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

Восьма студентська науково-технічна конференція

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

14 квітня 2018 року

Збірка тез

Одеса, 2018

Телекомунікаційні, інформаційні та комп'ютерні мережі та системи: теперішнє та майбутнє: матеріали восьмої студентської науково-технічної конференції, м. Одеса, 14 квітня 2018 року – Одеса, КЗІ ОНАЗ, 2018 – 30 с.

Дана збірка містить тези матеріалів, що представлені на восьмій студентській науково-технічній конференції «**Телекомунікаційні, інформаційні та комп'ютерні мережі та системи: теперішнє та майбутнє»**, що проводиться 14.04.2018 р. в коледжі зв'язку та інформатизації Одеської національної академії зв'язку ім. О.С. Попова.

До збірки включені тези доповідей за секціями:

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

Робоча мова конференції – українська.

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. – викладач

ЧЛЕНИ ОРГКОМІТЕТУ:

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

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

Осадчук Т. В. – методист

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

Бєльдюгіна С. С. – викладач циклової комісії телекомунікацій та радіотехніки

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

Тарашкевич В. – голова ради студентського самоврядування, студентка групи Р-31

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 автоматизації, телекомунікацій та радіотехніки

Баляр В. Б. – к.т.н., ст. викладач кафедри ТБ та РМ ОНАЗ ім. О. С. Попова

Маковеєнко Д.О. – к.т.н., доцент, доцент кафедри ТБ та РМ ОНАЗ ім. О. С. Попова

секція інформаційних технологій

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

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

секція комп'ютерних технологій та захисту інформації

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

Кільдишев В. Й. – к.т.н., доцент, доцент кафедри ІБ та ПД ОНАЗ ім. О. С. Попова

ЗМІСТ

Секція автоматизації, телекомунікацій та радіотехніки

1. Дутка П. І. Інтернетізація телевізійного мовлення 6

2. Медведенко В. В. Аналіз можливостей використання технології SDR у навчальному процесі 8

3. Васильєв П. С. Організація телефонних розмов з використанням GSM-мосту 10

4. Нечитайло В. Д., Тростянецький Д. К. Автоматизація процесів за допомогою комп'ютерного програмування 12

Секція інформаційних технологій

1. Гончар К В., Бочаров Д. В. Аналіз можливостей використання технологій доповненої реальності в навчальному процесі 15

2. Максимишин О. І., Олійник В. С Системи автоматизованого оцінювання компетенцій студентів в поточному навчанні 18

3. Соколовський А. С. Розробка Android-додатку 20

Секція комп'ютерних технологій та захисту інформації

1. Куляк А. А. Створення алгоритму емпіричного визначення доцільності генерації даних у блокчейн-просторі 23

2. Шалюк Д. А. Методи оптимізації для захисту табличних даних 25

3. Бєлоциця Ю. О. Аналіз безпеки Telegram IM 27

СЕКЦІЯ АВТОМАТИЗАЦІЇ, ТЕЛЕКОМУНІКАЦІЙ ТА РАДІОТЕХНІКИ

ІНТЕРНЕТИЗАЦІЯ ТЕЛЕВІЗІЙНОГО МОВЛЕННЯ

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

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

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

Анотація. *Розглянуті взаємовплив телебачення та Інтернету; два основні підходи до телемовлення в мережі інтернет - Internet-TV і IPTV. Наведено порівняльні діаграми використання Інтернет мережі у телевізійному мовленні.*

Головна мета – розглянути актуальні проблеми інтернетизації сучасного цифрового телебачення.

Протягом всієї історії існування телебачення в ньому використовувалися останні технічні досягнення: спочатку радіотехніка, потім електроніка і, нарешті, інформаційні та комунікаційні технології. Нові телекомунікаційні технології дозволили поширювати інформацію, порушуючи всі традиційні уявлення про час, географії, формі.

Інтернет має «телевізійну» основу, оскільки оперує відео і звуком - основними образотворчими засобами телебачення. Інтенсивно відбувається і зворотний процес - телебачення активно виходить в Мережу, і його традиційні взаємини з аудиторією змінюються під впливом нових технологій, які більш функціональні. Саме в нинішній період інтернетизації всіх телевізійних процесів створюються особливі умови взаємопроникнення телебачення і інтернет-технологій з багатьох напрямків - як в сфері створення телевізійного контенту, так і по доставці його аудиторії.

Головні переваги, які нам дають цифрові технології - відмінне зображення та звук, втім у динамічному суспільстві соціум прагне одержувати не тільки якісну, але й оперативну та об'єктивну інформацію. В епоху високих технологій людина з пасивного споживача інформації перетворилися на активного учасника комунікації. У суспільстві, що використовує інтернет-технології, кожна людина отримала можливість доступу практично до будь-якого джерела інформації.

Розвиток інтерактивності на телебаченні йде паралельно з розвитком цифрового мовлення, тобто традиційного мовлення, але з використанням нових

способів передачі цифрового сигналу. Розвиток технологічних новацій йде паралельно в двох сферах - off-line і on-line. Off-line - має на увазі традиційну середу, в якій існує і розвивається традиційне телебачення. On-line - це середовище, яке представлена віртуальним простором електронних мереж, зокрема, мережі Інтернет. Майже всі українські телеканали транслюються в режимі on-line: як загальнонаціональні, так і регіональні.

З точки зору споживання контенту, посилюється роль нелінійного відео. Також зростає кількість терміналів, на яких можна дивитися відео, в тому числі і телевізійні програми (ТВ, комп'ютери, ноутбуки, планшети, смартфони). Також відбувається поділ джерел контенту на три потоки: контент, що надходить до користувача за допомогою мовлення, контент в мережі Інтернет і власний користувальницький контент. Розширився спектр пристроїв - носіїв контенту. Якщо раніше основним джерелом користувацького контенту залишався комп'ютер або ноутбук, то в наші дні велику пам'ять мають смартфони, планшети, а також знімні карти пам'яті. Головна особливість телевізорів майбутнього - інтеграція телевізійних та інтернет-принципів.

Можна виділити два основних підходи до телемовлення в мережі інтернет: Internet-TV і IPTV. Інтернет-мовлення включає в себе передачу по мережі Інтернет відео- і аудіоінформації. Інформацію можна передавати в Мережу в прямому ефірі - це "живе мовлення", і в запису - це "відео-на-замовлення". Більшість інтернет-каналів використовують поєднання живого мовлення і відео за запитом, тобто змішане мовлення.

IP-телебачення - це цифрове телебачення нового покоління, яке передається за допомогою Інтернет мережі та надає можливість переглядати телевізійні програми, як на екрані комп'ютера, планшета, смартфону, так і на екрані телевізору. Ключовий зв'язок між глобальною мережею і IPTV полягає в тому, що користувач в будь-якому випадку звертається до провайдерів.

