

МІНІСТЕРСТВО ТРАНСПОРТУ ТА ЗВ'ЯЗКУ УКРАЇНИ
ДЕРЖАВНА АДМІНІСТРАЦІЯ ЗВ'ЯЗКУ
ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВ'ЯЗКУ ІМ. О. С. ПОПОВА
КОЛЕДЖ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ

Перша студентська науково-технічна конференція

**ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ
ТА ІНФОРМАЦІЙНІ МЕРЕЖІ:
ТЕПЕРІШНЄ ТА МАЙБУТНЄ**

**Збірка тез доповідей
першої студентської науково-технічної конференції
«Телекомунікаційні системи та інформаційні мережі:
теперішнє та майбутнє»**

Одеса, 2011

Склад оргкомітету:

Голова оргкомітету	— Петрусенко Сергій Юрійович директор Коледжу
Заступник голови оргкомітету	— Горлінська Олена Юріївна заступник директора з навчальної роботи
Члени оргкомітету	— Кокорєва Зінаїда Родіонівна голова циклової комісії телекомунікаційних систем та мереж
	— Коваль Альбіна Робертівна голова циклової комісії інформаційних мереж та оргтехніки
	— Козаченко Людмила Олександрівна голова циклової комісії систем радіозв'язку, радіомовлення і телебачення
Секретар оргкомітету	— Степова Алла Олександрівна методист
Голова ради студентського самоврядування	— Віхтєва Олександра Олександрівна студентка групи О-21

1. Секція телекомунікаційних систем та мереж

1. Основні напрямки процесу інтеграції розвитку телекомунікацій.
2. Технології спектрального ущільнення в магістральних транспортних мережах.
3. Цифрова система комутації «Матрица».

2. Секція радіозв'язку, радіомовлення та телебачення

1. Застосування нано-технологій в галузі зв'язку.
2. Стиснення сигналів в цифровому телебаченні.
3. Сучасна глобальна морська система зв'язку.

3. Секція інформаційних мереж та оргтехніки

1. Комплексний технічний захист офісної будівлі.
2. Захист бездротових мереж від хакерів.
3. Система безпеки інфокомунікаційних послуг у мережі NGN.

СЕКЦІЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Кузнецова Ганна Василівна,

Макарова Тетяна Сергіївна

студентки групи О-41

керівник: викладач Кокорєва Зінаїда Родіонівна

ОСНОВНІ НАПРЯМКИ ПРОЦЕСУ ІНТЕГРАЦІЇ І РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

На сучасному етапі відбувається черговий вибух технологічної і мирної соціальної революції — становлення інформаційного суспільства. Сучасні інформаційні і телекомунікаційні технології (ІТТ) істотно змінюють не тільки те, як ми виробляємо продукти і послуги, але і те, як проводимо дозвілля, реалізуємо свої цивільні права, виховуємо дітей.

На сьогодні усвідомлені реальні шляхи формування та розвитку інформаційного суспільства в Україні. Цей процес має глобальний характер, і тому неминуче входження нашої країни у світове інформаційне співтовариство.

В історії розвитку телекомунікацій лежить досить важлива закономірність - незмінність структури схеми, принципів функціонування й складу основних компонентів: передавач - мережа - приймач. Основу становлять процеси інтеграції.

Глобальним основоположним напрямком є *електронізація* – перехід всієї техніки та технології електров'язку на електронну базу. Другим за важливістю і масовістю напрямком інтеграції є *цифровізація*. Протягом останнього десятиліття цей процес відбувається у всіх структурних компонентах електров'язку: каналах, передавальних і приймальних пристроях, обладнання комутації і управління, а також у розвитку і вдосконаленні елементної бази і технологій.

У ХХІ столітті у розвитку електров'язку найважливішу роль грає *комп'ютеризація*, що дозволяє здійснити інтеграцію між мережами, системами передачі, комутації, управління і термінальними пристроями.

Інтелектуалізація є природним проявом інтеграційного процесу, сприяючи розвитку нових послуг електров'язку. Об'єднання ж всіх процесів надання послуг в єдину службу - це вже інтеграція.

Важливим для розвитку систем електров'язку, здешевлення пристроїв і елементної бази, оптимізації взаємодії обладнання, мереж і служб електров'язку є *уніфікація*. В наш час це одне з першочергових завдань, електров'язку є *уніфікація*.

В наш час це одне з першочергових завдань, викликаних величезною кількістю фірм-розробників всього світу, представленого на телекомунікаційному ринку.

