**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ**

**TP-LINK UKRAINE**



TP-LINK®
The Reliable Choice

# ТЕЗИ

**НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

## «ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

**6 – 7 червня 2018 р.**

**м. Київ**

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
STATE SERVICE OF SPECIAL COMMUNICATION
AND INFORMATION PROTECTION OF UKRAINE
TP-LINK UKRAINE

# PROCEEDINGS

OF THE SCIENTIFIC AND PRACTICAL CONFERENCE

## «OPERATIONAL AND SECURITY PROBLEMS OF INFORMATION AND COMMUNICATION SYSTEMS»

June, 6 – 7, 2018
Kyiv, Ukraine

---

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
TP-LINK UKRAINE

# ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

## «ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

6 – 7 червня 2018 р.
м. Київ, Україна

---

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
НАЦИОНАЛЬНЫЙ АВИАЦИОННЫЙ УНИВЕРСИТЕТ
ГОСУДАРСТВЕННАЯ СЛУЖБА СПЕЦИАЛЬНОЙ СВЯЗИ
И ЗАЩИТЫ ИНФОРМАЦИИ УКРАИНЫ
TP-LINK UKRAINE

# ТЕЗИСЫ

НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

## «ПРОБЛЕМЫ ЭКСПЛУАТАЦИИ И ЗАЩИТЫ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ»

6 – 7 июня 2018 г.
г. Киев, Украина

**УДК 621.39: 004.9 (082)**

Проблеми експлуатації та захисту інформаційно-комунікаційних систем: Тези науково-практичної конференції; м. Київ, 6 – 7 червня 2018 р., Національний авіаційний університет. – К.: Вид-во ТОВ «Центр учбової літератури», 2018. – 98 с.

**ISBN: 978-611-01-0740-2**

## ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

УДК 621.311 (043.2)

**В.Е. Авраменко, О. П. Ткаліч**
*Національний авіаційний університет, м. Київ*

## Технологія «Інтернет речей» для систем енергопостачання міста

В теперішній час найбільш опрацьованим варіантом застосування технологій Internet of Things в енергетиці є «розумні мережі» (Smart Grids). Робота такої мережі заснована на тому, що постачальник і споживач отримують об'єктивну картину по використанню енергоресурсів за рахунок моніторингу на всіх ділянках мережі і, як наслідок, отримують можливість оперативного управління. У разі аварій такі мережі здатні автоматично ідентифікувати проблемні ділянки і протягом короткого часу направляти електроенергію по резервними схемами, відновлюючи електропостачання.

Інформаційна мережа Smart Grid об'єднує безліч технічних елементів і вузлів.

В домені споживачів електроенергії такими елементами є смарт-лічильники, електричні прилади, системи акумулювання енергії, електротранспорт, а також об'єкти розподіленої генерації.

В домені передачі і розподілу енергії елементами інформаційної системи є блоки вимірювання фаз, контролери підстанцій, об'єкти розподіленої генерації, системи акумулювання енергії.

Управління енергомережею проводиться за допомогою наступних систем :

- «розумної» маршрутизації енергопотоків (Smart Routing) - системи контролю навантаження і якості, самовідновлення мереж в результаті аварійних подій, зберігання енергії і ін .;
- «Розумних» вимірювань (Smart Metering) - сучасні інтелектуальні прилади обліку (Smart Meter), системи інтелектуальної будівлі (Smart Home), «розумні» побутові прилади.В операційному домені елементами інформаційної системи є SCADA-системи.

Для забезпечення безпечної передачі електроенергії і для стабільної експлуатації мереж і обладнання необхідно досягнення

оптимального балансу між пропозицією електроенергії і її споживанням. Таким чином, вкрай важливо володіти точними, оперативними даними про виробництво енергії, а також мати можливість контролювати і автоматично управляти її подальшим використанням.

Технології PLC є найбільш економічною та ефективною, завдяки чому ідеально підходять для інтелектуальних мереж.

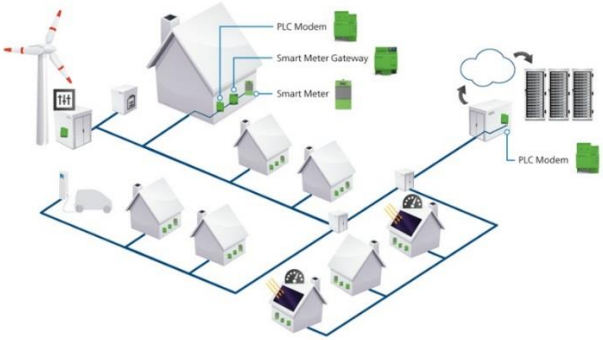



Рис.1 Розумна мережа з використанням технології PLC

Топологія мережі (рис.1) побудована таким чином, що кожен будинок зв'язується з розподільчою станцією через лінії електропередачі. Дані про енергію ретранслюються від шлюзу інтелектуального вимірювача до PLC модему доступу. Звідси дані передаються на розподільну станцію. На розподільчій станції медіаперетворювач збирає дані про енергію всієї мережі та ретранслює до постачальника енергії.

Перевага системи полягає в тому, що вона не вимагає ніяких специфічних каналів передачі інформації, так як кінцеве обладнання підключено безпосередньо до мережі харчування, позбавляє необхідності укладання всіх можливих інформаційних кабелів.

**Висновки:** Розвиток технологій «розумних» мереж (Smart Grid) і «розумних» лічильників (Smart Metering) несе в собі перспективу того, що всі промислові і побутові енергоприймачі знайдуть здатність до взаємодії в інформаційній мережі, стануть керованими і будуть виконувати функції вимірювання власного споживання електроенергії і потужності. Це дасть реальний інструмент для енергозбереження та підвищення енергоефективності.

УДК 004.658.2 (043.2)

**В. Ю. Алексєєнко, О. Г. Голубничий**
*Національний авіаційний університет, м. Київ*

# ВЕБ РЕСУРС З КАТАЛОГІЗАЦІЇ ТА СИСТЕМАТИЗАЦІЇ ІНФОРМАЦІЇ ПРО БЛОКЧЕЙН ТА ЦИФРОВІ АКТИВИ ЯК НЕВІД'ЄМНА ЧАСТИНА ТЕХНОЛОГІЇ

## 1. Проблема розповсюдження специфічної інформації в мережі «Інтернет»

За рахунок швидкого розвитку технологііі блокчейн (*Blockchain*) в світовій мережі інтернет з'являєтеся багато різної інформації з розвитку в даній галузі. Все більше і більше з'являться нових досягнень та робочих місць в галузі розробки на мовах *Solidity, JavaScript, C++*. В зв'язку з цим інформація про технологію з'являється в багатьох місцях і в суспільства немає доцільного, централізованого джерела яке б могло надати всю необхідну інформацію у доступному місці та в доступній формі. Також нерівномірність створення такої інформації впливає на швидкість її розповсюдження.

### 1.1. Що таке блокчейн?

Блокчейн, по своїй суті, є розподіленою облікової книгою записів про події в цифровому світі. Ця система децентралізована і доступна безлічі користувачів. Записи в неї можна вносити тільки за згодою більшості користувачів. І ще, одного разу записана інформація вже ніколи не може бути змінена або стерта.

Наприклад: Блокчейн біткойнів містить в собі точну і достовірну інформацію про всі коли-небудь здійснені в мережі біткойн-транзакції.

Максимально стисло блокчейн (*Blockchain*) – це вибудувана за певними правилами безперервний послідовний ланцюжок блоків, що містять інформацію. Блокчейн як вічний цифровий розподілений журнал економічних транзакцій, може бути запрограмований для запису не тільки фінансових операцій, але і практично всього, що має цінність.

## 2. Пропозиція щодо вирішення проблеми

Інформація яка з'являється у мережі має певну цінність для користувачів і повинна мати легкий доступ. Тому вирішенням проблеми буде веб ресурс, який збираючи інформацію з різних джерел, проводить її подальшу каталогізацію та сортування з подальшою архівацією.

Наприклад:

- Новини – через їх велику кількість люди не встигають відстежувати актуальність інформації, тому створення архіву на основі блокчейну дає змогу робити в ньому записи, де інформація не може бути видалена або змінена.
- Каталог розробників – створення архіву достовірних соціальних акаунтів найбільших розробників в галузі технології блокчейн, оскільки зловмисники вводять в оману людей створюючи фейкові акаунти.
- Архів блокчейн гаманців – створення бази даних посилань на репозиторії з блокчейн гаманцями для різних платформ, що допоможе полегшити транзакції між користувачами та уникнути зловмисників.
- Створення каталогу криптовалютних бірж – для уникнення користувачами потрапляння на фішингові сайти, створених для викрадення коштів у вигляді цифрових активів.

## 3. Результати досліджень та теперішня стадія проекту

На даний момент триває створення та розвиток даного веб ресурсу, іде збір інформації від представників цільової аудиторії, щоб на основі цього розробити комфортний дизайн та впровадити необхідний функціонал з його подальшим вдосконаленням та розширенням.

**Висновки:** за рахунок створення подібного ресурсу, люди, які тільки починають знайомитися з технологіями блокчейн та цифровими активами зможуть швидко та зручно знаходити достовірну інформацію, новини, ділитися нею з суспільством.

**Список використаних джерел:**

1) https://ru.bitcoinwiki.org,
2) https://forklog.com/.

УДК 004.75

**Д.А. Басун, І.Є.Терентьєва**
*Національний авіаційний університет (м. Київ)*

## Використання бездротових сенсорів у системах охоронної сигналізації

Прогрес у галузі мікроелектроніки та безпровідних технологій передачі даних став основою для створення безпровідних сенсорних мереж (БСМ), які набувають дедалі ширшого застосування у вітчизняних системах охоронної сигналізації.

БСМ є одним із сучасних і перспективних напрямків розвитку розподілених самоконфігурованих систем для охорони, моніторингу й безпеки управління ресурсами та процесами.

Проте при розробці та побудові систем охоронних сигналізацій на базі нових технологій бездротової передачі даних виникає низка важливих питань, які потребують вирішення: визначення оптимального розміщення первинних перетворювачів в мережі, вибір типу безпровідної технології передачі даних, та головне довготривала автономна робота компонентів системи.

Тому розробка нових методів моделей та компонентів систем для підвищення ефективності роботи охоронних сигналізацій на базі безпровідних сенсорних мереж є актуальною.

Мета бакалаврської роботи полягає у вирішенні питання підвищення часу автономної роботи бездротової сенсорної мережі за рахунок спільного застосування протоколу маршрутизації та алгоритму розподілу навантаження.

У роботі здійснено аналіз стану розробки та сфери використання БСМ. На їхній основі, сформульовано вимоги до функцій і характеристик безпровідних вузлів та мереж. Виділено переваги й існуючі обмеження, які стримують широке використання БСМ. Використано класифікацію БСМ. Вказано перспективи використання і виділено існуючі проблеми при створенні безпровідних сенсорних мереж.

Було розглянуто існуючі види охоронних систем, в яких можливе використання бездротових сенсорних мереж. Описано БСМ, що дозволяє оцінювати час її життя для фіксованих маршрутів руху стоку,

а також оптимізувати час перебування стоку в точках маршруту за критерієм максимізації часу життя.

Дані залежності досліджувалися при імітаційному моделюванні БСМ. Використано методику розрахунку параметрів моделі, що враховує останні роботи по тематиці дослідження і особливості сучасних бездротових стандартів передачі даних.

Виявлено велику різноманітність підходів з визначення часу життя мережі як розподільної системи. Запропоновано визначення, що враховує здатність БСМ до самовідновлення.

Доведено, що запропонована модель відрізняється від існуючих тим, що описує функціонування кожного вузла мережі інтегральною характеристикою споживаної ним потужності, а також враховує послідовність зміни конфігурацій мережі та пов'язані з нею накладні витрати.

Таким чином, на основі комплексного аналізу запроваджених даних топологій і алгоритмів маршрутизації БСМ запропоновано алгоритм маршрутизації БСМ, орієнтований на збільшення «часу життя» мережі для систем охоронної сигналізації.

**Висновки**:

- використання протоколу маршрутизації GEAR спільно з алгоритмом розподілу навантаження дозволяє збільшити час життя мережі;
- спільне використання алгоритмів вимагає передачу більшої кількості повідомлень запитів, що збільшує завантаженість мережі і збільшує енергоспоживання сенсорних вузлів;
- отримані результати можуть бути використані при розробці гібридних протоколів маршрутизації в сенсорних мережах.

## Список літератури

1. Баскаков С. С. Исследование способов повышения эффективности маршрутизации по виртуальным координатам в беспроводных сенсорных сетях // Вестник МГТУ им. Н. Э. Баумана. Сер. Приборостроение. 2009. № 2. С. 112–124.

2. Комаров М. М., Восков Л. С. Позиционирование датчиков беспроводной сети как способ энергосбережения // Датчики и системы. 2012. Т. 1. С. 34–38.

УДК 004.056.53 (043.2)

**Д.І. Бахтіяров, А.Т. Дехтяренко, А.В. Сілін**
*Національний авіаційний університет, м. Київ*

## ДОСЛІДЖЕННЯ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ

Побічні електромагнітні випромінювання - вид електромагнітних хвиль, що виникають в результаті роботи електричних приладів, зокрема протікання електричного струму по провідниках. Так як електромагнітні випромінювання є збудження електромагнітного поля, то при передачі конфіденційної інформації через локальну мережу або на монітор за допомогою інтерфейсів VGA, DVI, HDMI, виникають електромагнітні випромінювання, які при попаданні на провідник (антену пристрою, що зчитує), породжують в ньому струм, схожий з оригіналом. Після дискретизації ліченого сигналу можна відновити дані, що передаються через провідник, а це може привести до витоку конфіденційної інформації.

Найпростішим прикладом може бути рація. Потрапивши на потрібну частоту можна перехопити переговори. Однак ці випромінювання мають властивість затухати при видаленні від джерела мовлення і з певного моменту злитися з електромагнітним шумом. Небезпека даного мовлення полягає в тому, що будуть існувати певні місця доступні зловмисникам для зчитування побічних електромагнітних випромінювань з достатнім співвідношенням сигнал / шум щоб провести дискретизацію і скористатися каналом витоку інформації. Однак сигнал може не тільки безпосередньо надходити від різних провідників, по яких безпосередньо передається інформація, електромагнітні випромінювання можуть спокійно ретранслюватись через різні електропровідники, наприклад, система опалення або різна проводка. Коротка схема каналу ПЕМВН представлена на рисунку 1.

Канал витоку інформації ПЕМВН є пасивним, тобто інформація не витече, якщо не буде передаватися через різні провідники / випромінювачі. Даний факт також вказує на те, що помітити витік через даний канал інформації досить складно, навіть досвідченому фахівцеві зі спеціальним обладнанням. Також зловмисники можуть скористатися різними шкідливими програмами для штучного створення факту передачі інформації через провідники / випромінювачі для подальшого

перехоплення. Подібні можливості впливу на інформацію усуваються шляхом ізолювання робочих станцій від глобальної мережі Інтернет.

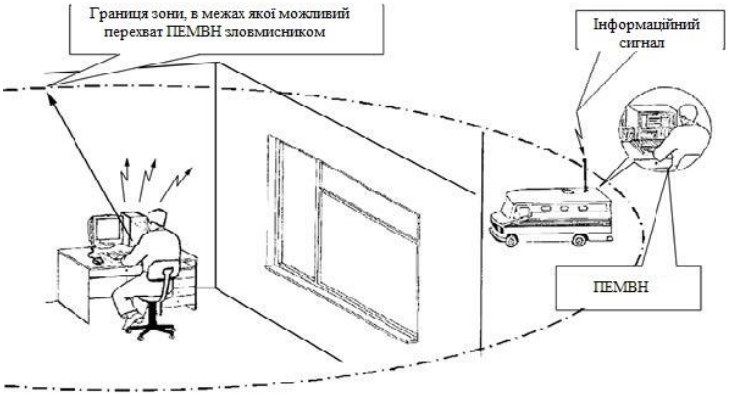



Рис. 1. – Схема витоку інформації по каналу ПЕМВН

Існують 2 способи захисту від подібних атак на канал витоку інформації ПЕМВН:

1) Активний метод;

2) Пасивний метод.

Наочна схема показує роботу даних методів показана на рисунку 2.

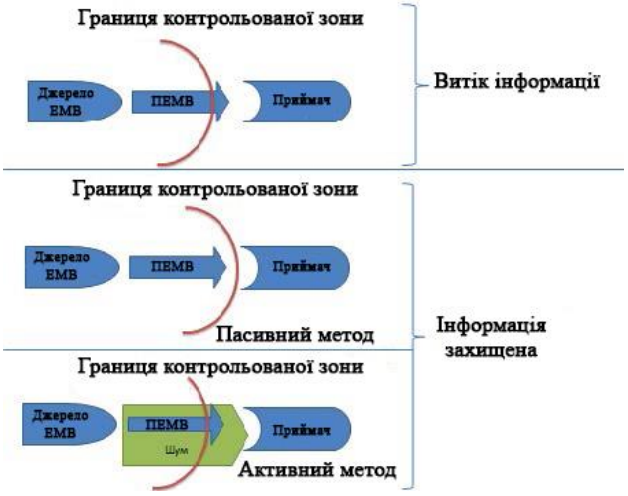


Рис. 2. – Схема роботи методів захисту від витоку інформації по каналу ПЕМВН.

Активний метод полягає в перекритті корисного сигналу більш потужним шумом. Даний метод захисту здійснюється апаратно, через спеціальні пристрої так звані «Генератори шуму». Генератори шумів спеціально створюють потужні електромагнітні випромінювання, які не мають інформативної цінності і ускладнюють або роблять зовсім неможливим аналіз корисного сигналу щодо навколишнього шуму. Треба зауважити, що генератори шумів від побічних електромагнітних випромінювань мають свої недоліки, такі як:

- Досить потужне джерело випромінювання не є корисним для здоров'я;
- Наявність маскуючого сигналу говорить про наявність конфіденційної інформації;
- Не можна гарантувати абсолютну захищеність інформації.

Пасивний метод полягає в зменшенні потужності самого випромінюваного сигналу. Здійснення подібного методу полягає в ізоляції випромінюючих провідників, пристроїв, а також периметра приміщення спеціальними матеріалами, що поглинають електромагнітні поля. Основною перевагою пасивного методу є те, що він усуває недоліки активного методу. Однак при застосуванні пасивного методу екранується абсолютно все, що призводить до досить серйозних витрат.

Найбільш оптимальним у співвідношенні ціна / якість є комбінований підхід, з використанням активного і пасивного методу.

**Список літератури**

1. Косарев В.И. 12 лекций по вычислительной математике. – М.: Изд-во МФТИ, 2000. – 224 с.

2. Рэк. МСЭ-R Стандарт М.1225.

3. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Захист інформації в телекомунікаційних системах – К.: НАУ, 2007. – 321 с.

4. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебное пособие/Г.А. Бузов, С.В. Калинин, А.В. Кондратьев / М.: Горячая линия-Телеком, 2005.

УДК 621.39.005 (043.2)

**О. О. Бережна, Д. І. Бахтіяров, Г.Ф. Конахович**
*Національний авіаційний університет, м. Київ*

## ЗАХИСТ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ VPN ТЕХНОЛОГІЇ

Останнім часом в світі телекомунікацій спостерігається підвищений інтерес до віртуальних приватних мереж. Це обумовлено необхідністю зниження витрат на утримання корпоративних мереж за рахунок більш дешевого підключення віддалених офісів і віддалених користувачів через мережу Internet. Необхідно відзначити, що при об'єднанні мереж через Internet, відразу ж виникає питання про безпеку передачі даних, ось чому виникла необхідність створення механізмів, що дозволяють забезпечити конфіденційність і цілісність інформації, яка передається. Мережі, побудовані на базі таких механізмів, і отримали назву VPN.

У роботі розроблена така корпоративна мережа, що дозволяє об’єднати віддалені сегменти розподіленої мережі з належним станом захищеності і мінімальними фінансовими затратами.

Об’єктом роботи стала корпоративна мережа українського філіалу дистриб’ютора IT-продукції на території України та поза її межами «ELKO Ukraine».

Методами роботи є структурний аналіз потоків корпоративної інформації та побудова схеми системи захисту інформації в окремих потоках даних корпоративної мережі з розподіленою структурою за допомогою використання можливостей VPN технології.

Метою роботи є оцінка рівня захищеності інформації в корпоративній мережі з розподіленою структурою приватного підприємства «ELKO Ukraine», що має ряд віддалених філіалів на території України та закордоном. На базі оцінки захищеності повинні бути представлені вимоги до побудови захищеної корпоративної мережі підприємства з використанням VPN технології.

Перш ніж побудувати систему захисту, необхідно спочатку проаналізувати модель системи, яку треба буде захищати (Рис. 3.1), виділити її основні можливості та загрози, що можуть бути реалізовані.

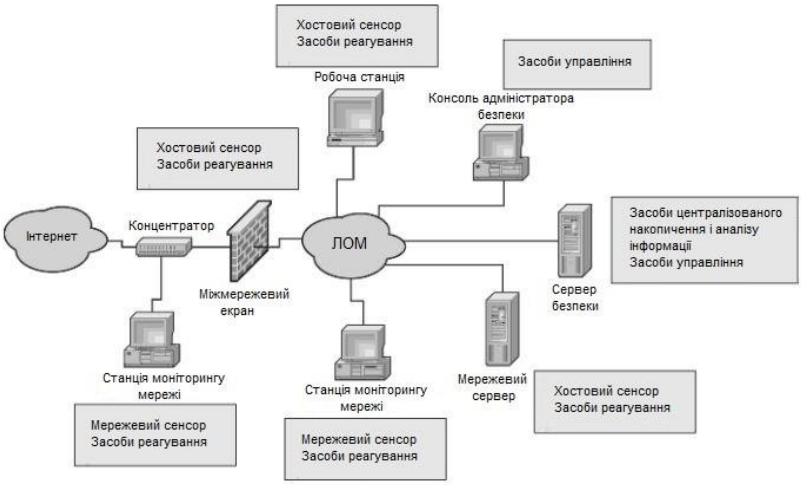



Рис. 3.1. Схема незахищеного сегменту корпоративної мережі Українського філіалу компанії «ELKO Ukraine»

В ході виконання роботи було розглянуто основні принципи побудови корпоративних мереж з розподіленою структурою. Також було проаналізовано основні можливості технології VPN, приведено повну класифікацію можливих реалізацій розгортання VPN мереж за різними принципами. Було проведено детальний аналіз основних протоколів VPN технології, що надають послуги захищеності циркулюючого трафіку в мережі. Також було проаналізовано стан захищеності корпоративної мережі компанії «ELKO Ukraine», що має розподілену структуру для зв'язку з віддаленими філіалами та закордонними представництвами. Також були висунуті основні вимоги до рівня захищеності інформаційного трафіку, що циркулює в корпоративній мережі.

**Висновки.** У роботі проаналізовані основні підходи до створення захищеної корпоративної мережі з використанням VPN технології та побудована захищена мережа з розподіленою структурою. Практична цінність отриманих результатів роботи полягає в отриманні об'єктивних показників необхідності та ефективності впровадження захищеної корпоративної мережі з розподіленою структурою дистриб'ютора IT-продукції «ELKO Ukraine».

