. Тарабара М. В., Колісниченко Р. Д. Цифровий частотомір на мікроконтролері

Секція інформатики та обчислювальної техніки

1. Воробйова О. О., Міненко В. А. Менеджери паролів та їх вразливість

2. Угрік В. А. Порівняння хмарних сховищ даних

3. Архіпова А. О., Кічуга М. Б. Створення автоматичної системи на основі апаратної платформи Arduino

ПЕРСПЕКТИВИ РОЗВИТКУ ПАСИВНИХ ОПТИЧНИХ МЕРЕЖ PON В м. ОДЕСА

Вербецька А. М., студентка 3-го курсу, група С-31, спеціальність «Монтаж, обслуговування та ремонт станційного обладнання».

Науковий керівник: викладач **Кокорєв В. В.**

Анотація. *Розглядається мережа PON, її архітектура, різновиди та обладнання. Розглядається перспектива впровадження та розвитку мережі PON на базі уже існуючої оптичної мережі в м. Одеса. Приведено розрахунки бюджету оптичної потужності для сегменту проектованої мережі, її структурну схему та схему на місцевості. Підібрано обладнання, виходячи з розрахунків та визначено клас сегменту мережі. Розглянуто економічну сторону даного проекту.*

Поява нових послуг зв’язку, розвиток мереж зв’язку, в першу чергу Internet, призвели до збільшення потоків даних, які передаються і як наслідок до необхідності збільшення пропускної здатності мережі на всіх її дільницях і особливо на мережах абонентського доступу. На основі кабелів з мідними витими парами не вдається організувати передачу високошвидкісних потоків на відстань більше 100м. В останні роки завдяки зменшенню вартості оптичного кабелю (ОК), інших пасивних елементів, а також оптоелектронних пристроїв стало можливим застосування волоконно-оптичних технологій на мережах абонентського доступу.

Сьогодні прокладати ОК для організації мережі абонентського доступу стає вигідно як при відновленні старих, так і при будівництві нових мереж. Значно збільшити їх пропускну здатність дозволяє впровадження пасивних оптичних мереж (passive optical network-PON). Основою пасивної оптичної мережі є розгалужена архітектура з пасивними оптичними розгалужувачами на вузлах, яка забезпечує широкополосну передачу з можливістю нарощування вузлів мережі та її пропускної здатності, ці мережі не містять проміжних регенераторів або підсилювачів. Технології PON повністю відповідають стратегії розвитку мереж доступу, яка зветься «волокно в дім» або FTTx, де під індексом «x» розуміють кінцевий пункт представлення послуг волокном [1].

Розподільна мережа доступу PON заснована на деревовидній волоконно-кабельній архітектурі з пасивними оптичними розгалужувачами на вузлах, представляє економічний спосіб забезпечити широкосмугову передачу інформації. При цьому архітектура PON має необхідну ефективність нарощування вузлів мережі і пропускної спроможності, залежно від справжніх і майбутніх потреб абонентів.

Схематично PON можна уявити у вигляді дерева. Оптоволоконна лінія розгалужується від центральної станції з використанням пасивних оптичних

дільників сигналу (спліттерів). Активне обладнання встановлюється тільки на межах мережі, а всередині таке обладнання не потрібне. Термінал оптичної лінії (OLT), розташований на стороні центральної станції, зв'язується з безліччю оптичних мережевих терміналів (ONT), які розташовані в приміщеннях абонентів. Залежно від PON-технології, кількість споживчих терміналів, які обслуговуються одним інтерфейсом OLT, досягає 16, 32, 64 і більше [2].

Задача проектування PON зводиться до послідовності наступних операцій: вибір місця встановлення ONU, вибір топології мережі, трас проходження кабелю та місць встановлення розгалужувачів, розрахунок бюджету втрат потужностей для кожної гілки мережі та визначення оптимальних коефіцієнтів ділення всіх розгалужувачів, врахування фінансових затрат на впровадження та розвиток мережі.

Найбільш відповідальна задача проектування – розрахунок бюджету втрат потужностей та визначення оптимальних коефіцієнтів ділення потужності всіх розгалужувачів [4].

Для прикладу приведені розрахунки бюджету втрат на сегменті мережі, що має наступний вид:

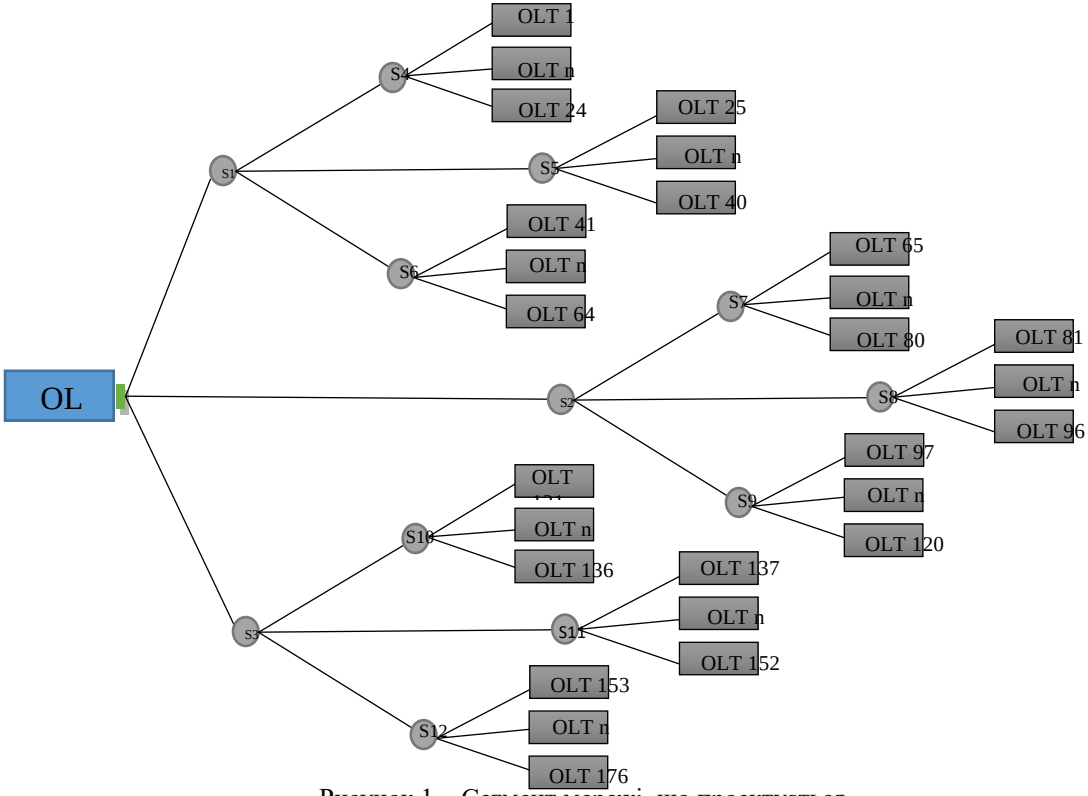


Рисунок 1 – Сегмент мережі, що проектується

Для кожної оптичної лінії наведемо всі втрати як суму затухань всіх компонентів:

$$A_{\Sigma} = (l_1 + \cdots + l_n) \cdot \alpha + N_p \cdot A_p + N_C \cdot A_C + (A_{\text{РОЗ1}} + A_{\text{РОЗ}m}), \text{дБ}$$

де A_{Σ} – сумарні втрати в лінії (між OLT і ONU), дБ;

l_n – довжина n-ділянки, км;

α – коефіцієнт затухання оптичного кабелю, дБ/км;

N_p – кількість роз'ємних з'єднань;

A_p – середні втрати в роз'ємному з'єднані, дБ;

N_C – кількість зварних з'єднань;

A_C – середні втрати в зварному з'єднані, дБ;

$A_{\text{РОЗ}m}$ – втрати в m-оптичному розгалужувачі, дБ.

Висновки:

Визначивши загасання на кожній оптичній лінії, необхідно підібрати розгалужувачі з таким коефіцієнтом ділення, щоб сумарне затухання на кожному ONU було приблизно рівним.

Також надано приблизні розрахунки щодо вартості підключення абонента до даного сегменту мережі, приведено приклади обладнання PON та оптичних кабелів.

Перелік посилань:

1. http://susolya-byk.narod.ru/vosp/37.htm/Пасивні оптичні мережі, їх застосування, стандарти, топології цих мереж.

2.http://wiki.kspu.kr.ua/index.php/PON/ Технологія пасивних оптичних мереж.

3. Рекомендація ITU-T G.983.1. Широкополосные оптические сети доступа на базе пассивных оптических сетей.

4. http://deps.ua/knowegable-base-ru/articles/item/465-praktika-proektirovanija-passivnyh-opticheskih-setej-pon.html/Практика проектирования пассивных оптических сетей (PON).

5. Рекомендація ITU-T G.984.1. Gigabit-capable Passive Optical Networks (G-PON): General characteristics.

6. Рекомендація ITU-T G.984.1. Gigabit-capable Passive Optical Networks (G-PON): General characteristics.

7. Алексеев Е.Б. Оптические сети доступа. Учебное пособие – М: ИПК при МТУ СИ, 2005 г. – 140 с.

8. http://shron.chtyvo.org.ua/Odnoroh_PM/Pasyvni_optychni_merezhi_xPON.pdf/ Оптичні мережі доступу (xPON) Однорог П. М., Михайленко Є. В., Котенко М. О., Омецінська О. Б.