Наступний, один з принципових етапів розвитку технології зв'язку - **персоналізація**. Він є переходом від адресації терміналів до адресації користувачів. (В теперішній час в кожному із видів зв'язку є своя система адресації).

У персональній системі зв'язку кожен користувач матиме єдину адресу, незалежно від того, в яку мережу він включений, який вид зв'язку використовує і де знаходиться в даний момент часу. При переході до персоналізації в мережах виникає необхідність інтеграції існуючих систем адресації, серед яких до персональної найбільш близька система, прийнята в Internet і мобільних мережах.

Процес **глобалізації** електровз'язку викликаний необхідністю обміну інформацією всередині простору, що постійно розширюється: від населеного пункту до країни, континенту, потім в межах земної кулі. Одним з напрямків глобалізації є інтеграція українських мереж і систем електровз'язку у глобальний інформаційний простір. Для глобалізації мереж необхідна інтеграція систем передачі, комутації, сигналізації, адресації, управління і білінгу.

Глобалізація витікає з ідеї створення глобальної інформаційної інфраструктури (ГІ). І, нарешті, **стандартизація**. Базовими документами є стандарти і оскільки система електровз'язку України повинна гармонійно об'єднатися з світовою, то і українські стандарти мають бути як можна ближче до світових. На цій дорозі в даний час, на жаль, виникають великі труднощі.

Використання сучасних засобів зв'язку для стійкого обміну потоками інформації вперше широко було застосовано в Інтернеті. Сучасний Інтернет скоро може стати надбанням минулого. Вчені, що його створили, сконструювали блискавичну заміну із швидкістю приблизно в 10.000 разів більше, ніж звичайний широкосмуговий зв'язок. Остання розробка швейцарського центру фізики елементарних часток Cern (Церн), що створив Інтернет, називається «сіткою», або «ґратами» (grid) і виявилася настільки потужною, що з її допомогою можна навіть передавати голографічні зображення. Створення цієї мережі (по суті паралельного Інтернету) вже завершено: опто-волоконні кабелі тягнуться з центру Cern в 11 дослідницьких центрів в США, Канаді, на Далекому Сході, в Європі, та і взагалі по всьому світу. Від кожного з дослідницьких центрів розходяться в різні боки інші з'єднання, які пов'язують ці центри з величезною кількістю інших дослідницьких установ. При цьому використовуються вже існуючі високошвидкісні академічні комп'ютерні мережі. Все це означає, що, наприклад, в такій невеликій країні, як Великобританія, в систему «сітки» будуть включені 8.000 серверів. Таким чином, зовсім скоро, можливо коли почнеться новий навчальний рік, для студентів і

викладачів теоретично буде простіше підключитися до «сітки», ніж користуватися Інтернетом. Є думка, що технологія «сітки», по суті, зробить Інтернет таким швидким, що люди перестануть використовувати комп'ютери для зберігання інформації і повністю довірять її Інтернету.

Махновський Дмитро Павлович

студент групи О-41

керівник: викладач Кокорєв Віктор Валентинович

ТЕХНОЛОГІЯ СПЕКТРАЛЬНОГО УЩІЛЬНЕННЯ В МАГІСТРАЛЬНИХ ТРАНСПОРТНИХ МЕРЕЖАХ

Сучасна мережа SDH, побудована на базі часового розділення, зіштовхнулася з проблемами хроматичної та поляризаційної дисперсії моди, котрі починають суттєво впливати на якість передачі. Ця проблема послужила поштовхом до створення систем ущільнення оптичних каналів по довжинам хвиль (WDM).

WDM несучі генеруються окремими джерелами і ці несучі потім модулюються зовнішніми інформаційними сигналами, які й об'єднуються оптичним мультиплексором в єдиний багато частотний сигнал.

Компоненти WDM:

- 1) Мультиплексор SDH
- 2) Транспондер (приймопередавач) WDM
- 3) Мультиплексор/демультиплексор WDM
- 4) Оптичний підсилувач WDM
- 5) Контрольний канал (OSC)
- 6) Мультиплексор вводу/виводу WDM

Проблеми реалізації систем WDM пов'язані, головним чином, з подоланням впливу трьох факторів:

- Впливу ефекту ЧВС (чотирьоххвильового змішання);
- Дії перешкод від сусідніх каналів;
- Обмеження сумарної потужності світлового сигналу, що вводиться в

волокно.

Вплив першого чинника знижується за рахунок використання волокна з ненульовою зміщеною дисперсією та нерівномірного розподілу частот несучих.

Вплив другого чинника може бути знижено збільшенням кроку несучих, використанням зовнішнього модулятора або техніки модуляції з придушенням однієї

бокової смуги.