УДК 004 (043.2)

**Я.Ю. Бобко, В.В. Антонов, Д.І. Бахтіяров**
*Національний авіаційний університет, м. Київ*

# КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ БЕЗДРОТОВОЇ ЛОКАЛЬНО-ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

Локальна мережа на підприємстві дозволяє співробітникам спростити обмін файлами, що скорочує витрати робочого часу і, отже, збільшує продуктивність персоналу. Якщо цей момент розглядати в перспективі – він теж передбачає отримання, хоч невеликий і неявній, але, все ж, прибутку.

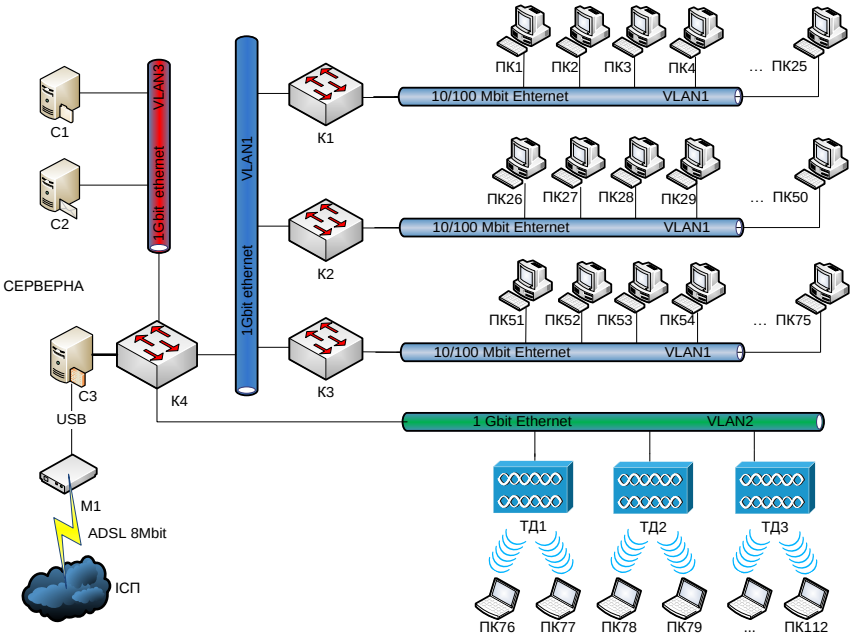
При використанні програмного забезпечення, що передбачає роботу декількох користувачів (спеціалізованих бухгалтерських, юридичних та інших програм), створення та налаштування локальної мережі вкрай обов'язкова. Це дозволить одночасно кільком співробітникам використовувати централізований сервер для спільної роботи.

Локальна мережа на підприємстві дозволяє всім співробітникам отримати доступ в інтернет, навіть тим, чиє робоче місце не обладнане ПК. Організація інтернету по локальній мережі економічно більш вигідна, ніж покупка персональних модемів для кожного співробітника. До того ж, контролювати інтернет-серфінг співробітників в цьому випадку набагато простіше.

Можливість доступу з будинку до файлів, розташованих на робочому комп'ютері – корпоративна пошта, робочі файли і т. д. Ця можливість з'явиться тільки в тому випадку, якщо були здійснені створення і налаштування локальної мережі, що дозволяють забезпечити доступ до інтернету всім комп'ютерам офісу.

Комунікативні вигоди. Для великих офісів (особливо розташованих на декількох поверхах) установка і налаштування локальної мережі життєво необхідна. Чат і відеочат (для цього необхідно буде придбати веб-камери) дозволяють працівникам, фізично знаходяться на значній відстані, ефективно взаємодіяти.

Контроль і віддалений доступ. Ці вигоди не потребують докладному описі. І якщо перше оцінить керівництво компанії, то віддалений доступ до комп'ютерів користувачів – пряма вигода для програміста – адміністратора та служби тех. підтримки.




У роботі модернізовано існуючу локально-обчислювальну мережу підприємства ТОВ «Фаркоп» з додаваннята бездротового сегменту, розроблено та реалізовано комплекс заходів, сукупність яких дозволила забезпечити ефективний захист інформаційних ресурсів підприємства. Беручи до уваги результати опитування американського інституту комп'ютерної безпеки Computer Security Institute, який показав, що інсайдери турбують сучасні компанії значно більше, ніж віруси - в політику безпеки включені проблеми захисту мережі та співробітників компанії від атак, заснованих на використанні соціотехніки.

**Література**

1.Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, техноло-гии, протоколы. 5-е издание. Учебник. – Санкт-Петербург, Питер, 2016.

2.Щербо В.К. Стандарты вычислительных сетей. – М.: Кудиц – Образ, 2015, 216 с.

УДК 621.39.005 (043.2)

**Р. Л. Богданович, О. П. Ткаліч**
*Національний авіаційний університет, м. Київ*

## СТРУКТУРОВАНА КАБЕЛЬНА МЕРЕЖА РОЗУМНОГО БУДИНКУ

Існує декілька можливих рішень для побудови системи «розумного будинку» - дротові та бездротові системи. Основними перевагами дротової системи є: надійність, швидкість відгуку та довгий термін служби, адже система не має пристроїв на батарейках, які вимагали б регулярної заміни.

Принципи СКС застосовуються в системах автоматизації будівель для створення кабельної інфраструктури слабкострумових систем, де використовується така ж магістральна і горизонтальна кабельна структура, як в телекомунікаційних і мережевих системах. Зазвичай прокладка дротів автоматизації здійснюється разом з прокладкою силової та телефонної лінії. Під час монтажу кабелів дотримуються загальних правил монтажу СКС.

В роботі було проведено ознайомлення з технологіями для автоматизації будівель таких як : C-Bus, X-10, LonWorks, KNX. Для проектування мережі «розумного будинку» було обрано відкриту технологію KNX.

Відповідно до даної технології в якості керуючої лінії виступає прокладена паралельно основній проводці будівлі, спеціальна вита пара. Всі пристрої автоматичної системи управління підключаються до даної лінії, і через неї здійснюється зв'язок між пристроями, задіяними системою, рис.1. Для передачі необхідної інформації від передавачів генерується серія сигналів, які по загальній лінії зв'язку відразу передаються на всі підключені приймачі, проте, на інформацію, що надходить реагують тільки ті приймачі, яким вона адресована, тому що кожен приймач в системі має власний унікальний адресу. Обмін інформацією по лінії напряму передбачає до 255 логічних і до 32 767 фізичних адрес. Швидкість передачі інформації - до 1200 біт / с. KNX - протокол може працювати з радіоканалом, з інфрачервоним каналом, з силовою проводкою (1200/2400 біт / с при 230 В, 50 Гц), а також здійснювати передачі по витій парі (зі швидкістю до 9600 байт / с).

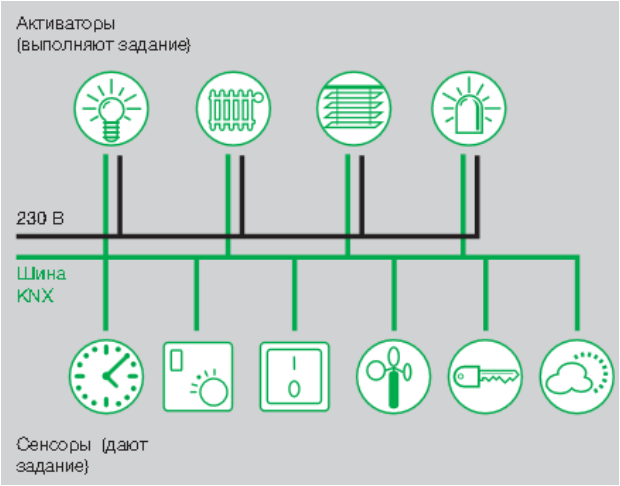



Рис. 1. Принцип технології KNX

Одночасний доступ до шини декількох шинних пристроїв однієї лінії незалежно один від одного може призвести до поява колізій. Тому застосовують метод CSMA/CA ( Carrier Sense Multiple Access/Collision Avoidance).

Цей метод працює так: якщо два абонента одночасно починають передачу, то на шину без затримки виходить абонент, що володіє більш високим пріоритетом (Collision Avoidance), при цьому інший абонент поступається і процес передачі повторюється через деякий час. Якщо обидва абонента мають однаковий пріоритет, то проходить той, який володіє меншою фізичною адресою.

**Висновки:** перед проектуванням СКС «розумного будинку» потрібно з відповідальністю поставитись до вибору технології автоматизації. Так як вона повинна з легкістю об’єднувати такі системи як: інженерну (освітлення, клімат), комп'ютерну, аудіо-відео мультирум систему.

## Використана література

1. «Побудова сенсорної мережі аеропорту та її інтеграція з бездротовою мережею аеропорту стандарту 802.11» О.П. Ткаліч, Р.С. Одарченко, О.Ю. Устинов, Д.О. Колодинський.

УДК 687.39.002 (043.5)

**Вітюк О.С, Конахович Г. Ф.**
*Національний авіаційний університет, м. Київ*

# ЗАСТОСУВАННЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ RSA.

Під ЕЦП розуміється вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронно-цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

## Принцип функціонування

Одним із видів електронно-цифрового підпису є електронно-цифровий підпис на основі криптографічної системи RSA. Розглянемо принципи його функціонування. Спочатку необхідно розрахувати пару ключів (закритий та відкритий). Для цього відправник (автор) електронних документів обчислює два великих простих числа P та Q, потім знаходить їх добуток N=Q*P та значення функції φ(N)=(P-1)*(Q-1). Потім відправник обчислює число E та число D. Пара чисел (E, N) є відкритим ключем. Цю пару чисел автор передає партнерам з листування для перевірки його цифрових підписів. Число D зберігається автором як секретний ключ для підписання.Узагальнена схема формування та перевірки цифрового підпису RSA зображена на рис. 1.

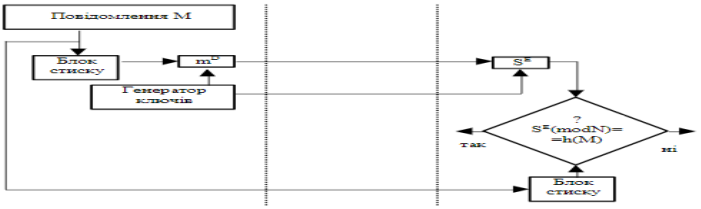



Рис. 1. Узагальнена схема цифрового підпису RSA

Припустимо, що відправник хоче підписати повідомлення M перед його відправкою. Спочатку повідомлення M (блок

інформації, файл, таблиця) стискують за допомогою хеш-функції h(·) в ціле число m:

$m=h(M)$

Потім розраховують цифровий підпис S під електронним документом M, використовуючи хеш-значення m та закритий ключ D:

$S=m(mod(N)$

Пара (M, S) передається партнеру-одержувачу як електронний документ M, підписаний цифровим підписом S, причому підпис S сформований володарем секретного ключа D. Після прийому пари (M, S) одержувач обчислює хеш-значення повідомлення M двома різними способами. Перед усім він відновлює хеш-значення m, застосовуючи криптографічне перетворення підпису S з використанням відкритого ключа E:

$m'=S(modN)$

Крім цього, він знаходить результат хешування прийнятого повідомлення M за допомогою такої ж хеш-функції h:

$M=h(M)$

Якщо виконується рівність обчислених значень,то одержувач признає пару (M, S) дійсною. Доведено, що тільки власник секретного ключа D може сформувати цифровий підпис S по документу M, а знайти секретне число D по відкритому числу E не легше, ніж розкласти модуль N на множники.

**Висновки:** Надійність системи ЕЦП залежить від багатьох факторів, у тому числі і від її структури. Для підвищення надійності системи вцілому необхідно підвищувати, в першу чергу, надійність найслабкіших ланок – ключів шифрування і генераторів випадкових послідовностей, за рахунок відповідно підвищення складності та створення комбінацій.

**Використана література:**

1.Бернет С., Пэйн С. Криптография. Офиц. Рук-во RSA Security. – 2002. – 384 с.

УДК 621.39.005 (043.2)

**К. А. Гайдук, І. Є. Терентьєва**
*Національний авіаційний університет, м. Київ*

## БЕЗДРОТОВА СЕНСОРНА МЕРЕЖА ЗАКЛАДУ

Бездротові сенсорні мережі являють собою системи моніторингу та управління, автоматизації та контролю, які активно розвиваються у сьогоденні. Стимуляцією розвитку та удосконалення бездротових сенсорних мереж послугував прогрес в бездротових технологіях зв'язку та мікроелектроніці. У роботі розглянуто які переваги людству надасть розробка і введення сенсорних мереж в усі сфери життя.

Бездротова сенсорна мережа (Wireless Sensor Network) - це самоорганізована, розподілена і стійка до відмови окремих елементів мережа безлічі датчиків (сенсорів) і обчислювально-комунікаційних пристроїв, об'єднаних між собою за допомогою радіоканалу. Область покриття подібної мережі може варіюватися від кількох метрів до декількох кілометрів.

Бездротові сенсорні мережі - це нова перспективна технологія, але вона тільки набуває свого поширення, тому всі пов'язані з нею проекти в основному знаходяться в стадії розробки. Тематика сенсорних бездротових мереж ще не достатньо вивчена, наразі є ряд невирішених проблем і обмежень, але переваги привертають компанії для розробки стандартів передачі інформації в сенсорних мережах. Технології бездротових сенсорних мереж широко використовуються у багатьох прикладних областях. Зазначимо основні області застосування даної технології:

- автоматизація будівель;
- контроль систем вентиляції, кондиціонування і освітлення;
- застосування у сферах медичної області;
- системи оборони і забезпечення безпеки;
- пожежна сигналізація;
- системи промислового моніторингу та управління;
- моніторинг стану сільськогосподарських угідь;

- управління енергопостачанням;

На сьогоднішній день існує багато технологій бездротового зв'язку, але ми виділимо найпоширеніші з них:

- стандарт Wi-Fi
- стандарт WiMAX
- стандарт Bluetooth
- стандарт HomeRF
- стандарт ZigBee

У дипломній роботі було проведено детальний аналіз особливостей найпоширеніших технологій бездротового зв'язку та приведено порівняльну характеристику, на основі якої виділено ZigBee, як оптимальний стандарт для сенсорної мережі.

ZigBee - технологія побудови бездротових мереж передачі даних значного числа вузлів, які взаємодіють один з одним невеликими обсягами інформації. Самоорганізація, захищеність, висока стійкість, низьке енергоспоживання роблять ZigBee-мережу відповідною основою для бездротової інфраструктури.

**Висновки:** з розвитком обчислювальної техніки і засобів зв'язку настала ера бездротових мереж. У роботі були наведені приклади основних областей застосування бездротових сенсорних мереж та методи їх використання, а також проведено аналіз та порівняння основних стандартів бездротового зв'язку, на основі якого виділено стандарт ZigBee.

**Використана література**

1. Міночкін А.І., Романюк В.А., Жук О.В. Перспективи розвитку сенсорних мереж // Зв‘язок. – 2008. – № 1. – С. 16 – 22.
2. Галкін П. В. Аналіз моделей та оптимізації збору інформації в бездротових сенсорних мережах // Східно – Європейський журнал передових технологій. – Харків, 2014. – Вип. 71. – С. 24–30

УДК 621.391.8 (043.2)

**Д.В.Гігіняк, О.П. Ткаліч**
*Національний авіаційний університет, м. Київ*

# МЕТОД ПІДВИЩЕННЯ ПОКАЗНИКІВ ЯКОСТІ ПЕРЕДАЧІ МЕДІАДАНИХ В МЕРЕЖАХ БЕЗДРОТОВОГО ЗВ'ЯЗКУ

Технології бездротових мереж розвиваються стрімкими темпами, витісняючи або частково замінюючи дротові мережі. Найбільшої популярності здобула бездротова технологія Wi-Fi. Точки доступу до цієї мережі встановлені майже у кожній квартирі та у громадських місцях. З ростом популярності технології одночасно виникають проблеми з якістю передачі медіаданих в цій мережі. На прикладі технології Wi-Fi було розглянуто та запропоновано методи підвищення якості передачі медіаданих в мережах бездротового зв'язку.

## 1. Огляд показників якості передавання мультимедійного трафіка.

Знання характеристик трафіка, створеного користувачами є незамінною умовою для грамотного проектування мереж зв'язку.

Питаннями поліпшення характеристик продуктивності і надійності мережі займаються методи забезпечення якості обслуговування (QoS). Розрахунки отримані при застосуванні методів QoS допомагають зменшити затримки передачі трафіку, уникнути втрат пакетів в періоди перевантаження мережі. Ці методи спрямовані на компенсацію негативних наслідків тимчасових перевантажень, що виникають в мережах з комутацією пакетів. У методах QoS використовуються різні алгоритми управління чергами, резервування, зворотній зв'язок, що дозволяють знизити негативний вплив черг до задовільного для користувача рівня.

## 2. Підвищення показників якості передачі даних в мережі Wi-Fi з використанням технології MIMO.

Технологія Wi-Fi описується сімейством стандартів IEEE 802.11, що налічує багато категорій. Найбільшу популярність здобули стандарти 802.11n та 802.11ac, завдячуючи своїм показникам передачі даних, що значно перевершують попередні стандарти.

Особливими ці стандарти робить технологія MIMO(Multiple Input Multiple Output), що за допомогою просторового кодування сигналу, дозволяє значно збільшити полосу пропускання каналу та покращити якість зв'язку у мережі у порівнянні з технологією SISO(Single Input Single Output). У поєднанні з технологією Beamforming, що в процесі роботи точки доступу аналізує сигнал від користувача та змінює діаграму направленості,тобто оптимізує своє випромінювання, можна досягти дуже високих показників якості передавання сигналу.

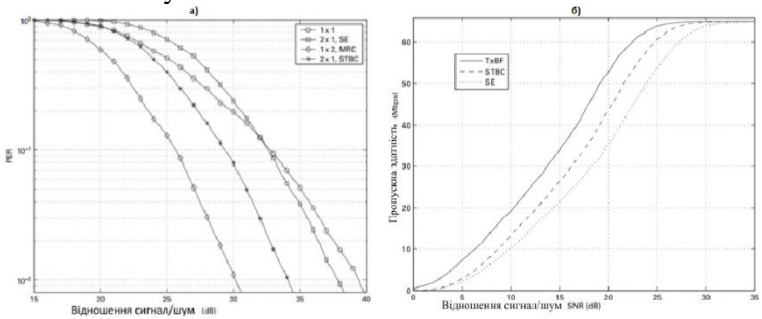



Рис 1. Порівняння MIMO та SISO(а), Wi-Fi з технологією Beamforming та без(б) .

**Висновки:** Таким чином були розглянуті методи підвищення показників якості передачі медіаданих у мережах бездротового зв'язку. Були запропоновані технології MIMO та Beamforming для збільшення полоси пропускання каналу та покращення якості зв'язку у мережі, порівняні методи передачі сигналу в системах MIMO (Wi-Fi) – мультиплексування(SDM), рознесення сигналу на прийом і передачу(CSD/SE), адаптивну передачу(Beamforming), а також продемонстрований приріст, котрий вони можуть дати.

## Використана література

1. «Програмне забезпечення для оцінювання пропускної здатності MIMO-Системи» Р.С. Одарченко, О.П. Ткаліч, С.М. Креденцар.

УДК 621.39.005 (043.2)

**Д. В. Гобош, І. Є. Терентьєва**
*Національний авіаційний університет, м. Київ*

## КОРПОРАТИВНА VOIP-МЕРЕЖА НА ПЛАТФОРМІ ASTERISK

VoIP (Voice over Internet Protocol) або IP-телефонія - це технологія, яка забезпечує передачу голосу в мережах з пакетною комутацією по протоколу IP, окремим випадком яких є мережі Інтернет, а також інші IP-мережі. Для зв'язку мережі Інтернет (IP - мережі) з телефонною мережею загального користування PSTN (Public Switched Telephone Network), яка відноситься до глобальних мереж з комутацією каналів, використовуються спеціальні аналогові VoIP-шлюзи.

Платформа Asterisk – програмна АТС, що надає користувачам унікальні можливості. Цей програмний продукт є сучасним масштабованим рішенням, сумісним практично з будь-яким обладнанням. IP-телефонія Asterisk поєднує в собі функції традиційної АТС з численними додатковими сервісами VoIP. Інтерактивне голосове меню, голосова пошта, факс-сервер, статистика дзвінків, запис розмов, онлайн статистика, відеозв'язок - все це можна легко встановити в офісі, необхідно лише замовити необхідне обладнання. Завдання об'єднання мережі філій і офісів в єдину комунікаційну інфраструктуру є першочерговим як для великих, так і для малих компаній. Безкоштовні дзвінки всередині мережі - одне з головних вимог до корпоративної телефонії, яку легко можна реалізувати за допомогою побудови IP-телефонії на базі IP-АТС Asterisk. Asterisk забезпечує достатню кількість протоколів для підтримки з'єднань між традиційними системами телефонії та ВП мережами включаючи H.323, Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), and Skinny Client Control Protocol (SCCP).

Відповідно до поставленої мети в роботі вирішені наступні завдання:

1. Розглянуто сучасні комунікаційні протоколи, технології і методи організації IP-телефонії.
2. Проаналізовано існуючу структуру телефонної мережі.
3. Розроблено схему телефонної мережі для офісу компанії.

4. Здійснено аналіз і вибір обладнання, яке буде здійснювати роботу мережі на основі IP-телефонії.

5. Розроблено інструкцію з налаштування програмної АТС для користувачів IP-телефонії.

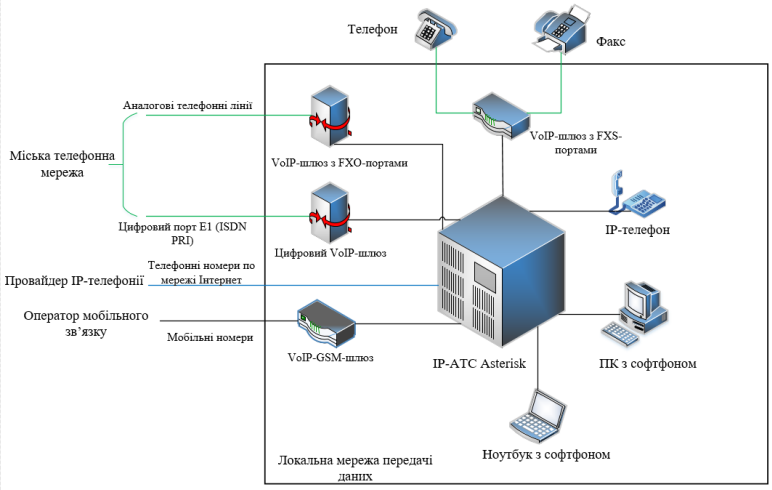



Рис. 1. Організація системи телефонного зв'язку на базі IP-АТС Asterisk

**Висновки:** Asterisk є дуже гнучким продуктом, що дозволяє налаштувати його практично під будь-які завдання компанії. Є дійсно революційним продуктом, що дозволяє не пропустити не одного дзвінка. В якості робочої станції (сервера) для Asterisk може використовуватися звичайний персональний комп'ютер, наявний у вас в офісі.