В інтерактивному телебачення існує чотири основних напрямки, що відрізняються як функціональністю, так і змістом: розширене, персональне, інтерактивне, "інтелектуальний дім".

Середовища й засоби передачі і прийому інформаційних та інтерактивних даних - це наземне і супутникове ТВ мовлення, мобільне і кабельне ТБ, хмарні технології та інші. Кожен з перерахованих способів має переваги і обмеження.

Висновки

Поява комп'ютерної техніки та мережі Інтернет дозволило надати абоненту нову властивість при перегляді – інтерактивність, тобто взаємодію з програмним забезпеченням з метою отримання або передачі додаткової інформації. Відповідно,

телебаченню довелося відповідати цьому новому «досвіду», а саме, стати інтерактивним. Розвиток інтерактивності на телебаченні йде паралельно з розвитком цифрового мовлення, тобто традиційного мовлення, але з використанням нових способів передачі цифрового сигналу. Таким чином, на зміну багаторічному пасивному прийому пакетів ТВ програм у глядачів з'являються можливості активної участі в цьому процесі.

Перелік посилань:

1. https://medianany.com/blog_oresta_biloskurskogo/2316310/ . «Есть ли будущее у IPTV в Украине».

2. http://irvispress.ru/catalog/tv/sovremennye-tehnologii-tv/televidenie-i-internet/» IPTV и Интернет ТВ, в чем разница?»

3. https://biz.nv.ua/ukr/experts/gumenjuk/telebachennja-majbutnogo-jak-industrija-migruje-vinternet-316958.html «ТВ майбутнього: як індустрія мігрує в інтернет»

4. http://mediasat.info/2016/12/02/ericsson-consumerlab/ « Интернет vs телевидение»

5.http://www.sib.com.ua/arhiv_2010/2010 IPTV в Украине – проблемі и их решение

6.https://niir.ru/news/publikacii/2436-2/razdel-7-interaktivnoe-tv-veshhanie/ «Интерактивное телевизионное вещание»

7. http://bourabai.kz/dbt/itv3.htm «Развитие Интернет-телевидения».

АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SDR У НАВЧАЛЬНОМУ ПРОЦЕСІ

Медведенко В.В. ., студент 3-го курсу, група Р-31, спеціальність 5.05090306 «Монтаж, технічне обслуговування і ремонт обладнання радіозв'язку, радіомовлення та телебачення».

Науковий керівник – викладач Сідень С.В.

викладач каф. ТЕД та СРЗ ОНАЗ ім. О. С. Попова

Анотація. *Мета роботи- показати можливості використання технології SDR навчальному процесі.*

Відомо, що основною проблеми бездротових систем є обмеженість радіочастотного ресурсу. З появою нових технологій передавання даних та кількості бездротових пристроїв ця проблема стає більш складною.

Розвиток систем бездротового зв'язку призводить до освоєння нових частотних діапазонів і, можливо, до розподілу смуги пропускання кількома радіосистемами. Це призводить до збільшення кількості завад і до погіршення електромагнітного середовища.

Для нормального функціонування бездротових систем та пристроїв необхідно забезпечувати умови електромагнітної сумісності радіоелектронних засобів. У ряді випадків, коли радіоелектронні засоби випромінюють сигнали за межами своєї смуги радіочастот погіршується електромагнітна обстановка та ефективність всієї системи. Тому для забезпечення електромагнітної сумісності, а, як наслідок, ефективної роботи бездротових систем, необхідно мати обладнання для швидкого моніторингу електромагнітних випромінювань.

Звичайно, для аналізу електромагнітної обстановки використовують дорого вартісне обладнання. Однією з перспективних технологій для первісного/попереднього аналізу електромагнітних випромінювань радіоелектронних засобів є технологія SDR (Software Defined Radio) [1].

SDR – це приймально або приймально-передавальних пристрій, що базується на використанні спеціального програмного забезпечення, за допомогою якого можна приймати, записувати, оброблювати та відтворювати сигнали радіочастотного діапазону.

Принцип роботи SDR базується на оцифрувані прийнятого сигналу і його подальшій обробці у цифровій формі. На рис. 1 проілюстрована структурна схема SDR [1].

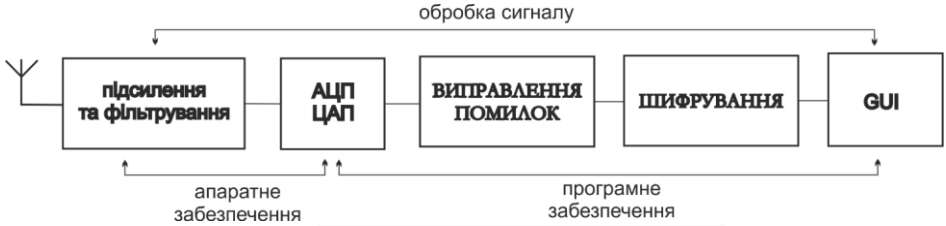

Рисунок 1 – Структурна схема SDR

Основними перевагами технології SDR є:

- простота та зручність у використанні;
- мінімальна ціна;
- компактність.

Треба відзначити, що за допомогою даної технології можна проводити моніторинг радіочастотного ресурсу онлайн, та вимірювати основні параметри спектрів бездротового обладнання, а саме ширину спектру, його амплітуду та інші.

Крім того, за допомогою SDR можна аналізувати рівні позасмугового випромінювання радіоелектронних засобів та перевіряти дозволені рівні та смуги випромінювання.

Висновок. Виходячи з наведених переваг, треба відзначити, що дана технологія може бути використана у навчальному процесі, для підготовки спеціалістів зі спеціальності «Телекомунікації та радіотехніка» при вивченні дисциплін «Електромагнітна сумісність радіоелектронних засобів», «Радіочастотний моніторинг» та ін.

Перелік посилань:

1. Конспект ЭМС ч.1 (Електронний ресурс)-Режим доступу до ресурсу: http://www/studfiles.ru/preview/5170771/.

2. Ильюшко С. Г. Анализ и методика расчета електромагнитной совместимости и систем связи, радиолокации и телевидения/ С. Г. Ильюшко. – Петропавловск-Камчатський: КамчатсГТУ,2007 -106 с.

3. Ефимов В. И. Электромагнитная совсестимомтьрадиоэлетронных средств и систем/ В. И.Ефимов В. И. , А. А. Тихомиров – Томск, 2012. -229 с.