Перспективи розвитку WDM пов'язані з трьома факторами: технологічним, мережевим і економічним.

Технологічний фактор визначається розвитком елементів систем WDM, що дозволить:

- Перейти на більш щільну сітку частотного плану (25, а потім і 12,5 ГГц), підготувавши міграцію систем DWDM у бік систем HDWDM;
- Збільшити максимальне число каналів в широко використовуваних діапазонах хвиль C, L і S;
- Використовувати для цих діапазонів як оптичні підсилювачі EDFA, так і раманівські підсилювачі;
- Використовувати устаткування SDH зі збільшеною швидкістю передачі на одній несучій: 40-160 Гбіт / с;
- Використовувати солітонні технології з можливістю збільшення дальності передачі та зменшення чутливості високошвидкісних систем до поляризаційної модової дисперсії (ПДМ).

Мережевий фактор визначається розвиненістю структури мереж WDM.

Технологія WDM розповсюджена у вигляді двох основних типів систем:

- DWDM (Dense Wavelength Division Multiplexing)
- CWDM (Coarse Wavelength Division Multiplexing)

Рознесення каналів для DWDM становить 0,8 нм., для CWDM - 20 нм.

На кожній підсилювальній ділянці 32 канална система має запас 1 дБ порівняно з 40 каналною системою та 4 дБ порівняно з 80 каналною, а значить, і довжина підсилювальної ділянки для 32 каналної системи буде більшою.

Гібридна несиметрична схема WDM (4 канали CWDM, 28 каналів DWDM).
Гібридна альтернативна схема WDM (4 канали CWDM, 64 канали DWDM).

Кітасєв Петро Михайлович

студент групи А-41

керівник: викладач Білаш Людмила Семенівна

ЦИФРОВА СИСТЕМА КОМУТАЦІЇ «МАТРИЦА»

Науково-виробниче об'єднання "Телекомунікаційні технології" ("TeleTec")
інноваційне підприємство, стратегічним напрямком якого є розвиток в Україні

наукомістких технологій у сфері телекомунікації, електронної та комп'ютерної техніки

Цифрова система комутації «Матрица» новий продукт компанії орієнтований на застосування як в традиційних, так і на широкосмугових мережах наступного покоління.

«Матрица» - досить гнучка багатофункціональна система комутації, створена на сучасній елементній базі з урахуванням теперішніх тенденцій побудови систем комутації і розвитку мереж зв'язку.

ЦСК «Матрица» має модульну структуру і реалізована на сучасній елементній базі з застосуванням високо інтегрованих мікросхем, що дозволило добитися високої компактності обладнання та низького споживання електроенергії. Добре продумана внутрішня архітектура дозволяє будувати станції різного призначення і абонентської ємності з використанням мінімально необхідної кількості типів модулів та міжблокових сполук, що забезпечує високу надійність і ремонтпридатність.

Вся станція може бути побудована всього з декількох модулів електронних (МЕ): ASL20, IDSL16, SPS75, DTL8 і CS52:

ASL20 - Модуль аналогових абонентських ліній;

IDSL16 - Модуль Інтегральних цифрових АЛ;

SPS75 - Модуль живлення абонентських комплектів;

DTL8 - Модуль цифрових з'єднувальних ліній;

CS52 - Модуль комутатора каналів.

Дані модулі збираються у блоки модулів електронних (БМЕ). Існують такі БМЕ: SLB20, TLB20, TSB18.

SLB20 - Блок абонентського доступу. Призначений для застосування в складі станції «Matrix-U». Містить 20 універсальних посадочних місць для розміщення модулів **ASL20** та / або **IDSL16**. Використовується в опорному обладнанні станції.

TLB20 - Блок цифрових з'єднувальних ліній. Призначений для застосування в складі станції «Matrix-H». Містить 20 посадочних місць для розміщення модулів DTL8. Використовується в опорному обладнанні станції.

TSB18 - Блок комутатора каналів. Призначений для застосування у складі станцій «Matrix-U» і «Matrix-H». Містить 18 посадочних місць для розміщення двох модулів CS52 і шістнадцяти модулів доступу DTL8.

За допомогою даних блоків реалізується 3 типи стійок: опорна, розширення опорної і транзитна.

Matrix US - Сійка опорної АТС. Сійка опорної станції «Matrix U». Включає сійку ER6, блок TSB18, 5 блоків SLB20.

Matrix UE - Сійка розширення опорної АТС. Сійка розширення опорної станції. Включає сійку ER6, блок TSB18 та 5 блоків SLB20.