**Використана література**

1. Меггелен Дж., Мадсен Л., Сміт Дж. Asterisktм: Майбутнє телефонії, 2-е видання. – Пер. з англ. – СПб: Символ-Плюс, 2009. – 656 с., іл.

2. Call Центр. IP ТЕЛЕФОНИЯ ДЛЯ ОФИСА [Електронний ресурс] / Call Центр – Режим доступу до ресурсу: http://callcenters.by/wiki/voip-hardware/298-ip-telefoniya-dlya-ofisa.

УДК 004.75

**І.І. Голод, І.Є.Терентьєва**
*Національний авіаційний університет (м. Київ)*

## Проектування мережі нового покоління NGN

Останнім часом ринок телекомунікацій зростає швидкими темпами, в зв'язку з цим, звісно, поліпшується якість зв'язку, а також якість наданих послуг. Але також збільшується навантаження та вимоги до телекомунікаційних мереж.

Від самого початку, для окремих типів інформації були збудовані окремі мережі зв'язку. Наприклад, телефонна мережа, телеграфна мережа, мережі передачі даних та інші.

І з часом виникла ідея об'єднати окремі мережі зв'язку в одну – загальну. Першою спробою об'єднання в загальну мережу було створення концепції мереж ISDN. Але згодом, від ідеї формування глобальної мережі ISDN було вирішено відмовитись. Частково причинами відмови були: висока вартість ISDN-обладнання та швидкий розвиток IP-мереж.

Глобальна мережа NGN прийшла на зміну концепції ISDN. Мережа NGN, на відміну від ISDN, ґрунтується на мережі передачі даних на базі протоколу IP.

Особливістю NGN можна назвати необмежений набір наданих послуг.

Мережа нового покоління (NGN) - сучасна мережа з пакетною комутацією, що складається з безлічі вузлів доступу. NGN будується за технологією Gigabit Ethernet (GbE) і MPLS (Multiprotocol Label Switching) і забезпечує можливість підключення на швидкостях до 10 Гбіт / с, а також має всі можливості щодо забезпечення якості обслуговування (підтримка QoS, CoS) і надає необхідні можливості як для складання набору необхідних послуг, так і налаштування їх параметрів. На базі мережі нового покоління можливе надання найповнішого спектра послуг, від традиційної голосової телефонії, до повноцінного відеоконференцзв'язку. При цьому у мереж NGN спостерігається ще маса переваг, серед яких мінімізація витрат на експлуатацію та обслуговування мережі, що досягається за рахунок створення єдиного універсального мультисервісного середовища, мінімізація витрат на управління IT-інфраструктурою, можливість

побудови корпоративної мережі будь-яких масштабів, гнучке управління як власною мережею, так і наданими йому ресурсами оператора та можливість організації єдиного веб-інтерфейсу для управління послугами.

**Висновки**:

Мережі NGN, будучи результатом злиття мережі інтернет і телефонних мереж, об'єднують в собі їх кращі риси. Мережі NGN володіють наступними характеристиками:

- адаптованість для передачі трафіку будь-якого виду, що можна порівняти з адаптованістю мережі інтернет;
- гарантована якість голосового зв'язку і критично важливиі додатків передачі даних;
- низька вартість передачі даних в розрахунку на одиницю об'єму інформації наближається до вартості передачі даних в мережі інтернет.

**Список літератури**

1.Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 5-е издание. Учебник. – Санкт-Петербург, Питер, 2016.

2.Остров, Д.В. Информационная безопасность в рекомендациях, требованиях, стандартах. 2008.

УДК 621.391(043.2)

М.О. Гусак

# ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ПЕРСПЕКТИВНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НВЧ ДІАПАЗОНУ

У радіозв'язку, радіолокації, радіоастрономії, супутниковій радіонавігації, телекомунікаціях та інших областях науки та техніки велике значення мають X (8–12 ГГц), Ku (12–18 ГГц), K (18–26,5 ГГц) та Ka (26,5–40 ГГц) частотні діапазони за визначенням їх назв та смуг частот відповідно до IEEE.

Особливий характер поширення мають хвилі міліметрового діапазону (Ka діапазон) [1]. На деяких частотах цього діапазону відбувається резонансне поглинання енергії в парах води й у газах атмосфери, що показано на рис. 1, на якому наведені залежності загасання радіохвиль від частоти, причому суцільною лінією показано загасання в атмосфері, штриховою – додаткове згасання в дощі різної інтенсивності (1 – 16 мм/год; 2 – 4 мм/год; 3 – 1 мм/год; 4 – 0,25 мм/год), позначки $H_2O$ і $O_2$ показують максимуми поглинання хвиль у парах води та кисні атмосфери).

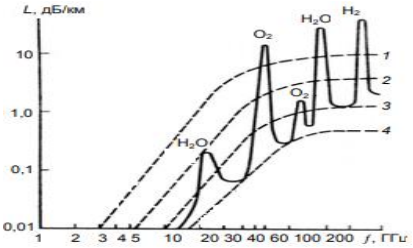



Рис. 1. Резонансне поглинання енергії в атмосфері.

Значення частот (довжин хвиль) вікон прозорості та піків поглинання в атмосфері наведено в табл.1.

Раціональним для перспективних телекомунікаційних систем НВЧ діапазону є використання вікон прозорості та складних сигнально-кодових конструкцій на фізичному рівні [2]. Це суттєво визначатиме енергетику (потужність передавача, чутливість приймача, затухання

тощо) ліній зв'язку у радіоканалах таких телекомунікаційних систем. Більше порівняно із сантиметровими хвилями поглинання міліметрових хвиль у гідрометеорах зменшує дальність радіозв'язку, тому для компенсації цього згасання виникає необхідність підвищувати енергетичний потенціал радіолінії.

Таблиця 1. Характер розповсюдження радіохвиль НВЧ

| Частота, довжина хвилі | Вікна прозорості | | | | Піки поглинання | | | |
|---|---|---|---|---|---|---|---|---|
| $f$, ГГц | 35 | 94 | 140 | 230 | 22 | 60 | 120 | 183 |
| λ, мм | 8,6 | 3,2 | 2,1 | 1,3 | 1,3 | 5,0 | 2,5 | 1,64 |

Показано, що енергетика НВЧ радіолінії може бути охарактеризована співвідношенням сигнал/шум:

$$\frac{P_{\text{С}}}{P_{\text{Ш}}} = P_{\text{ПРД}} G_{\text{ПРД}} G_{\text{ПРМ}} \big/ \left( L_{\Sigma} k T \Delta f \right),$$

де $k = 1{,}38 \cdot 10^{-23}$ Дж/К – сталаБольцмана; $\Delta f$ і $T$ – смуга пропускання та ефективна шумова температура приймальної системи (у точці, де визначається $\left(P_{\text{С}}/P_{\text{Ш}}\right)_{\text{ВХ}}$) відповідно.

Величина $P_{\text{ПРД}} G_{\text{ПРД}}$ є ефективною ізотропно випромінюваною потужністю (ЕІВП), а $G_{\text{ПРМ}}/T$ – добротністю приймальної системи, які мають важливу роль в енергетиці радіолінії. Для якісного зв'язку потрібно, щоб $\left(P_{\text{С}}/P_{\text{Ш}}\right)_{\text{ВХ}}$ було не меншим необхідного $\left(P_{\text{С}}/P_{\text{Ш}}\right)_{\text{ВХ min}}$.

Список літератури

1. M.O.Ajewole, L.B.Kolawole, and G.O.Ajayi, "Theoreticalstudyoftheeffectofdifferenttypesoftropicalrainfallonmicrowave and millimeter-wave propagation", *RadioScience*, vol. 34, No. 5, pp. 1103-1124, 1999.

2. Голубничий А.Г. Правила кодирования и структура обобщённых бинарных последовательностей Баркера/А.Г. Голубничий // Проблеми інформатизації та управління. – 2013. – № 4 (44). – С. 20–26.

Науковий керівник – к.т.н., доц. Голубничий О.Г.

УДК 621.39.005 (043.2)

**Т.С. Декало, Р.С. Одарченко, А.Г. Тараненко**
*Національний авіаційний університет, м. Київ*

# СИСТЕМИ МОНІТОРИНГУ ТА РЕЄСТРАЦІЇ БПЛА З ВИКОРИСТАННЯМ МОБІЛЬНИХ МЕРЕЖ

Головний обов'язок, який покладено на комплекси БПЛА, - проведення розвідки важкодоступних районів, в яких отримання інформації звичайними засобами, включаючи авіарозвідку, ускладнене або ж є небезпечним для здоров'я та навіть життя людей. Застосування комплексів БПЛА відкриває можливість оперативного і недорогого способу обстеження важкодоступних ділянок місцевості, періодичного спостереження заданих районів, використання в геодезичних роботах і у випадках надзвичайних ситуацій. Отримана інформація повинна в режимі реального часу передаватися на пункт управління для обробки і прийняття адекватних рішень, що є реальним завдяки засобам моніторингу. Безпілотний літальний апарат – літальний апарат, який літає та сідає без фізичної присутності пілота на його борту. Однак техніка все одно потребує контролю людини, отже, повністю уникнути використання людської робочої сили неможливо. За таких умов впровадження систем дистанційного моніторингу БПЛА стає актуальним.

Систему дистанційного моніторингу можна розглядати як сукупність віддалених апаратно-програмних модулів та центрального модуля. Віддалені модулі отримують дані від обладнання та відсилають центральному модулю, який зберігає та оброблює отриману інформацію. Саме тому проектування системи дистанційного моніторингу розділяють на чотири задачі: розробка програмного та апаратного забезпечення дистанційного модуля, вибір технології передачі даних, вибір протоколу передачі даних, розробка програмного забезпечення центрального модуля.

Технологія GSM дуже часто застосовується в системах контролю та моніторингу, і для цього існують дуже вагомі підстави. Дана технологія є однією з найпоширеніших технологій бездротового зв’язку в Україні, адже 98 відсотків площі країни мають GSM покриття, тому обладнання, оснащене GSM-модемом, може працювати практично в будь-якій місцевості. Також за її допомогою розробники

систем моніторингу матимуть різноманітні можливості передачі даних.

4G (LTE) — мобільний інтернет четвертого покоління. Його переваги в порівнянні з 3G, в першу чергу, в більш високій швидкості передачі даних, більш стабільному з'єднанні та в більш високій ємності мережі. До четвертого покоління відносяться технології, які дозволяють здійснювати передачу даних зі швидкість, яка перевищує 100 Мбіт/с. Прикладами технологій 4G є Wi-Fi і WiMax, які мають теоретичну границю швидкості передачі в 1 Гбіт/с. Саме завдяки цим перевагам даний стандарт більш підходить для моніторингу за БПЛА.

П'яте покоління мобільного зв'язку, що діє на основі стандартів телекомунікацій, наступних за існуючими стандартами 4G / IMT-Advanced. В даний час стандартів для розгортання 5G-мереж не існує. Передбачається, що 5G забезпечуватимуть більш високу пропускну здатність у порівнянні з технологіями 4G, що дозволить забезпечити більшу доступність широкосмугового мобільного зв'язку, а також використання режимів device-to-device, наднадійні масштабні системи комунікації між пристроями, більш короткий час затримки, менші витрати енергії батарейок, ніж у 4G-обладнання, що сприятливо позначиться на розвитку Інтернету речей.

Однак для моніторингу безпілотників більше підходить технологія LoRaWAN, оскільки вона має низьке енергоспоживання, що особливо важливо для тривалих польотів БПЛА. До переваг застосування даної технології також слід віднести високу дальність радіосигналу, до 30 км на відкритій місцевості і до 8 км в місті. Слід відмітити унікальну пропускну здатність радіосигналу, яка забезпечує стійкий зв'язок в важкодоступних місцях. Саме тому ми вважаємо, що використання даної технології є найбільш доцільним в даному випадку.

**Висновки.** Останніми роками напрям бездротових комп'ютерних мереж та віддаленого доступу зазнав бурхливого розвитку. Нами було розглянуто системи моніторингу за БПЛА та розроблений пристрій, який допоможе в вирішенні цієї задачі. На основі проведеного аналізу, було прийнято рішення, що для безпілонтиків найбільше підходить технологія LoRaWAN, яка дозволить здійснювати віддалений контроль і керування будь-якими технологічними процесами.

УДК 621.39.005 (043.2)

**Ю.В. Жуган, Д. І. Бахтіяров, Г.Ф. Конахович**
*Національний авіаційний університет, м. Київ*

## СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ОРГАНІВ УПРАВЛІННЯ ПІДПРИЄМСТВА

На сьогодні, зі збільшенням кількості інформації, що обробляється, збільшився ризик розкрадання та знищення інформації. В організаціях, що займаються обробкою даних, повинна бути розроблена система, яка задовольняє всі критерії безпеки для даної установи або організації, а також забезпечує цілісність, доступність та конфіденційність даних, їх повноту та актуальність. Від забезпечення інформаційної безпеки залежать системи телекомунікацій, банки, атомні станції, системи управління повітряним і наземним транспортом, а також системи обробки і зберігання секретної та конфіденційної інформації. Для нормального і безпечного функціонування цих систем необхідно підтримувати їх безпеку і цілісність. Архітектура системи управління виробництвом і технологія її функціонування дозволяє зловмисникові знаходити або спеціально створювати лазівки для прихованого доступу до інформації, причому різноманітність навіть відомих фактів злочинних дій дає достатні підстави припускати, що таких лазівок існує або може бути створено багато. Мета роботи полягає в аналізі існуючої інформаційної системи безпеки і розробці системи захисту найбільш вразливих ділянок корпоративної мережі для органів управління підприємством. Забезпечення захисту інформації в корпоративній мережі і захист баз даних, що знаходяться на сервері. Концепція безпеки корпоративної мережі системи управління підприємством розглянута на прикладі організації «BS-BUD», яка займається обробкою і проектуванням креслень для будівництва будівель в Україні.Інформація, що циркулює в рамках локальної мережі, є критично важливою. Локальна мережа дозволяє користувачам розділяти креслення будівель, програми і дані, що збільшує ризик. Отже, кожен з комп'ютерів, що входять в мережу, потребує надійного захисту. У сферу забезпечення безпеки потрапляють всі апаратні, програмні та інформаційні ресурси, що входять в корпоративну мережу «BS-BUD» (рис.1).

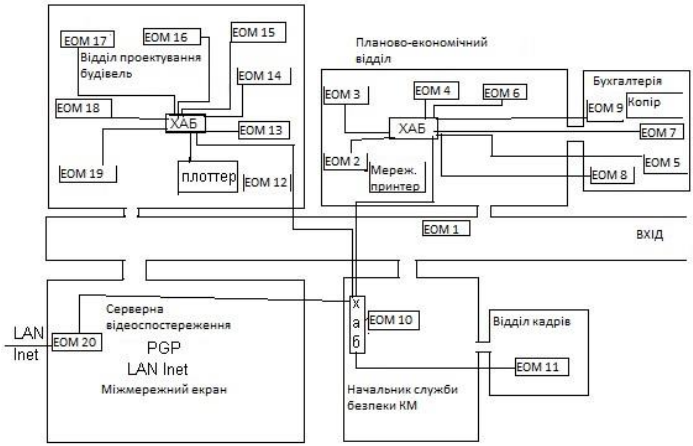



Рис.1 Схема корпоративної мережі органів управління підприємством «BS-BUD»

Для вирішення проблеми захисту інформації основними засобами, які використовують для створення механізмів захисту:

1. Технічні засоби - реалізуються у вигляді електричних, електромеханічних, електронних пристроїв.

2. Програмні засоби - програми, спеціально призначені для виконання функцій, пов'язаних із захистом інформації.

**Висновок.** Найближчим часом прогрес в області розвитку засобів обчислювальної техніки, програмного забезпечення і мережевих технологій дасть поштовх до розвитку засобів забезпечення безпеки, що потребують багато в чому переглянути існуючу наукову парадигму інформаційної безпеки.

На прикладі організації «BS-BUD», за рахунок аналізу існуючих інформаційних систем безпеки, були організовані засоби і способи захисту корпоративної мережі від несанкціонованого доступу до секретної інформації для установи, яка займається обробкою інформації.

УДК 656.13:658

**Д.М. Кириченко, О.П.Ткаліч, А.Г.Тараненко**
*Національний авіаційний університет, м. Київ*

# РАДІОПЛАНУВАННЯ ТА КОНТРОЛЬ ТРАФІКУ

Радіо-планування вимагає великих матеріальних, трудових і тимчасових витрат, а також ефективний розрахунок усіх фізичних параметрів. Для раціонального проведення планування необхідні висококваліфіковані фахівці, потужне програмне забезпечення з високоякісною апаратурою, актуальний картографічний матеріал.

## Опис моделей розповсюдження радіохвиль, їх характеристика

На підставі аналізу була вибрана «рекомендована модель розповсюдження радіохвиль», адже вона дозволяє її модифікувати, методом підбору постійних коефіцієнтів, досягається відповідність результатів теоретичних розрахунків і вимірювань для конкретної місцевості. Так само модель дозволяє вам незалежно коригувати кожен з основних своїх параметрів.

Враховуючи загасання радіохвиль були досліджені методи їх обчислення

## Моделювання радіо-планування

Провівши моделювання та порівняння моделей виробів досягнута максимальна якість сигналу, за допомогою обраного правильного частотного діапазону, спроектована мережа таким чином, що в ній було мінімум мертвих зон без покриття.

Було виявлено, що бажано робити вибір на користь більшої кількості точок доступу зі зниженою потужністю, ніж меншої кількості більш потужних приймачів сигналу Wi-Fi. Більш потужний передавач точки доступу створює більше покриття, але знижує ємність мережі і доступність для мобільних пристроїв. Прикладів таких помилок безліч: часто в офісі смартфон показує максимальний рівень сигналу Wi-Fi, але втрата пакетів призводить до постійних проблем з роботою в мережі.

Була використана технологія MIMO (Multiple Input Multiple Output) – це метод просторового кодування сигналу, який дозволяє збільшити смугу пропускання каналу, в якому передача даних і отримання даних здійснюються системами з декількох антен. Швидкість бездротового з'єднання з 54 Мбіт / сек зросла до 300 Мбіт / сек. На рис1. зображено модель каналу MIMO.

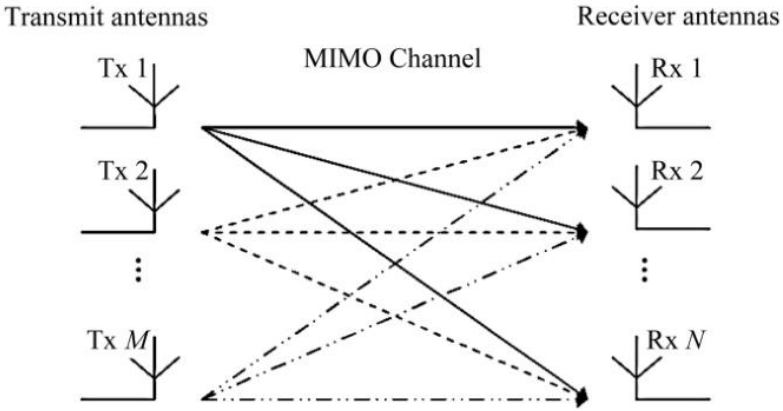



Рис.1 Модель каналу MIMO

**Висновки:** в наш час складно уявити життя без Інтернету. Глобальна мережа стала не від'ємною частиною роботи та відпочинку людини. Для оптимального користування Інтернетом потребується ефективне радіочастотне планування, що включає в себе якісне покриття, високошвидкісне з'єднання та обмін даними та максимальної пропускної здатності мережі.

**Використана література**

1. «Програмне забезпечення для оцінювання пропускної здатності MIMO-Системи» Р.С. Одарченко, О.П. Ткаліч, С.М. Креденцар

УДК 621.39.005 (043.2)

**С.Р. Кисельов, І.Є. Терентьева**
*Національний авіаційний університет, м. Київ*

# Корпоративна телекомунікаційна мережа компанії

Одним з головних напрямків побудови менеджменту підприємства і його удосконалення, стало масове використання новітніх телекомунікаційних систем.

Повна інтегрована автоматизація менеджменту підприємства припускає охоплення наступних інформаційно-управлінських процесів: зв'язок, збір, збереження і доступ до необхідної інформації, аналіз інформації, підготовка тексту, підтримка індивідуальної діяльності, програмування і рішення спеціальних задач.

До сучасних технічних засобів автоматизації інформаційно-управлінської діяльності відносяться:

- персональні комп'ютери, об'єднані в мережі;
- електронні друкарські машинки
- комунікаційні засоби, телефони;
- засоби для автоматизації архівації документів;
- електронна пошта;
- інтегровані мережі установ;

1. Для мережі кожного підрозділу корпорації виконати вручну розробку ескізів загального плану проекту та багаторівневого проекту (у вигляді малюнків для кожного плану: робочої групи, відділу (план

поверху), будівлі, кампуса) відповідно до вимог, передбачених у завданні на курсове проектування і індивідуальним варіантом вихідних даних.

2. Виконати побудову моделей багаторівневого проекту мережі корпорації з використанням інструментальних засобів програми NetCracker Proffesional.

3. Для кожної мережі:

Конкретизувати архітектурні особливості з урахуванням рольового розподіл комп'ютерів.

4. Здійснити вибір активного мережного обладнання (робочих станцій, серверів, комунікаційного обладнання) з використанням бази даних (БД) NetCracker Proffesional і виписати його основні характеристики (найменування, тип, виробник, кількість портів і т.п.).

5. Встановити на сервери додатки, передбачені індивідуальним завданням і визначити види трафіку, створюваного кожним з них.

6. Для міжмережевих телекомунікацій встановити трафики типу InterLAN traffic або Small InterLAN traffic відповідно.

Висновки. Дуже важливо виконати налаштування максимально надійно, адже на підприємстві дуже великий потік інформації щодня, тому інформацію треба швидко оброблювати, зберігати та використовувати надалі.

УДК 621.39.091 (075.8)

**М.М.Книженко, Р. С. Одарченко**
*Національний авіаційний університет, м. Київ*

# ТЕХНОЛОГІЯ ШИРОКОМОВНОГО ТЕЛЕБАЧЕННЯ ВИСОКОЇ РОЗДІЛЬНОЇ ЗДАТНОСТІ З ВИКОРИСТАННЯМ 5G.

Кількість підключених до всесвітньої павутини пристроїв і вимоги абонентів до швидкості мобільного доступу до інтернету збільшуються з кожним роком. Таким чином необхідним є поява мережі п'ятого покоління (5G). Виходячи з ключових можливостей 5G, які набагато перевищують змоги застарілих систем маємо можливість розробити рішення, які спрямовані на вирішення існуючих обмежень.

## 1. Концепт multicast телебачення в 5G

Впровадженням технологій широкомовного телебачення, використовуючи 5G досліджують в проекті 5G-Xcast, , який орієнтований на засоби передачі мовлення та багатокористувацького зв'язку для п'ятого покоління бездротових систем.