ОРГАНІЗАЦІЯ ТЕЛЕФОННИХ РОЗМОВ З ВИКОРИСТАННЯМ GSM-МОСТУ

Васильєв П.С., студент 3-го курсу, групи О-31, спеціальності 5.05090302 «Монтаж, ремонт та обслуговування апаратури зв'язку та оргтехніки »

Науковий керівник: - К.Ф.Н., викладач **Кокорєв О.В.,**

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

Анотація. *Розглядається організація телефонних розмов за допомогою GSM- мосту та створення програми обмеження часу розмов при використанні GSM-мосту.*

В даній роботі виконується розробка програмного забезпечення для GSM обладнання ECCOM BASIS. Розроблене програмне забезпечення є білінговою системою для найдрібніших операторів зв'язку.

В теперішній час проблема коли дуже помітні тенденції зменшити роботу людини або перекласти її на ЕОМ. Тому навіть найменші операції такі як обробка телефонного виклику та розмови повинен виконувати комп'ютер. Сучасний ринок програмного забезпечення може запропонувати безліч продуктів для обслуговування Міні-АТС, GSM обладнання та інші можливі телекомутаційні пристрої. Але в загальному огляді практично не має таких білінгових систем, які мали б можливість точно відповідати потребам дрібних операторів зв'язку. Тобто прості в використані,

головною якістю яких була б мобільність та гнучкість. Котрі б не потребували постійного нагляду з боку адміністратора мережі.

Варіант вирішення цієї проблеми можна побачити в даній роботі. Де для мобільності та гнучкості використання була розроблена програма дистанційного керування всією системою котра відповідає за можливість як виконувати прийняті команди з віддаленого терміналу, так і предоставляти деяку зворотню інформацію, яка б була корисна для адміністратора.

Крім того, розроблене програмне забезпечення вирішує проблему зв'язану з тим, що в теперішній час розповсюджено дуже багато різноманітних операційних систем, що може зменшити мобільність білінгової системи. Вирішена ця проблема була за допомогою бази даних MySQL, через яку фактично і здійснюється передача інформації між адміністратором (користувачем) та віддаленим GSM обладнанням.

Висновки:

В результаті виконаної роботи був розроблений програмний продукт, який має задовольнити потреби дрібних операторів зв'язку, котрим необхідно знати активність своїх абонентів, стежити за роботою всієї система, але водночас не обов'язкова присутність адміністратора зв'язку в системному приміщені.

Структура та реалізація розробленого програмного забезпечення дозволяє:

- підвищити якість обслуговування абонентів, за рахунок зменшення витрат часу на збирання статистичних даних;
- розміщувати апаратну та програмну частину обладнання в будь-якому місті зручному для розміщування, а не для людини, присутність якої необов'язкове;
- передавати статистичні дані на будь-який комп'ютер далі, та на будь-яку операційну систему через доступ к базі даних MySQL.

Таким чином, запровадження розробленого програмного забезпечення є раціональним рішення для дрібних операторів зв'язку та підприємств, які мають власне GSM обладнання для власного використання.

Перелік посилань:

1. ECCOM BASIS.Сайт підтримки обладнання ECCOM BASIS. // web: http://www.gsm-ec.com
2. MSDN. Сайт підтримки розробки програмного забезпечення ОС Windows. // web: http://msdn.microsoft.com
3. MySQL. Офіціальний сайт підтримки розробки баз на основі MySQL. – // web: http://dev.mysql.com

4. Стеклов В.К., Беркман Л.Н. Телекомунікаційні мережі. К.:Техніка, 2001. - 392с

5. Орлов.С. IP PBX принимает вызов/LAN, 2003, №4.

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ ЗАСОБАМИ КОМП'ЮТЕРНОГО ПРОГРАМУВАННЯ

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

Тростянецький Д. К. студент 3-го курсу, група О-31, спеціальність 5.05090302 «Технічне обслуговування і ремонт апаратури зв'язку та оргтехніки».

Науковий керівник – викладач **Бєльдюгіна С. С.**

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

Анотація. *Головна мета дослідної роботи – розглянути недоліки smart технологій, показати рівень розвитку в цілому та продемонструвати їх можливості у повсякденному житті людини*

У сучасному світі люди шукають спрощення та поліпшення свого життя. Людині постійно потрібно вирішувати багато питань і робити чимало справ у побуті і повсякденні. Але чимало з них навіть замислюються і помічають, як самі кожен день активно користуються різними гаджетами котрі спрощують їх життя. Саме тому, багато технологій у сфері автоматизації постійно допомагають їй.

Домашня автоматизація в сучасних умовах - надзвичайно гнучка система, яку користувач конструює і налаштовує самостійно в залежності від власних потреб. Це передбачає, що кожен власник розумного будинку самостійно визначає, які пристрої і де встановити і які завдання і як вони будуть виконувати.

Головні переваги "Smart" технологій - дуже висока безпека, економічність у споживані енергії та екологічність, забезпечення комфортного існування, автономність, а також важливий фактор - мультизадачність. Усе це покликано створити привабливі для користувача умови споживання, а також вирішити його дрібні побутові проблеми.

Хоча технології розвиваються вже понад двадцяти років, вони все одно рухаються вперед і мають доволі перспективне майбутнє. З кожним роком нові розробки надають нам все більше можливостей в роботі, житті, дослідженнях, тощо. На нашу власну думку, все через те, що це приносить неабияку користь людині. Дає змогу робити декілька справ одночасно без особливої участі в них. Завдяки цьому

зберігається багато часу, який на даний момент є дуже цінним. Саме ця ідея прислідується людством та розробниками цього напряму - не залишати багато часу на речах де не потрібно багато уваги.

З точки зору використання, весь процес базується на трьох основних пристроях: *Контроллер (хаб)* - керуючий пристрій, що з'єднує всі елементи системи один з одним і зв'язує її з зовнішнім світом. *Датчики (сенсори)* - пристрої, які отримують інформацію про зовнішні умови. *Актуатор* - виконавчі пристрої, безпосередньо виконують команди. Це найчисленніша група, в яку входять розумні (автоматичні) вимикачі, розумні (автоматичні) розетки, розумні (автоматичні) клапани для труб, сирени, клімат-контролери і так далі, де контроллер є важливим пристроєм, який спілкується з іншими елементами.

У результаті проведення наукової роботи розробили наглядний приклад автоматизації процесів за допомогою програмування і тим самим показали більш сучасний підхід. А також на основі вивчених матеріалів зробили висновки щодо цієї технології. По-перше, знайшли плюси та недоліки смарт розробок. По-друге, оцінили перспективи і розвиток у цій галузі, які демонструють усім знайомі компанії Google, Apple, Xiaomi в продовж 5-10 років.