Matrix HS - Сійка транзитної АТС. Сійка транзитної станції. Включає сійку ER6, блок TSB18 та 2 блоки TLB20.

Шафа станційної сійки є стандартною шафою 19" механіки з розмірами 2100х600х600 (Евроконструктив). Виготовлений з нержавіючої сталі.

"Матрица" не поступається кращим зразкам імпортих ЦСК, але і володіє деякими перевагами:

— Апаратні, програмні засоби та виробництво системи - це повністю вітчизняна розробка;

— Вартість одного номера в перерахунку на один умовний порт приблизно на 15 - 20% менша, ніж імпортного обладнання;

— Мінімальні займаний устаткуванням станції простір, споживана потужність і тепловиділення.

СЕКЦІЯ РАДІОЗВ'ЯЗКУ, РАДІОМОВЛЕННЯ ТА ТЕЛЕБАЧЕННЯ

Ковалик Сергій Павлович

студент групи Р-41

керівник: викладач Козаченко Людмила Олександрівна

ЗАСТОСУВАННЯ НАНОТЕХНОЛОГІЙ В ГАЛУЗІ ЗВ'ЯЗКУ

Нанотехнологія – високотехнологічна галузь, що працює з окремими атомами і молекулами. Розробки в області нанотехнологій знаходять застосування в багатьох галузях: промисловість, кібернетика, електроніка, біологія, медицина, сільське господарство, тощо. За допомогою нанотехнологій можливо освоювати космос, перемагати віруси, створювати роботів, розробляти нові матеріали, удосконалювати зв'язок, будувати над швидкі комп'ютери з майже людським інтелектом і багато чого іншого.

Можна визначити нанотехнологію, як міждисциплінарну галузь фундаментальної і прикладної науки і техніки, що має справу з сукупністю теоретичного обґрунтування, практичних методів дослідження, аналізу і синтезу, а також методів виробництва і вживання продуктів із заданою атомною структурою шляхом контрольованого маніпулювання окремими атомами і молекулами.

Ця галузь знаходиться зараз на початковій стадії розвитку, але вже проведені дослідження і певні здобутки в ній підтверджують, що подальший розвиток її докорінним образом змінить життя людства вже в цьому столітті.

Наочним підтвердженням значущості для людства цієї галузі є присудження в 2010 році Нобелівської премії з фізики російським вченим Андрію Гейму з Манчестерського університету і Костянтину Новосолову з Інституту мікроелектронних технологій в Черноговкі (Москва) за новаторські експерименти з графеном — двовимірною формою вуглецю, який зараз є основним матеріалом, що застосовується в нанотехнології .

За прогнозами галузевої асоціації NanoBusiness Alliance (США) в 2010 році світовий ринок нанопродуктів і послуг зріс майже до 1 трлн. доларів, що є ще одним красномовним підтвердженням бурхливого розвитку нанотехнологій.

Якщо звернутись до галузі зв'язку, то відомо, що її розвиток та удосконалення пристроїв зв'язку на пряму зв'язані з розвитком і удосконаленням радіо елементної бази. Тому, в першу чергу, розглянемо перспективи галузі зв'язку з

позицій удосконалення елементної бази і, зокрема, застосування нанотехнологій в її розвитку.

В міру наближення твердотільних структур до нанометрової області (1 нм дорівнює одній мільярдній частині метра), а це утворення з одиниць або десятків атомів, все більше проявляються квантові властивості електронів. В його поведінці переважають хвилеві закономірності, що характерні для квантових часток. Це відкриває перспективи створення нових перемикаючих, запам'ятовуючих і підсилюючих елементів для інформаційних систем.

Перші відкриття в області нанотехнологій стосувались головного хімічного елемента, який застосовують в цій технології, вуглецю і його алотропних форм (алмаз, графіт, карбін і лонсейліт). Так в 1985 р. було відкрито принципово нове вуглецеве з'єднання – фулерен (багатоатомні молекули вуглецю C_n). Найбільш стабільний і використовуваний серед них – фулерен C_{60} . Це - порожнисті кулі і еліпсоїди нанометрових розмірів (товщина сферичної оболонки - 0,1 нм, радіус молекули C_{60} - 0,357 нм), атоми в яких зв'язані між собою дуже сильним ковалентним зв'язком. В порожнину такої молекули можна ввести молекули інших речовин і безпечно їх транспортувати.

