Міністерство освіти і науки
Одеська національна академія зв′язку ім. О.С. Попова

П’ята міжнародна науково-практична конференція

“ІНФОКОМУНІКАЦІЇ – СУЧАСНІСТЬ ТА МАЙБУТНЄ”

29-30 жовтня 2015 року

Збірник тез

Частина 2

Одеса
ОНАЗ
2015

УДК 621.39:004.9

Інфокомунікації – сучасність та майбутнє: матеріали п’ятої міжнар. наук.-пр. конф. м. Одеса 29-30 жовт. 2015 р. – Ч.2. – Одеса, ОНАЗ, 2015. – 127 с.

ISBN 978-617-582-002-5

Даний збірник містить тези матеріалів, що представлені на п’яту міжнародну науково-практичну конференцію “**Інфокомунікації – сучасність та майбутнє**”, що проводиться 29-30 жовтня 2015 р. в Одеській національній академії зв′язку ім. О.С. Попова.

У збірник включені тези доповідей за такими напрямками:
– інформаційні мережі та технології.

Робочі мови конференції – українська, російська, англійська.

ISBN 978-617-582-002-5

Програмний комітет

Воробієнко П.П.	голова, д.т.н., проф., ректор ОНАЗ ім. О.С. Попова
Каптур В.А.	заступник голови, к.т.н., проректор з наукової роботи ОНАЗ ім. О.С. Попова
Стрелковська І.В.	заступник голови, д.т.н., проф., директор Навчально-наукового інституту інфокомунікацій та програмної інженерії ОНАЗ ім. О.С. Попова

Організаційний комітет

Балан М.М.	к.т.н., доц. каф. інформаційної безпеки та передачі даних ОНАЗ ім. О.С. Попова
Бабич Ю.О.	ст. викл. каф. мереж зв'язку, заст. директора ННІ ІКПІ ОНАЗ ім. О.С. Попова ОНАС
Беркман Л.Н.	д.т.н., професор, завідуюча кафедрою телекомунікаційних систем Державного університету інфокомунікаційних технологій
Бобровнича Н.С.	к.е.н., доц., завідуюча кафедрою управління проектами та системного аналізу ОНАЗ ім. О.С. Попова
Бондаренко О.В.	д.т.н., проф., проректор з навчальної роботи ОНАЗ ім. О.С. Попова
Васіліу Є.В.	д.т.н., директор Навчально-наукового інституту радіо, телебачення та інформаційної безпеки ОНАЗ ім. О.С. Попова
Єгошина Г.А.	к.т.н, доц. каф. інформаційних технологій, заст. директора ННІ ІКПІ з наукової роботи ОНАЗ ім. О.С. Попова
Захарченко Л.А.	к.е.н., доцент, директор Навчально-наукового інституту економіки та Менеджменту ОНАЗ ім. О.С. Попова
Калінчак О.В.	к.е.н., доц., завідуюча кафедрою економічної теорії ОНАЗ ім. О.С. Попова
Климаш М.М.	д.т.н., професор кафедри Телекомунікації Національного університету „Львівська політехніка"
Корчинский В.В.	к.т.н., доц., доцент кафедры Информационной безопасности и передачи данных ОНАС им. А.С. Попова
Ларін Д.Г.	к.т.н, доц. кафедри інформаційних технологій ОНАЗ ім. О.С. Попова
Лемешко О.В.	д.т.н. професор кафедри телекомунікаційних систем, ХНУРЕ
Леонов Ю.Г.	д.ф.-м.н., профессор кафедры информационных технологий ОНАС им. А.С. Попова
Лісовий І.П.	д.т.н., проф. каф. телекомунікаційних систем ОНАЗ ім. О.С. Попова
Ложковський А.Г.	д.т.н., проф., завідувач кафедрою комутаційних систем ОНАЗ ім. О.С. Попова
Нікітюк Л.А.	к.т.н., проф., завідуюча кафедрою мережі зв'язку ОНАЗ ім. О.С. Попова
Орлов В.М.	д.е.н., проф., завідувач кафедрою економіки підприємства та корпоративного управління ОНАЗ ім. О.С. Попова
Поповський В.В.	д.т.н., проф., завідувач кафедрою телекомунікаційних систем та мереж Харківського національного університету радіоелектроніки
Розенвассер Д.М.	ст.викл. каф. ТЕЗ, заст. директора ННІ ІКПІ ОНАЗ ім. О.С. Попова
Семенко А.І.	д.т.н., професор кафедри телекомунікаційних систем Державного університету інфокомунікаційних технологій
Соловська І.М.	доц. каф. КС, заст. директора ННІ ІКПІ ОНАЗ ім. О.С. Попова
Степанов Д.М.	к.т.н., зав. каф. волоконно-оптических линий связи ОНАС им. А.С. Попова
Станкевич І.В.	к.е.н., в.о. зав. кафедрою менеджменту та маркетингу ОНАЗ ім. О.С. Попова
Сукачов Е.О.	д.т.н., професор кафедри технічної електродинаміки та систем радіозв'язку ОНАЗ ім. О.С. Попова
Сундучков К.С.	д.т.н., проф. каф. інформаційно-телекомунікаційних мереж НТУУ «КПІ»
Тіхонов В.І.	д.т.н., проф. кафедри мереж зв'язку ОНАЗ ім. О.С. Попова
Уривський Л.О.	д.т.н., проф., завідувач кафедрою телекомунікаційних систем Інституту телекомунікаційних систем НТУУ «КПІ»

СЕКЦІЯ 3. ІНФОРМАЦІЙНІ МЕРЕЖІ ТА ТЕХНОЛОГІЇ

УДК 621.39

Аванесов В.Н.
ОНАС им. А. С. Попова
vn93-93@rambler.ru
Научный руководитель – доц. Царёв Р. Ю.

ПЕРСПЕКТИВЫ ИНТЕГРАЦИИ SDN-ТЕХНОЛОГИИ С СЕТЯМИ TCP/IP

Аннотация. *В работе рассматриваются проблемы современных сетей в области обеспечения качества и решения основанные на уже используемой технологии MPLS и новой SDN, анализируется перспектива интеграции SDN с сетями TCP/IP.*

Согласно прогнозу Cisco, в период с 2014 по 2019 гг. мировой IP-трафик утроится и достигнет рекордного показателя в 2 зеттабайта. Это произойдет за счет глобального роста числа интернет-пользователей, персональных устройств и межмашинных соединений, увеличения скоростей ШПД и распространения продвинутых видеосервисов. Как ожидается, в результате суммарного действия этих факторов среднегодовой прирост глобального IP-трафика составит 23%, что будет означать максимальный рост за все десять лет подобных прогнозов. (Так, в прошлом году прогнозируемое значение роста на период 2013-2018 гг. составило 21%)[1].

Увеличение числа пользователей приведет к новым потребностям улучшения параметров качества обслуживания и появлению новых услуг. В свою очередь, это приведет к усложнению архитектуры мультисервисной сети и из-за этого возрастет стоимость реализации.

Одним из решений этой проблемы является интеграция SDN-технологии с современными TCP/IP сетями на базе открытого протокола OpenFlow. Это новый подход построения архитектуры сети, где уровень управления и уровень передачи данных будут разделены, а взаимодействие между ними будет обеспечиваться, через протокол OpenFlow. Это позволит значительно упростить устройства сетевого и канального уровней, так как все управляющие функции будут вынесены в котроллер, а маршрутизаторы и коммутатор будут заниматься только передачей данных. Построение программно-определяемых сетей на базе технологии SDN дает следующие преимущества, которые в традиционных архитектурах отсутствуют либо их использование существенно увеличивает стоимость владения инфраструктурой, а именно:

– полная программируемость сети за счет отделения уровня управления трафиком от уровня передачи данных и переноса функций управления на выделенные вычислительные ресурсы;

– максимально эффективное использование пропускной способности сетевого оборудования путем оптимизации пересылки сетевых потоков;

– создание изолированных виртуальных сетей для каждого клиента ит-услуг на базе единой физической инфраструктуры;

– динамическая подстройка емкости виртуальной сети и других параметров под растущие потребности клиента без изменения физической топологии;

– масштабируемость, которая обеспечивает увеличение числа логических сетей без снижения производительности уже существующих виртуальных конфигураций;

– повышение безопасности за счет “сквозного” управления защитными политиками в каждом сетевом устройстве для отдельных потоков;

– увеличение надежности функционирования сети с помощью централизованного управления конфигурацией сетевых параметров на уровне сессий, пользователей, устройств и приложений[2].

Критики считают, что внедрение SDN неоправданно, что использование существующей технологии MPLS будет более эффективно. В основе MPLS лежит механизм передачи данных по меткам. Обработка пакетов (на основе класса эквивалентности) в этой технологии похожа на ту, что использует SDN, однако, при измерении задержки при передаче потокового видео (самый популярный контент на данный момент) были получены следующие данные (схема сети, на которой проходили измерения приедена на рис.1):

- SDN ~ 150ms;
- MPLS ~ 200ms.

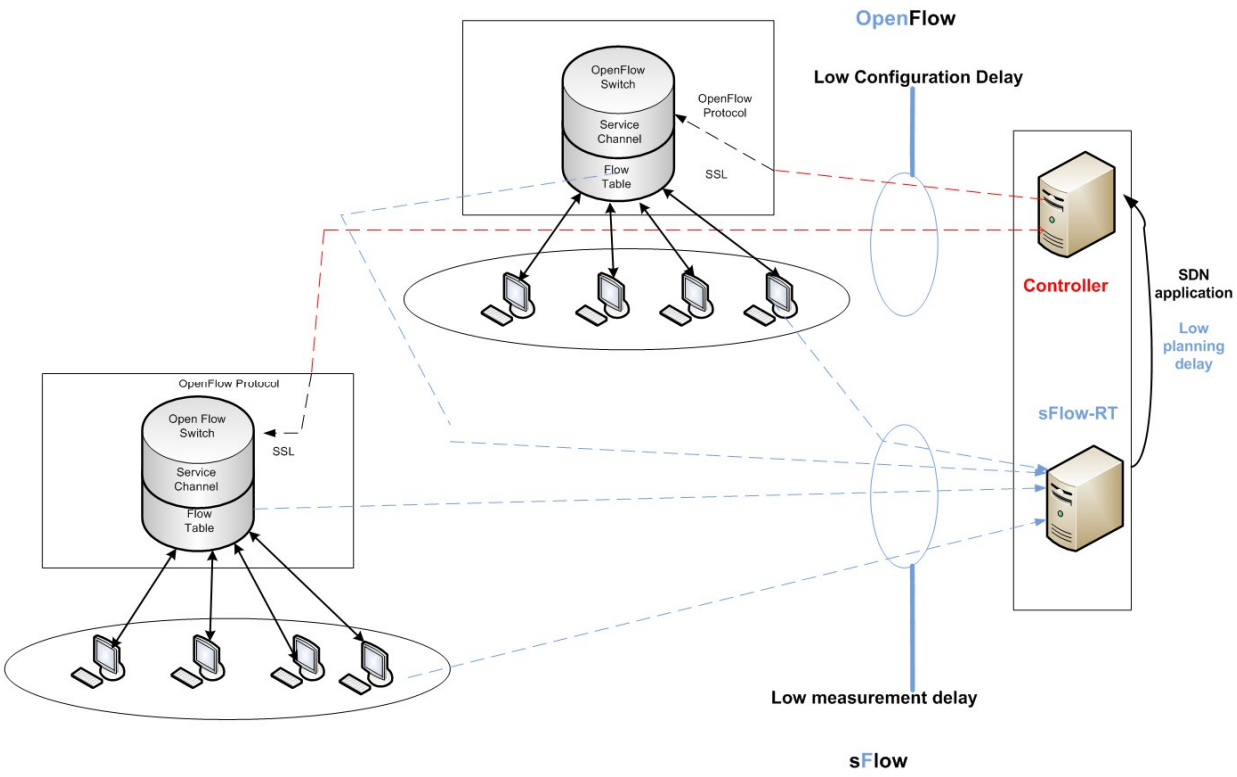


Рисунок 1 – Схема сети

Исходя из этого можно сказать, что с ростом числа пользователей и появлением новых услуг требования к параметрам качества обслуживания, а в первую очередь к задержке, так как потоковое видео –самый популярный контент на данный момент, будут только расти. На данном этапе MPLS может обеспечить требуемый уровень задержки, но в будущем придется пересмотреть архитектуру построения сети.

Другим трендом последних лет является виртуализация всего и вся. Как следствие, виртуализация добралась и до сетевых функций – маршрутизации, NAT, фильтрации и исследования трафика и т.д. Многие производители, выпускающие аппаратные решения в этой области, либо уже выпустили, либо готовят к выпуску виртуализированные версии своих продуктов.

Хорошей идеей в данном случае является симбиоз 2 технологий – SDN и NFV. Используя возможности SDN по изоляции трафика, созданию сервисных цепочек и балансировке нагрузки и применяя в рамках создаваемой инфраструктуры виртуализированные сетевые функции, можно добиться поразительного результата. Становится возможным персонализировать набор сетевых услуг вплоть до конкретного подразделения или сотрудника в корпоративном секторе либо до конкретного абонента в случае оператора связи. А это прямой путь к предоставлению сетевых услуг по столь популярной в настоящее время сервисной модели, когда конечный потребитель платит только за то, что ему необходимо.

За SDN будущее — эта технология помогает решить множество задач. Однако в реализациях SDN могут применяться разные механизмы, и впоследствии их спектр, вероятно, станет еще шире. Безусловно, появятся новые способы построения сетей SDN. Скорее всего, будут создаваться гибридные, комбинированные сети, где сочетаются новые и традиционные подходы.

Литература

1. Прогнозы Cisco по поводу увеличения IP-трафика - http://hi-tech.ua/article/cisco-prognoziruet-trehkratnoe-uvelichenie-ip-trafika-s-2014-po-2019-godyi/
2. Преимущества SDN - http://rusteletech.ru/resheniya-sdn
3. Перспективы SDN - http://www.jetinfo.ru/jetinfo_arhiv/tekhnologii-virtualizatsii/kogda-s-sdn-zhit-khorosho/2015

УДК 621.396

Аскеров И.Э.
ОНАС им. О.С.Попова
Imamvcrdi.mamedov@mail.ru
Научный руководитель - д.т.н., проф. Лесовой И.П.

ПОВЫШЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ ОПТИЧЕСКОЙ ТРАНСПОРТНОЙ СЕТИ

Аннотация. *В работе исследовано влияние нелинейных эффектов на параметры функционирования оптической транспортной сети.*

Среди всех нелинейных эффектов в волоконно-оптических системах передачи с разделением сигналов по длине волны четирехволновое смешение (ЧВС) оказывает наибольшее негативное влияние. Исследована зависимость эффекта ЧВС от параметров системы DWDM, а также влияние этого эффекта на показатели эффективности функционирования системы.

Данное исследование проведено на примере 40-канальной системы с одинаковыми спектральными полосами между каналами. Задача исследования - вычислить, сколько паразитных гармоник попадает в каждый из каналов системы. Исходными данными для моделирования являются: количество каналов - 40, общая полоса длин волны, использует система - 1550,4 - 1542,6 нм, ширина полосы между каналами - 0,2 нм, мощность каждого из каналов - 5 мВт, оптическое волокно со следующими характеристиками: длина волны нулевой дисперсии - 1550 нм, затухание - 0,2 дБ / км, наклон дисперсионной характеристики – 0,09. Зависимости количества комбинационных продуктов от номера оптического тракта показана на рис. 1.

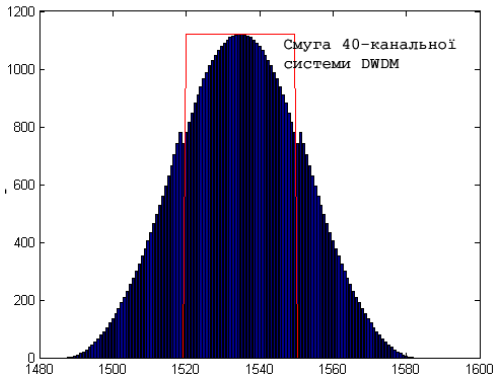


Рисунок 1. Количество комбинационных продуктов, возникающих в результате четырехволнового смешения

В отдельных оптических трактах количество паразитных волн есть более 1000, что, в некоторых случаях может существенно ограничить возможности системы передачи.

Вывод. Выбор ширины полосы между соседними каналами может использоваться для уменьшения негативного влияния эффекта чотирихвильового смешивания.

Литература

1. Иванов А.Б. Волоконная оптика. Компоненты, системы передачи, измерения. – М.: Syrus Systems, 1999. - 672 с.

2. Р. Фриман Волоконно-оптические системы связи. // ТЕХНОСФЕРА, Москва. – 2004. С. 371.

УДК 378.047

Безвербний І.А.
Інститут кібернетики НАН України ім.В.М.Глушкова
harzy@ukr.net

РОЗГОРТАННЯ ПРОГРАМНОГО КОМПОНЕНТА НАВЧАЛЬНОГО ПРИЗНАЧЕННЯ НА БАЗІ ХМАРНОГО РІШЕННЯ

Анотація. *Розглянуто особливості хмаро орієнтованого рішення надання доступу до електронного освітнього ресурсу у процесі навчання інформатичних дисциплін. Наведено критерії вибору математичного програмного забезпечення при встановленні його «у хмарі», висвітлено основні риси проектування інформаційно-технологічної інфраструктури для реалізації програмного компоненту на базі віртуального сервера з операційною системою Ubuntu. Охарактеризовано аспекти педагогічного застосування.*

Використання електронних освітніх ресурсів і математичного програмного забезпечення є нині невід'ємним атрибутом навчального процесу у вищому навчальному закладі. Це зумовлено тим, що ринок програмного забезпечення невпинно розвивається і в багатьох випадках можна підібрати підходяще рішення, що дасть можливість зекономити час і зусилля педагога і студентів при підготовці і опрацюванні навчального матеріалу. Зокрема, в процесі навчання інформатичних дисциплін знайшли своє місце такі засоби, як системи комп'ютерної математики (СКМ), що застосовуються для виконання математичних обрахунків, моделювання, побудови графіків під час як аудиторної і поза-аудиторної, так і навчально-дослідницької діяльності студентів [1]. При використанні СКМ можна досягнути глибшого розуміння матеріалу, що вивчається, за рахунок перегляду демонстрацій, надання інтерпретацій математичних співвідношень, самостійного конструювання різноманітних об'єктів тощо [1, 2].

Вибір підходящого математичного програмного забезпечення навчального призначення залежить від наукових і навчальних цілей, із урахуванням вхідних даних та результату, що необхідно отримати. Наприклад, якщо треба побудувати аналітичну модель досліджуваного явища чи об'єкта, доцільніше використовувати такі пакети, як Mathematica, Maple, Maxima, а для опрацювання великих масивів даних зручно застосовувати систему Matlab [2].

Вибір математичного пакету обумовлений різними чинниками, серед яких не останню роль відіграє вартість продукту, ліцензійні умови використання, вимоги до наявного обладнання тощо. Зокрема у Дрогобицькому державному педагогічному університеті імені Івана Франка в процесі педагогічного експерименту з навчання інформатичних дисциплін бакаліварів інформатики була використана СКМ Maxima [2]. Вибір був обумовлений тим, що система є вільно поширеною, оснащена зручною системою меню, що дає змогу виконувати символьні перетворення, розв'язувати рівняння, обчислювати границі, похідні, інтеграли

тощо, не знаючи мови для опису команд щодо виконання цих дій. Крім того, дана є досить потужною, багато в чому не поступається у розв'язуванні задач з дослідження операцій таким системам як Maple та Mahtematika [1].

Використання засобів даного типу «у хмарі» є перспективним напрямом їх розвитку, коли виникає більше можливостей адаптації середовища навчання до рівня навчальних досягнень, індивідуальних потреб та цілей того, хто вчиться [1]. При цьому застосовується технологія «*віртуального робочого столу*» [2, 3]. Робота з програмним забезпеченням, що встановлено на віртуальному комп'ютері, нічим не відрізняється від того, що встановлено на персональному робочому місці студента, звернення може здійснюватися через браузер. Зберігання і опрацювання даних відбувається у ЦОД (центрі опрацювання даних), не потребує витрачання навчального часу на інсталяцію і оновлення, що створює умови для більш диференційованого підходу до організації навчання, дає можливість зосередитися на вивченні основного матеріалу [3].

У ході педагогічного експерименту була реалізована хмарна версія системи Maxima, встановлена на віртуальному сервері з операційною системою Ubuntu 10.04 (Lucid Lynks). В репозитарії цієї операційної системи є версія системи Maxima на основі редактора Emacs, що і була встановлена на віртуальний робочий стіл студента [2].

Була використана модель віртуальної гібридної хмари, що містить віртуальну корпоративну (приватну) підмережу і загальнодоступну підмережу [3]. До загальнодоступної підмережі користувач може мати доступ через протокол RDP (Remote Desktop Protocol) [3]. будь-якого пристрою, в будь-якому місці і в будь-який час, за наявності Інтернет-з'єднання.

В даному випадку, комп'ютер користувача – це RDP–клієнт, тоді як віртуальна машина, яка знаходиться у хмарі – це RDP–сервер [3]. У межах приватної підмережі, користувач не може звернутися безпосередньо до RDP-сервера, бо той не під'єднаний до Інтернет. Комп'ютери у приватній підмережі мають вихід в Інтернет через VPN – шлюз. Отримати доступ до шлюзу можна з будь-якого пристрою, але за умови, що на ньому встановлено VPN – з'єднання [3].

Використання хмаро орієнтованого компонента навчального призначення в педагогічному експерименті підтвердило свою ефективність [2], що свідчить про доцільність застосування хмарних рішень організації доступу до навчальних ресурсів у процесі навчання. Виникає можливість зосередити увагу студентів на засадничих поняттях, принципах, підходах за рахунок вивільнення часу і зусиль, які йдуть на встановлення, підтримування, обслуговування програмного забезпечення, та навіть значною мірою знівелювати реальні просторові та часові межі реалізації доступу до необхідних електронних ресурсів [2]. Даний підхід сприяє поглибленому вивченню матеріалу, підвищенню ІКТ-компетентностей студентів, модернізації навчального середовища, створення умов для залучення у навчальний процес передових програмних засобів і технологій.

Література

1. Шишкіна М.П. Фундаменталізація навчання інформатичних дисциплін у сучасному високотехнологічному середовищі / М.П.Шишкіна, У.П. Когут // Інформаційні технології в освіті: Збірник наукових праць. Випуск 15. - Херсон: ХДУ, 2013. - с.309-317.

2. Шишкіна М.П. Формування фахових компетентностей бакалаврів інформатики у хмаро орієнтованому середовищі педагогічного університету / М.П.Шишкіна, У.П. Когут, І.А.Безвербний // Проблеми підготовки сучасного вчителя. – Умань: ФОП Жовтий О.О., 2014. –вип.9. – ч.2. – С. 136-146

3. Шишкіна М.П. Моделі організації доступу до програмного забезпечення у хмаро орієнтованому освітньому середовищі // Інформаційні технології в освіті. – вип.22. – 2015. – С. 120-129

УДК 621.391.3

Буряк К.Г.
ОНАЗ ім. А. С. Попова
koslan843@gmail.com
Науковий керівник -доц. І. В. Шерепа

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ СИСТЕМ УПРАВЛІННЯ НА АВТОМАТИЗОВАНИХ ТРАНСПОРТНИХ ЗАСОБАХ

Анотація. *Проведено аналіз перспективних систем управління транспортом, наведені економічні і технічні слідства їх впровадження.*

Транспорт є однією з найважливіших складових частин економіки кожної країни. Транспортні послуги забезпечують підвищення ефективності суспільного виробництва, нормальне функціонування економіки, створюють умови для раціонального розподілу по території країни виробничих сил

Сучасна світова транспортна система включає в себе наступні види транспорту [1]: водні: морський, внутрішній водний, сухопутні (залізничний, автомобільний), трубопровідний, повітряний.

Автоматизація транспорту сьогодні розвивається за кількома напрямками. Ускладнення завдань, які виконуються машинами і механізмами і зростаючі вимоги споживачів до електронного оснащенню транспорту, призводять до розвитку технічних рішень, що забезпечують кращу керованість транспортного засобу (оснащення бортовими комп'ютерами, системами навігації та ін.). Розвиток отримали транспортні довідково-інформаційні системи. Такі системи орієнтовані на клієнтів транспортних компаній і дозволяють їм в режимі реального часу отримувати інформацію про розклад, маршрутах, вартості послуг, наявність вільних місць тощо. Існують і інформаційно-довідкові системи, призначені для організації обміну інформацією між учасниками ринку вантажоперевезень: вантажовласниками, перевізниками, експедиторами тощо. У таких системах щодня розміщується інформація про вантажі і вільних (попутних) машинах. Інформація відразу стає доступною всім користувачам. Підібравши відповідний вантаж (або машину), користувач системи зв'язується безпосередньо з фірмою, яка надала інформацію, і домовляється про перевезення. Активно розробляються корпоративні інформаційні системи, орієнтовані на підвищення ефективності управління транспортним підприємством. При цьому велика увага приділяється контролю над просуванням вантажів, оптимізації перевезень, організації розкладів і т.п.

Стандарт інтелектуальних транспортних систем US DoT ITS [2,3] описує весь комплекс автоматизованих систем управління транспортом. Це запропонована транспортним департаментом США ініціатива, спрямована на створення єдиного інформаційного простору, об'єднуючого автомобілі, шляхове обладнання, диспетчерські зали та ЦОД по всій країні.

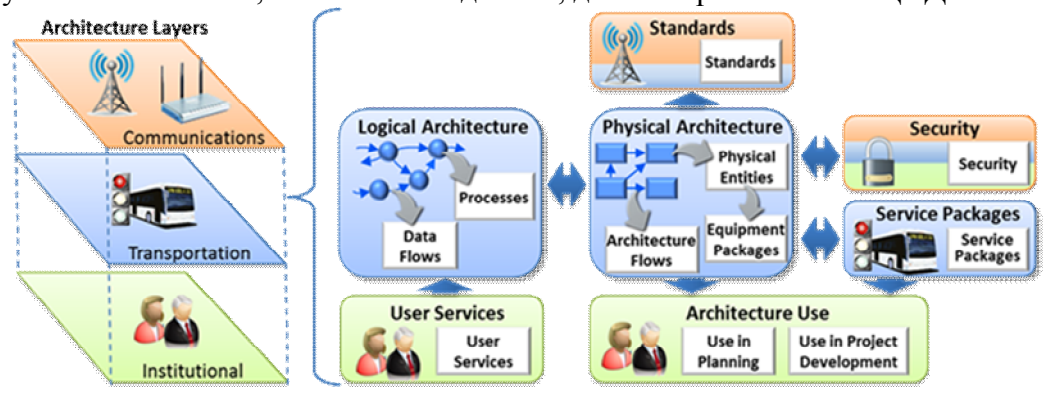


Рис 1 Архітектура стандарту US DoT ITS

Створення єдиної архітектури ІТС дозволяє контролювати три основні напрями [4]:

Безпека. Основна мета - зниження аварійності на дорогах. Сюди ж входить моніторинг природних і техногенних катаклізмів.

Мобільність. Збір інформації про пробки від рухомих в потоці автомобілів та інформування учасників руху.

Захист навколишнього середовища. Зниження шкоди навколишньому середовищу від автотранспорту за допомогою моніторингу ситуації в реальному часі і своєчасного прийняття рішень.

У процесі розробки та впровадження автоматизованих систем виникають проблеми різноманітного характеру. Наприклад, розвиток автоматизованих систем на транспорті до останнього часу проходить таким чином, що окремі функціональні підсистеми раніше залишаються замкнуто-автономними. Використовуючи по суті одну і ту ж інформацію, в системах ведеться її самостійна нескоординованих обробка, а в результаті інформація на виході має суттєві відмінності. Крім того, найчастіше подібна вхідна інформація передається з одного джерела в різні системи різними повідомленнями, що призводить до дублювання передачі інформації і підвищує навантаження на канали зв'язку.

***Висновок*:** очікуються значні економічні добутки від впровадження даної технологій, а також значне підвищення безпеки як на територій Україна так і на територій інших країн.

Література

1. https://ru.wikipedia.org
2. http://www.iteris.com
3. http://www.its.dot.gov
4. http://habrahabr.ru

УДК 681.54., 681.3.062

Вашпанов Ю.А.
ОНАХТ
vashpanov@mail.ru

ИСПОЛЬЗОВАНИЕ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ ДЛЯ СИСТЕМ АВТОМАТИЧЕСКОГО КОНТРОЛЯ

Анотація. *В докладе рассматриваются вопросы использования современных беспроводных сенсорных сетей технологий от компании National Instruments в системах автоматического контроля и управления химических производств.*

Технологии развития беспроводных сенсорных сетей являются в настоящее время наиболее актуальными для систем контроля и управления технологических производств. Последние достижения в области телекоммуникационных технологий приводят к ощутимому уменьшению экономических и материальных затрат, которые имеют место при инсталляции и обслуживании проводных средств.

В докладе рассмотрена архитектура беспроводной сети на базе современных беспроводных узлов измерений (WSN Measurement Nodes) от компании National Instruments USA [1], которая разрабатывалась для автоматизации измерений внутри промышленной зоны химического предприятия.

Моделирование на базе LabView модулей для автоматического контроля и управления было проведено, чтобы улучшить метрологическую точность измерения интеллектуальных сенсоров аммиака [2] в широком диапазоне.

Разработаны алгоритмы обработки и управления потоковыми данными, программные модули в программной среде NI LabView™ для измерительных сенсорных устройств с

помощью the DAQ Assistance Express [3]. Результаты потоковых измерений в программной среде LabView™ в реальном масштабе времени выводиться на экран оператора как в виде таблиц данных, так могут быть также организованы в виде данных графиков.

Разрабатываемая компьютерная система на основе интеллектуальных сенсоров аммиака в сочетании с современными беспроводными технологией может быть полезной в химической промышленности для автоматического обнаружения в промышленной зоне предприятий опасных концентраций аммиака в режиме реального времени измерений.

Література

1. NI Wireless Sensor Network Architectures, http://sine.ni.com/np/app/main/p/ap/imc/lang/en/pg/1/sn/n17:imc,n21:11297/fmid/487.

2. Vashpanov, Yu.A.; Jung, J.I.; Kwack, K.D. Photo-EMF sensitivity of porous silicon thin layer – crystalline silicon hetero-junction to ammonia adsorption. *Sensors* 2011, *11*, 1321-1327.

3. The DAQ Assistance Express VI, http://zone.ni.com/devzone/cda/tut/p/id/4656.

УДК 004.75

Волошин Д.М.
ОНАЗ ім. О.С.Попова
wwww.dima.vol@mail.ru
Науковий керівник - доц. Царьов Р.Ю.

АНАЛИЗ ПЕРСПЕКТИВ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ SDN

Аннотация. *В работе дается оценка перспектив развития и использования технологии программно-конфигурируемых сетей.*

В последние годы, наблюдается стабильная тенденция к росту объема глобального IP-трафика. Согласно аналитическим прогнозам ведущих компаний, к 2016 году объем мирового IP-трафика может достичь отметки в 1,3 зеттабайта в год [1]. Одновременно с ростом объемов IP-трафика, происходит изменение его структуры. Вначале 2000-х 90% всего IP-трафика (Интернет трафика) приходилось на протоколы доступа к web-ресурсам (FTP и HTTP). С 2011 года произошло существенное изменение структуры IP-трафика – весь его объем практически поровну разделился между тремя типами приложений: web-приложениями, p2p-сетями и видео сервисами. К 2016 году доля трафика видео сервисов от общего объема составит не менее 50%[1]. Такие тенденции приводят к тому, что сети становятся технологически все более сложными, операторам и провайдерам сложно обеспечить требуемый уровень качества услуг.

Одним из возможных вариантов решения указанной проблемы является технология SDN (Software Defined Networking). Технология SDN предполагает разделение процесса управления сетью (обеспечения качества) и процесса передачи данных. Такой подход к организации сети, позволит получить сеть, построенную на базе простых дешевых коммутаторов, для управления которой используется высоко интеллектуальный сервер (контроллер)[2].

На рисунке 1 представлена архитектура построения сети на базе технологии SDN и сеть с традиционной архитектурой.

Целью работы является оценка перспектив развития и использования технологии SDN в мире. В общем случае, процесс оценки перспектив развития и внедрения новой сетевой технологии может быть описан функцией тангенса гиперболического (рис.2) [3], где наблюдаемый параметр p – это число внедренных в мире проектов на базе технологии SDN.

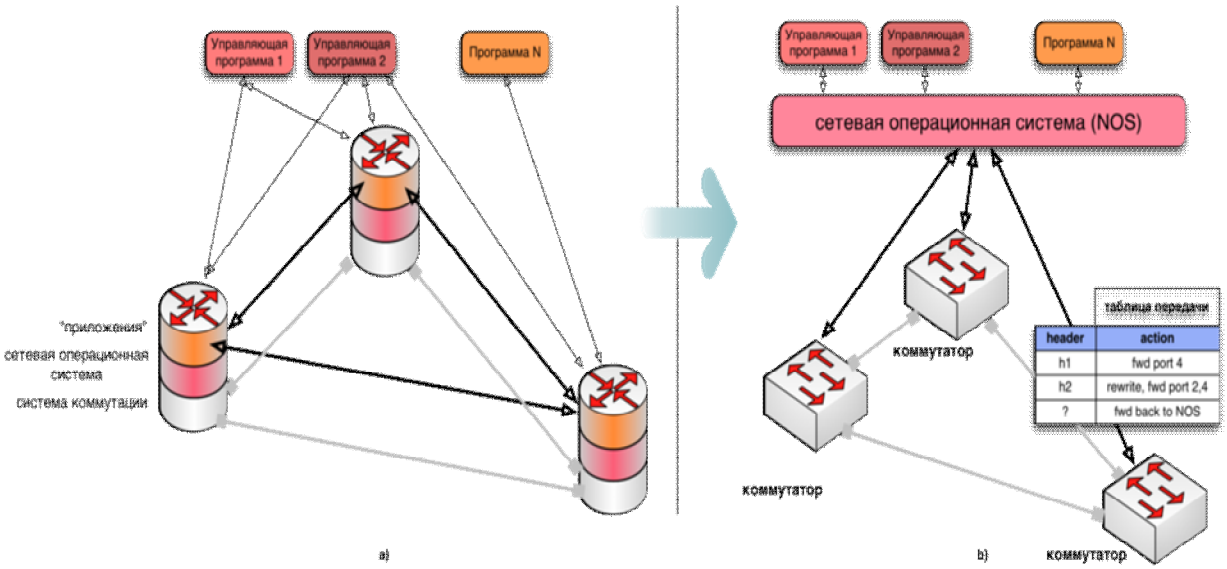


Рисунок 1 - Разделение системы управления и передачи в архитектуре SDN. (a) Традиционная архитектура с автономными сетевыми элементами, (b) архитектура SDN с централизованной управляющей функцией)

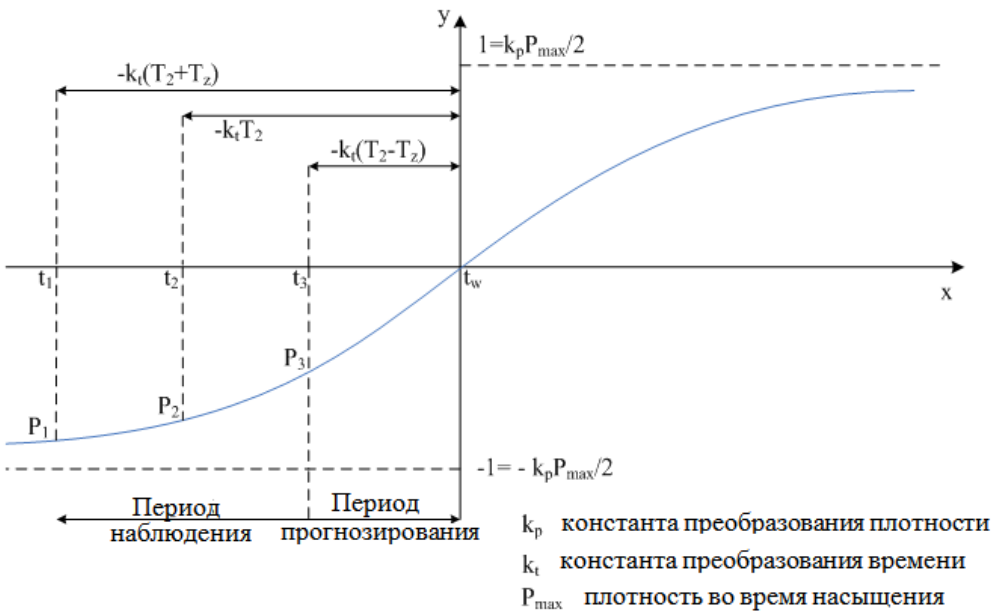


Рисунок 2 – Функция гиперболического тангенса

Идея состоит в следующем – в момент времени T (интервал времени от точки, которая рассматривается к точке насыщения) можно сложить систему уравнений для 3 выбранных моментов наблюдения, в которых между фиксированными значениями действующих проектов на базе технологии SDN с одинаковым приростом T_z[3]:

$$\begin{cases} 1 - k_p P_1 = th[-k_t(T_2 + T_z)], \\ 1 - k_p P_2 = th[-k_t T_2], \\ 1 - k_p P_3 = th[-k_t(T_2 - T_z)] \end{cases} \quad (1)$$

где k_p – коэффициент преобразования плотности действующих проектов на базе технологии SDN, k_t – константа преобразования времени, T_z – интервал приращения времени.

Эта система уравнений имеет следующие решения[3]:

$$k_p = \frac{2(P_1 P_3 - P_2^2)}{P_2(2P_2 P_3 - P_2 P_3 - P_1 P_2)} \quad (2)$$

$$T_2 = T_z \frac{arth(1 - k_p P_z)}{arth(1 - k_p P_2) - arth(1 - k_p P_3)} \quad (3)$$

$$p_{max} = \frac{2}{k_p} \quad (4)$$

где T_2 – период времени, $T_2 = T\omega - T_2$,$T\omega$ – момент перехода в область насыщения, T_2 – момент наступления события P_2. С помощью указанных уравнений можно определить момент перехода сетей на базе технологии SDN в область насыщения.

В качестве интервала наблюдения выберем период в 3 года, в качестве стартовой точки – 2008 год. В табл. 1 приведены статистические данные на реализованные и анонсированные проекты построения/модернизации сети на базе технологии SDN[2].

Таблица 1 – Динамика роста числа проектов сетей на базе технологи SDN

Год	**Число действующих проектов на базе SDN**	**Число потенциально возможных проектов**	**%**
2008	3(в тестовом)	500	0,6
2011	450	2500	18
2014	2900	5800	50

Тогда: $P_1 = 0{,}06$, $P_2 = 0{,}18$, $P_3 = 0{,}5$, $T_z = 3$.

Используя формулы (1) – (4) получается, что период перехода в область насыщения $T_2 \approx 5$ лет, тогда сама точка входа в область насыщения $T\omega = 2014 + 5 = 2019$ год.

По результатам прогноза видно, что массовое внедрение технологии SDN ожидается к 2019 году.

Следует отметить, что согласно данным SDNCentral [1], мировой рынок SDN составил в 2014 г. $3,4млрд, а к 2018 г. достигнет $35,6 млрд. По прогнозам ResearchandMarkets, в 2012-2016 гг. среднегодовой прирост глобального рынка SDN сетей составит 151%. Такие ведущие фирмы мировые компании, как HP и Google, уже создали собственные SDN сети, что так же свидетельствует о том, что технология SDN имеет неплохие перспективы.

Литература

1. Обзор развития мирового рынка телекоммуникаций [Электронный ресурс] / TheCiscocorp. – Режим доступа: \www/ URL: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html

2. Thomas Nadeau. SDN: Software Defined Networks. London: 2013. – p.384

3. Vivek Tiwari. SDN and OpenFlow for Beginners with hands on labs. Berlin:2014. – p.156

4. Elena Verizhnikova. Technology of SDN-startup is the machine of the future. URL: http://firrma.ru/data/articles/1739/

УДК 621.39

Горобець О.Ю.
ОНАЗ ім. О.С.Попова
E–mail: Gorobets-A@mail.ru
Науковий керівник – к.т.н., доц. Шмельова Т.Р.

АНАЛІЗ ВАРІАНТІВ ПОБУДОВИ БЕЗПРОВОДОВОЇ МЕРЕЖІ НА ОСНОВІ СТАНДАРТУ IEEE 802.11

Анотація. *В даній роботі проаналізовано варіанти побудови безпроводової мережі на основі стандарту IEEE 802.11 та наведена статистика використання топологій мережі. Зазначено дії, які необхідно зробити при проведенні радіообстеження об'єкта для Wi-Fi. Приведено основі характеристики стандартів сімейства IEEE 802.11, а також представлена загальна класифікація мережевих атак з діаграмою рівня їх небезпеки та протоколи безпеки безпроводових мереж. Розглянуто необхідність впровадження безпроводових мереж Wi-Fi на базі стандарту IEEE 802.11 в Україні та Світі.*

На сьогоднішній день ми можемо спостерігати бурхливий розвиток безпроводових мереж: на ринку з`являється велика кількість обладнання, що відкриває все більше можливостей в області телекомунікацій як на побутовому рівні, так і на промисловому, стрімкими темпами зростає якість, швидкість і захищеність обміну інформацією [1].

Перспективою розвитку безпроводових мереж є не лише поліпшення їх характеристик у великих містах, а й побудова у менших населених пунктах.

На сучасному етапі розвитку мережевих технологій, технологія безпроводових мереж Wi-Fi є найбільш зручною в умовах, які вимагають мобільності, простості установки і використання. Wi-Fi – стандарт широкосмугового бездротового зв'язку сімейства 802.11 розроблений у 1997 р. Як правило, технологія Wi-Fi використовується для організації безпроводових локальних комп'ютерних мереж, а також для створення так званих гарячих точок високошвидкісного доступу до Інтернету.

Основні характеристики стандартів групи IEEE 802.11

IEEE 802.11 – це набір стандартів безпроводової мережі, розроблений інститутом інженерів електротехніки та електроніки. Першим серед стандартів було розроблено одноіменний IEEE 802.11 [3]. Роботу над ним розпочали ще в 1990 році. з метою створення єдиного стандарту для радіоустаткування, яке працювало на частоті 2,4 ГГц. При цьому ставилося завдання досягти швидкості 1 і 2 Мбіт/с при використанні методів DSSS і FHSS відповідно.

Робота над створенням стандарту закінчилася через 7 років. Мета була досягнута, але швидкість, яку забезпечував новий стандарт, виявилася занадто малою для сучасних потреб. Тому робоча група з IEEE почала розробку нових, більш швидкісних, стандартів. Їхні основні характеристики наведені в табл. 1.2.

Таблиця 1.1 – Основні характеристики стандартів сімейства IEEE 802.11

Назва стандарту	Частота, що використовується, ГГц	Швидкість передачі данних	Радіус зони покриття, м
IEEE 802.11a	2,4 та 5	54 Мбіт/с	100
IEEE 802.11b	2,4	11(22) Мбіт/с	300
IEEE 802.11g	2,4	54 Мбіт/с	300
IEEE 802.11n	2,4-2,5 та 5	600 Мбіт/с	>400
IEEE 802.11ac	5-6	6 Гбіт/с	500

Аналіз топології побудови мережі IEEE 802.11

Під топологією (компонуванням, конфігурацією, структурою) комп'ютерної мережі звичайно розуміється фізичне розташування комп'ютерів мережі один відносно одного й

спосіб з’єднання їх лініями зв’язку. Важливо відзначити, що поняття топології ставиться, насамперед, до локальних мереж, у яких структуру зв’язків можна легко простежити. У глобальних мережах структура зв’язків звичайно схована від користувачів не занадто важлива, тому що кожний сеанс зв’язку може виконуватися по своєму власному шляху [2].

Топологія визначає вимоги до устаткування, тип використовуваного кабелю, можливі й найбільш зручні методи керування обміном, надійність роботи, можливості розширення мережі.

Існує три основних топології мережі:

– шина, при якій всі комп’ютери паралельно підключаються до однієї лінії зв’язку й інформація від кожного комп’ютера одночасно передається всім іншим комп’ютерам;

– зірка, при якій до одного центрального пристрою приєднуються інші периферійні пристрої, причому кожний з них використовує свою окрему лінію зв’язку;

– кільце, при якій кожний комп’ютер передає інформацію завжди тільки одному комп’ютеру, наступному в ланцюжку, а одержує інформацію тільки від попереднього комп’ютера в ланцюжку, і цей ланцюжок замкнутий в «кільце» .

На практиці нерідко використовують і комбінації базових топологій, але більшість мереж орієнтовані саме на ці три (рис. 1).

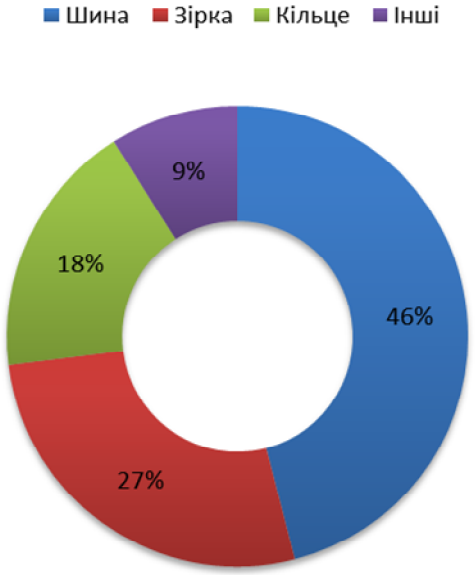


Рис.1 Статистика використання топологій мережі

При проведенні радіообстеження об'єкта для Wi-Fi необхідно зробити наступні кроки: отримати план приміщення; візуально оглянути весь об'єкт; визначити місця знаходження майбутніх користувачів WLAN; визначити тип і модель точок доступу в майбутньої мережі; визначити попередні місця встановлення точок доступу; перевірка місць положення точок доступу і реального рівня параметрів мережі.

Загальна класифікація мережевих атак

Одне з визначень мережевої атаки – мережева атака може бути визначена як будь-який метод, процес або засіб, що використовується для виконання зловмисної спроби порушення мережевої безпеки.

Існує багато причин, по яких люди хочуть атакувати корпоративні мережі. Людей, які проводять мережеві атаки часто називають хакерами або кракерами.

У цілому мережеві атаки можна класифікувати чотирма типами (рис. 2): внутрішні небезпеки; зовнішні небезпеки; структуровані небезпеки; неструктуровані небезпеки.

Протоколи безпеки безпроводових мереж

– WPA – технологія захищеного доступу до бездротових мереж;

– EAP – протокол розширеної аутентифікації (Extensible Authentication Protocol);
– TKIP – протокол інтеграції тимчасового ключа (Temporal Key Integrity Protocol);
– MIC – технологія перевірки цілісності повідомлень (Message Integrity Check).

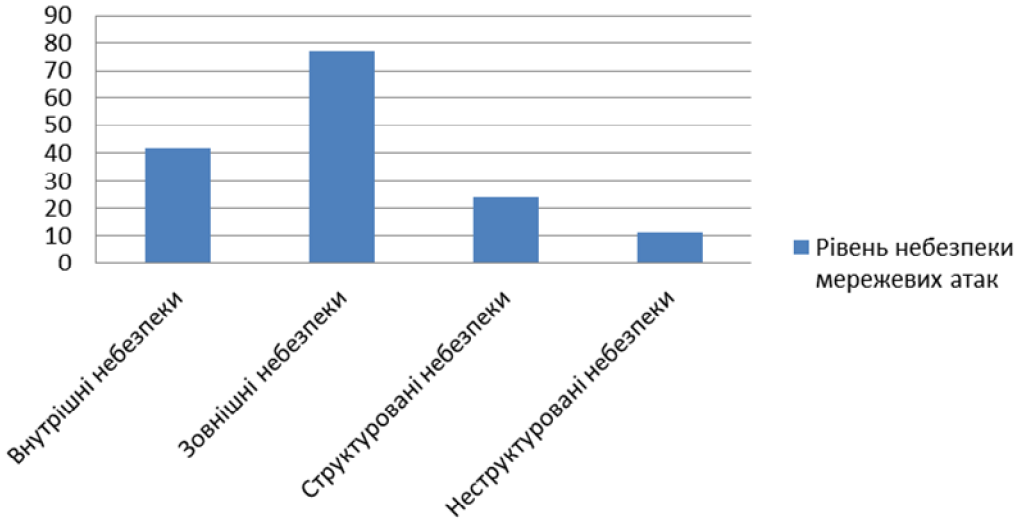


Рис.2 – Діаграма рівня небезпеки мережевих атак

Висновок. На сьогоднішній день безпроводові мережі Wi-Fi на базі стандарту IEEE 802.11 набули найбільш стрімкого розвитку в Україні та Світі. В першу чергу цьому сприяє розвиток та розширення ринку пристроїв, які мають можливість підключення до безпроводових мереж. Ще одним важливим фактором в процесі утвердження Wi-Fi технологій є необхідність побудови мереж в умовах, де впровадження проводового зв'язку неможливо або недоцільне з економічних міркувань. Так, наприклад, прокладання кабельних мереж в місцях зі складним рельєфом або несприятливими погодніми умовами навряд чи обійдеться дешевше та гарантуватиме ту саму надійність що і побудова Wi-Fi мережі.

Література

1. Дьяков М. Беспроводные сети: что вы о них знаете? // 374.ru - 2011, №083
2. Артамонов Г.Т. Топологія обчислювальних мереж і середовищ. - М.: Радіо і зв'язок, 1985. - 192 с.
3. Стандарт IEEE 802.11

УДК 681.325

Д.т.н., проф.. Дичка І.А., магістрант Шолтун Д.В.
НТУУ КПІ»
dychka@scs.ntu-kpi.kiev.ua
к.т.н., доц.. Голуб В.І, Ващілін О.В.
УДППЗ «Укрпошта»

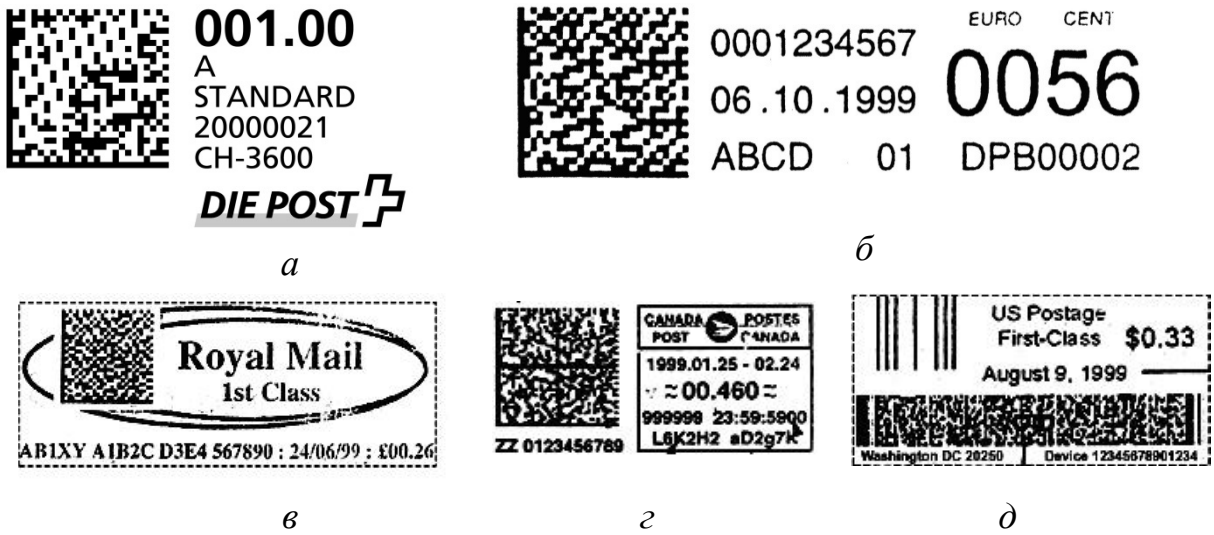
АВТОМАТИЧНА ІДЕНТИФІКАЦІЯ ПОШТОВИХ ВІДПРАВЛЕНЬ НА ОСНОВІ ТРИКОЛІРНИХ ЦИФРОВИХ ПОШТОВИХ МАРОК

Анотація. *Розглядається можливість застосування триколірних (біло-чорно-сірих) цифрових поштових марок в системі поштового зв'язку України для автоматизації виробничих процесів.*

Світова поштова мережа, що налічує понад 700 тисяч відділень пошти, є найбільшою фізичною системою розповсюдження у світі, в якій щорічно обробляється понад 440 млрд

одиниць поштової кореспонденції [1]. Тому гостро постає питання автоматизації виробничих процесів у поштовій галузі, оскільки це дасть змогу ефективніше використовувати людські, технічні та фінансові ресурси, а також значно прискорить час оброблення поштових відправлень.