Висновки

У результаті проведення наукової роботи нами був розроблений наглядний приклад автоматизації процесів за допомогою програмування. Тим самим показано більш сучасний підхід. На основі вивчених матеріалів зробили висновки:

Поява smart технологій у світі надало людям багато можливостей, які спростили їх життя. Крім того ця технологія є більш екологічно-безпечною та не має шкідливого впливу на людський організм, забезпечує комфортне існування, автономність, а також має важливий фактор – мультизадачність.

Перелік посилань:

1.Усе що необхідно знати про технології розумного будинку - https://ru.wikipedia.org/wiki/Умный_дом

2. Історія - https://ru.wikipedia.org/wiki/Домашняя_автоматизация#История

3. Винаходи: http://fishki.net/1819149-top-10-velikih-izobretenij-srednevekovja.html

4. Згадки письменників: http://interesno.cc/article/7491/25-knig-kotorye-predskazali-budushhee

5. Google Assistant : https://ru.wikipedia.org/wiki/Google_Assistant

6. Apple home pod - https://ru.wikipedia.org/wiki/Apple_HomePod

7. Xiaomi smart home- http://wifika.ru/sistema-umnyiy-dom-xiaomi-smart-home.html

8. Sleepsensor by HOLI - https://smart-home.market/holi-sleepsensor-naskolko-horosho-my-na-samom-dele-spim-s3142

9. Інші цікаві винаходи https://www.crn.ru/news/detail.php?ID=116717

10. Назад в Будущее https://lifehacker.ru/2016/09/16/dom-budushhego/

11. Розумний помічник із майбутнього http://www.lookatme.ru/mag/live/future-research/194385-smart-home

СЕКЦІЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ДОПОВНЕНОЇ РЕАЛЬНОСТІ В НАВЧАЛЬНОМУ ПРОЦЕСІ

Гончар К.В., Бочаров Д.В. студенти 3-го курсу, групи К-31, спеціальність «Обслуговування програмних систем і комплексів»

Науковий керівник – к.т.н., доц., **Вороной С.М.** кафедра комп'ютерних наук ОНАЗ ім. О. С. Попова

Анотація. *Розглянуто актуальність використання технологій доповненої реальності в навчальному процесі. Проведено аналіз сучасних засобів розробки додатків доповненої реальності, детально розглянуто процес розробки на базі платформи Unity за допомогою бібліотеки ARToolKit.*

Використання інформаційного середовища в навчальних цілях сьогодні є найбільш перспективним напрямом в системі вищої освіти. Створення сучасного освітнього інформаційного середовища неможливе без комп'ютеризації навчального процесу. Застосування комп'ютерної техніки сприяє активізації пізнавальної діяльності студентів, що і підвищує ефективність лекційних, семінарських, практичних і лабораторних занять. Сьогодні значна увага приділяється таким методикам навчання, які здійснюються із застосуванням навчальних комп'ютерних програм, що реалізують діяльнісний підхід до навчання. До таких методів можна віднести методи інтерактивного навчання, суттєвою відмінністю яких є оперативна зміна темпу подання навчального матеріалу, форми подання, модифікації його змісту тощо, в залежності від результатів. Одним з найсучасніших підходів є використання технологій доповненої реальності в задачі інформатизації навчального процесу. В навчальному процесі існує велика потреба візуалізації (моделювання) різних процесів і предметів, які неможливо відтворити і показати в навчальній аудиторії або лабораторії. Саме додатки доповненої реальності дають можливість візуалізації процесів і предметів, які необхідно, але неможливо продемонструвати в навчальній аудиторії.

Технологія доповненої реальності (AR - Augmented reality) дозволяє істотно розширити область даних, що сприймаються людиною за рахунок об'єднання сприйняття реального світу з цифровим контентом. Ця технологія формувалася ще в 60-х роках як частина віртуальної реальності (virtual reality). Однак термін «доповнена реальність» бу запропонований тільки на початку 90-х дослідником корпорації Боїнг Томом Кандела. У 1994 році Пол Мілгром запропонував таксономію «віртуальність - реальність», яку він назвав континуумом змішаної реальності. З

одного боку, континуум містить реальне навколишнє середовище - реальність, а з іншого боку – віртуальну реальність. Особливості віртуального навколишнього середовища - віртуальність. Все між ними змішана реальність. Змішана реальність – це система, що з'єднує реальний світ з віртуальним світом з подальшим створенням нового навколишнього середовища, де фізичні та цифрові об'єкти взаємодіють і співіснують [1].

В основі будь-якої програми доповненої реальності, що використовує аналіз зображення, яке надходить з камери, лежить система комп'ютерного зору. Однією з найбільш відомих бібліотек, що реалізують подібний функціонал, є OpenCV. Вона надає достатню кількість низькорівневих можливостей і дуже хороша для вилучення максимуму інформації з зображення. Але для додатків доповненої реальності потрібно швидко і якісно знайти в кадрі обмежений набір заздалегідь відомих об'єктів і відобразити над зображенням віртуальний об'єкт [2].

Для розробки систем доповненої реальності необхідна програмна бібліотека, яка здатна розпізнавати 2D маркери і накладати поверх реального зображення додатковий контент. Також важливим пунктом є підтримка широкого спектру пристроїв, що допоможе забезпечити більшу доступність додатка. Всім цим умовам задовольняє бібліотека доповненої реальності ARToolKit [3]. Значна перевага бібліотеки - відкритий код. Бібліотека ARToolKit дозволяє розробити додаток доповненої реальності для найпопулярніших платформ: Android, iOS, Windows, Linux. Зазвичай для розробки програми під кожну операційну систему необхідне своє середовище розробки, але ARToolKit підтримує найпопулярнішу в світі платформу розробки для створення кросплатформених ігр та інтерактивного контенту - Unity [4].

ARToolKit надає можливості віртуальним тривимірним об'єктам бути накладеними на відеопотік в реальному часі. Даний пакет заснований на використанні чорно-білих маркерів і працює наступним чином (рис.1.):

1. Камера захоплює відеопотік зображень реального часу і відправляє їх пристрою обробки.

2. Програмне забезпечення пристрою виконує пошук будь-яких маркерів на кожному кадрі.

3. Якщо маркер був знайдений, модуль використовує математичний апарат для обчислення позиції камери щодо даного маркера.

4. Як тільки позиція камери визначена - графічна модель відображається безпосередньо в такій позиції.

5. Дана модель відображається поверх відеоряду і закріплюється за маркером.

6. Фінальне зображення подається на дисплей пристрою.