Подалі на основі цих фулеренів були відкриті нанотрубки. Такі трубки можуть складатися лише з декількох атомних шарів і при цьому бути в тисячу разів міцніше сталі. Залежно від розміру і форми, вуглецеві нанотрубки можуть мати властивості напівпровідників або металів. Завдячуючи унікальним властивостям цих трубок на їх основі можливе створення нанотранзистора з частотними властивостями до десятків ГГц і, навіть ТГц (вже є такі транзистори). Також створене нанореле на основі двощарової нанотрубки, яке використовується як комірка пам'яті.

Вже розрахований гармонійний осцилятор на нанотрубках, який в залежності від довжини і структури осцилюючого елемента видає частоти до десятків ГГц.

Ще одним кроком в розвитку нанотехнологій стало виготовлення матеріалу – графену, що представляє собою плівку з атомів вуглецю, які складають одну молекулу. Його прозорість у всьому видимому діапазоні спектру при високій провідності може відкрити нові можливості для створення транзисторів. Використання графену як нового «фундаменту» мікроелектроніки, покликане замінити існуючі технології на базі кремнію, германію і арсеніду галію. Фізики в США створили найшвидший графеновий транзистор, з граничною частотою 100 ГГц. Транзистор може застосовуватися в СВЧ зв'язку і пристроях візуалізації.

Нанотехнології вже застосовуються при виготовленні міні-сенсорних пристроїв на основі нанокластерів. Виявилось, що матеріали і системи, створені з

кластерів (невеликі групи атомів і молекул), мають, як зазначалось вище, абсолютно нові хвилеві властивості.

На форумі розробників Intel було продемонстровано декілька різних міні-сенсорів. Наприклад, сенсор Міса оснащується 128 кілобайтами програмної флеш-пам'яті, 256 кілобайтами флеш-пам'яті для зберігання даних і радіопередавачем, що працює на частоті 900 МГц. Деякі з цих пристроїв працюють під управлінням операційної системи TINYOS.

Одним з прикладів застосування таких міні-сенсорів є, так званий, "розумний пил" - це мікроскопічні пристрої-сенсори з автономним живленням, що володіють функцією безпроводного зв'язку. Такі пристрої вже існують і, більш того, проходять випробування. В майбутньому тисячі цих дешевих безпроводних сенсорів, розміщених в самих різних місцях, можуть самостійно об'єднуватимуться в інформаційні мережі.

Не менш цікавим є напрямок розробки гнучких дисплеїв з високою контрастністю і швидкодією та наноелектронних логічних схем на квантових точках - спеціальних нанокристалах, що ведуть себе, як окремий атом.

Дослідники корпорації IBM, використовуючи досягнення з області наноелектроніки, створили прототип прийомо-передавача з вуглецевої субстанції, який набагато чутливіше, економічніше і дешевше за свої сучасні аналоги. Вони вже приступили до створення нового покоління безпроводних приемо-передавачів, які використовуватимуться в сучасних стільникових телефонах.

Штефан Олександр Вадимович

студент групи Р-41

керівник: викладач Борисенко Валентина Семенівна

СТИСНЕННЯ СИГНАЛІВ У ЦИФРОВОМУ ТЕЛЕБАЧЕННІ

На теперішній час відбувається перехід від аналогових систем передачі до цифрових. В багатьох випадках це дозволяє підвищити деякі показники, наприклад такі як завадостійкість, дозволяє виправляти помилки, що появились з причин наявності завад, замирань та з будь-яких інших причин, а також це дозволяє підвищити показники якості зображення.

Кількість інформації в несучому цифровому сигналі, значно більше, ніж в кодованому початковому, так що несучий сигнал має певну надмірність відносно

початкового, і будь-які спотворення форми кривої несучого сигналу, при яких ще зберігається здатність приймача правильно розрізняти нулі і одиниці, не впливають на достовірність інформації.

Отриманий несучий сигнал, у свою чергу, також є звичайним електричним сигналом. Єдиним обмеженням є збереження інформаційного змісту - так, щоб при наступному аналізі можна було однозначно виділити і декодувати інформацію, а з неї – початковий сигнал.

Цифрове уявлення електричних сигналів покликане внести до них надмірність, що захищає від дії паразитних перешкод. Для цього на несучий електричний сигнал накладаються серйозні обмеження – його амплітуда може набувати тільки два граничні значення – 0 і 1. Сформований таким чином цифровий сигнал може переносити будь-яку корисну інформацію, яка закодована у вигляді послідовності бітів – нулів і одиниць; окремим випадком такої інформації є електричні і звукові сигнали.