У проекті спочатку будуть проаналізовані вимоги до майбутніх медіа, включаючи Ultra-High-Definition Television (UHDTV), High Dynamic Range Imaging (HDR), High Frame Rates (HFR), широкий колірний простір. Потім буде визначено специфікації верхнього рівня для транспортних і прикладних шарів, необхідних для їх вирішення. Для забезпечення безперешкодного доступу до контенту та послуг у будь-який час, в будь-якому місці та з будь-якого пристрою.

## 2. Удосконалення архітектури 5G для впровадження broadcast.

Для того, щоб можливо було впровадити технології широкомовного телебачення необхідно використати Multi-Path Transfer Control Protocol, Quick UDP Internet Connection, Multilink Point-to-Point Protocol.

Multi-Path TCP - це набір розширень специфікації протоколу управління передачею, дозволяє використовувати протокол TCP для декількох шляхів для максимального використання ресурсів та збільшення надлишковості.

MP-QUIC – мережевий протокол транспортного рівня, був розроблений, щоб забезпечити захист безпеки разом зі зменшенням часу затримки зв'язку та транспорту і оцінкою пропускної здатності в кожному напрямку, щоб уникнути заторів.

MPPP – надає методи для поширення трафіку через кілька фізичних каналів. Дозволяє розширити пропускну здатність, забезпечує балансування навантаження.

**3. Розробка процедур взаємодії обладнання користувачів з мережею.**

Для забезпечення даних процедур, до вже існуючої архітектури додати додатковий функціонал:

1. Multi-Link в мережах різних рівнів
2. 5G-Xcast функції для різних рівнів
3. Multicast Coordination Entity (MCE)
4. Non-3GPP InterWorking Function (N3IWF)

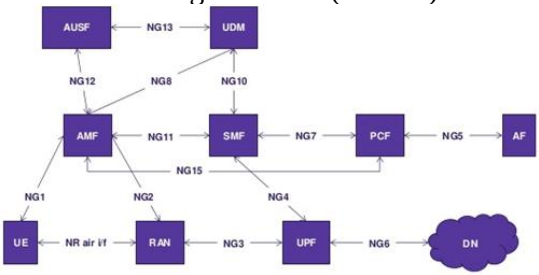



Рис.1 Архітектура 5G

**Висновки:** Таким чином було розроблено нову архітектуру 5G з використанням технологій Multi-Link, яка має ряд переваг і зможе забезпечити нові вимоги майбутніх медіа, в порівнянні з попередніми поколіннями.

**Використана література:**

1. 5G-Xcast [Електронний ресурс] – Режим доступу до ресурсу: http://5g-xcast.eu/author/5GXCast/.
2. Мультикаст [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/post/217585/.

УДК 004.052.44

**А.Ю. Коберник, А.Г. Тараненко**
*Національний авіаційний університет, м. Київ*

# СИСТЕМА МОНІТОРИНГУ МЕРЕЖІ БАЗОВИХ СТАНЦІЙ

Технологічний розвиток засобів передачі даних об'єктивно сприяє розвитку телекомунікаційної інфраструктури. Розробники систем цілком логічно зацікавлені в більшому охопленні абонентів, що вимагає розширення інфраструктури. Відповідно, виникає проблема поєднання декількох стандартів обладнання різної якості – від бюджетного до преміального рівня. Внаслідок постійного розширення телекомунікаційних мереж суб'єктивно збільшується кількість сегментів, з яких складаються мережі зв'язку. Ці та інші проблеми розвитку передбачають різні підходи і рішення.

## 1. Розрахунок параметрів стільникової мережі

Розрахунок стільникової мережі включає в себе визначення розмірності кластера; числа секторів обслуговування в одному стільнику; числа базових станцій, які необхідно встановити на території міста; радіус одного стільника; потужності передавача БС.[1] Для візуального відображення отриманих результатів розрахуємо гістограму залежності кількості базових станцій від розмірності кластера, при різних видах секторизації (рис. 1).

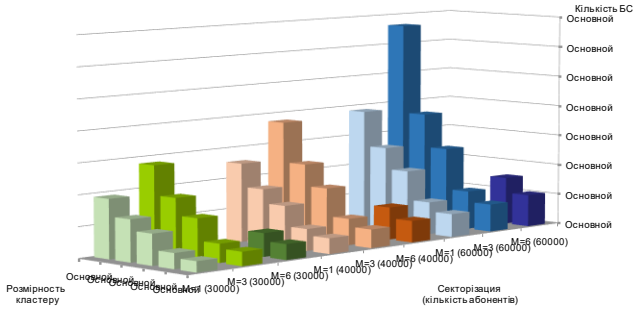



Рисунок 1. Залежність кількості базових станцій від розмірності кластера при різних видах секторизації

Аналізуючи результати, можна вважати, що при збільшенні кількості абонентів мережі, радіус стільника потрібно зменшувати, відповідно зростає потреба в додаткових базових станціях. Секторизація стільників призводить до підвищення числа базових станцій. Розмірність кластера доцільно зменшувати, що також помітно з рис.1.

**2. Дослідження системи забезпечення якості послуг мобільного оператора**

Оперативна діагностика і виявлення аварій є досить складним завданням, яке може бути вирішене тільки комплексом організаційно-технічних заходів.

OSS – Operations Support Systems - це набір програм, які допомагають постачальнику послуг зв'язку контролювати, аналізувати та управляти комп'ютерною мережею і забезпечувати задану якість послуг для своїх абонентів. Такі системи допомагають скоротити час на виявлення можливих проблем, які можуть привести до збоїв в роботі обладнання та інформаційних систем.[2]

**Висновки.** З метою зменшення витрат на моніторинг телекомунікаційної мережі доцільно використовувати єдину систему комплексного моніторингу телекомунікаційної мережі, яка дозволить об'єднати декілька різних мереж в одну, використавши при цьому єдиний базовий модуль збору інформації з різним програмним забезпеченням і з єдиним центром обробки інформації про стан мережі. OSS-рішення підвищують ефективність операційних процесів планування, будівництва і експлуатації мережі операторів зв'язку, а також дозволяють інженерам виконувати свою роботу швидше, ефективніше, якісніше.

**Використана література:**

1. Сукачов Е.О. Сотовые сети радиосвязи с подвижными объектами: учеб. пособ. /Сукачев Э.А. – [3-е изд., перераб. и дополн.]. – Одесса: ОНАС им. А.С. Попова, 2013. – 256 с.
2. Системи підтримки операційної діяльності – OSS /[електронний ресурс] - електронні текстові дані – режим доступу: //http://www.snt.ua/is/89988.ua.php (18.02.2018).

УДК 39.005 (043.2)

**Д.О. Кострица, Д.І. Бахтіяров, Р. Л. Богданович**
*Національний авіаційний університет, м. Київ*

# ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Проблема забезпечення захисту інформації є однією з найважливіших для сталого функціонування інформаційної структури підприємства, а також для мінімізації ризиків на підприємстві.

Для підвищення обізнаності користувачів в області ризиків, пов'язаних з інформаційними ресурсами було вирішено розробити політику інформаційної безпеки для підприємства ТОВ "InfoTech" України міста Києва.

**Концепція хорошої політики безпеки**

Ось кілька ключових моментів, що відрізняють правильно сформовану політику безпеки:

1. Вона повинна бути реалізована за допомогою процедур і засобів системного адміністрування, шляхом публікації правил допустимого використання мережевих ресурсів, або іншими методами, прийнятними для даної організації.

2. Вона повинна підтримуватися в межах, де це тільки можливо, автоматизованими засобами забезпечення безпеки, або санкціями до порушників, там, де застосування автоматизованих засобів захисту неможливо.

3. Вона повинна чітко визначати області і ступеня відповідальності користувачів, адміністраторів мереж, серверів та сервісів, а так само управлінського персоналу.

**Захист локальної мережі**

Існує кілька проблем, через які мережі можуть стати слабким місцем у захисті інформаційної системи. Класична проблема - атака класу «відмова в обслуговуванні». Цей тип атак полягає в приведенні мережі в стан, нездатності обмінюватися даними з авторизованими,

законними користувачами. Рішення багатьох з цих проблем в тому, щоб захистити пакети з маршрутною інформацією будь-яким чином: паролем, електронним підписом, шифруванням

Захист мережі необхідна і від можливості «сніффінга». Це можливість перехоплення пакетів локальної мережі з метою аналізу трафіку. Для захисту від сніффінга необхідно забезпечити захист всіх точок підключення до мережі, всього обладнання апаратних і поверхових розподільних шаф. Хорошу допомогу в цьому може надати сучасне мережеве обладнання. Наприклад, система безпеки BaySecure, вбудована в маршрутизатори і комутатори BayNetworks, дозволяє визначити, скільки разів мережевих карт комутатор повинен обробляти пакети, а з яких - ні.

Сервіс забезпечення безпеки не може і не повинен бути доступний ззовні мережі підприємства. Сервер, на якому розташовується сервіс безпеки, повинен надавати мінімальний набір інших сервісів. В ідеалі в мережі повинен бути виділений сервер безпеки.

**Висновок:**

В результаті виконання роботи було розроблено політику інформаційної безпеки. Саме політикою безпеки визначаються кроки і заходи, що вживаються на кожному рівні моделі. Саме Політика безпеки є тим стрижнем, навколо якого будується безпеку системи в цілому. Це важливо донести до розуміння як керівництва організації, так і рядових співробітників.

**Список використаної літератури:**

1. Сбиба В.Ю, Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб: Питер, 2008.
2. Костров, Д.В. Информационная безопасность в рекомендациях, требованиях, стандартах. 2008.
3. Доля А.В. Внутренние угрозы ИБ в телекоммуникациях. 2017.

УДК 621.39.005 (043.2)

**В. М. Кузьмич**
*Національний авіаційний університет, м. Київ*

# МОДЕЛЬ СИСТЕМИ “РОЗУМНИЙ ДІМ” НА БАЗІ RASPBERRY

Розумний дім - це сукупність елементів, які об'єднують усі електроприлади в домі єдиним розумом, що дозволяє вам керувати ними, як одним цілим. Недоліками всіх існуючих рішень є їх висока вартість і складність в налаштуванні, модернізації і розширенні. Тому проблема створення системи для управління будинком з можливістю легкого розширення та низькою собівартістю є актуальною.

## 1. Концептія “Розумного дому” в телекомунікаціях

“Розумна” будівля повинна бути спроектована так, що всі сервіси могли б інтегруватися один з одним з мінімальними витратами (з точки зору фінансів, часу і трудомісткості), а їх обслуговування було б організовано оптимальним чином.

Концепція інтелектуальної будівлі містить в собі такі положення:

- Створення інтегрованої системи управління будівлею - системи з можливістю забезпечення комплексної роботи всіх інженерних систем будівлі: освітлення, опалення, вентиляції, кондиціонування, водопостачання, контролю доступу та інших.
- Відсутність обслуговуючого персоналу будівлі і передача функцій контролю і прийняття рішень системі.
- Реалізація механізму негайного відключення і передачі управління людині будь-якою підсистемою інтелектуальної будівлі.
- Забезпечення коректної роботи окремих підсистем в разі відмови загальної керуючої системи або інших частин системи.
- Мінімізація вартості обслуговування і модернізації систем будівлі.

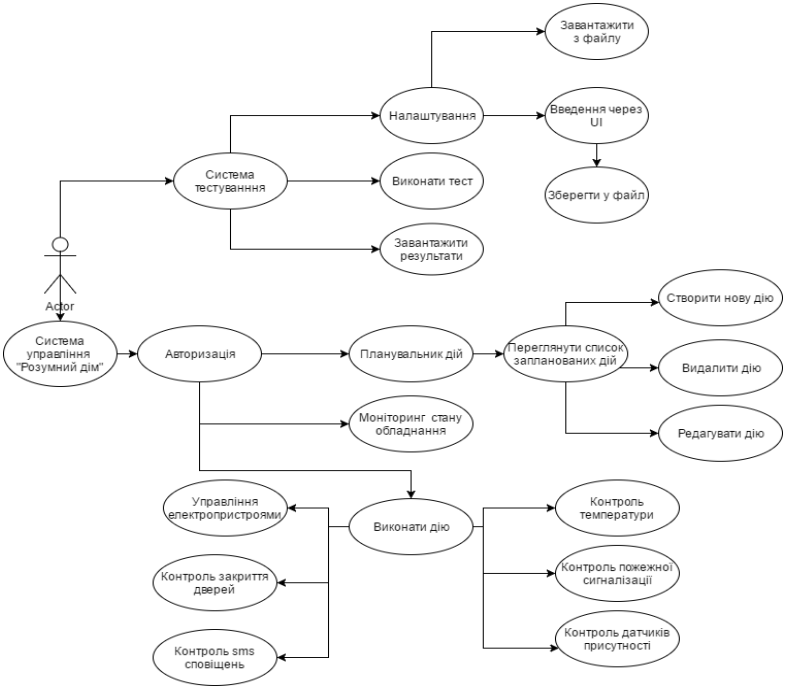
## 2. Покращення існуючих рішень моделей “Розумний дім” за допомогою комп’ютера Raspberry.

Raspberry Pi — одноплатний коп’ютер розміром з банківську картку, отримавший дуже широке використання і популярність.

Причиною успіху проекту можна назвати низьку ціну, відкритий характер розробки та орієнтацію на навчання та експерименти.

До Raspberry Pi ми можемо підключати датчики, за допомогою яких можливо отримувати зовнішні дані про стан середовища навколо системи. Таким чином, у нас є змога розширювати нашу систему.

## 3. Варіанти використання системи




**Висновки:** Таким чином було розроблено нову модель системи “Розумний дім”, яку можливо легко розширювати та яка має низьку собівартість, в порівнянні з попередніми аналогами.

**Використана література:**

1. Raspberry Pi [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Raspberry_Pi
2. Розумний дім [Електронний ресурс] – Режим доступу до ресурсу: http://sutem.com.ua/7smartbus.php.

**Науковий керівник:** к.т.н., доц. Курушкін В.Є.

УДК 621.39.091 (075.8)

**П.А.Купріянов, Г.Ф. Конахович, Д.І. Бахтіяров**
*Національний авіаційний університет, м. Київ*

# КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ.

Інформаційна безпека - це стан захищеності інформаційного середовища, захист інформації являє собою діяльність щодо запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається, тобто процес, спрямований на досягнення цього стану. Метою реалізації інформаційної безпеки будь-якого об'єкта є побудова системи забезпечення інформаційної безпеки даного об'єкту.

## Актуальність інформаційної безпеки сьогодення.

У зв'язку з масовим впровадженням комп'ютерів в усі сфери діяльності людини обсяг інформації, яка зберігається в електронному вигляді, виріс в тисячі разів, а з появою комп'ютерних мереж навіть відсутність фізичного доступу до комп'ютера не дає гарантії збереження інформаційних ресурсів. Все більше з'являється спеціалізованих засобів захисту інформації, які орієнтовані на рішення, як правило, тільки одного завдання забезпечення безпеки системи або в рідкісних випадках, деякого обмеженого набору завдань. Розширення застосування сучасних інформаційних технологій робить можливим поширення різних зловживань, пов'язаних з використанням обчислювальної техніки.

## Аналіз та модернізація інформаційно-обчислювальної мережі.

Моя мета модернізувати та розробити заходи комплексної системи захисту інформації локальної обчислювальної мережі ТОВ «Artline Computers» з детальною розробкою засобів захисту електронної пошти. Для реалізації необхідно провести модернізацію існуючої інформаційно-комунікаційної мережі організації. Для цього до складу мережі повинні бути введені два комп'ютери. Перший з встановленим ПЗ ViPNet Coordinator. Другий - з встановленим ПЗ ViPNet

Для повноцінного використання обраних засобів захисту електронної пошти була проведена модернізація існуючої локальної обчислювальної мережі організації. Розрахунок основних характеристик модернізованої локальної обчислювальної мережі, подвоєна затримка поширення сигналу і скорочення міжкадрової відстані показав її повну працездатність.

Для того щоб мережа працювала коректно, необхідно, щоб виконувалися три основні умови:

- кількість станцій в мережі не перевищує 1024;

- подвоєна затримка поширення сигналу (Path Delay Value, PDV) між двома найбільш віддаленими одна від одної станціями мережі не перевищує 575 бітових інтервалів;

- сумарна величина зменшення міжкадрового інтервалу при проходжен-ні всіх повторювачів (Path Variability Value, PVV) при проходженні послідовності кадрів через усі повторювачі не більше ніж на 49 бітових інтервалів (при відправці кадрів станція забезпечує початкову міжкадрову відстань в 96 бітових інтервалів).

**Результати виконаної роботи.**

Розрахунок основних характеристик модернізованої локальної обчислювальної мережі показав її повну працездатність. Сума всіх складових дає значення PDV, рівне 328,3. Так як значення PDV менше максимально допустимої величини 575, то ця мережа проходить за величиною максимально можливої затримки обороту сигналу. Величина зменшення міжкадрового інтервалу дорівнює 18,5, що менше граничного значення в 49 бітових інтервалів. В результаті змонтована мережа буде працювати коректно.

**Висновки:** В ході виконання дипломної роботи була здійснена розробка комплексної системи захисту інформаційно-комунікаційної мережі та, на її основі подальша модернізація локальної обчислювальної мережі фірми ТОВ «Artline Computers».

**Використана література:**

1. Заборовский В.С. Сетевые процессоры в современных системах защиты информации // Информационно-методический журнал «Защита информации. Конфидент». – № 2. – Март-апрель 2011 г.

2. Касперски Крис. Техника и философия хакерских атак. – М.: СОЛОН-Р. – 2009.

УДК 629.4.066

**А.В. Кутана, Р.С. Одарченко**
*Національний авіаційний університет, м. Київ*

## Доступ до мережі Інтернет на залізничному транспорті

У січні 2018 року було прийнято Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 роки. Однією з головних задач є усунення цифрового розриву, що являє собою неможливість доступу до мережі Інтернет та інших цифрових технологій на місці навчання, на роботі, вдома тощо. Цифровий розвиток передбачає виконання комплексу завдань, що позитивно вплинуть на економіку, бізнес, суспільство та життєдіяльність країни в цілому, тож забезпечення швидкісним доступом до Інтернет всіх груп населення є найголовнішою потребою та базою цифровізації. Подорожі та туризм також створюють ряд важливих причин для забезпечення доступом до мережі Інтернет - від телекомунікаційних мереж та спостереження за своїм розумним будинком до інструментів безготівкових розрахунків. Подорожувати та бути завжди підключеним до Інтернету - одна з головних ідей нового бачення туризму, тож забезпечення якісним швидкісним підключенням до Інтернет пасажирів транспорту, зокрема – залізничного, є пріоритетним завданням. Звертаючись до проблеми широкосмугового доступу на залізниці, необхідно чітко розуміти масштаби проблеми – протяжність колій, кількість напрямків та розклад руху пасажирських потягів, кількість рухомого складу (вагонів) та їх місткість. Пасажиропотік та забезпеченість пасажирів сучасними засобами зв'язку також вплине на технологію забезпечення доступу та підключення. Метою роботи є розробка вихідних даних для систем/и доступу до Інтернет для пасажирських потягів УкрЗалізниці, аналіз технологій доступу та вибір оптимального рішення виходячи зі зроблених припущень. УкрЗалізниця являє собою підприємство з розгалуженою структурою, в рамках якої діють регіональні технічні підрозділи, силами яких буде здійснюватися поточна експлуатація та обслуговування проектованих систем. Рішення складається з двох частин – абонентського доступу (абонент - система) та магістрального доступу (система – мережа інтернет). Задля забезпечення масовості доступу до Інтернет рішення для абонентської частини має забезпечувати доступ з будь-якого

термінального обладнання. Найбільш розповсюдженим стандартом доступу є технологія Wi-Fi. Забезпечення зворотньої сумісності та розмаїття абонентських терміналів вказує на необхідність використання обладнання стандарту 802.11 ac (b/g/n). Вибір технології магістрального доступу потребує дослідження типових технологій доступу до Інтернет:

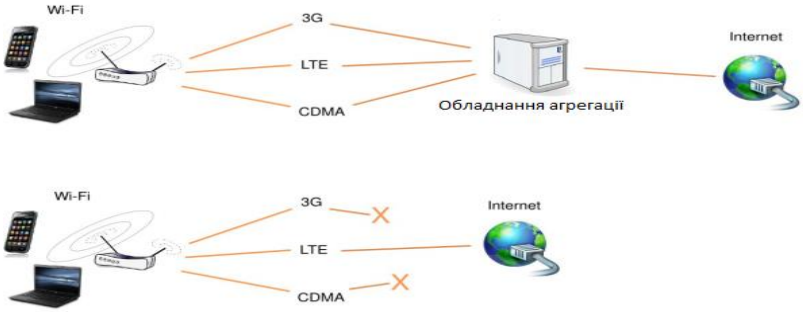



Рис.1 Порівняння рішення доступу з агрегації ап-лінку та без.

**Висновки**

Проведені дослідження, в т.ч. вимірювання швидкості, порівняння існуючого покриття мереж операторів для різних технологій зв'язку та вартість обладнання доступу, дозволили зробити висновки щодо доцільності використання агрегації IP-трафіку з забезпеченням безпеки та цілісності даних, що передаються, за допомогою технології VPN. При цьому буде досягнуто задані параметри системи доступу щодо кількості абонентів, що обслуговуються, та якості зв'язку.

**Використана література:**

1. Auvik [Електронний ресурс] – Режим доступу до ресурсу: https://www.auvik.com/media/blog/network-basics-link-aggregation/
2. IBM [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/support/knowledgecenter/en/ssw_aix_61/com.ibm.aix.networkcomm/etherchannel_overview.htm

УДК 004.52.014.52 (042.1)

**С.П. Максимов, В.В. Антонов**
*Національний авіаційний університет, м. Київ*

**Структурована кабельна мережа підприємства**

Структурована кабельна система (СКС) - закінчена сукупність кабелів зв'язку і комутаційного устаткування, що відповідає вимогам відповідних нормативних документів. Включає набір кабелів і комутаційних елементів, і методику їх спільного використання, що дозволяє створювати регулярні структури зв'язків у локальних мережах різного призначення

СКС є невід'ємною частиною будь-якого сучасного будинку або групи будинків. Під СКС розуміється кабельна система, принцип побудови якої відповідає таким основним ознакам: структуризації, універсальності й надмірності..

Структуризація дозволяє розбивку кабельної проводки та її аксесуарів на окремі частини або підсистеми, кожна з яких виконує строго певні функції та оснащена стандартним інтерфейсом для зв'язку з іншими підсистемами та мережним обладнанням.

Універсальність *СКС* проявляється у тому, що вона створюється на принципах відкритої архітектури із заданим стандартним набором основних технічних характеристик, призначених для забезпечення роботи будь-якої, а не конкретної мережної технології. Під час побудови СКС використовується узагальнений підхід без прив'язки до конкретного типу кабелю або комутаційного обладнання. Це дає можливість на будь-якому рівні однаково легко застосовувати як оптичні, так і електричні технології передачі сигналів.