9. http://book.itep.ru/4/41/pon.htm/ Пассивные оптические сети (PON/EPON/GEPON) Семенов Ю.А. (ИТЭФ-МФТИ).

10. http://istrade.com.ua/index.php?route=product/category&path=55/ Интернет магазин сетевого оборудования. Оптические панели.

11. http://www.telcon.ru/equipment/split/ Официальный сайт компании «Телсон».

12. Дані, надані провайдером телекомунікацій «Альфа Інет».

НЕСАНКЦІОНОВАНИЙ ДОСТУП ДО ІНФОРМАЦІЇ В ВОЛОКОННО-ОПТИЧНИХ ЛІНІЯХ ЗВ'ЯЗКУ ПРИ ВТРАТАХ У ВОЛОКНІ

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

Науковий керівник: викладач **Фіньковська М. С.**

Анотація. *Метою роботи є аналіз можливих методів несанкціонованого доступу (НСД) до інформації в волоконно-оптичних лініях зв'язку (ВОЛЗ) при втратах в волокні. Досліджено метод НСД на вигині ОВ. Підрахований критичний кут, зменшення якого приведе до порушення дії закону повного внутрішнього відбиття. Досліджено залежність загасання від радіусу вигину ОВ на двох довжинах хвиль 1310 нм та 1550 нм.*

На сьогоднішній день кожен бажає передавати свої дані по лінії зв'язку, яка б володіла тими вимогами, які висуває їй суспільство. Насамперед велика пропускна здатність, якість зв'язку, доступність, надійність. Саме ці вимоги надають ВОЛЗ. Волоконно-оптичні лінії зв'язку – це вид зв'язку при якому інформація передається по оптичним діелектричним хвилеводам, відомих під назвою «оптичне волокно». Швидкість потоку інформації, що передається по ВОЛЗ, може досягати декількох терабіт в секунду. Також оптоволоконні канали дозволяють збільшувати ємкість мережі.

В сучасному суспільстві з огляду на зростання обсягу конфіденційної інформації, що передається по ВОЛЗ, дедалі більшого значення набуває проблема її захисту від НСД. Утім хоча ВОЛЗ забезпечують підвищений рівень захисту переданої інформації, завжди існує принципова можливість здійснити несанкціоноване зняття інформації (НЗІ) з ОК. Здійснити НЗІ з ВОЛЗ можливо, але тільки маючи фізичний контакт до ОВ, так як захисна оболонка й елементи конструкції ОК настільки сильно послаблюють можливе випромінення через волоконний світловод (ВС), що світло практично не проникає за межі оболонки. Дана тема на сьогодні є актуальною, тому моя робота присвячена аналізу можливих методів НСД до інформації в ВОЛЗ.

Були розглянуті три основних методи НСД до ВОЛЗ:

– розривний спосіб;
– безрозривний без примусового відводу потужності;
– безрозривний з примусовим відводом потужності.

Перші два методи не викликають інтерес. Перший метод легко виявити, зважаючи на те, що зловмисник не зможе зняти інформацію, адже система відстежить розрив кабелю і зупинить подальшу передачу даних. Другий метод дуже кропіткий, для його реалізації потрібно пройти дуже велику довжину кабелю, адже потужність, що розсіюється є величиною занадто малою[4].

Інтерес представляє третій спосіб НСД. Його можна реалізувати багатьма шляхами, але найцікавішим для мене виявився вигин ОВ. У місці такого вигину порушується закон повного внутрішнього відбиття і спостерігається випромінювання світлової енергії за межі ВС. Суть цього методу НСД полягає в тому, що світло поза межами ВС не розсіюється, а направлено виводиться з ВС. Саме цей метод був проаналізований і досліджений мною.

Для початку було проаналізовано, що відбувається в ВС при проходженні в ньому світла, як змінюється кут падіння на вигині. Відповідно до закону повного внутрішнього відбиття, кут падіння на межі середовища, оптично більш щільного (серцевина) з середовищем менш щільним (оболонка), повинен бути більше критичного кута ($\varphi_п > \theta_{кр}$). Якщо світло у СВ розповсюджується згідно з цим законом, то не буде спостерігатись випромінення через оболонку[5, 6]. Щоб дізнатись, під яким кутом повинен рухатись промінь в ВС, щоб світло не заломлювалось на межі серцевина-оболонка ОВ, був підрахований критичний кут $\theta_{кр}$ для оптичного кабелю виробництва ВАТ «Одескабель» марки ОКЛБг–3–ДА12–2×4Е–0,40Ф3,5/0,35Н3,5 – 36/0. Підраховані показники заломлення n_1 та n_2 для ОВ, яке згідно ряду Селмейера має таку рецептуру: в якості матеріалу серцевини вибрано скло з добавками брому – 3,5% BrO_4, 96,5% SiO_2, а в якості матеріалу оболонки скло з добавками германію – 4,1% GeO_2, 95,9% SiO_2 [7]. Проаналізовані випадки, в яких $\varphi_п > \theta_{кр}$ та $\varphi_п < \theta_{кр}$.

Телекомунікаційні стандарти встановлюють граничний (мінімальний) радіус вигину ОК без прив’язки до довжини хвилі. На даний момент воно складає не менше двадцяти діаметрів кабелю.[8] Тобто кабель з діаметром в 2 мм має граничний радіус вигину 40 мм. Щоб зрозуміти, наскільки великі втрати відбуваються на вигині ОВ з радіусом меншим, ніж двадцять діаметрів кабелю, був проведений дослід. Дослід полягав в тому, що було проведено вимірювання загасання на довжинах хвиль 1310 нм і 1550 нм при різних значеннях радіусу вигину волокна, в результаті отримана залежність загасання від радіусу вигину ОВ (рис. 1).

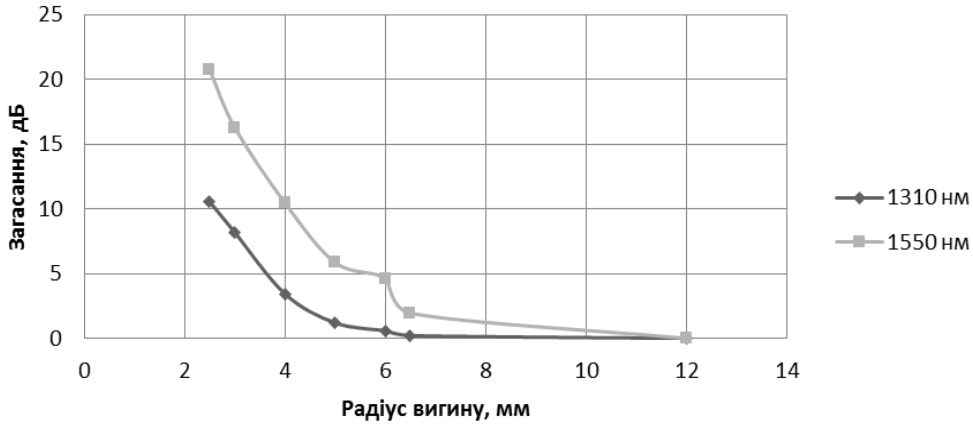


Рисунок 1 – Залежність загасання від радіусу вигину ОВ

Існують наступні методи захисту інформації ОК, які зараз набувають актуальності, до них відносяться: розробка технічних засобів захисту від НСД до інформаційних сигналів, які передаються по ОВ; розробка технічних засобів контролю НСД до інформаційного сигналу, який передається по ОВ; розробка технічних засобів захисту інформації, яка передається по ОВ, реалізуючи принцип маскування, додавання завад, оптичної або квантової криптографії [13].

Висновки:

1. Здійснити НСД до інформації в ВОЛЗ все ж можливо, тільки маючи фізичний доступ до ОВ, оскільки захисна оболонка й елементи конструкції ОК настільки сильно послаблюють можливе випромінення через волоконний світловод (ВС), що світло практично не проникає за межі оболонки.
2. Розрахунки критичного кута показали, що якщо збільшити кут падіння до значення більшого ніж критичний кут $\varphi_{п} > \theta_{кр}$, то буде спостерігатись виконання закону повного внутрішнього відбиття, і все світло залишиться в ВС без випромінення. Якщо зменшити цей кут падіння, то з’явиться кут заломлення і, як наслідок, – частина світла буде випромінюватись. В результаті зловмисник може перехватити корисну інформацію.
3. Наведено залежність, яка показує, що зі зменшенням радіусу вигину – збільшується загасання. До того ж виявлено, що на довжині хвилі 1550 нм спостерігається більше загасання при одних і тих же радіусах вигину, порівняно з 1310 нм, а саме майже в два рази більше. Це свідчить, що саме на цій довжині хвилі слід проводити виміри, щоб знайти місце вигину і завадити спробі НЗІ.
4. В сучасному світі зі стрімким розвитком телекомунікаційних систем

збільшується потреба в захисті конфіденційної інформації, яка передається волоконно-оптичними лініями зв'язку, тому сьогодні існує багато методів для захисту від НЗІ із ОК. Зловмисник «не стоїть на місці» і розробляє нові методи НСД, а це означає, щоб захистити свою інформацію від потрапляння в руки зловмисника – слід використовувати новітні способи захисту або доповнювати уже існуючі.