Всесвітній поштовий союз спонукає застосовувати нові інформаційні технології в галузі поштового зв'язку, щоб відповідати вимогам часу, розвиткові ринку комунікацій та розширювати асортимент послуг. Однією з таких технологій є DPM – технологія цифрових поштових марок (DPM – Digital Postage Mark), що ґрунтується на застосуванні графічного (штрихового) кодування інформації [2]. Деякі передові країни, зокрема США, Канада, Німеччина, Велика Британія, Швейцарія на даний час продовжують впроваджувати у поштовій галузі власні технології, що ґрунтуються на DPM (рис. 1).



а *б* *в* *г* *д*

Рис. 1. Приклади цифрових поштових марок:
а – Швейцарії; *б* – Німеччини; *в* – Великої Британії; *г* – Канади; *д* – США.

У зазначених прикладах цифрових поштових марок застосовуються штрихові (графічні) коди PDF417 (США) та Data Matrix.

Поширені на даний час двовимірні графічні коди, в тому числі QR-код [3] дозволяють забезпечити певний рівень захисту інформації, що особливо важливо для DPM. При цьому для збільшення рівня захисту необхідно збільшувати ємність графічно-кодової позначки. Значний ефект можна отримати використовуючи для ідентифікації поштових відправлень не чорно-білий, а триколірний графічний код. Автори пропонують, як можливий варіант, застосовувати в системі поштового зв'язку України триколірний (чорно-сіро-білий) графічний код (рис. 2).

Додавання третього (сірого) кольору не призводить до необхідності застосування нових технічних засобів для виготовлення (чорно-білий принтер) та зчитування (сканер) графічно-кодованих зображень, а лише потребує модернізації програмних засобів. Проте використання трійкової (а не двійкової) системи числення в процесах створення та оброблення графічно-кодової частини DPM дозволяє істотно підвищити інформаційну щільність подання даних [4].

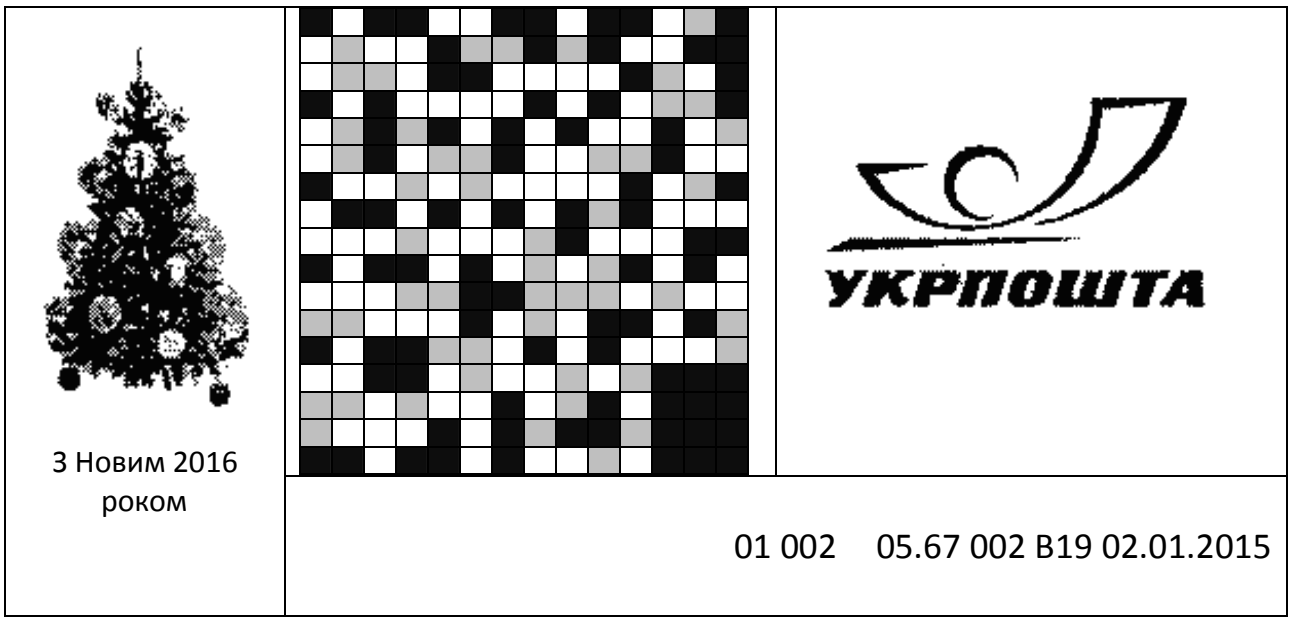


Рис. 2. Структурна організація цифрової поштової марки: 1 – зарезервована ділянка для провайдера поштових послуг, 2 – графічно-кодова (цифрова) частина,
3 – логотип, 4 – інформація у формі, придатній для читання людиною

У графічно-кодованому вигляді подаються поштові реквізити (тип та дата відправлення, вага, вартість, адреси відправника та отримувача тощо), а також службова інформація, що попередньо створені з використанням комп'ютерного алфавіту (ASCII). Для подання даних у графічно-кодованому вигляді первинне алфавітно-цифрове повідомлення має бути спочатку ущільнене, а потім, за потреби, закодоване завадостійким коректувальним кодом (рис. 3).

Рис. 3. Узагальнена схема створення графічно-кодової позначки цифрової поштової марки

ГК-позначка графічного коду складається з ГК-знаків, кожний з яких містить k примітивних елементів (елементарних квадратів).

Елементарний квадрат (комірка) може бути розфарбований в один з трьох кольорів – білий, чорний, сірий, і, отже, подає одну трійкову цифру.

Нехай об'єм ГК-позначки становить V ГК-знаків. Тоді $V \leq 3^k$. Практичний інтерес становлять значення $k = 5, 6, 7, 8$, тобто ГК-знаки, що мають структура як показано на рис. 4.

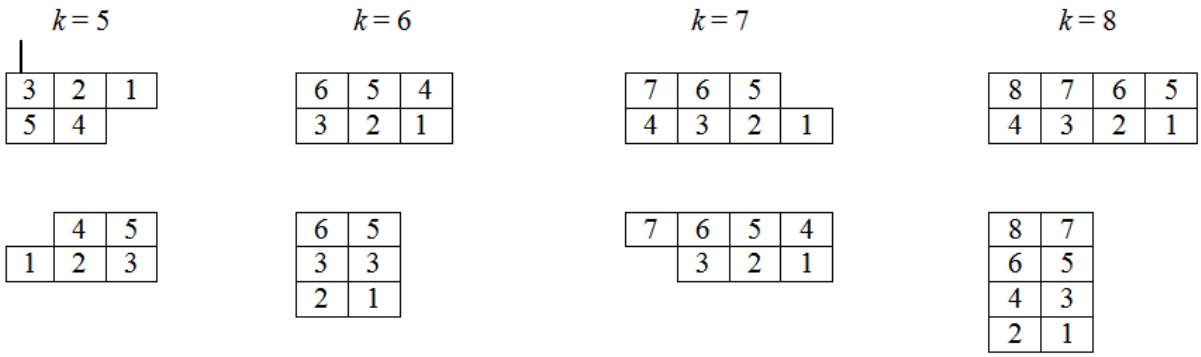


Рис. 4. Структури ГК-знаків при k = 5, 6, 7, 8

Сукупність усіх 3^k ГК-знаків утворює множину, яку називають символікою графічного коду. Їй відповідає числова множина $\Omega = \{0, 1, 2, .. , 3^k - 1\}$, тобто ГК-знаку відповідає число, що належить діапазону $0 \div 3^k - 1$.

З метою забезпечення надійного зберігання графічно-кодованої інформації пропонується кодувати дані, що підлягають поданню у графічно-кодованому вигляді, завадостійким коректувальним кодом Ріда-Соломона. Код Ріда-Соломона оперує з многозначними (а не двійковими) символами, тому числове значення ГК-знака розглядається як один многозначний символ з множини Ω [5].

При кодуванні-декодуванні даних кодом Ріда-Соломона операції над многозначними символами виконують за модулем простого числа P, де $P < 3^k - 1$.

Ущільнення повідомлення, яке належить подати у графічно-кодованому вигляді, пропонується здійснювати в такий спосіб, коли двом суміжним символам (символам ASCII) ставиться у відповідність числова величина ω, якій відповідає один ГК-знак: $\omega = ax+b$, де a, b – числові значення символів (порядкові номери символів у використовуваному алфавіті), x – потужність основного набору алфавіту. Величину ω назвемо кодовектором. Такий спосіб ущільнення передбачає поділ алфавіту на набори символів. Наприклад, в табл. 1 використовуваний алфавіт поділено на три набори.

Таблиця 1. Структурна організація алфавіту при поданні даних у графічно-кодованому вигляді

Числове значення символа	Набори символів		
	Основний (Н)	Перший додатковий (Д1)	Другий додатковий (Д2)
0	А	А	(
1	Б	В	)
2	В	С	>
.			
.			
.			
41	9	@	<
42	.	:	#
43	space	space	space
44	ПД1	ПН	ПН
45	ПД2	ПД2	ПД1

В табл. 1 x = 46, відповідно a, b Є {0, 1, 2, … 45}, а ω Є $\{0, 1, 2, \dots 46^2-1\}$, максимальне значення ω дорівнює $\omega_{max} = (x-1)x + (x-1) = x^2-1$. До складу кожного набору входять два символи-перемикачі: ПД1 – символ переходу з поточного набору в перший додатковий набір, ПД2 – символ переходу з поточного набору в другий додатковий набір, ПН – символ повернення до основного набору.

Потужність x основного набору пов'язана з потужністю символіки графічного коду таким чином: $\mathbf{x = \left[\sqrt{3^k}\right]}$, де [c] – ціла частина величини c.

Наприклад, якщо k = 7, то x = 46; якщо k = 8, то x = 80. При k = 7 потужність символіки графічного коду становить 3^7 = 2187 графічно-кодових знаків. Для ущільненого подання алфавітно-цифрових повідомлень відповідно до запропонованого способу будуть використовуватись 46^2 = 2116 ГК-знаків, решта 2187 – 2116 = 71 ГК-знаків можуть використовуватись для службових цілей.

Таким чином, вхідному алфавітно-цифровому потоку даних (вхідному повідомленню) після перетворення буде відповідати послідовність десяткових чисел – кодовекторів з множини Ω, а кожне десяткове число буде подаватись як k-розрядне 3-кове число (ГК-знак). Отримана в такий спосіб числова послідовність може безпосередньо наноситись на носій (якщо завадостійке кодування не застосовується), або оброблятись за правилами коду Ріда-Соломона, а потім наноситись на носій.

Після зчитування графічно-кодової позначки для відновлення первісного алфавітно-цифрового повідомлення здійснюються обернені перетворення.

Оцінимо ступінь ущільнення вхідних алфавітно-цифрових даних. Вхідне повідомлення завдовжки n алфавітно-цифрових символів передає 8n біт інформації. При обробленні повідомлення його довжина може зрости на q символів перемикачів ($q < n$), а після перетворення «2 → 1» становитиме $(q + n)/2$ кодовекторів, кожному з яких відповідатиме k-розрядний трійковий ГК-знак.

Тоді коефіцієнт ущільнення U вхідного повідомлення становитиме

$$U = \frac{8n}{k(n+p)/2} = \frac{16}{k} \cdot \frac{n}{n+p}.$$

Наприклад, якщо k = 7, а p = 0,2n (символ-перемикач з'являється приблизно один раз на 5 алфавітно-цифрових символів), то U = 1,9.

Використання триколірних цифрових поштових марок для ідентифікації поштових відправлень дозволить в 1,5 – 2,0 рази підвищити інформаційну щільність подання даних у графічно-кодованому вигляді порівняно з існуючими графічними кодами та забезпечить високу швидкість обробки кореспонденції в системах поштового зв'язку.

Література

1. S28 Standard: Communication of postal information using two-dimensional symbols. Universal Postal Union, 2001.

2. S36-2 Standard: Digital Postage Marks (DPM) – Applications, security and design. Universal Postal Union, 2002.

3. Голуб В.І. Щодо вибору ефективної системи автоматичної ідентифікації // Зв´язок.- 2012, №2. – С. 49-51.

4. Тринари [Електронний ресурс]: [сайт] / Троичная логика и троичная цифровая техника. – Електрон. дані. – Тринари., © 2007-2015ю – Режим доступу: http://www.trinary.ru (дата звернення: 11.09.2015).

5. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с.

УДК 621.395

Дмитрієв П.В.
ОНАЗ ім. О.С.Попова
paxa@nm.ru
Науковий керівник - доц. Царьов Р.Ю.

СИСТЕМИ МОНИТОРІНГУ ЯКОСТІ ПОСЛУГ МЕРЕЖ ЗВ'ЯЗКУ

Анотація. *В роботі аналізується необхідність застосування систем моніторингу якості послуг зв'язку .*

Високі темпи розвитку інформаційних та телекомунікаційних технологій, зростання кількості мультимедійних застосувань та відеотрафіку користувачів призведе до суттєвих змін в організації мереж доступу. Операторів, які надають послуги, турбує питання забезпечення сталої та якісної роботи мережі, у зв'язку з цим все актуальнішою стає проблема моніторингу стану мережі. Особлива увага приділяється системам спостереження та збору статистичної інформації в каналах зв'язку [1].

Саме системи моніторингу дозволяють вчасно розпізнавати та реагувати на аномалії, що відбуваються в мережі. Призначення системи моніторингу полягає в наступному: інформаційно-аналітична підтримка основних управлінських функцій розподіленої мережі передачі даних; моніторинг і контроль вилучених об'єктів, передача обробленої інформації й можливість оперативного реагування, якщо буде потреба; забезпечення оперативною моніторинговою інформацією органів керування й реагування для визначення проблемних моментів і ухвалення рішення із приводу усунення аномалій мережі.

Системи моніторингу та контролю дозволяють вирішувати наступні задачі[2]:

– цілодобовий контроль стану об'єкту моніторингу;

– виявлення інцидентів (аварій/пошкоджень) на об'єкті моніторингу;

– збір, обробка, аналіз та накопичення інформації щодо процесу технічної експлуатації об'єкту моніторингу;

– контроль та оцінка показників якості сервісів та послуг, що пропонує об'єкт експлуатації;

– формування добових/тижневих/місячних/квартальних/річних звітів щодо функціонування об'єкті моніторингу.

Системи моніторингу можна поділити на дві групи – локальні та розподілені[2,3]. Розподілені системи моніторингу є більш розповсюдженими, архітектура розподіленої системи моніторингу наведена на рисунку 1.

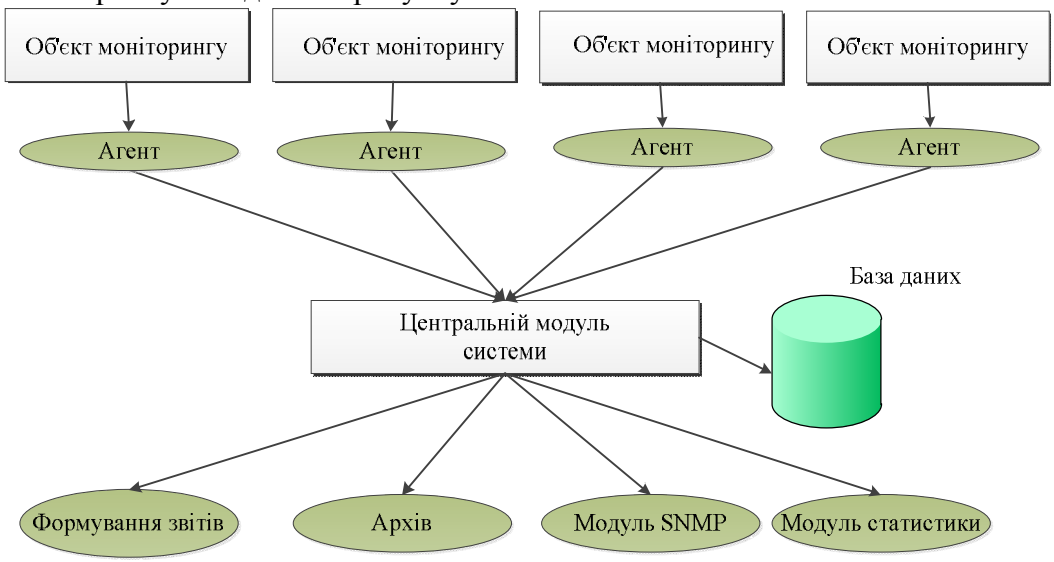


Рисунок 1 – Розподілена система моніторингу

Агенти системи контролюють стан окремих елементів об'єкту моніторингу, збирає статистику та передає до центрального модулю, який в свою чергу оброблює та аналізує отримані данні, формує звіти щодо якості роботи об'єкту моніторингу, інформує персонал про виявлені проблеми.

Приймаючи до уваги те, що система моніторингу є дуже важливим елементом мережі оператора/провайдера слід дуже ретельно підходити до процесу вибору та впровадження цієї системи.

Процес вибору та впровадження системи дистанційного моніторингу та контролю функціонування мережі дуже складний, і його доцільно розділити на декілька етапів[4]:

1. На першому етапі потрібно визначити вимоги до системи;
2. На другому етапі необхідно проаналізувати можливості представлених на ринку систем моніторингу;
3. На третьому етапі необхідно відібрати системи моніторингу, які мають найбільші функціональні можливості і в максимальному ступеню відповідають визначеним раніше вимогам.

Отже підводячи підсумки слід відзначити, що система моніторингу – це важлива складова частина мережі, яка дозволяє контролювати якість послуг, що надаються, процес вибору системи є складним і потребує наявності специфічних знань.

Література

1. Бройдо В. Л. Вычислительные системы, сети и телекоммуникации / В. Л. Пройдо. С.-П.: Питер, 2006. 702 с.

2. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем. — К.: Наук. думка, 1990. — 184 с.

3. Кузнєцова М.Г. Застосування механізмів підвищення живучості для забезпечення захищеності інформаційного ресурсу в розподілених системах // Реєстрація, зберігання і обробка даних. —2006.—Т. 8, № 3. — С. 40–47.

4. Mead N., Ellison R., Linger R., Longstaff T., Mc Hugh J. Survivable Network Analysis Method. TECHNICAL REPORT. CMU/SEI-2000-TR-013. ESC-2000-TR-013. 2000. 00tr013.pdf

УДК 621.395.7

Доброва О. А.
ОНАС им. А. С. Попова
o-dobrova@mail.ru
Научный руководитель – доц. Царёв Р. Ю.

МЕТОДИКА ВЫБОРА СИСТЕМ ФИЛЬТРАЦИИ КОНТЕНТА

Аннотация. *Работа посвящена вопросам защиты пользователей сети Интернет от потенциально опасного контента, анализируются возможные угрозы и предлагается методика выбора системы фильтрации контента для защиты от этих угроз.*

На сегодняшний день остро стоит проблема угрозы безопасности пользователя в Интернете. Использование сети Интернет позволяет расширить кругозор, развить коммуникабельность, повысить образовательный уровень. Так, посещение специальный форумов для общения со людьми из других стран позволит значительно улучшить уровень знания иностранных языков. С другой стороны, некоторая часть информации (порнография, сцены насилия, пропаганда наркотиков, алкоголя, терроризма, нацизма и т.п.), которая хранится в сети Интернет, может нанести пользователю (особенно ребенку) психологическую травму, привить ему неправильные морально-этические качества; в

результате общения в сети можно стать жертвой психологического запугивания, подвергнуться притеснению и сексуальному преследованию.

Можно выделить три группы угроз психологической безопасности детей и подростков в Интернете:

– нежелательные контакты (могут привести к финансовому мошенничеству, сексуальному преследованию);

– кибербуллинг: оскорбления, агрессивные нападки, преследования в Сети;

– «опасные» материалы (материалы террористического характера, порнография, видеоролики, изображения и тексты сексуального, экстремистского характера, призывы к насилию).

Для защиты от негативной стороны использования сети Интернет рекомендуется использовать комплексный подход, который включает организационные и технические меры [1].

К категории организационных методов защиты относятся законы, запрещающие публикацию того или иного контента, давление на интернет-провайдеров, владельцев сайтов и пользователей с целью заставить их убрать нежелательные материалы или изменить их и самоцензура.

К категории технических методов относится аппаратно-програмные комплексы, позволяющие блокировать опасные ресурсы по IP-адресу, искажение DNS-записей, блокирование сайтов по URL, пакетная фильтрация, фильтрация через HTTP прокси-сервер, фильтрация контента размещенного на сайте и фильтрация результатов поиска. Следует отметить, что на данном этапе всего лишь 20% пользователей сети Интернет прибегают к техническим средствам защиты. Это можно объяснить тем, что большинство таких средств, достаточно сложны в настройке и не могут обеспечить защиту от всех[2].

В общем случае, технические средства фильтрации контента могут применяться для следующих целей (рис. 1):

– обеспечение цензуры;

– обеспечение контроля не целевого использования времени проведено в сети интернет;

– обеспечение защиты несовершеннолетних от ресурсов опасных для него и несовместимых с моральными принципами конкретного социума;

– обеспечение выполнения/соблюдения различных социальных, культурных, правовых норм;

– обеспечение защиты авторского права (борьба с пиратством);

– обеспечение защиты экономических интересов (например, бесплатные VoIP программы и сервисы, такие как Skype, могут блокироваться, так как их использование ведет к убыткам компаний стационарной и сотовой связи);

– ведение/противодействие информационной войне.

Рисунок 1 - Сферы применения фильтрации интернет-контента

С учетом того что системы фильтрации контента могут применятся для выполнения разных задач, а так же имеют разный функционал, то процесс выбора системы становиться достаточно сложным. В связи с этим, предлагается осуществлять выбор системы фильтрации контента следующую методику:

1.Определить цель использования системы;

2. Сформировать группу факторов, которые будут применяться для оценки функциональности системы.

3. Для каждого фактора определяется весовой коэффициент β, который показывает важность характеристики и ее влияние на конечную эффективность системы (значения весовых коэффициентов определяются на основе мнений экспертов). При этом следует учитывать, что сумма всех весовых коэффициентов всех факторов равна 1:

$$\sum_{i=1}^{n} \beta_i = 1, \tag{1}$$

где $i \in [1:n]$-количество факторов, которые применяются для выбора системы фильтрации контента.

4. Сформировать экспертные оценки по каждому фактору по 10-балльной шкале;

5. Рассчитать целевую функцию γ, которая оценивает функциональные возможности работы системы:

$$\gamma = \sum_{i=1}^{n} O_i * \beta_i \rightarrow max \tag{2}$$

где O_i – *i*- й фактор, β_i,– весовой коэффициент *i*-го фактора.

Согласно мнениям экспертов, при выборе системы фильтрации контента нужно принимать во внимание следующие факторы, которые определяют итоговую эффективность системы:

- стоимость;
- простота освоения и использования (степень дружелюбности);
- прозрачность;
- мультиплатформенность (поддержка работы с разными ОС);
- блокировка по IP-адресов;
- фильтрация шифрованного трафика
- фильтрация DNS-запросов и их переадресация;
- блокировка интернет-адресов (URL);
- фильтрация контента;
- фильтрация электронной почты;
- сопровождаемость (наличие технической поддержки, обновлений).

Каждый из перечисленных факторов по своему важен, согласно экспертам, их весовые коэффициенты представлены в таблице 1.

Проиллюстрируем работу предложенной методики на конкретном примере. Пусть нам необходимо обеспечить защиту пользователей от ресурсов опасных для него и несовместимых с моральными принципами конкретного социума. Для выбора системы фильтрации контента рассматриваются следующие популярные продукты - UserGate Web Filter, Netcube, K9 Web Protection, Microsoft Forefront Threat Management Gateway. Опираясь на мнения экспертов, характеристик каждого продукта были оценен в соответсвии с предложенной методикой, результаты оценивания показаны в табл. 2.

Таблица 1 – Критерии сравнения систем

№ зп.	Критерий	Весовой коэффициент
1	Стоимость	0,15
2	Простота освоения и использования	0,1
3	Прозрачность	0,05
4	Мультиплатформенность	0,075
5	Блокировка по IP-адресов	0,075
6	Фильтрация шифрованного трафика	0,125
7	Фильтрация DNS-запросов	0,05
8	Блокировка интернет-адресов (URL);	0,075
9	Фильтрация контента	0,125
10	Фильтрация электронной почты	0,05
11	Сопровождаемость	0,125

Таблица 2– Сравнение систем фильтрации контента

№ зп.	Критерии	Весовой коэф.	UserGate Web Filter	Netcube	K9Web Protection	Microsoft Forefront Threat Management Gateway
1	Стоимость	0,15	9	7	9	7
2	Простота освоения и использования	0,1	8	4	9	6
3	Прозрачность	0,05	9	6	6	5
4	Мультиплатформенность	0,075	5	7	1	3
5	Блокировка по IP-адресов	0,075	6	4	5	4
6	Фильтрация шифрованного трафика	0,125	10	10	10	10
7	Фильтрация DNS-запросов	0,05	10	10	0	0
8	Блокировка интернет-адресов (URL);	0,075	10	7	0	9
9	Фильтрация контента	0,125	8	0	10	6
10	Фильтрация электронной почты	0,05	10	7	0	5
11	Сопровождаемость	0,125	9	7	5	8
12	Итоговый рейтинг		8,55	6,075	6,125	6,35

По результатам оценки наиболее эффективным является продукт UserGate Web Filter.

В работе предложена методика выбора оптимальной системы фильтрации контента для защиты пользователей, продемонстрирована ее работа на примере.

Литература

1. OpenNet Initiative Access Denied: The Practice and Policy of Global Internet Filtering — Cambridge: MIT Press, 2008.

2. King, Gary, Jennifer Pan, and Margaret E Roberts. (2013). How Censorship in China Allows Government Criticism but Silences Collective Expression. American Political Science Review.
3. https://www.entensys.com/ru/products/usergate-web-filter/overview
4. https://www.netcube.ru/
5. http://www1.k9webprotection.com/
6. http://www.microsoft.com/ru-ru/softmicrosoft/ThreatMG2010.aspx

УДК 621.395

Дума М.
ОНАЗ ім. О.С.Попова
camamey@ukr.net
Науковий керівник – к.т.н. Гладких В.М.

ДОСЛІДЖЕННІ ВПЛИВУ НОВІТНІХ МЕРЕЖЕВИХ СЕРВІСІВ НА ПАРАМЕТРИ ЯКОСТІ ОБСЛУГОВУВАННЯ

Анотація. *Розглядаються зміни статистичних характеристик мережевого трафіку, зумовлені значним впливом новітніх сервісів на якість обслуговування. Для дослідження цих змін розроблена імітаційна модель яка дозволяє генерувати мережевий трафік зі схожими з реальними вихідними характеристиками .*

В сучасних телекомунікаційних мережах передачі даних відбуваються зміни структури трафіку які зумовлені переходом до концепції надання сервісів WEB 2.0 та WEB 3.0[1].

Кількісно та якісно трансформування веб-сервіси впливає на користувальницький трафік[2]. Підвищення рівня інтерактивності призводить до збільшення обсягів даних, одержуваних користувачами, та до зниження межі допустимої затримки. Це призводить до необхідності проведення додаткових досліджень трафіку в сучасних мережах доступу враховуючи специфіку нових веб-сервісів.

Таким чином предметом дослідження магістерської роботи є статистичні характеристики сучасного мережевого трафіку. Мета роботи полягає в дослідженні впливу новітніх сервісів сучасних мереж доступу на параметри якості обслуговування.

Для досягнення поставленої мети:

- проведено аналіз існуючих моделей оцінки пропускної здатності і параметрів якості обслуговування мережевого трафіку;
- проведено вимір і обробка статистичних результатів виміру трафіку в сучасній мережі доступу з метою виявлення нових особливостей, викликаних появою нових сервісів;
- за допомогою імітаційного моделювання досліджено вплив статистичних характеристик трафіку на якість обслуговування з метою виявлення найбільш значущих чинників.

Найбільш придатним для моделювання мережевого трафіку на даний момент є комплекс імітаційного моделювання NS2 з програмним модулем РаскMIME[3]. Цій програмний пакет має високу продуктивність. В NS2 реалізована підтримка реального стека протоколів TCP/IP. Додатковою перевагою NS2 є відкритий програмний код і високий ступінь поширеності серед дослідників[4].

Розроблена імітаційна модель на побудована відповідно з виміряними параметрами. Вона дозволяє генерувати мережевий трафік зі схожими з реальними вихідними характеристиками, такими як: кількість переданих та прийнятих байт даних, кількість переданих запитів, кількість TCP-сесій за вказаний період часу.

Попередній аналіз результатів дозволяє зробити наступні висновки:

1. Характеристики трафіку істотно змінюються за рахунок переходу мережі Інтернет на WEB2.0.

2. Збільшення інтенсивності TCP-сесій за рахунок додаткових з'єднань, створюваних браузерами, опосередковано збільшує кількість переданих пакетів, погіршуючи параметри якості обслуговування.

3. За допомогою імітаційного моделювання були встановлені залежності середньої затримки пакету в черзі маршрутизатора і відсотка втрат пакетів від коефіцієнта використання каналу. Додаткові імітаційні моделі дозволили висунути припущення, що причина розбіжності оцінок параметрів якості обслуговування з відповідними оцінками стандартних моделей телетрафіка полягає в груповому характері надходження пакетів HTTP-трафіку, викликаного алгоритмом роботи веб-сервера.

Література

1. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы //Учебник для вузов. - Спб.: Питер, 2010. - Изд. 4-е. - 916 с.

2. O'Reilly T. What Is WEB2.0 Design Patterns and Business Models for the Next Generation of Software // http://www.oreillynet.eom/lpt/a/6228, 2005.

3. Кучерявый Е.А. NS2 как универсальное средство имитационного моделирования сетей связи // https://www.cs.tut.fi/~yk/ns2ru/ns2.pdf

4. Wiegle M. PackMime-HTTP: Web Traffic Generation in NS2 // http://www.isi.edu/nsnam/ns/doc/node552.html. 2007

УДК 621.395

Духно В.М.
ОНАЗ ім. О.С.Попова
duhnoodessa@mail.ru
Науковий керівник – к.т.н., проф. Нікітюк Л.А.

ВИЗНАЧЕННЯ ОСНОВНИХ ТЕХНІЧНИХ ХАРАКТЕРИСТИК СЕРВІСНОЇ ПЛАТФОРМИ ДЛЯ НАДАННЯ ПОСЛУГИ VoD

Анотація. *Визначаються основні технічні характеристики сервісної платформи і пропонується математична модель оптимізації сервісної платформи для надання послуги VoD, відповідно вимогам користувачів.*

Послуга VoD є досить затребувана на сьогоднішній день, завдяки практично необмеженим можливостям для формування ексклюзивних контентних пропозицій. Вона надає можливість абонентам у будь-який час за допомогою інтерактивного каталогу послуг, замовляти і переглядати відеоконтент, збережений на сервері провайдеру.

Для зручності вибору і пошуку назви програм і фільмів класифікуються в каталозі за тематичними категоріями (наприклад: драма, бойовик, комедія і т. д.). Каталог дозволяє одержати докладний опис обраного контенту (наприклад: акторський склад, ім'я режисера, тривалість, рейтинг, короткий зміст, відгуки) і, крім цього, переглянути уривок або ролик обраного фільму, для того щоб визначитися з його придбанням.

Відтворений VoD контент характеризується функціональністю, наприклад: перемотування в будь-які сторони, прискорене перемотування, відтворення з довільної позиції або визначеної сцени, «пауза», зупинка, пропуск сцен тощо, що не поступається DVD плейєрам [1].

Отже актуальним завданням стає підвищення якості надання цієї послуги шляхом зменшення часу відгуку системи на запит користувача.

Метою даної роботи є створення підходу до оптимізації сервісної платформи надання послуги VoD, шляхом зменшення часу відгуку системи на запит користувача.

Вказана ціль досягається вирішенням наступних дослідницьких задач:

1. Визначення принципів організації платформи для надання послуги VoD.
2. Дослідження існуючих технологічних рішень щодо якісного надання послуги VoD.
3. Розробка математичної моделі оптимізаціїї сервісної платформи надання послуги VoD за критерієм мінімізації часу відгуку системи на запит користувача.

Основними компонентами сервісної платформи надання послуги VoD є мережа доступу до контенту й сервер, на якому накопичується та зберігається контент (див. рис. 1).

Якісне надання послуги VoD може бути досягнуто за рахунок структурної оптимізації компонентів сервісної платформи й використання ефективних методів інженірінгу трафіку і створення контенту.

Критерієм оптимальності надання послуги є час відгуку мережі, який зводиться для того, щоб мінімізувати час перебування у черзі, та який складається з наступних параметрів:

$$T_{\text{відг}} = \overline{T_{\text{зап.}}} + \overline{T_{\text{лз}}} + \overline{T_{\text{вк}}} + T_{\text{ч.}} + T_{\text{об.сер.}} + \overline{T_{\text{кон.}}} + \overline{T_{\text{лз з.н.}}} + \overline{T_{\text{вк з.н.}}} \leq T_0; \qquad (1.1)$$

де

$\overline{T_{\text{зап.}}}$- середній час проходження запиту від абонента до сервера;

$\overline{T_{\text{лз}}}$– середній час проходження по лінії зв’язку одного запита;

$\overline{T_{\text{вк}}}$- середній час обробки на вузлах комутації одного запита;

$T_{\text{ч.}}$- час перебування запиту у черзі;

$T_{\text{об.сер.}}$- час обробки запиту на сервері;

$\overline{T_{\text{кон.}}}$- середній час проходження контента від сервера до абонента;

$\overline{T_{\text{лз з.н.}}}$- середній час проходження контенту по лінії зв’язку в зворотньому напрямі;

$\overline{T_{\text{вк з.н.}}}$- середній час обробки на вузлах комутації в зворотньому напрямі;

T_0- обмеження на час відгуку мережі;

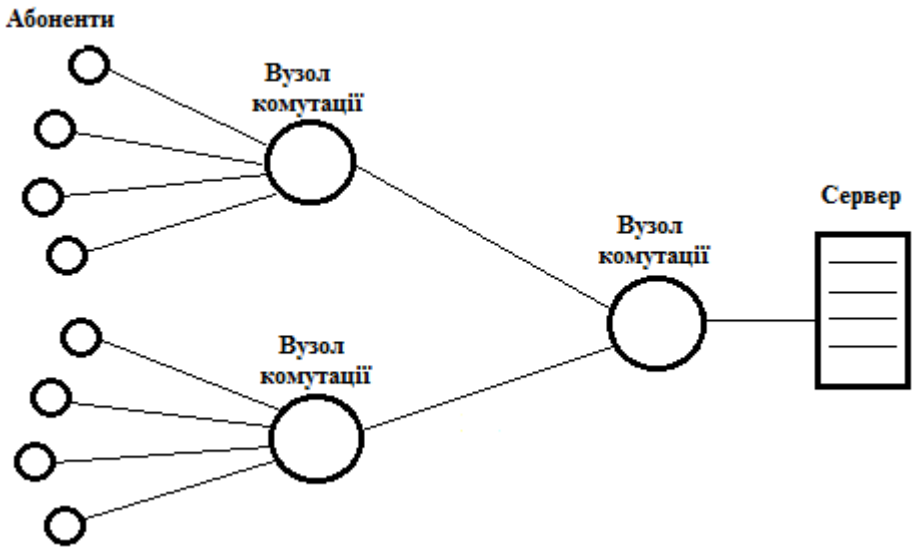


Рисунок 1 – Структурна схема сервісної платформи для надання послуги VoD

Час відгуку мережі, згідно умові (1.1) умовно можна розділити на дві частини. Час проходження запиту($\overline{T_{\text{зап.}}} + \overline{T_{\text{лз}}} + \overline{T_{\text{вк}}}$), а потім контенту по мережі($\overline{T_{\text{кон.}}} + \overline{T_{\text{лз з.н.}}} + \overline{T_{\text{вк з.н.}}}$), середній час яких має незмінний характер. Та час обробки запиту на сервері($T_{\text{ч.}} + T_{\text{об.сер.}}$), який в даній роботі буде розраховуватись для подальшого задовільнення умови.

Для рішення задачі використовуються методи теорії черг. На рисунку 2 наведено систему з чергою , що розглядається.

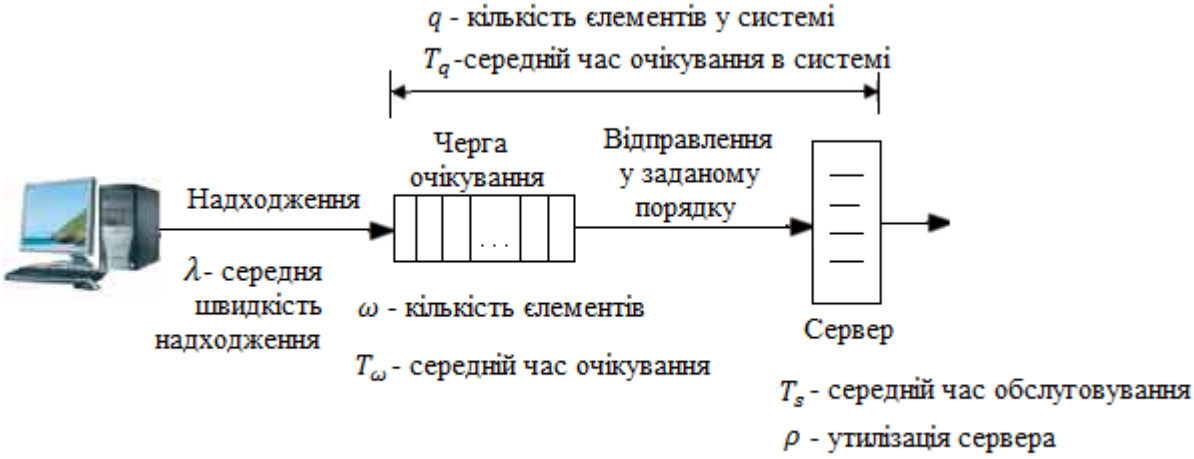


Рисунок 2 – Базова схема системи з чергами до серверу

Для розрахунків параметрів роботи системи використовується модель розподілу **M / D / 1**. Час обслуговування якої є детермінованим, за рахунок того, що система має постійний час обслуговування [2].

Враховуючи обрану модель **M / D / 1** вираз (1.1) буде мати наступний вид:

$$T_{\text{відг}} = \overline{K} + T_q \leq T_0; \quad (1.2)$$

де середній час проходження запиту по мережі у прямому,та контента у зворотньому напрямку є:

$$\overline{K} = \overline{T_{\text{зап.}}} + \overline{T_{\text{лв}}} + \overline{T_{\text{вк}}} + \overline{T_{\text{кон.}}} + \overline{T_{\text{лв.к.н.}}} + \overline{T_{\text{вк.л.н.}}}; \quad (1.3)$$

А час перебування запиту у системі, а саме час перебування у черзі та час обробки на сервері, згідно з [3], має вид:

$$T_q = \frac{T_s(2-\rho)}{2(1-\rho)}; \quad (1.4)$$

де T_s –середній час обслуговування на сервері;

ρ- утилізація сервера при обслуговуванні(частка часу , коли сервер зайнятий);

Згідно умові (1.2) виразимо час перебування запиту у черзі:

$$T_q \leq T_0 - \overline{K}; \quad (1.5)$$

Якщо параметр T_q більше ніж $(T_0 - \overline{K})$, то умова може бути виконана завдяки разпаралелюванню черзі, продублювавши контент на декількох серверах.

Таким чином кількість серверів (N_S) визначається наступним чином:

$$N_S = \frac{(T_0 - \overline{K}) \cdot 2(1-\rho)}{T_s(2-\rho)}; \quad (1.6)$$

Черга до кожного із серверів буде виконувати умову, завдяки якої користувач буде отримувати бажану послугу з відповідною якістю надання, тобто $T_{\text{відг}} \leq T_0$.

Література

1. http://library.kiwix.org/wikipedia_uk_all/A/Triple-play.html
2. Крылов В.В. Теория телетрафика и ее приложения / В.В. Крылов, С.С Самохвалова // СПб.: БХВ-Петербург, 2005.
3. Математичні основи оптимізації телекомунікаційних систем: підручник. За загальною редакцією Захарченко М.В. / Захарченко М.В., Горохов С.М., Балан М.М., Гаджієв М.М., Корчинський В.В., Ложковский А.Г. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – 240с.

УДК 004.931-932

Жуков О.А.
ХНУРЕ
aleksandr.a.zhukov@gmail.com
Науковий керівник – к.т.н., доц. Омельченко А.В.

МЕТОД ВИДІЛЕННЯ КОНТУРІВ НА ЦИФРОВИХ ЗОБРАЖЕННЯХ

***Анотація**: Розглядаються питання, пов'язані з виділенням контурів зображень, як їх попередня обробка для семантичного пошуку. Проаналізовано результати роботи існуючих операторів дискретних наближень двовимірного градієнта. Виявлено ряд проблем щодо попередньої обробки і виділення контурів для різних типів насиченості зображень. Запропоновано використовувати для кожного типу насиченості зображень найбільш підходящі параметри фільтрації та оператори.*

Для системи, яка розпізнає об'єкти на цифровому зображенні, найбільш корисною інформацією є відомості про контури зображення, що проходять на межах однорідних областей, для яких різниця яскравості будь-яких двох елементів зображення (пікселів, групи пікселів) не перевищує певного порогу. Тому, по завершенні попередньої обробки зображення, така система в першу чергу здійснює пошук контурів зображення.

Градієнтні (диференціальні) методи визначення світових кордонів (контурів) на зображенні - це методи, засновані на визначенні в кожній точці простору значень збільшення (градієнта) яскравості і напрямів найбільшої їх зміни з подальшим визначенням максимальних значень градієнта яскравості, їх статистичної обробки і поділу по порогах (рівням), що характеризує ізолінії яскравості [1].

Найбільш розповсюдженим способом пошуку контурів є обробка зображення за допомогою ковзної маски, яка являє собою якусь квадратну матрицю, що відповідає групі пікселів вихідного зображення. Оперування такою матрицею в будь-яких локальних перетвореннях називається фільтрацією або маскуванням.

У разі лінійної просторової фільтрації відгук задається сумою добутку коефіцієнтів фільтра на відповідні значення пікселів в області, покритої маскою фільтра [2]. Тобто, при використанні подібної маски відгук у кожній точці зображення задається виразом:

$$R = w_1 \cdot z_1 + w_2 \cdot z_2 + \ldots + w_n \cdot z_n = \sum_{i=1}^{n} w_i \cdot z_i \,,$$

де z_i – значення яскравості пікселя, що відповідає коефіцієнту w_i маски.

Відгук маски визначається для позиції її центрального елементу. Наприклад для маски 3x3 елемента, результат *R* лінійної фільтрації в точці (*x*,*y*) зображення складе:

$$R = w(-1,-1) f(x-1,y-1) + w(-1,0) f(x-1,y) + \ldots + w(0,0) f(x,y) + \ldots$$
$$+ w(1,0) f(x+1,y) + w(1,1) f(x+1,y+1)$$

Найбільш розповсюдженими методами виділення контурів зображень, заснованих на різних дискретних наближеннях двовимірного градієнта є оператори Робертса, Собела, Прюітт, Шарру, Хрящева та метод Канні [3].

Оператор Робертса заснований на диференціюванні амплітуди сигналу. Реалізація масок розмірами 2x2 немає чітко вираженого центрального елемента, що істотно відображається на результаті виконання фільтрації. Але є корисна властивість - висока швидкість обробки зображення.

Оператор Прюітта ґрунтується на понятті центральній різниці, але недоліком цього оператора є чутливість до шуму на зображенні.

Оператор Собеля також спирається на понятті центральної різниці, але вага центральних пікселів збільшується вдвічі та він не має повну обертальну симетрією.

Оператор Шарру дозволяє істотно знизити негативні ефекти оператора Собеля. В матрицях згортки ваги центральних пікселів перевершують ваги крайніх пікселів в 3,3 рази.

Оператор Хрящева ґрунтується на підході, за яким розраховуються матриці згортки розмірами 5×5. Вага пікселів залежить від відстані до центрального пікселя.

Основні характеристики представлених вище операторів показано у табл.1.

Таблиця 1 – Характеристики операторів виділення контурів

Назва оператору	Розмір маски	Взаємність масок	Кількість значущих елементів маски
Робертса	2×2	Так (поворот на -90°)	2
Прюітта	3×3	Так (транспонування)	6
Собеля	3×3	Так (транспонування)	6
Шарру	3×3	Так (транспонування)	6
Хрящева	5×5	Так (поворот на 90°)	18

Виділення контурів кожним з операторів для зображення наведеного на рис.1 (а) показані на рис.1 (б-е).

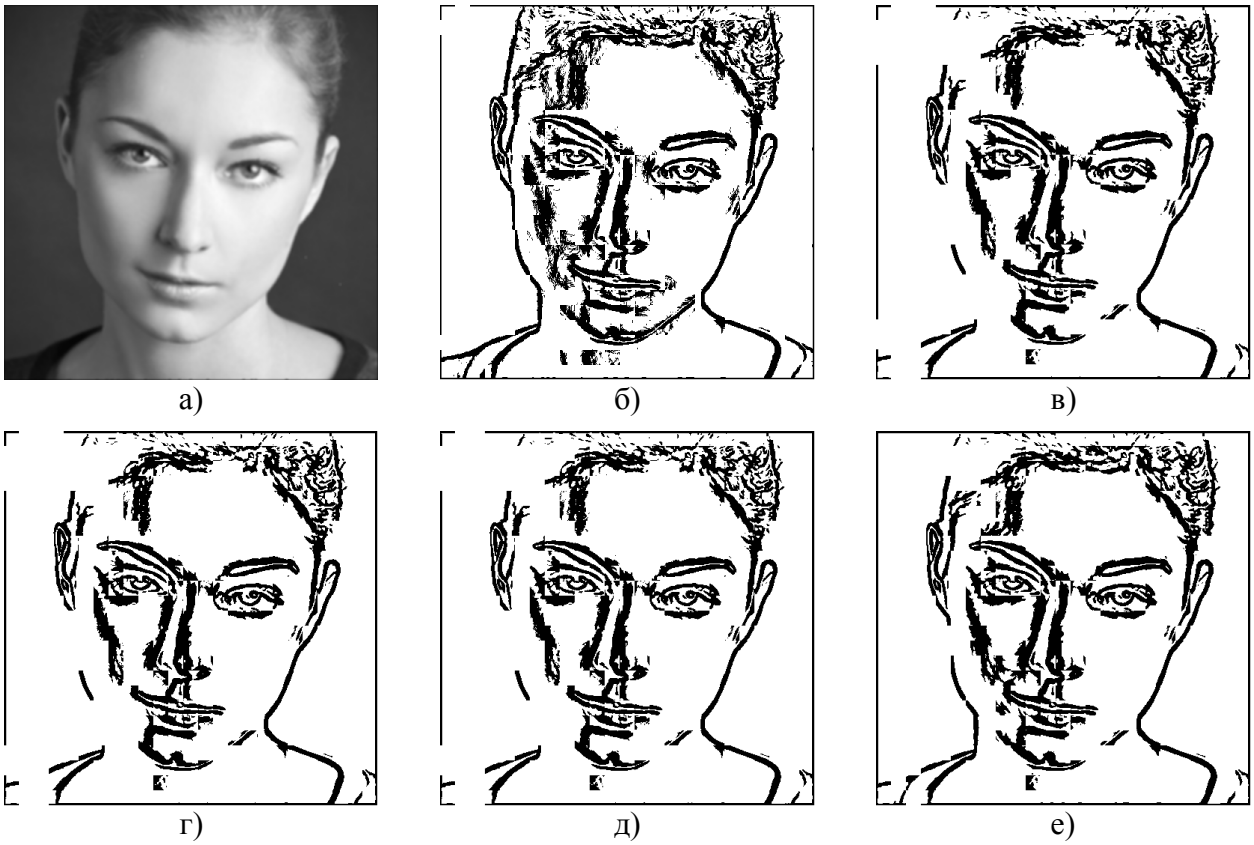


Рисунок 1 – Вихідне зображення (а), оператор Робертса (б), оператор Прюітта (в), оператор Собеля (г), оператор Шарру (д), оператор Хрящева (е)

При виділені контурів об’єктів виникає ряд проблем: завеликий час обчислення и виділення контуру, знаходження помилкових та пропуск істинних контурів, перешкоди у вигляді шуму та ін. Тому необхідно у досліджені та порівнянні існуючих операторів

виділення контурів зробити аналіз для яких типів зображень доцільно використовувати ті чи інші оператори виділення контурів.

Чутливість, специфічність, помилки першого і другого роду є вихідними величинами при побудові ROC-кривих, аналіз яких знайшов застосування і в задачі оцінки детекторів контурів.

В табл.2. представлені основні оцінки результатів виділення контурів для трьох типів зображення (слабкою, середньою та сильною насиченістю дрібними деталями), які попередньо були оброблені фільтром Гаусса, де під параметром №1 – помилка першого роду, №2 – помилка другого роду, №3 – чутливість, №4 – специфічність.

Таблиця 2 – Результати оцінки якості детектування контурів

Зображення	Параметри фільтра Гаусса	Оператор виділення контуру	Параметри			
			1	2	3	4
Літак	$size = 3,\ \sigma = 1$	Прюітта	0,06324	0,01296	0,98703	0,93675
Портрет	$size = 5,\ \sigma = 2$	Шарру	0,12034	0,20324	0,79675	0,87965
Мапа	$size = 3,\ \sigma = 1$	Собеля	0,33202	0,12995	0,87004	0,66797

Отримані результати показують, що застосування фільтра Гаусса покращує якість детектування контурів, але доцільно використовувати великий ступінь розмитості для зображень зі слабкою насиченістю, але при збільшені параметрів фільтру час виконання фільтрації збільшується приблизно в 3 рази. Всі перевірені оператори виділення контурів дають різні результати. Тому найбільш доцільним є використання оператора виділення контурів Прюітта для зображень зі слабкою насиченістю, Шарру – середньою насиченістю і Собеля для сильної насиченості дрібними деталями.

Література

1. Гонсалес Р.С., Вудс Р. Э. Цифровая обработка изображений. М.: Техносфера, 2006. 1072 с.

2. Власов А.В. Методология двухкаскадного маскирования изображений в системах инфотелекоммуникаций / Власов А.В., Ширяев А.В. // Автоматизированные системы управления и приборы автоматики. Харьков - №1 (162). – 2013. – С. 31 – 36.

3. Баранник В.В. Анализ методов обнаружения границ объектов на изображениях и их классификация / В.В. Баранник, А.В. Власов // Сучасна спеціальна техніка. 2012. №3. С. 17-27.

УДК 004.045:621.396.967.2

Заволодько Г.Е.
НТУ "ХПІ"
ann.zavolodko@gmail.com

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПІДВИЩЕННЯ ЯКОСТІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СПОЖИВАЧІВ СИСТЕМАМИ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

Анотація. *Наводиться аналіз показників якості виявлення траєкторії повітряних об'єктів за даними вторинних систем спостереження повітряного простору у єдиній постановці питання виявлення, як одного із складових інтегрального показника якості інформаційного забезпечення у даній інформаційній системі: виявлювач імпульсів відповіді, виявлювач сигналів відповіді, виявлювач повітряного об'єкта та власне виявлювач траєкторій.*

Основними елементами процедури контролю повітряного простору (ПП) є аналіз повітряної обстановки й прийняття рішень. Рішення приймає особа на основі аналізу, відповідним чином підготовленої інформації, про стан повітряної обстановки. Правильне рішення може бути прийнято лише тоді, коли є досить повна, точна, достовірна й безперервна інформація про повітряну обстановку в зоні управління. Отже, якість прийняття рішень визначаються якістю й складом інформації, на основі якої особа приймає рішення.

Підвищення надійності інформаційного забезпечення (ІЗ) користувачів системи контролю ПП неможливо без використання інформаційних технологій (ІТ) у процесі отримання, збору, обробки, збереження й розповсюдження аеронавігаційних даних. Природна еволюція призводить до об'єднання СС чи інших датчиків інформації, розосереджених на певній ділянці контрольованого простору, в інформаційну мережу [1]. Основним джерелом інформації про повітряну обстановку в системі контролю використання ПП є системи спостереження (СС), які розділяються на первинні та вторинні (запитальні) [1,2]. При цьому слід зазначити, що ведучою є первинна СС. Інформація вторинної СС використається при формування формуляру повітряного об’єкту (ПО) на етапі первинної обробки інформації.

Зміна структури ІЗ яка обумовлена переходом до автоматичного залежного спостереження дещо змінює підхід до ІЗ споживачів. Дійсно, перехід вторинних СС до основних джерел інформації ставить задачу супроводу ПО за даними цих СС. Необхідно також відзначити, що раніше функція супроводу ПО вирішувалася на основі інформації первинних СС. Якщо теорія і практика побудови фільтрів супроводу ПО за даними первинних СС досить докладно розглянута в існуючій технічній літературі, то розгляд цих питань для вторинних СС має деякі пробіли. Дійсно, специфіка побудови вторинних СС зумовила наявність деяких параметрів, які відсутні в первинних СС [3].