Надмірність передбачає введення до складу СКС додаткових інформаційних розеток, кількість і місце розташування яких визначається площею й топологією приміщень, де працюють робітники. Застосування надмірності забезпечує можливість швидкої адаптації СКС під конкретні виробничі потреби.

У загальному випадку СКС відповідно до міжнародного стандарту ISO / IEC 11801 містить в собі три підсистеми:

Підсистема зовнішніх магістралей складається з зовнішніх магістральних кабелів між кросовою зовнішніх магістралей і кросової будівлі, комутаційного обладнання у КЗМ та КБ, до якого

приєднуються зовнішні магістральні кабелі та комутаційних шнурів і/або перемичок у КБ Підсистеми зовнішніх магістралей є основою для мережі зв'язку між компактно розташованими на одній території будинками. Ця підсистема має, як правило, кільцеву топологію..

Горизонтальна підсистема утворена внутрішніми горизонтальними кабелями між кросовими поверху й інформаційних розеток робочих місць, самими інформаційними розетками, комутаційним обладнанням у КП, до якого підключаються горизонтальні кабелі, і комутаційними шнурами, і/або перемичками в КЗМ.

Підсистема робочого місця забезпечує підключення мережевого обладнання на робочих місцях. Обладнання,що застосовується для її реалізації обладнання цілком і повністю залежить від конкретного додатка. Вона не є частиною СКС і виходить за рамки дії стандартів ISO / IEC 11801 та TIA / EIA-568-A.

Стандарти визначають структуру і параметри слабкострумових кабельних систем, які встановлюються в одному, декількох або комплексі будівель.

Фактичний вміст американського стандарту TIA / EIA-568-A практично еквівалентний європейському стандарту ISO / IEC 11801 Основні відмінності у форматі стандартів. Також посилання на TIA / EIA-568-A виконуються відповідно до міжнародних стандартів (МЕК та МСЕ-Т), тоді ISO / IEC 11801 використовує переважно європейські посилання (стандарти EN та ETSI). Однак ця різниця практично не впливає на фактичний зміст стандарту, оскільки більшість еталонних стандартів ідентичні і мають однакове числове позначення. Стандарт ISO / IEC 11801 включає в себе більше додатків, які є інформативними (не нормативними).

**Висновоки:** кабельна проводка в обов'язковому порядку є багато в чому унікальним проектом зі своїми індивідуальними і в багатьох випадках неповторними особливостями, самими несподіваними проблемами і, як показує практика, часто дуже оригінальними способами їх вирішення. У таких специфічних умовах різко зростають роль людського фактора взагалі і значення кваліфікації проектувальника зокрема.Тому правильно спроектована та збудована СКС є основою працездатності як маштабного підприємства,так і невеликого офісу.

УДК 004.056.5:004.8(043.5)

**К.О. Марук, О.Г.Голубничий**
*Національний авіаційний університет, м. Київ*

# ОБЕРНЕНІ ЗАДАЧІ ОЦІНЮВАННЯ ПАРАМЕТРІВ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ З ВИКОРИСТАННЯМ МЕТРИКИ L1

## Поняття коректно поставлених та некоректно поставлених задач

Серед математичних задач виділяють клас задач, процеси розв'язання яких нестійкі до мінімальних змін вихідних даних. Вони характеризуються тим, що мінімальні зміни даних можуть призвести до великих змін у розв'язанні. Задачі подібного типу належать до класу некоректно поставлених задач. Поняття коректної постановки задач було введено Ж.Адамаром. Згідно його трактувань, задача називається коректно поставленою на парі площин, якщо задовольняються умови:

1. для будь-якого елементу u є U існує розв'язок із площини;
2. розв'язок визначається однозначно;
3. задача стійка до змін на площинах U, F.

Задачі, які не задовольняють перерахованим умовам, називають некоректно поставленими.

## Методи числового розв'язку некоректно поставлених задач

Універсального методу розв'язку некоректно поставлених задач немає, тому в кожному конкретному випадку необхідно використовувати конкретний відомий нам метод як інструмент для знаходження розв'язку. Найбільш розповсюдженими методами в обчислювальній техніці вважаються метод підбору, метод регуляризації розв'язку операторних рівнянь та метод максимальної правдоподібності. Метод підбору заключається в тому, що для елементів z деякого раніше заданого підкласу можливих рішень M деякого лінійного простору F ($M \subset F$) вираховується оператор A.

Метод регуляризації полягає в знаходженні регуляризуючих операторів та визначенні параметра регуляризації по додатковій

інформації про задачу. Метод максимальної правдоподібності заключається в оцінюванні невідомого параметру шляхом максимізації функції правдоподібності.

**Ефективність застосування метрики L1 для оцінювання параметрів інформаційно-телекомунікаційної системи (на прикладі задачі корекції спотворень, що виникають у ІТКС дистанційного зондування земної поверхні)**

В процесі дистанційного зондування земної поверхні отримуємо зображення зі спотвореннями, що виникають в результаті розкалібрування фотоелементів між собою.

Модель спотворень:

$$y_{r,c} = x_{r,c} * g_c\,, \quad r = \overline{1,R}, c = \overline{1,C}$$

Для визначення ефективності оцінювання параметрів при використанні метрики L1 користуються поняттям «показник ефективності». Показник ефективності – нормоване середньоквадратичне відхилення $\sigma$ значень оцінених коефіцієнтів $\widetilde{g_c}$ від значень реальних коефіцієнтів $\widehat{g_c}$:

$$\sigma = 100 * \sqrt{\frac{1}{C} * \sum_{c=1}^{C} (\frac{\tilde{g}_c - \hat{g}_c}{\widehat{g_c}})^2}\,, \quad \%$$

Використання L1 дозволяє підвищити ефективність(точність) оцінювання параметрів ММП на ≈ 30% у порівнянні з L2:

L1: $\sigma_{min} = 0.443\%$

L2: $\sigma_{min} = 0.628\%$

**Висновки:** Таким чином було визначено, що використання метрики L1 дозволяє підвищити ефективність (точність) оцінювання параметрів інформаційно-телекомунікаційних систем для розглянутого типу обернених задач оцінювання параметрів інформаційно-телекомунікаційних систем, що досягається за рахунок «коректнішого» одночасного врахування великих та малих значень відхилень у єдиному інтегральному показнику.

УДК 004.72.056.52 (043.2)

**О.С. Мензюк, Д.І. Бахтіяров, Г.Ф. Конахович**
*Національний авіаційний університет, м. Київ*

## Методи визначення вразливості комп'ютерної мережі підприємства

При побудові комп'ютерної мережі підприємства одним із ключових питань постає забезпечення інформаційної захищеності даної системи, адже витік конфіденційної корпоративної інформації може завдати значних збитків.

Для початку потрібно визначити шо ж таке безпека та можливі шляхи її досягнення. В цілому безпека являє собою шляхи досягнення якоїсь мети, можливість протистояти присутності реального ворога. Припустимо те, що в цьому випадку завжди існують «зловмисники», які хочуть переконатися, що у певного підприємства чи користувача мережі нічого не працює. Вони можуть намагатися викрасти ваші файли. Або ж спробувати видалити вміст вашого жорсткого диска. Вони хочуть переконатися, що у вас нічого не працює, ваш телефон не може вийти на зв'язок, і так далі. Так ось, безпечною є така система, яка дійсно може щось робити незалежно від того, що намагається зробити з нею зловмисник.

Розгляд складових інформаційної безпеки:

Policy-являє собою принципи, які повинна приводити у виконання ваша система, тобто її призначення.

Threat model-друга частина системи безпеки, основному це набір припущень про те, що собою являє злочинець або противник.

Mechanism-в основному це програмне або апаратне забезпечення або будь-яка частина системного дизайну, реалізації, яка буде намагатися переконатися, що наша система виконує своє призначення до тих пір, поки поведінка хакера відповідає моделі загроз.

Таким чином, кінцевий результат полягає в тому, що поки наша модель загроз залишається вірною, то нашій системі вдається виконувати своє призначення.

Для ефективної протидії різного виду загрозам їх варто ідентифікувати та аналізувати. Тому важливим кроком до нашої мети-забезпечення інформаційної безпеки є класифікація та порівняльний

аналіз загроз безпеці інформації і методів протидії, а також систем виявлення загроз на початковому етапі атаки.

Для досягнення поставленої мети вирішувалися наступні задачі:

-аналіз основних властивостей загроз.

-визначення результатів впливу загроз.

-системний аналіз методів захисту від загроз.

-дослідження систем виявлення вторгнень на початкових етапах загроз.

Також при побудові комп'ютерної мережі підприємства часто постає питання забезпечити не тільки дротовий, але й бездротовий зв'язок на території підприємства. Одним Із найпростіших та найдоступніших методів є використання бездротової мережі Wi-Fi. У даній роботі було проведено аналіз існуючих вразливостей бездротової мережі та методів захисту Wi-Fi. На основі цього аналізу буде обрано метод який найкраще підходить для корпоративної мережі.

Для корпоративних застосувань, з урахуванням проведеного аналізу на вразливість найкраще всього підходить WPA2 Enterprise. В ньому, 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. Хоч на сьогодні WPA2-Enterprise в поєднанні з сертифікатами безпеки забезпечує надійний захист корпоративних Wi-Fi-мереж, але лише при правильному налаштуванні і використанні. Зламати такий захист практично неможливо "з вулиці", тобто без фізичного доступу до авторизованих клієнтським пристроїв, проте, адміністратори мереж іноді допускають помилки, які залишають зловмисниками "лазівки" для проникнення в мережу.

**Висновки:** Тому на перше місце виходить підготовка високо кваліфікованих фахівців не тільки з проектування але й експлуатації комп’ютерних мереж а також ефективне використання існуючих технологій захисту даних. Тоді правильно побудована, та належним чином обслуговувана комп’ютерна мережа може стати непробивним бар'єром для зловмисників.

УДК 621.39

**В.В. Онойченко, В.П. Климчук**
*Національний авіаційний університет, м. Київ*

## МОДЕЛЬ МЕРЕЖІ IP-ТЕЛЕФОНІЇ ДЛЯ IT-ПІДПРИЄМСТВА

В даний час існує безліч різних програм, що дозволяють вести телефонні переговори через Інтернет або локальну мережу. Така можливість вже нікого не дивує, для цього потрібні лише комп'ютер, підключений до мережі, відповідна програма і мікрофон з навушниками. Звичайно, таке рішення явно не підходить для організації телефонії в серйозній фірмі (все ж подібні засоби носять скоріше розважальний характер), проте ідея передачі голосу через мережу передачі даних дуже приваблива, особливо якщо фірма має безліч офісів в різних містах. І в цьому випадку рано чи пізно виникає питання про впровадження IP-телефонії.

IP-телефонія, по суті, є способом організації телефонного зв'язку з використанням мережі передачі даних для передачі голосу. Переваги такої організації телефонного зв'язку очевидні, і головне з них - суттєве зниження витрат на дзвінки між офісами, розташованими в різних містах. Крім цього, даний підхід дозволяє ввести єдиний номерний план для всієї організації, коли не потрібно пам'ятати телефонні коди міст, в яких знаходяться філії компанії. Ну і звичайно, не варто забувати про впровадження додаткових сервісів. Для побудови мережі IP-телефонії для IT-підприємтва, я вирішив довіритись Asterisk.

Asterisk — заслужений лідер програмних рішень IP АТС, визнаний у всьому світі. За багато років розвитку цієї платформи тільки ледачий конкурент зі своїм платним рішенням IP-телефонії не взявся поливати відвертою неправдою можливості Asterisk IP PBX, розхвалюючи свій продукт. На нашому ринку найбільш активні розповсюджувачі неправдивої інформації про Asterisk — це локальні представники розробників Oktell і 3CX, їхні дистриб'ютори та дилери. Звичайно, їх можна зрозуміти: у них є мета заробити більше грошей на різниці у вартості ліцензій для кінцевого споживача. Коли ви берете в руки калькулятор, то всі описувані менеджером переваги їхнього продукту виливаються в кругленьку суму навіть для маленької компанії з кількістю працівників до 10 осіб.

Основні можливості, які мають цінність для бізнесу, реалізовані в усіх продуктах. Тільки в Asterisk вас ніхто не обмежує — ні кількістю внутрішніх номерів, ні зовнішніми лініями зв'язку, ні кількістю одночасних розмов, ні зобов'язанням купувати додатково ліцензію на Windows — як для сервера PBX, так і для робочих станцій співробітників, оскільки програми операторів Oktell і 3CX «заточені» під Windows — без альтернатив для інших ОС. Для зв'язування регіональних офісів потрібно буде купити комплект ліцензій і для другого, третього і так далі офісів. Якщо захочете поставити в якомусь офісі Asterisk і звернетеся за консультаціями до представників Oktell або 3CX — ви можете отримати відмову в наданні будь-якої підтримки, хоча ціна питання може зрушити переговори з мертвої точки. Інформація про Asterisk настільки поширена і легко доступна в Інтернеті, що будь здатний технічний фахівець розбереться в підтримці системи Asterisk і знайде відповідь на ту чи іншу задачу. Для зручності адміністрування є багато веб-платформ, розроблених для Asterisk, і особливо розвинена — FreePBX. Це безкоштовний продукт, що володіє можливостями платних контакт-центрів. До нього є і платні модулі — питання смаку, необхідності та інших факторів, які важливі для вирішення саме ваших завдань.

**Висновок:** через простоту налаштовування та отримання всіх необхідних можливостей які необхідні будуть для IT-підприємства я буду використовувати Asterisk для побудови моделі мережі IP-телефонії, так як це не буде потребувати зайвих коштів.

УДК 621.396.49

**К. Л. Патрикей, В. П. Климчук**
*Національний авіаційний університет, м. Київ*

## УДОСКОНАЛЕНА СИСТЕМА РАДІОЗВ'ЯЗКУ ЗА ТЕХНОЛОГІЄЮ EME

Починаючи з першої половини XX століття і до сьогодні супутникові системи зв'язку характеризуються швидкими темпами розвитку, їх дослідженням та удосконаленням займаються найвидатніші науковці світу. Такі темпи розвитку пояснюються численними достоїнствами, які роблять супутниковий зв'язок унікальним і ефективнішим засобом зв'язку. Проте за роки освоєння космічного простору на космічні орбіти було виведено тисячі космічних апаратів і після використання їх не повертають на Землю, тому що це економічно недоцільно. Тому в космічному просторі накопичилося багато космічного сміття, що є недопустимо. Україна є космічною державою, тому досить актуальним питанням, виходячи з даної теми, є пошук таких супутникових систем зв'язку, які будуть екологічно безпечними, як для України, так і для всієї планети.Методом порівняння було виявлено, що технологія EME (від англ. "Earth-Moon-Earth" – «Земля-Місяць-Земля) відповідає вимогам екологічної безпеки, наведених вище. Технологія заснована на ідеї використовувати Місяць – супутник Землі, в якості пасивного ретранслятора. Ця ідея виникла ще в 40-х роках XX століття та є актуальною сьогодні. Крім того вона є економічно вигідною та доступною в реалізації.В роботі було проаналізовано сучасні системи зв'язку, їх переваги й недоліки. Це дозволило наочно прослідкувати основні аспекти при побудові проекту розвитку технології EME в Україні та вибору способу передачі сигналу для ефективної передачі даних. Для реалізації даного виду радіозв'язку потрібна більш досконала апаратура, зокрема потужність передавача має досягати 500...1000 Вт., діаметр антени передавача має становити 4...10 м, крім того, антена повинна бути постійно орієнтована на Місяць, що вимагає застосування системи автоматичної орієнтації діаграми випромінювання антени. При реалізації технології враховуються такі технічні аспекти, як поляризація, ефект Фарадея, лібраційний федінг, ефект Допплера, шум неба (шумова температура), втрати на трасі,

деградація сигналу, схиляння (положення Місяця), ґрунт-ефект, фази Місяця, кращий час для роботи. Розробка структурної схеми передавача за технологією EME спирається на типову структурну систему радіозв'язку, але із суттєвими відмінностями. В якості способу передачі сигналу ми пропонуємо використовувати технологію ортогонального частотного мультиплексування (OFDM), з допомогою якої можна уникнути руйнівних інтермодуляційних завад.

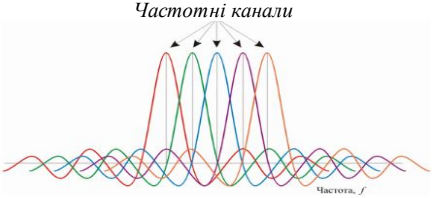



Рис. 1. Частотне розділення каналів з ортогональними несучими каналами

При OFDM послідовний цифровий потік перетворюється у велике число паралельних потоків (субпотоків), кожен з яких передається на окремій несучій. Технологія передбачає використання OFDM-модулятора.

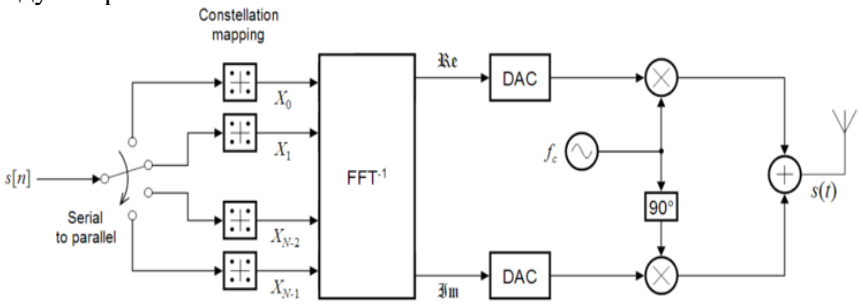



Рис. 2. OFDM-модулятор

Для його реалізації в передавальних пристроях використовується зворотне швидке перетворення Фур'є (IFFT), що переводить попередньо мультиплексований на N-каналів сигнал з тимчасового подання до частотне.

В цілому, розробка проекту розвитку технології EME в Україні є перспективним напрямком в галузі супутникового зв'язку, її реалізація допоможе вийти на новий, ефективніший рівень використання цього виду зв'язку не лише для вітчизняної, але і для зарубіжної науки.

УДК 621.39.005 (043.2)

**Педосюк В.В., Мачалін І.О.**
*Національний авіаційний університет, м. Київ*

# СИСТЕМИ САНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Уряди всіх держав завжди хочуть мати можливість контролювати людей і формувати за рахунок цього свою політику. В результаті тенденції до незаконних перехоплень інформації, з поваги до законів про права людей було введено термін законного перехоплення (Lawful Interception), який використовується для опису засобів і механізмів для правоохоронних органів та інших урядових установ, щоб мати технічну можливість і юридичний дозвіл на виконання законного перехоплення інформації у осіб, які, як підозрюється, зробили незаконні дії. Однак, навіть якщо таке законне перехоплення інформації може часто надати корисну інформацію про незаконні дії (наприклад, тероризм або викрадення людини), в історії були випадки, коли перехоплення також було використано для незаконного контролю осіб, які були або політичними противниками, або просто інакомислячі.

LI не є стабільним з точки зору архітектури, так як воно завжди повинне адаптуватися до нових способів і моделей комунікації. Для фіксованого та мобільного телефонного зв'язку перехоплення може бути реалізоване досить легко, оскільки зв'язок проходить через невелику кількість мереж, що належать державним або приватним компаніям на території цієї ж держави. Для цих компаній досить легко контролювати свою мережу і також створити умови для державного конролю, де органи влади можуть підключити свої пристрої моніторингу. У більшості випадків це навіть дуже зручно, оскільки ці мережі мають централізований контроль, і там, умовно кажучи, є всього кілька з'єднань з однієї мережі в іншу.

Проте для Інтернету і особливо для VoIP, перехоплення, як видається, є дуже слабкоконтрольованим з боку державних органів. Це відбувається через саму природу Інтернету. Інтернет є глобальною мережею, яка має багато різних маршрутів для відправки інформації на різні напрямки, а також, що важливіше, для глобальної мережі централізоване управління відсутнє.

Моніторинг наземних ліній зв'зку є добре відомомою процедурою для правоохоронних органів і спецслужб. Але держава стикається з головною проблемою перехоплень - відстеження та перехоплення кінцевого користувача, який використовує мобільний телефон і/або VoIP; оскільки обидві ці технології дозволяють користувачеві легко змінити своє фізичне місце розташування.

Місце розташування об'єкта є надзвичайно важливим для оперативних дій, адже терорист може переховуватись у великому натовпі людей чи аеропорту. Тому навіть використовуючи триангуляційні методи відстеження з базових станцій, є висока ймовірність похибки і велика площа, яку потрібно перевіряти, застосовуючи співробітників правоохорнних органів. В таких випадках є можливість використовувати гібридні системи перехоплення та відстеження з використанням геопозиціонування за технологією GPS. Це дозволило б підвищити точність відстеження з 200-300 метрів до 5-30 метрів, тобто більш, ніж в 10 разів.

**Висновки.** На фоні глобального розвитку телекомунікаційних технологій в світі стали частішими випадки тероризму особливо у місцях з дуже великим скупченням людей. Майже завжди телекомунікаційне обладнання так чи інакше залучається терористами для здійснення злочинів. Тому методи перехоплення інформації та відслідковування об'єкту є чи не найнагальнішими питаннями науковців в сфері державного контролю телекомунікацій. Але не зважаючи на підвищену потребу в заходах і методах перехоплення, будь-яка держава має забезпечувати своїм громадянам одне із основних прав людини - право на свободу та приватне життя.

УДК 621.39.005 (043.2)

**А. В. Романова, О. П. Ткаліч**
*Національний авіаційний університет, м. Київ*

## СЕНСОРНА МЕРЕЖА НА ПЛАТФОРМІ QIVICON

Готова платформа для «розумного будинку» дозволяє без зайвих зусиль натисканням на електронному девайсі регулювати все в будинку, або змінювати налаштування системи управління.

Під час проектування сенсорної мережі «розумного будинку» було вирішено поєднувати бездротові технології з проведеною в житло дротовою мережею. Однак в основі мережі лежить бездротова технологія, що дозволяє користувачеві економити кошти [1].

Існує безліч готових варіантів платформ, які лежать в основі «розумного будинку». Було проаналізовано декілька з готових найпопулярніших серед користувачів систем управління: HomeMatic, Open-ZWave, QIVICON та Розумний Дім 1-М. Головною характеристикою при виборі платформи була можливість використання обладнання від різних виробників та широкий спектр властивостей. Отже, спираючись на детальний аналіз кожної з систем, було вирішено проектувати сенсорну мережу на платформі QIVICON. Дана система дозволить побудувати з нуля таку мережу, яку тільки забажає її власник, бо QIVICON – це гнучкий засіб проектування, що робить ставку на відкрите програмне забезпечення, тобто можна комбінувати різноманітні види та типи датчиків від різних виробників.