Перелік посилань:

1. http://izmer-ls.ru/w/r01.html/Листвин А.В. Листвин В.Н. Рефлектометрия оптических волокон. Типы оптических волокон.
2. http://www.teralink.ru/?do=printt&id=16/Преимущества и недостатки ВОЛС Р.Р.Убайдуллаев, к.ф.-м.н., Тералинк Волоконно-оптические сети, ЭКО-ТРЕНДЗ, М., 2000.
3. http://zakon3.rada.gov.ua/laws/show/2594-15/Закон від 31.05.2005 № 2594-IV Про внесення змін до Закону України "Про захист інформації в автоматизованих системах" Верховна Рада України.
4. http://5fan.ru/wievjob.php?id=47247/Разработка методов защиты волоконно-оптических линий связи от несанкционированного доступа на основе использования концепции кодового зашумления.
5. https://www.youtube.com/watch?v=HN37Jz8DHYg/Полное внутреннее отражение.
6. Иоргачев Д.В., Бондаренко О.В., Дащенко А.Ф., Усов А.В. Волоконно-оптические кабели. Теоретические основи, конструирование и расчёт, технология производтваи експлуатация. - Одеса: Астропринт, 2000.-536 с.
7. В. И. Корнейчук, Т. В. Макаров, И. П. Панфилов, О. П. Проживальский. Учебное пособие. Издание четвёртое стереотипное. Проектирование волоконно-оптических систем передачи. Таблица «Коэффициэенты ряда Селмейера для кварцевых стекол» // Одесса, 2006.
8. http://www.optik64.ru/doc06.htm/ИП Гавриков Юрий Владимирович Формула предельного радиуса изгиба оптического кабеля.
9. Руководство по эксплуатации Измеритель оптической мощности Acterna OLP-55 BN 2277/98.11 01/04.11 Русский.
10. Руководство по эксплуатации Источники оптические лазерные Acterna OLS-55, OLS-56 BN 2279/98.11 01/04.11 Русский.
11. https://www.youtube.com/watch?v=2DvaubDDbss/Tap Optical Fibre.
12. http://www.fod.ru/pdf/manual/5503.pdf/Волоконно-оптический ответвитель-прищепка Модель FOD 5503.
13. http://www.rusnauka.com/5_SWMN_2011/Informatica/4_79758.doc.htm/ Шматок А.С., Таценко А.В. ОНАС им. А.С. Попова, Украина Методы и средства защиты волоконно-оптических линий связи от несанкционированного доступа.

РОЗРОБКА КЛІЄНТ-СЕРВЕРНИХ ДОДАТКІВ В СОЦІАЛЬНИХ МЕРЕЖАХ

Краєв О. В., студент 2-го курсу, група О-21, спеціальність «Монтаж, обслуговування та ремонт апаратури зв'язку і оргтехніки».

Науковий керівник: викладач **Грачова Ю. М.**

Анотація. *Розроблено додаток в соціальній мережі "Вконтакте" для навчання студентів Коледжу зв'язку та інформатизації ОНАЗ ім. О. С. Попова. Мета роботи – введення сучасних технологій в систему навчальної та методичної діяльності коледжу, формування інформаційного освітнього середовища, ефективна організація роботи навчальних груп та викладачів, мобільна безперервна освіта та самоосвіта.*

Різні архітектурні рішення, які застосовуються при проектуванні програмного забезпечення, визначають продуктивність системи, зручність її розвитку і використання. Однією з них є архітектура клієнт-сервер, яка на сьогоднішній день користується великою популярністю. Це така архітектура програмного забезпечення, в якій функції розподілені між постачальниками послуг (серверами) і замовниками послуг (клієнтами).[1]

Основні функції архітектури клієнт-сервер – функції зберігання, обробки і представлення даних. У випадку, якщо обробка даних відносно нескладна, може бути досить дволанкової архітектури (клієнтський додаток і сервер баз даних).

Протягом останніх десяти років фахівці з обчислювальної техніки працюють над вдосконаленням клієнт-серверних додатків. При використанні складних алгоритмів обробки використовуються триланкова і багатоланкова архітектури, в яких функція обробки даних винесена відповідно на один або декілька окремих серверів. Розробляються програми, що забезпечують спільну роботу великої кількості користувачів з джерелом даних в мережі. Вони реалізуються на основі моделі сервера додатків, де мережевий додаток розділений на дві або більше частин, кожна з яких може виконуватися на окремому комп'ютері (рис. 1). Виділені частини додатка взаємодіють один з одним, обмінюючись повідомленнями в заздалегідь узгодженому форматі. [2]

Компоненти в триланковій архітектурі розподіляються наступним чином:

1. Представлення даних (інтерфейс, як правило, графічний GUI) – на стороні клієнта.

2. Прикладний компонент (програмний код) – на виділеному сервері додатків (виконує функції проміжного ПЗ).

3. Управління ресурсами – на сервері БД, яка і видає запитувані дані.

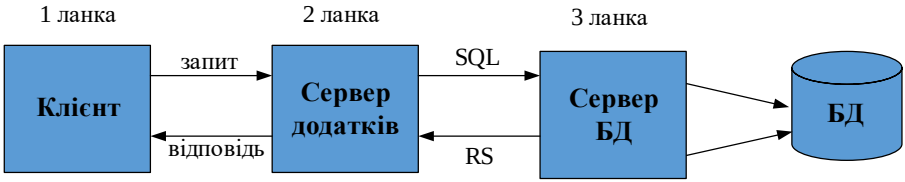


Рисунок 1 – Триланкова клієнт-серверна архітектура

Сервер бази даних забезпечує виконання основного обсягу обробки даних. Формовані користувачем або додатком запити надходять до сервера БД у вигляді інструкції мови SQL (Structured Query Language - структурована мова запитів). Сервер БД виконує пошук і витяг потрібних даних, які потім передаються на комп'ютер користувача. Системи керування БД, що працюють з серверами додатків, дозволяють безлічі користувачів різних ЕОМ (іноді розташованих досить далеко один від одного) отримувати доступ до одних і тих самих баз даних.

Соціальна мережа – яскравий приклад реалізації клієнт-серверної архітектури. В якості клієнта виступає браузер користувача, а сервером додатків є web-сервер.

Розробку програми можна поділити на наступні етапи:

- складання завдання, яке містить мету, задачі, мову програмування, framework і чистий код, методи здійснення передачі даних, інтерфейси і зовнішній вигляд програми, графічний дизайн;
- створення API додатку (серверної частини);
- написання клієнтської частини;
- тестування;
- відладка.

На сучасному етапі спостерігається масове впровадження інформаційних технологій в усі сфери освіти. Провідною метою інформатизації системи освіти є перетворення сучасних інформаційних ресурсів та інформаційно-комунікаційних технологій в ресурс освітнього процесу, що забезпечує формування якісно нових результатів освіти.[3] Розроблено клієнт-серверний додаток в соціальній мережі "Вконтакте", який студенти будуть використовувати для навчання як під час аудиторних занять, так і для самостійної роботи. При запуску додатку зі сторінки користувача, його ідентифікатор та секретний ключ передається на віддалений сервер, де знаходиться додаток. Після чого додаток виконує ініціалізацію та перевірку ключа. Якщо він валіден – додаток запускає основний інтерфейс. Якщо користувач зареєстрований в системі - відображається перелік дисциплін. Якщо не зареєстрований – запускається інтерфейс введення пароля. Далі студент може використовувати завантажені матеріали лекцій для самостійного вивчення та виконувати перевірку знань за допомогою тестів. Всі взаємодії в основному

інтерфейсі здійснюються за допомогою AJAX (завантаження лекцій/тестів, відправка/перегляд результатів).

Для написання серверної частини програми використовується мова програмування PHP та бази даних MySQL (PhpMyAdmin). PHP - це мова програмування, спеціально розроблена для написання web-додатків (сценаріїв), що виконуються на web-сервері. [13] PHP доступний для більшості операційних систем, включаючи Linux та різних модифікацій Unix. В PHP включена підтримка більшості сучасних web-серверів, таких, як Apache, Microsoft InternetInformation Server та ін. MySQL - це найбільш популярна система керування базами даних, яка дуже часто застосовується в поєднанні з PHP [12.]

Клієнтська частина розробляється на мові JavaScript. JavaScript - прототипно-орієнтована мова програмування сценаріїв. Найбільш широке застосування знаходить в браузерах як мова сценаріїв для надання веб-сторінкам інтерактивності. Для забезпечення високого рівня абстракції і досягнення прийнятного ступеня крос-браузерності при розробці веб-додатків використовуються бібліотеки JavaScript - JQuery та JQueryUI. Більшість фреймворків автоматизованого тестування JavaScript-коду дозволяють запуск тестів в браузері. Це здійснюється за допомогою HTML-сторінки.[11] HTML (Hyper Text Markup Language - «мова гіпертекстової розмітки») - стандартна мова розмітки документів у Всесвітній павутині. CSS (Cascading Style Sheets - каскадні таблиці стилів) - формальна мова опису зовнішнього вигляду документа, написаного з використанням мови розмітки HTML. CSS використовується для задання кольорів, шрифтів, розташування окремих блоків та інших аспектів представлення зовнішнього вигляду веб-сторінок. [10]

Взаємодіє програма з соціальною мережею "ВКонтакте" за допомогою API (тип додатку IFrame) [8].

Висновки:

Розробка клієнт-серверної програми в соціальній мережі - це досить трудомістка робота, яка включає в себе багато операцій і вимагає від програміста поглиблених знань. Але створення подібних додатків дозволяє отримати багато переваг, а саме:

1. Соціальна мережа – звичне середовище для студентів. Інтерфейс, способи комунікації та публікації контенту в цьому середовищі користувачами вивчені досконально. Цьому сприяє якісне юзабіліті (зручність і зрозумілість) системи, а також активний і тривалий досвід використання (70% користувачів відвідують мережу частіше, ніж 1 раз на добу). Тестування програми в групах показало, що більшість раді, що можуть використовувати її для навчання.