Слід зазначити, що вторинна обробка інформації в системі контролю використання повітряного простору завжди виконувалася з використанням ІТ. Успіхи у широкому використані цифрової обробки сигналів дозволили використати ІТ з етапу первинної обробки інформації, що забезпечило:

- підвищення ефективность ІЗ споживачів;
- здійснити сумісну оптимізацію обробки сигналів та даних.

Існуючі вторинні СС збудовані за принципом несинхронної мережі, обслуговування першого вірно прийнятого сигналу запиту (СЗ) та відкритої системи масового обслуговування з відмовами [3]. Така побудова останніх відчиняє широкі можливості з несанкціонованого використання відповідачів цих систем, а також для повної паралізації шляхом постановки корельованих завад необхідної інтенсивності. При роботі відповідача тільки в полі дії багатьох вторинних СС, що створюють внутрішньосистемні завади, коефіцієнт готовності відповідача (КГ) P_0 завжди менше одиниці. КГ відповідача залежить від інтенсивності потоку ЗС, утвореного потоком ЗС від запитальних СС, потоком навмисних корельованих завад, а також потоком ЗС, що утворився з потоку навмисних і ненавмисних некорельованих завад.

Будемо вважати, що на вхід СС можуть надходити флуктуаційні й імпульсні (хаотичні, внутрішньосистемні й т.д.) завади. Проведемо порівняльний аналіз ймовірності виявлення трас ПО за даними вторинних СС виявлювачем що синтезованого в [4]. Модульність побудови виявлювача трас ПО дозволяє розглядати цю структуру в наступних послідовностях попередніх виявлень:

а) виявлювач ПО - виявлювач СВ - виявлювач траси ПО (І варіант);

б) виявлювач СВ - виявлювач ПО - виявлювач траси ПО (ІІ варіант);

в) виявлювач ПО - виявлювач траси ПО - виявлювач ОС - (ІІІ варіант).

Отримаємо вирази для виявлення трас ПО при використанні першого варіанту.

Нехай у виявлювачі ПО використовується логіка K/N, для виконання якої необхідна наявність імпульсів СВ на одних і тих же ділянках дальності K із N запитів (K виступає в

якості цифрового порога). У пристрої виявлення СВ застосовується логіка n/n, для виконання якої потрібна наявність усіх імпульсів в кожній повторній посилки. У пристрої виявлення траєкторій використовуються критерії виявлення траєкторій l/m.

Тоді ймовірність D_1 виявлення ПО за результатами виявлення одиночним СВ для зазначеної логіки визначається як

$$D_1 = \sum_{i=0}^{N-K} C_N^i P_0^{N-i} (1-P_0)^i \sum_{i=0}^{N-K-i} C_{N-i}^l P_1^{N-l-i} (1-P_1)^l,$$

де P_1 - ймовірність виявлення одиночних імпульсів СВ.

Ймовірність виявлення СВ можна визначити з наступного виразу

$$D_{11} = \sum_{i=0}^{N-K} C_N^i P_0^{N-i} (1-P_0)^i \left[\sum_{l=0}^{N-K-i} C_{N-i}^l P_1^{N-l-i} (1-P_1)^l \right]^n,$$

Ймовірність виявлення траси ПО вторинною СС для аналізованого варіанта побудови можна визначити з наступного виразу

$$D_{111} = \sum_{i=1}^{m} C_m^i D_{11}^i (1-D_{11})^{m-i}. \quad (1)$$

Отримаємо вирази для виявлення трас ПО для другого варіанта побудови виявлювача.

Ймовірність D_2 виявлення n-імпульсних СВ визначається як

$$D_2 = P_1^n P_0.$$

Ймовірність виявлення ПО на виході виявлювача ПО визначається як

$$D_{22} = \sum_{i=0}^{N-K} C_N^i (P_0 P_1^n)^i.$$

Ймовірність виявлення траси ПО на виході виявлювана траси визначається як:

$$D_{222} = \sum_{i=1}^{m} C_m^i D_{22}^i (1-D_{22})^{m-i}. \quad (2)$$

Отримаємо вирази для виявлення траси ПО в третьому варіанті побудови виявлювача.

Ймовірність виявлення ПО на підставі результатів виявлення одиночних СВ визначається як

$$D_3 = \sum_{i=0}^{N-K} C_N^i P_0^{N-i} (1-P_0)^i \sum_{l=0}^{N-K-i} C_{N-i}^l P_1^{N-l-i} (1-P_1)^l.$$

Ймовірність виявлення траси ПО за одиночним ВС можна визначити як:

$$D_{33} = \sum_{i=1}^{m} C_m^i D_3^i (1-D_3)^{m-i}.$$

Ймовірність виявлення траси ПО на виході виявлювача визначається як

$$D_{333} = D_{33}^n. \quad (3)$$

Оцінимо вплив флуктуаційної завади у каналі СВ, КГ ЛВ вторинних СС і критерію виявлення траси на значення цифрового порога виявлення ПО запитальних СС для пачки СВ рівний 25.

Представлені на рис.1-3 залежності дозволяють проводити порівняльний аналіз існуючих і перспективних вторинних СС за якістю виявлення трас ПО при дії у каналі відповіді флуктуаційних і імпульсних завад.

Представлені порівняльні характеристики якості виявлення трас ПО вторинними СС показали, що перший варіант виявлювача найбільш кращий в порівнянні з іншими, розглянутими в роботі. Дійсно, така структура виявлювача трас ПО найменш чутлива до

негативної дії КГ відповідача запитальних СС.

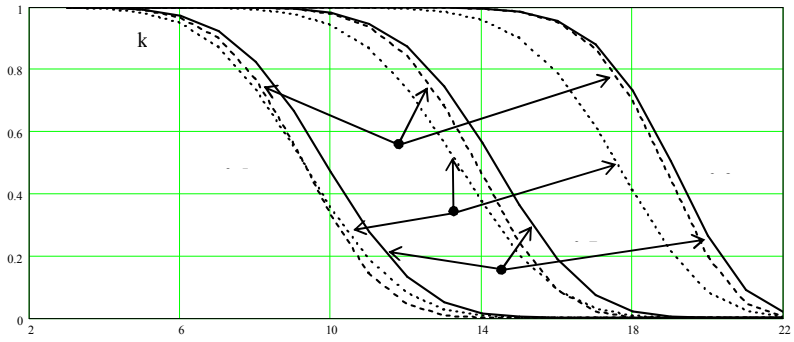


Рис.1. Імовірність виявлення траси ПО

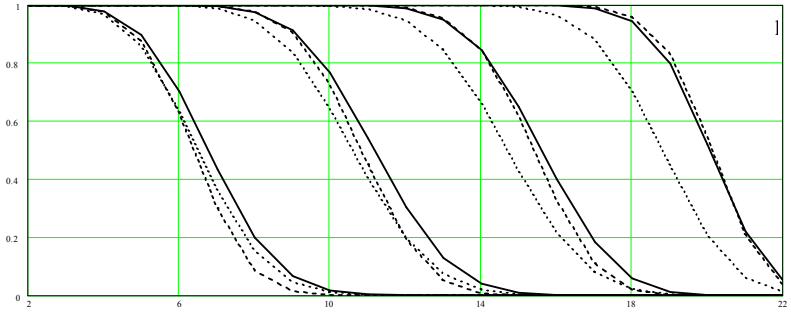


Рис.2. Імовірність виявлення траси ПО

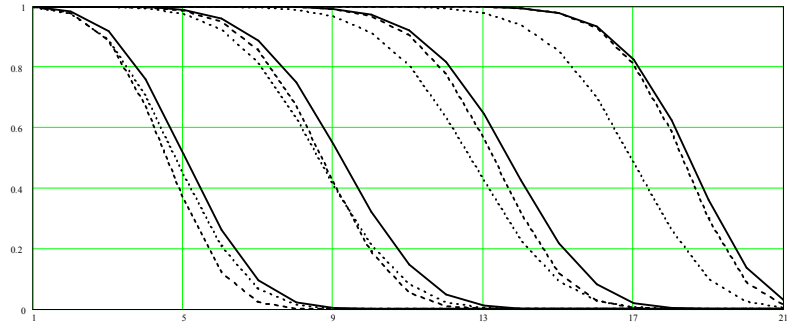


Рис.3. Імовірність виявлення траси ПО

Дослідження, яки наведені вище дозволяють зробити наступні висновки:

- використання ІТ з етапу первинної обробки інформації забезпечило можливість оптимізувати виявлення СВ та трас ПО на основі критерію Неймана-Пірсона;
- обрати оптимальну структуру виявлювача ПО за критерієм мінімізації впливу КГ ЛВ на якість ІЗ.

Література

1. Обод І.І. Інформаційна мережа систем спостереження повітряного простору / І.І.Обод, О.О.Стрельницький, В.А.Андрусевич. – Харків.:ХНУРЕ, 2015.- 270 с.

2. Комплексне інформаційне забезпечення систем управління польотами авіації та протиповітряної оборони / В.В.Ткачев, Ю.Г.Даник, С.А. Жуков, І.І.Обод, І.О. Романенко. – К.: МОУ, 2004. -342 с.

3. Обод І.І. Завадозахищеність запитальних систем спостереження повітряного простору / І.І.Обод, І.В.Свид, І.А.Штих. – Харків.:ХНУРЕ, 2014.- 310 с.

4. Обод І.І. Синтез квазиоптимального обнаружителя трасс воздушных объектов запросными системами наблюдений единой информационной сети / І.І.Обод, А.Э Заволодько. – Системи обробки інформації: Збірник наукових праць. - Вип. 2(76). – Х.: ХУПС. -2009. - С. 72-74.

УДК 621.395.7

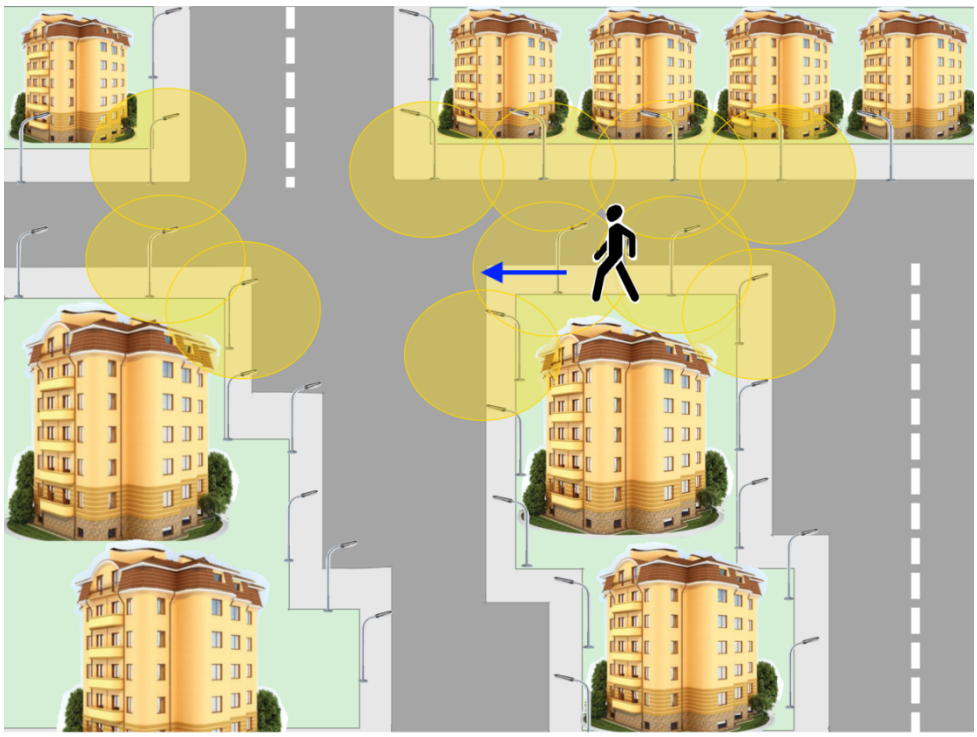
Карюхина В.С.
ОНАС им. А.С. Попова
karukhina@inbox.ru
Научный руководитель – проф. Сименс Э.,
к.т.н., с.н.с. Каптур В.А.

SMARTLIGHTING SYSTEM

Abstract. *SmartLighting is the system of street lighting target for economical consumption of the necessary power. In the article the following issues are represented: practical necessity for development of SmartLighting system, possible benefits after implementation of this system, the main principles of the system and challenges that should be done during a work under the project.*

For today the question of saving ecological conditions has high priority. Whatever the security issue on the night time is also very important. Thus, there is dilemma. How to satisfy two requirements: supply necessary amount of the light for streets during night and save amount of electrical energy as much as it possible. To optimize energy usage FILA group on the base of Anhalt University of Applied Science in Köthen (Germany) developed concept of the SmartLighting system.

The goal of the project is to create a large-scale wireless sensor network over the existing street lighting infrastructure in order to create a SmartLighting system. In this system the maximum amount of power will be used only at the spots, at which it is needed and only when it is needed. The system fully relies on pedestrians' traffic, calculates and provides necessary lighting zones depending on their movement direction, while the street areas without any movements remaining unlighted. This leads to a decrease of overall street lamps' working time, saving a huge amount of energy and prolonging the lamps' life cycle.



Pic.1 – Main principle of SmartLighting system

During the work on SmartLighting project the following challenges must be solved:

1. HID lamps based system and optimization of its control in the SmartLighting environment

With the consistent improvement of LED light sources they gradually substitute HID metal halide and incandescent lamps, which dominate today's outdoor lighting systems. Nevertheless HID lamps will be used and produced f or at least 30 years more due to cost intensity of transition to LEDs. Therefore, expanding SmartLighting concept to HID lamps still can potentially give economical benefits. But using HID lamps in a SmartLighting system is associated with a range of challenges. This type of lamps requires special treatment: high warm up time (up to 5 minutes for metal halides), high starting voltage, negative differential resistance, inability to immediately restart the lamp after turning it off, lamp life deterioration after a certain amount of on/off and dimming cycles – all it makes HID lamps SmartLighting unfriendly. Research must be conducted to find if there is a way to effectively handle them in a SmartLighting system without significantly affecting lamps characteristics while at the same time using the full functionality of SmartLighting**.** To perform such a test-bed which represents a scenario close to real conditions will be created. On the basis of this test-bed effects of frequent dimming with different voltage ramp-up/down speeds will be thoroughly studied. This investigation will give a hint on how to better control the lamps in a SmartLighting system. It will help to balance influence of dimming on lamp's life with power efficacy dimming gives, to achieve greater economical benefits.

2. Protocols for multi-hop data routing in wireless ad-hoc networks

SmartLighting system represents a use-case scenario of a static wireless ad-hoc network. Each node has its own CPU and continuously generates data (service data, control data, payload) which must be shared between all nodes. For today it was decided to use WLAN network of IEEE 802.11s standard with HWMP routing protocol, or, as an alternative, the WiFi ad-hoc mode with OLSR routing. In the further development, the specially tailored protocol will be integrated into the SmartLighting system to optimize data transmission. Data packets will include information about neighbours' addresses, their geographical positions, data from motion sensors, information about failing of the spot, synchronization data, etc.

3. Autoconfiguration and topology discovery algorithms for sensor network

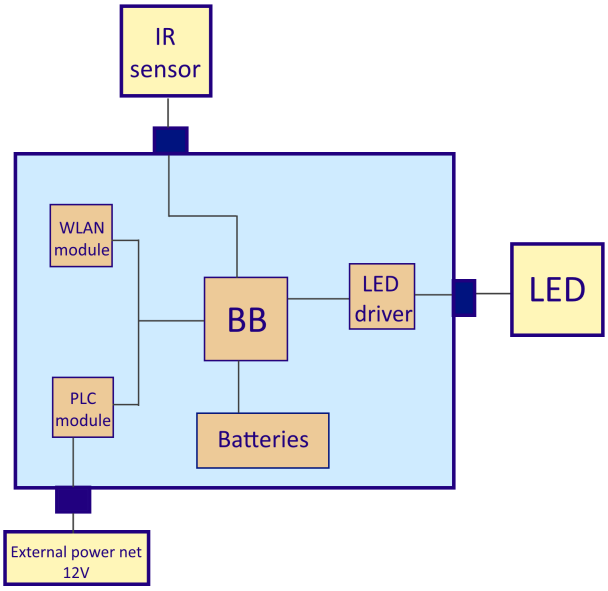
It goes without saying that such sensor network will include a lot of nodes. When the quantity of elements increases, it becomes more complex to configure each node separately in manual mode. To make this network scalable, it is necessary to support autoconfiguration functionality. One of the features of the proposed project is an original implementation of the addressing scheme, based on special formatting of IPv6 header. Each node will be assigned with a unique IPv6 header, containing information about the node's geographical position, forwarding direction and the node's ID. Such implementation scheme will decrease total load on the application layer, reducing the data overhead and, therefore, improving overall sensor network performance.

4. Software testing

One of the most important parts for project development process is a testing of the system on the virtual space. For this purpose the software should be developed to represent the result of proper work of routing protocol, autoconfiguration feature, etc. Testing application should have a space for building different topology, source and destination nodes, traffic generator, and graphical representation of the main principle of SmartLighting system work.

5. Prototype of a LED based system with 20 lamps interconnected

The main architecting idea of the prototype is to transmit the signal form the infrared sensor through BeagleBone to WLAN module or to PLC (power line communication) module for further transmission trough the network. At the output the LED will illuminate to show reaction on the signal going from the infrared sensor. The first point that should be under the testing is the routing and autoconfiguration process. All existing data of concrete node is stored and processed on the BB (system on chip based PC). After testing stage it will be possible to analyse and detect drawbacks, correct them and present a ready to use product.



Pic.2 – SmartLighting design scheme

The goal of the project in the global scale is to integrate such SmartLighting system into lighting systems of cities. It will give comfort lightning conditions for pedestrians during night time. Moreover it will give ability to save the nature resources in order to reduce power consumption.

References

1. S. Zinov, E. Siemens, The Smart Lighting Concept. Proceeding of the first Workshop on Problems of Autonomous Power Systems in the Siberian Region. Köthen, 2013.

2. D. Dugaev A wireless mesh network NS-3 simulation model: implementation and performance comparison with a real test-bed. Proceedings of 2nd ICAIIT conference, Köthen, Germany, 2014.

3. D. Dugaev, S. Zinov, E.Siemens, V. Shuvalov, A survey and performance evaluation of ad-hoc multi-hop routing protocols for static outdoor networks. Proceeding of: International Siberian Conference on Control and Communications (IEEE SIBCON-2015) Omsk, Russia, 2015.

УДК 621.396

Климач М.М.
ОНАЗ ім.. О.С. Попова
klumach@ukr.net
Науковий керівник – доцент Шерепа І.В.

ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНКИ ЯКОСТІ НАДАННЯ ПОСЛУГ VoIP

Анотація. *Розглядаються суб'єктивні і об'єктивні методи оцінки якості VoIP. Досліджується метод обчислення MOS використовуючи штучну нейронну мережу. Вирішується завдання обчислення MOS використовуючи тільки показники QoS мережі.*

Одна з найбільших технічних проблем при передачі голосу і відео по мережах з пакетною комутацією, полягає в забезпеченні гарантованої якості обслуговування (QoS), що дозволяє отримати звук і зображення без спотворень і перешкод[1]. Більшість існуючих мереж з пакетною комутацією побудована для виконання завдань і додатків не чутливих до затримки сигналу. Голос і відео навпаки дуже вимогливі до швидкості передачі інформації, і

затримка пакету більша, ніж на 200 мс, означає, що цей пакет вже не потрібний, оскільки дані встигли застаріти. Отже, мережі для передачі голосу і відео мають бути розроблені, побудовані так, щоб максимально збільшити ефективність проходження пакетів з урахуванням вимог QoS. Актуальною залишається проблема оцінки якості послуг в мережах IP[2].

Забезпечення якості обслуговування (QoS) є основною вимогою при реалізації послуг мультимедійного трафіку. Завдання забезпечення якості обслуговування полягає в гарантуванні передачі пакетів з визначеною затримкою, та кількістю втрачених пакетів.

Основними характеристиками QoS визначаються: - затримка доставки пакету. Цей параметр відіграє роль в основному при передачі голосових і відео-повідомлень;- джиттер - зміни в затримках при доставці пакету; - втрата пакету - при перевантаженні, мережа вимушена викинути окремі пакети.

Вимірювання якості мовного повідомлення здійснюється з використанням суб'єктивних та об'єктивних методів.

Традиційно, суб'єктивна якість голосу визначається шляхом експертної оцінки і підрахунком середнього балу MOS (від англ. Mean Opinion Score) від 1 до 5 (шкала ITU), де 1 - найгірше, а 5 - найкраще отримане якість голосу. Цей підхід, однак, вимагає певних експертних навичок і тому не використовується в автоматизованих системах.

Серед об'єктивних методів оцінювання варто виділити прийняту в 2012 р МСЕ Рекомендацію G.107, в якій був описаний підхід до оцінки якості послуг у телекомунікаціях.. Результатом обчислень відповідно до E-моделлю є число, зване R-фактором ("коефіцієнтом рейтингу"). Значення R-фактору однозначно зіставляються з оцінками MOS.

При розрахунку R-фактора враховуються 20 параметрів, в числі яких:

- затримка пакетів;
- коефіцієнт втрати пакетів;
- втрати даних через переповнення джиттер буфера;
- спотворення, що вносяться при перетворенні аналогового сигналу в цифровий і наступному стисканні (обробка сигналу в кодеках) та ін.

Таким чином, E-модель і R-фактор можуть бути використані для об'єктивної оцінки якості передачі мови в технології VoIP.

Проте практична реалізація E-моделі викликає труднощі, пов'язані з великою кількістю математичних обчислень, необхідністю наявності вхідного мовного повідомлення та інше.

Проблему визначення та передбачення якості передачі мови в мережах IP можуть вирішити штучні нейронні мережі (ШНМ). У магістерській роботі розроблена і реалізована програма, що працює за принципом нейронних мереж і дозволяє об'єктивно оцінити якість мови, переданої по IP мережах.

Розглянемо формалізовану модель штучного нейрона. Штучний нейрон складається з синапсів, кожному з яких відповідає певна вага синаптичного зв'язку, суматора і функції активації[3].

Математично цю модель можна записати у вигляді:

$$y = \varphi(\sum_{i=1}^{N} w_i x_i + b)$$

де - $x_1 ... x_n$ - вхідні сигнали, $w_1 ... w_n$ - синаптичні ваги нейрона; b - порогове значення; y - вихідний сигнал нейрона; $\varphi(v)$ - функція активації. Запропонована нейронна мережа має двошарову архітектуру. Вхідними сигналами ШНМ ($x_1 ... x_n$) є параметри QoS (затримка, втрати пакетів, джитер та інші), а також спотворення, що виникають в кодеку.

На початковій стадії моделювання та навчання нейронної мережі застосовувалися порогові функції активації:

$$\varphi(v) = \begin{cases} 1, v \geq 0; \\ 0, v < 0; \end{cases}$$

Надалі навчання нейронної мережі проходило методом зворотного поширення помилки (backpropagation). В якості тестових зразків використовувалися зразки ITU-T Test Signals for Telecommunication Systems [4].

Для спотворення тестових зразків використовувалося вільно поширюване програмне забезпечення WANem [5]. Це програмне забезпечення дозволяє імітувати роботу мережі з різними показниками QoS.

Тестові і відповідні їм спотворені сигнали оброблялися згідно з алгоритмом PESQ і визначався показник MOS спотворених сигналів. Всі спотворені мовні сигнали записувалися.

Надалі порівнювалися показники MOS отримані за допомогою алгоритму PESQ і розробленого програмного забезпечення.

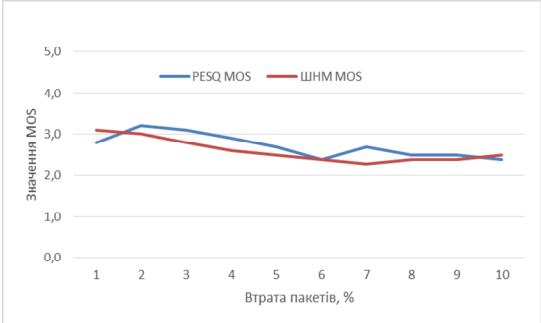


Рис.1

На рис.1 показано приклад порівняння значень MOS для кодека G.729, отриманих за допомогою алгоритму PESQ та розробленої ШНМ.

Висновки. Запропоновано модель для розрахунку MOS, використовуючи ШНМ. Вирішувалося завдання обчислення MOS без використання оригінального мовного сигналу, використовуючи тільки відомі мережеві показники якості обслуговування. У проведеному дослідженні змінювався відсоток втрати пакетів і час затримки. Інші параметри (наприклад, джитер) залишалися незмінними. Також MOS обчислювався для різних кодеків, що використовують для кодування мовного сигналу. Результати досліджень вказують на можливість використання ШНМ при обчисленні показника MOS.

Література

1. Яновский Г.Г. Качество обслуживания в сетях IP // Вестник связи. – 2008. – №1. – с. 1–16.
2. Яновский Г.Г. Оценка качества передачи речи в сетях IP // Вестник связи. – 2008. – №2. – с. 4–12.
3. Саймон Хайкин Нейронные сети. Полный курс // Вильямс/ - 2006. –с. 28-33
4. http://www.itu.int/net/itu-t/sigdb/genaudio/AudioForm-g.aspx?val=1000050
5. http://wanem.sourceforge.net/

УДК 621.396

Костянтинов К.В.
ОНАЗ ім. О.С.Попова
bolgrad06@mail.ru
Науковий керівник - д.т.н., проф. Лісовий І.П.

АНАЛІЗ ШЛЯХІВ ПЕРЕХОДУ ДО МЕРЕЖ НАСТУПНОГО ПОКОЛІННЯ

Аннотация. Робота присвячена дослідженню відношення сигнал / шум оптичного сигналу транспортної мережі з маршрутизацією за довжиною хвиль при реальних параметрах передачі.

Транспортна мережа повинна забезпечувати наступні процедури, прийняті в NGN : розподіл трафіку , вирівнювання навантаження , маршрутизацію трафіку , по зв'язках різної топології (« точка- точка » , « точка- многоточка » тощо) , дублювання трафіку , мультиплексування (об'єднання) і демультиплексирование (поділ) і т.д. Чим успішніше

обслуговує технологія транспортної мережі пакетний графік , тим ефективніше технічне рішення .

Реалізація оптичної транспортної мережі нового покоління є дуже складним завданням. Тут потрібна підтримка розширюється різноманітності клієнтських сигналів з одночасно змінюються вимогами, такими як гарантується якість обслуговування (Quality Of Service - QoS), гнучкість, масштабованість і живучість, пов'язану зі швидкістю передачі даних і незалежністю протоколу.

У цифрових системах передачі одним з основних параметрів для оцінки якості переданого сигналу є ймовірність помилок (Bit Error Ratio - BER). А величина BER безпосередньо пов'язана з відношенням сигнал / шум оптичного сигналу (Optical Signal-To-Noise Ratio - OSNR). Тому, знаючи значення OSNR, можна судити про якість сигналу.

У роботі виконано аналіз OSNR для лінії передачі, що містить тільки оптичні підсилювачі.

Згідно Рекомендації MCE-T G696.1, OSNR M-канальної ВОСП-WDM з кількістю підсилювальних ділянок N_{span} , що містить додатковий підсилювач потужності, (N_{span}–1) лінійних підсилювачів і попередній підсилювач, можна розрахувати за наступною формулою:

$$OSNR = P_{out} - 10\lg M_{ch} - \alpha_s - NF_{ASE} - 10\lg\left(N_{span} + \frac{10^{0,1\cdot G_{BA}}}{10^{0,1\cdot \alpha_S}}\right) - 10\lg(hf\cdot\Delta f_{ch}), \quad (1)$$

де P_{out} - рівень вихідної потужності групового сигналу в дБм;

M_{ch} – кількість оптичних трактів у волокні;

αs – загасання оптичного сигналу на одній дільниці підсилення в дБ;

NF_{ASE} - коефіцієнт шуму оптичного підсилювача, обумовлений посиленою спонтанної емісією (Amplified Spontaneous Emission - ASE) в дБ;

N_{span} – кількість підсилювальних дільниць;

G_{BA} - коефіцієнт підсилення підсилювача потужності;

h - постійна Планка;

f - частота, відповідна довжині хвилі 1.55 мкм;

Δf_{ch} - смуга частот оптичного тракту.

При швидкості передачі даних в одному оптичному тракті 10 Гбіт /с і беручи до уваги, що величина OSNR обмежена 24 дБ для ймовірності помилки 10^{-12} , дальність зв'язку складає 3 підсилювальні дільниці (Рис. 1).

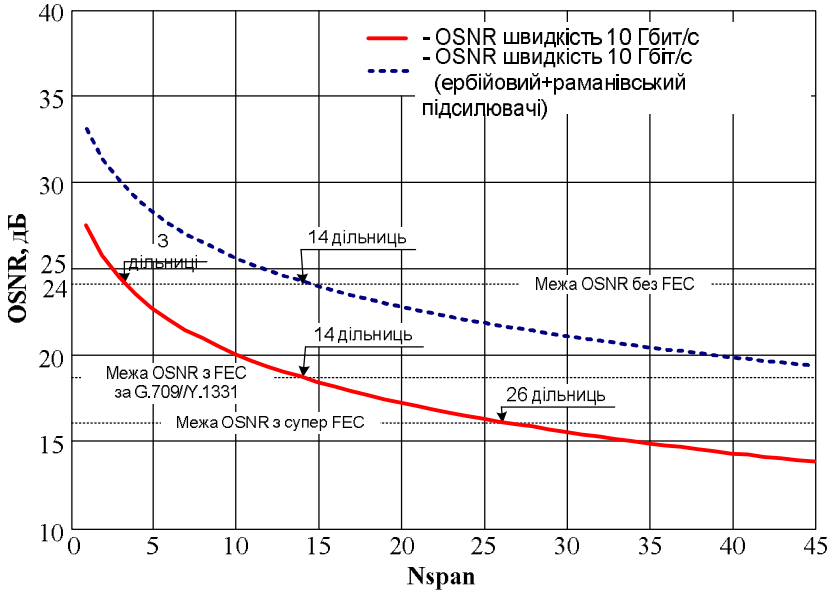


Рисунок - 1 Залежність OSNR від кількості підсилювальних дільниць N_{span} для STM-64, $P_{ch.out}$ = 3дБм, α_s = 22дБ, NF_{ASE} = 6.5 дБ

Розподілене раманівське підсилення (РРУ) є додатковою можливістю для збільшення дальності передачі. Виграш OSNR, очікуваний від використання РРУ в конфігурації підсилювача з накачуванням зустрічною хвилею, може бути розрахований з використанням ефективного коефіцієнта шуму NF_{eff}.

Максимальну дальність зв'язку з використанням ербійових та раманівських підсилювачів можна визначити шляхом підстановки NF_{eff} замість NF_{ASE} в формулу (1) і враховуючи, що $\alpha_s = G_{Raman} + G_{LA}$, де G_{Raman} - коефіцієнт підсилення раманівського підсилювача, а G_{LA} - коефіцієнт посилення лінійного підсилювача.

Припускаючи раманівське посилення рівним 9.3 дБ і коефіцієнт шуму ербієвого підсилювача 6.5 дБ, ефективний коефіцієнт шуму NF_{eff} дорівнює 1 дБ (штрихова лінія на рис. 1).

Висновок. В даний час теоретична гранична дальність передачі з використанням комбінації з ербієвого і раманівського підсилювачів без застосування кодів, що виправляють помилки (Forward Error Correction - FEC) досягає 14 підсилювальних ділянок (по 22 дБ). Застосування кодів, що виправляють помилки, наприклад, згідно рекомендацій МСЕ-Т G.709 / Y .1331 дозволяє створити систему з 40 підсилювальними ділянками.

Література

3. Иванов А.Б. Волоконная оптика. Компоненты, системы передачи, измерения. – М.: Syrus Systems, 1999. - 672 с.

4. Р. Фриман Волоконно-оптические системы связи. // ТЕХНОСФЕРА, Москва. – 2004. С. 371.

УДК 621.395

Коц Ю.В.
ОНАЗ ім. О.С.Попова
yuliyakots@yandex.ru
Науковий керівник – к.т.н., проф. Нікітюк Л.А.

ДОСЛІДЖЕННЯ МЕТОДІВ РОЗРОБКИ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОКОМУНІКАЦІЯХ

Анотація. *Проводилось дослідження основних концепцій систем штучного інтелекту в інфокомунікаціях. Розглядались функціональні можливості систем ШІ. Проводилась оцінка та аналіз ефективності впровадження інтелектуальних систем управління в інфокомунікаціях.*

Застосування систем штучного інтелекту – новий потенціальний напрямок у інфокомунікаціях. Зважаючи на те, що сучасні інфокомунікаційні мережі достатньо складні, працюють зі значними масивами даних, надають широкий спектр послуг та включають в себе велику кількість пристроїв, підходи, що застосовувалися раніше, не є раціональними. Отже набувають актуальності інтелектуальні технології, особливо при вдосконаленні функцій управління.

Метою дослідження є оцінка та аналіз ефективності впровадження інтелектуальних технологій в системі управління інфокомунікаційною мережею. Для досягнення цієї мети було виконано такі завдання:

- розглянуто принципи побудови та функції систем штучного інтелекту, їх застосування в інфокомунікаціях.;
- досліджено основні концепції систем управління в інфокомунікаціях.
- проаналізовано функціональні можливості інтелектуальних систем управління та виконано їх порівняння з традиційними системами управління;

- виконано оцінку рівня розробок систем управління з використанням штучного інтелекту у порівнянні з існуючими підходами.

Система штучного інтелекту - це комп'ютерна, креативна система (багатофункціональна, інтегрована, інтелектуальна) зі складною структурою, що використовує накопичення і коригування знань (синтаксичної, семантичної, прагматичної інформації) для постановки і досягнення мети (цілеспрямованої поведінки), адаптації до змін середовища і внутрішнього стану шляхом зміни середовища або внутрішнього стану[1]. Широкого розповсюдження СШІ зазнали у системах управління. Під інтелектуальною системою управління розуміється система управління, здатна до «розуміння» та навчання щодо об'єкта управління, зовнішнього середовища та умов роботи [2]. Головна архітектурна особливість, яка відрізняє інтелектуальні системи управління від традиційних – механізм отримання, зберігання та обробки знань для реалізації своїх функцій.

Основними задачами інтелектуальної системи управління є: інтерпретація даних, діагностика, моніторинг, проектування, прогнозування, планування, навчання, управління, підтримка прийняття рішень [3]. Використання інтелектуальних систем управління дозволить виявляти позаштатні ситуації у роботі, вимірювати, накопичувати та відображати статистичні дані, інформувати про можливість виникнення критичної ситуації, робити прогноз впливу навколишнього середовища та видавати рекомендації щодо покращення показників функціонування мережі в залежності від ситуації, що склалася, а також підвищить продуктивність мережі до рівня її пікової продуктивності.

Рис. 1 – Функціональна схема інтелектуальної системи управління

Для оцінки рівня розробки інтелектуальних систем управління пропонується використання цільової функції γ, яка має вид:

$$\gamma = \frac{A_i}{A_0} + \frac{B_i}{B_0} + \frac{C_i}{C_0} + \cdots + \frac{Z_i}{Z_0} \rightarrow max;$$

де $A_0, B_0, C_0 \ldots Z_0$ – нормуючі параметри, $A_i, B_i, C_i \ldots Z_i$ – параметри системи, що розглядається (існуючої, чи побудованої на базі ШІ).

Пропонується розглядати такі параметри, як функціональність системи, швидкість прийняття рішень, навченість та ін.

Як показали розрахунки, інтелектуальна система управління є більш ефективною у порівнянні з традиційними системами управління, її параметри наближені до параметрів оптимальної системи управління. Впровадження таких систем в інфокомунікаціях є досить

доцільним, адже це дозволить зменшити час реагування на позаштатні ситуації, спростить керування та мінімізує вплив «людського фактору» на роботу мережі.

***Література*:**

1. Системы искусственного интеллекта : учеб. пособие. В 2-х частях. / С. Н. Павлов. — Томск: Эль Контент, 2011. — Ч. 1. — 176 с.
2. Вагин В.Н., Головина Е.Ю., Загорянская А.А., Фомина М.В. Достоверный и правдоподобный вывод в интеллектуальных системах. М., 2004г. – 704с.
3. http://libeldoc.bsuir.by/bitstream/123456789/3980/1/

УДК 004.75:004.94

Кунаховець С.С.
ОНАЗ ім. О.С. Попова
kaprizzna-ya@i.ua
Науковий керівник — доц. ОНАЗ Нікітченко В.В.

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ВНУТРІШНЬОЇ ВЗАЄМОДІЇ СКЛАДОВИХ ОБЧИСЛЮВАЛЬНОЇ ХМАРИ ІЗ ВИКОРИСТАННЯМ ПРОТОКОЛУ AMQP

Анотація. *Обговорюються особливості взаємодії між різними складовими обчислювальної хмари, а саме обмін повідомленнями між його програмними модулями. Використовуються реалізація обчислювальної хмари засобами Openstack, протокол AMQP для обміну повідомленнями, та AMQP-брокер RabbitMQ. Отримано кількісні параметри роботи протоколу AMQP та проведено їх аналіз.*

На даний час значного поширення набула така форма надання послуг, як хмарні обчислення [1]. Маємо кілька різновидів таких сервісів, зокрема побудованих у відповідності до моделей SaaS – Software as a Service, PaaS – Platform as a Service, і IaaS – Infrastructure as a Service. Найбільш повною за функціональними можливостями тут є модель IaaS, котра забезпечує можливість аренди інфраструктурних ресурсів — серверів, пристроїв зберігання даних, мережного устаткування. Дана модель передбачає надання користувачам інтерфейсу для купівлі та управління віртуальними машинами і мережами необхідної клієнтам потужності та конфігурації.

Не дивлячись на велику кількість наявних хмарних рішень, на даний момент не існує загальноприйнятого стандарту побудови хмарної інфраструктури. Це пояснюється тим, що великі провайдери хмарних послуг, такі як Amazon, Microsoft чи Google, не відкривають специфікації своїх продуктів. Через це було засновано низку відкритих та вільних хмарних проектів, найбільш успішним серед яких можна назвати Openstack [2]. Openstack був заснований NASA та Rackspace, і дозволяє створювати як комерційні, так і дослідницькі хмарні рішення. На даний час активну участь в розробці приймають RedHat, SUSE, HP, IBM, Canonical, Nebula, AT&T та інші.

Openstack являє собою сукупність технологічних проектів, що їх розробка ведеться значною мірою незалежно, і котрі взаємодіють між собою через визначені програмні інтерфейси. На поточний момент Openstack включає такі проекти як Nova для забезпечення власне віртуалізації обчислень, Neutron для віртуалізації мережі та надання деяких додаткових послуг, наприклад DHCP, Swift для зберігання об'єктів, Glance для зберігання віртуальних образів, Keystone для забезпечення аутентифікації та авторизації, та Horizon, що забезпечує web-інтерфейс з користувачами. Кожен з проектів визначає власний API, що також дозволяє розробникам під'єднувати власні реалізації сервісів за умови відповідності API.

Використання власних API є лише однією з можливостей організації взаємодії між компонентами обчислювальної хмари Openstack. Серед іншого потрібно зауважити обмін повідомленнями, котрий реалізується із застосуванням протоколу AMQP [3]. AMQP — це відкритий протокол для передачі повідомлень між компонентами системи, з низькою затримкою та на високій швидкості. При цьому окремі складові системи обмінюються повідомленнями через спеціальний брокер, котрий серед іншого здійснює маршрутизацію повідомлень, за потреби гарантує доставку, розподіляє повідомлення у відповідні черги та ін. Openstack використовує AMQP-брокер RabbitMQ [4].

Далі будемо досліджувати протокол AMQP, з метою встановлення особливостей його поведінки в різних мережних умовах, що в свою чергу дає можливість створювати умови для підвищення якості обміну повідомленнями. На існуючій платформі Openstack зафіксуємо типову сесію обміну AMQP-повідомленнями за допомогою аналізатора протоколів Wireshark. Збережену у Wireshark сесію піддамо обробці в моделюючій системі Opnet Modeler, а саме в її програмному модулі ACE (Application Characterization Enviroment).

Відразу після імпорту в ACE нам стає доступною деяка статистична інформація щодо досліджуваного файла трафіка. Як видно з рис.1, протокол AMQP досить невибагливий до пропускної здатності каналів.

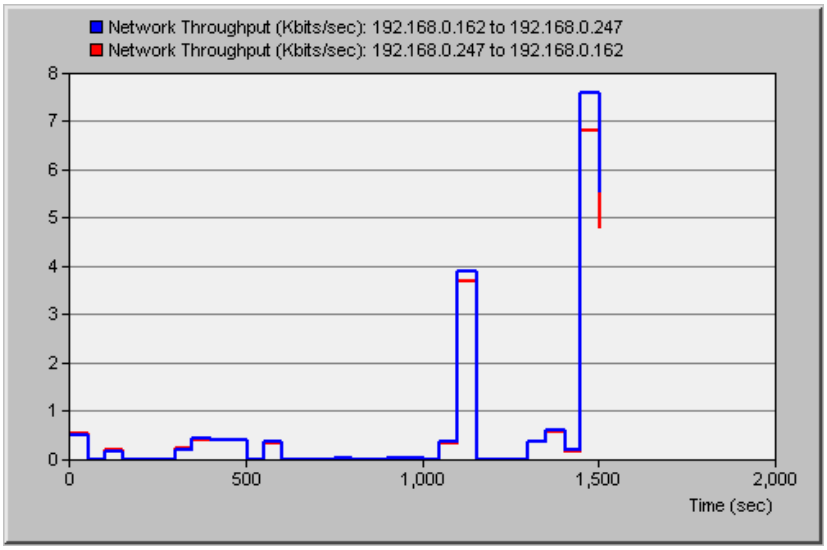


Рисунок 1 — Тривалість та інтенсивність досліджуваної транзакції

Розглянемо деякі з отриманих нами з ACE даних щодо здійсненої AMQP-транзакції.

Ступінь ефективності роботи протоколу серед іншого залежить від розміру пакетів, котрі використовуються досліджуваним програмним додатком. Так, про розміри пакетів прикладного рівня можна судити, керуючись інформацією з рис. 2.

На діаграмі відображено обмін повідомленнями AMQP на протязі всього інтервала дослідження. У верхній частині діаграми зображено шкалу відліку часу в секундах. Кожна чорна горизонтальна лінія позначає мережний вузол. Кожна стрілка відображає один пакет даних. Пакет даних прикладного рівня загалом може складатись з кількох пакетів мережі. Місце розташування початку й кінця стрілки вказує на час початку і закінчення передачі повідомлення відповідно.

Більше інформації про пакети досліджуваного протокола можна отримати, застосувавши до них утиліту AppDoctor. Загальний час AMQP-сесії розподіляється між вузлами з адресами 192.168.0.247 і 192.168.0.162 (див. рис. 3).

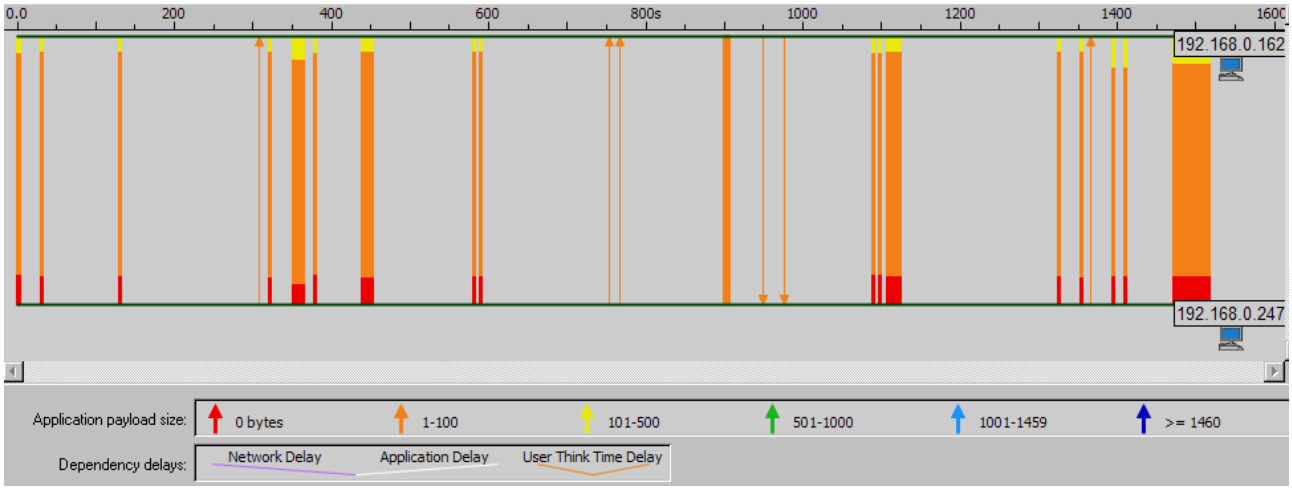


Рисунок 2 — Діаграма роботи прикладного рівня для протокола AMQP

При цьому час витрачається переважно на роботу кінцевих хостів, а складова мережі на тривалість транзакції практично не впливає.

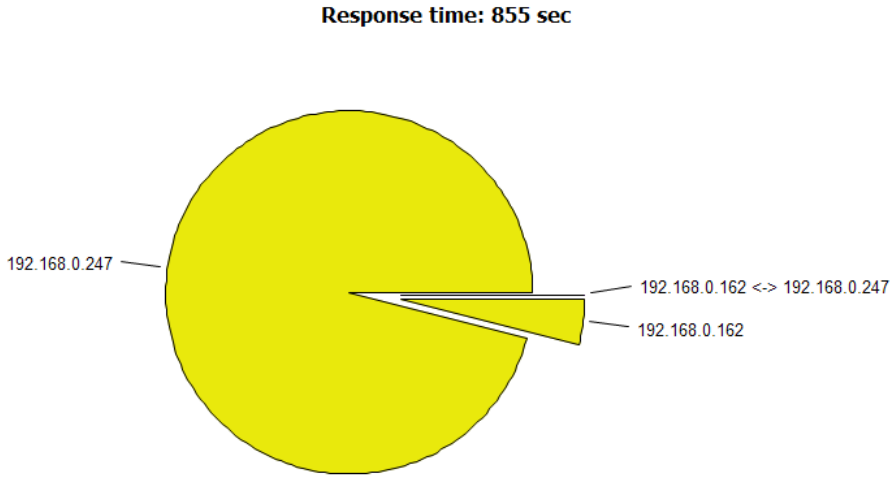


Рисунок 3 — Складові часу виконання транзакції

Жовтим кольором тут зображено затримку за рахунок програмного забезпечення (Tier Processing в термінології Opnet). Затримка ПЗ (час відгуку ПЗ) – це повна тривалість обробки даних програмними компонентами на кожному рівні.

Далі розглянемо статистичні показники інформаційного обміну між програмними компонентами, що взаємодіють по протоколу AMQP. Вони зведені в таблицю 1.

Після фіксації всіх вищезазначених параметрів обміну перейдемо до аналізу їх на наявність місць, де виникають труднощі або можуть виникнути в майбутньому (будемо позначати їх “Вузьке місце ” та “Потенційно вузьке місце” відповідно).

Таблиця 1 — Статистика взаємодії по протоколу AMQP

Параметр	**Взаємодія 192.168.0.162 -> 192.168.0.247**
Сумарний час сеансу (сек)	1517.866523
Зміна напрямків передачі даних	1471
Повідомлення протокола AMQP	1890
Обсяг даних (байти)	80635

Параметр	Взаємодія 192.168.0.162 -> 192.168.0.247
Середній обсяг повідомлення (байти)	42.66
Пакети мережі	2613
Середній обсяг мережного пакета (байти)	254757
Очікування (мс)	0,00
Час очікування (сек)	0.000000
Смуга пропускання (Kb/s)	100000
Затримка за рахунок мережі (сек)	0.016563
Затримка протокола (сек)	0.000401
Затримка узгодження між рівнями (сек)	0.000000
(A « B) Максимальна кількість переданих даних в одній сесії (байт)	335
(B « A) Максимальна кількість переданих даних в одній сесії (байт)	335

Саме ця інформація має найбільше значення для подальших рекомендацій, адже вона характеризує переваги та недоліки реалізації протоколу AMQP. Деякі проблемні місця, на які необхідно звернути увагу першочергово, приведені в таблиці 2.

Таблиця 2 – Наявність вузьких та потенційно вузьких місць

Параметр	192.168.0.162 - 192.168.0.247
Затримка програмного забезпечення	Вузьке місце
Взаємодія	Вузьке місце
Затримка узгодження між рівнями	Немає вузького місця
Час очікування	Немає вузького місця
Ефективність смуги пропускання	Немає вузького місця
Затримка протокола	Немає вузького місця
Скидання зв’язку	Потенційно вузьке місце
TCP Frozen Window	Немає вузького місця
TCP Nagle's Algorithm	Немає вузького місця

Результати дослідження сесії обміну повідомленнями по протоколу AMQP говорять про доцільність його використання для організації взаємодії між компонентами обчислювальної хмари. Покращити часові показники такої взаємодії можна насамперед за рахунок більш якісної програмної реалізації брокера та клієнтів AMQP.

Література

1. Peter Mell, Timothy Grance The NIST Definition of Cloud Computing // NIST Special Publication 800–145.
2. Офіційний сайт проекту Openstack: http://www.openstack.org.
3. Офіційний сайт AMQP: https://www.amqp.org.
4. Офіційний сайт проекту RabbitMQ: https://www.rabbitmq.com.

УДК 621.391

Кустов А.
ОНАС им. А. С. Попова
artem.ron1@mail.ru
Научный руководитель – доц. Царёв Р. Ю.

ОПТИМИЗАЦИЯ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ ЦЕНТРА ОБРАБОТКИ ДАННЫХ

Аннотация. *Работа посвящена исследованию механизмов оптимизации использования ресурсов центра обработки данных.*

В настоящее время все большую популярность приобретаю так называемые облачные сервисы. Физическую основу любого облачного сервиса составляет центр обработки данных (ЦОД). Основная задача ЦОД - предоставление ресурсов набору облачных приложений (сервисов), работа которых обеспечивается путем распределения ресурсов физического оборудования между приложениями [1].

Возникает задача оптимального распределения ресурсов ЦОД между приложениями (сервисами). Одним из методов, который позволит повысить эффективность использования ресурсов является применение технологии виртуальных машин. Виртуализация позволит перераспределить нагрузку на физические сервера и повысить эффективность их использования. Общая схема распределения ресурсов ЦОД между приложениями с применением технологии виртуализации показана на рис. 1 [2].