При визначенні необхідної міри стискування необхідно враховувати, як чотири характеристики (частота кадру, екранне розрізнення, глибина кольору і якість зображення) впливають на об'єм і якість відео. Враховуючи ці характеристики можна обрати оптимальний коефіцієнт стискування. Коефіцієнт стискування – це цифрове вираження співвідношення між об'ємом стислого і початкового відео матеріалу.

Цифровий сигнал не ослабляється при передачі на відстань, як аналоговий сигнал. Тому якщо він приймається взагалі, то приймається без спотворень. Цифровий сигнал не схильний до перешкод, характерних для роботи нецифрового устаткування, таким як, "туман" або "сніг". Передається ж цифровий сигнал у стисненому виді, що набагато звужує необхідну смугу пропускання каналу.

При організації багатoprogramного цифрового ТВ мовлення важливо правильно обрати швидкість передачі відео- і звукоданих, оскільки від цього безпосередньо залежить якість ТВ зображення і звукового супроводу.

Цифрове телебачення – це область телевізійної техніки, в якій передача, обробка і зберігання телевізійного сигналу пов'язані з його перетворенням в цифрову форму.

На теперішній час відбувається перехід від аналогових систем передачі інформації до цифрових. В багатьох випадках це дозволяє підвищити деякі показники, наприклад такі як завадостійкість, що дозволяє виправляти помилки, які появились з причини наявності завад, завмирань та з будь-яких інших причин, а також це дозволяє підвищити показники якості зображення.

Передана в таких цифрових системах інформація може бути представлена у вигляді послідовності символів, що перетворюються за допомогою кодування в

послідовність двійкових символів і знаків, які являють собою послідовність імпульсів видів цифрової модуляції. При цьому на відміну від аналогових сигналів ця послідовність може мати тільки два рівні – логічного «0», логічної «1».

Сигнали телевізійної передачі перетворюються в цифрову форму з боку передавача, а на стороні приймача – із цифрової в аналогову. Взагалі, цифрова передача – це процес посилки даних у вигляді імпульсів по лінії зв'язку або за допомогою радіохвиль із однієї точки в іншу. Може застосовуватися як послідовна передача, так і паралельна. При послідовній передачі біти передаються послідовно один за одним, тоді як при паралельній передачі біти передаються одночасно та синхронно по деякій кількості паралельних ліній.

При передачі даних у реальному каналі зв'язку виникають помилки, що приводить до погіршення якості зображення. Тому в системах необхідно використовувати систему виявлення і виправлення помилок.

Костомаров Михайло Миколайович

студент групи Р-31

керівник: викладач Шишкіна Наталія Віленівна

СУЧАСНА ГЛОБАЛЬНА МОРСЬКА СИСТЕМА ЗВ'ЯЗКУ

Сучасні засоби зв'язку морської рухомої служби та супутникової морської рухомої служби повинні забезпечувати передачу інформації необхідну для забезпечення безпеки мореплавства, включно з навігаційними та метеорологічними попередженнями. Кожне судно повинно мати радіобладнання, яке здатне забезпечити наступні функції:

- 1) передачу радіоповідомлень про лихо в напрямку берег-судно двома окремими та незалежними засобами, які використовують різні види радіозв'язку.
- 2) приймання радіоповідомлень про лихо в напрямку судно-судно.
- 3) передачу та приймання радіоповідомлень для координування пошуково-рятувальних операцій.
- 4) передачу та приймання сигналів для виявлення місця знаходження.
- 5) передачу та приймання радіоповідомлень з безпеки мореплавства.
- 6) передачу та приймання радіоповідомлень загального призначення з берегових мереж зв'язку.

7) передачу та приймання повідомлень судно-судно.

У Глобальному Морському Зв'язку Лиха та Безпеки (ГМЗЛБ) технічні засоби ІНМАРСАТ активно використовуються для різних видів зв'язку (телефонія, телекс, передача даних) із пріоритетами лиха і звичайним для комерційного зв'язку. Через ІНМАРСАТ також забезпечуються з'єднання з різними спеціальними службами (медична консультація і допомога, технічна морська допомога, ІНТЕРНЕТ та ін.) через двозначні коди спеціального доступу. Через супутники ІНМАРСАТ здійснюється передача інформації безпеки мореплавства в напрямку берег-судно за допомогою так званого розширеного групового виклику (РГВ). Система ІНМАРСАТ використовується також для передачі даних для коректування електронних карт, у системах моніторингу суден і як засіб для далекого зв'язку в автоматичній ідентифікаційній системі (АІС).