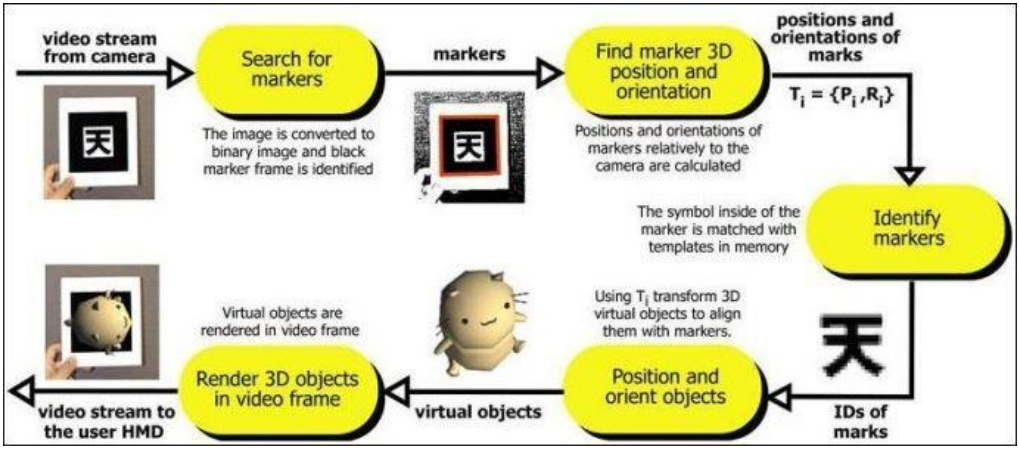

Рисунок 1 – Загальні принципи роботи ARToolKit

Висновок. Роль сучасних інформаційних і комунікаційних технологій в удосконаленні та модернізації поточної системи освіти залишається важливою протягом багатьох років. А з впровадженням у навчальний процес недорогих і доступних комп'ютерів та іншої обчислювальної техніки, які об'єднуються в мережі або мають доступ до Інтернету, збільшується доступність використання інформаційних технологій в освіті. У представленій роботі проведено аналіз можливостей використання технологій доповненої реальності в навчальному процесі та розглянуто питання створення додатка доповненої реальності за допомогою бібліотеки ARToolKit.

Перелік посилань:

1. Kipper G. Augmented Reality: An Emerging Technologies Guide to AR // Syngress – 2012. – pp. 208

2. OpenCV [Электронный ресурс]. – Режим доступа: http://www.softintegration.com/products/thirdparty/opencv/

3. How does ARToolKit work? [Электронный ресурс]. – Режим доступа: www.hitl.washington.edu – англ.

4. The Absolute Beginner's Guide to Unity - How to help yourself, and get help when you can't. [Электронный ресурс]. – Режим доступа: http://wiki.unity3d.com/index.php/The_Absolute_Beginner%27s_Guide_to_Unity

СИСТЕМИ АВТОМАТИЗОВАНОГО ОЦІНЮВАННЯ КОМПЕТЕНЦІЙ СТУДЕНТІВ В ПОТОЧНОМУ НАВЧАННІ

Максимишин О.І., Олійник В.С. студент 3-го курсу, групи 3-31, спеціальність 5.05010301 «Розробка програмного забезпечення»

Науковий керівник – к.т.н., доц., **Єгошина Г.А.**

Кафедра інформаційних технологій ОНАЗ ім. О. С. Попова

Анотація. *Розглянуто актуальність розробки системи автоматизованого оцінювання компетенції студентів в поточному навчанні. Представлено концепцію системи та її реалізацію на Visual C++. Система призначена для створення тестових завдань, автоматичного оцінювання результатів тестування та моніторингу успіхів студентів в поточному навчанні.*

Сьогодні компетентнісний підхід у вітчизняній освіті знаходиться в стадії становлення, ступивши до нас з практики західно-європейського педагогічного досвіду. Поява концепції компетентнісного підходу зумовлено входженням України в європейський освітній простір та у зв'язку з недостатністю знаннєвого підходу в організації сучасного освітнього процесу.

Компетентнісний підхід – це постійна переорієнтація домінуючою освітньої парадигми з переважною трансляцією знань, формуванням навичок на створення умов для оволодіння комплексом компетенцій, що означають потенціал здатності випускника до виживання і стійкої життєдіяльності в умовах багатофакторного, соціально-політичного, ринково-економічного, інформаційного та комунікативно-насиченого простору [1].

На відміну від знаннєвого предметного досвіду компетентність не передається. Кожен суб'єкт повинен створити свою компетентність для себе, заново, як продукт індивідуальної творчості і саморозвитку. Таким чином, розробка системи автоматизованого оцінювання компетенцій студентів в поточному навчанні є актуальною задачею і має практичне значення [2].

Зміни, що відбуваються в розвитку організацій переконливо доводять, що сучасні фахівці повинні володіти значно більшими можливостями і ресурсами для ефективної діяльності. Безумовно, виробничі завдання не постійно повторюються, але при цьому їх можна узагальнити, систематизувати і, в підсумку, звести до конкретного набору загальних технологій, алгоритмів або стратегій, що ще раз підкреслює доцільність автоматизації процесу оцінювання та аналізу компетенцій випускників.

Головною перевагою подібних систем є можливість одночасного тестування великої кількості студентів з усієї навчальної програми з автоматичною перевіркою

результатів, підвищуються об’єктивність оцінювання та зниження навантаження на викладача.

Але тестові завдання мають ряд недоліків:

- тест не дозволяє перевіряти і оцінювати знання пов'язані з творчістю;
- у тестуванні присутній елемент випадковості;
- для повторного проходження тесту має бути підготовлено інший варіант;
- відсутність єдиного стандарту опису тестів;

Для вирішення першого пункту пропонуємо додати до тестів завдання з розгорнутою відповіддю, що повинно перевірятися викладачем [3]. Звісно це збільшить кількість навантаження на викладача, а з іншої сторони дозволить більш детально оцінити практичні навички студентів.

Важливою особливістю розробленої системи є можливість надання студентам різних варіантів тестових завдань [4], тобто завдання та варіанти відповідей розташовуються у випадкових послідовностей.

Розроблено формат тестів: zip архів з директоріями матеріалів та файлом-маніфестом XML, у якому описано структура тесту та посилання на зовнішні медіа-матеріали.

Система комп’ютерного оцінювання складається з трьох основних компонентів:

1. Система створення та редагування тестів;
2. Система контролю навчання - відповідає за адміністрування користувачів, надає доступ до бази тестів та оброблює результати тестування;
3. Система тестування - надає доступ до бази тестів та передає відповіді до системи контролю навчання.

Розроблений програмний продукт дозволяє користувачеві вирішувати такі завдання:

1. Створення і підтримка бази тестових завдань, з можливістю ефективної навігації і пошуку в цій базі.
2. Розробка на основі бази тестових завдань навчальних тестів, як найпростіших, орієнтованих на завдання поточного, проміжного контролю, так і професійних, що володіють високим рівнем якості та забезпечують уявлення про справжні бали учнів.
3. Проведення тестування, як індивідуального, так і масового, з високим рівнем масштабованості та захисту від фальсифікації результатів тестування.