На рис. 1 схематично зображено те, як QIVICON здійснює передачу даних користувача. Основою для включення в домашню мережу QIVICON є пристрій Home Base, який підключається до роутера і забезпечує зв'язок між компонентами розумного будинку. Налагодження та управління платформою проводиться через браузер на ПК або через додаток для смартфона. QIVICON використовує бездротові протоколи, призначені для Smart Home. Основні налаштування підтримують HomeMatic, HomeMatic IP, ZigBee Pro та включення DECT ULE. Домашня база QIVICON також включає в себе два USB-порти, що дозволяють використовувати додаткові протоколи. Всі з'єднання з домашньою базою QIVICON відбуваються

просто через стандартний маршрутизатор, як кабельним, так і бездротовим шляхом через Wi-Fi.

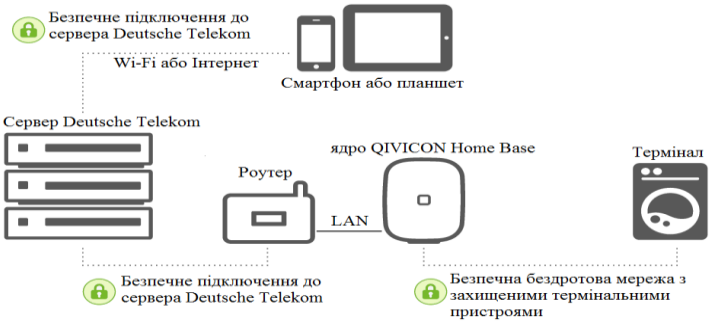



Рис. 1. Передача інформації в системі

На основі даної платформи розроблено варіант побудови сенсорної мережі «розумного будинку». Експериментальна архітектура сенсорної мережі складається з: управління світлом та електроживленням, клімат-контролю, системи безпеки, відеоспостереження та системи розваг. Кожна з цих систем поділяється на багато додаткових підсистем.

Завдяки тому, що QIVICON забезпечує безпечне збереження даних користувача на хмарних сервісах, проблем із перевантаженням центрального серверу немає. Це є великою перевагою даної платформи, завдяки зручності та економності використання. Отже, сенсорна мережа на платформі QIVICON працює без затримок, збоїв та легко підлаштовується під користувача, «спостерігаючи» за зміною налаштувань системи.

**Висновки:** проаналізувавши платформу QIVICON, можна впевнено стверджувати, що вона є безпечною та зручною для недосвідченого користувача та є оптимальним варіантом для створення «розумного будинку», адже дозволяє побудувати таку мережу, яку бажає користувач.

## Використана література

1. «Побудова сенсорної мережі аеропорту та її інтеграція з бездротовою мережею аеропорту стандарту 802.11» О.П. Ткаліч, Р.С. Одарченко, О.Ю. Устинов, Д.О. Колодинський.

УДК 004 (043.2)

**В.Ю. Савчук, В.В. Антонов, Д.І. Бахтіяров**
*Національний авіаційний університет, м. Київ*

## ЛОКАЛЬНА ОБЧИСЛЮВАЛЬНА МЕРЕЖА ПІДПРИЄМСТВА

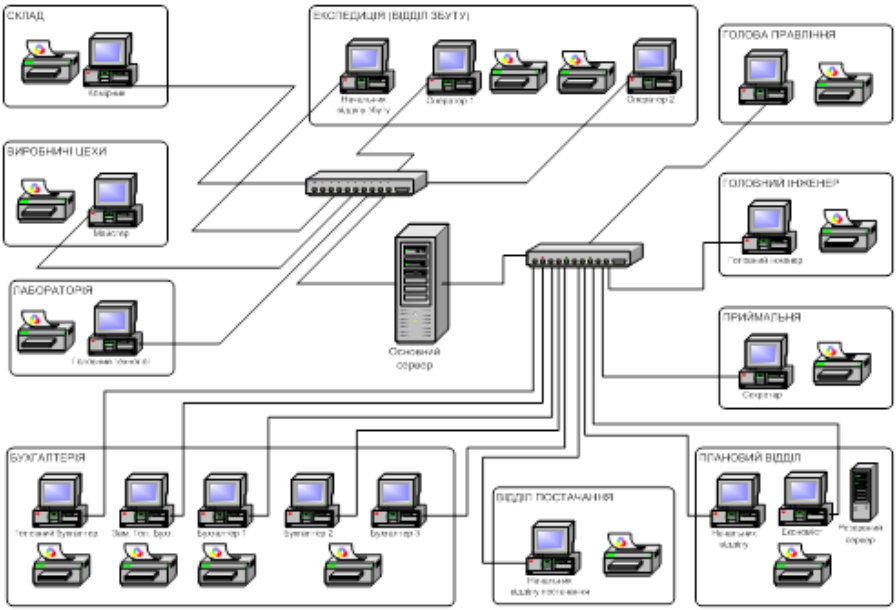
Реалізація проекту ЛОМ дозволить: скоротити паперовий документообіг всередині компанії; підвищити продуктивність праці; скоротити час на обробку інформації з використанням спеціалізованого програмного забезпечення; працювати з загальними пристроями: принтерами, факсами та іншою периферією; збільшити обсяг продажів готової продукції.

Розробка і впровадження даної системи забезпечить автоматизацію роботи компанії, дозволить підвищити точність і оперативність роботи з документацією, автоматизувати формування різних звітних документів, що значно зменшить тимчасові, а відповідно і матеріальні витрати. Використання мережевого програмного забезпечення «M.E.Doc» в ЛОМ підвищить точність і оперативність обліку важливої інформації, звільнить від виконання додаткових функцій, таких як багаторазове заповнення однотипних документів і виконання розрахунків для аналізу даних, опису і зберігання великого обсягу інформації на папері. Обробка інформації на ЕОМ здійснюється набагато легше і швидше, ніж вручну, що дозволяє економити час, який витрачає працівник на виконання даної операції.

Додатково встановлене програмне забезпечення дозволить здавати, не виходячи з офісу, бухгалтерську звітність до податкової інспекції в електронному вигляді, чого вимагає законодавство України.

Отримання необхідної інформації в мережі Інтернет, а також за допомогою електронної пошти дозволить прискорити виробничий процес, а, отже, збільшити обороти підприємства за рахунок зростання обсягів продажів продукції, що виготовляється.

Економічна ефективність обумовлюється скороченням трудовитрат на організацію роботи з ведення бухгалтерського обліку та отримання інформації щодо необхідних форм, а також зниженням цін на закупівлю продуктів харчування та харчової сировини за рахунок пошуку в мережі Інтернет нових, більш вигідних, постачальників.




Крім економії часу поліпшення показників якості роботи пов'язано зі своєчасним отриманням інформації, що зберігається в БД «M.E.Doc», підвищенням контролю правильності введення інформації, використання більш інформативних і наочних документів, скорочення рутинних обчислень при отриманні вихідних документів.

З усього вище перерахованого можна зробити висновок про доцільність, і швидше навіть необхідності розробки даного проекту.

**Література**

1.Олифер В.Г., Олифер Н.А. «Компьютерные сети. Принципы, тех-нологии, протоколы, 5-е изд» СПб, Питер-пресс, 2016

2.«Администрирование сети на основе Microsoft Windows 10. Учебный курс MCSE». Москва, Русская редакция, 2017

3.Кульгин М. «Технология корпоративных сетей. Энциклопедия». СПб, Питер, 2016

УДК 004.725.5

**А.В. Сілін, О.П. Ткаліч**
*Національний авіаційний університет, м. Київ*

## Інтеграція хмарних технологій в домашніх мережах. Система NAS

### 4. Що являє собою NAS та необхідність його впровадження в домашніх мережах

NAS-пристрої є повноцінними комп'ютерами або серверами, які виконують спеціалізовану задачу: мережеве зберігання даних і управління дисковими масивами. У зв’язку зі збільшенням обсягу данних та потреби у високій швидкості доступу до них необхідне впровадження рішень які зможуть посприяти задоволенню потреб користувачів.

### 5. Ефективність застосування мережевих сховищ

- Варіативність у виборі платформи та легкість масштабування
- Можливість тонкого налаштування необхідних послуг та функцій
- Багатофункціональність і багатозадачність.
- Централізований та авторизований доступ та синхронізація данних
- Низька ціна експлуатації
- Висока швидкість доступу до данних в локальних мережах, що використовують технології GbE та 10 GbE.
- Можливість встановлення додаткових плагінів

### 6. Схема побудови домашньої мережі з мережевим сховищем

Домашня мережа (Рис 1) складається з:

- Android TV приставок.
- Персональних комп’ютерів

- Мобільних пристроїв, що будуть з'єднуватися зі сховищем через WI-FI маршрутизатор
- Маршрутизатора, що сполучає елементи системи та дасть змогу підключитися до сховища з WAN.
- Коммутатор, що виступатиме у якості основного каналу зв'язку локальних пристроїв зі сховищем

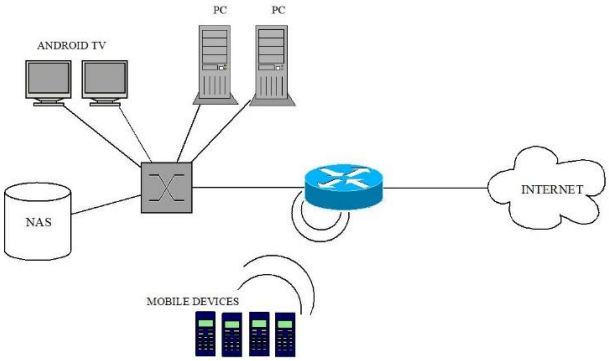



Рис.1 Домашня мережа з NAS сховищем

**Висновки:** В ході виконання дипломної роботи була визначена ефективність використання NAS сховищ в порівнянні з хмарними технологіями. Зроблено огляд всіх можливих апаратних платформ, файлових та операційних систем, Raid масивів і обрано найоптимальніші для застосування в моїй домашній мережі та проведена її модернізація. Працездатність ОС була перевірена у віртуальному середовищі. Система працювала справно та нарікань виявлено не було

**Список використаних джерел:**

1. https://habr.com/post/353012/
2. https://www.ixbt.com/storage/nas-howto-part2.shtml
3. https://doc.freenas.org/11/freenas.html

УДК 004.7(075.4)

**Д.М. Скиба, Р.С. Одарченко, А.Г. Тараненко**
*Національний авіаційний університет, м. Київ*

## КОМП'ЮТЕРНА МЕРЕЖА ДЛЯ ПОТРЕБ КАФЕДРИ ТКС

За допомогою емулятора Cisco Packet Tracer було реалізовано локальну мережу (LAN) для кафедри ТКС з метою покращення навчального процесу, а саме, для швидкого обміну інформацією, зберігання всіх необхідних навчальних матеріалів, та інформації щодо навчального процесу в єдиній базі даних, доступ до якої мають всі авторизовані користувачі (студенти)-тільки для перегляду та адміністратори (викладачі), які мають права повного доступу.

### Обладнання для реалізації мережі

Так як маємо невелику за площею мережу, яка містить не більше 15 комп'ютерів, використали комутатор 3 рівня (L3), який має можливість працювати на 3 рівні моделі OSI, та точку бездротового доступу для підключення до мережі з мобільних пристроїв (ноутбуки, смартфони і т.д.). Та завдяки витій парі з'єднали кінцеві пристрої та мережеве обладнання.

### Опис практичної частини

Було налаштовано комутатор використовуючи консольний кабель, так як це початкове налаштування пристрою. Завдяки програмі емуляції терміналу – Putty отримали доступ до налаштування, а саме до командного рядка, в якому було реалізовано:

- Віддалений доступ до комутатора, завдяки протоколу Telnet.
- DHCP та DNS сервера - для автоматичного отримання базового налаштування 2 (ip адреси, маски підмережі, шлюзу та доменного імені) підключеним до мережі ПК.
- NAT-трансляція локальних адрес (сірі ip) в глобальний (білий ip), тобто щоб пристрої мали доступ в інтернет.
- RADIUS server або AAA - для реалізації аутентифікації, авторизації та збору відомостей про використані ресурси, розроблений для передачі відомостей між центральною платформою і обладнанням.

- Розділили мережу на три віртуальні мережі (VLAN), окрему для серверів, адміністраторів та студентів, для зручності використання ACL (Access Control List), а саме, дозволили доступ до серверів тільки з мережі адміністраторів та створили фільтр від небажаних зовнішніх проникнень та заборонили доступ по Telnet з мережі інтернет.

Завдяки ОС Windows Server 2012 R2 налаштували FTP сервер– для зберігання інформації та завершили налаштування раніше згаданих DNS та AAA серверів.

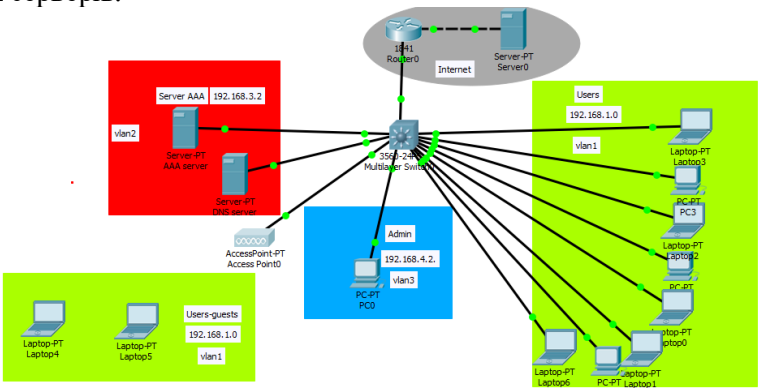



Рис.1. Схема локальної мережі

## Висновки

В результаті проведених налаштувань маємо повноцінну локальну мережу, здатну задовольнити навчальний процес та взаємодіяти з мережею інтернет.

## Використана література

1. Р.С. Одарченко, О.П. Ткаліч, О.О. Полігенько Експериментальні дослідження пропускної здатності мереж стандарту IEEE 802.11 n.

УДК 621.396.49 (043.2)

**В.С. Слюсаренко,О.Г. Голубничий**
*Національний авіаційний університет, м. Київ*

# ДОСЛІДЖЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМ ЗВ'ЯЗКУ З КОДОВИМ РОЗДІЛЕННЯМ КАНАЛІВ

У кодовому розділенні каналів (*CDMA − Code Division Multiple Access*) застосовують ортогональні коди фіксованої довжини, де кожному мобільному користувачу виділяється одна з послідовностей набору в якості коду для розширення спектру. При цьому взаємна кореляція між сигналами користувачів дорівнює нулю в рамках однієї базової станції. Розмежування абонентів відбувається за рахунок різної форми широкосмугових сигналів (кодів). Такі широкосмугові системи зв'язку називаються адресними системами зв'язку.

Функції Уолша, які можна отримати шляхом відображення рядків матриць Адамара, вважаються одними з найбільш ефективних для формування ортогональних послідовностей широкосмугових сигналів в системах *CDMA*. У роботі за допомогою комп'ютерного моделювання було проведено дослідження функціонування та завадостійкості чотирьохканальної системи *CDMA* (табл. 1, 2, рис. 1).

*Таблиця 1. Результати моделювання системи CDMA при використанні системи ортогональних сигналів на основі функцій Уолша*

| $h^2$ | BER1 (канал 1) | BER2 (канал 2) | BER3 (канал 3) | BER4 (канал 4) |
|---|---|---|---|---|
| 0,1 | $101{,}214\cdot10^{-3}$ | $107{,}286\cdot10^{-3}$ | $104{,}714\cdot10^{-3}$ | $100{,}429\cdot10^{-3}$ |
| 0,12 | $80{,}786\cdot10^{-3}$ | $86{,}786\cdot10^{-3}$ | $85{,}786\cdot10^{-3}$ | $80{,}857\cdot10^{-3}$ |
| 0,15 | $59{,}214\cdot10^{-3}$ | $63{,}214\cdot10^{-3}$ | $63{,}286\cdot10^{-3}$ | $58{,}714\cdot10^{-3}$ |
| 0,18 | $43{,}786\cdot10^{-3}$ | $46{,}286\cdot10^{-3}$ | $45{,}714\cdot10^{-3}$ | $43{,}786\cdot10^{-3}$ |

*Таблиця 2. Результати моделювання системи CDMA при використанні системи неортогональних сигналів*

| $h^2$ | BER1 (канал 1) | BER2 (канал 2) | BER3 (канал 3) | BER4 (канал 4) |
|---|---|---|---|---|
| 0,1 | $145{,}286\cdot10^{-3}$ | $139{,}857\cdot10^{-3}$ | $146{,}214\cdot10^{-3}$ | $153\cdot10^{-3}$ |
| 0,12 | $130{,}929\cdot10^{-3}$ | $124{,}571\cdot10^{-3}$ | $130{,}643\cdot10^{-3}$ | $140{,}071\cdot10^{-3}$ |
| 0,15 | $115{,}429\cdot10^{-3}$ | $105\cdot10^{-3}$ | $113{,}714\cdot10^{-3}$ | $123{,}929\cdot10^{-3}$ |

| | | | | |
|---|---|---|---|---|
| 0,18 | $101{,}357\cdot10^{-3}$ | $92{,}571\cdot10^{-3}$ | $103{,}071\cdot10^{-3}$ | $112{,}357\cdot10^{-3}$ |

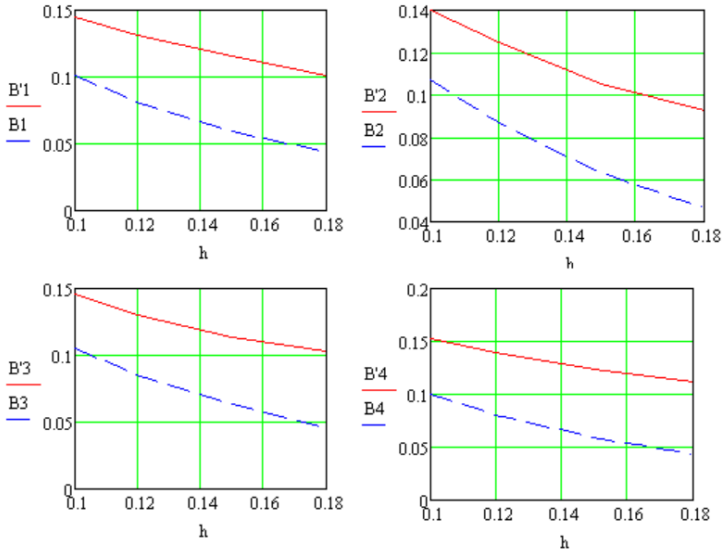



*Рис. 1. Завадостійкість CDMA при використанні систем ортогональних сигналів (штрихова лінія) та неортогональних сигналів (суцільна лінія).*

У табл. 1, 2 та на рис. 1 в якості показника завадостійкості використано імовірність бітової помилки при передаванні інформації (*BER – Bit Error Rate*), що залежить від співвідношення сигнал/шум $h^2$.

Показано, що використання ортогональних систем сигналів є більш ефективним у порівнянні з будь-якими іншими неортогональними системами сигналів. Перспективою подальших досліджень є аналіз та синтез систем широкосмугових сигнально-кодових конструкцій [1], зокрема для систем авіаційного зв'язку [2].

## Список літератури

1. Голубничий А.Г. Правила кодирования и структура обобщённых бинарных последовательностей Баркера / А.Г. Голубничий // Проблеми інформатизації та управління. – 2013. – № 4 (44). – С. 20–26.

2. Антонов В.В. Визначення параметрів розбірливості мови, що є прийнятними для авіаційних систем захищеного радіозв'язку / В.В. Антонов, О.Г. Голубничий // Захист інформації. – 2012. – Т. 14. – № 1 (54). – С. 99–103.

УДК 621.396.93 (043.2)

**Н.А. Слюсаренко, О.Г. Голубничий**
*Національний авіаційний університет, м. Київ*

## ДОСЛІДЖЕННЯ ШИРОКОСМУГОВИХ СИСТЕМ ЗВ'ЯЗКУ

Широкосмуговими (шумоподібними) сигналами (ШСС) називають такі сигнали, у яких добуток ширини спектру $\Delta F$ на тривалість $\Delta T$ набагато більший одиниці. ШСС успішно використовують в системах зв'язку рухомого і бездротового доступу, в супутниковому зв'язку та навігації. Основним принципом побудови систем з ШСС є те, що в таких системах ширина спектру ШСС завжди набагато більша за ширину спектру повідомлення, яке передається.

Основна ідея розширення спектру полягає в тому, щоб розподілити інформаційний сигнал по широкій смузі частот радіодіапазону, що призводить до збільшення частотної надлишковості системи зв'язку.

Перша розроблена схема розширеного спектру відома як метод стрибкоподібної зміни частоти *(FHSS − Frequency Hopping Spread Spectrum).* У системі зв'язку, що відповідає міжнародному стандарту для безпроводових комунікацій малого радіуса дії *Bluetooth* використовуються ШСС, які формуються за технологією *FHSS*. Метод розширення спектру за допомогою псевдовипадкових послідовностей *(DSSS − Direct Sequence Spread Spectrum)* є більш сучасним і перспективнішим методом розширення спектру. Він використовується в сімействі стандартів *IEEE* 802.11, а також в широкосмуговій системі стільникового зв'язку третього покоління *CDMA* та використовує для розширення спектру псевдовипадкові послідовності (ПВП). До ПВП висуваються вимоги щодо їх кореляційних функцій, оскільки вони визначають властивості систем з розширеним спектром. АКФ ПВП повинна мати вузьку основну та якомога менші бічні пелюстки [1].

У роботі за допомогою комп'ютерного моделювання безпроводової системи зв'язку стандарту *IEEE* 802.11 було проведено дослідження функціонування систем зв'язку з розширеним спектром. Для розширення спектру частот за методом *DSSS* використовується ПВП Баркера 1 1 1 -1 -1 -1 1 -1 1 -1 1 (рис. 1). Для порівняння

ефективності використання ПВП Баркера у системах з ШСС була використана послідовність 1 1 1 1 1 1 1 1 1 1 1 (рис. 2).

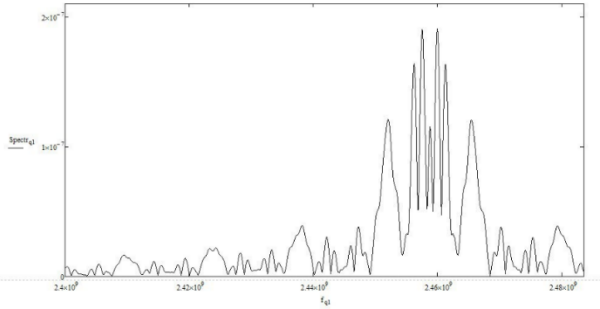


*Рис. 1. Спектр сигналу ШСС з використанням ПВП Баркера*

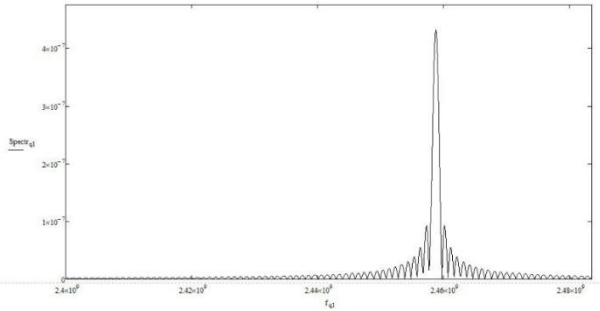


*Рис. 2. Спектр сигналу ШСС з використанням іншої послідовності*

Отже, використання кодів Баркера дозволяє досягти більшої ширини та рівномірності спектру ШСС, а з цим і кращих характеристик системи зв'язку (завадостійкість, прихованість тощо).