2. Безкоштовність. Немає необхідності купувати спеціальне програмне забезпечення і розміщувати сервера для зберігання цифрових даних і організації комунікації в мережі. Соціальні мережі це надають безкоштовно.

3. Студенти залучені в соціальні мережі більше, ніж в будь-які інші веб-ресурси.

4. Соціальні мережі володіють функціоналом, що дозволяє оперативно ділитися зі студентами важливою інформацією.

5. Навчаючись в соціальних мережах, студенти освоюють навички XXI сторіччя, а саме, оволодіння засобами і способами комунікації з іншими людьми і пошук/аналіз інформації в епоху інформаційного суспільства.

6. Підтримка навчального курсу за допомогою соціальної мережі дозволяє студентам, які пропускають з тих чи інших причин аудиторні заняття, не випадати з освітнього процесу.

7. Можливість постійної взаємодії студентів і викладачів в мережі в зручний для них час забезпечує безперервність навчального процесу. З'являється можливість більш детального планування навчальної роботи студентів.

8. Економія паперу. Лекційний матеріал та тестові завдання тепер не потрібно роздруковувати, достатньо його прикріпити у вигляді файлу в соціальній мережі.

Саме соціальна мережа "Вконтакте" через високу ступень активності та залучення в неї сучасних студентів була обрана в якості майданчика для організації навчальної роботи із застосуванням інформаційно-комунікаційних технологій.

Необхідно і надалі розробляти ефективні методики застосування соціальних мереж в освітньому просторі.

Перелік посилань:

1. http://www.4stud.info/networking/lecture5.html/ Компоненты сетевого приложения. Клиент-серверное взаимодействие и роли серверов.

2. http://www.4stud.info/networking/application-server.html/ Серверы приложений.

3. http://www.moluch.ru/conf/ped/archive/21/1799/ Социальные сети как средство обучения и взаимодействия участников образовательного процесса.

4. http://www.journal-discussion.ru/publication.php?id=974 / Социальные сети как современная образовательная середа.

5. http://vk.com/dev/ Разработка приложений.

6. https://vk.com/dev/users.get / Список методов users.get.

7. https://vk.com/dev/auth_mobile/ Авторизация клиентских приложений.

8. https://vk.com/dev/IFrame_apps/ IFrame-приложения.

9.https://ru.wikipedia.org/wiki/ Интерфейс программирования приложений».

10. http://htmlbook.ru/ Справочник по HTML CSS.

11. http://javascript.ru/tutorial/intro – Javascript

12. http://www.php.su/mysql/ PHP и MySQL.

13. http://www.php.su/ Ресурс по PHP.

14. http://ubuntu.ru/about / «Об Ubuntu.

15. https://ru.wikipedia.org/wiki/VPS/ Виртуальный хостинг VPS.

СЕКЦІЯ РАДІОЗВ'ЯЗКУ, РАДІОМОВЛЕННЯ ТА ТЕЛЕБАЧЕННЯ

ВИКОРИСТАННЯ ПЛАНШЕТІВ ТА СМАРТФОНІВ ДЛЯ ПРИЙОМУ МОБІЛЬНОГО ТВ

Бондаренко В.С., Лапчевський Є.В., студенти 2-го курсу, група Р-21, спеціальність 5.05090306 «Монтаж, технічне обслуговування і ремонт обладнання радіозв'язку, радіомовлення та телебачення».

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

Анотація. *Розвиток цифрових технологій сприяв зростанню персонального споживання інформації. Впровадження мобільного телевізійного мовлення дозволило транслювати телебачення на мобільні портативні пристрої у спеціальному форматі з можливістю використання функції інтерактивності. Надані порівняльні характеристики зросту використання мобільного телебачення у світі.*

Протягом останніх років стрімкий розвиток цифрових технологій сприяв зростанню персонального споживання інформації. Впровадження стандарту DVB-H (мобільне ТВ мовлення) дозволило транслювати телебачення «наживо» безпосередньо на мобільні портативні пристрої. Тепер немає жодних обмежень - дивитися телевізійні програми можна, де завгодно і коли завгодно. Мобільне телебачення - це прийом телевізійних програм у спеціальному форматі на мобільні термінали з можливістю використання функції інтерактивності. Мобільне телебачення − збірне поняття, що відноситься до будь-якої технології доставки телеканалів до портативного пристрою абонента.

У наш час інженери прагнуть мінімізувати розміри апаратури радіозв'язку, застосовуючи замість енергоємних електронних ламп, малогабаритні напівпровідникові елементи. Спочатку на їх основі створювалися схеми з окремих елементів, але потім ці схеми почали об'єднувати в структури на одному цілісному кристалі – монокристальні чипи. Використовуючи малогабаритні мікросхеми, побудовані на монокристалах, ми економимо енерговитрати на виробництві та експлуатації техніки зв'язку.

До теперішнього часу не прийнято єдиного стандарту мобільного телебачення. Існує близько 10 стандартів, які використовуються в різних регіонах світу. Кожен із стандартів мобільного телебачення має свою зону впливу: в Європі поширений DVB-H, MediaFLO популярний у Північній Америці, а DMB-T − в Азії і низці європейських країн

Мобільне телебачення – це прийом телевізійних програм в спеціальному форматі на мобільні термінали з можливістю використання функції інтерактивності. Послуга мобільного телебачення надається двома основними способами – через мережу мобільного зв'язку (як потік відеоданих) або через окрему виділену мережу. Головна відмінність цих способів полягає в моделі передачі даних – за першого способу дані стають доступними лише окремому користувачу, тоді як за другого способу – для всіх власників терміналів мобільного зв'язку.

Зараз більшість фахівців віддають перевагу стандарту DVB-H, заснованому на стандарті наземного телевізійного мовлення DVB-T, який працює в ряді країн Європи. DVB-H розширює деякі встановлювані параметри, орієнтовані на умови прийому цифрових сигналів в мобільних умовах. У той час, як мережа DVB-T створювалась, головним чином, для прийому на антени, встановлені на дахах будівель, мережа DVB-H повинна розроблятися так, щоб її сигнали могли прийматися на портативні термінали не тільки поза будівель, але і за бетонними стінами. Це означає, що щільність потоку потужності мовного сигналу повинна бути набагато більше. Для створення необхідних значень можна використовувати різні варіанти мережевої архітектури, вибір яких залежатиме від робочого діапазону частот, допустимих значень максимальної потужності передавача і висот установки антени:

– використовується існуюча мережа DVB-T, сигнал DVB-H передається в тому ж мультиплексивному потоці;

– мережі DVB-T і DVB-H використовують ієрархічну передачу в одному і тому ж частотному каналі, причому найвищий пріоритет - у DVB-H;

– мережа «тільки DVB-H».

Що стосується топології мережі, то найбільш проста архітектура мережі − це мережа, в якій працює один головний передавач і кілька ретрансляторів, які підвищують рівень сигналу на кордонах осередки. Ці ретранслятори необхідні, коли, наприклад, немає можливості підвісити антену основного передавача досить високо, або для заповнення зон радіотіні в зоні прийому.

Якщо потрібно забезпечити мовлення на території цілої держави, на площах у сотні і тисячі квадратних кілометрів, то потрібно кілька радіочастотних каналів. Якщо для сигналів DVB-H може бути зарезервований повний мультиплексований потік, то різко зростає гнучкість в плануванні мереж.

Є два основні варіанти архітектури для систем мовлення за стандартом DVB-H. Перший з них, найбільш характерний для традиційних мовників, резервує частину наявного частотного каналу для передачі сигналу DVB-T, а все, що залишається в смузі пропускання, виділяє під програми DVB-H. Це дозволяє мовним компаніям додатково транслювати новий потік, що просто неможливо в аналоговому телебаченні. Методи роботи з сигналом DVB-H в обох моделях однакові.

Класичні телефони для перегляду TV мають вбудований тюнер для прийому телевізійного сигналу. Тюнер цей може бути як цифровим, так і аналоговим. Робота

класичного аналогового TV-тюнера зводиться до того, щоб вловлювати сигнали, поширювані на певній частоті. Як і FM-тюнер, TV-тюнер сканує певний діапазон частот і вловлює ті радіохвилі, які відповідають каналу, обраному користувачем в меню телефону. Після цього спеціальне обладнання та програмне забезпечення пристрою витягують з отриманого сигналу відео і звук.

Стандарт зв'язку GSM 2G міг забезпечувати передачу даних зі швидкістю 171,2 Кбіт /с, з приходом мереж 3G ця швидкість зросла до 2 Мбіт / с. Крім того, застосування 3G дозволило більш економно використовувати доступний діапазон частот, так як всі користувачі одночасно отримали можливість працювати з одним і тим же радіопотоком.

Для перегляду ТВ-програм на Android-девайсах розроблений незвичайний ТВ-тюнер AVerTV Mobile 510- компактний і легкий пристрій з інтерфейсом microUSB. Вага гаджета складає всього 7,5 г, що дозволяє постійно носити його з собою. Кишеньковий ТВ-тюнер підтримує прийом сигналу цифрового мовлення стандартів DVB-T і DVB-T2. У комплект поставки крім ТВ-тюнера входить високочутлива антена. Вона оснащена зручним кріпленням і присоскою, що дозволяють розміщувати її як завгодно.