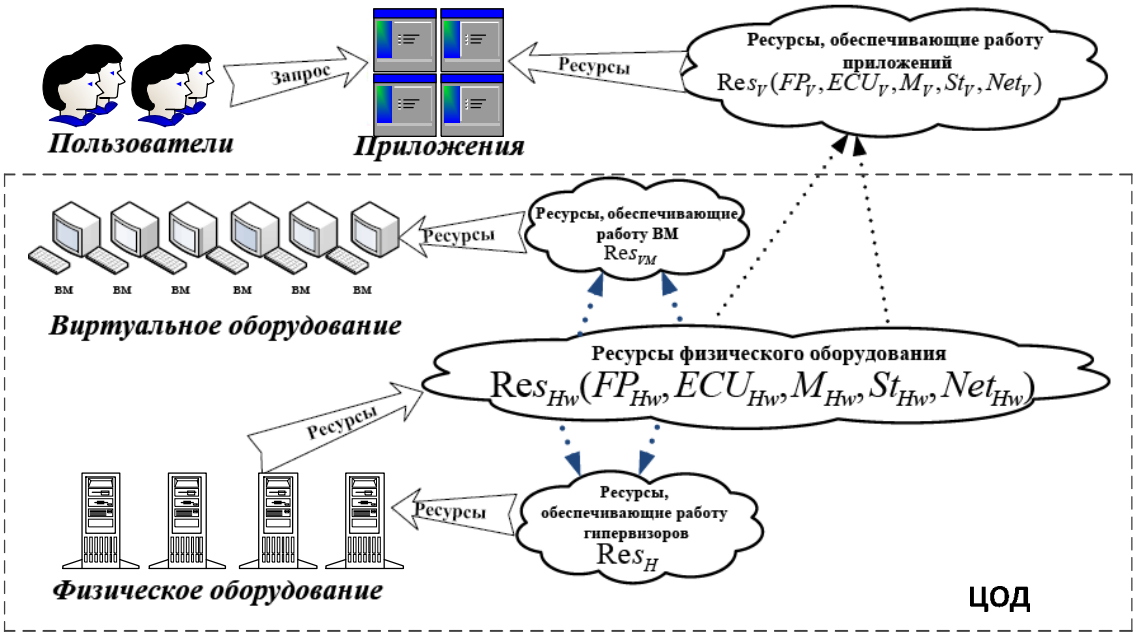


Рисунок 1 - Схема распределения ресурсов ЦОД

В общем случае, объем ресурсов, которые могут быть выделены из ресурсов физического оборудования для обеспечения работы некоего приложения можно определить как:

$$ResV(FPV,ECUV,MV,StV,NetV) = ResHw(FPHw,ECUHw,MHw,StHw,NetHw) - ResH(FP\square\square,ECUH,MH,StH,NetH) - ResVM(FPVM,ECUVM,MVM,StVM,NetVM)*m \quad (1)$$

где FPV – суммарное число ядер процессоров, которое может быть выделено под виртуализацию; $ECUV$ – суммарная производительность процессора, которая может быть

выделена под виртуализацию; MV – суммарное значение объема предоставляемой оперативной памяти, которое может быть выделено под виртуализацию в Гб; StV – суммарное значение предоставляемого объема устройств хранения данных, которое может быть выделено под виртуализацию в Гб; $NetV$ – суммарное значение показателей производительности сети, которое может быть выделено под виртуализацию;

$FPHw$ – суммарное значение количества ядер процессоров, полученное от физического оборудования всех серверов в инфраструктуре; $ECUHw$ – суммарное значение показателей производительности процессора, полученное от физического оборудования всех серверов в инфраструктуре; MHw – суммарное значение объемов предоставляемой оперативной памяти, полученное от физического оборудования всех серверов в инфраструктуре в Гб; $StHw$ – суммарное значение предоставляемых объемов устройств хранения данных, полученное от физического оборудования всех серверов в инфраструктуре в Гб; $NetHw$ – суммарное значение показателей производительности сети, полученное от физического оборудования всех серверов в инфраструктуре;

FPH – суммарное значение количества ядер процессоров, требуемое для обеспечения работы всех элементов распределения ресурсов физических серверов (гипервизоров); $ECUH$ – суммарное значение показателей производительности процессора, требуемое для обеспечения работы всех элементов распределения ресурсов физических серверов (гипервизоров); MH – суммарное значение объемов предоставляемой оперативной памяти, требуемое для обеспечения работы всех элементов распределения ресурсов физических серверов (гипервизоров) в Гб; StH – суммарное значение предоставляемых объемов устройств хранения данных, требуемое для обеспечения работы всех элементов распределения ресурсов физических серверов (гипервизоров) в Гб; $NetH$ – суммарное значение показателей производительности сети, требуемое для обеспечения работы всех элементов распределения ресурсов физических серверов (гипервизоров);

$FPVM$ – суммарное значение количества ядер процессоров, требуемое для обеспечения работы одного экземпляра ВМ; $ECUVM$ – суммарное значение показатель производительности процессора, требуемое для обеспечения работы одного экземпляра ВМ; MVM – суммарное значение объема предоставляемой оперативной памяти, требуемое для обеспечения работы одного экземпляра ВМ в Гб; $StVM$ – суммарное значение предоставляемого объема устройства хранения данных, требуемое для обеспечения работы одного экземпляра ВМ в Гб; $NetVM$ – суммарное значение показателей производительности сети, требуемое для обеспечения работы одного экземпляра ВМ.

$ResV$ – общее количество ресурсов, которые могут быть выделены под виртуализацию;

$ResHw$ – суммарное количество вычислительных ресурсов физического оборудования всех серверов в инфраструктуре;

$ResVMH$ – суммарное количество ресурсов, требуемых для обеспечения работы всех элементов распределения ресурсов физических серверов (гипервизоров);

$ResVM*m$ – количество ресурсов, требуемых для обеспечения работы одного экземпляра ВМ умноженное на m – количество экземпляров ВМ любого типа, запущенных в системе в момент времени t.

Очевидно, что вероятность одновременного использования всех сервисов мала, поэтому необходимо решить задачу быстрого перераспределения ресурсов выделенных для простаивающих приложений и быстрого выделения требуемых ресурсов при запуске приложения.

При анализе сложных вычислительных систем целесообразно учитывать такие критерии как: C_S – стоимость системы, P_S – производительность системы, R_S – надежность системы. Таким образом, оптимизация распределения ресурсов ЦОД должна обеспечивать минимизацию стоимость и максимизацию производительности и надежности.

В общем виде целевую функцию можно представить как:

$$R_S \rightarrow max$$
$$P_S \rightarrow max \quad (2)$$
$$C_S \rightarrow min$$

Решение сформулированной задачи оптимизации позволит быстро и эффективно распределять ресурсы ЦОД между запущенными приложениями, добиться максимальной производительности и надежности системы при минимизации затрат на ее эксплуатацию.

Литература

1. Батура, Т. В., Мурзин, Ф. А., Семич, Д. Ф. Облачные технологии: основные понятия, задачи и тенденции / Т. В. Батура, Ф. А. Мурзин, Д. Ф. Семич // Программные продукты и системы и алгоритмы. 2014. –№ 1.

2. Игнатов, Н. А. Построение задачи оптимизации предоставления виртуальных ресурсов в центрах обработки данных, основанных на облачных технологиях / Н. А. Игнатов // Известия Петербургского университета путей сообщения – Санкт-Петербург. – 2014. – № 1(38). – С. 69-74.

3. Пападимитриу Х., Стайглиц К. Комбинаторная оптимизация. Алгоритмы и сложность – М.: Мир, 1985.

УДК 681.2.083:555.7

Ліщина Н.М.
Ліщина В.О.
Луцький НТУ
Луцький НТУ
lischyna@gmail.com

ПРОБЛЕМА ВИБОРУ ПЛАТФОРМИ ДЛЯ СТВОРЕННЯ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ УНІВЕРСИТЕТУ

Анотація. *Розглядаються проблеми запровадження у вищих навчальних закладах електронного документа та електронного документообігу. Здійснено опис основних технологічних платформ провідних виробників. Обґрунтовано можливості вирішення сучасних проблем запровадження електронного документообігу на базі застосування портальних технологій, зокрема Microsoft SharePoint та Lotus Notes/Domino від IBM. Виділено особливості служби Microsoft SharePoint Online як частини пакету Office 365.*

Проблеми запровадження у вищих навчальних закладах (ВНЗ) електронного документа та електронного документообігу стають все більш актуальними. Введення системи електронного документообігу (СЕД) зможе допомогти ВНЗ організувати їх роботу з документами і керувати ними протягом усього їх життєвого циклу [3]. На відміну від документів на паперових носіях зі своїми жорсткими рамками, статичною формою і обмеженими можливостями перехід до динамічних цифрових електронних документів забезпечує особливі переваги при створенні, спільному використанні, поширенні та збереженні інформації. Електронні документи, як динамічні сховища інформації, можуть одночасно використовуватися співробітниками однієї робочої групи, відділу або підприємства загалом. Доступ до них здійснюється протягом кількох секунд. Прискорений доступ до інформації разом зі значною економією коштів може забезпечити й стратегічно важливі конкурентні переваги [1]. Таку роботу з електронними документами забезпечують інформаційні системи, які значаться як системи електронного документообігу.

При виборі системи електронного документообігу слід враховувати всю множину чинників, і остаточне рішення бажано приймати на основі комплексного аналізу

можливостей СЕД залежно від вимог і специфіки замовника. Критерії, за якими були розглянуті системи, досить універсальні і відповідають завданням автоматизації документообігу як в комерційних, так і в державних установах. Оскільки за експертними оцінками в найближчі два роки очікується стрімке зростання переходу на відкрите програмне забезпечення (ВПЗ), то окрему увагу приділено СЕД Alfresco, найбільш поширеній на заході системі електронного документообігу саме через відкритість коду (повний Open Source), що спонукає до зниження витрат на ліцензії.[2].

Alfresco – це система управління корпоративними інформаційними ресурсами (ECM) та документообігом, один із лідерів на ринку вільного програмного забезпечення серед програм для організації електронного документообігу. Використовується для управління документами, записами, веб-публікацією, груповою роботою в організації. Це система з відкритим кодом, тобто розповсюджується вільно, проте існує і платна версія.[1].

Розгляд основних технологічних платформ провідних виробників для побудови СЕД і корпоративних порталів, представлених на ринках України, дозволяє, серед безлічі продуктів, виділити три основні групи:

1. Продукти на основі SharePoint від Microsoft.
2. Продукти, побудовані на платформі Lotus Notes/Domino від IBM.
3. Інші продукти, що розвиваються самостійно і що пропонують свої рішення, у тому числі і безкоштовні, але доки не займаючі істотні частки ринку. Оскільки третя група продуктів займає незначну частку ринку, то це означає, що рішення або не мають необхідної функціональності, або погано адаптовані для вітчизняних умов і користувачів. Тому обмежимося порівнянням перших двох платформ: SharePoint від Microsoft і Lotus Notes/Domino від IBM.

Сімейство продуктів SharePoint. SharePoint - ця скорочена назва продуктів і технологій Microsoft SharePoint. Їх можна використати з метою створення сайтів, для спільної роботи і обміну даними з іншими користувачами, для управління документами впродовж усього їх життєвого циклу, публікації звітів. SharePoint включає наступні продукти і технології: SharePoint Foundation, SharePoint Server, Microsoft SharePoint Server 2010, SharePoint Online, SharePoint Designer, SharePoint Workspace, EOS for SharePoint 2010. Microsoft SharePoint Foundation – безкоштовний додаток до Windows Server, що надає базову інфраструктуру для спільної роботи – редагування, зберігання документів, контроль версій тощо. Також він включає в себе таку функціональність, як «маршрути» руху документів, списки завдань, нагадування, онлайн-дискусії. Раніше Microsoft SharePoint Foundation був відомий як Windows SharePoint Services (WSS).[3].

Microsoft SharePoint Server – платний компонент для інтеграції функціональності SharePoint в роботу застосунків MS Office. Він є надбудовою над Microsoft SharePoint Foundation і розширює його можливості. Microsoft SharePoint Foundation пропонує базові засоби для створення веб-застосунків. До таких засобів належать веб-частини, списки даних, бібліотеки документів, середовища виконання робочих потоків і шаблони веб-сайтів. Microsoft SharePoint Server має додаткові важливі прикладні функції, а саме: систему створення сайтів по запитах користувачів, функції бізнес-аналізу, технологію Forms Services, вбудовані функції пошуку та засоби побудови соціальних мереж. Всі зазначені функції можуть бути доопрацьовані та доповнені розробниками з метою створення простих у використанні веб-панелей для моніторингу основних бізнес-процесів.

Microsoft SharePoint Online – послуга в „хмарі”, що дозволяє створювати сайти і робочі області для спільної роботи з колегами, партнерами та замовниками. Для зберігання документів на сайтах SharePoint служать бібліотеки. Документ до бібліотеки може бути внесений декількома способами: із спеціального меню настільного клієнта Word 2010, завантажений із жорсткого диска натисканням на посилання „Add document” сайту або переписуванням файлу в провіднику Windows, оскільки будь-яка бібліотека Share Point може бути відкрита в Провіднику Windows як мережева папка.

Бібліотеки сайту SharePoint Online сервісу Office 365 можуть бути налаштовані для підтримки механізмів повідомлень. Зокрема, за допомогою механізму повідомлень користувачі можуть електронною поштою отримувати листи у разі додавання або змінм документів у їх бібліотеці. При цьому співробітник, який вніс зміни або опублікував новий документ, звільняється від обов'язку повідомляти зацікавлених осіб – SharePoint Online зробить цю роботу за нього.

Виділяють такі особливості бібліотеки сайту SharePoint Online :

– можливість створювання особистого сайту співробітника (mySites) для збереження документів, посилань, контактів, публікацій матеріалів та спілкування в соціальній мережі підприємства;

– можливість створювання портали (team Sites) для спільної роботи з бібліотеками документів, робочими планами і календарями;

– можливість створювання внутрішні портали (intranet Sites) компанії для публікації новин, планів заходів та бізнес-інформації;

– створювання закритих порталів (extranet Sites) документів і бізнес-даних для партнерів і замовників;

– легка і швидка розробка професійних веб-сайтів для широкої аудиторії;

– можливість створення документів Office і збереження їх безпосередньо на порталах SharePoint Online;

– можливість управління правами доступу до документів для захисту службової інформації;

– можливість слідкувати за певними версіями документів й організовувати колективну роботу щодо підготовки документів.

Сімейство продуктів Lotus Notes/Domino. Якщо дати формальне визначення Lotus Domino і Notes – то це система і засоби створення і ведення розподілених баз даних колективного доступу, інтегровані з можливостями електронної пошти, призначені для збору, організації та розподілу інформації і знань. Lotus Domino і Notes самі по собі, а також у поєднанні з іншими продуктами сімейства Domino включають усі технології, які призначені для створення середовища колективної роботи. Та все ж якщо говорити про ключові технології, важливі з точки зору розуміння архітектури продукту і можливостей його застосування, то можна виділити наступні: документоорієнтована база даних; засоби розробки додатків; система електронної пошти; система реплицірування (тиражування) документів, інформації і додатків; засоби захисту інформації і розмежування доступу; засоби календарного планування і складання розкладів; Web- технології і технології Internet/Intranet; засоби інтеграції з реляційними базами даних, системами управління ресурсами підприємств(ERP).

Висновки. Результати порівняння СЕД на основі SharePoint від Microsoft і Lotus Notes/Domino від IBM дають підстави стверджувати, що продукти компанії Microsoft і IBM мають усі функціональні можливості для організації СЕД і порталу організації. Це інструменти для спільної роботи, зберігання контенту, роботи з поштою і офісними додатками, передачі миттєвих повідомлень, засоби автоматизації бізнес процесів і реалізації інших можливостей.

Література

1. Електронний документообіг: сучасні тенденції та проблеми провадження [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/34_VPEK_2012/Philologia/7_121024.doc.htm

2. DOCFLOW Украина: все об электронном документообороте, бизнес-конференция [Електронний ресурс] – Режим доступу: http://www.docflow.ua/conference

3. Ткачук Г. І. Використання електронної системи документообігу у ВНЗ / Г. І. Ткачук, С. А. Постова // Магістратура в умовах євроінтеграційних процесів вищої школи. – Житомир: ЖДУ, 2014. – С. 254.

УДК 621.397

Лунгул А.
ОНАЗ ім. О.С.Попова
nastyalungul@mail.ru
Науковий керівник - доц. Царьов Р.Ю.

ПРОЦЕС ВИБОРУ СИСТЕМ МОНІТОРИНГУ ЯКОСТІ ПОСЛУГ МЕРЕЖ ЗВ'ЯЗКУ

Анотація. *В роботі аналізуються проблеми процесу вибору оптимальної системи моніторингу якості послуг зв'язку.*

Останні роки спостерігається стабільна тенденція щорічного зростання обсягу глобального IP-трафіку. Таке зростання обсягів трафіку можна пояснити наступними тенденціями та прогнозами розвитку мереж [1]:

1. Завершення переходу мереж національних операторів телекомунікацій від мідних ліній зв'язку до оптичних.
2. Стрімким збільшенням числа безпроводових пристроїв.
3. Збільшенням кількості глобальних корпоративних мереж.

Очікується, що за період з 2014 по 2018 роки обсяг глобального корпоративного трафіку збільшиться у 6 разів. При цьому основними застосуваннями будуть корпоративні відео конференції, які показують щорічне зростання на 42 %.

Приймаючи до уваги зростання кількості мультимедійних застосувань та долі відеотрафіку, можна зробити висновок, що повстає питання забезпечення сталої та якісної роботи мережі. Оператори зв'язку та провайдери послуг потребують якісної служби технічної експлуатації. Однією зі складових частин технічної експлуатації є система моніторингу та контролю якості послуг[2]. Системи моніторингу дозволяють контролювати рівень якості послуг, що надають і у разі виникнення проблем з рівням якості інформувати про це технічний персонал.

Відповідно до рекомендацій [3,4] міжнародного союзу електрозв'язку, якість послуг залежить від наступних характеристик мережі:

– затримки передачі IP пакетів (IPTD - IP packet transfer delay). Затримка передачі IP пакетів визначається для всіх пакетів, що надійшли до точки призначення через певну ділянку мережі або NSE (Network section ensemble – сукупність мережних секцій), в тому числі враховуються вдалі (правильні) та помилкові пакети. IPTD – це час $(t_2\text{-}t_1)$ між двома відповідними пов'язаними подіями, вхідною подією $IPRE_1$ (IP packet reference event – подія передачі IP пакета), що відбулася в час t_1, та вихідної події $IPRE_2$, що відбулася в час t_2, де $(t_2>t_1)$ та $(t_2\text{-}t_1)\leq T_{max}$.

– варіації затримки IP пакетів (IPDV - IP packet delay variation). Варіація затримки IP пакетів з кінця в кінець між двома точками мережі визначається, виходячи із спостереження відповідних (актів прибуття)IP пакетів на вхідній та вихідній точках вимірювання. Двоточкова варіація затримки пакетів (v_k) для одного IP пакета k (к-того IP пакета) між хостом-джерелом SRC та хостом призначення DST є різницею між абсолютною затримкою IP пакета (x_k) та визначеною відносно (визначеним відношенням) затримки передачі пакета $d_{1,2}$, між цими (тими ж) двома точками вимірювання MP's: $v_k=x_k\text{-}d_{1,2.}$ Відносна затримка передачі IP пакета $d_{1,2}$, між SRC та DST є абсолютною затримкою IP пакета, що отримана (виміряна) для першого IP пакета між цими двома точками вимірювання.

– коефіцієнта помилкових IP пакетів (IPER - IP packet error ratio) – параметр, що характеризує коефіцієнт помилкових IP пакетів. Коефіцієнт помилкових IP пакетів визначається як:

$$IPER = N_П/N, \quad (1)$$

де $N_П$ - загальне число отриманих помилкових пакетів, N – загальне число всіх отриманих пакетів (правильних та помилкових).

– коефіцієнта втрати IP пакетів (IPLR - IP packet loss ratio), визначається як:

$$IPLR = N_B/N, \quad (2)$$

де N_B - загальне число втрачених пакетів, N – загальне число всіх переданих пакетів.

– проценту доступності IP сервісу (PIA - Percent IP service availability). Показує відсоток доступності сервісу протягом загального часу надання послуги і визначається як

$$PIA = \frac{T - (Nf \times \tau)}{T} \times 100\% \quad (3)$$

де Nf – сумарна кількість усіх невдалих сеансів вимірювань за звітний період; T – тривалість надання сервісу в годинах; τ - періодичність тестування в годинах.

Очевидно, що система моніторингу повинна бути в змозі контролювати ці параметри. Крім того до системи моніторингу висувають ще декілька додаткових вимог, наприклад підтримка роботи протоколу SNMP, прогнозування позаштатних ситуацій, виявлення аварій, формуванні різних типів звітів тощо. Ці фактори, а також наявність на ринку великої кількості систем моніторингу та контролю якості послуг роблять процес вибору системи дуже складним. Для вибору системи моніторингу пропонується застосувати алгоритм середньої інтегральної експертної оцінки. Суть алгоритму полягає в наступному:

1. Формується група систем кандидатів на впровадження.
2. Визначається група показників, які описують функціонал системи.
3. Формується група експертів (експертами можуть виступати як фахівці з експлуатації і проектування мереж та і фахівці з розробки систем моніторингу).
4. Для кожного показника визначається ваговий коефіцієнт, який показує важливість показника та його вплив на кінцеву ефективність системи моніторингу.
5. Для кожної з систем моніторингу експерти по кожному показнику виставляють оцінку за 10-бальною шкалою;
6. Визначається цільова функція, що оцінює загальний функціонал системи моніторингу.
7. Обирається та система в якої значення цільової функції максимальне.

На рисунку 1 наведено схема запропонованого алгоритму.

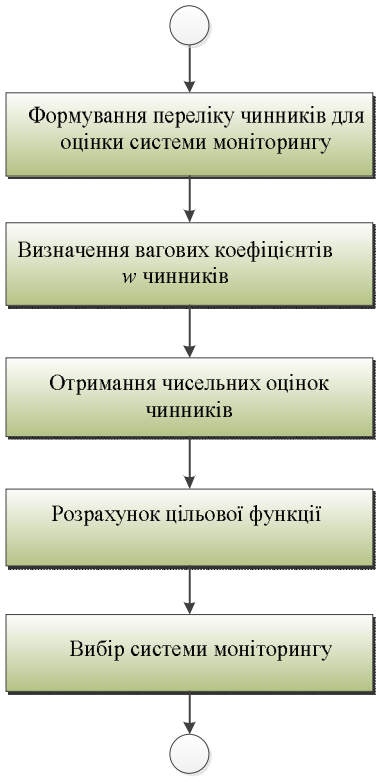


Рисунок 1 – Алгоритм вибору системи моніторингу

В роботі проведено дослідження щодо необхідності використання систем моніторингу якості послуг та запропоновано алгоритм вибору системи моніторингу на базі середньої інтегральної експертної оцінки.

Література

1. Бройдо В. Л. Вычислительные системы, сети и телекоммуникации / В. Л. Бройдо. С.-П.: Питер, 2006. - 702 с.

2. Кузнєцова М.Г. Застосування механізмів підвищення живучості для забезпечення захищеності інформаційного ресурсу в розподілених системах // Реєстрація, зберігання і обробка даних. —2006.—Т. 8, № 3. — С. 40–47.

3. IP Packet Transfer and Availability Performance Parameters: Рекомендация ITU-T Y.1540. - 2002.

4. Network Performance Objectives for IP-Based Services: Рекомендация ITU-T Y.1541. – 2002

УДК 621.396

Мамедов И.Э.
ОНАС им. О.С.Попова
Imamvcrdi.mamedov@mail.ru
Научный руководитель - д.т.н., проф. Лесовой И.П.

ИССЛЕДОВАНИЕ ПОМЕХ ОПТИЧЕСКОЙ ТРАНСПОРТНОЙ МНОГОВОЛНОВОЙ СЕТИ

Аннотация. *В работе рассмотрен один из основных ограничивающих факторов скорости передачи и длины регенерационного участка, который, на сегодняшний день, сравнительно мало изучен - это поляризационная модовая дисперсия.*

Рост информационных потоков в волоконно-оптических сетях, внедрение оборудования с интерфейсами STM-16/64/256 (2.4, 10 Гбит/с и 40 Гбит/с), делают актуальным изучение такого явления, как поляризационная модовая дисперсия [1]. Эффект ПМД стал критическим по мере достижения высоких скоростей в оптическом тракте, а вследствие накопительного характера поляризационной модовой дисперсии, ее негативное влияние усиливается с ростом длины линии.

Анизотропия профиля сердцевины одномодового волокна, в результате чего появляются два разных эффективные показатели преломления для основных состояний поляризации, приводит к различным групповых скоростей распространения мод с ортогональными поляризациями и появления задержки сигналов на приемной стороне $\Delta\tau$, которую называют дифференциальной групповой задержкой. Дифференциальная групповая задержка $\Delta\tau$ не постоянна величина, а меняется со временем, причем случайно [1]. Усредненная во времени ДОС между двумя ортогональными ОСП в линии связи описывается соотношением [2]:

$$\langle \Delta\tau \rangle = D_{PMD}\sqrt{L} \qquad (1)$$

где $\Delta\tau$ - усредненная по времени дифференциальная групповая задержка, L - длина волокна, - ПТД параметр волокна, измеряется в пс / √км.

ПМД типичного волокна, как правило, составляет от 0.05 до 2 пс / √км. В то же время коэффициент ПМД определяется выражением [1]

$$D_{PMD} = 0.5\left|\Delta\tau \sin(2\theta)\right| \qquad (2)$$

где 2θ - угол между вектором Стокса, представляет состояние поляризации передаваемого импульса, и направлением входного ПСП в пространстве Стокса, причем θ =

0 или θ = 90 °, когда входной ОСП совпадает с одним из входных ПСП, и θ = 45 °, когда оба входных ОСП одинаковы. На практике Δτ соответствует максимальной задержке, которая может иметь место между ОСП передаваемого импульса.

Поляризационной модовой дисперсией называют среднее значение дифференциальной групповой задержки, которое определяется по формуле:

$$PMD = \sqrt{\langle \Delta\tau^2 \rangle} \tag{3}$$

Усреднения выполняют, вычисляя Δτ в разные выборочные моменты времени t1, t2, t3, ..., tN в пределах времени Δt с последующим определением среднеквадратичное.

Анализ поведения Δτ показывает, что эта случайная величина лучше подпадает под распределение Максвелла, а стандартное отклонение связано со средним значением дифференциальной задержки соотношением

$$\langle \Delta\tau^2 \rangle = \frac{3\pi}{8} \langle \Delta\tau \rangle^2_{Max} \tag{4}$$

где Max- усреднения по функции распределения Максвелла (среднее значение).

Для дифференциальной групповой задержки в 0,3т, где Т - длительность символа, запас мощности составляет для приемника, ограниченного тепловым шумом, примерно 0,5 дБ, а для приемника с зависимым от сигнала шумом - 1 дБ. Это означает, что для получения запаса, равного 1 дБ или менее, дифференциальная задержка не должна превышать 0,1Т, то есть

$$\langle \Delta\tau \rangle = D_{PMD}\sqrt{L} < 0.1T \tag{5}$$

Изменение Δτ во времени - главная отличительная черта поляризационной модовой дисперсии от хроматической и модовой дисперсии. Это в значительной степени усложняет методы и устройства ее компенсации.

Максимальная скорость (Мбит / с) связана с коэффициентом ПМД соотношением:

$$B_{\max} = \frac{\varepsilon}{D_{PMD}}\sqrt{L} \tag{6}$$

где параметр ε (доля тактового интервала) выбирается в зависимости от того, какой коэффициент ошибок является приемлемым. Так, при $P_{пом} = 10^{-12}$ ε = 0,1.

На рис. 1 приведена зависимость максимальной скорости передачи информации и длины регенерационного участка от дисперсии ПТД.

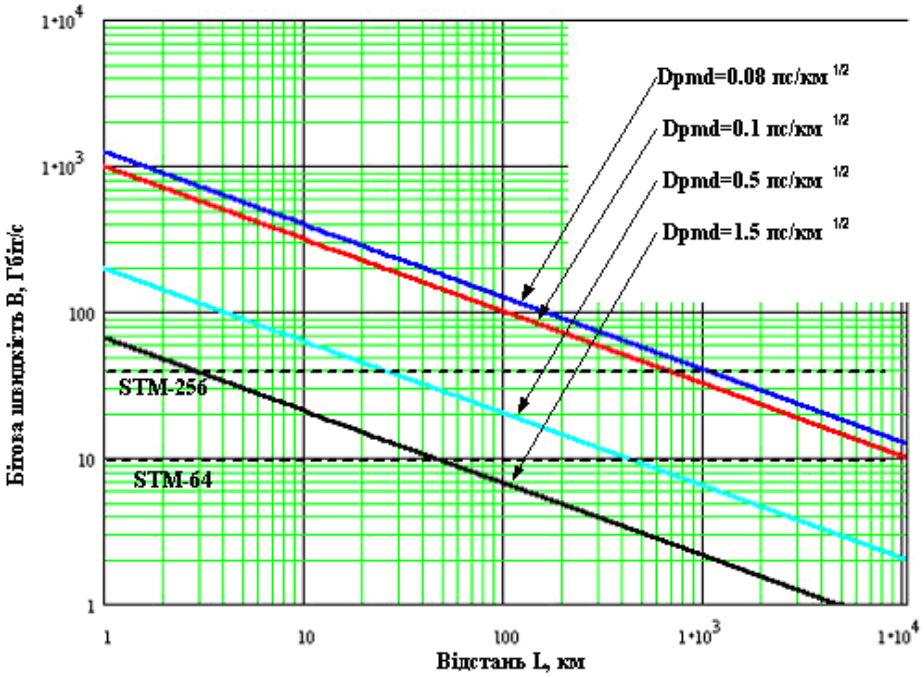


Рисунок - 1. Влияние ПМД на максимальную скорость передачи информации

Выводы. Совершенствование техники ослабление влияния ПМД дает возможность увеличения длины оптоволоконных связей для скоростей передачи более 10 Гбит /с.

Литература

1. Иванов А.Б. Волоконная оптика. Компоненты, системы передачи, измерения. – М.: Syrus Systems, 1999. - 672 с.

2. Р. Фриман Волоконно-оптические системы связи. // ТЕХНОСФЕРА, Москва. – 2004. С. 371.

УДК 004.021

Назиров Э.К.
ХНУГХ им. А.Н. Бекетова
nazirov@i.ua
Научный руководитель – к.т.н., доц. Карпенко Н.Ю.

ОБЗОР ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ В СИСТЕМАХ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Аннотация. *Рассматриваются возможности использования математических моделей при построении систем поддержки принятия решения на различных этапах возникновения, развития и ликвидации чрезвычайных ситуаций на региональном уровне.*

За 2014 год Украина пережила оккупацию территорий, непризнанную войну на территориях Донецкой и Луганской областей, увеличение террористических актов на территории остальных областей Украины, серьезное падение экономики, нехватку энергоресурсов и угрозу дефолта по международным обязательствам. Все эти события способствовали как многократному увеличению чрезвычайных ситуаций (ЧС), так и росту риска их возникновения. Поэтому проблема создания новых моделей и методов поддержки принятия решения для предупреждения и ликвидации ЧС актуальна как в силу многократно возросшего их количества, так и в силу того, что в настоящее время созрела необходимость использования современных систем, позволяющих снизить масштабы и последствия при их ликвидации. Поскольку чрезвычайные ситуации обычно возникают в условиях экстраординарных ситуаций, то и управление в условиях ЧС отличается гибкостью, необходимостью работы при недостатке информации, высоким темпом изменения ситуации, потребностью оперативного формирования наиболее эффективных решений, отличающихся высокой результативностью, что накладывает требования к минимизации времени и потерь при ликвидации ЧС. Учет большого количества параметров в условия недостатка информации и динамически изменяющейся структуры сил и ресурсов для ликвидации ЧС приводят к выводу, что задачи синтеза моделей поддержки принятия решений, можно характеризовать как задачи математического моделирования сложных систем. Их отличительными признаками являются наличие большого числа взаимосвязанных и взаимодействующих элементов, связи которых зачастую нелинейны, подверженность влиянию случайных факторов, непостоянство структуры и функционирования и интегративность системы, заключающаяся в том, что система в целом обладает свойствами, не присущими ни одному ее элементу.

Модель поддержки принятия решения при ликвидации ЧС на региональном уровне разбивается на этапы (подзадачи) в рамках применения декомпозиции системы.

Этапы развития чрезвычайной ситуации делятся на:

- предположение о конкретном виде ЧС;
- прогноз охвата и распространения ЧС;

- прогноз смертельных и санитарных потерь, зон и срочности эвакуации населения;
- выбор доступных средств оповещения населения и сил ликвидации;
- формирование из имеющихся сил и средств команд ликвидации с учетом требуемых квалификационных признаков и наличия необходимого материального ресурса;
- формулирование первоначальных задач и их оперативное изменение для работающих в зоне ЧС сил и средств, направленное на минимизацию человеческих жертв и материального ущерба в зоне действия чрезвычайной ситуации.

На первом этапе производится мониторинг, определенных в рамках модели возникновения ЧС, параметров, которые являются входными данными для последующей оценке сложности ситуации. Ядром для сравнения данных является интеллектуальный модуль, который представляет собой экспертную систему принятия решений и оценки уровня угроз. Задачами этого модуля являются – сравнение поступивших входных данных с границами имеющихся экспертных, принятие решения о наступлении конкретного типа ЧС, распространение которого описывается имеющейся в модуле математической моделью.

Второй этап базируется на привязанной к конкретному местоположению информации о рельефе и застройке местности, климатических условиях (скорость и направление ветра, влажность, концентрация определённых веществ и т.п.) и имеющихся типовых моделях распространения конкретного вида ЧС. На основании этих данных система строит предполагаемую модель распространения (скорость и направление распространения) ЧС. На этом этапе система выполняет оптимизацию (агрегирование описаний) модели с целью сокращения времени реакции для получения результата. Здесь используются элементы имитационного моделирования и принципы построения многоагентной системы. Для оценки скорости и направления распространения ЧС на данном этапе предлагается задействовать геоинформационные системы, имеющие многослойные геоинформационные данные и системы мониторинга, позволяющие получать оперативную информацию об изменениях в параметрах окружающей среды.

Целью третьего этапа является объединение информации о распределении плотности населения в районе ЧС и полученной на втором этапе модели распространения ЧС. Для кластеризации опасных зон предлагается использовать карты Кохонена, как один из видов искусственной нейронной сети.

На четвертом этапе система формирует, выбирая из имеющихся ресурсов, схемы оповещения населения и руководителей сил ликвидации. Здесь применяются математические модели, которые описывают дистанцию эффективного оповещения населения, в зависимости от выбора метода. Это могут быть системы, использующие модели поддержки принятия эффективных проектных решений для территориальных систем звукового оповещения, построенные на базе использования эффективных генетических алгоритмов. Или технологии индивидуальной поддержки принятия решения в критических ситуациях, ориентированные на помощь в принятии решения конкретным лицам, оказавшимся на территории распространения чрезвычайной ситуации.

Пятый этап решает проблемы когнитивного анализа развития ситуации, учета факторов неопределенности в процессе принятия решения, оптимальным распределением имеющихся для ликвидации ресурсов и оценкой темпов использования этих ресурсов. Для решения поставленных задач используются мультиагентные динамические модели, или модели, построенные на основе нечетких когнитивных технологий.

Литература

1. Методы создания и функционирования системы поддержки принятия решений в условиях чрезвычайных ситуаций техногенного характера / И. В. Шостак, В. О. Давиденко // Наука і техніка Повітряних Сил Збройних Сил України . - 2011. - № 2. - С. 168-172. - Режим доступу: http://nbuv.gov.ua/j-pdf/Nitps_2011_2_43.pdf

2. Управление в чрезвычайных ситуациях на основе нечетких когнитивных технологий / Смородинова Т. М. // Научная библиотека диссертаций и авторефератов

disserCat . -2005. - http://www.dissercat.com/content/upravlenie-v-chrezvychainykh-situatsiyakh-na-osnove-nechetkikh-kognitivnykh-tekhnologii#ixzz3VWtwN44o

3. Поддержка принятия решений для управления в условиях чрезвычайных ситуаций на основе когнитивных и динамических моделей / Ямалов И.А. // Научная библиотека диссертаций и авторефератов disserCat. -2007. – http://www.dissercat.com/content/ podderzhka-prinyatiya-reshenii-dlya-upravleniya-v-usloviyakh-chrezvychainykh-situatsii-na-os#ixzz3VWwDGSnc

4. Технологии экстренных вычислений для индивидуальной поддержки принятия решений в критических ситуациях / Карбовский В.А. // Библиотека университета информационных технологий механики и оптики. - 2014. - https://isu.ifmo.ru/pls/apex/f?p=2005:0::DWNLD_F:NO::FILE:A59C0AB76AEC5A243F0C50FA6A5F36A7

5. Модель поддержки принятия эффективных проектных решений для территориальных систем звукового оповещения / Тетерин И.М. // Академия государственной противопожарной службы – Архив публикаций конференций – 2008 - http://agps-2006.narod.ru/ttb/2008-3/08-03-08.ttb.pdf

6. Математическое моделирование и методы оценки рисков в чрезвычайных ситуациях геодинамического характера / Данилов Р.М. // 2012 - Диссертации в Техносфере: http://tekhnosfera.com/ matematicheskoe-modelirovanie-i-metody-otsenki-riskov-v-chrezvychaynyh-situatsiyah-geodinamicheskogo-haraktera

7. Модели принятия решений при предупреждении чрезвычайных ситуаций / Копылов С.А. // 2004 - - Диссертации в Техносфере: http://tekhnosfera.com/modeli-prinyatiya-resheniy-pri-preduprezhdenii-chrezvychaynyh-situatsiy

8. Информационная поддержка принятия решений при ликвидации техногенных чрезвычайных ситуаций на основе моделирования сценариев управления / Куликов О.М. // 2002 - Диссертации в Техносфере: http://tekhnosfera.com/informatsionnaya-podderzhka-prinyatiya-resheniy-pri-likvidatsii-tehnogennyh-chrezvychaynyh-situatsiy-na-osnove-modelirova#ixzz3VX25IJXi

УДК 621.391

Площник В.В.
ОНАЗ ім. О.С. Попова
vladdrift5@gmail.com
Керівник – к.т.н.,доц. Флейта Ю.В

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТАНДАРТІВ БЕЗПРОВОДОВИХ МЕРЕЖ IEEE 802.11

Анотація. *Приведено порівняльний аналіз стандартів IEEE 802.11. Встановлено, що стандарт постійно вдосконалюється в напрямку збільшення швидкості передачі даних та кількості абонентів на канал.*

Безпроводові технології призначені для передачі інформації на відстань між двома й більше об’єктами не вимагая при цьому їх зв’язку проводами. На сьогодні існує безліч безпроводових технологій, відомих користувачам по їхніх маркетингових назвах, таким як Wi-Fi, WiMAX, Bluetooth та інші. Кожна технологія має певні характеристики, які визначають її область застосування.

Впровадження Wi-Fi може забезпечити потреби користувачів не лише по широкосмуговому доступу і Інтернет, але і в частині передачі мови поверх Wi-Fi. Крім того, Wi-Fi надає можливості по побудові цільових мереж, що може сприяти розширенню клієнтської бази і представленню користувачам принципово нових послуг.

Стандарт IEEE 802.11 є базовим стандартом для побудови безпроводових локальних мереж (Wireless Local Network — WLAN). Стандарт IEEE 802.11 постійно вдосконалювався, а тому зараз існує сімейство, до якого відносять модификации з буквеними індексами a, b, c, d, e, g, h, i, j, k, I, m, n, o, p, q, r, s, u, v, w. Однак тільки 4 з них a, b, g, n користуються найбільшою популярністю у виробників устаткування, інші ж являють собою доповнення, удосконалення або виправлення прийнятих специфікацій.

Наведемо порівняльний аналіз стандартів IEEE 802.11 [1-4].

IEEE802.11 – перший, початковий стандарт безпровідних мереж, який ґрунтований на безпровідній передачі даних в частотному діапазоні 2,4 ГГц. Є сильно застарілим і практично не застосовується. Можлива швидкість обміну даними складає 1-2 Мбіт/с.

IEEE802.11a – стандарт грунтований на безпровідній передачі даних в діапазоні 5 ГГц. Стандарт використовує три піддіапазони, що не перетинаються. Максимальна швидкість передачі даних складає 54 Мбіт/с. У поганіших умовах, наприклад, за наявності перешкод передача даних може здійснюватися з меншими швидкостями 48, 36, 24, 18, 12 і 6 Мбіт/с.

IEEE802.11b - стандарт, який працює в діапазоні 2,4 ГГц. Весь діапазон розділений на три незалежні канали,тобто на одній території, не впливаючи на роботу один одного, можуть працювати три безпровідні мережі. У цьому стандарті передбачені два види модуляції – DSSS і FHSS. Максимальна швидкість передачі даних – 11 Мбіт/с. Упродовж досить тривалого періоду цей стандарт активно використовувався для побудови безпровідних мереж, але незабаром його замінив прогресивніший стандарт G.

IEEE802.11b – це поліпшена версія стандарту b, яка забезпечує більш високу швидкість передачі даних. В інтерпретації деяких компаній відрізняється від оригіналу модуляцією PBCC і подвоєною максимальною швидкістю – до 22 Мбіт/с. Також у рамках цієї модифікації були запропоновані рішення для передачі даних зі швидкістю до 44 Мбіт/сек.

IEEE802.11e – основне призначення цього стандарту пов'язане з використанням засобів мультимедіа. Він працює за принципом призначення пріоритетів різним видам трафіку – таким як аудіо і відео додаткам. Пріоритет отримують такі застосування як VoIP і Streaming Multimedia.

IEEE802.11g – стандарт, працюючий в діапазоні 2,4 ГГц. Поступово витісняється досконалішим стандартом n. Максимальна швидкість передачі даних – 54 Мбіт\з, що врази більше максимальної швидкості його попередника. Він, як і стандарт b, розділений на три незалежні канали, що дозволяє працювати трьом безпровідним мережам на одній території. Для збільшення швидкості обміну даними в цьому стандарт використовується метод модуляції з ортогональним частотним мультиплексуванням (OFDM), а також метод двійкового пакетного згортального кодування (PBCC). Основні переваги цього стандарту – нижче споживання енергії, велика дальність.

IEEE802.11i – стандарт, який усуває недоліки в області безпеки попередніх стандартів. Він вирішує проблему захисту даних канального рівня і дозволяє створювати безпечні безпровідні мережі практично будь-якого масштабу.

IEEE802.11e – стандарт з поліпшеним QoS (Quality of Service), що дозволяє забезпечити гарантовану якість обміну даними, шляхом розставляння пріоритетів різним пакетам даних. Потрібний для роботи таких сервісів як VoIP або IP – TV.

IEEE802.11n – стандарт безпровідних мереж останнього покоління, ґрунтований на безпровідній передачі даних в діапазоні 2,4 – 2,5 або 5,0 ГГц. За швидкістю він значно перевищує стандарти b і g, забезпечуючи швидкість на рівні Fast Ethernet. Теоретично, в лабораторних умовах, він здатний забезпечити передачу даних зі швидкістю до 600 Мбіт/с і використовує для цього відразу 4 антени – по 150 Мбіт/с на кожну. Основна його перевага – це додавання до фізичного рівня підтримки протоколу MIMO (Multiple Input Multiple Output). Окрім цього він сумісний з попередніми стандартами 802.11b/g, 802.11a і 802.11n.

Порівняння основних модифікацій стандарту IEEE 802.11 представлені в таблиці 1.

Таблиця 1 – Порівняння основних модифікацій стандарту IEEE802.11.

Стандарт	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Частотний діапазон,ГГц	5.15 – 5.25 5.67 – 5.85	2.4 – 2.483	2.4 – 2.483	2.4 – 2.483 5.15 – 5.25 5.67 – 5.85
Доступ до радіоканалу	CSMA – CA	CSMA – CA	CSMA – CA	CSMA – CA64
Кількість абонентів на один канал	50	10	50	Більше 100
Максимальна швидкість обімну даними	54 Мбіт/с	11 Мбіт/с	54 Мбіт/с	480 Мбіт/с
Метод модуляції	OFDM	BPSK, CCK	OFDM	BPSK, QPSK,
Дальність дії в приміщенні	10 – 20	20 – 100	20 – 50	10 – 20

З проведеного аналізу видно, що безпровідні мережі стандарту IEEE 802.11 постійно розвиваються і удосконалюються. Основним напрямком розвитку є збільшення швидкісті передачі даних та кількісті абонентів на канал. Тому дослідження, спрямовані на подальше підвищення ефективності мереж стандарту IEEE 802.11 є актуальними.

Література

1. Мережі бездротового широкосмугового доступу http://www.dut.edu.ua.
2. Problems and solutoions to Wi-Fi. http://www.wifinotes.com/.
3. Official IEEE 802.11 working group project timelines. http://www.ieee802.org/.
4. Еволюція швидкості передачі даних в мережах Wi-Fi http://habrahabr.ru /post/254559/.

UDC 621.391

Tikhonov V.I., Polikarpov O.S.
O.S. Popov Odesa national telecommunication academy
victor.tykhonov@onat.edu.ua, qaswed0@gmail.com

PRINCIPLES OF TOPOLOGY METHOD IMPLEMENTATION IN TELECOMMUNICATION NETWORK MODELS

Abstract*. The paper introduces an adaptation approach to apply the classic math category of topological space for telecommunication systems analysis to give a new impulse for the students and engineers to implement their theoretical knowledge in network applications. The topological space category may be used as one of the simplest and most universal models of telecommunication networks worth to apply at first-glance view towards a network object.*

Introduction

Systems analysis aims to study relationships between the predefined primitive entities associated within a set of elements. The terms “analysis” and “synthesis” come from Greek meaning "to take apart" and "to put together" respectively. “Analysis” may be defined as dissimilation process of breaking down a something whole into distinguished parts. Instead, the “synthesis" will assimilate separate parts in a coherent whole system. The system analysis is closely related to the logical term “holistic approach” and math term “topological space” [1]. The topological space is a fundamental cognitive category of math analysis to describe physical objects behavior. However, the classic topology concept has not been exhaustively adopted yet to study

info-communication network and systems. *This work aims to originate an adaptation approach to network simulation in terms of topological spaces*.

Understanding of classic definition topology

To approach the understanding of topology as a key category of math analysis and construct an alternative definition for this term we will quote one of the classic formalism given in the section 12.5-1 of the mathematic reference book for engineers, page 386 [1]:

A class C *of objects («points») is a topological space if and only if it can be expressed as a union of a family* J *of point sets which contains: 1) the intersection of every pair of its sets; 2) the union of the sets in every subfamily.* J *is topology for the space* C*, and the elements of* J *are called open sets relative to the topology* J*. A family* B *of open sets is a base for the topology* J *if and only if every set of* J *is the union of the sets in* B*. A given space may admit more than one topology; every space* C *admits the indiscrete (trivial) topology comprising only* C *and the empty set, and the discrete topology comprising all the subsets of* C.

We will trigger some questions to be discussed. Firstly, we we retrieve some critical notions mentioned in definition :

a) elementary objects (class, point, object, point set, family, subfamily, element of family, set in subfamily) – 8 terms for elementary objects;

b) operations (union of sets, intersection of sets) – 2 basic operations;

c) rule ("A class *can be expressed* as a union of a family of point sets") ; this is the principal rule for someone's logic mind to justify whether class C is topological space or not). Towards these terms we have some comments.

1) It seems there are excessive number elementary notions (eight) for a clear definition, as some of them look like synonyms: a) class, set, family; b) subfamily is close to intuitively know "subset" not mentioned in definition; c) object, element of set, element of family. To our opinion the notion redundancy of topological space definition does not contribute to better assimilation the essence of "topology". In our work we propose to reduce the abundance terms to three ones: point, set of point, subset of set. Of course, these three terms may solely describe a plane vision of complex object structuring and therefore, will not be competent to construct the category of topology if not being advanced. To overcome this difficulty we apply the multilayer classes' concept of American mathematician John von Neumann [2]. According to this concept each of the three abstract objects (point, set, subset) obtains an order (or hierarchy level). Thus, we may unlimited replicate points, sets and subsets on different layers of an abstract model (along with their basic properties) with no care about searching new terms and symbols for them. Instead, the principal properties of basic terms are to be exhaustively introduced and clarified for real objects interpretation. Among those we emphasize the axiom about the distinctiveness and independence of all the point within a set. Next, a crucial factor of set theory understanding is correspondence between "set" and "subset" (i.e. is the subset $A1$ of set A which contains all points of A equal to A or not?). Other obscure issues: a) is the subset $A1$ of set A the result of unification related points of to A or not? b) Are the points of subset $A1$ of set A connected (related) to each other because of being gathered to $A1$ or not? To clarify these logical uncertainties the more accurate treatment of the terms "subset" and "union" is needed.

2) The addressing to someone's "expert" experience" about what means "can be expressed" is overly subjective and informal to our mind. Therefore, the entire definition based on this insight can't be accepted as a relevant formal object. Instead, more constructive explanations are to be brought.

Conclusion

The topological space category may be used as a simple and therefore, universal model for telecommunication network tasks. Consider the detail analysis of the form and matter of canonic term "topology" and "topological space" along with the classes' theory formal logic of [3] and actual network modeling achievements we formulated an alternative definition of network topology

as a special type of connected and open structure defined on the basic order set of distinguished primitive objects called “points”.

References

1. G. Korn, T. Korn, Mathematical Handbook for Scientists and Engineers: Definitions, Theorems, 1968. - 1097 pp.

2. Данилов Ю. А. Математик Дж. фон Нейман и его «Математик» / Ю. А. Данилов // Природа. - 1983. – Вып. 2. - С. 86-87. - Режим доступа: http://www.ega-math.narod.ru/Reid/Neumann2.htm.

УДК 621.395.7

Порхун А.О.
ОНАЗ ім. О.С.Попова
necidaaa@gmail.com
Науковий керівник – доц. Нікітченко В.В.

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ПОБУДОВИ ВІРТУАЛЬНИХ ТОПОЛОГІЙ В ОБЧИСЛЮВАЛЬНИХ ХМАРАХ

Термін «віртуалізація» включає в себе різні абстракції і технології імітації віртуальних комп'ютерів з різним ступенем незалежності від реального обладнання. Так, наприклад, на одному фізичному сервері можуть розміщуватися декілька систем, що працюють одночасно і є ізольованими одна від одної. Виділяють три типи віртуалізації: віртуалізація уявлень, віртуалізація застосунків та віртуалізація серверів (вузлів).

Найбільш популярним прикладом віртуалізації представлень є та ситуація, коли термінальний сервер Windows Server надає свої обчислювальні ресурси клієнтам і клієнтський додаток виконується на сервері, тоді як клієнт отримує лише «зображення» - представлення.

Віртуалізація застосунків дозволяє запускати програмне забезпечення в ізольованому від основної системи середовищі (т. зв. sandbox).

Віртуалізація серверів - це програмна імітація апаратного забезпечення комп'ютера за допомогою спеціального ПЗ. Основна перевага технології – можливість запуску декількох ізольованих один від одного операційних систем на єдиному апаратному забезпеченні.

Враховуючи бурхливе зростання популярності технологій віртуалізації, ми відзначаємо той факт, що інші компоненти комп'ютерної екосистеми також піддаються віртуалізації. Одна з нових течій в цій області - віртуалізація мереж (топологій). У ранніх реалізаціях віртуальних платформ можна було створювати віртуальні мережеві адаптери, але сьогодні можлива віртуалізація більш великих мережевих компонентів, наприклад, комутаторів, що підтримують зв’язок між віртуальними машинами, розташованими на одному сервері або розподіленими по декількох серверах.

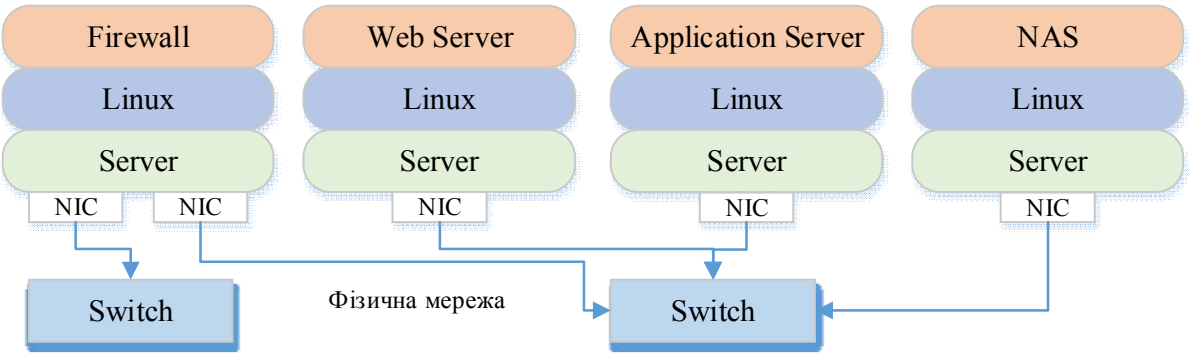


Рисунок 1 - Традиційна мережева інфраструктура

Ключова складова механізму віртуальних топологій - це абстрактне апаратне забезпечення, що дозволяє декільком операційним системам і застосункам спільно використовувати фізичне апаратне забезпечення (рисунок 2). Ця абстракція називається гіпервізором (hypervisor) або монітором віртуальних машин (virtual machine monitor). Кожна віртуальна машина (операційна система з набором застосунків) бачить базове апаратне забезпечення як систему, використовувану в монопольному режимі, хоча її окремі компоненти можуть бути розділені між декількома віртуальними машинами або взагалі не існувати.