Перспективою подальших досліджень є аналіз та синтез систем ШСС, зокрема для систем авіаційного зв'язку [2] та БПЛА [1].

## Список літератури

1. A. G. Holubnychyi and G. F. Konakhovych, "Spread-spectrum control channels for UAV based on the generalized binary Barker sequences," in *Proc. IEEE Int. Conf. Act. Probl. Unmanned Air Veh. Dev. APUAVD*, 2013, pp. 99–103.

2. Антонов В.В. Визначення параметрів розбірливості мови, що є прийнятними для авіаційних систем захищеного радіозв'язку / В.В. Антонов, О.Г. Голубничий // Захист інформації. – 2012. – Т. 14. – № 1(54). – С. 99–103.

UDC 621.316.174 (043.2)

**Titenko K., Kozhokhina O.**
*National aviation university, Kyiv*

## ARCHITECTURE FEATURES OF AVIONICS DATA BUSES

Data bus is a subsystem that transfers data between computer components inside a computer or between computers. 'Bus' refers to a system that permits interconnection and data exchange between the devices in a complex system. With such a large number of avionic systems, a modern aircraft requires a considerable amount of cabling. Aircraft cabling amounts to a significant proportion of the unladen weight of an aircraft and so minimising the amount of cabling and wiring present is an important consideration in the design of modern aircraft, both civil and military.

**Traditional and new generation avionic and automotive data bus (CAN data bus )**

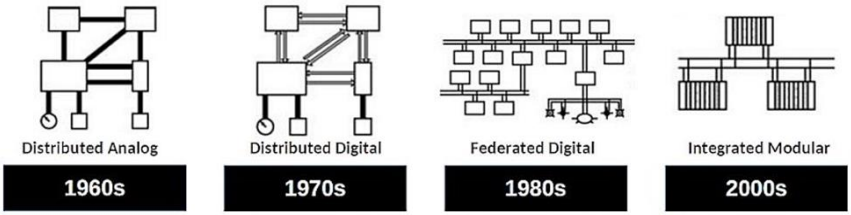



Figure.1 Evolution of avionics architectures.

CAN bus was installed for to improve safety and comfort, many electronic control units (ECU), such as anti-lock braking, engine management, traction control, air conditioning control, central door locking and powered seat and mirror controls, were added in automobiles. Controllers connected to the CAN bus can transmit data to the bus and receive data from the bus. If two or more terminals try to transmit at the same time, the bus arbitration logic connects the terminal with a higher-priority message. Architecture: multi-master bus, bitwise priority arbitration, event-triggered with no clock synchronization, multicast transmission with message filtering.

**Data bus for civil and military avionics**

There are various type of data bus in aviation. The two most common in the '90 were ARINC-429 for civil aviation and MIL-STD-1553 for military applications.

ARINC 429 architecture: serial point-to-point one-way protocol with only one transmitter on a twisted pair and one to twenty receivers.
The primary reason for moving away from ARINC-429 is that it is a single transmitter/multiple receiver architecture. This results in a large amount of physical wire. That adds weight and requires maintenance. A typical ARINC 429 data word on a real 429 bus is a 32-bit sequence (Fig. 2).

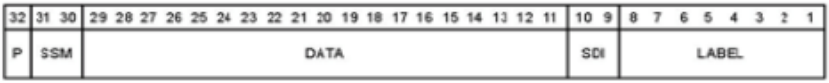



Figure.2 Typical structure of an ARINC-429 word

The first 8 bits, reading from right-to-left; the next two bits are often used to define the source/destination indicator; the next 19 bits are used for the actual data value; the next two bits define the sign/status matrix; the final bit is used for parity.

MIL-STD-1553 architecture: single master, the only device that can initiate communication; three functional modes of terminals allowed on the data bus: the bus controller, the bus monitor, and the remote terminal. MIL-STD-1553 is a powerful bus, but it is not as good a fit as many of the newer buses available in the commercial market.

**Conclusion:** This paper has described the conceptual design and implementation of a high-performance simulated avionics architecture that serves as the inter-process communications backbone.

**References:**

1. AIAA Paper 2003-5452, Presented at the AIAA Modelling and Simulation Technologies Conference, Austin, TX, August 2003
2. Aircraft Digital Electronic and Computer Systems: Principles, Operation and Maintenance.2007
3.https://pdfs.semanticscholar.org/49fb/b79cd9e8d513392b6b61771cbbb9b7bacbe5.pdf

УДК 687.39.002 (043.5)

**І.В. Третяк Д.М. Пробита**
*Національний авіаційний університет, м. Київ*

# ВИКОРИСТАННЯ GSM ШЛЮЗІВ ДЛЯ КОМПЛЕКСУ IP ТЕЛЕФОНІЇ.

IP-телефонія -це технологія, що дозволяє використовувати будь-яку IP-мережу як засіб організації та ведення телефонних розмов, передачі відеозображень та факсів у режимі реального часу. Однією з важливих проблем для комплексу телефонії є використання GSM шлюзів, як транків зв'язку, відмовитись від них не дозволяють соціально-економічні фактори, сам транк є відносно нестабільним, тому нами запропоновано вирішення данної проюлеми.

## Принципова схема комплексу телефонії

Комплекс телефонії (Рис 1)має складові:

- Прикінцеві термінали, на яких інстальовані софтфони.
- Маршрутизатори, що сполучають елементи системи.
- GSM шлюзи, що виступають у якості основного каналу зв'язку.
- Сервер Proxmox з системою віртуалізації. Містить у своєму складі ВМ CentOS з Asterisk та ВМ Windows з БД та ПЗ.

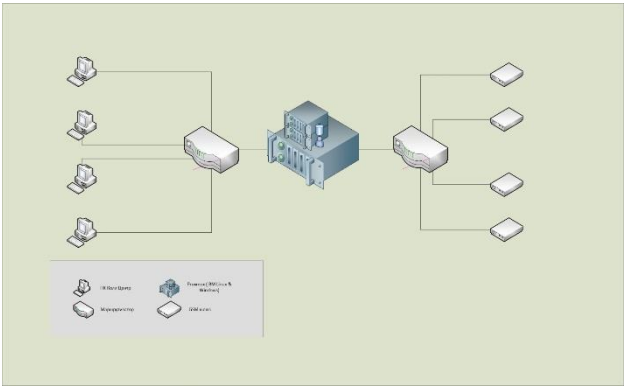


Рис.1 Комплекс телефонії

**Сценарії взаємодії.**

А) Оператор – клієнт.

Оператор ініціює виклик клієнту. У контексті [out_call_VIP] передбачено виклик скрипту, що дозволяє виконувати гнучке резервування каналів зв'язку, далі відбувається класичний сценарій виклику за контекстомю

Б) Клієнт – оператор.

Клієнт телефонує на номер, що ініціює CallBack. Потрапляючи в контекст [VIP_in] , де передбачений виклик скрипту, що дозволяє виконувати гнучке резервування каналів зв'язку, далі відбувається класичний сценарій CallBack.

**Вибір каналу зв`язку та виконання гнубкого резервування.**

Шлюзи надсилають інформацыю про стан своїх слотів до ПО (стан каналу, рівень сигналу, баланс, час напрацювання). Далі вираховується коефіцієнт надійності слоту. Таблиця з коефіцієнтами змінюється при кожній зміні критичних параметрів, або критичних значень другорядних параметрів. Таблиця надсилається в БД

В ході обслуговування системи, но основі статистичних даних, вираховується кількість абонентів, на яку потрібно резервувати в залежності від часу доби, дня року та кількості клієнтів. ПО отримує цю інформаціюз БД, після чого відправляє в БД значення, що використовується для резервування.

Скрипт використовує актуальні таблиці з БД, якщо телефонує VIP клієнт обирається канал з рекомендованих, якщо звичайний – всі крім рекомендованих.

**Висновки:** Таким чином ми маємо надійний канал зв'язку,

Не впливаючи на роботу мобільних операторів використавши перебір найбільш стабільних шлюзів та слотів.

**Використана література:**

1. Передача голосовых данных по сетям Cisco Frame Relay, ATM и IP - Стив Мак-Квери, Келли Мак-Грю, Стивен Фой
2. Call-центры и компьютерная телефония - Гольдштейн Б.С., Фрейнкман В.А.

УДК 004.738.2

**Д.В. Троцький, В.В. Антонов**
*Національний авіаційний університет, м. Київ*

# СИСТЕМА ОЦІНКИ ПОКАЗНИКІВ ЯКОСТІ IP ТЕЛЕФОНІЇ ПІДПРИЄМСТВА

Під IP-телефонією або мережевою телефонією розуміють технологію, що дозволяє використовувати будь-яку мережу з пакетною комутацією на базі протоколу IP (наприклад, мережу Інтернет) в якості засобу організації і ведення міжнародних, міжміських і місцевих телефонних розмов режимі реального часу.

Основними складовими якості IP-телефонії є:

а) якість мови,;

б) якість сигналізації;

Фактори, які впливають на якість IP-телефонії, можуть бути розділені на дві категорії:

а) фактори якості IP-мережі;

б) фактори якості шлюзу;

Для забезпечення якісної передачі мовних сигналів в IP-телефонії необхідна їхня наступна обробка:

а) Усунення всіх небажаних компонентів з вхідного аудіосигналу;

б) Придушення пауз в мові;

в) Стиснення голосових даних;

г) «Нарізування» стислих голосових даних на короткі сегменти рівної довжини, їх нумерація по порядку, додавання заголовків пакетів і передача;

д) Прийом і перевпорядкування пакетів в адаптивному «буфері ресинхронізації».

Вимоги до смуги пропускання описані в рекомендації ITU Y.1541. Затримка поширення з кінця в кінець при передачі мови не повинна

перевищувати 100 мс, а ймовірність перевищення затримки порога в 50 мс не повинна перевищувати 0,001.

При розрахунку необхідної продуктивності вузла доступу IP-телефонії розділимо всіх користувачів на три групи. Кількість пакетів, що передаються за секунду:

$$N_{\Sigma\_сек} = 142472, \text{ пакетів/сек}$$

При нормі затримки = 5 мс середній час обслуговування пакета (для розрахованої вище пропускної здатності) дорівнюватиме

$$\tau(0{,}005) = \frac{1}{142472 + \frac{1+0{,}2}{2 \cdot 0{,}005}} = 7{,}013 \times 10^{-6}$$

, секунд

При середньому значенні затримки в мережі доступу 5 мс коефіцієнт використання дорівнює:

$$\rho = 142472 \cdot 7{,}013 \times 10^{-6} = 0{,}999158$$

Визначимо параметри системи при її використанні на 50%:

$$\tau = \frac{0{,}5}{142472} = 3{,}509 \cdot 10^{-6}, \text{ секунд}$$

А затримка в мережі доступу:

$$\bar{t}_{ад} = \frac{3{,}509 \cdot 10^{-6} \cdot (1 + 0.2)}{2(1 - 142427 \cdot 3{,}509 \cdot 10^{-6})} = 4{,}211 \cdot 10^{-6}, \text{ секунд}$$

**Висновки:** після розрахунку показників якості системи IP-телефонії видно, що якість зв'язку можна оцінити такими характеристиками: рівень спотворення голосу, частота «зникнення» голосових пакетів, час затримки.

Затримки можна зменшити удосконалюючи телефонні сервери, розвиваючи мережі передачі даних і поліпшуючи апаратне забезпечення систем.

**Використана література**

1. IP – телефония. Мифы и реальность. //Компьютер-пресс. 1999, №4.
2. Новые системы связи. //Hard & Soft, 2000 рік., №5.

УДК 330.4:330.46

**Туруй О. Г., Конахович Г. Ф.**
*Національний авіаційний університет, м. Київ*

# ЗАХИСТ КОРПОРАТИВНОЇ МЕРЕЖІ ВИКОРИСТОВУЮЧИ ТЕХНОЛОГІЮ VPN.

VPN - це об'єднання локальних мереж або окремих машин, підключених до мережі загального користування, в єдину віртуальну (накладену) мережу, що забезпечує секретність і цілісність інформації, яка передається по ній. Суть даної технології полягає в тому, що при підключенні до VPN сервера за допомогою спеціального програмного забезпечення поверх загальнодоступної мережі у вже встановленому з'єднанні організується шифрований канал, що забезпечує високий рівень захисту переданої з цього каналу інформації за рахунок застосування спеціальних алгоритмів шифрування. Використання технології VPN необхідно там, де потрібен захист корпоративної мережі від дії вірусів, зловмисників, некомпетентних користувачів, а також від інших загроз, які є результатом помилок в конфігурації або адміністрування мережі.

Переваги VPN-технологій:

1. Простота використання. Це програмне, легко встановлюване (не вимагаюче практично ніяких настройок для клієнтського місця), інтегроване з мережним екраном рішення, що забезпечує безпеку як окремого комп'ютера в локальній мережі (або її фрагментів), так і локальної мережі в цілому.
2. Використання механізмів сповіщень і авторегістрації. При включенні в мережу VPN чергового мережного ресурсу механізми сповіщень і авторегістрації забезпечують моментальну настройку всіх учасників VPN, пов'язаних з новим ресурсом, на роботу з ним.
3. Відсутність будь-яких обмежень на кількість одночасних з'єднань по VPN. Рішення ідеально працює одночасно і в локальній мережі, і при взаємодії із зовнішніми ресурсами. Відсутні будь-які обмеження на кількість одночасних з'єднань по VPN. Забезпечується підтримка стандартних служб імен (DNS, WINS).
4. Мобільність. Мобільний користувач може працювати при будь-яких переміщеннях, навіть якщо у нього на комп'ютері розміщені серверні служби (за рахунок підтримки технології динамічного DNS).

5. Простота підключення партнерів або клієнтів до своїх ресурсів. При підключенні партнерів або клієнтів до своїх ресурсів: 2.86 a. організується точкове їх підключення до строго заданого ресурсу по заданих протоколах з криптографічною аутентифікацією трафіку, не залежною від IP- адреси джерела; b. за рахунок формування кожним модулем VPN унікальних віртуальних адрес не потрібне узгодження адрес взаємодіючих мереж; система дозволяє об'єднувати в VPN-вузли з однаковими IP-адресами.
6. Безперебійність роботи мережі VPN при наявності в мережах NAT-пристроїв. Присутні в мережах NAT-пристрої не порушують безперебійність роботи мережі VPN. Доступ до вузлів, що знаходяться за NAT-пристроями, можливий як шляхом настройки правил пропуску UDP-пакетів по заданому порту, так і за рахунок спеціальних механізмів підтримки автоматично створюваних на NAT-пристрої динамічних правил.
7. Забезпечення проходження між собою прямого трафіку при будь-яких конфігураціях. Модулі VPN забезпечують проходження між собою прямого трафіку при будь-яких конфігураціях, без перешифрування на проміжних вузлах.
8. Менша вартість. За наявності каскадів подвійне шифрування трафіку і, відповідно, його подвійна інкапсуляція не проводяться, що виключає витрати, пов'язані з цим.
9. Підвищена надійність і безпека функціонування інформаційних систем. Використовування симетричної ключової структури і наявність системи автоматичного розподілу ключів значно підвищують надійність і безпеку функціонування інформаційних систем в порівнянні з будь-якими іншими рішеннями VPN, що базуються на PKI-технологіях.
10. Можливість підтримки інфраструктури електронного цифрового підпису. В системі присутні всі необхідні рішення для підтримки інфраструктури електронного цифрового підпису, інтегровані з різними додатками.

**Використана література:**

1. Браун С. Виртуальные частные сети — №3(18), 2003, 503 с.
2. Запечников С.В., Милославская Н.Г., Толстой А.И. Основы построения виртуальных частных сетей — №10, 2003, 248 с.

УДК 004.451.25 (043.2)

**М.М. Федотов, О.П. Ткаліч, А.Г. Тараненко**
*Національний авіаційний університет, м. Київ*

# КОМПЬЮТЕРНА МЕРЕЖА НА ОСНОВІ WINDOWS SERVER 2016

На сьогодні набирає популярність малий та середній бізнес. Майже кожен з них потребує наявності робочих станцій, домену, корпоративної пошти або підключення до специфічних сервісів, наприклад 1С або MeDOC. Для цього потрібна платформа для розгортання на управління сервісами у домені.

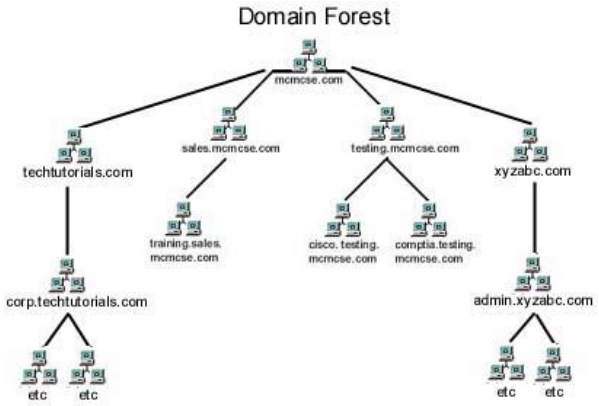
## 1. Вибір продукції компаній Microsoft

Родина ОС Windows одна з найбільш поширених у світі. На кінець 2017 доля ринку складала з 82%. Існує різноманіття програмного забезпечення для роботи вдома або в компанії. Наприклад, Microsoft Office, що використовуються майже усюди. Або для передачі даних використовується протокол SMB.

## 2. Використання служб у Windows Server 2016

- Information Services (IIS) – веб-сервер, що дозволяє розміщувати в Інтернеті сайти. Служба підтримує протоколи HTTP, HTTPS, FTP, POP3, SMTP. Для перевірки можна використовувати адресу 127.0.0.1.
- SMB – мережевий протокол, що знаходиться на 7 рівні моделі OSI, для віддаленого доступу до файлів та папок. Ця технологія використовує метод клієнт-сервер. Клієнтська частина являє собою зручний засіб для читання/запису файлів. А серверна частина використовується для файлової системи, пошти, принтерів і т.п..
- Active Directory – сервіс обслуговування каталогів у корпорацій Microsoft. На даний час являє взаємодію з багатьма службами авторизації, виконуючи роль об'єднання та інтеграцій. AD використовується для групових політик, наприклад, у корпоративний мережі.

- Microsoft Exchange Server – програмне забезпечення для реалізацій сервіса пошти, не використовуючи протоколи POP3 та SMTP. Exchange Server тісно взаємодіє з Active Directory, з AD відбувається синхронізація облікового записи для почтового сервісу.
- Домен-контролер – сервер керування облікових записів Active Directory. За допомогою цього сервера відбувається зберігання, керування та авторизації облікових записів, перевіряє справжність каталогів та інше.
- Windows PowerShell (PS) – варіація командного рядка з можливістю повністю замінити графічний інтерфейс (GUI). PS має власний каталог команд, який має назву командлети. У оболонці PS дозволяє створювати сценарії, у яких можна використовувати для виконання складних операцій.




**Висновки:** одна із найважливіших особливостей родини Windows Server – гнучкість у використанні та багатофункціональність операційних систем. Серверна ОС включає багато ролей та служб майже під будь-яку задачу.

**Використана література:**

1. «*Microsoft Windows Server 2016. Полное руководство*», *Рэнд Моримото*
2. *«Windows PowerShell 2.0. Справочник администратора», Станек Уильям Р.*

УДК 004.738.5

**Р.В. Федченко-Дубровін, І.О. Мачалін**
*Національний авіаційний університет, м. Київ*

# КОРПОРАТИВНА ЛОКАЛЬНА МЕРЕЖА З ВИКОРИСТАННЯМ ХМАРНИХ ТЕХНОЛОГІЙ

Корпоративна мережа - комунікаційна система, особливість якої полягає в тому, що всі співробітники компанії незалежно від розташування свого робочого місця отримують доступ до внутрішньої інформації та баз даних, можуть її обробляти і передавати один одному. Концепція такою мережі полягаю у наступному. Будь-яка організація - це сукупність взаємодіючих елементів, тобто підрозділів, кожен з яких може мати свою структуру. Елементи зв'язані між собою функціонально, тобто вони виконують окремі види робіт в рамках єдиного бізнес-процесу, а також інформаційно, обмінюючись документами, факсами, письмовими і усними розпорядженнями і так далі. При проектуванні завжди виникає необхідність закупівля, транспортування, розміщення, монтаж, налаштування різного роду обладнання. Крім цього, потрібно налаштувати безліч програмного забезпечення, відладити механізми взаємо праці працівників через ці програми. У процесі використання завжди потрібно вводити, з певною періодичністю, обслуговування всього обладнання, у результаті якого можлива заміна обладнання. Також, не слід забувати про актуальність версій програмного забезпечення, інакше кажучи, виникає потреба час від часу його оновлювати. Це все потребує багато часу та ще більше фінансових ресурсів.

Всі вище перераховані проблеми вирішує перехід на хмарні технології. Висловлюючись по простому, хмарні технології - це надання обчислювальних служб (сервери, бази даних, мережеве устаткування, програмне забезпечення, аналітика тощо) через інтернет. Це і є так звана хмара. Чому хмарні обчислення настільки популярні? Ось 4 поширені причини, чому організації переходять на хмарні обчислювальні служби:

1. Витрати. Хмарні технології дозволяють уникнути капітальних витрат на придбання обладнання та програмного забезпечення, налаштування і експлуатацію локальних центрів обробки даних, а це стійки з серверами, цілодобова подача електрики для

живлення і охолодження і кваліфіковані IT-фахівці для управління цією інфраструктурою. Ці витрати швидко зростають.

2. Масштабування. Переваги служб хмарних технологій включають можливість еластичного масштабування. В контексті хмарних служб – це означає виділення необхідного обсягу IT-ресурсів (наприклад, збільшення або зменшення обчислювальної потужності, обсягу сховища або пропускної здатності) тоді, коли це потрібно, і в відповідному географічному розташуванні.

3. Продуктивність. Для локальних центрів обробки даних зазвичай потрібні багато стійок і серверів, а також налагодження обладнання, оновлення програмного забезпечення та інша рутинна робота, яка забирає багато часу. Хмарні технології дозволяють уникнути багатьох з цих завдань, і ваші IT-фахівці зможуть витратити більше часу на виконання завдань, більш важливих для бізнесу.

4. Надійність. Хмарні обчислення роблять резервне копіювання даних, аварійне відновлення і безперервність бізнес-процесів більш легкими і менш витратними, так як дані можна копіювати на кількох дублюючих сайтах в мережі постачальника хмарних служб.

**Висновок:** абсолютно усю інфраструктуру можна перенести у хмару і разом з цим зекономити як час, так і фінансові ресурси. Нижче проілюстровані дві діаграми (рис. 1), де можна прослідкувати різницю в економічному плані (зліва – локальна інфраструктура, справа – хмара). Різниця витрат, протягом одного року, відрізняється в 5 разів.