Економічно виправданою і ефективною технологією для широкомовної передачі є DVB (зокрема, для доставки інформації на мобільний термінал використовується її модифікація DVB-H або DVB-SH / 3G). Стандарт DVB-H реалізує звичайний UHF-діапазон (470-700 МГц). DVB-SH (2170-2200 МГц) являє собою модифікацію, покликану переглянути використання існуючої наземної інфраструктури WCDMA. Найбільш актуально це для країн, де мережі 3G вже розгорнуті, а виділити звичайний UHF-діапазон для DVB-H не представляється можливим (наприклад, у Великобританії).

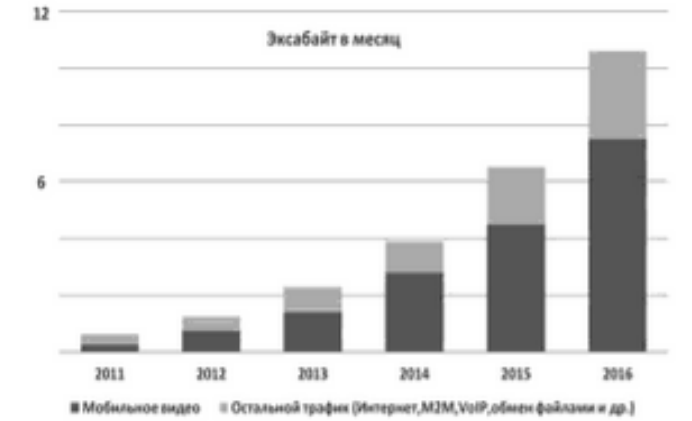
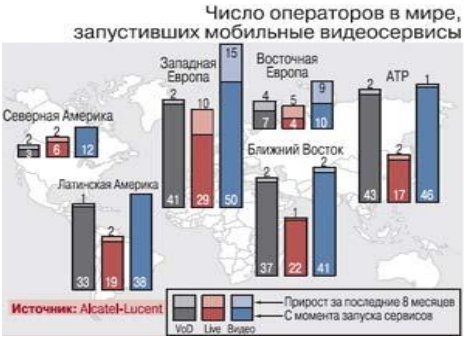


Рисунок 1 – Зростання популярності і затребуваності послуг мобільного ТБ



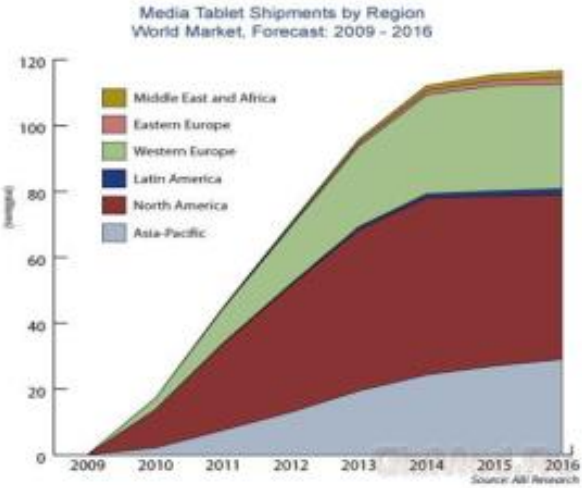


Рисунок 3 – Зріст популярності планшетів у всьому світі

Зростання популярності і затребуваності послуг мобільного ТБ демонструє динаміка і прогноз розподілу трафіку в мережах мобільного зв'язку. Зростання абонентської бази і доходів стримується фізичними обмеженнями наявних мереж, вимагаючи їх модернізації, а часто і впровадження нових високошвидкісних технологій.

Висновки:

1. Складність системи DVB-H більше пов'язана зі складністю всієї системи передачі, ніж з окремими методами, застосовуваними для забезпечення ефективної доставки сигналу цифрового телевізійного мовлення на портативні термінали.

2. Для створення необхідних значень щільності потоку потужності у мережах DVB-H можна використовувати різні варіанти мережевої архітектури, вибір яких

залежатиме від робочого діапазону частот, допустимих значень максимальної потужності передавача і висот установки антени.

3. Цифрове мовлення відео за технологією DVB-H (прийом на мобільні пристрої) дозволяє забезпечити прийом «живого» телебачення на мобільні мініатюрні термінали (КПК, стільникові телефони), тобто дати можливість реалізації персонального мобільного телебачення.

4. Мобільне ТВ мовлення дозволило транслювати телебачення «наживо» безпосередньо на мобільні портативні пристрої. Тепер немає жодних обмежень - дивитися телевізійні програми можна де завгодно і коли завгодно.

5. Зростання популярності і затребуваності послуг мобільного ТБ вимагає розширенню мереж та їх модернізації, а часто і впровадження нових високошвидкісних технологій.

6. Стандарт DVB-H має всі шанси стати глобальним лідируючим стандартом цифрового мобільного телемовлення

7. Стандарт DVB-H підтримується виробниками абонентських пристроїв, що сприяє швидкому переходу послуги мобільного ТБ в масовий сегмент.

Перелік посилань:

1. В. А. Серов. Эфирное цифровое телевидение DVB-T/H. – СПб.: БХВ-Петербург, 2010.

2. Бабин А.И. Технология мобильного телевидения стандарта DVB-H //– 2007. – № 12 – С. 152-154.

3. http://www.konturm.ru/Стандарт DVB-T.

4. http://www.iksmedia.ru/articles/3434320-Czifrovoe-mobilnoe-televidenie-goto.html/Цифровое мобильное телевидение готовится выйти в массы.

5. http://www.3dnews.ru/583627/Мобильное ТВ по DVB-H.

6. http://podberi-sotik.ru/article/articles/mobil-nye-telefony-s-tv-televizor-v-karmane/19.html/«Мобильные телефоны с TV: телевизор в кармане».

7. http://gizmod.ru/2013/11/26/yevolyuciya-planshetov-apple-i-ix/Эволюция планшетов.

8. http://www.remake.ru/analitika/technology/dvb-h.html/Плюсы и минусы нового стандарта мобильного телевидения DVB-H.

9. http://irvispress.ru/catalog/tv/sovremennye-tehnologii-tv/mobilnoe-televidenie-chto-eto-takoe/Телевидение, которое помещается в телефоне.

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ГЛУШІННЯ СИГНАЛУ СТАНДАРТУ GSM

Кислов Д. Ф., студент 4-го курсу, група Р-41, спеціальність 5.05090306 «Монтаж, технічне обслуговування і ремонт обладнання радіозв'язку, радіомовлення та телебачення».

Науковий керівник: викладач **Шалімов С. М.**

Анотація. *Розглядаються можливості перешкоджання розповсюдженню сигналу стільникового зв'язку стандарту GSM.*

Головна мета роботи – розглянути, практично застосувати та порівняти різні можливості перешкоджання розповсюдження сигналу стільникового зв'язку, визначити переваги та недоліки кожного із розглянутих приладів.

У наш час той хто володіє інформацією володіє світом. Саме тому зараз більшість організацій ставить своєю основною метою заволодіти інформацією конкурента, і не допустити втрату своєї у бік конкурентів.

Способом заволодіння вербальної інформації є підслуховування адміністративних нарад, важливих перемов, та інших засідань, які впливають на розвиток підприємства. Підслухування найчастіше відбувається за допомогою мобільного телефону стільникового зв'язку. У нашій країні серед стандартів мобільного зв'язку найбільш розповсюджений є GSM.

Один з найпростіших засобів радіоелектронної боротьби є електромагнітне екранування. Електромагнітне екранування це локалізація електромагнітного поля в певній частині приміщення. Воно дозволяє захистити як людину від впливу електромагнітного поля, так і радіоелектронні прилади від впливу зовнішніх полів і локалізувати їхні власні випромінювання, перешкоджаючи їх появі у навколишньому просторі. Екранування технічних засобів обробки інформації і приміщень, в яких відбувається прийом, передача та обробка конфіденційної інформації, дозволяє знизити рівні електромагнітних випромінювань до заданих величин. В результаті стає практично неможливим несанкціоноване вилучення інформації.

Найчастіше використовують у якості екрану клітку Фарадея - пристрій, винайдено англійським фізиком Майклом Фарадеєм в 1836 році для екранування апаратури від зовнішніх електромагнітних полів. Зазвичай вона представляє собою заземлену клітку, виконану з матеріалу, з добрими провідними властивостями. Принцип роботи клітки Фарадея дуже простий - при попаданні замкнутої електропровідної оболонки в електричне поле вільні електрони оболонки починають рухатися під впливом цього поля. В результаті протилежні сторони клітини набувають заряди, поле яких компенсує зовнішнє поле. В області високих частот дія такого екрану заснована на віддзеркаленні електромагнітних хвиль від поверхні

екрану і загасанні високочастотної енергії в його товщі внаслідок теплових втрат на вихрові струми.

Найпоширенішим засобом радіоелектронної боротьби є глушіння радіосигналу. Глушіння - цілеспрямоване створення активних перешкод для погіршення якості сигналу шляхом зниження його відношення сигнал / шум.

Глушіння може бути націлене на всіх, або на деяких певних одержувачів сигналу. Пристрій для глушіння представляє собою джерело перешкод (шумів). Шум - хаотичні коливання різної фізичної природи, що відрізняються складністю часової і спектральної структури. Шум кваліфікують за «кольором». Кольори шуму - система термінів, що приписують деяким видам стаціонарних шумових сигналів певні кольори виходячи з аналогії між спектром сигналу довільної природи (точніше, його спектральної щільності) і спектрами різних кольорів видимого світла.