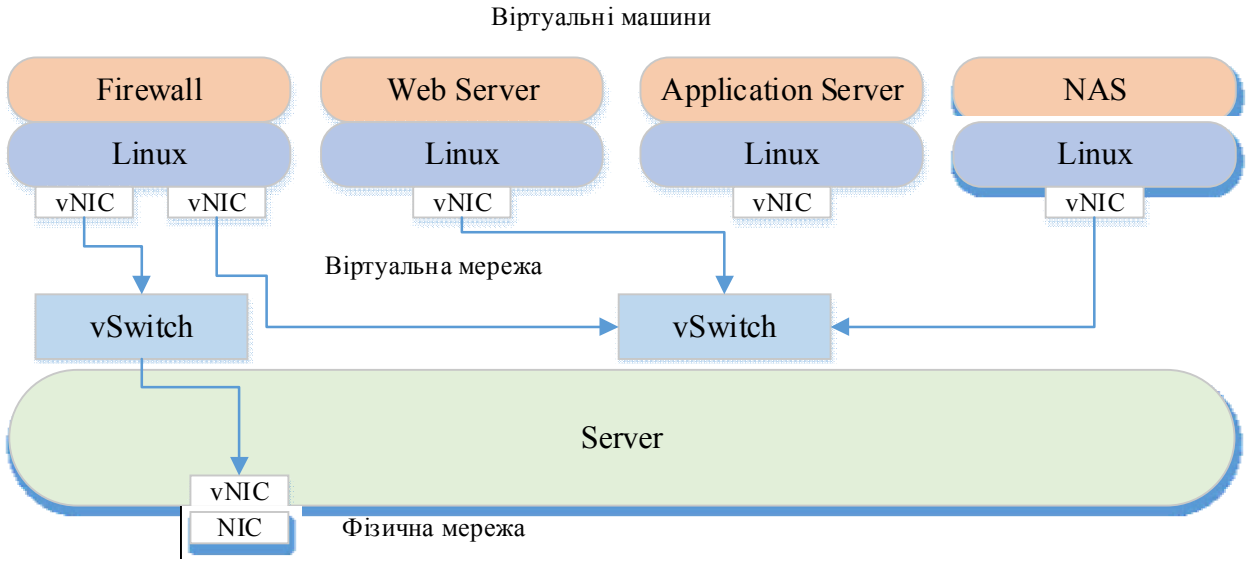


Рисунок 2 – Віртуалізована мережева інфраструктура

У нашій роботі ми будемо будувати обрані віртуальні топології за допомогою гіпервізора Xen, програмного забезпечення з відкритим вихідним кодом та утиліти Xentaur. Xen може організувати спільне безпечне виконання декількох віртуальних машин на одній фізичній системі з продуктивністю близькою до безпосередньої. Xentaur дозволяє організовувати гетерогенні мережі, що поєднують віртуальні машини Xen, емулятори мережевих пристроїв, реальні ком'ютери і мережеві пристрої, а також управляти ними і досліджувати їх роботу.

Вихідними даними нашої роботи є вісім віртуальних машин Xen, об'єднаних у мережу з використанням Xentaur. Ми використовуватимемо мережі декількох топологій («зірка», «дерево», «шина», гібридні топології) для проведення тестування їх показників (пропускної здатності, часу відгуку, затримки тощо).

Нижче наведено зразок конфігураційного файлу Xentaur.

```
domains =       [ 'qua1',  'qua2',  'dyn3',   'qua4',  'qua5',  'dyn6',  'qua7',  'qua8', ]
domain_types =[ 'quagga', 'quagga', 'xenomips', 'quagga', 'quagga', 'xenomips', 'quagga', 'quagga', ]
bridges  =                    [  'vlan101','vlan102','vlan103','vlan104','vlan105','vlan106', 'vlan107','vlan108', ]
vbridges_table = {
        'qua1'   : [ 'vlan101' ],
        'qua2'   : [ 'vlan102', 'vlan105' ],
        'dyn3'   : [ 'vlan101', 'vlan102', 'vlan103' ],
        'qua4'   : [ 'vlan103', 'vlan104', 'vlan106' ],
        'qua5'   : [ 'vlan104' ],
        'dyn6'   : [ 'vlan105',  'vlan106', 'vlan107' ],
        'qua7'   : ['vlan107', 'vlan108'],
        'qua8'   : ['vlan108'],
```

}

Подана конфігурація відповідатиме наступній віртуальній топології мережі:

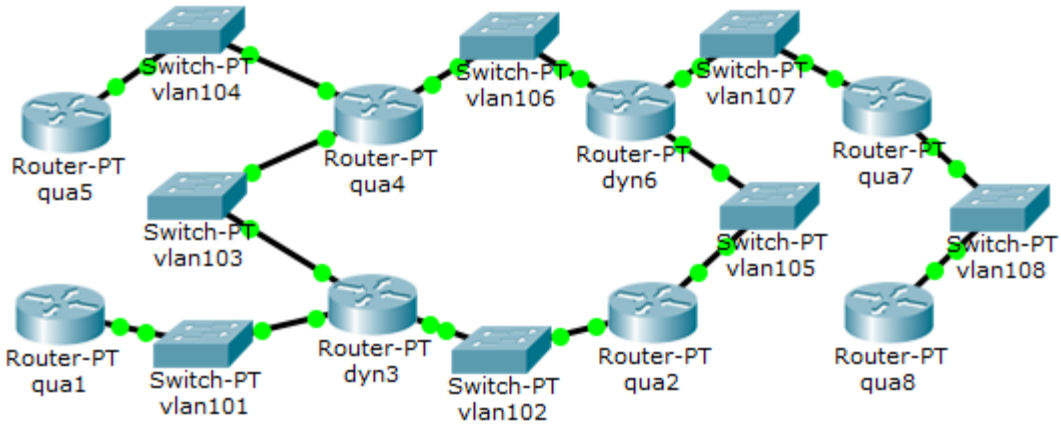


Рисунок 3 – Віртуальна топологія, що відповідає поданому конфігураційному файлу

Для проведення тестувань наявних топологій на кожному з віртуальних вузлів було встановлено MPICH, програмну реалізацію інтерфейсу MPI, що має у своєму наборі тести ефективності середи передавання: transfer (тест латентності та швидкості пересилань між двома вузлами) та nettest (тест пропускної здатності мережі при складних обмінах по різним логічним топологіям). Нижче подано результат проведення тесту для топології «кільце», що складається з чотирьох віртуальних вузлів.

NETTEST/MPI of 2003/07/08 is running with following parameters:
Message length unit is 1Kb = 1024 bytes
Messages: 1 to 16 units, step 0, multiplier 2
1000 times for each test routine, 2 iterations for whole test
Running chaos test with 4 logical links used.
Nodes: qua4 dyn6 qua2 dyn3

Network throughput values in MB/sec

Size,K	*Ring*	*Ring2*
1	*13.08*	*19.54*
2	*21.52*	*27.80*
4	*25.63*	*31.24*
8	*32.03*	*38.14*
16	*38,09*	*43.64*
1	*13.24*	*19,72*
2	*23.49*	*28,23*
4	*25.57*	*31.01*
8	*32.17*	*37,83*
16	*38,66*	*43.50*

Отримані результати свідчать про те, що пропускна здатність існуючої мережі на топології «кільце» є максимальною при двонаправленому обміні (Ring2) і становить 43,64 МБ/сек.

Також в нашій роботі було розглянуто наявні види віртуалізації, механізми реалізації віртуальних топологій та інструментарій для їхнього дослідження та керування ними.
Подальшою роботою над темою є більш поглиблене дослідження механізму віртуальних топологій, проведення тестів на розроблених конфігураціях заради виявлення можливих проблем та удосконалення їхнього функціонування. Також необхідно провести детальний

аналіз питань, що можуть виникати в процесі розгортання віртуальних топологій, а також сформувати перелік рекомендацій для їх усунення.

Література

1. Xen [Електронний ресурс] — Режим доступу: http://xgu.ru/wiki/Xen .
2. Xentaur [Електронний ресурс] — Режим доступу: http://xgu.ru/wiki/Xentaur .
3. David Chisnall. Definitive Guide to the Xen Hypervisor . Prentice Hall, 2007 .

УДК 621.391.3

Прохоров Д.Е.
ОНАЗ ім. О.С. Попова
danisproh@mail.ru

УДОСКОНАЛЕННЯ КОНЦЕПЦІЇ «РОЗУМНЕ МІСТО»

Анотація: *досліджено питання впровадження поновлювальних джерел енергії а саме сонячних панелей.*

Зростання вартості енергетичних ресурсів, основою яких є вуглеводні копалини (нафта, газ, кам'яне вугілля та ін), і зростаюча складність їх видобутку є стримуючими факторами для розвитку традиційної енергетичної інфраструктури. Переробка вуглеводневих паливних ресурсів робить негативний вплив на навколишнє середовище. Тому стає актуальним застосування джерел відновлюваної енергії, як у великих електричних мережах, так і в малих [1].

Метою роботи є: дослідження и розрахунок сонячних панелей які дозволили б на протязі року не залежати від зовнішньої електромережі і при цьому не мати обмежень у використанні електрики.

Розрахунок сонячної батареї

Стандартна інсоляція розраховується для площі в 1 квадратний метр. Однак точна площа елементів сонячної панелі нам не відома . Зате відома її номінальна потужність , яка визначається при 25 ° С для стандартного потоку сонячного світла в 1 кВт / м2. Цього цілком достатньо . Прийнявши потужність сонячного випромінювання біля поверхні Землі (максимальну інсоляцію) тієї ж самої - що, загалом , відповідає дійсності , - Ми отримаємо , що вироблення батареї відноситься до інсоляції квадратного метра також , як потужність батареї відноситься до потужності сонячного випромінювання в земної поверхні в ясну погоду , що припадає на 1 квадратний метр , тобто до +1000 Вт Помноживши місячну інсоляцію на співвідношення потужностей батареї і максимальної інсоляції, можна оцінити вироблення сонячної батареї за цей місяць.

Таким чином, вироблення фотоелектричної панелі будемо розраховувати за такою формулою:

$$E_{сб} = E_{інс} \cdot P_{сб} \cdot \eta / P_{інс} \quad (1)$$

де Есб - вироблення енергії сонячною батареєю ; Еінс - місячна інсоляція квадратного метра; Рсб - номінальна потужність сонячної батареї ; η - загальний ККД передачі електричного струму по проводах, контролера сонячної батареї і інвертора при перетворенні низьковольтного постійної напруги в стандартне (якщо передбачається використовувати низьковольтне напруга безпосередньо, то при досить товстих і коротких проводах η можна прирівняти до 1, тобто не враховувати); Рінс - максимальна потужність інсоляції квадратного метра земної поверхні (1000 Вт) . Інсоляція і бажана вироблення повинні бути в одних і тих же одиницях (або кіловат -годинах , або джоулях).

Відповідно, знаючи місячну інсоляцію , можна оцінити номінальну потужність сонячної батареї , необхідну для забезпечення необхідної місячної виробітку.

$$Рсб = Ринс \cdot Есб / (Еинс \cdot \eta) \quad (2)$$

Як правило, максимальна потужність сонячної батареї , заявлена виробником , досягається при напрузі на її виході , що перевищує напругу акумуляторних батарей на 15 .. 40 %. Більшість недорогих контролерів заряду можуть або підключати навантаження безпосередньо, « просажівая » вихідну напругу батарей набагато нижче оптимального , або просто відсікати цей « надлишок» . Тому ці втрати також можна закласти в ККД , зменшивши його на 10 .. 25 % (втрати потужності менше втрат напруги , оскільки при підвищеному навантаженні « просідання » напруги компенсується деяким збільшенням струму , хоча і не повністю; більш точно значення можна визначити, лише знаючи залежність напруги від струму навантаження для конкретної батареї). Однак існують моделі контролерів, які утримують ці втрати в межах 2 .. 5 %.

Потужність сонячного випромінювання змінюється від місяця до місяця , а номінальна потужність сонячної батареї незмінна, і саме на неї слід орієнтуватися при виборі місця для установки і визначенні витрат . Формула (2) зручна, щоб оцінити номінальну потужність батареї для конкретних умов інсоляції, але мало підходить для оцінки її можливостей протягом усього року. Тому побудуємо таблицю на підставі формули (1), щоб подивитися , коли і які режими енергопостачання можуть дозволити сонячні батарея номіналом потужності.

Вибір ємності акумуляторів: для цілорічної експлуатації (взимку) - не менше 800 А*год на кожну кіловат- годину розрахункового добового споживання в мінімально прийнятному режимі.

Номінальна потужність	1	2	3	4	5	6	7	8	9	10	11	12
Суммарна інсоляція, кВт•г / $м^2$ →	21.0	55.5	106.7	110.6	137.3	131.9	138.3	124.3	95.6	59.4	36.8	23.9
1.6 кВт	30 кВт•г	80 кВт•г	155 кВт•г	161 кВт•г	199 кВт•г	192 кВт•г	201 кВт•г	180 кВт•г	139 кВт•г	86 кВт•г	53 кВт•г	34 кВт·ч
1.8 кВт	34 кВт•г	90 кВт•г	174 кВт•г	181 кВт•г	224 кВт•г	216 кВт•г	226 кВт•г	203 кВт•г	156 кВт•г	97 кВт•г	60 кВт•г	39 кВт•г
2.0 кВт	38 кВт•г	101 кВт•г	194 кВт•г	201 кВт•г	249 кВт·ч	240 кВт•г	251 кВт•г	226 кВт•г	173 кВт•г	108 кВт•г	66 кВт•г	43 кВт•г
2.5 кВт	47 кВт•г	126 кВт•г б	242 кВт•г	251 кВт•г	312 кВт•г	300 кВт•г	314 кВт•г	282 кВт•г	217 кВт•г	135 кВт•г	83 кВт•г	54 кВт•г
3.2 кВт	61 кВт•г	161 кВт•г	310 кВт•г	322 кВт•г	399 кВт•г	384 кВт•г	402 кВт•г	361 кВт•г	278 кВт•г	172 кВт•г	107 кВт•г	69 кВт•г
5.3 кВт	101 кВт•г	267 кВт•г	514 кВт•г	533 кВт•г	662 кВт•г	636 кВт•г	667 кВт•г	599 кВт•г	461 кВт•г	286 кВт•г	177 кВт•г	115 кВт•г
8.0 кВт	152 кВт•г	404 кВт•г	776 кВт•г	805 кВт•г	999 кВт•г	960 кВт•г	1006 кВт•г	904 кВт•г	695 кВт•г	432 кВт•г	267 кВт•г	173 кВт•г
13.5 кВт	257 кВт•г	681 кВт•г	1310 кВт•г	1358 кВт•г	1686 кВт•г	1620 кВт•г	1699 кВт•г	1527 кВт•г	1174 кВт•г	729 кВт•г	452 кВт•г	293 кВт•г

Висновок. Двохкіловаттна сонячна батарея може підтримувати комфортний або близький до нього режим з травня до середини серпня і базові потреби з лютого по жовтень . Правда, в листопаді її потужності вистачить лише для аварійного режиму , а в грудні і січні навіть ці скромні вимоги вона не забезпечить. Лише номінальна потужність в 3.2 кВт дозволить розраховувати на аварійний мінімум протягом усього року, а період комфортного використання « сонячної електрики » розширюється на весь період довгих днів - з березня по вересень включно. .3 кВт номінальної потужності дозволяють в травні- серпні використовувати електрику від батарей практично без обмежень і круглий рік гарантують

базові потреби . 8 кВт уможливлюють цілорічне використання автономного електрики в помірному режимі , 13.5 кВт - в комфортному .

Література

1.Колот М.А., Левшов А.В., Коротков А.В. Алгоритм управления источниками и потребителями электроэнергии интеллектуального здания. Электромеханические и энергетические системы, методы моделирования и оптимизации. Сборник научных трудов XI Международной научно–технической конференции молодых ученых и специалистов в Кременчуге 10–11 апреля 2014 г. – Кременчуг: КрНУ, 2014. – С. хх–хх.

2. Стычинский З.А., Воропай Н.И. Возобновляемые источники энергии: теоретические основы, технологии, технические характеристики, экономика. – Иркутск 2010, – С. 28.

3. Кобец Б. Б.; Волкова И.О. Инновационное развитие электроэнергетики на базе концепции Smart Grid. – М.: ИАЦ Энергия, 2010. – С. 10-14.

УДК 621.391.3

Прохоров Д.Е.
ОНАЗ ім. О.С. Попова
danisproh@mail.ru

БЕЗПЕКА БЕЗПРОВОДОВИХ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІІ WI-FI

Анотація. *Проаналізовані можливості захисту бездротових локальних комп'ютерних мереж «Wi-Fi».*

Впровадження нових телекомунікаційних технологій призвели до того, що вони сприймаються вже не тільки як утилітарні засоби комунікації та доступу до інформації, але й є невід'ємною часткою життя та культури людства.

Метою даної роботи є дослідження технології бездротових локальних комп'ютерних мереж, аналіз методів обмеження доступу [1], порівняння методів аутентифікації та типи шифрування [1-4].

Wi-Fi – є джерелом підвищеного ризику несанкціонованого доступу. Крім того, проникнути в бездротову мережу простіше, ніж в звичайну, — не потрібно підключатися до проводів, досить опинитися в зоні прийому сигналу.

Бездротові мережі відрізняються від кабельних тільки на перших двох - фізичному (Phy) і частково канальному (MAC) - рівнях семирівневої моделі взаємодії відкритих систем. Вищі рівні реалізуються в проводових мережах, а реальна безпека мереж забезпечується саме на цих рівнях. Тому різниця в безпеці тих і інших мереж полягає у різниці в безпеці фізичного і MAC - рівнів. Якщо налаштуванню мережі не приділити належної уваги зловмисник може: дістати доступ до ресурсів і дисків користувачів Wi-Fi-мережі, а через неї і до ресурсів LAN; підслуховувати трафік, витягувати з нього конфіденційну інформацію; спотворювати інформацію, що проходить в мережі; -скористатися інтернет-трафіком; атакувати ПК користувачів і сервери мережі; упроваджувати підроблені точки доступу; розсилати спам, і здійснювати інші протиправні дії від імені вашої мережі.

Для захисту мереж передбачений комплекс заходів безпеки передачі даних. Різниця між WPA2 Personal і WPA2 Enterprise полягає в тому , звідки беруться ключі шифрування , що використовуються в механіці алгоритму AES. Для приватних (домашніх , дрібних) застосувань використовується статичний ключ (пароль, кодове слово, PSK (Pre - Shared Key)) мінімальною довжиною 8 символів, яке задається в настройках точки доступу, і у всіх клієнтів даної бездротової мережі однаковим. Для корпоративних застосувань , як випливає з назви , використовується динамічний ключ , індивідуальний для кожного працюючого

клієнта в даний момент. Цей ключ може періодичний оновлюватися по ходу роботи без розриву з'єднання , і за його генерацію відповідає додатковий компонент - сервер авторизації , і майже завжди це RADIUS -сервер.

Табл. 1. Параметри безпеки

Свойство	WPA	WPA 2 (Enterprise)
Ідентифікація	Користувач, компьютер	Користувач, компьютер
Авторизація	EAP або загальний ключ	EAP или загальний ключ
Целостність	64-bit Message Integrity Code (MIC)	CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code — CCM) Part of AES
Шифрування	Попакетний ключ через TKIP	CCMP (AES)
Розподіл ключів	Производное от PMK	Производное от PMK
Вектор ініціалізациї	Розповсюджений вектор, 65 бит	48-бит номер пакета (PN)
Алгоритм	RC4	AES
Довжина ключа, біт	128	до 256
Потрібна інфраструктура	RADIUS	RADIUS

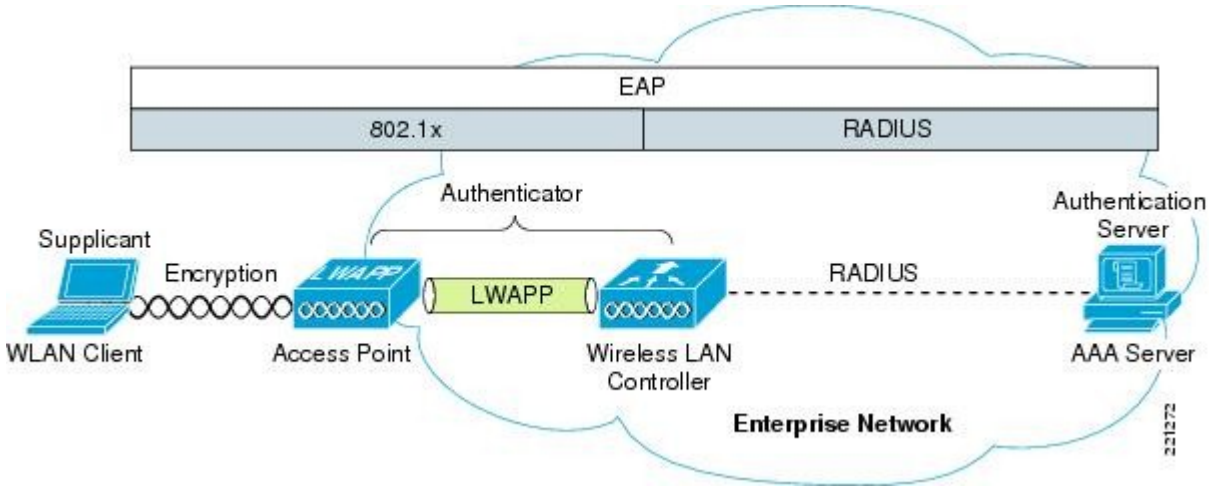


Рис. 1 EAP

Тут ми маємо справу з додатковим набором різних протоколів. На стороні клієнта спеціальний компонент програмного забезпечення, supplicant (зазвичай частина ОС) взаємодіє з авторизуйтесь частиною, ААА сервером. У даному прикладі відображена робота уніфікованої радіомережі, побудованої на легковагих точках доступу і контролері. У разі використання точок доступу «з мізками» всю роль посередника між клієнтів і сервером може на себе взяти сама точка. При цьому дані клієнтського супліканта по радіо передаються сформованими в протокол 802.1x (EAPOL), а на стороні контролера вони обертаються в RADIUS-пакети.

Застосування механізму авторизації EAP у нашій мережі призводить до того, що після успішної (майже напевно відкритої) аутентифікації користувача точкою доступу (спільно з контролером , якщо він є) остання просить к користувача авторизуватися (підтвердити свої повноваження) у інфраструктурного RADIUS –сервера.

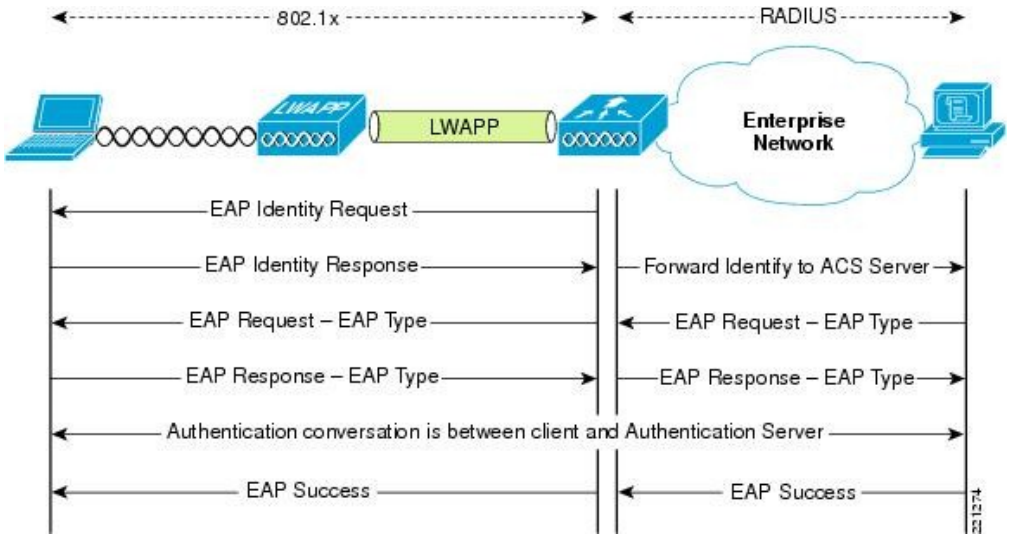


Рис. 2RADIUS -сервер

Використання WPA2 Enterprise вимагає наявності у вашій мережі RADIUS -сервера. На сьогоднішній момент найбільш працездатними є наступні продукти: Microsoft Network Policy Server (NPS) , колишній IAS - конфігурується через MMC, безкоштовний, але треба купити вінду; Cisco Secure Access Control Server (ACS) 4.2, 5.3 - конфігурується через веб-інтерфейс, наворочено по функціоналу , дозволяє створювати розподілені і відмовостійкі системи, коштує дорого; FreeRADIUS - безкоштовний, конфігурується текстовими конфігам , в управлінні та моніторингу не зручна.

При цьому контролер уважно спостерігає за подіями обміном інформацією , і чекає успішної авторизації , або відмови в ній . При успіху RADIUS -сервер здатний передати точці доступу додаткові параметри (наприклад, в якій VLAN помістити абонента , який йому привласнити IP-адресу, QoS профіль і т.п.). У завершенні обміну RADIUS -сервер дає можливість клієнту і точці доступу згенерувати і обмінятися ключами шифрування (індивідуальними , валідними тільки для даної сессіі).

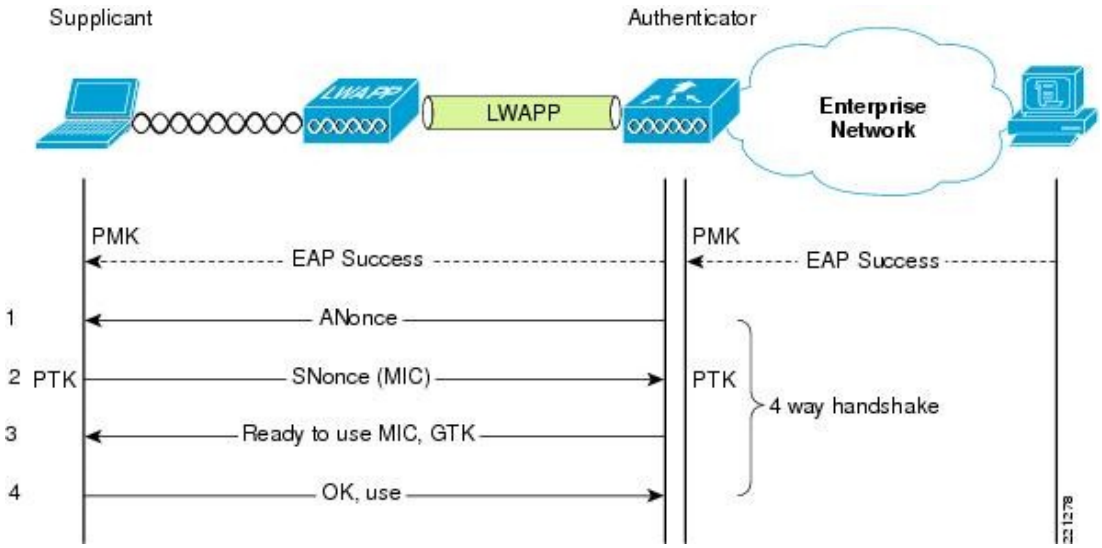


Рис. 3. Обмін ключами шифрування

Використовуемо протокол EAP є контейнерним , тобто фактичний механізм авторизації дається на відкуп внутрішніх протоколів. На даний момент скільки-небудь значиме поширення одержали наступні:

EAP - FAST (Flexible Authentication via Secure Tunneling) - розроблений фірмою Cisco; дозволяє проводити авторизацію за логіном - паролем , переданому всередині TLS

тунелю між супплікантом і RADIUS – сервером.

EAP-TLS (Transport Layer Security). Використовує інфраструктуру відкритих ключів (PKI) для авторизації клієнта і сервера (суппліканта і RADIUS-сервера) через сертифікати, виписані довіреною підтверджуючий центр (CA). Вимагає виписування і установки клієнтських сертифікатів на кожне бездротове пристрій, тому підходить тільки для керованої корпоративного середовища. Сервер сертифікатів Windows має засоби, що дозволяють клієнтові самостійно генерувати собі сертифікат, якщо клієнт - член домену. Блокування клієнта легко виробляється відкликанням його сертифіката (або через облікові записи).

EAP - TTLS (Tunneled Transport Layer Security) аналогічний EAP - TLS , але при створенні тунелю не вимагається клієнтський сертифікат. У такому тунелі , аналогічному SSL - з'єднанню браузера, проводиться додаткова авторизація.

PEAP - MSCHAPv2 (Protected EAP) - схожий з EAP - TTLS в плані початкового встановлення шифрованого TLS тунелю між клієнтом і сервером , що вимагає серверного сертифіката. Надалі в такому тунелі відбувається авторизація по відомому протоколу MSCHAPv2.

PEAP - GTC (Generic Token Card) - аналогічно попередньому , але вимагає карт одноразових паролів (і відповідної інфраструктури)є

Висновок. Отримати доступ до мережі , захищеної EAP - FAST , EAP - TTLS , PEAP - MSCHAPv2 можна, тільки знаючи логін-пароль користувача. Атаки типу перебору пароля, або спрямовані на уразливості в MSCHAP також неможливі або утруднені через те , що EAP - канал « клієнт-сервер» захищений шифрованим тунелем .

Література

1. Stewart S. Miller, Wi-fi security, 2003
2. Берд Киви журнал Компьютерра #34, Myths and truth

УДК 621.395.7

Родченко В.О.
Харківський національний університет радіоелектроніки
vita_rod@mail.ru
Науковий керівник – к.т.н., доц. Золотарьов В.А.

ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ БІБЛІОТЕЧНОЇ СИСТЕМИ ВУЗІВ ЗІ СПОРІДНЕНИМ ПРОФІЛЕМ НАВЧАННЯ

Анотація. *Було проаналізовано роботу електронних бібліотек 17 вищих навчальних закладів України та виявлено їх недоліки з позиції користувачі. На підставі цього спроектована корпоративна бібліотечна система між трьома Харківськими вузами зі спорідненим профілем навчання. Використовуючи бізнес-процесний підхід був створений новий модуль «Управління електронною бібліотекою». Даний модуль в подальшому може бути прийнятий в якості основи для програмної реалізації.*

Суттєву роль у підготовці майбутніх фахівців відіграє інформаційна система (ІС) «електронна бібліотека (ЕБ) вищого навчального закладу», що надає спеціалізовану навчальну та наукову інформацію

У роботі пропонується створення корпоративної бібліотечної системи (КБС) вузів спорідненого профілю, а саме об’єднання інформаційно-бібліотечних центрів Харківського національного університету радіоелектроніки, Національного технічного університету "Харківський політехнічний інститут", Національного аерокосмічного університету ім. М. Є. Жуковського "Харківський авіаційний інститут. Електронні бібліотеки даних вузів будуть

взаємодіяти на основі добровільності участі та взаємної вигоди в області накопичення, зберігання, пошуку і розповсюдження науково-технічної інформації.

Основною метою створення КБС є підвищення ефективності навчального процесу і науково-дослідних робіт, що проводяться у вузах.

Корпоративна бібліотечна система між трьома провідними технічними університетами Харкова забезпечить:

– підвищення ефективності інформаційного обслуговування за рахунок збільшення повноти наданої інформації та скорочення термінів обслуговування;

– підвищення ефективності інформаційно-бібліотечної діяльності КБС на основі координації та кооперації, а також шляхом взаємодії з іншими тематичними КБС;

– виключення дублювання при закупівлі та обробці інформації, створенні довідково-інформаційного фонду та організації інформаційного обслуговування;

– найбільш раціональне використання інформаційних ресурсів і технологій вузів КБС.

Для захисту інформації в КБС вузів спорідненого профілю обрано технологію IPsec, яка гарантує:

– цілісність переданих даних, тобто дані при передачі не перекручені, не втрачені і не про дубльовані;

– автентичність відправника, тобто, дані передані саме тим відправником, який довів, що він той. за кого себе видає;

– конфіденційність переданих даних, тобто дані передаються у формі, що запобігає їх несанкціонованому перегляду.

Так як інформаційна система електронних бібліотек використовується великою кількістю користувачів, то традиційні підсистеми управління доступом стають вкрай складними для адміністрування. Число зв'язків в них пропорційно добутку кількості користувачів на кількість об'єктів. Тому для даної інформаційної системи було прийнято рішення, використовувати рольове управління доступом.

Розроблений з використанням бізнес-процесного підходу модуль «Управління електронною бібліотекою» дозволяє сформувати вимоги до декомпозиції основної мети: забезпечення повною інформацією для прийняття рішень; представлення інформації з максимальною швидкістю та підготовленою для прийняття рішення (забезпечення надійного доступу до інформації; забезпечення ефективної оцінки і відбору даних з врахуванням їх цінностей); забезпечення контролю за інформаційними взаємодіями і узгодженістю рішень, що приймаються в системі (забезпечення максимальної простоти взаємодії користувача з персональним комп'ютером (ПК), забезпечення внутрішньосистемного представлення інформаційних зв'язків в процесі керування).

Побудова діаграми бізнес-варіантів використання системи «Управління електронною бібліотекою» для користувача та працівника бібліотеки дозволяє не тільки детально проаналізувати діяльність учасників системи для продуктивної роботи, але й з'ясувати місця їхнього перетинання (місця, куди інформація надходить від кількох користувачів системою, є найбільш конфліктними).

Розроблений модуль «Управління електронною бібліотекою», дозволяє здійснювати наступні нові функції: створення єдиного електронного каталогу бібліотек вищих навчальних закладів (на початковому етапі у м. Харкові); створення списку рекомендованої літератури, який формується на основі напрямку підготовки фахівця або його підписці до вибраних тем; опис змісту літератури згідно до запиту користувачів, додаванням до опису змісту; функція визначення найближчих бібліотек вищих навчальних закладів, в яких є вибрані ресурси; доставка літератури за місцем призначення.

Висновок: об'єднання бібліотечно-інформаційних центрів Харківського національного університету радіоелектроніки, Національного технічного університету та Національного аерокосмічного університету ім. М. Є. Жуковського відбулося з використанням технології VPN. Це дало змогу обмінюватися інформаційними ресурсами,

через відкриту мережу, при цьому забезпечуючи за допомогою протоколу IPSec достатній рівень захисту від несанкціонованого доступу ззовні. На онові розробленого модуля «Управління електронною бібліотекою» розробляється програмний продукт, який буде враховувати інформаційні зв'язки між структурними підмодулями, дозволить уникнути дублювань інформації в системі та оптимізує систему управління.

Література

1. Абызгильдин А.Ю., Электронная библиотека в вузе// Научные и технические библиотеки.– 2003.– №11.– 215с.
2. Лобузіна К.І. Сучасні підходи до інтеграції електронних інформаційних ресурсів бібліотек [Текст] / К.І.Лобузіна // Вісник Книжкової палати. – 2012. – №12. – С.15 – 12
3. Шаньгин В. Ф.Защитаинформациив компьютерных системах и сетях. / В.Ф.Шаньгин – М: ДМК Пресс, 2012. −592 с.
4. Соколова Н. В. Интеграция информационно-библиотечных ресурсов и сервисов – вариативность решений в рамках общей концепции / Н. В. Соколова // Электронная библиотека: современные технологии интеграции информационных ресурсов: сб.науч. тр. / [науч. ред. Е. Д. Жабко] – СПб., 2011. – С. 54 – 73.

УДК 004.056.5:004.735:004.738.5(0.83.94)

Розум'як М.В.
Національний авіаційний університет, м.Київ
Misharj1993@gmail.com
Науковий керівник – к.т.н., доц.. Пархоменко І.І.

ОРГАНІЗАЦІЯ БАГАТОРІВНЕВОГО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

Анотація. *Розглядається проблематика захисту корпоративних мереж, та спосіб організації багаторівневого захисту вузлів мережі. Приведено стандартний підхід до створення захищеної корпоративної мережі, та підхід на основі багаторівневого захисту. Розглянуто основні поняття щодо елементів захисту мережі. Наведено загальну схему комплексу засобів захисту корпоративної мережі.*

При побудові інформаційно-комунікаційних систем між офісами компаній гостро встає проблема захисту інформації, що циркулює всередині мережі.

Стандартним підходом до організації захисту інформації в корпоративних мережах є використання наступних засобів захисту інформації:

- фізичні засоби;
- апаратні засоби;
- програмні засоби;
- апаратно-програмні засоби;
- криптографічні та організаційні методи.

При цьому пропонується використання корпоративної брандмауер-системи, яка інтегрується в інфраструктуру мережі та забезпечує виконання встановлених правил доступу до захищеної мережі, а також відслідковує протоколи і послуги захисту, що використовуються.

Ця брандмауер-система є єдиною загальною точкою обміну даними між зовнішньою та захищеною корпоративною мережами і використовується як бар'єр між ними. При цьому ціллю є досягнення керованості та спостережності цієї точки. Цей підхід дає можливості аналізу даних, що виходять із мережі та надходять до неї, регламентування обміну даними

відповідно до політики безпеки, та реєстрації подій, що мають відношення до безпеки мережі.

Проте описаний вище підхід не є ідеальним рішенням тому що не досягається високого рівня захищеності на всіх рівнях мережі. Відштовхуючись від того, що універсальних засобів захисту не відомо, потрібно розглядати організацію багаторівневого захисту ресурсів мережі.

Для організації багаторівневого захисту необхідно визначити периметр мережі, межі внутрішньої мережі, та політику безпеки системи.

Периметр є границею мережі, яку слід посилено захистити. До складу периметру входять маршрутизатори, фаєрволи, системи виявлення вторгнень, пристрої VPN, ДМЗ-зона та екранована підмережа.

Маршрутизатори здійснюють здійснюють управління вхідним та вихідним трафіком, а також трафіком усередині мережі. Пограничний маршрутизатор є першим та останнім рубежем між захищеною та незахищеними мережами.

Файрвол або брандмауер аналізує трафік використовуючи набір правил, які вирішують передавати, чи ні трафік далі по мережі.

Система виявлення атак дозволяє виявляти та сигналізувати про вторгнення в мережу, або небезпечні події. Детектори виявлення атак розміщуються у найважливіших точках мережі. Детектори СВА шукають задані сигнатури критичних подій або статистично аналізують функціонування мережі і виявляють аномальні події.

VPN, віртуальна приватна мережа дозволяє організовувати захищені сеанси зв'язку використовуючи незахищені канали зв'язку.

Програмне забезпечення це додатки що функціонують у мережі. Важливим при цьому є архітектура програмного забезпечення. Оскільки основним завданням периметра мережі є захист даних що відносяться до додатків та сервісів.

Демілітаризована зона - це підмережа, що містить ресурси загального користування і підключається до брандмауера або іншого фільтруючого пристрою, який захищає її від зовнішніх вторгнень.

Екранована підмережа є областю, що розміщується поза брандмауером. Екранована підмережа використовується для ізоляції серверів, до яких необхідно забезпечити доступ із незахищеної мережі і які використовуються користувачами внутрішньої захищеної підмережі.

Внутрішня мережа – це мережа, яка захищена периметром. Вона містить всі сервери, робочі станції та інформаційну інфраструктуру.

Для забезпечення захисту внутрішньої мережі використовуються наступні пристрої "периметра": маршрутизатори для фільтрування вхідного та вихідного трафіка підмережі; внутрішні брандмауери для розподілу ресурсів; проксі-брандмауери для підвищення безпеки; детектори СВВ для моніторингу трафіка внутрішньої мережі.

У внутрішній мережі також використовуються: персональні брандмауери для посилення захисту хостів; антивірусне програмне забезпечення; посилення захисту операційної системи; керування конфігурацією системи; аудит.

Захист хоста – це процес зміни конфігурації операційної системи і додатків хоста з метою перекриття потенційних вразливостей системи. Посилення захисту хоста є останнім рубежем оборони системи.

Управління конфігурацією – процес встановлення і підтримки визначеної конфігурації для систем і пристроїв, що входять до мережі. Управління конфігурацією – це найкращий захід організації захищеної стандартної (базової) конфігурації, який призведе до зниження наслідків інцидентів до мінімуму. Управління конфігурацією дозволяє також контролювати неавторизоване встановлення програмного забезпечення.

Аудит – процес, який дозволяє контролювати стан захищеності мережі і своєчасно вносити зміни в архітектуру системи технічного захисту мережі.

Для вирішення проблеми захисту ресурсів та потоків корпоративних мереж пропонується побудова багаторівневої системи захисту інформації, що зображена на рисунку 1.

Виходячи з інформації наведеної вище, можна стверджувати, що багаторівневий захист корпоративної мережі дозволяє ефективніше організувати захист мережі та досягнути більш високий рівень захищеності, аніж традиційний підхід до захисту корпоративних мереж.

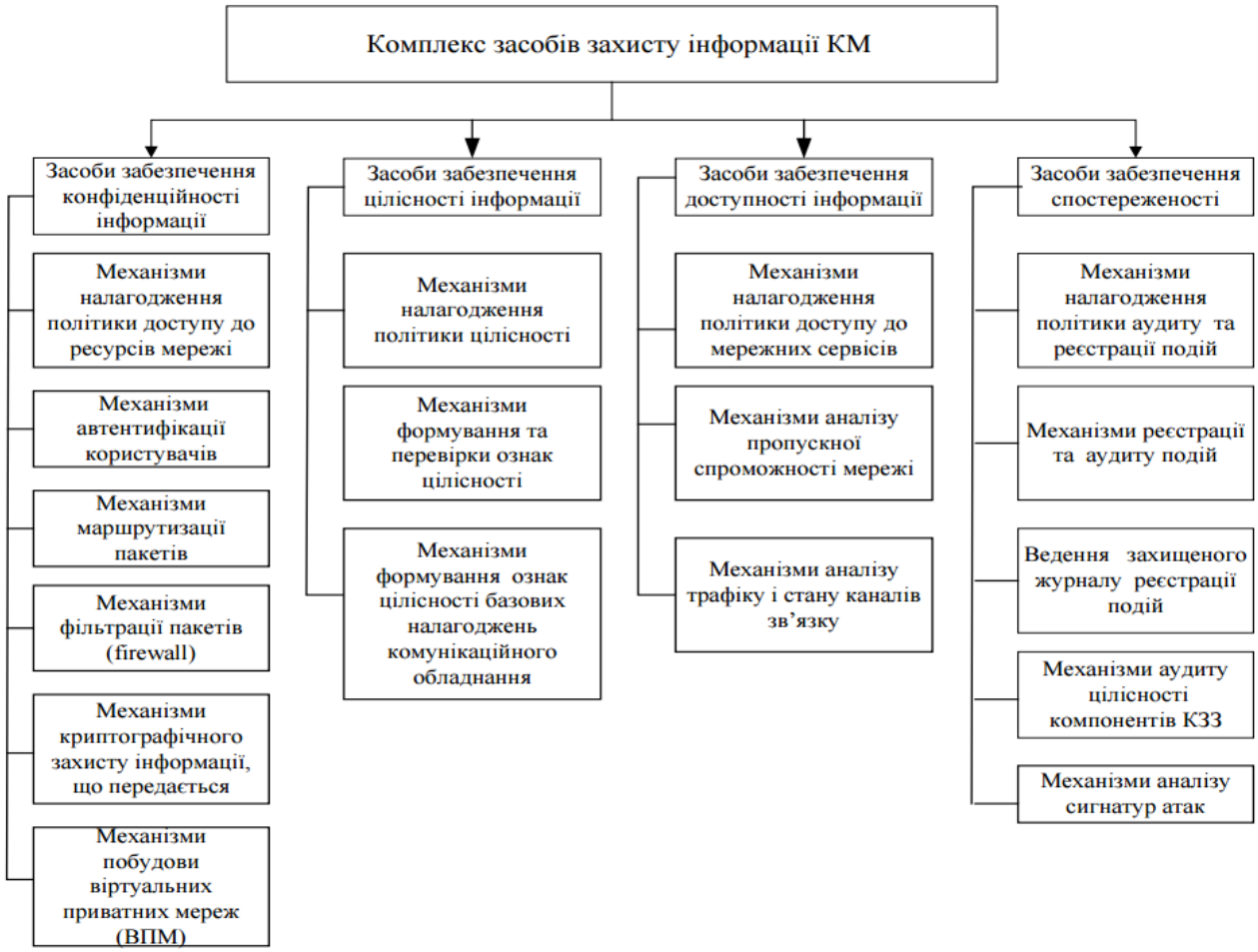


Рисунок 1. Схема комплексу засобів захисту корпоративної мережі

Література

1. Буточнов О.М., Гончар Г.В., Деревянко С.М., Короленко М.П. Захист інформації в комунікаційні мережі зв'язку ЄДАПС. // К.: Вісті Академії інженерних наук України. 2005, №2, с 37

2. Варінти захисту від загроз в комунікаціях розподілених мереж [Електронний ресурс] / В'ячеслав Василенко // Режим доступу до журн. : http://pnzzi.kpi.ua/15/15_p104.pdf

3. Методи захисту інформації в корпоративних ІС [Електронний ресурс] / Режим доступу до журн. : http://tmb.org.ua/new/index.php/i-i/4-/257-2013-09-20-08-52-30.html

УДК 621.396.2

Романов М. В.
Харьковский национальный университет радиоэлектроники
maxromanov4669@gmail.com
Научный руководитель – проф. Зеленин А.Н.

МОДЕЛИРОВАНИЕ РАБОТОСПОСОБНОСТИ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Аннотация. *Рассматриваются математические методы оценки надежности беспроводных сенсорных сетей и программные продукты для имитационного моделирования беспроводных сенсорных сетей, проводится их анализ с целью выбора системы, наиболее подходящей для оценки работоспособности беспроводных сенсорных сетей и с ее помощью оценивается влияние помех и мощности передачи радиосигнала на работоспособность беспроводных сенсорных сетей.*

В настоящее время распределенные системы все шире входят в нашу жизнь. Одним из направлений современных распределенных систем являются беспроводные сенсорные сети.

Беспроводная сенсорная сеть – это распределённая, самоорганизующаяся сеть множества датчиков (сенсоров) и исполнительных устройств, объединенных между собой посредством радиоканала [1]. Причем область покрытия подобной сети может составлять от нескольких метров до нескольких километров за счет способности ретрансляции сообщений от одного элемента к другому [2].

В данной работе на основании анализа и в соответствии с поставленными целями работы была выбрана система моделирования Castalia, для которой были разработаны модули, позволяющие выполнить моделирование влияния помех на надежность передачи пакета данных между двумя узлами и надежность сбора информации беспроводной сенсорной сетью.

При исследовании влияния помех на надежность коммуникационной среды между двумя узлами было получено, что с возрастанием величины помех число полученных пакетов не падает значительно, то есть можно говорить, что надёжность здесь уже не зависит от уровня помех, что может быть обусловлено хорошим протоколом канального уровня.

При исследовании влияния мощности радио-модуля на надежность коммуникационной среды между двумя узлами при уровне мощности в -5dBm было получено около семисот пакетов. С возрастанием величины мощности начиная с -3dBm число полученных пакетов возросло до восьмисот и стабильно, то есть можно говорить, что надёжность здесь уже не зависит от уровня мощности радио-модуля.

На основе проведенных исследований сделаны следующие выводы: при оценке надежности передачи пакета данных между двумя узлами с увеличением уровня помех до определенного значения сильного падения надежности не происходит, надежность связи между узлами зависит от топологии, уровень мощности сигнала не влияет существенно на надежность; при оценке надежности сбора информации сетью для рассмотренной сети колебания надежности не столь существенны при различных уровнях помех, что может быть обусловлено хорошими алгоритмами канального уровня.

Литература

1. Нечаев Д.Ю., Чекмарев Ю.В. Надежность информационных систем. – М.: ДМК Пресс, 2012. – 64 с.

2. Шахнович И.А. Современные технологии беспроводной связи. - М.: Техносфера, 2006. - 288 с.

УДК 004.045:621.396.967.2

Свид І.В., Обод А.І., Штих І.А.
ХНУРЕ
iryna.svyd@nure.ua

МЕТОДИ ПІДВИЩЕННЯ ЯКОСТІ НФОРМАЦІНОГО ЗАБЕЗПЕЧЕННЯ СПОЖИВАЧІВ ВТОРИННИХ СИСТЕМ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

Анотація. *Наводяться методи розв'язування суперечностей у інформаційному забезпеченні споживачів вторинних систем спостереження повітряного простору за рахунок спадкоємного переходу до запитальних каналів та запитальних систем передачі польотної інформації на основі включення просторових координат повітряних об'єктів до складу польотної інформації.*

Інформаційне забезпечення (ІЗ) системи використання повітряного простору здійснюється системами спостереження (СС) [1, 2], як правило, сумісними, які включають до свого складу первинну та одну чи дві вторинні (запитальні). Первинні СС, у традиційній побудові, перетворилися з інформаційного засобу в засіб небезпеки. Дійсно, створення високоточної зброї й оцінка місця розташування випромінюючих об'єктів засобами радіорозвідки поза зоною видимості СС не залишають шансів захисту останнього від вогневого впливу. Одним з ефективних способів зниження уразливості первинних СС до вогневого впливу є перехід від однопозиційної до багатопозиційної (БП) [1], зокрема до мережевої [2], побудови. Вторинні СС побудовані за принципами: несинхронної мережі; відкритих одноканальних систем масового обслуговування з відмовами. Реалізація у цих системах принципу обслуговування першого, правильно прийнятого, сигналу запиту не дозволяє віднести їх до завадостійких систем. Така побудова вторинних СС дозволяє стверджувати, що зацікавлена сторона одержує від таких систем значно більше інформації у порівнянні зі стороною, що експлуатує їх [3]. Крім того, сучасні вторинні СС не мають можливості роботи в рознесеному режимі. Ця особливість не дозволяє вирішити інформаційну задачу ідентифікації повітряних об'єктів (ПО) без розміщення на приймальних (невипромінюючих) пунктах БП СС вторинних СС, тобто випромінюючих об'єктів, що приводить до демаскування приймальних пунктів БП первинних СС. Таким чином, сучасна побудова вторинних СС обумовила ряд суперечностей у їхньому спільному функціонуванні з первинними СС у ІЗ користувачів.

Як показано у [4], інтегральним показником якості (ІПЯ) ІЗ сумісної СС може бути ймовірність ІЗ, яка може бути записана як

$$P_{inf} = D_{11}, D_{12}, D_{13}, P_{ppi}, P_{obe}, P_{por1}, P_{por2},$$

де P_{ppi} – імовірність правильного прийому ПІ, P_{obe} - імовірність об'єднання координатної та польотної інформації вторинної СС, P_{por1} – імовірність порівняння координатної інформації первинної та вторинної СС, P_{por2} – імовірність порівняння координатної інформації первинної та ідентифікаційної СС.

Імовірності правильного виявлення ПО кожним каналом сумісної СС $P_i = D_{1i}$, є функціями

$$D_{1i} = f(D_{0i}, F_{0i}, C_i, P_0) = f(q_{0i}, z_{0i}, C_i, P_0), \quad (1)$$

де $z_0(C)$ – аналоговий (цифровий) поріг виявлення сигналу (ПО), q_{0i} – відношення с/ш у каналі обробки, P_0 – коефіцієнт готовності (КГ) відповідача літака, що є характерним для вторинної та ідентифікаційної СС.

Вищевикладене показує що, з одного боку, запитальні СС вносять суттєвий вклад у ІЗ, а з іншого боку принцип побудови останніх не може забезпечити потрібну завадостійкість цих систем і, як наслідок, якість ІЗ.

Слід зазначити що недоліки запитальних СС значною мірою визначаються тим, що вони побудовані на принципах системи спостереження маючи при цьому два канала (запиту та відповіді) передачі сигналів запиту та відповіді. Таким чином, здійснив передачу просторових координат ПО за каналом відповіді у СС на спадкоємній основі, можливо перетворити її у запитальну систему передачі польотної інформації (СППІ).

Для запитальних СППІ не потрібно здійснювати вимір координат ПО на запитувачі, так як вони передаються з борту ПО. При цьому слід зазначити, що просторові координати ПО на борту обчислюються з значно більшою якістю у порівнянні з обчисленням їх на запитувачі. ІПЯ при використанні запитальних СППІ можна записати як

$$P_{inf} = D_{11}, P_{ppi}, P_{por1}, P_{por2}. \qquad (2)$$

Оцінимо можливість передачі просторових координат ПО за каналом відповіді запитальних СППІ. На рис. 1 наведені розрахунки імовірності передачі польотної інформації за каналами існуючих запитальних СС при передачі 12-ти розрядного інформаційного коду в залежності від КГ та щільності завад у каналі відповіді.

На рис. 2 наведені залежності $P_{ppi} = f(P_0, \lambda\tau)$ при передачі 50-ти розрядного інформаційного коду за існуючими стандартами каналу передачі польотної інформації. Розрахунки показують, що при щільності завад у каналі відповіді $\lambda\tau = 0{,}02$ запропонований варіант ІЗ показує задовільну якість.

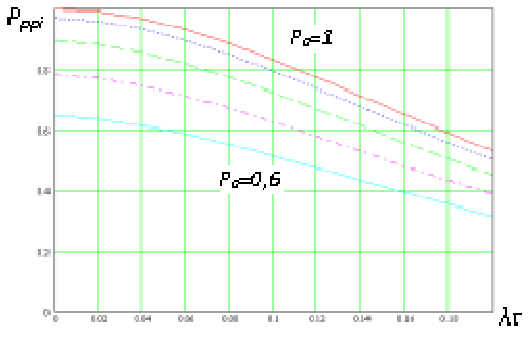


Рис. 1. Імовірність передачі польотної інформації

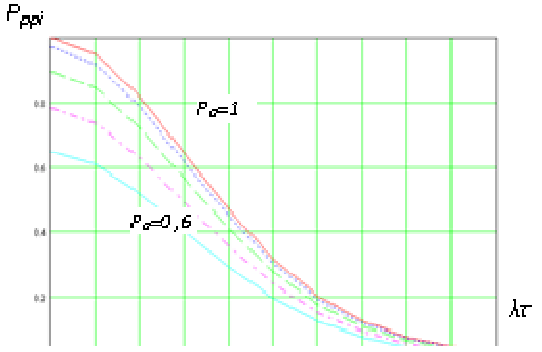


Рис. 2. Імовірність передачі польотної інформації

Як показано в [5] суттєвий вклад у зниження завадостійкості запитальних СППІ дає обраний метод передачі на основі позиційного коду. Використання багатопозиційних методів модуляції дозволить зменшити часову базу сигналу відповіді і, як наслідок, підвищити завадостійкість запитальних СППІ.