Висновок. Підвищення якості освіти є однією з актуальних проблем не тільки для України, але і для всього світового співтовариства. Вирішення цієї проблеми

пов'язано з модернізацією змісту освіти, оптимізацією способів і технологій організації освітнього процесу та, звичайно, переосмисленням мети і результату освіти. Запропонована в даній роботі система оцінювання компетенцій студентів в поточному навчанні дозволяє автоматизувати та підвищити ефективність процесів аналізу та формування компетенцій випускника.

Перелік посилань:

1. Ефремова Н. Ф. Компетенции в образовании: формирование и оценивание. М.: Национальное образование, 2012. 416 с.
2. Уиддет С., Холлифорд С. Руководство по компетенциям. М.: HIPPO, 2008. 240 с.
3. Челышкова М.Б. Теория и практика конструирования педагогических тестов: Учебное пособие. – М.: Логос, 2002. – 432 с.: ил.
4. Аванесов В.С. Композиция тестовых заданий. – М.: Центр тестирования, 2002. – 239 с.

РОЗРОБКА ANDROID-ДОДАТКУ

Соколовський А. С., студент 4-го курсу, групи З-41, спеціальність 5.05010301 «Розробка програмного забезпечення»

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

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

Анотація. *Операційна система Android є однією з найбільш популярних платформ для мобільних пристроїв. Одним з її основних переваг є відкритість. Дана операційна система побудована на основі відкритого початкового коду та поширюється на вільній основі. Доступ до початкового коду дозволяє розробникам максимально гнучко використовувати можливості платформи при розробці прикладного програмного забезпечення.*

При розробці додатків Android в більшості випадків використовується мова програмування Java - багатоплатформову мову, що дозволяє розробляти додатки, які не залежать від особливостей апаратного забезпечення різних пристроїв. Для підтримки цієї мови програмування в робочому середовищі повинен бути встановлений фреймворк Java SE Software Development Kit, також необхідна установка фреймворк Android Software Development Kit. Даний інструментальний

набір включає засоби для розробки, тестування і налагодження додатків Android. Android SDK поширюється на вільній основі.

Процес розробки додатків може бути значно прискорений за допомогою інтегрованих середовищ розробки. Однією з найбільш широко використовуваних середовищ є Eclipse. До її переваг можна віднести відкритість, високу гнучкість настройки середовища за рахунок модульності і підтримку найбільш популярних мов програмування і фреймворків. До складу середовища входить редактор коду, зневадник, також надається підтримка систем контролю версій, автоматизованого рефакторінга.

Плагін ADT (Android Development Tools, Інструменти розробки Android-додатків) для Eclipse - це розширення інтегрованого середовища Eclipse, яке надає можливість розробки, виконання, налагодження додатків для Android, доступу до Android SDK, а також підготовки та складання програми для публікації. Плагін ADT також включає в себе візуальний інструмент, застосовуваний для створення графічного інтерфейсу користувача. Щоб спроектувати новий інтерфейс за допомогою цього інтерфейсу, досить скористатися вже готовими компонентами, проте існує можливість додавати.

Розглянемо компоненти Android SDK, до яких можна отримати доступ за допомогою ADT і їх призначення. До складу Android SDK входять:

- Android Virtual Device Manager (AVD Manager).
- Dalvik Debug Monitor Server (DDMS).
- Hierarchy Viewer.
- Android Lint.

Android Virtual Device Manager (AVD Manager) - менеджер віртуальних Android-пристроїв. Даний компонент являє собою повнофункціональний емулятор віртуальних машин Android. Емулятор запускає повний стек системи Android, включаючи ядро Linux. віртуальний пристрій Android повністю моделює всі апаратні і програмні функції реального пристрою. Віртуально можуть відбуватися дзвінки, відправлятися повідомлення, емулюватися дані з різних датчиків (GPS, гіроскоп, датчик освітленості).

Dalvik Debug Monitor Server (DDMS) - сервер налагодження та моніторингу виконання процесів. Даний компонент дозволяє розробникам відстежувати і взаємодіяти з віртуальними машинами і реальними пристроями Android. Доступно перенаправлення портів, захоплення екранного зображення, доступ до стану процесів і потоків, доступ до інформації про використання heap-пам'яті, файловий браузер багато інших функцій.

Hierarchy Viewer - до складу Android SDK входить компонент, що дозволяє налагоджувати і оптимізувати графічний інтерфейс користувача. Візуальні компоненти надаються у вигляді ієрархії, для кожного з них є профілізація, що показує час промальовування компонента.

Android Lint - даний компонент призначений для сканування Android-додатки на наявність помилок і вразливостей. Відслідковуються також невідповідності розташування візуальних компонентів, використання ресурсів.світлодіодної лампочки.

Висновок. Робоче середовище, що складається з Java SE SDK, Android SDK, Eclipse IDE та ADT Eclipse plugin дозволяє ефективно розробляти програми Android, виконувати їх налагодження, тестування, публікацію і підтримку. Всі розглянуті компоненти поширюються на вільній основі та підтримуються різними спільнотами та компаніями, в тому числі й Google.

Перелік посилань:

1. Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability ISO 9241-11:1998
2. Баканов А.С., обозний А.А. Проектування призначеного для користувача інтерфейсу: ергономічний підхід .
3. Android для програмістів: створюємо додатки / П. Дейтел, Х. Дейтел, Е. Дейтел, М. Моргано. - СПб. : Санкт-Петербург, 2013. - 560 с.
4. Android Apps with Eclipse -http://books.google.com.ua/books/about/ Android_Apps_with_Eclipse.
5. Get the Android SDK - developer.android.com/sdk/index.html.
6. Eclipse Luna (4.4) - www.eclipse.org/downloads/.

СЕКЦІЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ ТА ЗАХИСТУ ІНФОРМАЦІЇ

СТВОРЕННЯ АЛГОРИТМУ ЕМПІРИЧНОГО ВИЗНАЧЕННЯ ДОЦІЛЬНОСТІ ГЕНЕРАЦІЇ ДАНИХ У БЛОКЧЕЙН-ПРОСТОРІ

Куляк А. А., студент 4-го курсу групи З-41 спеціальності «Розробка програмного забезпечення».

Науковий керівник – **Шнайдер С.П.,** викладач кафедри мереж зв'язку ОНАЗ ім. О. С. Попова

Анотація. *Дана наукова робота присвячена технологіям та галузям сучасного уявлення людства про фінансовий апарат та захист персональних даних – блокчейн, зокрема – його використання як основу захисту віртуальних грошових одиниць, а також проблематиці підтвердження дійсності даних – «майнінгу».*

Метою даної наукової роботи є створення алгоритму визначення доцільності генерації спеціальних даних - «майнінгу» - у блокчейн-просторі, застосовуючи емпіричний підхід.