Висновки:

У роботі розглянуті можливості перешкоджання розповсюдження сигналу стільникового зв’язку: екранування абонента за допомогою цільнометалевого екрану, екранування абонента за допомогою клітки Фарадея, глушіння сигналу за допомогою білого шуму.

Після проведення опитів стало зрозуміло, що екранування мобільної станції абонента за допомогою клітки Фарадея малоефективне через те, що для повного знищення сигналу у клітці потрібно забезпечити дуже щільне розміщення провідників. Мобільний телефон розміщений у середині металевого ящика повністю екрановано від проходження сигналу У випадку активного глушіння, за допомогою шуму смуга частот 800 – 1000 МГц. поглинається білим шумом, це запобігає проходженню сигналу від базової до мобільної станції абонента.

Для забезпечення перешкоджання витіку інформації під час проходження нарад найбільш ефективним є активне глушіння радіосигналу за допомогою генератора білого шуму оскільки для забезпечення радіоекранування однієї кімнати не потрібно додаткової підготовки приміщення. Потрібно лише увімкнути малопотужний генератор білого шуму.

На практиці у суспільному житті генератори білого шуму для глушіння сигналу GSM застосовуються не тільки у комерційній діяльності під час нарад , а й у театрах, навчальних закладах, лікарнях та інших установах.

Перелік посилань:

1. Закіров С.Г. Стільниковий зв'язок стандарту GSM. Сучасний стан, перехід до мереж третього покоління 2004.

2. Громаков Ю.О. Стандарти і системи рухомого радіозв'язку 2000.

3. Андріанов В.І. Засоби мобільного зв'язку. 1998.

4. Бурхливо В.Б. Електронний підручник по системі стільникового зв'язку з часовим поділом каналів стандарту GSM.

5. Антенно-фідерні пристрої систем сухопутного рухомого зв'язку / Под ред. А.Л. Бузова. М.: Радио и связь.1997 р.

6. Ратинський М.В. Основи стільникового зв'язку 2000.

7. http://en.wikipedia.org/wiki/GSM/ «GSM».

8.http://ekt.elit.sumdu.edu.ua/downloads/materials/Mob_sv_lec.pdf «Структура і організація мобільного звязку.

9.http://afu.com.ua/gsm/struktura-komponentov-seti/ Структрура компонентів мережі мобільного зв'язку.

10. Варакин Л.Е Системи зв'язку з шумоподібним сигналами 1985.

11. Добикін В. Д., Купріянов А. І., Пономарьов В. Г., Шустов Л. Н. Радіоелектронна боротьба. Силове поразку радіоелектронних систем 2007.

12. Цветнов В. В., Дьомін В. П., Купріянов А. І. Радіоелектронна боротьба. 1999.

13. https://ru.wikipedia.org/wiki/%D0%A8%D1%83%D0%BC/ Шум.

14. http://www.physel.ru/-mainmenu-29/-ainmenu-31/362-s-31---.html/ Розподіл зарядів в провіднику. Клітка Фарадея.

15. С. М. Аполлонский. Довідник за розрахунком електромагнітних екранів. 1988.

16.http://www.florentinesociety.ru/emi/Elektromagnitnye_Izlucheniya_Napravlennye_Na_Vas.pdf/ Електромагнітне випромінювання цілеспрямоване на вас.

17. http://www.modernarmy.ru/article/163/ РЕБ в сучасній війні.

Цифровий частотомір на мікроконтролері КР1878ВЕ1

Тарабара М.В., студент 4-го курсу, групи Р-41, **Колісниченко Р. Д.**, студент 3-го курсу група Р-31, спеціальності 5.05090306 «Монтаж, технічне обслуговування і ремонт обладнання радіозв’язку, радіомовлення та телебачення.

Науковий керівник: викладач **Козаченко Л. О.**

Анотація. *Розроблений і виконаний цифровий частотомір на мікроконтролері. Проведено аналіз використання застосованого мікроконтролера, його основні характеристики і можливості. Вироблена печатна плата і зібраний цифровий частотомір.*

Частотоміри є одними з розповсюджених вимірювальних пристроїв, оскільки вимір частоти є найпоширенішим виміром як в техніці зв`язку, так і в інших галузях.

Вимірюваннями частоти користуються при градуюванні шкал вимірювальних генераторів радіоприймальних і радіопередавальних пристроїв із плавним діапазоном; визначенні резонансних частот коливальних контурів і різних

резонаторів; визначенні смуги пропускання фільтрів і чотириполюсників; вимірюванні або контролі величини відхилення частоти від її номінального значення, привласненого даному пристрою – радіостанції, генераторному устаткуванню системи ущільнення і таке інше. Широке застосування безпошукового і безпідстроювального радіозв'язку, багатоканального високочастотного, супутникового, а також мобільного зв'язку виявилося можливим у результаті розвитку методів точного вимірювання частоти.

Застосування мікропроцесорних систем в цифрових електронно-лічильних частотомірах дозволяє автоматизувати установку необхідного діапазону частот і обчислювальних процедур, здійснити керування всіма блоками частотоміра і організувати їхню взаємодію, задавати необхідну тривалість «часових воріт» і формувати їх безпосередньо в мікропроцесорі; програмувати виконання набору функцій в багатофункціональних приладах, обробляти результати спостережень, здійснювати автоматичний контроль працездатності частотоміра, одержувати відображення результатів вимірювання в зручній формі, знижувати споживану потужність.

В даній роботі був розроблений і виготовлений цифровий частотомір на мікропроцесорі (МП) – мікроконтролері PIC16F628A.

Використання МП в ЕЛЧ дає можливість збільшити перелік завдань, розв'язуваних при вимірюваннях, розширити сервісні функції, забезпечити автоматичне повторення необхідних процедур вимірювання, знизити складність апаратурної реалізації за рахунок введення програмування [1].

Для виготовлення цифрового частотоміру був вибраний мікроконтролер PIC16F628A, який є головним блоком вимірювального приладу.

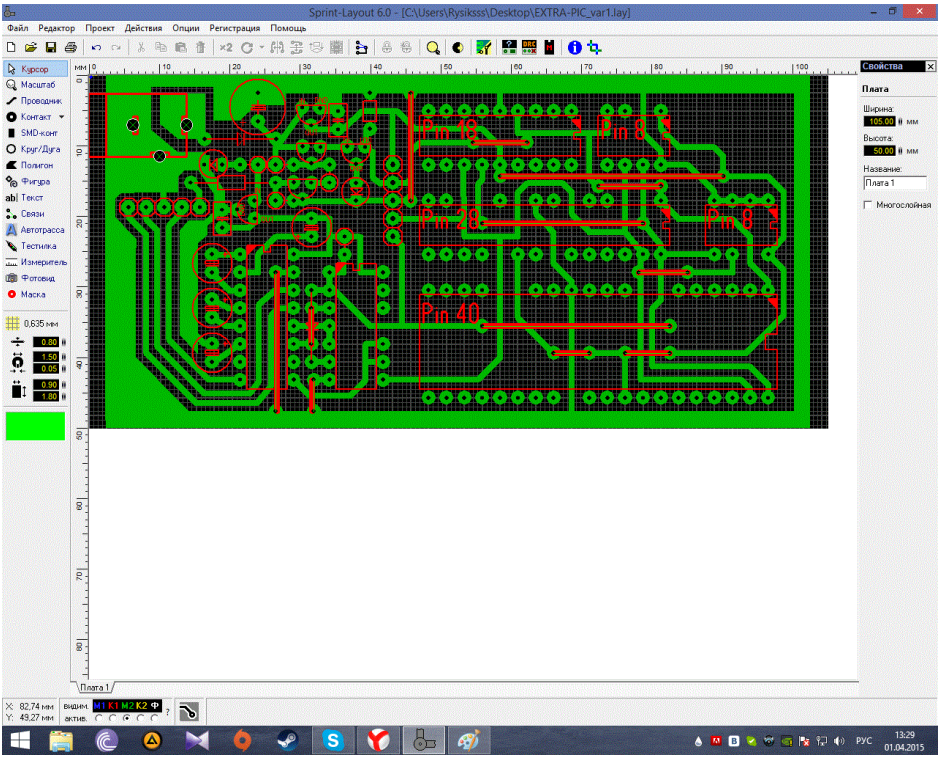
Мікроконтролер PIC16F628A є представником сімейства однокристальних 8-розрядних FLASH CMOS микроконтролерів компанії Microchip Technology Incorporated, USA [2]. Він призначений для використовування в системах управління, працюючих в масштабі реального часу. Мікроконтролер відрізняється малою кількістю зовнішніх виводів, низьким струмом споживання, високою продуктивністю, наявністю енергонезалежної пам’яті даних і можливістю багатократного перепрограмування пам’яті команд.

18-вивідні FLASH мікроконтролери PIC16F62X входять до складу поширеного сімейства PICmicro PIC16CXX. Мікроконтролери цього сімейства мають 8-розрядну, високопродуктивну і повністю статичну RISC-архітектуру. PIC16F62X мають 8-рівневий апаратний стек і велику кількість внутрішніх і зовнішніх переривань. У гарвардській архітектурі RISC ядра мікроконтролера розділені 14-розрядна пам'ять програм і 8-розрядна пам'ять даних. Такий підхід дозволяє

виконувати всі інструкції за один машинний цикл, крім команд розгалуження, які виконуються за два машинних цикли.