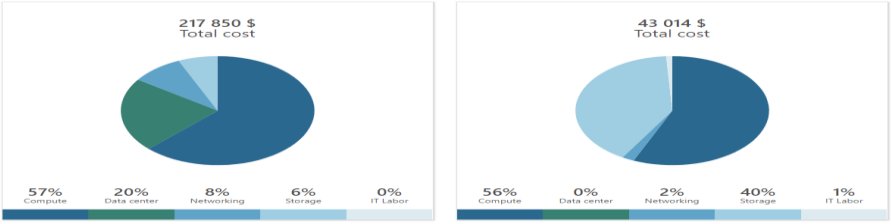



Рис. 1 Порівняльні діаграми

**Список використаних джерел**

1. Microsoft Azure, What is cloud computing? [Electronic resource] – https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/ – Title from the page.

УДК 621.39.005 (043.2)

**Т.В. Федюра, Р.С. Одарченко**
*Національний авіаційний університет, м. Київ*

## ВДОСКОНАЛЕННЯ СИСТЕМИ БЕЗПЕКИ МЕРЕЖ LTE

**Вступ.** Так як потреби мобільних користувачів ростуть стрімко, то поколінню 3G не завжди вдається їх задовольнити. Саме у цьому випадку доцільно використовувати LTE. Архітектура мереж LTE дуже відрізняється від схеми, використовуваної в існуючих мережах 3G. Ця відмінність породжує необхідність адаптувати і покращувати механізми забезпечення безпеки. Так як стандарт LTE є високошвидкісним, він збільшує швидкість поширення шкідливих програм. Загрозою також є атаки DoS (Denial of Service) на мережу. Додаткові сервіси також можуть бути уразливі для найрізноманітніших атак - як з Інтернету, так і з мобільної мережі.

Саме такі проблеми зумовили необхідність вдосконалення системи безпеки мереж LTE.

**Основна частина.** В даній доповіді запропонований варіант створення центру моніторингу кіберінцидентів в мережах LTE.

Основною задачею процесу системи управління є усунення інцидентів в гранично стислі терміни.

Однією з кращих систем управління кіберінцидентами серед присутніх на вітчизняному ринку є програмний продукт для обробки подій – netForensics nFX Open Security Platform. На рис. 1 зображено розроблену схему впровадження системи netForensics в мережу LTE. Основними модулями системи є сервер додатків (реалізує основну логіку обробки подій, представлення даних, взаємодії з користувачами); база даних nF DB (забезпечує зберігання інформації, що надходить до системи); модуль кореляції nF Engine (здійснює кореляцію зібраних даних); модуль автоматизації (здійснює автоматизацію процесів); агенти nF Agent (збирають інформацію безпосередньо з пристроїв). До складу системи також входять засоби щодо написання агентів збору даних з нестандартних систем захисту, засоби формалізації користувацьких правил кореляції і створення звітів. nF Agent впроваджуються програмно в Serving Gateway, PDN Gateway, MME, HSS, eNodeB, PCRF та UE. Агенти netForensics збирають повідомлення та сповіщення з керованих пристроїв. За

допомогою універсального агента можна легко розробити підтримку додаткових пристроїв за допомогою стандартної мови на базі XML. Ці агенти є інтерфейсами для розмежування пристроїв безпеки та програм, які нормалізують дані, надаючи кожній події/повідомленню ідентифікатор події netForensics. Це дозволяє nf Engine виконувати аналіз та змістовну кореляцію, а потім, коли необхідно, сповіщати. Всі ці дані розміщуються в базі даних Oracle. База даних подає як спеціальні звіти, так і заплановані звіти, які можна налаштувати через веб-інтерфейс.

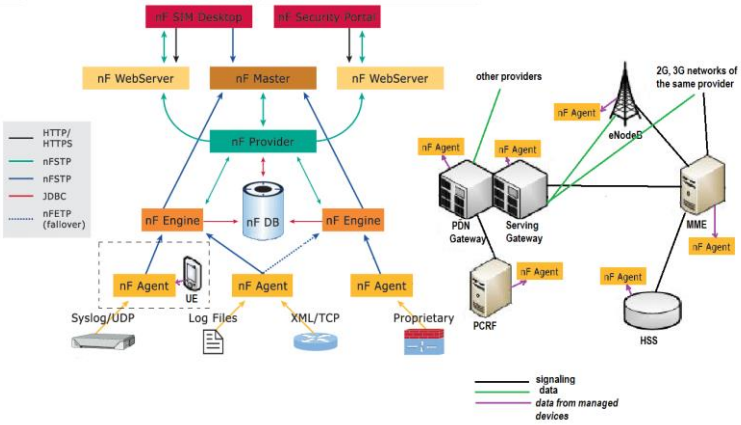



Рис. 1. - Система управління кіберінцидентами netForensics в мережі LTE

**Висновок.** Технологія LTE потребує проведення адаптації та покращення механізмів забезпечення безпеки внаслідок різних типів кіберінцидентів, які можуть з'явитись з наведених вище причин. В даній роботі запропонований варіант створення центру моніторингу кіберінцидентів в мережах LTE на основі netForensics nFX Open Security Platform. Всі елементи розробленої системи взаємодіють з мережею, проводять обробку подій, кореляцію зібраних даних. Основним елементом збору інформації є nF Agent, які впроваджуються програмно в Serving Gateway, PDN Gateway, MME, HSS, eNodeB, PCRF та UE. Агенти netForensics збирають повідомлення та сповіщення з керованих пристроїв.

УДК 621.391:004.056.53 (045)

**А.С. Чапліц, Р.С. Одарченко**
*Національний авіаційний університет, м. Київ*

## Система моніторингу якості обслуговування мережі при виникненні кіберінцидентів

На даний момент інформаційні системи обробляють величезний потік інформації, причому дана інформація повинна залишатися постійно доступною і конфіденційної. Потенційно висока продуктивність - це одне з основних переваг розподілених систем, до яких відносяться комп'ютерні мережі. Це властивість забезпечується принциповою, але, на жаль, не завжди практично реалізованої можливістю розподілу робіт між декількома комп'ютерами мережі.

Розподілена атака на відмову в обслуговуванні (DDoS-атаки) - це реальна і зростаюча загроза, з якою стикаються компанії в усьому світі. Цілями таких атак є - створення умов, при яких правомірні користувачі позбавляються можливості доступу до надаваних системою ресурсів (або цей доступ виявляється обмеженним).

Моніторинг комп'ютерної мережі - це безперервний процес спостереження за цифровою мережею з метою своєчасного виявлення в ній несправностей, помилок і зокрема DDos-атак з швидкою і адекватною реакцією на них. Моніторинг стану мережі здійснюється мережевим адміністратором за допомогою різних засобів оповіщення.

В роботі використовувався засіб моніторингу мережі - аналізатор протоколів (Protocolanalyzers). Він являє собою програмні або апаратно-програмні системи, які обмежуються лише функціями моніторингу і аналізу трафіку в мережах. Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються в мережах - зазвичай кілька десятків.

За допомогою аналізаторів мережі (сніферів) системні адміністратори і інженери мають можливість повністю спостерігати за процесом переданих даних в мережі і при наявності будь-яких несправностей, усувати їх при першій же діагностичної перевірки.

Сніфер є додатковою програмою, яка функціонує на канальному рівні за допомогою мережевого адаптера NIC (network interface card). Робота сніфера здійснюється в діогнастуючому режимі для усунення проблем всередині комп'ютерної мережі.

В процесі роботи пакетного сніффера, він намагається перехопити весь трафік проходить по дротах. Після перехоплення, він їх зберігає в окремий в форматі двійкового значення, і після застосування декодуючих програм може розшифрувати і проаналізувати пакети для отримання інформації в читаємому вигляді. Принцип роботи показано на рис. 1.

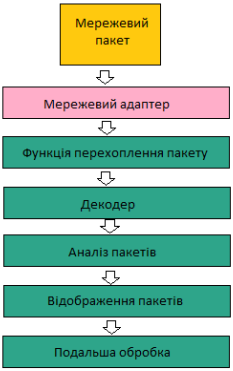



Рис. 1 Принцип роботи пакетного сніфера

Аналіз трафіку через сніфер дозволяє:

- виявити паразитний, вірусний і закільцований трафік, наявність якого збільшує завантаження мережевого обладнання та каналів зв'язку
- перехопити будь-який незашифрований (а часом і зашифрований) призначений для користувача трафік з метою отримання паролів і іншої інформації.
- локалізувати несправність мережі або помилку конфігурації мережевих агентів

**Висновки:** DDoS-атаки є реальною загрозою для функціонування будь-якої мережевої комп'ютерної системи. Хоча часто важко виявити і реагувати на розумно сплановані і підготовлені атаки. Проблема такого роду атак полягає в тому, що їх практично неможливо запобігти. Але за допомого сніфера при виникненні Ddos-атаки ми можемо зафіксувати різке збільшення трафіку на атакуючому вузлі мережі. Тож власник сервера може поставити апаратний або програмний механізм, здатний обмежити трафік та виділити шкідливий трафік, і тим самим захистити мережу від несанкціонованого доступу.

УДК 621.395.34

**В.О. Шевчук, В.В. Антонов**
*Національний авіаційний університет, м. Київ*

# СИСТЕМА АВТОМАТИЧНОГО ОБДЗВОНУ З ВИКОРИСТАННЯМ ПРОГРАМНОЇ АТС

На сьогоднішній день багато компаній середнього та малого бізнесу виказують інтерес до IP-телефонії. В першу чергу це пов'язано з можливістю зменшення витрат на телефонний зв'язок. При цьому IP-телефонія не потребує прокладення нових комунікацій, так як для неї використовуються вже існуючі підключення до мережі Інтернет. Це питання найбільш актуальне для компаній, чия робота пов'язана із постійними дзвінками великій кількості абонентів, наприклад для контакт-центрів, провайдерів телекомунікаційних послуг, інтернет-магазинів, банків, тощо.

Також часто в таких компаніях виникає потреба обдзвонити клієнтів стосовно різних питань: це може бути періодична задача (повідомлення про акції або нові послуги, заборгованість, реклама, пошук нових клієнтів) так і епізодична задача (якісь проблеми, технічні питання).

Всі ці потреби може задовольнити впровадження системи автоматичного обдзвону на базі програмної АТС. Така система має ряд беззаперечних переваг:

1. **Використання IP-телефонії**.

Це зменшить витрати на телефонний зв'язок всередині країни, а також дасть можливість міжнародним компаніям (наприклад аутсорсінговим контакт-центрам) обдзвонювати клієнтів за кордоном в рази дешевше.

2. **Автоматичний процесс обдзвону.**

Без використання даної системи зазвичай доводиться відволікати операторів кол-центру компанії від інших задач, що зменшує кількість успішних дзвонків через необхідність очікування з'єднання та вносить ризик помилок через людський фактор. Така ж система буде автоматично продзвонювати існуючий список номерів і передавати виклик оператору лише у разі якщо клієнт підняв слухавку

та відповів на дзвінок. Також є можливість відстежувати чи дзвінок прийняла справжня людина чи робот, не переводячи дзвінки з роботом до оператора, що дуже економить час.

3. **Можливість інтеграції у CRM-систему.**

Така система дозволить контролювати кількість і результативність викликів, не перевантажуючи операторів. Це можна реалізувати за допомогою API POST запитів або вбудованих звітів.

4. **Дешевизна впровадження.**

Впровадження такої системи обдзвону можливе з використанням не дуже дорогих комплектуючих для сервера, безкоштовної ОС CentOS, віртуальної АТС Asterisk, що також поширюється безкоштовно, та будь-яких софтфонів для операторів, наприклад Zoiper чи X-Lite.

Мінімальні характеристики серверу: 50GB HDD, 4 GB RAM, двох ядерний процесор.

5. **Можливість роботи у двох режимах.**

В даній системі обдзвону впроваджено два режими роботи: «стандартний» та «за групами». В «стандартному» всі оператори мають доступ до усього списку номерів та дзвінки розподіляться рівномірно на всіх. В режимі «за групами» всі оператори поділені на групи, кожна з яких отримує дзвінки лише від певного списку клієнтів.

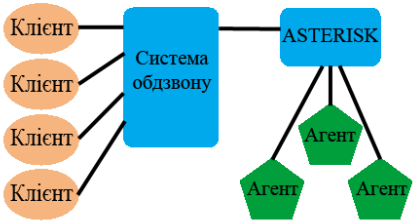



Рис. 1. Принцип роботи системи обдзвону на базі Asterisk

**Висновки:** в результаті проведеної роботи було розглянуто систему автоматичного обдзвону на базі програмної АТС Asterisk, переваги та можливості її використання. Впровадження системи у АТС call-центрів різних компаній може збільшити їх продуктивність від 100% до 300% в процесі обдзвону певного списку номерів при порівнянні із звичайним обдзвоном операторами.

УДК 006.3/.8 (043)

**Р.В. Шитлюк, В.О. Гнатюк**
*Національний авіаційний університет, м. Київ*

# ОГЛЯД СУЧАСНИХ ПІДХОДІВ ДО ФУНКЦІОНУВАННЯ ІТ-ПРОЦЕСІВ В ОРГАНІЗАЦІЯХ

Станом на сьогодні найдорожчим ресурсом в світі є інформація. Її цінність не обмежується записаними словами, числами чи зображеннями: ідеї, концепції та технології є прикладами нематеріальних форм інформації. Тому вимоги до організації систем, мереж, процесів та персоналу, який бере участь в їх функціонуванні, ростуть з кожним днем. Це пов'язано з ростом кількості ризиків та загроз – які виникають внаслідок використання наявних вразливостей у системах, процесах, мережах та персоналі.

Постійні зміни бізнес-процесів і систем, зовнішні зміни (наприклад, нові закони або регулятивні акти) та використання нових технологій (таких, як IoT) спричинюють ріст числа вразливостей та ризиків інформаційної безпеки (ІБ). Останнім часом все більше і більше організацій – як державних, так і приватних – висловлюють стурбованість станом інформаційної безпеки.

Так, згідно з міжнародним дослідженням компанії EY «Cybersecurity regained: preparing to face cyber attacks» 56% організацій стурбовані збільшенням впливу загроз на їхні стратегії та плани, 87% організацій у світі потребують збільшення бюджету на ІБ як мінімум на 50%, і працівники лише 12% організацій впевнені в тому, що зможуть розпізнати складну кібератаку.

Детальний аналіз даного опитування показує, що більшість організацій потребують не лише збільшення бюджету на ІТ та ІБ, а й створення умов для його ефективного використання.

Оскільки розвиток ІТ неможливий без існування відповідних бізнес-процесів, то виникає питання грамотної побудови ІТ-процесів в організації. Тільки впровадження зрілих ІТ-процесів дозволить спеціалістам повністю розкрити свій потенціал та принести максимальну користь для організації.

В свою чергу, будь-якому фахівцю в сфері ІТ дуже складно та трудоємнісно забезпечити виконання поставленої задачі без знань та використання відповідних стандартів. Необхідність дотримуватися

окремих державних стандартів закріплена на законодавчому рівні, в той же час як все більше і більше спеціалістів орієнтуються на використання в процесі роботі закордонних стандартів, таких як COBIT версії 5, та бібліотеки ITILv3.

Кожен з них існує як форма накопичення знань та досвіду багатьох спеціалістів, це збірки кращих світових практик і рекомендацій для створення, розвитку та підтримки служб IT в організаціях.Стандарт COBIT є розробкою Асоціації з аудиту та контролю інформаційних систем (ISACA). Реліз останньої, п'ятої версії даного стандарту відбувся в 2012 році. Він описує цілісну методологію керування і управління IT-процесами організації при одночасній підтримці балансу між отримання вигоди і оптимізацією ризиків та ресурсів. Простіше кажучи, завдання COBIT полягає в ліквідації розриву між керівництвом компанії з їх баченням бізнес-цілей та IT-службами, що здійснюють підтримку інформаційної інфраструктури, яка повинна сприяти досягненню цих цілей. Сімейство COBIT включає публікації, які описують бізнес-модель, процесну модель, рекомендації щодо впровадження, інформаційної безпеки, ризиків та інші. Варто зазначити, що стандарт постійно оновлюється за рахунок релізів нових і оновлення існуючих публікацій.На відміну від COBIT, бібліотека ITIL описує не керування функціонуванням IT-процесів, а власне процес їх організації, становлення, підтримки і їх вдосконалення протягом всього життєвого циклу. Третя версія даної бібліотеки була представлена в листопаді 2011 року. Одним з основних принципів ITIL є процесний підхід, що дозволяє розмежувати ланцюжок взаємодій IT-структури на окремі процеси і чітко описати принцип роботи кожного з них і точки їх взаємодії, виходячи з поставлених перед кожним структурним підрозділом і перед бізнесом в цілому завдань. Також в бібліотеці ITIL розглядаються завдання, процедури та зони відповідальності конкретних виконавців і структурних підрозділів за поставлену задачу.

Висновок: при використанні будь-якого з вищевказаних підходів, як для становлення IT в цілому, так і для організації окремих IT-процесів в організації можливо отримати позитивний результат. Варто пам'ятати, що обидва підходи не є такими, що суперечать один одному, а навпаки – доповнюють один одного.

УДК 004.073(043.2)

**М.Б. Якименко, О.П.Ткаліч, А.Г.Тараненко**
*Національний авіаційний університет, м. Київ*

## ОПТИМІЗОВАНА МУЛЬТИСЕРВІСНА ПЛАТФОРМА КАФЕДРИ ТКС

На кафедрі ТКС реалізовано концепцію мультисервісної мережі, тобто мережі яка являє собою багатоцільову цілісну структуру , в якій реалізовано сервіси передачі даних, голосу, системи відеоспостереження, IP телефонія . Постає задача пошуку нових рішень та підходів для збільшення продуктивності роботи існуючої системи, впровадження нових програмних рішень на базі існуючої технічної інфраструктури.

**Послуги реалізовані на кафедрі ТКС**

| Назва сервісу | Виміряна швидкість | Максимальна швидкість | Реалізація сервісу |
|---|---|---|---|
| Бездротова передача даних | 14 Мбіт/с | 100 Мбіт/с | Wi-Fi роутери, точки доступу Wi-Fi |
| Дротова передача даних | 78 Мбіт/с | 100 Мбіт/с | Вита пара, комутатори, маршрутизатори |
| Відеоспостереження | 10 Мбіт/с | 100 Мбіт/с | Камери відеоспостереження, можливість використання web-камери користувачів |
| IP телефонія | 100 Мбіт/с | 100 Мбіт/с | IP телефони, програмні SIP телефони |

Таблиця 1. Реалізація сервісів на кафедрі ТКС

**Концепція CRM мережі кафедри.**

CRM (Customer Relationship Management) – це система управління ресурсами клієнтів, створення системи єдиного електронного документообігу.

Розглянемо декілька основних методів реалізації CRM системи для автоматизації діяльності кафедри.

- Створення онлайн журналу відвідування студентами лекційних та практичних занять, замість використання паперових і громіздких журналів.
- Для студентів це:створення єдиної БД навчальних матеріалів : лекційного матеріалу, книг, завдань для лабораторних та практичних робіт, графіків проведення екзаменаційного контролю та проміжного модульного контролю, графік консультацій викладачів кафедри; можливість слідкувати за всіма змінами в розкладі
- Для викладачів це можливість миттєво отримати доступ до поточних даних про успішність студентів, оцінити загальний рівень успішності, скорегувати учбовий процес в разі необхідності, слідкувати за термінами та правильністю виконання практичних завдань, курсових, домашніх завдань; миттєвий доступ до даних про календарне планування.

**Практичне застосування підходів до оптимізації послуг**

Було створено та налаштовано FTP сервер для зберігання навчальних та методичних матеріалів. Розмежовано права доступу за яких, викладачі мають повний доступ до всіх ресурсів (можливість редагувати, видаляти, завантажувати, зчитувати дані), а студенти лише зчитувати та завантажувати.

Створено систему конференц зв'язку на базі Asterisk з використанням програмних SIP телефонів для оптимізації проведення виробничих нарад та вирішення термінових питань.

**Висновки**

В результаті проведених досліджень було вивчено та запропоновано два підходи до часткової оптимізації послуг реалізованих на кафедрі.

**Використана література:**

1. Р.С. Одарченко, О.П. Ткаліч, О.О. Полігенько. Експериментальні дослідження пропускної здатності мереж стандарту IEEE 802.11 n

УДК 621.39.005 (043.2)

**Tetiana Sokol**
*National aviation university, Kiev*

## HIGH FREQUENCY COMMUNICATION SYSTEMS ON THE AIRCRAFT

The Federal Aviation Administration required all aircraft operating in high traffic areas to be equipped with two-way communication radios. In this time period, technology has advanced radically in the area of solid state electronics . The type of aircraft communications that most frequently comes to mind is that which takes place between Pilot and Controller, and uses a "Very High Frequency" (VHF). Several other means are available and they include "High Frequency" (HF), "Satellite Communications" (SAT COM) — even some telephone systems can be used in flight.

VHF communication systems are the most widely used for maintaining contact between ground and aircraft. This employs "Line Of Sight" transmission, which translates to a range of about thirty miles for an aircraft operating at 1,000 feet above the ground, or about 135 miles with an aircraft operating at 10,000 feet.

Frequency range was extended from 132 MHz to 136 MHz.

To calculate frequency range the given formula may be using: VFR=1.33×(/H aircraft+/H ground station)

The equipment required for this voice link includes a transceiver or transmitter/receiver, antenna, microphone, audio panel.

The transceiver is where most of the action is. This device has eight separate functions to perform

Flight line troubleshooting can be greatly enhanced by understanding the inputs and outputs of a transceiver. For example, in most commercial aircraft, the transmitter/receiver is connected to an audio panel. This provides selector switches to connect the output of the receiver to the audio amplifier to make the signal strong enough to be heard through the flight deck speakers.

Conclusions: the fact that there are usually separate panels for both crew members, provides the ability to connect the output of the transceiver to either amplifier. So, if the audio signal is lost, an initial determination can be made simply by actuating switches if the problem is in the transceiver or audio amplifier.

НАУКОВЕ ВИДАННЯ

# ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

# «ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

6 – 7 ЧЕРВНЯ 2018 Р.

М. КИЇВ

ГОЛОВНИЙ РЕДАКТОР КОНАХОВИЧ Г.Ф.
КОМП'ЮТЕРНА ВЕРСТКА ЛАВРИНЕНКО О.Ю.
КОНТАКТНИЙ E-MAIL: conference.tks@i.ua

ВІДПОВІДАЛЬНІСТЬ
ЗА ЗМІСТ ТА ФОРМУ ВИКЛАДЕННЯ НАУКОВИХ РЕЗУЛЬТАТІВ
НЕСУТЬ АВТОРИ МАТЕРІАЛІВ ТЕЗ.



ЕЛЕКТРОННА ВЕРСІЯ ТЕЗ КОНФЕРЕНЦІЇ ЗРОБЛЕНА СПЕЦІАЛЬНО ДЛЯ РОЗМІЩЕННЯ НА САЙТІ
НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ
http://tks.nau.edu.ua