Зауважимо, що у запропонованому варіанті передача польотної інформації здійснюється за принципом «точка-точка». Перехід до принципу передачі «точка-багатоточка» запропонованому у [6, 7] дозволяє змінити принцип обслуговування запитувачів.

Одним з таких методів передачі інформації у запитальних СППІ є спосіб з адресною відповіддю. Розрахунки імовірності передачі неспотвореної інформації каналу запиту

передачі інформації з адресною відповіддю наведено на рис. 3. Розрахунки виконані при наявності у каналі запиту некорельованих завад інтенсивністю 5000 та каналі відповіді некорельованих завад інтенсивністю 1000 при передачі інформаційної посилки у складі 12, 50 та 100 розрядів.

Наведені розрахунки дозволяють зробити наступні висновки:

– реалізація запитального каналу передачі польотної інформації з включенням у склад передаваємої інформації просторових координат ПО дозволяє реалізувати адресний метод відповіді, що призводить до суттєвого підвищення якості ІЗ, за рахунок переходу від обслуговування окремого запитувача до обслуговування мережі;

– збільшення кількості розрядів передаваємої інформації у запитальному каналі передачі показує задовільну завадостійкість.

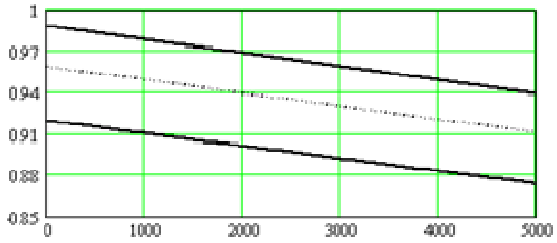


Рис. 3. Імовірність передачі неспотвореної інформації запитальним каналом передачі ПІ

Література

1. Farina A. Radar Data Processing Introduction and Tracking. Vol.1. / A.Farina, F.A. Studer. – Research Studies Press. Letch worth England, 1985. –350 p.

2. Lok J.J. C^2 for the air warrior // Jane's International Defense Review. – October 1999. – V.2. – P. 53-59.

3. Обод І.І. Завадозахищеність запитальних систем спостереження повітряного простору / І.І.Обод, І.В.Свид, І.А.Штих. – Харків.:ХНУРЕ, 2014.- 310 с.

4. Обод І.І. Інформаційна мережа систем спостереження повітряного простору / І.І.Обод, О.О.Стрельницький, В.А.Андрусевич. – Харків.:ХНУРЕ, 2015.- 270 с.

5. Обод І.І. Оцінка якості передачі інформації у запитальних каналах передачі систем спостереження повітряного простору /І.І.Обод, О.П.Черних, І.В.Свид // Східно-Європейский журнал передових технологій: - № 3/11(51). – Х.: 2011. - С. 52-54.

6. Обод І.І., Свид І.В. Запитальний спосіб передачі інформації. Патент на корисну модель № 58523.

7. Обод І.І., Свид І.В., Шевцова В.В. Запитальний спосіб передачі інформації. Патент на корисну модель № 79487.

УДК 621.39

Selezniov O. I., TE-6.01m
sech_92@ukr.net
ONAT named after A.S.Popov
Supervisor – associate professor Shmeleva T.R.

ANALYSIS OF OPENFLOW PROTOCOL

Abstract. *Basic information about OpenFlow protocol is given. OpenFlow switch structure is considered. General principles of flow processing, such as sequential flow entries matching, with OpenFlow protocol appliance are described. Simplest flow tables interaction is studied. Hybrid switching pipeline is mentioned. A table miss case is considererd.*

The OpenFlow protocol is the only standards-based SDN protocol in the world to abstract the network control plane (where forwarding decisions are made) from the network data plane (where packets are forwarded), which enables a network engineer to create a single network control policy that universally programs the entire network fabric. OpenFlow enables a central controller to remotely provision the underlying data plane device forwarding tables in a common, scalable way, and eliminates the vendor-specific, proprietary nature of legacy networking equipment. Specifically, OpenFlow enables automation through a centralized software controller that eliminates the need to program devices and interfaces for every network service request.

The OpenFlow protocol is managed by the Open Networking Foundation (ONF), which was an outgrowth of principal research done at Stanford University's Clean Slate Program led by Big Switch Networks founder, Guido Appenzeller. The ONF, a non-profit user-governed consortium, has now grown to include some of the largest users in the world, including Google, Facebook, Yahoo!, Deutsche Telekom, Verizon and Goldman Sachs. Given the explicitly user-driven governance model of the ONF, the OpenFlow protocol is not subject to conventional vendor politics and manipulation that plagues other vendor-controlled industry standards bodies.

An OpenFlow Switch consists of one or more flow tables and a group table, which perform packet lookups and forwarding, and an OpenFlow channel to an external controller (Figure 1). The switch communicates with the controller and the controller manages the switch via the OpenFlow protocol. Using the OpenFlow protocol, the controller can add, update, and delete flow entries in flow tables, both reactively (in response to packets) and proactively. Each flow table in the switch contains a set of flow entries; each flow entry consists of match fields, counters, and a set of instructions to apply to matching packets

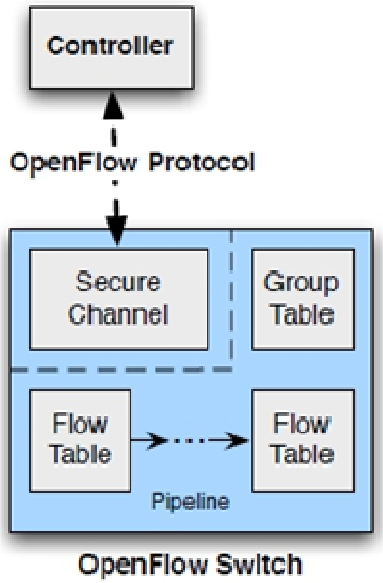


Figure 1. Main components of an OpenFlow switch.

Matching starts at the first flow table and may continue to additional flow tables. Flow entries match packets in priority order, with the first matching entry in each table being used. If a matching entry is found, the instructions associated with the specific flow entry are executed. If no match is found in a flow table, the outcome depends on configuration of the table-miss entry: for example, the packet may be forwarded to the controller over the OpenFlow channel, dropped, or may continue to the next flow table.

Flow entries may forward to a port. This is usually a physical port, but it may also be a logical port defined by the switch or a reserved port defined by this specification. Reserved ports may specify generic forwarding actions such as sending to the controller, flooding, or forwarding using non-OpenFlow methods, such as "normal" switch processing, while switch-defined logical ports may specify link aggregation groups, tunnels or loopback interfaces.

Actions associated with flow entries may also direct packets to a group, which specifies additional processing. Groups represent sets of actions for flooding, as well as more complex forwarding semantics (e.g. multipath, fast reroute, and link aggregation). As a general layer of indirection, groups also enable multiple flow entries to forward to a single identifier (e.g. IP forwarding to a common next hop). This abstraction allows common output actions across flow entries to be changed efficiently.

The group table contains group entries; each group entry contains a list of action buckets with specific semantics dependent on group type. The actions in one or more action buckets are applied to packets sent to the group.

OpenFlow-compliant switches come in two types: OpenFlow-only, and OpenFlow-hybrid. **OpenFlow-only** switches support only OpenFlow operation, in those switches all packets are processed by the OpenFlow pipeline, and can not be processed otherwise. **OpenFlow-hybrid** switches support both OpenFlow operation and normal Ethernet switching operation, i.e. traditional L2 Ethernet switching, VLAN isolation, L3 routing (IPv4 routing, IPv6 routing...), ACL and QoS processing. Those switches should provide a classification mechanism outside of OpenFlow that routes traffic to either the OpenFlow pipeline or the normal pipeline.

The OpenFlow pipeline of every OpenFlow switch contains multiple flow tables, each flow table containing multiple flow entries. The OpenFlow pipeline processing defines how packets interact with those flow tables (Figure 2). An OpenFlow switch is required to have at least one flow table, and can optionally have more flow tables. An OpenFlow switch with only a single flow table is valid; in this case pipeline processing is greatly simplified.

The flow tables of an OpenFlow switch are sequentially numbered, starting at 0. Pipeline processing always starts at the first flow table: the packet is first matched against flow entries of flow table 0. Other tables may be used depending on the outcome of the match in the first flow table.

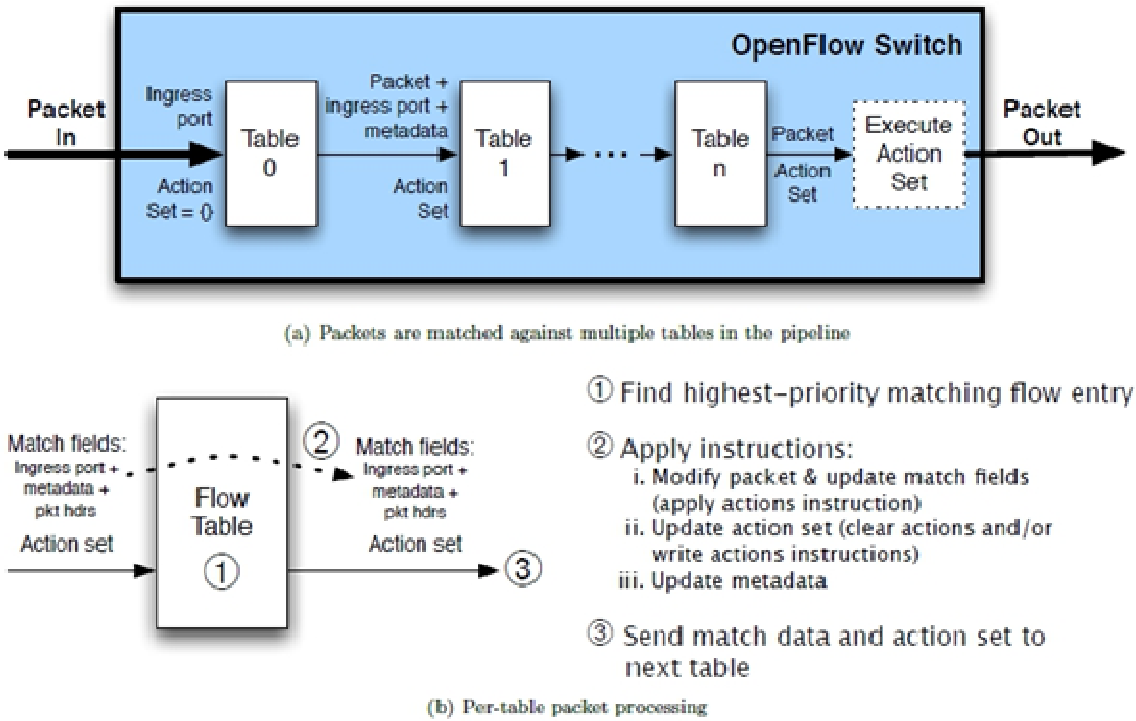


Figure 2. Packet flow through the processing pipeline

When processed by a flow table, the packet is matched against the flow entries of the flow table to select a flow entry. If a flow entry is found, the instruction set included in that flow entry is executed, those instructions may explicitly direct the packet to another flow table, where the same process is repeated again. A flow entry can only direct a packet to a flow table number which is

greater than its own flow table number, in other words pipeline processing can only go forward and not backward. Obviously, the flow entries of the last table of the pipeline can not include the Goto instruction. If the matching flow entry does not direct packets to another flow table, pipeline processing stops at this table. When pipeline processing stops, the packet is processed with its associated action set and usually forwarded.

If a packet does not match a flow entry in a flow table, this is a table miss. The behavior on a table miss depends on the table configuration. A table-miss flow entry in the flow table may specify how to process unmatched packets: Options include dropping them, passing them to another table or sending them to the controller over the control channel via packet-in messages.

Conclusion. Currently OpenFlow protocol development is governed by Open Networking Foundation, which includes numerous world networking leaders. This protocol is the most well described one for southbound interaction in SDN.

Logical components of OpenFlow switch are flow tables, group table and secure channel, through which a controller manages records in tables. Also OpenFlow switch may contain a traditional pipeline for a hybrid operation mode.

References

1. www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf
2. http://www.bigswitch.com/company/sdn-technology
3. http://networkstatic.net/openflow-proactive-vs-reactive-flows/

УДК 37.018.43:004.773.5:378

Селіванов С. В.
ОНАЗ ім. О.С.Попова
Wertys6@rambler.ru
Науковий керівник – доц. Царьов Р.Ю.

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ СИСТЕМ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Аннотация. *Рассматриваются перспективы использования дистанционного обучения в Украине.*

Бурное развитие информационных сетей и информационных технологий привело к тому, что такие услуги как образование можно предоставлять удаленно.

Система Дистанционного Обучения (СДО) - это программное обеспечение для организации дистанционной формы обучения, дополнительной системы поддержки учебного процесса, электронного документооборота, для создания электронных обучающих материалов, администрирования и оценки успеваемости в рамках изучаемой дисциплины, проведения консультаций. Дистанционное обучение подразумевает активное использование интернет технологий, позволяющих проводить обучение, если учитель и ученик находятся на расстоянии друг от друга.

Достоинства системы дистанционного обучения:

1. Технологичность - обучение с использованием современных программных и технических средств делает электронное образование более эффективным.

2. Доступность и открытость обучения - возможность учиться удалено от места обучения, не покидая свой дом или офис.

3. Свобода и гибкость - появляются новые возможности для выбора курса обучения. Можно одновременно учиться в разных местах, сравнивая курсы между собой.

4. Индивидуальность систем дистанционного обучения. Дистанционное обучение носит более индивидуальный характер обучения, более гибкое, обучающийся сам определяет темп обучения.

5. Внедрение дистанционного обучения уменьшает нервозность студентов при сдаче зачета или экзамена. Снимается субъективный фактор оценки.

Недостатки системы дистанционного обучения:

1. Отсутствие прямого очного общения между студентами и преподавателем.
2. Необходимость в персональном компьютере и доступе в Интернет, а также необходимость постоянного доступа к источникам информации.
3. Проблема аутентификации пользователя при проверке знаний. Есть необходимость в более совершенных системах авторизации (например: биометрической).
4. Для дистанционного обучения необходима жесткая самодисциплина и сознательность учащегося.

Мировая тенденция перехода к дистанционным формам образования прослеживается в росте числа вузов, ведущих подготовку по новым информационным технологиям. На рисунке 1 показана динамика распространения дистанционного обучения в мире [1].

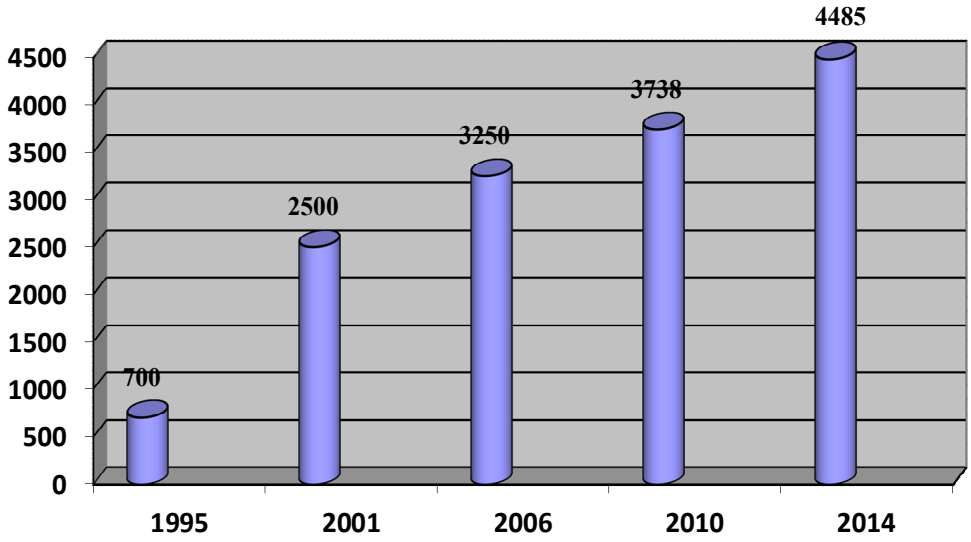


Рисунок 1 Динамика использования дистанционного образования в мире

Учитывая статистические данные по Украине о количестве ВУЗов [2], распространении Интернета [3] и исходя из того какое количество центров дистанционного образования на базе ВУЗов Украины насчитывается на данный момент [4] можно вывести статистику роста числа ВУЗов с дистанционным образованием по периодам. Данная статистика показана в виде графика на рисунке 2.

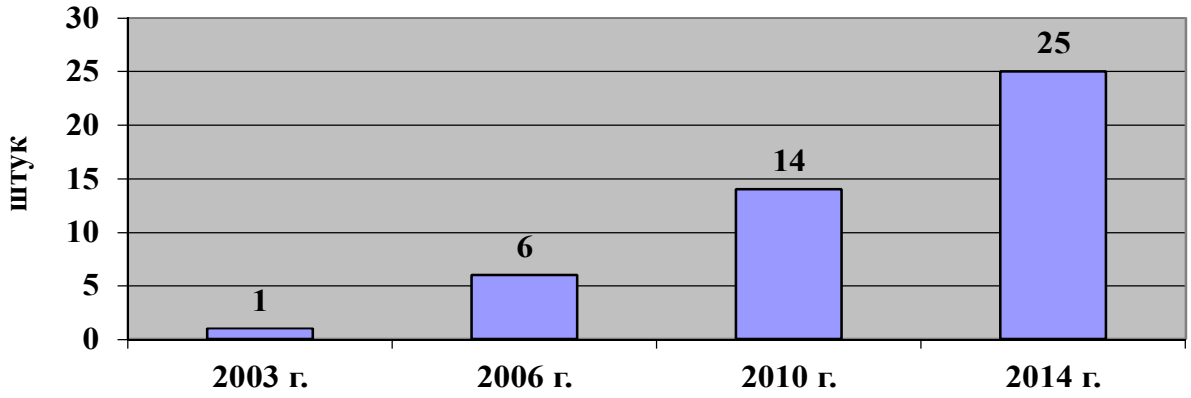


Рисунок 2 – Статистика роста числа ВУЗов Украины с ДО (по основным годам)

Для сравнения приведем количество ВУЗов с дистанционным образованием в таких странах: США [8] [9], Белоруссия [7], Польша [10], Россия [5] [6]. И для наглядности изобразим эти данные на диаграмме (рисунок 3).

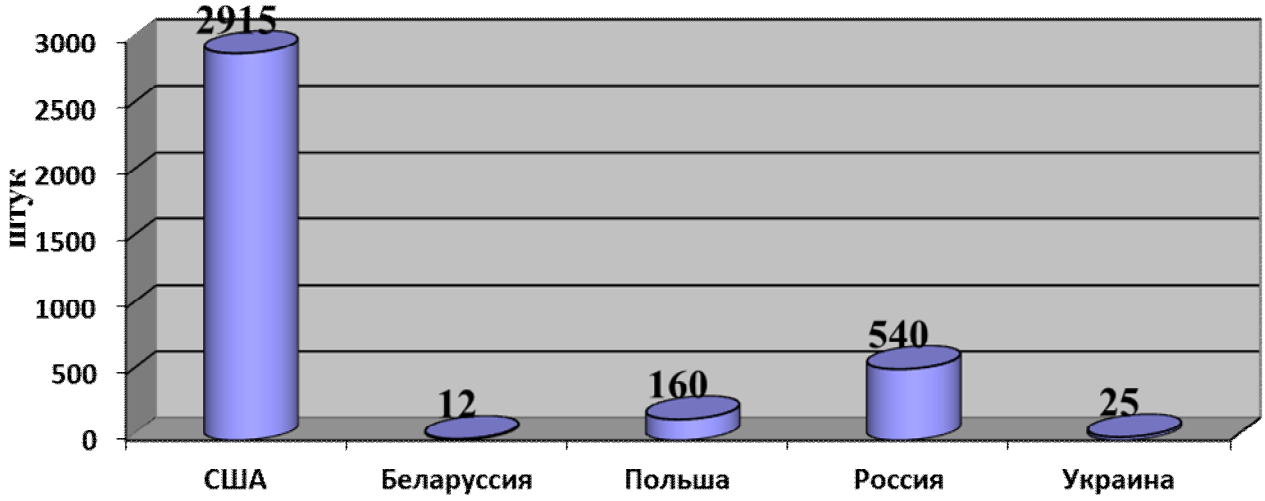


Рисунок 3 – Диаграмма количества ВУЗов с дистанционным образованием по странам

Как видно из диаграммы системы дистанционного образования в Украине развиваются очень медленно по сравнению с большинством стран, но достаточно уверенно. Главные причины медленного развития систем дистанционного образования в Украине:

1. Трудности с идентификацией студентов, обучающихся дистанционно – на данном этапе развития технологий проверить, кто именно сдает экзамен достаточно проблематично. Один из надежных вариантов решения - внедрение технологий биометрического контроля (сенсор отпечатка пальца).
2. Низкая пропускная способность электронных сетей (особенно это заметно во время проведения экзаменационных или обучающих телеконференций на удаленных площадках в небольших населенных пунктах).
3. Малое количество опытных преподавателей, знакомых с новейшими технологиями дистанционного общения.
4. Присутствующее недоверие к такой форме обучения.
5. Недостаточная поддержка и финансирование программ разработки, внедрения и развития дистанционного обучения.

Не смотря на эти причины прогноз развития систем дистанционного образования в Украине положительный, так как такой метод получения высшего образования становится

все более популярнее в нашей стране. Такая тенденция роста свидетельствует о наличии спроса на услуги дистанционного образования и с учетом этого, а так же с учетом реформы системы образования можно констатировать, что в Украине сформированы все условия для развития систем дистанционного образования.

Литература

1) По данным Евразийской Ассоциации дистанционного образования. [Электронный ресурс]. - Режим доступа: http://www.edu.ru

2) Державна Служба Статистики України. Вищі навчальні заклади. [Электронный ресурс]. - Режим доступа: http://www.ukrstat.gov.ua/operativ/operativ2005/osv_rik/osv_u/vuz_u.html

3) Ukraine Internet Usage and Marketing Report. [Электронный ресурс]. - Режим доступа: http://www.internetworldstats.com/euro/ua.htm

4) Центри дистанційної освіти на базі ВНЗ України. [Электронный ресурс]. - Режим доступа: http://www.osvita.org.ua/distance/ukraine/centers/

5) E-learning растет на демографических дрожжах. [Электронный ресурс]. - Режим доступа: http://www.hr-portal.ru/article/e-learning-rastet-na-demograficheskih-drozhzhah

6) Росстат. Образовательные организации высшего образования. [Электронный ресурс]. - Режим доступа: http://www.gks.ru/free_doc/new_site/population/obraz/vp-obr1.htm

7) Соколова М.В., Пупцев А.Е., Солодовникова М.Л.// Научное издание//Дистанционное образование в высшей школе Беларуси в контексте общества знания: проблемы и перспективы// Издательство Европейского гуманитарного университета г. Вильнюс, Литва, 2013. - С. 116-136.

8) Cnews. Дистанционное обучение в США и Европе. [Электронный ресурс]. - Режим доступа: http://www.cnews.ru/reviews/free/national2006/articles/do_usa/index.shtml

9) Wikipedia. Высшее образование в Польше. Высшее образование в США. [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/

УДК 621.395.7

Семенюк О.О.
ОНАЗ ім. О.С.Попова
semenyuk1994@icloud.com
Науковий керівник – доц. ОНАЗ Нікітченко В.В.

ПОРІВНЯЛЬНИЙ АНАЛІЗ MV* ФРЕЙМВОРКІВ ПОБУДОВАНИХ НА JAVASCRIPT

Анотація. *Розглядається сукупність MV* фреймворків для побудови front-end частини односторінкових web-додатків. На сьогоднішній день представлені десятки різних фреймворків, у кожного з яких є свої переваги і недоліки, тому вибір одного із них являє собою не зовсім просту задачу. Під час дослідження формується сукупність критеріїв для порівняння декількох найпоширеніших у застосуванні фреймворків, після чого здійснюється аргументований вибір примірника програмного забезпечення з декількох наявних.*

При побудові односторінкової програми або при створенні складного інтерфейсу користувача, або просто при скороченні кількості запитів HTTP розробники часто прибігають до використиння MV* фреймворку.

MV* фреймворк – бібліотека, яка забезпечує розробникам простий шлях до організації коду, використовуючи варіації патерну проектування, відомого як MVC (Model-View-Controller). MVC – мабуть, найпоширеніший шаблон проектування, за допомогою якого модель додатку та інтерфейс взаємодії з користувачем розділені на три окремі компоненти таким чином, щоб модифікація одного з компонентів надавала мінімальний

вплив на інші. Дана схема проектування часто використовується для побудови архітектурного каркаса, коли переходять від теорії до реалізації в конкретній предметній області [1]. Основна мета застосування цієї концепції полягає в відокремленні бізнес-логіки – моделі, від її візуалізації – уявлення (виду). За рахунок такого поділу підвищується можливість її повторного використання.

MVC-фреймворки на JavaScript, котрі допомагають у структуруванні коду, не завжди слідують описаному зразку, тому ми називаємо такі фреймворки патернами MV*, тобто, уявлення та модель, швидше за все, будуть, але до них додасться щось інше ніж просто контролер.

Вибір відповідного JavaScript MV* фреймворку для проекту кардинально впливає на нашу можливість виконувати завдання вчасно і підтримувати такий код у майбутньому. Web швидко розвивається, старі методики відходять у минуле і на зміну їм приходять нові, більш досконалі. На сьогоднішній день існує багато MV* фреймворків – Angular, Ember, React, Backbone, CanJS, ExtJS, Meteor, та ін. Нам потрібен надійний, перевірений фреймворк, але такий, щоб він нас не обмежував.

Завдання вибору JavaScript MV* фреймворку відноситься до категорії слабко структурованих. А значить, для її розв'язання використовують методи багатокритерійного прийняття рішень, такі як MAUT (Multi-Attribute Utillity Theory) – багатокритерійна теорія корисності, AHP (Analytic Hierarchy Process) – метод аналізу ієрархій, і ELECTRE (Elimininationation Et Choix Traduisant la Realite).

Приведемо алгорим встановлення узагалених показників якості та порівняння примірників JavaScript MV* фреймворків:

1. Формування списку альтернатив;

2. Вибір критеріїв оцінки, а також вибір додатковик критеріїв, які враховують специфіку данних об’єктів дослідження.

3. Вибір методу багатокритеріальної оцінки, який буде максимально враховувати особливості досліджуваних об’єктів.

4. Аналіз існуючих альтернатив, відповідно з обраним методом багатокритеріальної оцінки.

5. Визначення результатів дослідженя та формування висновків щодо якості об’єктів дослідження.

Спочатку, зі всього різоманіття зразків фреймворків оберемо декілька найпоширеніших для їх подальшої оцінки, а саме: Angular; Ember; CanJS; Backbone.

На другому етапі алгоритму будемо спиратись на положення міжнародного стандарту якості програмного забезпечення ISO/IEC 9126 [4]. Для більш повної оцінки досліджуваних зразків окрім типових критеріїв якості визначимо додаткові критерії.

Отриману структуру критеріїв приведемо на рис.1.

Маючи множину критеріїв оцінювання, потрібно робити вибір не за кожним критерієм окремо, а використовуючи деяку інтегральну оцінку, отриману аналітичним шляхом.

Дана задача має такі відмінні риси:

– невелика кількість альтернатив;

– завдання слабо структурована, тобто критерії оцінки мають в більшості випадків не кількісний, а якісний характер;

– характеристики якості деталізуються більш конкретними вкладеними характеристиками.

Все це вказує на доцільність використання методу аналізу ієрархій (AHP), який найбільш точно враховує особливості поставленої задачі.

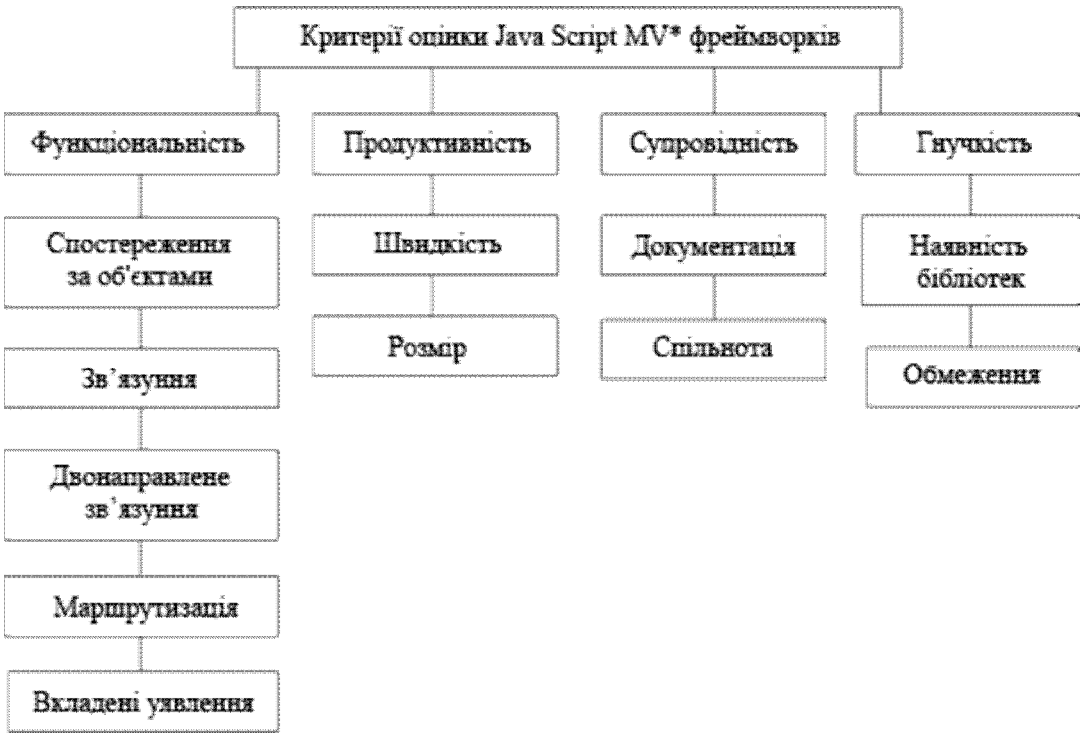


Рисунок 1 – Структура критеріїв оцінки JavaScript MV* фреймворків.

Обраний метод передбачає попарне порівняння між собою складових кожного рівня дерева. Приведемо приклад порівняння складових першого рівня ієрархії критеріїв оцінки у табл.1 та порівняння критеріїв другого рівня для критерія “Функціональність” у табл.2.

Таблиця 1 – Матриця порівнянь критериїв першого рівня.

Критерій	Функціональність	Продуктивність	Супровідність	Гнучкість
Функціональність	1	3	5	7
Продуктивність	1/3	1	5	7
Супровідність	1/5	1/5	1	3
Гнучкість	1/7	1/7	1/3	1

Таблиця 2 – Матриця порівнянь критеріїв другого рівня для критерія “Функціональність”.

Критерій	Спостереження за об’єктами	Зв’язування	Двунаправлене зв’язування	Маршрутизація	Вкладені уявлення
Спостереження за об’єктами	1	2	3	5	6
Зв’язування	1/2	1	3	4	6
Двунаправлене зв’язування	1/3	1/3	1	5	7
Маршрутизація	1/5	1/4	1/5	1	5
Вкладені уявлення	1/6	1/6	1/7	1/5	1

Анологічно порівнюються усі критерії. На наступному кроці, керуючись алгоритмом перевірки правильності суджень, проведемо наступні розрахунки для всіх критеріїв. Результати занесемо до табл.3., де:V_i – власний вектор матриці порівнянь, Q_i – вектор

пріоритетів, S_j – сума каждого j-го стовпчика матриці порівняння, L_{max} – максимальне власне значення матриці, I_r – випадковий індекс узгодженості, I – індекс узгодженості, R – відношення узгодженості. Якщо R < 0,10-– судження вірне, якщо більше – була допущена помилка при виставленні оцінок.

Таблиця 3 – Розрахунок перевірки правильності суджень виставлених парних порівнянь для критеріїв другого рівня критерія “Функціональність”.

	V_i	Q_i	S_j	P_j	L_{max}	I_r	I	R
Спостереження за об’єктами	2.825	0.405	2.2	0.891	5.431	1.12	0.108	0.096
Зв’язування	2.048	0.294	3.75	1.101				
Двунаправлене зв’язування	1.312	0.188	7.343	1.381				
Маршрутизація	0.549	0.079	15.2	1.197				
Вкладені уявлення	0.24	0.034	25	0.86				

Далі за аналогією з попередніми розрахунками, проведемо порівняння заданих альтернатив по всім вибраним критеріям. Приведемо приклад порівняння JavaScript MV* фреймворків. Процедура порівняння альтернатив включає розрахунки власного вектора матриці порівняння, індекса узгодженості та відношення узгодженості. В кінцевому результаті маємо загальні показники якості досліджуваних програмних продуктів наведених у табл.4

Таблиця 4 – Підсумкова оцінка альтернатив за критеріями 1 рівня.

	S	**S**	**S**	**S**	**Q**	**S**
Angular	0.481	0.056	0.085	0.181	0.54	**0.294**
Ember	0.3	0.164	0.188	0.194	0.312	**0.241**
CanJS	0.151	0.453	0.555	0.073	0.099	**0.281**
Backbone	0.069	0.327	0.172	0.552	0.048	**0.183**

З табл.4 випливає, що Angular є більш універсальною і повнофункціональною альтернативою JavaScript MV* фреймворка.

Література

1. Османі Е.: Разработка Backbone.js приложений . — СПб.: Питер, 2014. — 352 с.: ил. — (Серия «БестселлерыO’Reilly»).
2. ISO/IEC 9126-1:2001. Software engineering – Software product quality – Part 1: Quality model (Міжнародний стандарт)
3. Саати Т. : ПРИНЯТИЕ РЕШЕНИЙ Метод анализа иерархий - М.: Радио и связь, 1993. - 278 с.
4. Офіційний сайт проекту AngularJS [електронний ресурс]. Режим доступу:https://angularjs.org
5. Офіційний сайт проекту CanJS [електронний ресурс]. Режим доступу: http://canjs.com
6. Офіційний сайт проекту EmberJS [електронний ресурс]. Режим доступу: http://emberjs.com
7. Офіційний сайт проекту BackboneJS [електронний ресурс]. Режим доступу: http://backbonejs.org

УДК 621.395

Смолярчук С.А.
ОНАЗ ім. О.С.Попова
smoliarchuk@te.net.ua
Науковий керівник – к.т.н., проф. Нікітюк Л.А.

ДОСЛІДЖЕННЯ СТАНУ ТА ПЕРСПЕКТИВ РОЗВИТКУ КОРИСТУВАЦЬКИХ ПРИСТРОЇВ ІНФОКОМУНІКАЦІЙНИХ ПОСЛУГ

Анотація. *Досліджується поточний стан користувацьких пристроїв інфокомунікаційних послуг в Україні та перспективи їх подальшого розвитку.*

Інфокомунікації, які швидко розвиваються у всьому світі формують технологічну основу для створення нового типу послуг, які отримали назву – інфокомунікаційні послуги. Інфокомунікаційна послуга – мультипослуга, яка задовольняє телекомунікаційні та інформаційні потреби користувача з наданням можливості участі у процесі управління та формування запитуваної послуги[1]. Створення та надання такої послуги можливе лише на основі інтегрованої сервісної платформи, якою є інфокомунікаційна мережа. Але створення та впровадження таких послуг потребує рішення не тільки завдань з розширення функціональності телекомунікаційних мереж, але й завдань зі створення та надання якісного контенту та розвитку користувацьких пристроїв, які могли би у повному обсязі відповідати вимогам нового типу послуг:

−доступність незалежно від способу доступу до мережі;

−наявність у кінцевого користувача можливості управління послугою;

−забезпечення можливості отримання комплексу послуг у єдиному запиті.

Виходячи з цього можна зробити висновок, що створення та надання такого типу послуг, а також забезпечення наведених вище вимог висуває роль користувацьких пристроїв на новий рівень і робить актуальним дослідження стану та рівня розвитку таких пристроїв.

Метою даної роботи є дослідження поточного стану та оцінка перспектив розвитку користувацьких пристроїв інфокомунікаційних послуг в Україні.

Для досягнення даної мети було поставлено наступні завдання:

−дослідження предметної області;

−дослідження ринку користувацьких пристроїв та його поточного стану;

−оцінка перспектив розвитку користувацьких пристроїв в Україні.

Для рішення першої та другої задачі був проведений аналіз наявних на ринку користувацьких пристроїв та їх характеристик. Також було виконано розподілення пристроїв на класи та проаналізовані статистичні дані. На основі результатів вирішення першої задачі були зроблені певні висновки. Зокрема, станом на сьогодення зі всього різноманіття користувацьких пристроїв можливо виділити чотири основні групи:

−персональні комп’ютери (стаціонарні, ноутбуки, нетбуки та інш.);

−планшетні персональні комп’ютери;

−мобільні пристрої;

−гібридні пристрої;

Світові показники продажу даного типу пристроїв напряму характеризують популярність використовування даних пристроїв. Тому ґрунтуючись на цих показниках можна оцінити перспективи розвитку користувацьких пристроїв у найближчому майбутньому. У таблиці 1 наведено результати дослідження рівня світових продаж пристроїв компанією Gartner.[2]

Таблиця 1. Рівень продажу користувацьких пристроїв у світі

Тип	2012		2013		2014	
	к-сть, тис	%	к-сть, тис	%	к-сть, тис	%
PC(Стаціон. та ноутбуки)	341 273	15,40	299 342	13,01	277 939	11,23
Планшети	119 529	5,39	179 531	7,80	263 450	10,65
Мобільні телефони (Смартфони)	1 746 177	78,79	1 804 334	78,44	1 893 425	76,52
Інші пристрої (гібридні)	9 344	0,42	17 195	0,75	39 636	1,60

Для більш наглядного вигляду наведемо дані таблиці 1 у вигляді діаграми (рис.1):

Як видно на діаграмі, більша частина сегменту користувацьких пристроїв займає сектор мобільних пристроїв. У свою чергу за останні три роки спостерігається постійне зниження рівня продажу комп'ютерів та збільшення рівню продажу планшетних персональних комп'ютерів та гібридних пристроїв. Така тенденція збігається з принципами та вимогами, які висуває новий тип послуг, оскільки доступ до таких послуг повинен забезпечуватися незалежно від способу доступу до мережі та місцезнаходження. Щодо ринку України – то він повністю повторює світові тенденції.

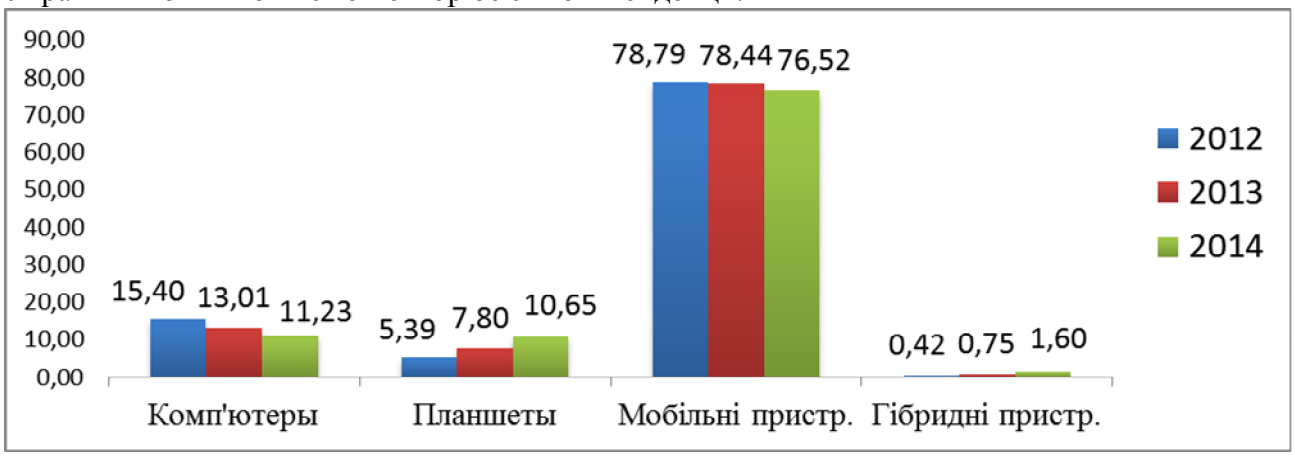


Рисунок 1. Діаграма рівня продаж користувацьких пристроїв

На рисунку 2 наведено дані Держкомстату України

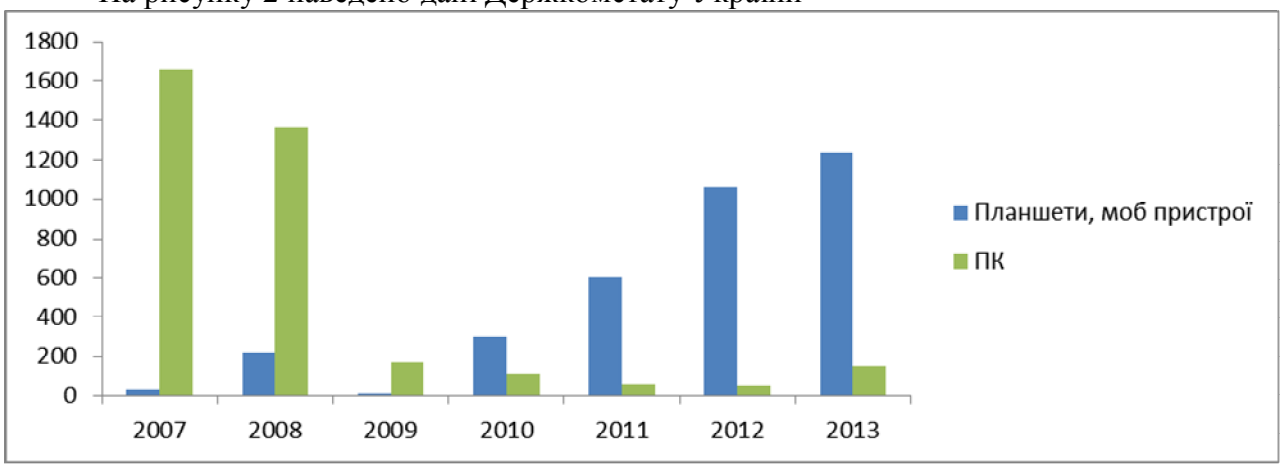


Рисунок 2 - Об'єми продажу користувацьких пристроїв в Україні

Але на відміну від світового ринку, ринок України не є таким стабільним, а його поточний стан та перспектива розвитку напряму залежить від економічної ситуації держави,

оскільки основна частина продукції є імпортною (98%). Але незважаючи на це, найбільший рівень продаж та зростання показують мобільні пристрої, планшети.

Для вирішення задачі оцінки перспектив розвитку користувацьких пристроїв в Україні були проаналізовані дані доходів від надання послуг зв'язку представлені Державною службою статистики України за 2010-2014 роки.

Як бачимо доля доходу від послуг комп'ютерного зв'язку зберігає позитивну динаміку, але така тенденція вочевидь буде зберігатися доки буде існувати приплив нових абонентів. Але без кардинальних змін ринку послуг, у першу чергу створення широкого спектру інфокомунікайних послуг, рівень позитивної динаміки буде зменшуватися, оскільки наступить насичення ринку, що у кінцевому результаті призведе до негативної динаміки та збільшенню відриву українського ринку від світових тенденцій.

Таблиця 2 – Рівень доходу від надання послуг зв'язку у млн. грн

Рік	Дохід від надання послуг комп. зв'язку	Загальний дохід від надання послуг зв'язку	Доля надання послуг комп. зв'язку від загального доходу
2010	4 238,50	47432,7	0,08935819
2011	4 749,30	50280,7	0,09445573
2012	5 401,60	52271,1	0,10333817
2013	5 697,20	52492,3	0,10853401
2014	6 190,40	52434	0,1180608

Але створення широкого спектру інфокомунікаційних послуг неможливе без заміни користувацьких пристроїв, оскільки сформульовані раніше вимоги до інфокомунікаційних послуг неможливо забезпечити при використанні пристроїв, поширених в Україні на сьогодення. Тому важливо до настання моменту насичення вивести на ринок України користувацькі пристрої нового покоління. Спрогнозувати орієнтовану дату настання моменту насичення можливо скориставшись логістичною функцією[1]. У якості параметру спостереження P, який змінюється у часі будемо розглядати долю надання послуг комп'ютерного зв'язку від загального доходу надання послуг зв'язку. Залежність парметру P від часу, являється функцією гіперболічного тангенсу, загальний вигляд якого наведений на рисунку 3.

Рисунок 3 Функція гіперболічного тангенсу

де k_p , k_t - константы перетворення;

$P_{\max}$ - значение параметра при насыщении

Для трьох обраних моментів спостереження, у котрих поміж значеннями параметру P однаковий приріст часу T_z можна скласти систему рівнянь:

$$\left.\begin{aligned} 1 - k_p P_1 &= th[-k_t (T_2 + T_z)], \\ 1 - k_p P_2 &= th[-k_t \cdot T_2], \\ 1 - k_p P_3 &= th[-k_t (T_2 - T_z)]. \end{aligned}\right\}$$

Ця система має наступні рішення

$$k_p = \frac{2 \cdot (P_1 \cdot P_3 - P_2^2)}{P_2 \cdot (2 \cdot P_1 \cdot P_3 - P_2 \cdot P_3 - P_1 \cdot P_2)};$$

$$T_2 = T_z \cdot \frac{arth(1 - k_p \cdot P_2)}{arth(1 - k_p \cdot P_2) - arth(1 - k_p \cdot P_3)};$$

$$P_{\max} = \frac{2}{k_p},$$

де T_2 – момент настання події P_2, який визначає період прогнозування ($t_w - t_2$),

t_w – момент переходу у область насичення

Згідно статистичним даним рівня доходу від надання послуг зв'язку Державної служби статистики України за 2010-2014 роки доля надання послуг комп. зв'язку від загального доходу параметру P при Tz = 2 роки становить відповідно : 2010 рік – 0,089: 2012 рік – 0,103; 2014 рік– 0,1186.

Скориставшись цими даними та зробивши підрахунки за наведеними формулами були отримані наступні результати:

Період T ≈ 13 років. Звідси момент переходу ринку у стан насичення можна розрахувати як $T_2 + 13 = 2012 + 13 = 2025$.

Виходячи з цього можна зробити висновок, що в Україні ринок користувацьких пристроїв, який напряму залежить від ринку послуг знаходиться у стадії зростання, але для ефективного розвитку він потребує кардинальних змін, зокрема виводу на ринок нового покоління користувацьких пристроїв до 2025 року та створення до цього часу широкого спектру інфокомунікаційних послуг, який забезпечить довгострокову перспективу зростання рівня розвитку користувацьких пристроїв в Україні.

Література

1. Услуги связи нового поколения **.** Л.А. Никитюк, Р.Ю. Царев
2. Gartner Research [електронний ресурс]. – Режим доступу: http://www.gartner.com/
3. Телекомунікаційні та інформаційні мережі: Підручник для вищих навчальних закладів. / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-КНИГА, 2010. - 640 с.: іл.

УДК 004.738.52

Струцинська О.Є.
ОНАЗ ім. О.С.Попова
struzinskaja@gmail.com
Науковий керівник – д.т.н., проф. Воробієнко П.П

ФОРМУЛЮВАННЯ ВИМОГ ДО WEB-РЕСУРСУ, ЩО ПРОСУВАЄТЬСЯ В ПОШУКОВИХ СИТЕМАХ

Анотація. *В рамках дослідження методів просування WEB- ресурсів в пошукових системах і на основі базових принципів їх роботи запропоновано розширений перелік вимог до якості WEB-ресурсу.*

Сьогодні Інтернет – це найбільша інформаційна база, яка складається із безлічі документів про будь-яку галузь науки, культури чи суспільства. Проте, слід зауважити, що вся ця інформація практично ніяк не упорядкована, що означає ускладнення пошуку відповідних (далі релевантних) користувацьким запитам відомостей. Однак отримання необхідної вичерпної та достовірної інформації в сучасних умовах є надзвичайно важливим в ході прийняття рішень або досягнення поставлених цілей.

Відповідно до вищесказаного, пошукові системи (Search Engine) є незамінним інструментом в отриманні достовірної інформації для сучасного користувача. В свою чергу, пошукова система має на меті створення інтерфейсу, що дозволяє розташувати в результатах пошуку найбільш релевантні документи на найвищих позиціях - процес ранжування. Зважаючи на інтенсивне збільшення кількості інформації, яка оброблюється пошуковими системами, виникає необхідність вдосконалення алгоритмів їх роботи, що зумовлює появу інноваційних рішень, які дозволяють підвищити ранжування документів.

В загальному випадку, пошукові системи включають в себе дві основні складові: пошукового робота, що виконує функцію формування якість бази даних пошукової системи методом шляхом дослідження всіх серверів мережі та базу даних пошукової системи (далі індекс). Індекс переважно формується за допомогою робота, мета якого знаходити нові посилання, а також власниками WEB-ресурсів, які мають можливість самостійно занести посилання на свій сайт до бази даних пошукової системи. Незалежно від робота також існує окреме програмне забезпечення, яке дозволяє виконувати сортування документів за рейтингом.

Функціонування пошукової системи можна звести до кількох основних етапів - отримання пошукового запиту від користувача, посилання його до власного індексу, у відповідності до ключових слів, які використав користувач, пошук по серверам та надання списку посилань, вже відсортованих за релевантністю[1].

Стрімке збільшення кількості інформації, яка щоденно потрапляє до мережі Інтернет стає причиною виникнення проблеми якості WEB-ресурсів, на які користувач потрапляє із видачі пошукової системи. Більшість користувачів мають недостатній рівень знань у тих областях, відомості з яких вони мають на меті знайти за допомогою пошукової системи. Тому оцінити достовірність і корисність пропонованої на WEB-ресурсі інформації виявляється доволі складно. На основі факторів, які безпосередньо впливають на результати ранжування може бути виокремлено ряд властивостей, які мають бути притаманними якісному WEB-ресурсу[3]. Хоча в науковій літературі за темою дослідження пропонується деякі варіанти вирішення даної проблеми, однак не існує достатньо вичерпного переліку вимог до якості WEB-ресурсу.

Тому метою роботи є надання розширеного переліку вимог до якості WEB-ресурсу, який рекомендовано до просування в пошукових системах у разі його відповідності:

1. Якісний вміст.

Ця вимога на сьогодні є першочерговою для всього інформаційного суспільства. Говорячи про WEB-ресурси, на увазі мається саме якість наповнення сайту – контенту, який може бути найрізноманітнішого формату, однак він має бути створений з певною метою и однозначно дозволяти користувачеві отримати бажаний результат від взаємодії з ним[3].

2. Регулярне оновлення.

Пошукові системи ранжують WEB-ресурси за багатьма факторами, частота оновлення WEB-ресурсу один з таких факторів. Це пояснюється тим, що якщо WEB-ресурс довго не оновлюється, то це означає, що він втрачає актуальність та корисність для користувачів, оскільки вебмайстер не приділяє йому достатньої уваги, не працює над його покращенням.

3. Об'єктивність інформації.

Вся інформація, що розміщаються на WEB-ресурсі має бути максимально об'єктивною, а не власною думкою або рекламою, в іншому разі відомості про це також повинні бути вказані.

4. Точність інформації.

Розміщаючи інформацію на WEB-ресурсі, треба впевнитись в її точності, тобто передбачити отримання користувачем відомостей про того, хто несе відповідальність за її точність, а також незалежні джерела, які підтверджують дану інформацію.

5. Простота та зручність використання.

На сьогодні одним із найважливіших чинників, що впливають на авторитетність WEB-ресурсів є передбачення простого та зручного інтерфейсу для користувацького доступу. Найбільшу увагу слід приділити саме зручності та зрозумілості структури WEB-ресурсу, зручності навігаційних елементів, виправданості використання та якості певних елементів дизайну (наприклад, анімаційних елементів) в ході розкриття змісту сторінки, поєднанню кольорів у дизайні, читаності текстів на вибраному фоні, відповідність заголовків до змісту сторінок[5].

6. Актуальність пропонованої інформації.

Якщо інформація, яка розміщається на WEB-ресурсі має принципово важливу актуальність і може втратити, необхідно проаналізувати чи не застаріла вона, а також чи передбачається отримання відомостей про останнє її оновлення.

7. Унікальність в мережі Інтернет.

Вся інформація, яка публікується на сайті має володіти високим рівнем унікальності, адже немає жодної причини вносити до індексу пошукової системи завідомо скопійований контент (або WEB-ресурс в цілому) через те, що він вже не несе ніякої корисної цілі для користувачів. Тому рекомендовано ретельно слідкувати за тим, щоб весь контент на WEB-ресурсі був унікальним і мав за першоджерело саме даний WEB-ресурс.