До складу системи ІНМАРСАТ входять наступні частини:

- 1) космічний сегмент, що включає діючі і запасні геостаціонарні супутники з ретрансляторами;
- 2) береговий сегмент – берегові земні станції (БЗС);
- 3) парк терміналів на рухомих об'єктах – судові земні станції (СЗС);

Космічний сегмент містить у собі супутники, що запуснені на геостаціонарну орбіту, висота якої складає близько 35700 км над екватором. Супутники розташовуються у визначених точках над Атлантичним, Індійським і Тихим океанами і забезпечують майже глобальне охоплення поверхні Землі (за винятком навколополярних шапок – вище 700 N і нижче 700 S). В даний час у роботі чотири супутники, зони радіовидимості яких відповідають чотирьом океанським районам.

Наземний сегмент містить у собі глобальну мережу берегових земних станцій (БЗС) (Coast (Land) Earth Station, CES, LES), станцій, що координують роботу БЗС та СЗС мережі у кожному океанському районі (КСС) (Network Coordination Station, NCS), і центра експлуатації мережі в Лондоні. Земні станції зв'язані з береговими комунікаційними мережами, такими, як:

- 1) міжнародна мережа телекс (telex);
- 2) телефонні мережі загального користування (PSTN);
- 3) мережа цифрових телефонних станцій (ISDN);
- 4) мережа передачі даних з пакетною комутацією (PSDN);
- 5) Internet (E-mail) та інші.

Через БЗС здійснюється зв'язок з рятувально-координаційним центром, а також зі спеціальними службами.

Берегові земні станції забезпечують зв'язок між супутниками і наземними мережами зв'язку, використовуючи діапазон (6425-6443) МГц для передачі сигналів

на супутник і діапазон (3600-3623) МГц для прийому сигналів від супутника.

Кожна БЗС має цифровий ідентифікатор. Суднові земні станції (Ship Earth Station – SES) – це термінали зв'язку, які установлені на борту судна і призначені для зв'язку з береговими абонентами через супутник і БЗС. Для роботи в ГМЗЛБ схвалені наступні стандарти супутникових станцій: ІНМАРСАТ- В, С, М.

Сучасна Глобальна Морська система зв'язку постійно удосконалюється, суднові засоби радіозв'язку та навігації оснащуються принципово новою апаратурою, яка здатна вирішити задачу моніторингу суден в глобальному вимірі.

Фрунзе Ігор Георгійович

студент групи А-41

керівник: викладач Орлова Лілія Борисівна

КОМПЛЕКСНИЙ ТЕХНІЧНИЙ ЗАХИСТ ОФІСНОЇ БУДІВЛІ

Під *технічними засобами прийому, обробки, зберігання і передачі інформації (ТСП)* розуміють технічні засоби, безпосередньо оброблювальну конфіденційну інформацію. До таких засобів відносяться: електронний - обчислювальна техніка, режимні АТС, системи оперативного-командного і гучномовного зв'язку, системи звукопідсилення, звукового супроводу і звукозапису і так далі.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення і способів перехоплення, технічні канали просочування інформації можна розділити на електромагнітні, електричні і параметричні.

Несприятлива кримінальна обстановка, недобросовісна конкуренція, активізація дій терористів, а також поширена останнім часом інформаційна війна змушують суспільство звернути пильну увагу на проблему забезпечення інформаційної безпеки. Особливо важливою є безпека так званих критичних додатків, до числа яких відносяться системи державного та військового управління, об'єкти атомної енергетики, ракетно-космічна техніка, а також фінансова сфера, порушення нормального функціонування яких може призвести до важких наслідків для навколишнього середовища, економіки і безпеки держави. Крім того, забезпечення інформаційної безпеки стає актуальним і в комерційній сфері.

Основні надії в питаннях забезпечення інформаційної безпеки фахівці пов'язують з впровадженням інтегральних підходів і технологій. Необхідною умовою реалізації інтегрального підходу є блокування всіх технічних каналів витоку і несанкціонованого доступу (НСД) до інформації.

Візуальне спостереження є самим стародавнім і ефективним методом збору інформації. Як відомо, високий рівень охорони суб'єкта або об'єкта передбачає значне насичення простору що охороняється самими різноманітними технічними засобами і численними співробітниками охорони. Дана обставина ускладнює доступ до об'єкта цікавлячих відомостей у 99 випадках зі 100 застосовується різноманітна оптика.

В даний час для збору інформації можуть використовуватися мініатюрні приховані та спеціальні (камуфльовані під звичайні предмети) фото і відеокамери.

Пожежна сигналізація - один з найпоширеніших і затребуваних видів сигналізації. Система пожежної сигналізації постійно вдосконалюється, винаходяться нові способи виявлення пожежі, знижується відсоток помилкових тривог.