Блокчейн, тобто ланцюжок блоків транзакцій — розподілена база даних, яка підтримує перелік записів, так званих блоків, що постійно зростає. База захищена від підробки та переробки. Кожен блок містить часову мітку та посилання на попередній блок хеш дерева. Така розподілена база даних закладена в основу криптовалюти Біткоїн [2] (вона була описана 2008 і реалізована 2009 року), де слугує «бухгалтерською книгою» для всіх операцій. Таку базу називають Блокчейн [1]. Блокчейн необхідний для підтвердження дійсності транзакції у мережі криптовалюти.

Згідно з технічною специфікацією, для підтвердження транзакцій у мережі існують обчислювальні засоби, які за певну винагороду виконують певні обчислення (як правило, обчислення пов'язані з криптографією) та знаходять такий блок, який буде легко перевірити у майбутньому. Для пошуку нових значень блоку використовують хеш-суму попереднього блоку. У більшості криптовалют використовується певна криптографічна функція – знаходження хеш-суми. У різних криптовалютах використовується різні алгоритми обчислення хеш-суми (наприклад, SHA-256, scrypt). Але не достатньо тільки знайти хеш-суму: вона повинна задовільнять певним умовам. Наприклад, у мережі Біткоїн критерієм коректності обчисленої хеш-суми є певне число нулів у початку хеш-суми (ця кількість визначається обчислювальною складністю «майнінгового пула» - сервер, який розподіляє обчислення нового блоку на інші «майнери»). На 2015 рік коректною хеш-сумою вважалась сума із 17 початковими нулями. Такому критерію задовольняє 1

хеш з 1.4×10^{20}. А оскільки для знаходження коректної хеш-суми необхідно враховувати усі дані про транзакції, які відбулися після генерації попереднього блоку, то деяку нефіксовану інформацію необхідно постійно змінювати (визначається технічною специфікацією певної криптовалюти). Таким чином, коректний хеш блоку знаходиться перебором значень, що робить обчислення дуже складною операцією. Якщо коректне значення хеш-суми знайдено, то блок вважається «змайненим» та додається до основного ланцюгу блоків. Така схема має назву «Proof-of-Work» («Доказ роботи»), тобто для знаходження хешу виконується важка робота, але для доказу її виконання достатньо тільки знайти хеш блоку з вже коректними даними, і якщо хеші співпадають, то проведена робота вважається доказаною.

Оскільки для «майнінгу» криптовалюти необхідні великі потужності, то чим більше «майнер» має засобів знаходження хешу, тим швидше він знайде коректний хеш та отримає винагороду. Тому людина, яка має намір займатись «майнінгом», буде шукати засіб для оцінки результатів «майнінгу» (заробіток, витрати на електроенергію тощо), оскільки якщо «майнінг» не буде приносити заробітку, то він буде невигідним для людини.

Для оцінки доцільності генерації даних у блокчейн-просторі, тобто доцільності «майнінгу», необхідно:

1. Визначити потужності пристрою для «майнінгу»;
2. Визначити приблизні витрати на електроенергію
3. Визначити можливе виділення тепла
4. Обчислення коефіцієнту доцільності

Для визначення потужності пристрою достатньо деякий час виконати на ньому алгоритм знаходження хеш-суми за певним алгоритмом, та базуючись на швидкості за проміжок часу отримаємо середню швидкість генерації хешу. Визначення витрат електроенергії можна приблизно обчислити виходячи з апаратного забезпечення пристрою. Визначення можливого виділення тепла необхідне, якщо людина хоче максимально ефективно використовувати витрачену електроенергію. На базі цих значень обчислюється коефіцієнт доцільності «майнінгу»

Перелік посилань:

1. https://prostocoin.com/blog/blockchain-guide - «Что такое блокчейн простыми словами»
2. https://coinmarketcap.com/ – Cryptocurrency market capitalizations
3. https://bitcoin.org/bitcoin.pdf «Bitcoin: A Peer-to-Peer Electronic Cash System»

4. https://whitepaperdatabase.com/ethereum-eth-whitepaper/ «Etherium (ETH) – Whitepaper»

5. https://ripple.com/files/ripple_consensus_whitepaper.pdf - «The Ripple Protocol Consensus Algorithm», Ripple Labs Inc, 2014

6. https://cryptonet.biz/ru/kak-vybrat-kriptovalyutu-dlya-pokupki-priznaki-perspektivnosti/ - «Как выбрать криптовалюту для покупки: признаки перспективности»

7. https://www.allcryptonews.com/kalkulyator-majninga-kak-poschitat-dohodnost-pravilno/ - «Калькулятор майнинга – как посчитать доходность правильно?»

8. https://www.nicehash.com/profitability-calculator - «Profitability calculator»

9. http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html - «Bitcoin mining the hard way: algorithms, protocols and bytes»

10. http://www.righto.com/2014/09/mining-bitcoin-with-pencil-and-paper.html - «Mining Bitcoin with pencil and paper»

МЕТОДИ ОПТИМІЗАЦІЇ ДЛЯ ЗАХИСТУ ТАБЛИЧНИХ ДАНИХ

Шалюк Д.А., студент 4-го курсу групи К-41 спеціальності «Обслуговування програмних систем і комплексів».

Науковий керівник – викладач Петренко І.С**.**

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

Анотація. *У даній роботі були розглянені методи оптимізації для захисту табличних даних. Для захисту даних було обрано Controlled Tabular Adjustment (CTA) метод. Під час реалізації CTA алгоритмів були задіяні різні методи оптимізації, такі як: лінійна, квадратична, конічна. Експериментальним шляхом було визначено, що модель конусу другого порядку є найбільш ефективна для реалізації CTA методу*.

Сьогодні люди стикаються з проблемою обробки величезного обсягу інформації. Дані можуть надходити з будь-яких сфер людського життя, починаючи з деяких особистих даних і закінчуючи різними галузями промисловості та бізнесу. Часто є потреба захисту конфіденційної інформації[1], наданої респондентами перед відкриттям даних публічно.

Для того, щоб описати термін "захист конфіденційності", ми повинні надати деякі визначення. Це зазвичай передбачає поняття гіпотетичного вторгнення, яке може порушити конфіденційність. Існує три основні сторони: (1) респондент, який надає дані, (2) агентство, яке збирає дані, випускає статистичні дані та проектує

контроль за статистичним розкриттям (Statistical Disclosure Limitation - SDL) і (3) гіпотетичний порушник, який має доступ до цих результатів і прагне використовувати їх для розкриття інформації про респондента [2].