8. Професіоналізм подання інформації.

В першу чергу, слід звернути увагу на чистоту мови, грамотність та благозвучність складу. Крім того, недопустимими являються наявність орфографічних або стилістичних помилок, невідповідність тематиці WEB-ресурс або заявленому заголовку сторінки[4].

9. Безпека користувача.

На рекомендованому для просування WEB-ресурсі ні в якому разі не може бути шкідливого коду, небезпечних налаштувань системи керування контентом, вірусів, зміни вікна результатів пошуку на інший ресурс та інш..

10. Наявність реклами сторонніх WEB-ресурсів.

На якісному WEB-ресурсі недопустима наявність будь-якого роду реклами, що згубно впливає на довіру користувачів і авторитет в пошукових системах.

11. Модерування коментарів.

Якщо на WEB-ресурсі передбачена можливість коментування користувачами необхідно слідкувати за вмістом цих коментарів і позбуватися небажаного тексту або спаму.

12. Наявність великої кількості гіперпосилань на сторонні WEB-ресурси.

Потрібно проаналізувати доцільність використання гіперпосилань на інші WEB-ресурс, їх вживання повинно бути контекстно необхідним і природнім, інакше це виглядає як пошуковий спам або навмисна реклама.

Проведені дослідження є актуальними, адже популярність пошукових систем стрімко зростає, що викликає необхідність створення практичних методів підвищення відвідуваності WEB-ресурсу за рахунок покращення видимості у видачі пошукових систем.

Література

1. Ашманов І.С., Іванов А.А. Оптимізація і просування сайтів в пошукових системах. - СПб.: Питер, 2009. - 400 с.
2. Попова Ю. У. Пошукова система Google.[Електронний ресурс]:[Республіканська научно-технічна бібліотека]. .– Режим доступу: http://top.bigmir.net/global/traffic?&y=2.
3. Академия вебмастеров. [Електронний ресурс]. – Режим доступу: https://support.google.com/webmasters/answer/6023933?hl=ru&ref_topic=6001171
4. Критерии оценки качества сайта.[Електронний ресурс]. – Режим доступу: http://www.templatebest.ru/stat_s7.php.
5. Оценка качества сайта. [Електронний ресурс]. – Режим доступу: http://www.melius.ru/services/web-development/quality/ .

УДК 621.395

Суський Г.В.,
Інститут компьютерно-інформаційних технологій, Київ
Gregg007@ bigmir.net

АФІЛІАТИВНИЙ ВПЛИВ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ: СОЦІАЛЬНІ ТА ТЕХНОЛОГІЧНІ АСПЕКТИ

Анотація: *в тезах аналізується вплив Інтернет-технологій на когнітивні потреби на спричинену ними афіліацію користувачів мереж, яка здійснюється відповідно до нормативів групи з використанням тих навчок і можливосей інформаційного пошуку, які засвоєні користувачем і мають співвіднесеність з метою користування Інтернетом.*

В середовищі дослідників інформатизації та пов’язаних з цим процесів стають все більш вживаними термінологічні запозичення із суміжних наук, що займаються соціальними та психологічними аспектами впливу мереж на сучасний соціум. Так термін «афіліація», що означає «приєднання до великої групи, а в психології тлумачиться, як «особистісна співвіднесеність своїх дій, думок, вчинків до вимог, умов, нормативів групи» [4], все частіше використовується і в дослідженнях комп’ютерних технологій та інструментів мережевих комунікацій.

Когнітивні моменти, що притаманні сьогодні всім пошуковим системам, не обійшли своїми можливостями й користувачів мереж. Переважна більшість з них шукає в мережах нової інформації, далі йдуть: спілкування в соціальних мережах, чатах тощо; пошук спеціальної інформації за темами, які цікавлять коритувача; користування електронною поштою; спілкування за допомогою спеціальних програм (Скайп, Сіпнет, ін.). Такі соціологічні дані отримує Інстиут соціології НАН України понад п’ять останніх років. Динаміку розподілу відповідей на запитання «З якою метою Ви використоуваєте Інтернет?» відображає таблиця 1[1, с. 167].

Таблиця 1. Варіанти відповідей серед користувачів Інтернет-мережі (%)

Варіанти відповідей	2009	2010	2012	2014
Знайомлюся з останніми новинами, поточною інформацією	47,8	49,1	52,5	58,8
спілкування в соціальних мережах, чатах тощо	36,7	37,1	44,5	46,5
користування електронною поштою;	47,8	48,2	45,2	40,9
пошук спеціальної інформації за темами, які цікавлять	48,7	43,6	45,2	45,2
спілкування за допомогою спеціальних програм (Скайп, Сіпнет тощо)	11,5	17,3	32,2	31,6

Як демонструють дані, розміщені в Табл.1, найбільш активна динаміка за останні п’ять років у бік зростання відзначалась за показником «спілкування за допомогою спеціальних програм (Скайп, Сіпнет тощо)», тут зафіксоване зростання майже втричі. Наведені дані ілюструють не тільки використання можливостей комунікативних інструментів та технолгій комп’ютерних мереж для зв’язку та спілкування, але й суттєво компенсують зафіксований психологами «дефіцит спілкування», який є сьогодні поширеним серед майже всіх верств населення (включаючи молодь та середній вік).

Окремою цариною в Інтернеті постає «конгломерат» новин та інформаційних повідомлень, де найбільш яскраво виділяється, наскільки система сучасного інформування структурно пов'язана із системою політики. Політикам вигідний PR, згадки про них у засобах масової комунікації, останні ж, в свою чергу, прагнуть викликати своїми повідомленнями реакцію в політичній сфері. Інша справа, коли йдеться про галузь навчання, пошук шляхів вдосконалення або набуття освіти. Тут найбільш важливою виявляється здатність індивіда до інтелектуального зростання. Афіліативність втаких групах підвищується, адже їх пов’язує й спільна мета – отримати якісно виший, ніж у них є, рівень освіти. Всі канали масових комунікацій, включаючи

Інтернет-мережу, припускають необхідність не тільки надання індивіду технічних можливостей електронного доступу, але й підвищення інтересу індивіда до цієї сфери. Людина в таких дослідженнях постає не складною єдністю тілесної і психічної реальності, а специфічним конструктом. Найчастіше персоніфіковано інформація подається через «образ комунікатора» електронних медіа, який тяжіє до нейтральності (щодо політичних позицій), інтелектуальності (аналітичності) та ідентифікацій з «образом» суспільства[5]. Інтернет-технології надають нові інструменти і можливості для втілення своєї ідентичності. Саме останне виступає аналогічно як конструкт ідентифікації в медіапросторі конкретного суспільства.

У країнах же, що розвиваються, сучасні комунікаційні засоби є привілеєм невеличкого прошарку населення. Тому можна передбачити, що у цих країнах посилюватимуться тенденції до «суспільства двох класів», аж поки сучасні засоби комунікації не стануть доступними широкому загалові [6].

Для ілюстрації інформаційної нерівності стосовно доступу та користування комп’ютером і мережею Інтернет співставимо (вибрані за 2011 рік) дані, що містилися у результатах крос-європейського дослідження, в шкалі відповідей на запитання «Як часто Ви користуєтесь Інтернетом або електронною поштою для особистих потреб?»: співставимо позиції «максимум плюс» і «максимум минус»[2, с. 60-61] (див. табл. 2).

Таблиця 2. Відповіді на запитання: «*Як часто Ви користуєтесь Інтернетом або електронною поштою для особистих потреб?»* (N= 1500; дані вибрані за 2011рік).

2011 рік	Бельгія	Болгарія	Греція	Кіпр	Німеччина	Польща	Росія	Україна
Користуюсь щодня	49,8	26,1	26,1	25,5	45,5	40,5	28,7	21,7
Кілька разів на тиждень	14,6	8,3	10,6	8,5	16,4	13,7	8,9	16,3
Не маю доступу до Інтернету ні на роботі, ні вдома	15,9	46,8	26,7	30,8	17,1	22,1	45,2	41,4

У більш традиційному для більшості країн «старої Європи» звертанні до друкованих медіа картина зберігається майже незмінною довгі роки (навіть не зважаючи на «партиципаторні» можливості Інтернету). Як наголошувалось вище, можна спрогнозувати, що у найближчі десятиліття стрімко розвиватимуться локальні джерела та агенції новин, які транслюватимуть новини національними мовами і задовольнятимуть місцеві потреби тієї чи іншої країни в інформації із решти світу. Інтерпретуючи відмінності у споживанні продукції ЗМІ, можна помітити, що на тлі тенденції «згортання» часу, який відводить аудиторія контакту із традиційними медіа, народжується новий вид журналістики, яку почали називати «журналістикою співучасті» (від англ. “partycipate” – брати участь). В даний час інтернет-журналістика або «партиципаторна» журналістика вже не просто онлайновий варіант традиційної журналістики, а особливий вид журналістики, який існує переважно в двох формах: громадянської журналістики (“citizen journalism”) та блогів – особистих онлайнових щоденників (“blogs”) [3]. Саме в останніх бере участь переважно молодь, яку приваблює можливість розмістити або «вивисіти» на відповідному сайті створені власноруч матеріали.

Цей різновид співробітництва в журналістських та наукових колах визначається терміном «фольксономія», яка на відміну від руху новин та інформації зверху до низу – «таксономії» (остання ще донедавна активно використовувалась й традиційними медіа), дозволяє громадянській журналістиці подавати новини та думки «онлайн», синхронно із перебігом подій. Проте, професійні журналісти, які здебільшого виступають від імені певних великих спільнот або «всього народу», розглядають можливості зникнення друкованих та інших традиційних медіа з великою долею скепсису [6]. Особливо викликають недовіру матеріали блоггерів, які стосуються жанру так званої «журналістики розслідувань» та верифікації дійсності (перевірки) фактів. За прогнозами Філіпа Мейера (автора книги «Газета, яка щезає»), остання газета, ймовірно, буде прочитаною «останнім читачем» у квітні 2040 року [3], за вісім років до 600-річного «ювілею» винаходу друкарського станка Гутенбергом.

На даному етапі розвитку науково-теоретичної думки, теорії всесвітньої комп’ютерізації, аналогічно до теорій глобалізації, нагадують «впорядкований хаос». При чому це стосується теоретизувань по обидва боки океану, адже й американська соціологічна думка, й європейська, продукуючи постмодерні, пост-некласичні, пост-гуманістичні підходи, не демонструють таких кроків, які б могли консолідувати оцінки і погліди на сучасні винаходи інформаційних технологій та мас-медійні теорії, або вибудувати певний стратегічний напрям гносеологічного чи онтологічного характеру для поєднання зусиль, або хоч часткової «афіліації» наукових досліджень власне технологічних можливостей комп’ютерних мереж із когнітивними потребами їхніх користувачів, які є об’єктом вивчення сучасної соціальної науки «по обидва боки океану».

***Висновки*:** проблема інформаційного вибору та відповідної цьому вибору афіліативності – виступає «квазіпроблемою», адже повністю однотипне та однозначне тлумачення (інтерпретування), а також повне співпадіння між конкретною ситуацією та інформацією про неї є так само неможливим, як між перцептивно охопленою та

репрезентованою реальністю. Одночасно ця проблема лежить в двох площинах: а) рівень володіння індивідом-користувачем комп'ютерними технологіями та його доступом до них; б) афіліативні можливості соціальних мереж як засобу «приєднання до групи» або нейтралізації дефіциту спілкування поступово будуть розвиватись, адже мають не тільки значний технологічний потенціал, але й суттєву перспективу щодо задоволення когнітивних потреб конкретного і потенційного користувача мереж.

Література

1. Бойко Н. Структураційні ознаки перебування в мережі Інтернет / Н.Бойко // Українське суспільство 1992-2012. Стан та динаміка змін.Соціологічний моніторинг /За ред. д.ек.н.В.Ворони, д.соц.н. М.Шульги. – К.: Інститут соціології НАН України, 2012. – С.466-474.

2. Головаха Е.І.,Горбачик А.П. Тенденції соціальних змін в Україні та Європі: за результатами «Європейського соціального дослідження» 2005-2007-2009-2011.– К.: Інститут соціології НАН України, 2012.–119 с.

3. Мейер Ф. Исчезающая газета / Филипп Мейер // Режим доступа: http://www.inosmi.ru/world/20080409/240723.html

4. Психология личности: словарь-справочник / Под ред.. П. П.Горностая и Т. М. Титаренко. – К: Рута, 2001. – 320 с.

5. Українське суспільство 1992-2009. Динаміка соціальних змін / За ред. д. ек. н. В.Ворони, д.соц.н. М.Шульги. – К.: Інститут соціології НАН України, 2009. – 560 с.

6. *Gerbner G.* Marketing Mayhen Globally // Servaes J., Lie R. (eds.) Media and Politics in Transition. Cultural Identity in the Age of Globalization. Acco Leuven / Amersfoort, 1997. – PP. 13-19.

UDC 621.391

Taher A.
ONAT named after A.S.Popov
abidalla_2004@yahoo.com

AN ENHANCEMENT OF THE LTE-BASED MOBILE COMMUNICATION PLATFORM

Abstract. *An enhanced dynamic scheme of time-frequency resource scheduling for OFDM radio channel as the last mile of a multiservice telecommunication network*

The Long Term Evolution (LTE) mobile communication technology of the fourth generation (4G) is an advanced platform for multimedia data integration upon the conventional TCP/IP protocol suite [1]. The LTE applies the enhanced method of Orthogonal Frequency Division Multiple Access (OFDMA) in contrast to its predecessor Code Division Multiple Access (CDMA). Ceteris paribus, it gives advantage of increased channel bandwidth utilization and dynamic resource allocation scheduling. For OFDMA data coding the three types of modulation used: pure quadrature phase-shift keying (QPSK) with 2-bit/symbol; quadrature amplitude modulation (QAM-16 with 4 bit/symbol and QAM-64 with 6 bit/symbol) with variation both phase and amplitude of the signal due to the pair coherent oscillators which independently modulated on amplitude according to the adopted symbol constellation scheme.

In contrast to CDMA the OFDM-coded and modulated carrier signal does not fill the entire spectrum bandwidth but occupies the discrete frequency grid allocated within the dedicated band. As a result, the information signal much better resists the interference of "white noise" smoothly spread over the frequency range. However, the QAM technique suffers the known problem of high peak-to-average ratio (PAR) of modulated signal which requires transmitter/receiver power dynamics and amplifier linearity. This type of modulation solely can be effective while high signal-

to-noise ratio (SNR) occurs (i.e. in short length of the channel). The core property of the LTE frame is 10 ms cycling in Down/Up link communication between the base station (BS) and user equipment (UE). It results in two way delay (TWD) of packets more than 20 ms which is tolerant to digital telephony, but does not meet requirements of high dynamic Machine-to-Machine systems (M2M) or Sensor Network (SN) device interaction. Depending on the dedicated channel frequency bandwidth (5, 10, 15 or 20 MHz) the number of LTE subcarriers per one symbol is 300, 600, 900 or 1200, and the overall number of symbols within a 10 ms frame is either 6 or 7. So, the minimal size of the LTE frame (with QPSK) is (2 bit×300×6)/8bit/byte=450 byte. This seems superfluous towards M2M processes.

This work presents an advanced method of the OFDM radio channel scheduling intended for the M2M high dynamic systems. The two core enhancements are prompted: 1) The number of subcarriers is optionally variable in a wide range since 10 (minimal number) up to the maximum (1200); 2) the number of symbols per one frame is also optional in range since 1 symbol (minimal) up to the non-limited number. It can be shown that symbol transfer frequency increases proportionally to subcarrier number decrement while the overall channel bit rate is nearly constant. Thus in 5 MHz band the time interval for one symbol transmission decreases 30 times, and further decrease due to the symbol per frame reduction from 6 to 1 will be 30×6=180 times (i.e. near 10 ms/180=55 microsecond).

Conclusion.

The proposed enhancement of the LTE based mobile communication platform with the OFDMA modulation technique will extend its application sphere onto the high dynamic machine-to-machine systems and sensor networks.

References

1. LTE-A PHY Layer Overview & Fem to Design Challenges. Available at https://www.youtube.com/watch?v=JyKJ4_CybiE.

UDC 621.391

Tikhonov V.I., Khristov O., Chernov O.
O.S. Popov Odesa national telecommunication academy
victor.tykhonov@onat.edu.ua
Khristov @gmail.com
Chernov @gmail.com

METRIZATION TOPOLOGICAL MODEL FOR TELECOMMUNICATION NETWORK

Abstract*. The paper introduces an original technique to construct the metric tensor for an open telecommunication network with symmetric object relationships in terms of geometric properties for an abstract point of multidimensional locally Euclidian space. The proposed technique is highly scalable ranging from one open node to an arbitrary open network. This approach targets geometric presentation and system analysis of hierarchical network frameworks.*

Introduction

The theory of topological and metrical spaces is a powerful research tool for systems analysis in various fields of science and technology including telecommunication and information network design. Analysis and synthesis are mutually connected metods to study and develope physical objects and systems. “Analysis” means braking the whole one entity into distinguished parts to study their relationships, while “synthesis" will construct parts in a coherent system with predefind properties. Related logical terms to system analysis are “topological space”, «metric space» and «tensors». The topological space category may be used as one of the simplest and universal models for telecommunication networks. This type of model is efficient at first-step study

of an object. More detail investigation needs to evolve topological space into metric math object with geometric interpretation in terms of tensor analysis. However, the known publication focusing tensor approach in network systems design do not exhaustively reflect the wide spectrum of actual applications. *Yet, this work aims to advance known researches in applyied tensor analysis by developing a practical algorithm of metric tensor design for an arbitrary open telecommunication network.*

Metric tensor design for topological space

Figure 1-a,b shows two topologically equivalent graphical presenration for an open network created by the set $S=\{e_k\}$ of three domestic elements $e_k \in S$, $k=1,2,3$ and one extrinsic zero-element $e_0=\varnothing$ (i.e. empty element $\varnothing$). The elment $\varnothing$ in Fig.1-a may be interpreted as layer 2 switch in a local Ethernet network. The scheme in Fig.1-b schows the element $\varnothing$ as non-affiliated communication to individual elements of the set S.

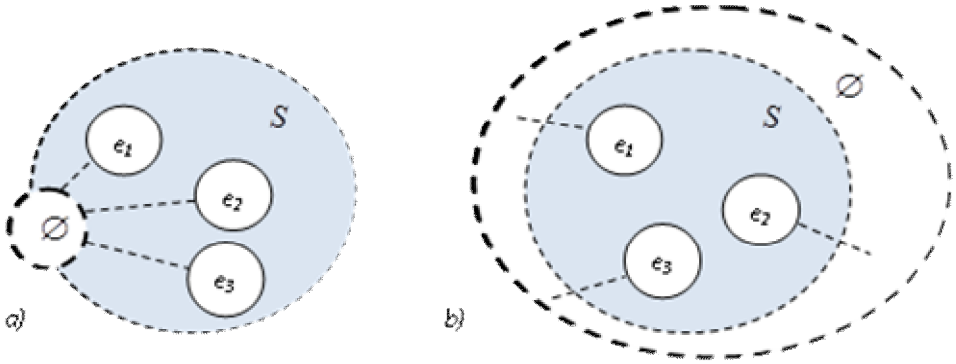


Figure 1 – Open network in the form of discrete topological space

This network frameworks in Fig.1-a and Fig1-b correspond to discrete topological space $TSp(S)$ with matrix graph depicted in Fig.2-a. According to our assumption all the mutual relationships in any pair of elements is symmetric ; this result into symmetric matrix $G(S)$ in Fig.2-a. Besides, any relationship in every couple of element is estimated in bynary logic values: either «yes» or «no» (i.e. «1» or «0»).

To build the metric property of the scheme we will sum all the values in any row of the matrix $G(S)$ and put it in the diagonal cells of matrix $M'(G)$ in Fig.2-b. Next, we will cut matrix $M'(G)$ into the matrix $M(G)$ in Fig.2-c. It is clear that each of two network frameworks in Fig.1 are fully equivalent to any of three matrices in Fig.2.

$G(S)$	0	1	2	3
0	0	1	1	1
1	1	0	0	0
2	1	0	0	0
3	1	0	0	0

a)

$M'(G)$	0	1	2	3
0	3	1	1	1
1	1	1	0	0
2	1	0	1	0
3	1	0	0	1

b)

$M(G)$	1	2	3
1	1	0	0
2	0	1	0
3	0	0	1

c)

Figure 2 – Network metric design for discrete topological space

Now, we will interpret matrix $M(G)$ in Fig.2-c as a metric tensor of an abstract 3-dimensional Euclidian space wirh orthnormal basis $\vec{E}=\{\vec{e}_1,\vec{e}_2,\vec{e}_3\}$:

$$M(G)=\left\langle \vec{E}\times\vec{E}\right\rangle=\begin{bmatrix}\langle\vec{e}_1\times\vec{e}_1\rangle & \langle\vec{e}_1\times\vec{e}_2\rangle & \langle\vec{e}_1\times\vec{e}_3\rangle\\ \langle\vec{e}_2\times\vec{e}_1\rangle & \langle\vec{e}_2\times\vec{e}_2\rangle & \langle\vec{e}_2\times\vec{e}_3\rangle\\ \langle\vec{e}_3\times\vec{e}_1\rangle & \langle\vec{e}_3\times\vec{e}_2\rangle & \langle\vec{e}_3\times\vec{e}_3\rangle\end{bmatrix}=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}, \quad (1)$$

where $\langle\vec{e}_k\times\vec{e}_n\rangle=|\vec{e}_k|\cdot|\vec{e}_n|\cdot\cos\beta_{kn}$ is scalar product of two vectors $\vec{e}_k$ and $\vec{e}_n$; $|\vec{e}_k|$ is module of vector $\vec{e}_k$ (its length); β_{kn} is angle between vectors $\vec{e}_k$ and $\vec{e}_n$. So, we may conclude that discrete topological space as a model of related telecommunication network with N nodes will bejective (mutually) mapped into the $N-$dimensional Euclidian space with orthonormal bases.

Metric tensor design for indiscrete (trivial) topological space

The discrete topological space is one of two marginal frameworks; another one is indiscrete (i.e. anti-discrete or trivial) topological space depicted in Fig.3 for a network with 3 nodes. This type of network structures is also referred as "mesh network" (each node is connected to anyone else). The correspondent matrix graph $M(G)$ is constructed in Fig.4.

$$M(G)=\left\langle \vec{E}\times\vec{E}\right\rangle=\begin{bmatrix}3 & 1 & 1\\ 1 & 3 & 1\\ 1 & 0 & 3\end{bmatrix}. \quad (2)$$

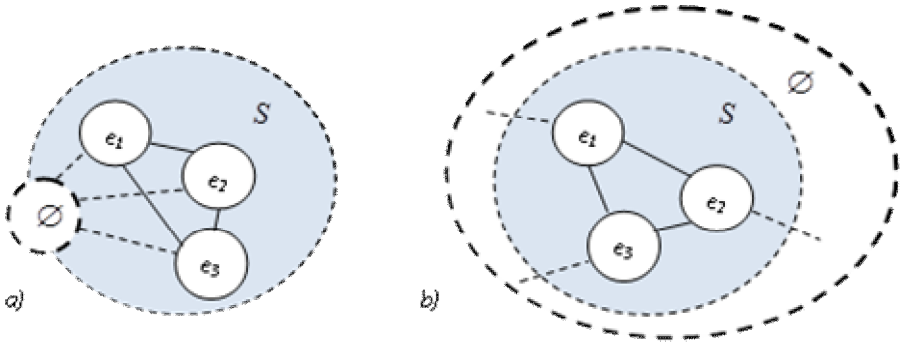


Figure 3 – Open network in the form of anti-discrete topological space

G(S)	0	1	2	3
0	0	1	1	1
1	1	0	1	1
2	1	1	0	1
3	1	1	1	0

a)

M′(G)	0	1	2	3
0	3	1	1	1
1	1	3	1	1
2	1	1	3	1
3	1	0	1	3

b)

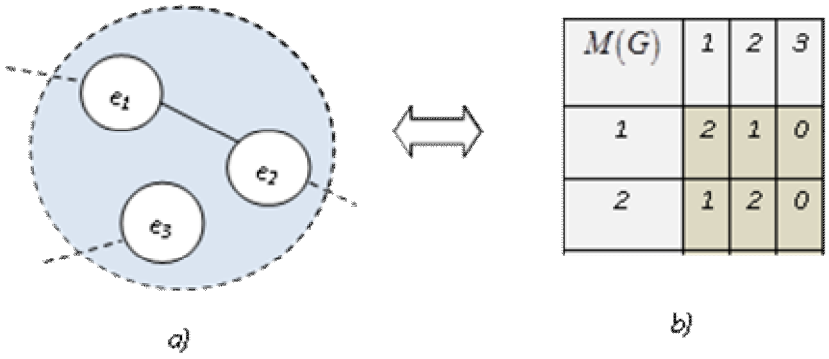
M(G)	1	2	3
1	3	1	1
2	1	3	1
3	1	1	3

c)

Figure 4 – Network metric design for anti-discrete (trivial) topological space

It is obvious from (2) that mesh network topology in Fig.3 is mapped into the system of three vectors each of the length $|\vec{e}_1|=|\vec{e}_2|=|\vec{e}_3|=\sqrt{3}$, where $\cos\beta_{12}=\cos\beta_{13}=\cos\beta_{23}=\frac{1}{|\vec{e}_1|\cdot|\vec{e}_2|}=\frac{1}{3}$. Thus $\beta_{12}=\beta_{13}=\beta_{23}=\arccos\frac{1}{3}\approx 70^0\approx 1.23rad$. It is known that the system of three vectors with the scalar

product matrix (2) defines the 3-dimensional Euclidian space with non-orthogonal and not normal basis, that is the Rieman metric tensor $M(G)$ in (2). The same way we may define metric tensor with binary relationships for any type of topological space. For instance, we have the network in Fig.5-a. The related metric tensor is matrix $M(G)$ in Fig.5-b. In that case we have : $|\vec{e}_1| = |\vec{e}_2| = \sqrt{2}$; $|\vec{e}_3| = 1$; $\beta_{13} = \beta_{23} = \frac{\pi}{2}$; $\cos\beta_{12} = 0.5$; $\beta_{12} = \frac{\pi}{3}$.



M(G)	1	2	3
1	2	1	0
2	1	2	0

Figure 5 – Network metric design for an arbitrary topological space

Conclusions

1. The topological space is a fundamental cognitive category of math analysis to describe physical objects behavior. However, the classic topology concept has not been exhaustively adopted yet to study info-communication network and systems.

2. The work originates an adaptation approach to network simulation in terms of generic topological spaces. This will give a new impulse for the students and engineers to implement their theoretical knowledge in network system applications.

3. The topological space category may be used as one of the simplest and therefore, one of the most universal and ubiquitous models of open or closed telecommunication networks. This type of model is worth to apply when first-glance point of view towards a network object is actualized.

References

1. Frank Stowell. “System Approach Applications in Information Technology”. 2012, 359 p.

2. Тихонов В.И. Фрактальная топологическая модель открытой телекоммуникационной сети / В.И. Тихонов // Наукові праці ОНАЗ ім. О.С.Попова. – 2010. – №1. – С.49-58.

3. Gerard Buskes, Arnoud van Rooij. “Topological Spaces: From Distance to Neighborhood”, Springer-Verlag New York, Inc., 1997, 309 p.

4. G.Korn, T. Korn, “Mathematical Handbook for Scientists and Engineers: Definitions, Theorems”1968, 1097 p.

UDC 621.391

Tikhonov V.I., Zelinska A.V., Tsumanets Yu.O.
O.S. Popov Odesa national telecommunication academy
victor.tykhonov@onat.edu.ua,
anvigreen@yandex.ru, tsunamys28@gmail.com

TOPOLOGICAL SPACE AS THE TELECOMMUNICATION NETWORK MODEL

Abstract. *The paper introduces an adaptation approach to apply the classic math category of topological space for telecommunication systems analysis to give a new impulse for the students and engineers to implement their theoretical knowledge in network applications. The topological space category may be used as one of the simplest and most universal models of telecommunication*

networks worth to apply at first-glance view towards a network object.

Introduction

Systems analysis aims to study relationships between the predefined primitive entities associated within a set of elements [1]. The terms “analysis” and “synthesis” come from Greek meaning "to take apart" and "to put together" respectively. “Analysis” may be defined as dissimilation process of breaking down a something whole into distinguished parts. Instead, the “synthesis" will assimilate separate parts in a coherent whole system. The system analysis is closely related to the logical term “holistic approach” [2] and math term “topological space” [3]. The topological space is a fundamental cognitive category of math analysis to describe physical objects behavior. However, the classic topology concept has not been exhaustively adopted yet to study info-communication network and systems. *This work aims to originate an adaptation approach to network simulation in terms of generic topological spaces.*

Topological space as a simple system model

We will understand a “system” as an abstract math model of a real object in terms of its partitions interaction. Thereby, the three following steps of abstraction are made to design a system:

1) The object focusing behind the environmental background;

2) The object-to-elements set decomposition;

3) The elements properties along with their relationships definition.

One of the simple techniques to implement the abovementioned steps is to design a topological space $TSp(S)$ on the set $S=\{e_k\}$ of elements $e_k \in S$, $k=0,1,2,...,N$, where $e_0=\varnothing$ is so called “zero set element” (or empty set element”) consider being a special open entity related to any non-zero element $e_k, k>0$, and also related to the set S outside, Fig.1. All the non-zero elements of the set S are considered as uniformed primitive objects with no essential properties. Similarly, all the relationships look like non-directed non-weighted arcs on the depicted graph.

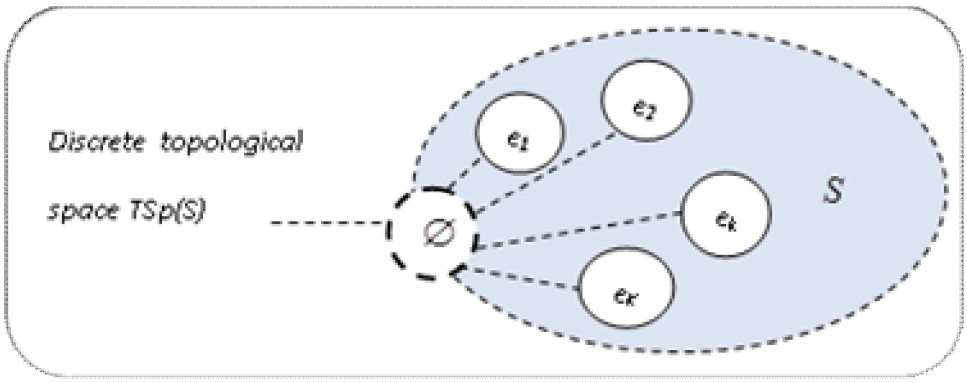


Figure 1 – Discrete topological space as a simple system model

If no other non-zero inter-element relationships took place except their links to zero-element $\varnothing$, then so called “*discrete topological space*” is defined on the set S with the correspondent “*discrete topology*”. This type of topology is also referred to as the “*strongest topology*”. The term “topological space on the set of elements” means that all the system parts are somehow connected to each other creating a certain “structure” (i.e. “topological structure”). In other words, in contrast to the non-coherent elements in the set S, there is a continuous path from any non-zero element e_k to any other non-zero element e_n. An appropriate interpretation for a discrete topological space is an open Ethernet network, where zero-element is OSI Layer 2 Ethernet switch Sw, and non-zero elements are terminal workstations WS_k, Fig.2. The Ethernet switch Sw as zero-element $\varnothing$ essentially differs from all the other (non-zero) elements of the set S. It is actually an extrinsic entity in contrast to domestic elements WS_k. Therefore, the so called star topology of the Ethernet network in Fig.2 must be classified as a discrete topological space where no direct inter domestic links exist.

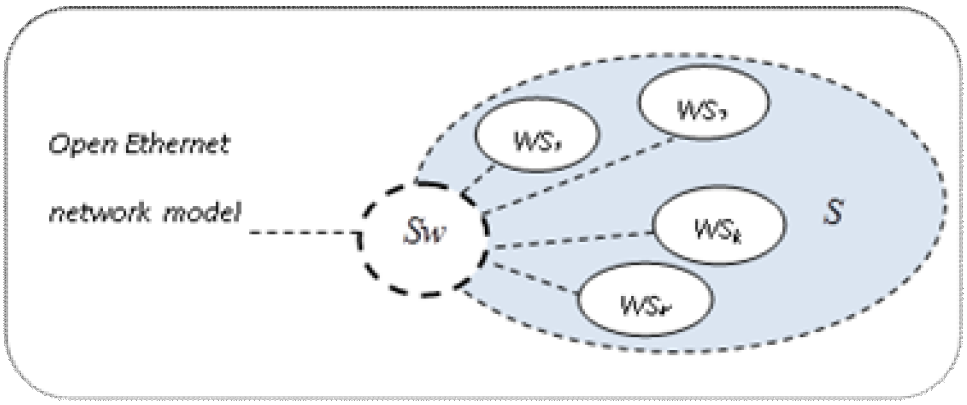


Figure 2 – Discrete topological space as open Ethernet network model

The discrete topological space $TSp(S)$ we map into the open network matrix graph $G(S)$, Fig.3-a. One may see that there are no cross-links in the shaded part of the matrix graph.

The opposite type of space is so called "anti-discrete" or "trivial" topology where all the non-zero elements are directly linked to each other, Fig.3-b.

An appropriate interpretation for trivial topological space is the wireless network with the so called fully crossed or "mesh topology" (this term is very close to the term "trivial topological space").

a)

$G(S)$	0	1	2	...	k	...	K
0	1	1	1	1	1	1	1
1	1	1					
2	1		1				
...	1			1			
k	1				1		
...	1					1	
K	1						1

b)

$G(S)$	0	1	2	...	k	...	N
0	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1
...	1	1	1	1	1	1	1
k	1	1	1	1	1	1	1
...	1	1	1	1	1	1	1
K	1	1	1	1	1	1	1

Figure 3 – The open matrix graph: a) discrete topology; b) trivial topology

Between the two marginal types of topological spaces there may exist different intermediate forms. Figure 4-b shows an open network graph for a telecommunication transport network with the ring topology depicted in Fig.4-a. Considering the given reasoning we will propose an equivalent definition of topological space evolved from the classic formalism to make this category more intuitively visible towards telecommunication network as an object of system analysis:

Alternative definition of topological space.

The topological space $TSp(S)$ on the finite set $S=\{e_k\}$ of domestic elements $e_k \in S,\ k=1,2,...,N$ is a binary logic structure of mutual relationships between the elements which are preliminary grouped on the common background $\varnothing$ associated with the so called extrinsic open zero-element $e_0=\varnothing$.

To compare the alternative definition of topological space formulated above we will quote one of the classic related formalism given in the section 12.5-1 of the mathematic reference book for engineers, page 386 [4] :

Classic definition of topological space :

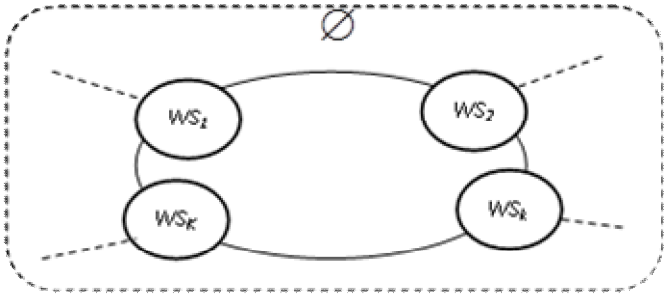
A class C of objects («points» x) is a topological space if and only if it can be expressed as a union of a family F of point sets S which contains

1) the intersection of every pair of its sets;

2) the union of the sets in every subfamily f of F;

F is topology for the space C, and the elements of F are called open sets relative to the topology F.

a)



b)

G(S)	0	1	2	...	n	...	N
0	1	1	1	1	1	1	1
1	1	1	1				1
2	1	1	1	1			
...	1		1	1	1		
k	1			1	1	1	

Figure 4 – The open ring topology: a) depicted graph; b) matrix graph

One may see that two definitions (classic and alternative ones) look very different, and it is not so easy either to apply classic form to the telecomunication network. The equivalence of these two formalisms with respect to a finite set of elements is demonstrated in [5].

Conclusions

1. The topological space is a fundamental cognitive category of math analysis to describe physical objects behavior. However, the classic topology concept has not been exhaustively adopted yet to study info-communication network and systems.

2. The work originates an adaptation approach to network simulation in terms of generic topological spaces. This will give a new impulse for the students and engineers to implement their theoretical knowledge in network system applications.

3. The topological space category may be used as one of the simplest and therefore, one of the most universal and ubiquitous models of open or closed telecommunication networks. This type of model is worth to apply at first-glance point of view towards a network object is actualized.

References

1. A Cognitive Psychology of Mass Communications /5-th Edition, Study Guide by Gram101 Textbook Reviews.

2. Frank Stowell. System Approach Applications in Information Technology / 2012, 359 p.

3. Gerard Buskes, Arnoud van Rooij. Topological Spaces: From Distance to Neighborhood/ Springer-Verlag New York, Inc., 1997. -309 p.

4. G.Korn, T. Korn, Mathematical Handbook for Scientists and Engineers: Definitions, Theorems/1968. - 1097 p.

5. Тихонов В.И. Фрактальная топологическая модель открытой телекоммуникационной сети / В.И. Тихонов // Наукові праці ОНАЗ ім. О.С.Попова. – 2010. – №1. – С.49-58.

UDC 621.391

Abdulghafoor Raed Yahya [1], Tkachova O.B [2]
[1] Odessa National Academy of Telecommunications named after O.S. Popov
71dkh@ukr.net
Scientific advisor – D.Sc., Duravkin Ie.V.
[2] Kharkov National University of Radio Electronics
Korov4enko@mail.ru

A METHOD FOR INCREASING SERVICES AVAILABILITY OF CLOUD COMPUTING

Abstract *- The paper is focused on analysis of services availability of cloud computing solutions. A method for increasing the availability of services through the use of information about the popularity of the service and the utilization of inter-segment data channels are suggested. Suggested method bases on choosing the optimal location of services registry.*

Introduction

Cloud computing can be described as " cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts). One of the main challenges faced by cloud computing management system, such as OpenStack, is to ensure in services availability. Services availability and reliability are the key parameters of cloud quality [1].

The existing management methods do not have specialized tools to ensure the services availability and reliability. Services availability of cloud-based networks is mainly achieved due to structural redundancy [2, 3]. For example, in OpenStack technology the couple of servers can be using for common cloud controller: active server and redundant server. The redundant servers usually use to provide a specified set of services, such as external Web-interface for API, task scheduler, authorization services, images services and dashboard.

However, this approach leads to an unjustified cost increasing without any guarantees to provide a specified QoS level [4]. Thus, the development of method for increasing services availability and service reliability is important task.

The analysis of existing methods for increasing services availability has shown that the replication is one of the most effective methods. Application of this method allows increasing the services availability and improving the scalability of geographically distributed multi-service network. Method to ensure the services availability that based on using services replication is proposed in this paper.

Main part

Cloud computing focuses on maximizing the effectiveness of the shared resources and services. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. cloud computing includes six general characteristics that impact to service reliability and service availability. This is virtualization, geographic distribution, resilient computing, massive scale, homogeneity, advanced security [5].

Area which services by registry may be limited as a multi-subnet, and a certain part of one big subnet. This is connected with fact that cloud-based networks can include a set of geographically distributed subnets of different sizes. The increase in the number of applications to the service resets the server and the emergence of failures in service and a significant deterioration

in the availability of services. This in its turn reduces the overall level of network QoS and its competitiveness.

All services in cloud computing available due to next component: controller node, network node, compute nodes and block-storage nodes. The basic structure for different service zones (service registry) of cloud computing is represented on Figure 1.

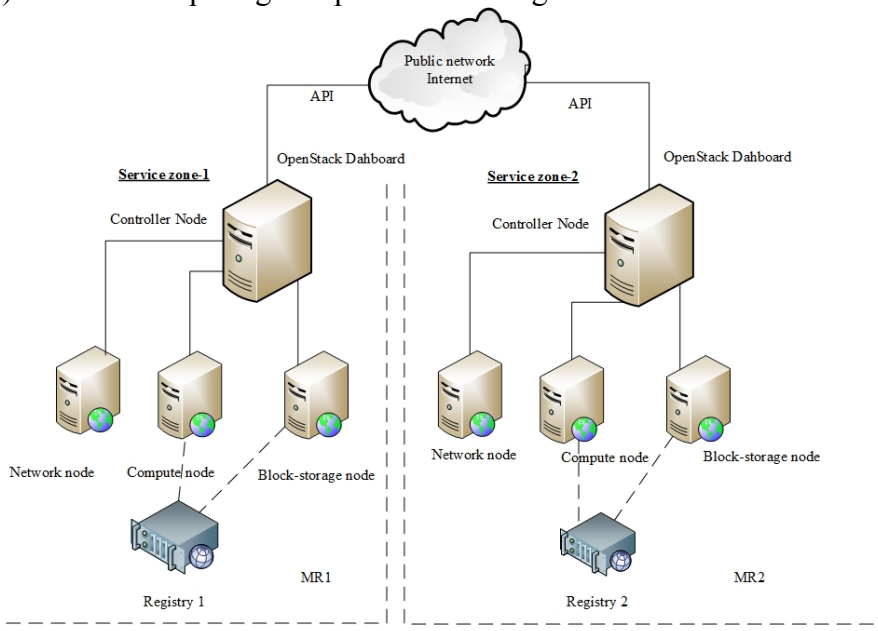


Figure 1. Structural scheme of service registries in basic cloud computing architecture

When a new service is deployment the service provider publishes information about a new service (service location, quality indicators of services, etc) in the registry service. In general, registry service for OpenStack architecture can be representing as follow:

$$I(S_i)=\{add,c,t,sp,a,r,...\},$$
$$\forall(S:S\in Net)\exists(add,c,t,sp,a,r)\in I(S_i),$$

where *Net* - is a set of cloud computing elements, $I(S_i)$ – the set of records in the registry services about S_i, consisting of the elements $(add,c,t,sp,a,r,...)$; *add* – the location of S_i service, *c* – a servise cost, *t* – response time, *sp* – service performance, *a* – a service availability, *r* – a service reliability, etc.

The elements *c, t, sp, a, r* belongs to *L*: $(c,t,sp,a,r)\in L$, where *L* – set of quality of service indicators S_i, search the services with required QoS values is made on the basis of their, $L\subset I(S_i)$. The service is available for use only after registration. Launching a virtual machine or instance involves many interactions among several services.

The set of service registry *R* can be located in geographically distributed heterogeneous network. In such a case Each registry has its own service area MR_j, the boundary of local registry defines by a network administrator:

$$Net\supset R=\{R_1,R_2,\ldots,R_v,\ldots,R_h\},$$
$$Net\supset MR=\{MR_1,MR_2,\ldots,MR_j,\ldots,MR_h\}$$
$$Net\supset S=\{S_1^1,S_2^1,...,S_i^1,S_{i+1}^2,...,S_n^j\},$$

where R – a set of services registry that implementing in *Net*, *MR* – set of service areas that make up the cloud-based network, S – set of services, v – the number of service registry, j – the number of service zone, h – an amount of services registry and service zones in cloud-based networks. The serial number of service registry coincides with the serial number of service zone for which it is responsible: $v = j$.

In the registration process the service S_i^j is assigned a serial number (i) and the numbers of service zone (j). In the case of the removal of the service from the registry, the serial number of the rest of the services may vary. However, the number of field service for the service remains the same throughout the life cycle.

If requested by the user requested service is not detected, registry R_L, send a request to the remote registry $R_{rem\,j}$ that bordering with its service zone for the detection of the desired resource. In the event that the required remote service registry $R_{rem\,j}$, the registry R_L receives reply. This reply includes indicators of quality of service and its location. Further, the service registry provides the information to the customers.

In order to reduce the number of repeated requests to the remote registry, information about the service is temporarily recorded in the registry R_L. The remote S_i^j receive the new serial numbers. Thus, the service zone remains unchanged. Thus, in the registry may store information about local services I_L and remote services I_{rem}:

$$R_1 = \{I(S_1^1), I(S_2^1), ..., I(S_i^1), I(S_{i+1}^2), ..., I(S_n^j)\}$$

$$I = I_L \cup I_{rem}$$

$$I_{rem} = \{add, t_{reg}\} \times L = \{(add, t_{reg}, c, t, th, a, r)\}$$

The description of the remote services introduces an additional parameter. This parameters is a time of registration $t_{reg.}$ The time of registration it is time period during which information about the remote server to be stored in the service registry. In the case of repeated custom's request to the remote service the t_{reg} service extends.

When the registering time is over $t_{reg} = 0$, information about the service is removed. It is do for rational use of server resources and reducing the number of entries in the registry

Detection time information on the location of the service is reduced in the case of the growing popularity of remote resource for customers. But despite the reduction in search time remote service, the growing popularity of services in general, results in an undesirable decrease in the level of service quality. This is related to the fact that most of the time in providing services consists of a direct interaction between the user and the service provided by the network.

Conclusion

The method of replication which allows to increase the services availability and service reliability of cloud computing in the case of grows a services popularity and distribution is suggested in the paper. Application of the method allows performing two types of replication: local replication and remote replication. This method also allows increase the availability and productivity of resources and improve the scalability of geographically distributed network.

References

1. Jinesh Varia , Architecting for the Cloud: Best Practices, January 2011, http://jineshvaria.s3.amazonaws.com/public/cloudbestpractices- jvaria.pdf.

2. Gegeshidze G.A. Fundamentals of network planning and management / G.A. Gegeshidze, M.L. Once. - Ganatleva. - 1968. - 303 p.

3. Kashi Venkatesh Vishwanath and Nachiappan Nagappan , Characterizing Cloud Computing Hardware Reliability, Microsoft Research, http://research.microsoft.com/pubs/ 120439/socc088- vishwanath.pdf.

4. Vishnevsky V. M. Theoretical bases of designing of computer networks. / V.M.Vishnevsky - M: Technosphere, 2003. - 512 p.
5. Cloud computing tutorial. Simply easy lerning, 2014, http://www.tutorialspoint.com/cloud_computing/cloud_computing_tutorial.pdf

УДК 621.396

Топехін Д.С.
ОНАЗ ім. О.С.Попова
dtopekhin@ukrtelecom.ua
Науковий керівник – проф. Ложковський А.Г.

ДОСЛІДЖЕННЯ ОРГАНІЗАЦІЇ КОРПОРАТИВНИХ МЕРЕЖ З ВИКОРИСТАННЯМ IP-ТЕХНОЛОГІЙ

Анотація. *Розглянуті питання актуальності створення корпоративної телекомунікаційної мережі (КТМ) на базі мережі передачі даних з використанням технології Voice over IP (VoIP), як альтернатива парку внутрішніх АТС, які вичерпали свій технологічний ресурс.*

1. Актуальність створення КТМ обумовлена тим, що існуючий парк внутрішніх АТС вичерпав свій технологічний ресурс та вимагає заміни, з іншого боку - наявність внутрішньої інфраструктури дозволяє застосовувати сучасні рішення, використовуючи власні ресурси, а не купувати сервіси у традиційних операторів. Таким чином, існує можливість значно розширити сферу застосування мережу передачі даних (МПД), використовуючи її не тільки для передачі даних, але й для організації аудіо та відео телефонії. Останнім часом широкого поширення набула технологія VoIP, яка дозволяє при найменших витратах організувати телефонний зв'язок з наданням повного спектру послуг. Під IP-телефонією розуміється технологія, що дозволяє використовувати мережі з комутацією пакетів, для організації телефонних розмов та передачі факсів в режимі реального часу. Для здійснення викликів з одних мереж в інші, наприклад, з телефонною мережею загального користування (ТмЗК) до мереж Ethernet, необхідно використовувати шлюзи, які крім інших функцій виконують переклад телефонних номерів в IP-адреси та навпаки.

2. Дослідження питань пов'язаних з побудовою мережі для передачі голосу із застосуванням технології IP-телефонії на базі протоколу SIP включає в себе теоретичний, практичний та експериментальний аналіз VoIP технології. Результатами дослідження стало впровадження даної технології в корпоративну мережу телекомунікаційної компанії.

Теоретичний аналіз. Комутація пакетів має три основні проблеми: джиттер, затримка та втрата пакетів. Для компенсації цих недоліків застосовуються кодеки та різні протоколи реального часу, які дозволяють виявити і з деякою часткою ймовірності відновити втрачені пакети.

Експериментальний аналіз. При порівнянні протоколів SIP та H.323 можна зробити висновок, що протокол SIP простіший, більш орієнтований на Інтернет мережі, та потребує менше часу на встановлення з'єднання, ніж у протокол H.323.

Тести з різним устаткуванням, яке підтримує протокол SIP, таких як: IP-телефони, шлюзи та аналогові телефонні адаптери, довели працездатність та сумісність з ключовими вузлами SIP-мережі тестованого устаткування.

Практичний аналіз. Результатами дослідження стало впровадження VoIP технології в корпоративну мережу телекомунікаційної компанії. На даний момент мережа є працездатною, повнофункціональною. Базою побудованої схеми корпоративної мережі на протоколі SIP є ЛОМ реалізована за стандартом Fast Ethernet з пропускною здатністю 100 Мбіт/с. В якості SIP-сервера виступила IP-АТС Asterisk. Мобільність користувачів та

адресація, подібна до адресації електронної пошти, забезпечується службою доменних імен, яка встановлена на DNS – сервер.

3. При проведенні розрахунку капіталовкладень на організацію досліджуваної КТМ та телефонної мережі побудованої на базі системи Avaya Definity, сума витрат на обладнання та будівельно-монтажні роботи при однаковому наборі надаваних послуг, потребують майже однакових капіталовкладень. Проте доцільніше розгортати мережі з використанням VoIP-технології, оскільки, нарощування числа абонентів не потребує витрат, на відміну від мережі на базі системи Avaya Definity, яка вимагає придбання додаткової АТС.

Висновки. У процесі розробки та впровадження КТМ на основі технології VoIP виявлені наступні її переваги: більш висока відмовостійкість; використання єдиної транспортної мережі; гнучкість та масштабованість; економія на телефонних рахунках.

Література

1. Кучерявый А.Е., Гильченок Л.З., Иванов А.Ю. Пакетная сеть связи общего пользования. – СПб.: Наука и техника, 2004. – 272 с.
2. Бертсекас Д., Галлагер Р. Сети передачи данных: Пер. с англ. – М.: Мир, 1989.
3. Б. С. Гольштейн, А.В. Пінчук, А. Л. Суховіцкій: IP-телефонія .- М.: Радіо зв'язок
4. А.В. Росляков, М.Ю. Самсонова, І.В. Шибаєв. IP-телефонія.-М.: Еко-Тренд,
5. В. Г. Оліфер, Оліфер Н. А. Нові технології та обладнання IP-мереж .- СПб. БХВ-Петербург, 2001
6. В.Г. Оліфер, Н.А. Оліфер. Підручник: «Комп'ютерні мережі. Принципи, технології, протоколи ». С-Пб.: Питер, 2001

УДК 621.391

Хинкиладзе Д.
ОНАС им. А. С. Попова
Dato_manager@yahoo.com
Научный руководитель – доц. Царёв Р. Ю.

АНАЛИЗ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ ПОИСКОВЫХ СИСТЕМ ИНТЕРНЕТА

Аннотация. *Работа посвящена исследованию принципам функционирования современных поисковых систем*.

Интернет состоит из миллионов сайтов и содержит эксабайты информации. Чтобы пользователи могли узнать о существовании этой информации и воспользоваться ей, существуют поисковые системы. Они реализуют право человека на доступ к информации. Поисковая система - это техническое средство, с помощью которого пользователь интернета может найти данные, уже размещенные в сети.

Запросу пользователя могут соответствовать тысячи, а иногда и миллионы веб-страниц, для того чтобы отобрать те которые соответствуют запросу пользователя в максимальной степени используют средства поиска[1].

Средства поиска и структурирования, называемые поисковыми механизмами, реализуются в виде агентов, пауков, кроулеров и роботов и используются для сбора информации о документах, находящихся в Интернет[2]. Каждый поисковый механизм имеет собственный набор правил, определяющих, как собирать документы.

Агенты - самые "интеллектуальные" из поисковых средств. Они могут осуществлять не только поиск, но и выполнять транзакции от Вашего имени. Агенты могут искать сайты специфической тематики и возвращать списки сайтов, отсортированных по их посещаемости, находить и индексировать другие виды ресурсов, не только страницы.

Общий поиск информации в Сети осуществляют программы, известные как пауки. Пауки сообщают о содержании найденного документа, индексируют его и извлекают итоговую информацию.

Кроулеры просматривают заголовки страниц и возвращают только первую ссылку.

Роботы могут быть запрограммированы так, чтобы переходить по различным ссылкам различной глубины вложенности, выполнять индексацию и проверять ссылки в документе..