Мікроконтролери цієї серії задовольняють ряду параметрів для їх використання від зарядних пристроїв до віддалених датчиків з малим споживанням електроенергії. FLASH технологія і велика кількість периферійних модулів, сумісних з попередніми мікроконтролерами, дозволяють швидко і зручно розробляти програмне забезпечення. Висока продуктивність, мала вартість, легкість у використанні та гнучкість портів вводу/виводу - роблять PIC16F62X універсальними мікроконтролерами

Для розробки печатного монтажу була використана програмаSprint-Layout 4.0R. Це досить проста і зручна програма для ручного створення однобічних і двобічних друкованих плат, розміри яких не перевищують 300x300 мм . Програма працює у середовищі Windows 95, 98, ME, NT, 2000, XP і виконує всі необхідні для цього функції.



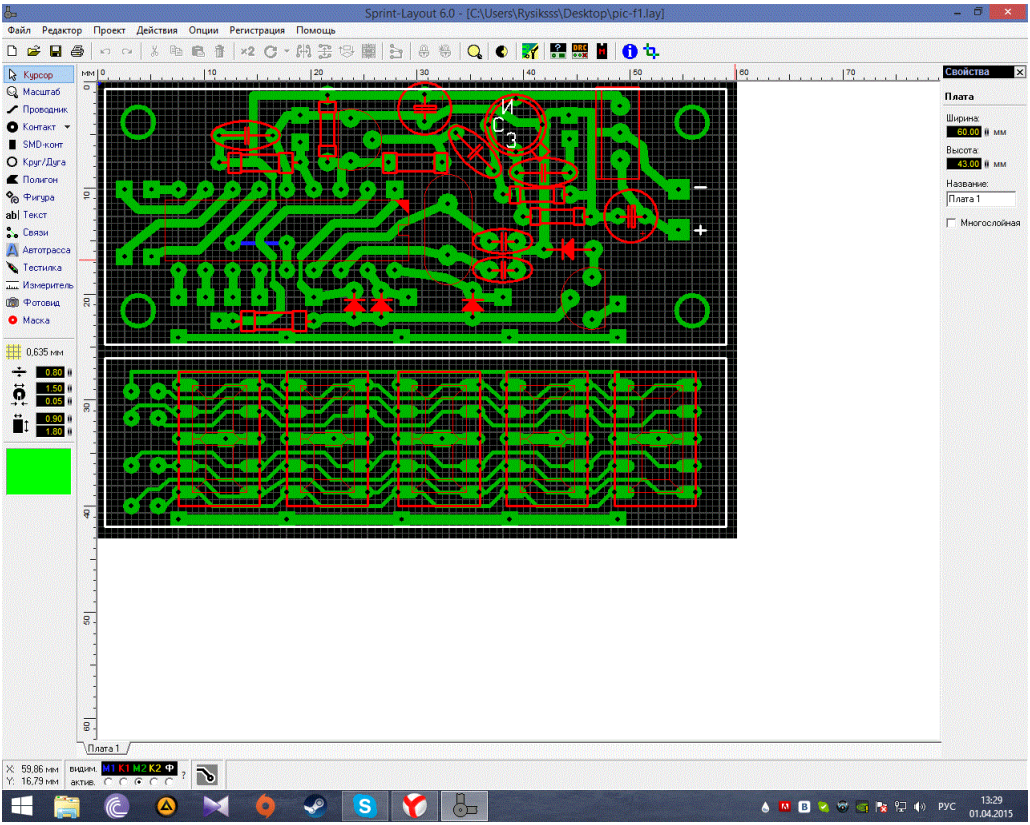


Рисунок 1 – Вигляд печатної плати

Перелік посилань:

1. http://elikt.narod.ru/shem/digital/shem07.htm/ Частотомер 1 Гц - 50 Мгц. Богомолов Дмитрий (г. Москва).

2. http://www.cqham.ru/forum/showthread.php?13104/ Частотомер на 1878ВЕ1 от Богомолова (печатная плата)

3. http://www.vsegta.ru/izm/frm/fmt14.htm/ Каталог радиолюбительских схем. Частотомер на микроконтроллере.

4. http://kazus.ru/shemes/showpage/0/989/1.html/ Простой программатор для КР1878ВЕ1.

5. Підручник «Вимірювання в системах зв’язку» «Книга 1.Загальні електрорадіовимірювання» Л. В. Коломієць, П. П. Воробієнко, М. Т. Козаченко, М. Б. Налісний, Л. О. Козаченко, О. В. Грабовський. – Одеса: ВМВ, 2009.

МЕНЕДЖЕРИ ПАРОЛЕЙ ТА ЇХ ВРАЗЛИВОСТІ

Воробйова О.О., студентка 4-го курсу, група О-42;

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

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

Анотація. *Розглядаються різноманітні та найпопулярніші менеджери паролів. В основі роботи дослідження основних методів атак на менеджери паролів.*

Головна мета дослідницької роботи – провести порівняльний аналіз менеджерів паролів, створити програму для здійснення атак на менеджери, визначити найкращий, на нашу думку, менеджер паролів. Для цього була створена програма і динамічно приєднувана бібліотека в інтегрованому середовищі розробки C++ Builder.

Менеджер паролів – програмне забезпечення, яке допомагає користувачеві працювати з паролями і PIN-кодами. У такого роду програмного забезпечення зазвичай є місцева база даних або файли, які містять зашифровані дані паролів. Багато менеджерів паролів також працюють як заповнювач форми, тобто вони заповнюють поле користувач і пароль автоматично в формах. Зазвичай вони реалізовані як розширення браузера.

Переваги менеджера паролів в тому, що його також можуть використовувати як захист від фішингу. На відміну від людей, програма менеджер паролів може звертатися з автоматизованим скриптом логіна не сприйнятливим до візуальних імітацій, які схожі на веб-сайти. Менеджер паролів, може згенерувати вам безліч різних паролів для кожного сайту, який ви використовуєте. З цією вбудованою перевагою використання менеджера паролів є вигідним.

Менеджери паролів, які досліджені в нашій роботі:

- Password Manager Deluxe
- Kaspersky Password Manager
- Sticky Password
- KeePass
- RoboForm
- Dashlane
- Last Pass

Як відомо, менеджери паролів не зберігають майстер-пароль де-небудь на комп'ютері, і кожен раз при використанні менеджера користувач повинен вводити його вручну. Для перехоплення таких паролів, як правило, використовують кейлогери плюс запис руху курсора і знімки екрану, якщо мала місце віртуальна клавіатура.

Однак у нашому випадку ми не будемо писати складні тіньові драйвери для перехоплення натискань клавіш і знімків екранів, оскільки вони можуть поставити нашу атаку в лабораторні умови і легко визначаються антивірусами.

Ми розглянемо цікавий, але не новий спосіб отримання пароля прямо з вікна введення через виклик API SendMessage. Цей спосіб чудовий тим, що багато антивірусів не розпізнали його як потенційно небезпечну дію, а реалізується він буквально парами рядків коду, плюс для його запуску не потрібна наявність прав адміністратора.

Після запуску дана програма, використовуючи таймер, буде відстежувати положення курсора на екрані і визначати текст під ним, тобто досить навести на необхідне поле курсор, щоб миттєво дізнатися пароль.

DLL Hijacking є досить новою технікою атаки, суть даного методу полягає в підміні dll бібліотек, які використовуються тим чи іншим додатком.

Ця вразливість може бути проексплуатована, коли вразливий додаток відкриває файл з директорії контрольованої зловмисником.

Такою директорією може бути USB диск, розпакований архів або мережеві папки із загальним доступом. Все що потрібно від користувача - зайти в контрольовану директорію і відкрити файл вразливим додатком. Файл, який відкривається користувачем, може бути абсолютно нешкідливий, але процес відкриває файл, якщо він вразливий, завантажує DLL з робочої директорії (директорії з файлом).

Висновки:

Після проведення атак усім менеджерам були поставлені оцінки за трьох бальною шкалою. Також в роботі оцінювались такі критерії, як: інтерфейс (його зрозумілість та зручність) і вартість програми.

За усіма цими критеріями, найкращим менеджером паролів є Sticky Password. Він показав найкращі результати за параметрами захищеності як мастер-пароля, так і баз даних. Також він є єдиним менеджером паролів, який помітив підміну динамічної бібліотеки і закрив програму, не даючи зловмиснику отримати доступ.

Перелік посилань:

1. 1. Яремчук С. Менеджеры паролей - Мой Компьютер. - 08.01.2007 - №03 (434).
2. Parker, Jason (11 April 2014). "Take control of password chaos with these six password managers".
3. https://xakep.ru/2014/09/08/password-manager-pentest/ Ищем слабые места современных менеджеров паролей Александр Ващило.
4. http://www.computerra.ru/reviews/419570/ Крупин А. Менеджеры паролей для мобильников – Компьютерра – Онлайн. – 16 апреля 2009.

ДОСЛІДЖЕННЯ ТА ПОРІВНЯННЯ ХМАРНИХ СХОВИЩ ДАНИХ

Угрік В. А., студентка 3-го курсу, група О-31, спеціальність «Монтаж, обслуговування та ремонт апаратури зв'язку і оргтехніки»

Науковий керівник: викладач Малюта С. О.

Анотація. *Розглядаються, досліджуються та порівнюються хмарні сховища даних.*

Головна мета дослідницької роботи – розглянути та порівняти хмарні сховища даних за різними параметрами, визначити переваги та недоліки кожного хмарного сховища та обрати серед них найкраще.