Контроль за статистичним розкриттям [3] (SDC) або обмеження розкриття інформації (SDL) прагне захистити статистичні дані таким чином, що вони можуть бути звільнені без надання конфіденційну інформацію, яка може бути пов'язана з конкретними фізичними або юридичними особами.

Методи SDL[4] можна визначити як сукупність методів зменшення ризику розкриття інформації про фізичних, юридичних осіб та інших організацій. Методи SDL мінімізують ризик розкриття до прийнятного рівня, відкриваючи максимально можливу кількість інформації.

У цій роботі ми розглянемо модель мінімально віддаленого контролю табличного регулювання (CTA) [5].

Мета цієї моделі знайти найближчу безпечну таблицю до деякого оригінального набору даних, який містить конфіденційну інформацію $\min \|z - a\|_{l(w)}$ [6].

Відповідно до заданої норми $l(w)$ CTA можна сформулювати наступні задачі оптимізації:

Лінійного програмування (LP) для l_1-норми, квадратичного програмування (QP) для l_2-норми. У цій роботі розглядається альтернативне переформулювання l_1-CTA як оптимізаційна модель конусу другого порядку[7] (SOC). Експериментальним шляхом було визначено, що ця модель найбільш ефективна з усіх розглянутих.

Перелік посилань:

1. https://uk.wikipedia.org/wiki/Конфіденційна_інформація - «Конфіденційна інформація»

2. A. Hundepool, J. Domingo-Ferrer and others, Statistical Disclosure Control, John Wiley & Sons,Ltd (2012).

3. https://en.wikipedia.org/wiki/Statistical_disclosure_control - «Statistical disclosure control»

4. http://www.stat.cmu.edu/~jiashun/Research/Year/Privacy.pdf - «Statistical Disclosure Limitation»

5. https://link.springer.com/chapter/10.1007/0-387-23529-9_4 - «Controlled Tabular Adjustment»

6. Castro J. and Giessing S. Quality issues of minimum distance controlled tabular adjustment. Paper presented at the European Conference on Quality in Survey Statistics, Cardiff, 2426 April, (2006)

7. https://en.wikipedia.org/wiki/Second-order_cone_programming - «Second-Order Cone optimization»

АНАЛІЗ БЕЗПЕКИ Telegram IM

БЄЛОЦИЦЯ Ю.О., студент 3-го курсу, групи К-31, спеціальність 5.05010101 «Обслуговування програмних систем та комплексів»

Науковий керівник – к.т.н., доцент, викладач **Великодний С.С.**

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

Анотація. *Мессенджер Telegram – один з самих відомих методів обміну інформацією. Цей продукт має безліч переваг, основних з яких є: безкоштовність, умовна відкритість коду (не всі частини коду є у вільному доступі) та безпечність. Телеграм вважається одним з найбезпечніших мессенджерів наразі, але у цій роботі було проведено аналіз його протоколу безпеки MTProto, на основі фактів отриманих під час цього аналізу було зроблено висновок, що у телеграму є більш безпечні альтернативи.*

Основою для аналізу було обрано Android версію телеграму, з таких причин: умовно відкритий початковий код, який написаний мовою програмування C++ та Java з використанням механізму Java Native Interface (JNI) – цей механізм дозволяє запускати код написаний мовою C/C++ або Assembly під керуванням JVM (Java Virtual Machine), тобто не використовувати статичне зв'язування, що дає можливість деобфускації коду.

Схема роботи MTProto: маємо двох агентів — Аліса та Боб, вони обидва мають свій ID майстер-ключа (ключ, який використовується для робочих ключів при передачі даних), довжина якого дорівнює 64 біти. Після того, як обидва ключі передали один одному, формується їх цифровий відбиток — auth key, довжина якого становить 2048 біт, але повна схема складається з ще кількох операцій. Контент (повідомлення) отримує атрибути, такі як: ID повідомлення, ID чату і так далі. Це означає, що Аліса має якийсь контент(payload), та цифровий відбиток ключа, але вона не одразу отримає цей контент. Перш за все payload перетворюється на бітовий рядок, цей процес здійснюється за допомогою hash-функції SHA-1(яка, до речі, була

зламана) з цього бітового рядка протокол отримує ключ повідомлення, взагалі цей рядок власне і є ключем.

Auth-key разом з ключем повідомлення переходять на наступний етап – проходять через функцію формування ключа (KDF) — це означає, що з'являється ще один перетворений ключ, прикладом подібного технічного рішення є протокол Діффі-Геллмана, метод, що дозволяє обом агентам, не маючи інформації один про одного, отримати спільний секретний ключ. Після того, як KDF відпрацювало отримаємо два значення зміних — AES key та AES initialization vector. Далі значення цих зміних порівнюється зі значенням payload і, якщо вони збіглися — повідомлення розшифровується.

Офіційна документація телеграм стверджує, що відправлені мережеві дані повинні бути у вигляді: auth-key→msg-key→payload. У ході дослідження було виявлено, що це не так, виявлено випадкові дані. Однак це слідство того, що всі вихідні дані шифруються ще раз за допомогою AES-CTR, який використовує з тимчасовим ключем, що додається до даних.

Аналіз коду призвів до знаходження такого методу атаки, як повторення: зловмисник просто повторює деякі раніше використані дані — коли зловмисник отримає деякі дійсні дані та повторно відсилає їх. Тобто зловмисник не знає, який контент був відправлений, але він зможе його отримати за допомогою цього методу.

Висновок. Telegram не самий безпечний мессенджер, бо не взяв за основу якусь модель протоколу, як наприклад XMPP, який використовує Jabber. Або не закрив свій протокол, як це зробив WeChat. За допомогою аналізу коду та отримання responce-відповіді був знайдений метод атаки, за допомогою якого можливо отримати інформацію з повідомлення. Тобто у телеграм є більш захищені альтернативи, як наприклад TOX, Jabber.

Перелік посилань:

1. https://github.com/DrKLO/Telegram
2. https://core.telegram.org/api
3. RFC 2631 – Метод узгодження ключів Діффі–Геллмана E. Rescorla
4. Чєрнов А. В. Аналіз програм, які заплутують.
5. Analysis of the 12 days program
6. Intellect. Как работает асимметричное шифрование понятным языком. 20 мая 2012.
7. Summary of ANSI X9.42: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography(Description of ANSI 9 Standards)

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

Здано в набір 27.03.2018 р. Підписано до друку 31.03.2018 р.
Тираж 20 прим. обсяг 0,2 друк. арк.
Віддруковано в коледжі зв'язку та інформатизації ОНАЗ ім. О.С. Попова
© КЗІ ОНАЗ, 2018.