Кроме механизмов поиска, различные поисковые системы используют различные алгоритмы ранжирования, однако основные принципы определения релевантности (соответствия) страницы запросу следующие:

– количество слов запроса в текстовом содержимом документа (т.е. в html-коде);
– тэги, в которых эти слова располагаются;
– местоположение искомых слов в документе;
– удельный вес слов, относительно которых определяется релевантность, в общем количестве слов документа.

Процесс поиска информации, состоит из следующих этапов:

– сбор информацию в Интернет с различных сайтов;
– исследование по запросу;
– ранжирование результатов;
– индексация сайтов.

Сбор данных осуществляется поисковый робот. Он предназначен для перебора страниц Интернета с целью занесения информации о них в базу данных поисковой системы.

Индексация– составление для каждой страницы обратного (инвертированного) файла индекса. Индекс служит для того, чтобы быстро по нему производить поиск и состоит из списка слов из текста и информации о них (позиции в тексте, вес и др.). Инвертированным файлом индекса называется такой индекс поисковой системы, в котором перечислены слова коллекции документов, а для каждого слова перечислены все места, в которых оно встретилось.

При поиске, в первую очередь, анализируется запрос, введенный пользователем, в результате которого вычисляются веса для каждого из слов. Весом слова называется отношение частоты использования этого слова к общему количеству слов, выраженное в процентах. [3]. Далее, производится поиск по инвертированным индексам, находятся все документы в базе, которые наиболее подходят под данный запрос. Соответствиедокумента запросуопределяется по формуле:

$$similarity(Q,D) = SUM\left(w(qk) \cdot w(dk) \right) \quad (1)$$

где similarity(Q,D) – схожесть запроса Q документу D; w(qk) – вес k-го слова в запросе; w(dk) – вес k-го слова в документе.

Документы, наиболее схожие с запросом, попадают в результаты поиска.

После того, как наиболее схожие документы были отобраны из основной коллекции, они должны ранжироваться, чтобы в верхних результатах отражались наиболее полезные для пользователя ресурсы. Для этого используется специальная формула ранжирования, которая для разных поисковых систем имеет разный вид, однако для всех из них основными факторами ранжирования являются[4]:

–вес страницы;
–авторитетность домена;
–релевантность текста запросу;
–релевантность текстов внешних ссылок запросу, а также множество других факторов ранжирования.

Поскольку механизм ранжирования не раскрывается поисковыми системами, его можно описать следующей упрощенной формулой:

$$Ra(x) = \left(m \cdot Ta(x) + p \cdot La(x)\ \right) \cdot F\left(PRa\right) \qquad (2)$$

где Ra(x) – итоговое соответствие документа а запросу x; Ta(x) – релевантность текста (кода) документа а запросу x; La(x) – релевантность текста ссылок с других документов на документ а запросу x; PRa – показатель авторитетности страницы а, константа относительно x;F(PRa) – монотонно неубывающая функция, причем F(0)=1, можно допустить, что F(PRa)=1+q·PRa;m,p,q – некие коэффициенты.

Формула (2) даёт очень общее представление об алгоритмах ранжирования документов в результатах поиска [4].

Сегодня, существует достаточно много поисковых систем, но в общем случае большинство пользователей используют лишь несколько из них. На рис. 1 показана популярность поисковых систем в Украине, а на рисунке 2 показана популярность поисковых систем в мире[5].

В настоящее время на украинском рынке отмечаются серьезные изменения. Так, поисковая система Google, которая уже долгое время является самым популярным поисковиком Уанета, продолжает уверенно завоевывать новые позиции. А вот рейтинг системы Яндекс, который начал падать более года назад, продолжает свое снижение. В настоящий момент нет никаких оснований предполагать, что популярность этой поисковой системы начнет увеличиваться[6].

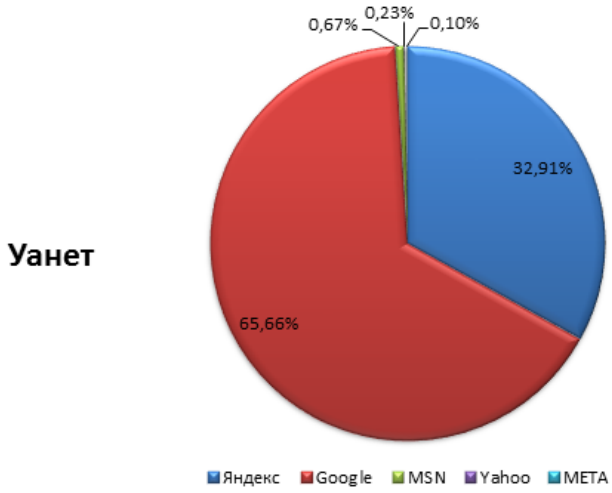


Рисунок 1 – Популярность поисковых систем в Украине

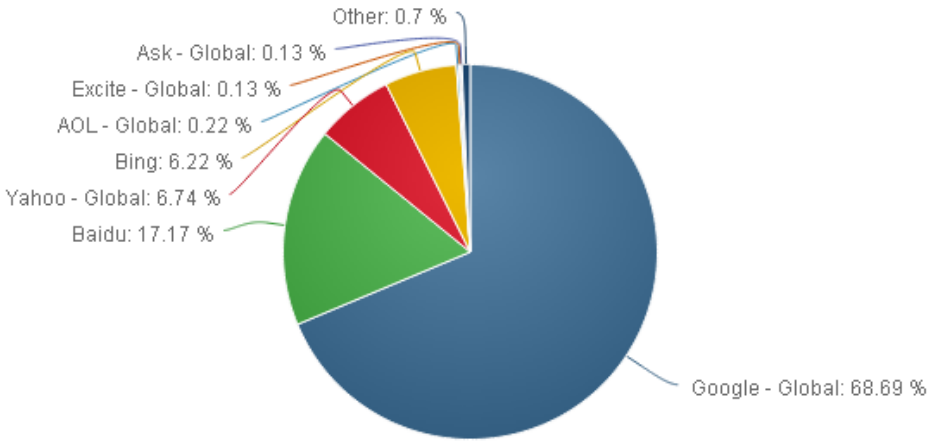


Рисунок 2 – Популярность поисковых систем в мире

В работе проведен анализ принципов функционирования поисковых систем. Результаты анализа позволили определить основные факторы и принципы ранжирования сайтов и отдельных веб-документов в поисковой выдаче.Также была проанализирована статистика использования различных поисковых систем и можно уверенно утверждать, что наиболее популярной поисковой системой на сегодня является Google.

Литература

1. Осипов Г.С., и др. Семантический поиск в среде Интернет. // Препринт. - Переславль-Залесский: ИПС РАН, 2003. – 350 с.

2. Маннинг К., Рагхаван П., Шютце Х. Введение в информационный поиск. М.: Вильямс, 2011. –600 с.

3. Людкевич С. Ранжирование документов в поисковых машинах. http://www.promo-techart.ru/analvsis/range.htm, 2006. - С. 1-3.

4. Гулин А., Карпович П., Расковалов Д., Сегалович И. Оптимизация алгоритмов ранжирования методами машинного обучения // Тр. Росс.сем. по оценке методов информационного поиска. СПб.: НУ ЦСИ, 2009. 163–168.

5. http://www.bestseoblog.ru/rejting-poiskovyx-sistem/ - статситика популярности поисковых систем в мире

6. http://uaweb.ua/publication/top_5_search_engine_2015.html - статистика популярности поисковых систем в Украине

УДК 621.397

Царёв Р.Ю.
ОНАС им. А.С. Попова,
c4r@mail.ru
Научный руководитель - Никитюк Л. А.,

ОПТИМИЗАЦИЯ НАБОРА КОМПЛЕКТУЮЩИХ ЭЛЕМЕНТОВ СЕРВЕРА ДЛЯ ОРГАНИЗАЦИИ ПЛАТФОРМЫ ПРЕДОСТАВЛЕНИЯ УСЛУГИ IPTV

Аннотация. *В работе предложен метод выбора набора комплектующих элементов сервера, входящего в состав сервисной платформы для предоставления услуги IPTV в режиме одноадресного вещания.*

Неотъемлемой частью сервисной платформы предоставления услуги IPTV является сервер, на котором накапливается и хранится видеоконтент. Задача повышения эффективности предоставления услуги IPTV может быть решена путем оптимизации выбора компонент сервера (таких как системная плата, процессор, оперативная память, жесткие диски, корпус с блоком питания) из множеств представленных аналогов. Оптимизация выбора комплектующих, рассматривается с точки зрения обеспечения гарантированного качества предоставления услуги, при заданной средней интенсивности поступающих на сервер запросов пользователей. Суммарные затраты на комплектующие должны быть минимизированы.

Пусть M - множество комплектующих сервера, мощностью m. Каждый комплектующий элемент, в свою очередь, представлен конечным набором возможных вариантов N_i ($i=\overline{1,m}$), мощностью n_i . Необходимо, из каждого множества N_i ($i=\overline{1,m}$) выбрать по одному элементу $x_{kl} \in N_i$, таким образом, чтобы их общая стоимость C_i была минимизирована при соблюдении следующих условий [1]:

– выбранные комплектующие должны быть совместимы между собой, указанное условие выполняется, если выбираемые элементы совместимы с системной платой - центральным элементом сервера;

– среднее время обслуживания запроса сервером $\overline{T_{OB}}$ не должно превышать некоторой заданной величины T_0.

Указанная задача может быть формализована в терминах моделей комбинаторной оптимизации [2,3] и сведена к следующему общему виду. Найти минимум целевой функции:

$$\gamma = \min_i \{C_1, C_2, ...C_{n1}\},$$
$$\text{где } C_i = \sum_k \sum_l c_{kl} \cdot x_{kl} \cdot e_{kl} \to \min, \quad (1)$$

где c_{kl} - стоимость *l-го* компонента сервера *k-го* набора;

x_{kl} - переменная определяющий выбор *l-го* компонента сервера *k-го* набора, $x_{kl} \in \{0,1\}$, $k = \overline{1,(m-1)}$, $l = \overline{1,\max(n_2, n_3, ...n_i)}$;

e_{kl} - элемент булевой матрицы $E_i = \|e_{ij}\|$, ($i = \overline{1,n_1}$) размерностью ((m -1) x $\max(n_2, n_3, ...n_i)$), отражающей совместимость компонентов *i*-го набора комплектующих с системной платой сервера (n_1 – мощность множества доступных для выбора системных плат, n_2, n_3,.. n_i – соответственно мощности множеств остальных наборов компонентов сервера) и может принимать значения:

$$e_{ij} = \begin{cases} 1, & \text{если имеет место совместимость,} \\ 0 & \text{в противном случае,} \end{cases}$$

при ограничении:

$$\overline{T_{\text{î á}}} \le T_0 \quad (2)$$

Указанное ограничение обеспечивает гарантированное качество предоставления услуги при выполнении условия [4,5]:

$$\rho \le 0.8 RPS_{\text{Ser}} \quad (3)$$

где ρ– утилизация сервера, RPS_{Ser} – производительность сервера.

Известно, что время обслуживания связано с утилизацией сервера следующей зависимостью [6]:

$$\overline{T_{\text{î á}}} = \frac{\rho}{\overline{\gamma}}, \quad (4)$$

где $\overline{\gamma}$ – средняя интенсивность поступающих на сервер запросов пользователей.

В работе [1], показано, что производительность сервера RPS_{Ser} зависит от производительности его компонентов:

$$RPS_{SER} = \frac{1}{10} \cdot \sum_k \sum_l x_{kl} \cdot e_{kl} \cdot RPS_{kl}^{CPU} + \frac{1}{100} \cdot \sum_k \sum_l x_{kl} \cdot e_{kl} \cdot RPS_{kl}^{MEM} + \sum_k \sum_l x_{kl} \cdot e_{kl} \cdot RPS_{kl}^{HDD} \quad (5)$$

где RPS_{kl}^{CPU} – производительность *l-го* процессора *k-го* набора, RPS_{kl}^{MEM} – производительность *l-ой* оперативной памяти *k-го* набора, RPS_{kl}^{HDD} – производительность *l-ой* системы хранения *k-го* набора.

Значения RPS_{kl}^{CPU}, RPS_{kl}^{MEM}, RPS_{kl}^{HDD} можно рассчитать, используя формулы (11)-(13) из работы [1].

С учетом (5) выражение (4) можно записать следующим образом:

$$\overline{T_{\text{î á}}} = \frac{1}{\overline{\gamma}} \cdot \left(\frac{1}{10} \cdot \sum_k \sum_l x_{kl} \cdot e_{kl} \cdot RPS_{kl}^{CPU} + \frac{1}{100} \cdot \sum_k \sum_l x_{kl} \cdot e_{kl} \cdot RPS_{kl}^{MEM} + \sum_k \sum_l x_{kl} \cdot e_{kl} \cdot RPS_{kl}^{HDD}\right) \quad (6)$$

Тогда ограничение (2) будет иметь вид:

$$\frac{0,8}{\overline{\gamma}} \cdot \left(\frac{1}{10} \cdot \sum_k \sum_l x_{kl} \cdot e_{kl} \cdot RPS_{kl}^{CPU} + \frac{1}{100} \cdot \sum_k \sum_l x_{kl} \cdot e_{kl} \cdot RPS_{kl}^{MEM} + \sum_k \sum_l x_{kl} \cdot e_{kl} \cdot RPS_{kl}^{HDD}\right) \le T_0 \quad (7)$$

Предложенную задачу можно решить методом полного перебора [2,3]. Метод полного перебора не всегда позволяет найти решения за приемлемый временной промежуток, поэтому для решения предлагается использовать следующий алгоритм:

1. Рассчитываем RPS_{kl}^{CPU}, RPS_{kl}^{MEM}, RPS_{kl}^{HDD};

2. Рассчитываем коэффициенты $\Pr_{kl}$, показывающие отношение стоимости комплектующего компонента к его производительности:

$$\Pr_{kl} = \frac{c_{kl}}{RPS_{kl}} \quad (8)$$

где c_{kl} - стоимость *l-го* комплектующего компонента *k-го* набора, RPS_{kl} - производительность *l-го* комплектующего компонента *k-го* набора, которая определяется как:

$RPS_{kl} = RPS_{kl}^{CPU}$ - для процессоров,

$RPS_{kl} = RPS_{kl}^{MEM}$ - для оперативной памяти;

$RPS_{kl} = RPS_{kl}^{HDD}$ - для системы хранения,

$RPS_{kl} = PWR - PWR$ – мощность блока питания установленного в корпусе.

3. Выбираем первую системную плату $i=1$.

4. Выбираем первый набор комплектующих компонентов *(k=1);*

5. Выбираем такой компонент, у которого значение Pr минимально.

6. Проверяем совместимость выбранного комплектующего компонента с выбранной системной платой - если совместимы, то переходим к шагу 6. Если не совместимы, то возвращаемся к шагу 5 и выбираем минимальное значение среди оставшихся элементов.

7. Проверяем, выбраны все наборы комплектующих компонентов или нет – (*k> m-1)*. Если все компоненты выбраны, то переходим к шагу 8, если нет, то переходим к следующему набору (*k=k+1)* и повторяем для него шаги 5 и 6.

8. Определяем стоимость сервера C_i на базе выбранных компонентов.

9. Проверяем, перебраны ли все системные платы($i > n_1$), если да – переходим к шагу 10, если нет - выбираем следующую системную плату – ($i= i +1$).

10. Проверяем выполнение ограничения (7). Если ограничение выполняется то найденное значение C_i и есть решение задачи, если нет, то возвращаемся к шагу 3.

Литература

1. Никитюк Л. А. Модель выбора оптимального набора ресурсов сервера для услуги IPTV [Текст] / Л. А.Никитюк, Р. Ю.Царёв // Збірник наукових праць ОНАЗ ім.. О. С. Попова. – 2014

2. Пападимитриу Х. Комбинаторная оптимизация. Алгоритмы и сложность/ Х.Пападимитриу, К.Стайглиц – М.: Мир, 1985.

3. Левитин А.В. Алгоритмы: введение в разработку и анализ/ А.В. Левитин – М.: Вильямс, 2006.

4. МСЭ-Т Recommendation Y.1540. IP Packet Transfer and Availability Performance Parameters // December, 2002.

5. МСЭ-Т Recommendation Y.1541. Network Performance Objectives for IP-Based Services // May, 2002.

6. Кульгин М. Технологии корпоративных сетей – СПб.: Питер, 1999. – 704 с.

УДК 614.8

Шевченко Р.І.
НУЦЗ України
shevchenko605@rambler.ru

МОДЕЛЮВАННЯ ЗОВНІШНЬОГО ІНФОРМАЦІЙНО-КОМУНІКАТИВНОГО ВПЛИВУ КАСКАДНОГО ТИПУ НА СИСТЕМУ МОНІТОРИНГУ НАДЗВИЧАЙНИХ СИТУАЦІЙ ПРИРОДНОГО ТА ТЕХНОГЕННОГО ХАРАКТЕРУ

Анотація: *В роботі розглядається можливість моделювання одночасних зовнішніх інформаційно-комунікативного впливів, що призводить до виникнення каскадного ефекту критичності функціонування системи моніторингу надзвичайних ситуацій. Сформовані припущення моделювання. Дана оцінка можливих негативних ускладнень у розвитку критичності системи моніторингу та процесу управляючого впливу на об'єкт контролю.*

Незважаючи на неодноразове декларування необхідності створення єдиної системи моніторингу надзвичайних ситуацій [1-4]. Істотного покращення в цьому напрямку, на сьогоднішній день, не досягнуто. Більш того реалії сьогодення загострили низку додаткових проблем, які до цього часу майже не обговорювались, а саме, проблематика впливу на систему (системи) моніторингу надзвичайних ситуацій природного та техногенного характеру зовнішніх чинників різної природи, і у тому числі нерегламентованої складової соціального впливу, що потребує проведення комплексного дослідження за запропонованою тематикою

В рамках запропонованого інформаційно-комунікативного підходу [5,6] можливо розглянути так званий каскадний розвиток зовнішнього впливу на систему моніторингу надзвичайних ситуацій.

В цьому випадку справедливі наступні припущення:

1) в межах (i) системи моніторингу надзвичайних ситуацій (k) та (k+1) впливи зовнішнього характеру незалежні (це справедливо в рамках нетривалого зовнішнього каскадного впливу та є достатньою умовою для оцінки можливостей інформаційно-комунікативного компенсування), а від так до формування показнику інтегральної критичності можна застосувати принцип суперпозицій;

2) інертність (i) системи моніторингу по відношенню до (k) та (k+1) є не змінна та залежить виключно від функціональних характеристик системи моніторингу, які у процесі каскадного впливу залишаються не змінними (це справедливо за виключенням виникнення критичностей, які провокують можливі функціональні зміни системи);

$$[t_{TP}^{inc\,k}, t_{eaTP}^{inc\,k}] = [t_{TP}^{inc\,k+1}, t_{eaTP}^{inc\,k+1}]; [t_{TP}^{off\,k}, t_{eaTP}^{off\,k}] = [t_{TP}^{off\,k+1}, t_{eaTP}^{off\,k+1}], \qquad (1)$$

де $t_{TP}^{inc\,k}$, $t_{TP}^{inc\,k+1}$ - час початку та $t_{TP}^{off\,k}$, $t_{TP}^{off\,k+1}$ - час кінця (k) та (k+1) зовнішніх впливів техногенного (T) або природного (P) характеру; $t_{eaTP}^{inc\,k}$, $t_{eaTP}^{inc\,k+1}$ - час початку та $t_{eaTP}^{off\,k}$, $t_{eaTP}^{off\,k+1}$ - час завершення дії підсистеми оцінки зовнішнього впливу та компенсування викликаних (k) та (k+1) впливами критичностей;

3) критичний вплив (k+1) виникає у часовій зоні різкого зростання критичності (k) впливу за відсутності компенсування у наслідок наявної інерційності системи, як у найбільш

складному та небезпечному періоді. Виникнення (k+1) впливу в інших часових періодах слід розглядати як окремі впливи на систему, що не призводять до каскадного розвитку критичності.

4) час завершення (k) та (k+1) зовнішнього впливу не співпадає у часі та може приймати варіанти розвитку А або В.

$$A - t_{TP}^{off\ k+1} < t_{TP}^{off\ k};\ B - t_{TP}^{off\ k+1} > t_{TP}^{off\ k}. \quad (2)$$

У разі одночасного припинення зовнішніх впливів посткритичний період функціонування системи моніторингу слід вважати не каскадним сценарієм розвитку критичності системи.

Відповідно до висунутих припущень динаміка зміни критичності системи моніторингу надзвичайних ситуацій викликана можливим каскадним зовнішнім впливом природного або техногенного характеру та прогнозуєма дієвість управляючого рішення щодо об'єкту моніторингу представлена на рис. 1 та таблиці 1.

На рисунку 1 використані наступні позначення:

А та В виконання умов припущення (2);

К1, К2, К3, К4 – негативні тенденції інформаційно-комунікативної критичності системи моніторингу викликані каскадним зовнішнім впливом;

Y1, Y2, Y3, Y4, Y5 – негативні тенденції управляючого впливу на об'єкт моніторингу викликані каскадним зовнішнім впливом;

k^{APT} - межа інформаційно-комунікативної критичності;

$y(x)^{кр}$ - межа стабільності контролю (управління) за об'єктом моніторингу).

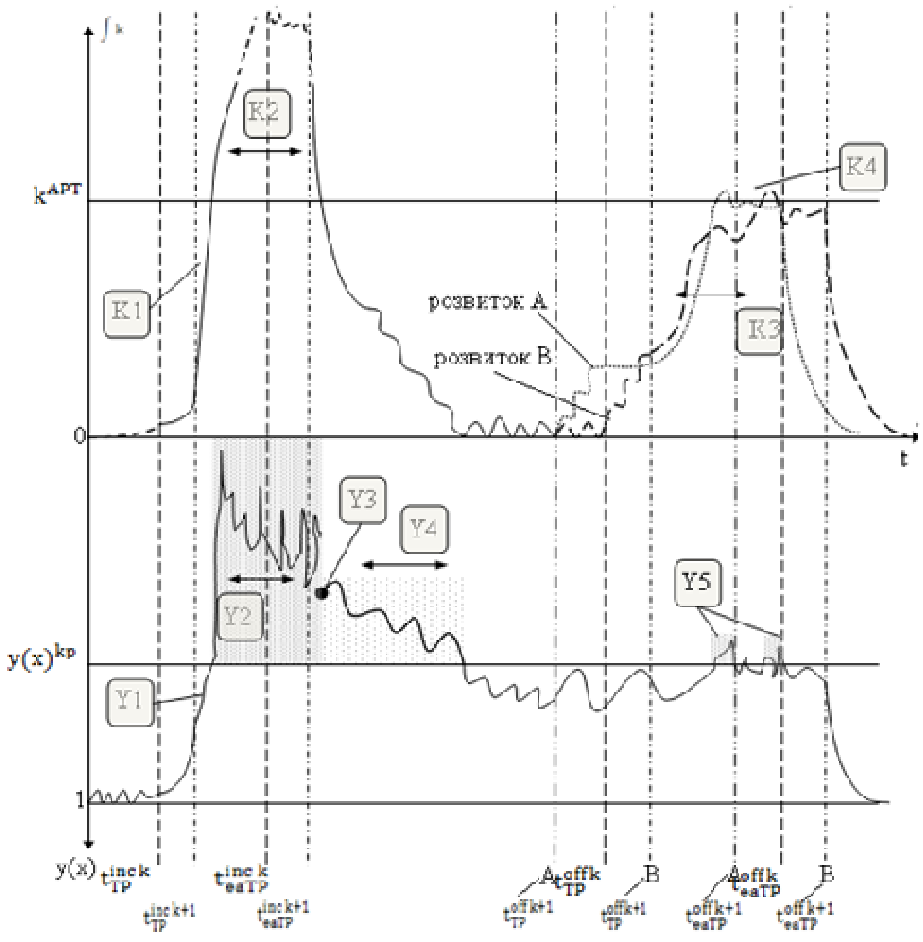


Рис. 1 Аналіз динаміки зміни критичності $\int k$ системи моніторингу надзвичайних ситуацій, що викликана каскадним зовнішнім впливом природного або техногенного характеру та прогнозуєма дієвість управляючого рішення $y(x)$ щодо об'єкту моніторингу в межах [0;1]

Таблиця 1. Оцінка негативних ускладнень у розвитку критичності системи моніторингу та процесі управляючого впливу на об'єкт контролю що викликані можливим каскадним сценарієм зовнішнього впливу природного або техногенного характеру

Група ускладнень	Умовне позначення (рис. 1)	Природа каскадного ускладнення
Процесу виникнення інформаційно-комунікативної критичності	К1	Зростання швидкості наростання критичності системи у критичній часовій зоні, а від так скорочення часу виходу системи моніторингу за межі інформаційно-комунікативної стійкості
	К2	Розростання у часі зони інформаційно-комунікативної нестійкості
	К3	Розростання зони пост критичної інформаційно-комунікативної критичності
	К4	Можливість виникнення локальних короткотермінових зон інформаційно-комунікативної нестійкості
Ефективності управляючого впливу на об'єкт моніторингу	Y1	Зростання швидкості втрати ефективності управляючого впливу на стан безпеки об'єкту моніторингу
	Y2	Розростання «чорної» зони непрозорості управляючого впливу
	Y3	Зростання невизначеності (часової та абсолютного значення) точки виходу з зони непрозорості управляючого впливу
	Y4	Розростання «сірої» зони обмеженої ефективності управляючого впливу
	Y5	Збільшення вірогідності у пост критичній зоні виникнення короткотермінових повторних «чорних» зон непрозорості управляючого впливу

Висновки. Аналіз прогнозуємої поведінки функціонування системи моніторингу надзвичайних ситуацій природного та техногенного характеру у режимі критичності від дії каскадних впливів зовнішнього характеру доводить відсутність суттєвого функціонального резерву системи до складних інформаційно-комунікативних умов. Стала функціональна схема державної системи моніторингу надзвичайних ситуацій взагалі не передбачає наявність підсистеми внутрішнього інформаційно-комунікативного компенсування та дієвих функціональних зв'язків з зовнішніми підсистемами компенсування, як в рамках єдиної державної системи моніторингу надзвичайних ситуацій (наприклад міжоб'єктовий, міжрегіональний рівень тощо), так і між галузевої співпраці (наприклад з система моніторингу соціальної небезпеки, транскордонними система моніторингу надзвичайних ситуацій інших держав тощо).

Література

1. Національна доповідь про стан техногенної та природної безпеки в Україні у 2014 році [Електрон.ресурс]. – Режим доступу: www.mns.gov.ua/content/annual_report_2014.html

2. Абрамов Ю.А. Основные требования к созданию единой системы мониторинга чрезвычайных ситуаций / Ю.А. Абрамов, В.В. Тютюник, Р.И. Шевченко // Системи обробки інформації. - Сб. науч. тр. . - Харьков: ХУПС 2005. – Вып. 6 (46).- С. 203-207.

3. Абрамов Ю.А. Взаимосвязь инициирующих и поражающих факторов чрезвычайных ситуаций природного характера на территории Украины / Ю.А. Абрамов, В.В. Тютюник, Р.И. Шевченко // Проблеми надзвичайних ситуацій. - Сб. наук. пр. . - Харків: УЦЗУ 2007. – Вип. 5 - С. 8-17.

4. Макиев Ю.Д. Аннотация на монографию «Современные системы мониторинга и прогнозирования чрезвычайных ситуаций»: Стратегия гражданской защиты: проблемы и исследования /Ю.Д. Макиев Том 4, 2014, № 1(6) –С. 85-90

5. Шевченко Р.І. Застосування АВС-аналізу для формування інформаційного фільтру другого порядку підсистеми збору та контролю стану об'єктів моніторингу надзвичайних ситуацій / Р.І. Шевченко// Збірник наукових праць Харківського університету Повітряних Сил – Харків: ХУПС ім. Івана Кожедуба, 2015. – № 2 (43). – С. 166 – 175.

6. Шевченко Р.І. Розробка методу критичних та ускладнюючих сигналів для формування інформаційного фільтру підсистеми збору та контролю стану об'єктів моніторингу надзвичайних ситуацій / Р.І. Шевченко// Системи обробки інформації – Харків: ХУПС ім.. Івана Кожедуба, 2015. – № 7 (132). – С. 204 – 209

УДК 621.395

Шевчук М.С.
ОНАЗ ім. О.С.Попова
di.margarita@yandex.ua
Науковий керівник – к.т.н., проф. Нікітюк Л.А.

ХАРАКТЕРИСТИКА ВИКОРИСТАННЯ ХМАРНОЇ ТЕХНОЛОГІЇ SAAS КОМПАНІЯМИ СВІТУ

Анотація. *Досліджується використання хмарної технології SaaS компаніями світу*

На сьогоднішній день мобільність – одна з основних вимог користувачів Інтернет-послуг, вже недостатньо передачі відео, аудіо контенту або простих повідомлень, їм бажано мати дані послуги в будь-який момент в будь-якому місці. Хмарні технології пропонують не тільки ці умови, а ще і можливість значно зменшити вимоги до апаратного забезпечення. Хмарні технології - це зручна середа для зберігання та обробки інформації, що об'єднує в собі апаратні засоби, ліцензійне програмне забезпечення, канали зв'язку, а також технічну підтримку користувачів. Робота в хмарах спрямована на зниження витрат і підвищення ефективності роботи підприємств. Особливістю хмарних технологій є можливість масштабованості. Клієнт може працювати з хмарними сервісами з будь-якої точки планети і з будь-якого кінцевого пристрою, що має доступ в мережу Інтернет.

Колись хмарні технології були одною із складових нашого майбутнього, але вже сьогодні це стало нашою реальністю - є сервіси, які реалізують концепцію хмари і набувають популярності не тільки в межах своєї країни, але і за кордоном. Що є також не менш важливим – це те, що в Україні є представники цих компанії і фірми, що почали надавати свій унікальний продукт. Тому дослідження хмарної технології SaaS є актуальною темою і метою на сьогоднішній день.

Мета данної роботи – зробити аналіз сучасного ринку хмарних технологій, дослідити зростання об'єму прибутку компаній, що надають такі послуги: Saas, PaaS, IaaS, VPC, EPC, дослідити яку роль технологія SaaS займає у прибутку компаній, що надають послуги за допомогою цієї технології.

Обрана мета може бути досягнута рішенням наступних завдань:

- аналіз сучасного ринку хмарних технологій
- порівняння прибутку 2013 і 2015 року компаній, що надають послуги хмарних технологій
- аналіз прибутковості хмарних технологій
- дослідження ролі SaaS у компаніях, що надають послуги за допомогою цієї технології

Серед основних хмарних технологій необхідно виділити Saas, PaaS, IaaS, VPC, EPC, вони мають найбільший попит серед користувачів і їх реалізацією займаються такі відомі компанії як Google, Microsoft, Cisco і IBM, що тільки укріпляє їх позиції на ринку хмарних технологій.

За даними IDC, ринок SaaS в світі склав близько 20 млрд дол. В 2013 році і зросте до 32 млрд дол. В 2015-му. Проте за інформацією STL (рис. 1), яка наводить свої дані на базі вторинного аналізу досліджень низки аналітичних агентств, включаючи Bain Analysis, Forrester, IDC, William Blair & Co., в 2015 році обсяг цього ринку досягне лише 17,5 млрд долларів. Прибуток з хмарної технології PaaS також зросте на 5,5 млрд. дол. IaaS та EPC зменшать показники прибутку на 1 і 3,5 млрд. дол. відповідно Це можна наглядно побачити на рис.1.

Отже видно, що такі технології як SaaS і PaaS набувають популярності і особливо SaaS, що явно є лідером продаж серед інших, VPC витримує свої позиції не змінюючи їх, IaaS та EPC навпроти має тенденцію до зниження попиту і відповідно це зменшує прибуток компаній, що реалізують дану послугу.

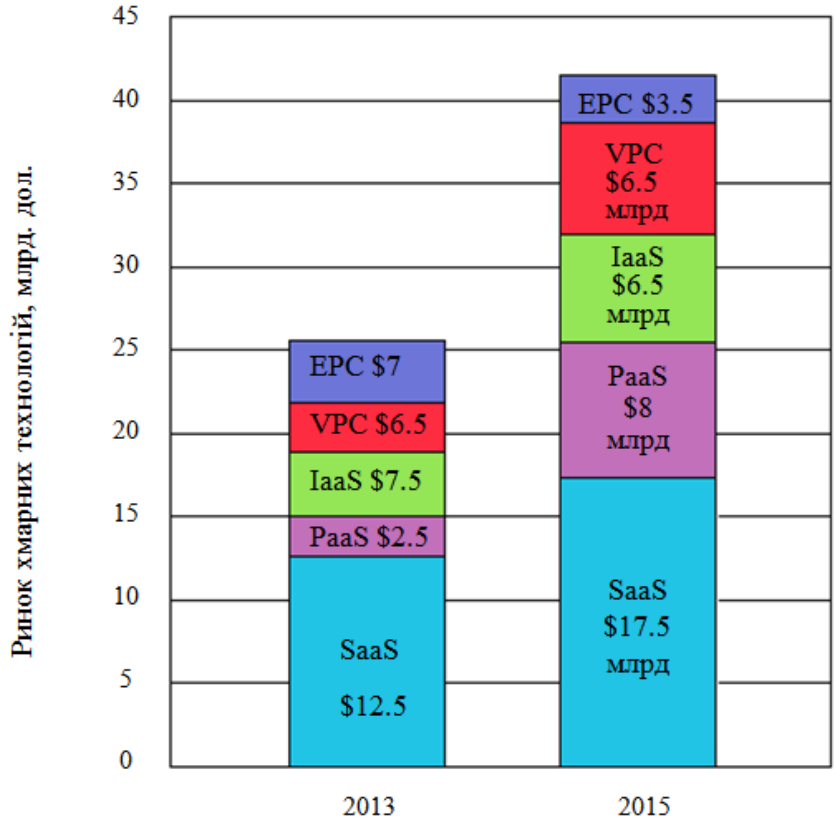


Рис.1 Оцінка ринку хмарних обчислень

На наступному малюнку розглядається технологія SaaS у контексті різних компаній, так як вона являє собою поки що найуспішнішою технологією серед усій хмарних технологій. На рис. 2 представлено дві шкали. Нижня відноситься до червоних смуг - це дохід від надання ПО у вигляді послуг. Очевидно, що Salesforce.com - це лідер даного ринку і компанія Intuit знаходиться на другому місці, так як у них досить високий прибуток за рахунок постачання послуг за допомогою SaaS. Верхня шкала (сині смуги) показує частку SaaS в обороті компанії. Це означає, що з усього софтверного обороту компанії Salesforce.com близько 90% припадає на надання ПО у вигляді SaaS, в компанії Intuit - близько 40%, а в компанії Microsoft, яка займає четверте місце за оборотом, SaaS в продажах ПЗ становить трохи більше відсотка. Неможливо не помітити компанію IBM і Oracle що

мають дуже маленькую частку SaaS, але приблизно 10-20% прибутку саме від программного забезпечення як послуги.

Оскільки ринок США займає більше 60% світового, то позначені на малюнку тенденції можна вважати близькими до загальносвітових.

Отже, згідно з проведенними дослідженнями, можна стверджувати, що ринок хмарних технологій не тільки розвивається, а ще має перспективу для свого розвитку і інвесторам, що націлені на довгострокові інвестиції необхідно звернути на хмарні технології ще більшу увагу. Самою продуктивною є технологія, що має концепцію «программне забезпечення як послуга». Очевидно, що компанії IBM, Microsoft і Salesforce.com, що використовують SaaS лідирують завдяки великому досвіду роботи. IBM і Microsoft мають серйозні напрацювання з надання традиційних («нехмарних») продуктів для колективної роботи, а також з поставки ПЗ для корпоративної роботи на базі хостингу.

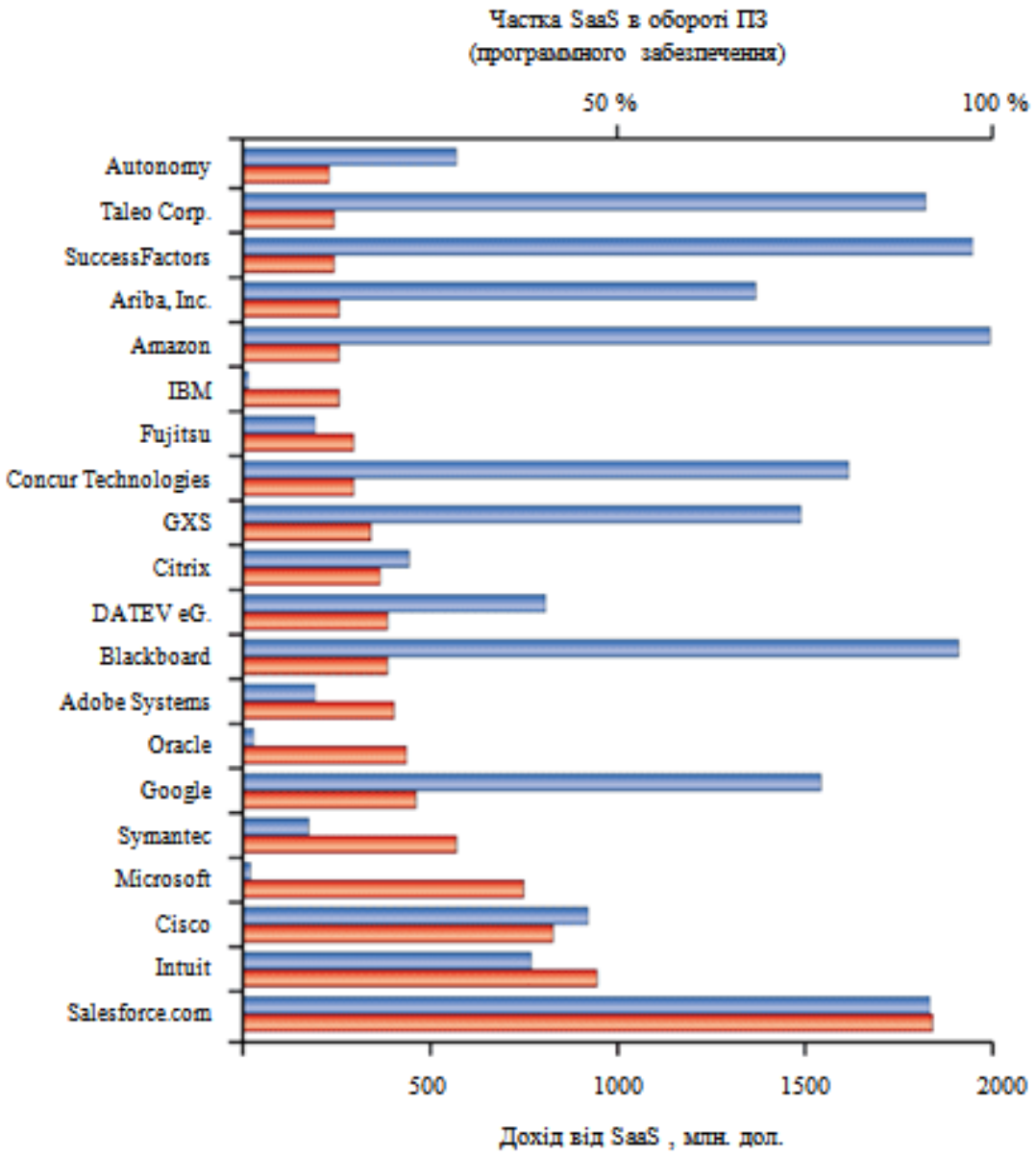


Рис.2 Співвідношення прибутку від технології SaaS і її долі у великих корпораціях

Salesforce.com просуває свої рішення для колективної роботи на хвилі пропозиції свого популярного CRM-рішення та PaaS-інфраструктури. На данний момент на ринку послуг хмарних технологій є багате різноманіття послуг та пропозицій і рішення вибору

необхідного залежить від потреб користувача і обмежене грошовими коштами потенційного замовника.

Література

1. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі / Київ «САММІТ-КНИГА», 2010.
2. Сайт compress: http://compress.ua/article.aspx?id=23954

УДК. 621.395.7

Ятова А.
ОНАЗ ім. О.С.Попова
Rusalka26041994@i.ua
Науковий керівник - доц. Царьов Р.Ю.

АНАЛІЗ МЕТОДІВ ОЦІНКИ ЯКОСТІ НАДАННЯ ПОСЛУГИ IP-TV

***Анотація**: В роботі проведено аналіз методів які застосовуються для оцінки якості надання послуги IPTV.*

Одним з найбільш затребуваних відео сервісів є сервіс IP-телебачення. IP-телебачення (Internet Protocol Television, IPTV) це надання послуг цифрового телебачення та інших аудіо - та відеопослуг по широкосмуговим мережам передачі даних з використанням основних протоколів, що підтримують мережу Інтернет. IPTV займає все більшу частку ринку на тлі поступового скорочення інших платформ платного ТБ. Частка ринку IPTV послуг збільшилася з 10% в 2011 році до 11,5% у 2012 та 12,9% у 2013. Доступність високошвидкісних широкосмугових мереж створюють ідеальні умови для росту і впровадження IPTV, за оцінками експертів до 2018 року частка ринку IPTV збільшиться до 18% від загального обсягу [1,2]. Послуга IPTV є однією з найбільш затребуваних послуг на українському ринку.

Згідно зі статистичними даними [3] на Україні в 2013 році кількість абонентів IPTV склало трохи більше 340 тисяч (5,5 % від загального числа абонентів платного телебачення), роком раніше цей показник становив лише 2,5 %. У той же час, за підсумками IV кварталу 2013 року кількість абонентів кабельного ТБ скоротилося на 7,6 %.

Враховуючи вище викладене, можна зазначити, що контроль якості послуги IPTV є однією з актуальних завдань для українських операторів зв'язку. В роботі аналізуються методи, які дозволяють оцінити якість послуги.

В загальному, випадку для оцінки якості послуги можна застосувати наступну модель (рис. 1):

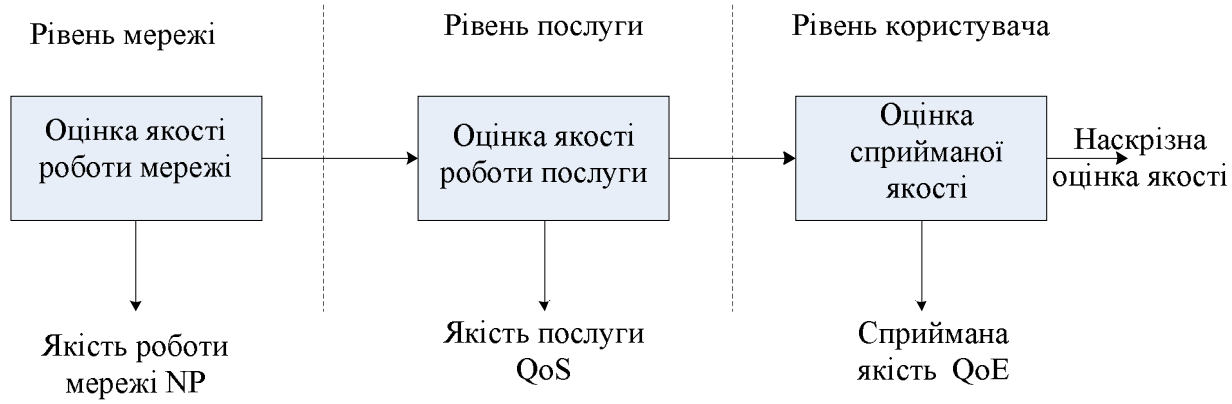


Рисунок 1 – Модель оцінки якості послуги

Перший рівень моделі відображає показники якості функціонування на рівні мережі (Network Performance NP), другій рівень моделі відображає показники якості послуги - доступність, повноцінність і безперервність послуги, третій рівень відображає як сприймає послугу користувач.

Для оцінки якості передачі відео (послуги IPTV), застосовується два підходи – суб'єктивний та об'єктивний. Суб'єктивний підхід полягає у тому, що для оцінки якості відео необхідно організувати групу експертів, які переглядають відео та оцінюють його якість. Останнім часом постійне використання суб'єктивного підходу в процесі експлуатації послуг IPTV не є економічно доцільним - необхідність постійно утримувати групу експертів . Тому більшу популярність останнім часом набули методи об'єктивної оцінки, що ґрунтуються на збиранні та аналізі мережевих характеристик.

До об'єктивних методів відносяться: параметр доставки інформації MDI (Media Delivery Index); метод VQM (Video Quality Measurement); метрика MPQM (Moving Picture Quality Metric); метрика NQM (Noise Quality Measure); метрика PSNR (Peak Signal to Noise Ratio). Характеристика цих методів наведена у табл. 1

Таблиці 1 - Характеристика об'єктивних методів оцінки якості IPTV

№ пп.	Метод	Показник (що вимірюється)	Методика проведення (як вимірюється)	Робота у режимі реального часу	Характеристика
1	MDI (RFC 4445 IETF)	Затримка, джитер, % втрат	Моніторинг мережі, вимір мережевих характеристик на різних сегментах мережі	+	Дозволяє визначити необхідний обсяг буферу на приймальній стороні, не залежить від типу кодеку. Дозволяє локалізувати несправність, контролює одночасно велику кількість потоків. Не підтримує ретельний аналіз транспортного відео потоку, не враховує не лінійність алгоритмів стискання відео.
2	VQM (BT.168 3 ITU-R)	Оцінює видимий результат погіршення відео (змазаність, мерехтіння, блочність, шум, спотворення кольору)	Порівнюється вихідний відео потік з відео потоком отриманим у кінцевій точці. Отримані показники комбінуються у єдину метрику.	-	Гарно взаємодіє з суб'єктивними методами. Не контролює стан мережі.
3	MPQM	Оцінка сприйняття. Аналізує контрастність, розмитість, розсипання зображення, завмирання, порушення кольоровості, артефакти.	Порівнюється вихідний відео потік з відео потоком отриманим у кінцевій точці та оцінює за п'ятибальною шкалою.	+	Дозволяє контролювати якість послуги IPTV на будь-якій ділянці мережі , будь-якому етапі надання послуги. Орієнтовано на сприйняття відео глядачем. Затратний метод з точки зору ресурсів.
4	NQM	Розкид контрасту залежно від дозволу зображення і просторової частоти, розкид значень яскравості	Розрізняють частотне спотворення і шум та досліджують, окремо, вплив кожного з них на сигнал	-	Дозволяють покращити алгоритми відновлення відео. Не оцінюють якість передачі відео в цілому

№ пп.	Метод	Показник (що вимірюється)	Методика проведення (як вимірюється)	Робота у режимі реального часу	Характеристика
		сусідніх елементів, залежність контрасту від просторових частот, ефекти, що маскують контраст.			
5	PSNR	Вимірює співвідношення сигналу до шуму або пікове відношення сигналу до шуму між вихідним сигналом і сигналом на виході системи. Втрати.	Вимірювання на різних ділянках мережі. розраховується через MSE. Результатом є значення в дБ. Норма - 30-40 дБ.	+	Відносно простий. Не враховує вплив специфічних для відео застосувань.

Кількість втрачених пакетів, затримка та джитер є домінуючим факторами, що впливає на якість відео [4,5] тому можна зробити висновок, що метод MDI потрібно застосовувати в будь якому разі, а інші методі застосовуютьсь у разі необхідності контролю додаткових параметрів якості.

Література

1. Обзор развития мирового рынка телекоммуникаций [Электронный ресурс] / The Cisco corp. – Режим доступа: \www/ URL: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html

2. Прогноз развития рынка IPTV [Электронный ресурс] / UA Digital TV – Режим доступа: \www/ URL: http://uadigital.tv/iptv-2018/

3. Л. А. Никитюк «Услуги связи нового поколения» / Л.А. Никитюк, Р. Ю. Царёв // журнал «Зв'язок » - 2012 р.- №1. - с23.

4. IP Packet Transfer and Availability Performance Parameters: Рекомендация ITU-T Y.1540. - 2002.

5. Network Performance Objectives for IP-Based Services: Рекомендация ITU-T Y.1541. – 2002.

УДК 004.056

Бишовець Б.М.
ОНАЗ ім. О.С.Попова
bogdanbyshovets@gmail.com
Науковий керівник – д.т.н., проф. Горицький В.М.

МЕТОД ПРОТИДІЇ ПЕРЕХОПЛЕННЮ ІНФОРМАЦІЇ ПО ТЕХНІЧНИМ КАНАЛАМ ВИТОКУ НА ОСНОВІ КОДОВОГО ЗАХИСТУ

Анотація. *Розглядаються методи протидії перехопленню інформації по технічним каналам витоку.*

В даний час самим здійсненим фізичним середовищем для передачі інформації, а також найперспективнішим середовищем для передачі великих потоків інформації на значні відстані вважається оптичне волокно. У зв'язку з надзвичайно широким поширенням оптичного волокна як середовище передачі досить актуальною є проблема його захищеності від несанкціонованого знімання інформації.У інформаційному суспільстві головним

ресурсом є інформація. Саме на основі володіння інформацією про самі різні процеси і явища можна ефективно і оптимально будувати будь-яку діяльність. Поважно не лише виробити велику кількість продукції, але виробити потрібну продукцію в певний час. З певними витратами і так далі.

Інформація сьогодні коштує дорого і її необхідно охороняти. Масове вживання персональних комп'ютерів, на жаль, виявилося пов'язаним з появою програм-вірусів, що само відтворюються, перешкоджають нормальній роботі комп'ютера, руйнівних файлову структуру дисків і що завдають збитку інформації, що зберігається в комп'ютері. Інформацією володіють і використовують її всі люди без виключення. Кожна людина вирішує для себе, яку інформацію йому необхідно отримати, яка інформація не має бути доступна іншим і так далі. Людині легко, зберігати інформацію, яка у нього в голові, а як бути, якщо інформація занесена в «мозок машини», до якої мають доступ багато людей.

Вже в перших роботах по захисту інформації були викладені основні постулати, які не втратили своєї актуальності й донині: абсолютний захист створити не можна; система захисту інформації повинна бути комплексною; СЗІ повинна бути адаптуємою до умов, що змінюються. До цих аксіом потрібно додати: по-перше, СЗІ повинна бути саме системою, а не простим, багато в чому випадковим і хаотичним набором деяких технічних засобів й організаційних заходів, як це найчастіше спостерігається на практиці; по-друге, системний підхід до захисту інформації повинен застосовуватися, починаючи з підготовки технічного завдання й закінчуючи оцінкою ефективності і якості СЗІ в процесі її експлуатації.

Насамперед, СЗІ повинна мати цільове призначення. Причому, чим більш конкретно сформульована мета захисту інформації, детально з'ясовані наявні для цього ресурси й визначений комплекс обмежень, тим більшою мірою можна чекати одержання бажаного результату. Якщо ціль забезпечення інформаційної безпеки проста принципово досяжна, то виявляється досить порівняно нескладних по складу й структурі СЗІ.

Для запобігання втрат інформації розробляються різні механізми її захисту, які використовуються на всіх єтапах роботи з нею. Захищати від пошкоджень і зовнішніх дій треба і пристрої, на яких зберігається секретна і важлива інформація, і канали зв'язку.

Пошкодження можуть бути викликані поломкою устаткування або каналу зв'язку, підробкою або розголошуванням секретної інформації. Зовнішні дії виникають як в результаті стихійних лих, так і в результаті збоїв устаткування або крадіжки. Для збереження інформації використовують різні способи захисту: безпека будівель, де зберігається секретна інформація; контроль доступу до секретної інформації; – розмежування доступу; дублювання каналів зв'язку і підключення резервних пристроїв; криптографічні перетворення інформації;

В даний час найкращим фізичним середовищем для передачі інформації, а також найперспективнішим середовищем для передачі великих потоків інформації на значні відстані вважається оптичне волокно. Волоконно-оптичні лінії зв'язку - це вид зв'язку, при якому інформація передається по оптичних діелектричних хвилеводах, відомих під назвою "оптичне волокно".

У зв'язку з надзвичайно широким поширенням оптоволокна як середовище передачі досить актуальною є проблема його захищеності від несанкціонованого знімання інформації. Оптичне волокно в даний час вважається найдосконалішим фізичним середовищем для передачі інформації, а також найперспективнішим середовищем для передачі великих потоків інформації на значні відстані.

Література

1. Убайдуллаєв Р.Р. Волоконно-оптичні мережі. М., Еко-Трендз, 2000.
2. Фріман Р. Волоконно-оптичні системи зв'язку. М., Техносфера; 2004.
3. Запечніков С.В., Милославська Н.Г., Толстой А.І., Ушаков Д.В. Інформаційна безпека.
4. Домарєв В. В. Захист інформації та безпека комп'ютерних систем 1999.
5. Ярочкін В. І. Інформаційна безпека. Підручник для вузів. М, 2003.

ЗМІСТ

СЕКЦІЯ 3. ІНФОРМАЦІЙНІ МЕРЕЖІ ТА ТЕХНОЛОГІЇ