Хмарне сховище даних (або як його ще називають «хмара») - це одна з моделей віртуального сховища, в якому дані користувачів зберігаються і обробляються на серверах, розподілених по всій мережі. Сервери можуть розташовуватися, в географічному відношенні, на великих відстанях один від одного (до розташування на різних континентах).

Основним призначенням будь-якого хмарного сховища є надання послуг клієнтам по зберіганню та обробці різних даних. Такі сервіси допомагають користувачам комп'ютерів звільнитися від використання зовнішніх носіїв. Відпадає потреба носити з собою флешки (які дуже часто губляться або виходять з ладу, в самий невідповідний момент), зовнішні жорсткі диски та інші подібні сховища інформації. Наприклад, виконуючи певну роботу на комп'ютері, Ви не встигли вчасно закінчити її на робочому місці і прийняли рішення продовжити виконання завдання на дому. Але для цього необхідно, щоб вся інформація і дані, необхідні для виконання завдання, були під рукою. Цю проблему буде набагато простіше вирішити, якщо всі роботи Ви виконували, використовуючи можливості і ресурси хмарних сервісів. Адже доступ до них можна здійснювати з будь-якого комп'ютера, який має доступ до Інтернету.

Основні переваги використання даних сервісів:

- сховище даних, повний доступ до цих даних з будь-якого комп'ютера, підключеного до мережі;
- виконання всіх обчислень і обробка даних не залежить від потужності Вашого комп'ютера, вільного дискового простору, всі роботи проводяться з використанням ресурсів хмарного сервісу, віддалено, а при необхідності можна вивести тільки результат;
- надання безкоштовних та платних послуг, вартість яких досить доступна і є тенденція на постійне їхнє зниження.

Розглядаються 5 хмарних сховищ даних: Dropbox, Google Диск (Google Drive), Яндекс.Диск, Облако Mail.Ru, Microsoft OneDrive (скорочено OneDrive).

Для початку роботи з будь-яким хмарним сховищем необхідно встановити на всі комп'ютери або мобільні пристрої спеціальну програму-клієнт хмарного сховища і вказати папки жорсткого диска комп'ютера, які треба помістити у "хмару". Ця програма скопіює зазначені папки та файли в хмарне сховище і буде стежити на тому комп'ютері, де вона запущена, за змінами файлів в цих папках.

Кожне хмарне сховище даних надає користувачеві безкоштовний об'єм пам'яті для використання. Dropbox надає 2 Гб, Google Drive – 15 Гб, Яндекс.Диск – 10 Гб, Облако Mail.Ru – 25 Гб, OneDrive – 15 Гб. Також, кожне хмарне сховище, крім Облако Mail.Ru, надає послуги для розширення безкоштовного об'єму пам'яті. Крім цього користувач може замовити платний тариф послуг.

Хмарні сховища можуть бути сумісні з різними операційними системами: Windows, MacOS, Linux, Android, iOS та Windows Phone.

Для того щоб мати доступ до даних у сховищі через мережу Інтернет, необхідно створити власний акаунт (обліковий запис).

Через акаунт можливо переглядати всі дані, завантажені у папку хмарного сховища. Можливо переглядати графічні, текстові, відео- та аудіофайли, а також файли MS Word, MS Excel та MS PowerPoint, та ін. у різних форматах.

Конфіденційність і захист даних виконуються згідно з політикою конфіденційності, політикою (умовами) використання та угодою користувача.

Висновки:

У роботі розглянуті та досліджені хмарні сховища, їх параметри, функції, переваги та недоліки. На основі порівняння різних параметрів обрано найкраще хмарне сховище даних серед розглянутих. Причини зростаючої популярності хмарних технологій зрозумілі: можливості їх застосування дуже різноманітні і дозволяють економити як на обслуговуванні та персоналі, так і на інфраструктурі. Апаратне забезпечення може бути сильно спрощено при обробці даних та зберіганні інформації у віддалених центрах даних. Всі ці проблеми майже повністю перекладаються на провайдер послуг. Найголовнішим недоліком, який можна відразу помітити, є повна залежність від постачальника цих послуг. Фактично підприємство (користувач) виявляється заручником провайдера сервісів і провайдера доступу в мережу Інтернет. Хоча надійність постачальників хмарних обчислень зростає, для забезпечення надійності та безпеки даних необхідно докласти чимало зусиль, наприклад, мати дублюючі канали зв'язку, що дублюють потужності для можливості перемикання на них і, звичайно ж, подумати про доступність інформації і безпеки.

Перелік посилань:

1. https://ru.wikipedia.org/wiki/ Dropbox.
2. https://www.dropbox.com/ Официальный сайт Dropbox
3. https://ru.wikipedia.org/wiki/ Google Диск.

4. https://support.google.com/ Конфиденциальность и безопасность в Диске Google.
5. http://www.google.com/ Политика конфиденциальности.
6. https://ru.wikipedia.org/wiki/ Яндекс.Диск.
7. http://legal.yandex.ru/ – Яндекс. Правовые документы.
8. https://ru.wikipedia.org/wiki/ Облако Mail.Ru.
9. https://cloud.mail.ru/LA/ Лицензионное соглашение .
10. https://ru.wikipedia.org/wiki/ – Microsoft OneDrive.
11. http://www.microsoft.com/ Microsoft заявление о конфиденциальности.

СТВОРЕННЯ АВТОМАТИЧНОЇ СИСТЕМИ НА БАЗІ АПАРАТНОЇ ПЛАТФОРМИ ARDUINO

Архіпова А.О., студентка 3-го курсу, група С-312/32, спеціальність 5.05090301 «Монтаж, обслуговування і ремонт станційного обладнання електрозв’язку»,

Кічуга М.Б., студентка 3-го курсу, група О-31, спеціальність 5.05090302«Технічне обслуговування і ремонт апаратури зв'язку та оргтехніки».

Науковий керівник: викладач **Бєльдюгіна С. С.**

Анотація. *Розглядається відкрита електронна платформа типу Arduino з метою дослідження та створення на її основі автоматичної системи. Також до основних цілей відноситься дослідження розповсюдження даної платформи та її вплив на сучасний розвиток електроніки.*

У нашій роботі розглядається можливість використання відкритих електронних платформ, на прикладі плати Arduino UNO, для створення різноманітних пристроїв різного спрямування.

На даний момент існує величезна кількість різноманітних відкритих електронних платформ для створення прототипів і не тільки. До цього списку відносяться плати Arduino, RassberiPi, STM32 F3 і т.д. Всі вони використовуються людьми для різних цілей, починаючи від індикаторів світла та закінчуючи малопотужними FM станціями. Це різноманіття викликане великою зручністю даних платформ при роботі та їх використанні. Але так було не завжди, до 2004 року на ринку електронних конструкторів спостерігалась монополія «LEGO mindstorms», який коштував досить дорого, був досить вузько спрямованим та мав закриту будову. Тому він досить сильно обмежував роботу з ним, але коли почали з’являтись перші відкриті платформи (у тому числі й Arduino UNO), обмеження почали зникати, почали з’являтися нові ідеї, проекти і навчальні програми.

У ході даної роботи були проведені як теоретичні, так і практичні дослідження. До теоретичних досліджень належать: дослідження конструкції, розповсюдження та впливу платформи Arduino. У свою чергу до практичних належать: здобуття практичних навичок у роботі з Arduino, при створенні 2-х-сторонніх плат, та проектування автоматичних систем, на прикладі вимірювача вологості та температури; сигналізації на приближення. Все це дозволило краще ознайомитися з самою платформою та сучасним робоконструюванням. Також ми працювали з такими програмами як: sprint layout, multisim, Arduino Software, crocodile technology, miniBlog та processing.

Висновки:

З проведеної роботи ми можемо зробити наступні висновки:

1. Платформа Arduino є досить зручною при роботі та експлуатації.
2. Вона ідеально підходить для початку вивчення мікропроцесорної електроніки та програмування мікроконтролерів.
3. На її основі можна легко створювати прості та середні за складністю проекти, декілька з яких представлені у нашій роботі.
4. У зв'язку з тим, що Arduino містить внутрішній АЦП, її можна використовувати як основу при вивченні предмету ОЦОС.

Вплив Arduino на навколишній світ, на перший погляд, здається непомітним, але все ж вона зробила значний внесок у розвиток суспільства та електроніки. Це пов'язано з тим, що ця платформа дала багатьом людям можливість реалізації нових проектів, а це є основним чинником для розвитку сучасної електроніки.

Перелік посилань:

1. https://ru.wikipedia.org/wiki/Arduino/ страница на сайте «Википедия» про Arduino.

2. http://arduino.ru/Hardware/ArduinoBoardUno/официальное техническое описание платы Arduino Uno.

3. http://arduino.ru/Reference/официальное описание языка программирования Arduino.

4. Улли Соммер «Программирование микроконтроллерных плат Arduino/Freeduino». – СПб.: БХВ-Петербург, 2012. – 256 с..

5. https://day.arduino.cc/#/ офіційний сайт «Arduino Day 2015».

6. http://skbrii.ru/офіційний сайт СКБ «Робототехника и искусственный интеллект».

7. ДСТУ 3334-96 Плати друковані. Загальні вимоги до технологічних процесів регенерації, знешкодження та утилізації розчинів.

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

Здано в набір 25.03.2015 р. Підписано до друку 25.03.2015 р.
Тираж 20 прим. обсяг 1,32 друк. арк.
Віддруковано в коледжі зв'язку та інформатизації ОНАЗ ім. О.С. Попова
© КЗІ ОНАЗ, 2015.