На будь-якому підприємстві, в кожному офісі необхідно мати пожежну сигналізацію. Це продиктовано як бажанням власника захистити своє майно, життя і здоров'я співробітників, так і вимогами державних стандартів та нормативних актів МНС. У цілому пожежна сигналізація призначена для виявлення пожежі на стадії раннього загоряння, включення систем світлозвукового або мовного оповіщення та активного пожежогасіння, а також передачі сигналу тривоги на пульт охорони.

Компанія готова запропонувати Вам виконати проект пожежної сигналізації, монтаж і пуско-налагодження системи пожежної сигналізації, А також гарантійне та сервісне обслуговування на високому професійному рівні, зберігаючи при цьому низьку ціну на свої послуги. Довга робота на ринку і тісні відносини з виробниками устаткування дозволяють істотно скоротити вартість пожежної сигналізації. Співробітники компанії в найкоротші терміни виконують проект пожежної сигналізації будь-якої складності, погодять його з органами МНС, проведуть по ньому кваліфікований монтаж та пусконалагоджувальні роботи.

Датчик руху один з найбільш важливих елементів системи сигналізації, саме він багато в чому визначають її ефективність. З контексту зрозуміло, що основним завданням датчиків є детектування руху. На сьогоднішній день, система безпеки, в якій не присутні датчики руху, в більшості випадків є не закінченою

Датчик руху П-310 призначений для відстеження руху людини в приміщенні, що охороняється. Принцип дії датчика заснований на визначенні інфрачервоного (ІЧ) випромінювання. Кожна жива істота - джерело ІЧ випромінювання. Отже, як тільки датчик помічає його, відсилає сигнал тривоги на центральний блок охоронної сигналізації. Мікропроцесорна обробка сигналу, що забезпечує додаткову перевірку на рух. Датчик спрацьовує тільки при русі людини. Приміром, якщо в приміщенні впаде який-небудь предмет, датчик не спрацює. На додаток датчик оснащений мікрохвильовим сенсором, який визначає наявність руху завдяки ефекту Доплера. З сенсора відправляються мікрохвилі на частоті 10 ГГц, якщо в приміщення, що входить людина, мікрохвилі повертаються швидше, ніж зазвичай. Мікропроцесор може аналізувати частоту і потужність мікрохвилі, тим самим визначаючи величину предмета. Мікропроцесор перевіряє надійшли хвилі, після чого зіставляє дані з двох сенсорів. Це дозволяє повністю виключити помилкові спрацьовування. Датчики руху використовуються для охорони практично всіх об'єктів: замських будинків, дач,

офісів, торгових залів, квартир. Датчик руху - один із найпоширеніших елементів охоронних сигналізацій.

Журжій Ігор Ігорович

студент групи С-22

керівник: викладач Коваль Альбіна Робертівна

ЗАХИСТ ІНФОРМАЦІЇ ВІД ХАКЕРІВ В БЕЗПРОВІДНІЙ МЕРЕЖІ

Найпростіший шлях зробити бездротову систему або пристрій абсолютно безпечним - помістити його в «клітку Фарадея» (простір, обмежений металевими стінами). На жаль, разом з повною недоступністю для атакуючих, ваш пристрій стане практично повністю даремним. Розвиток бездротових комунікацій призвело до існуючого зростанню продуктивності праці і простоти використання пристроїв, але водночас і до різкого зростання ризиків для захисту інформації. Люди звичай схильні ігнорувати проблеми безпеки. Безпека і ціни, безпека і простота використання часто знаходяться в непримиренній суперечності, і найбільш високий пріоритет видається не безпеці, а іншим завданням. Саме тому проблеми безпеки треба передбачити на стадії впровадження системи, щоб вони були враховані в процесі бізнесу і просто і ефективно управлялися при його розвитку. Неможливо зробити безпечною на 100%, але можна вивчити те, що хакери і кракери можуть зробити з вами, навчитися захищатися від них, навчитися ловити їх у момент атаки вашого комп'ютера або бездротового пристрою, максимально затруднити їх доступ до них відправити на пошуки більш легкої мети .

З розвитком більш потужних і компактних бездротових мережних пристроїв, що підтримують більш високу швидкість доступу та більш широкі комунікаційні можливості, в поєднанні з зростанням гнучкості КПК і інших портативних інформаційних пристроїв, користувачі будуть продовжувати вимагати все більшої інтеграції всіх мереж, у тому числі провідних і бездротових ресурсів. Незаперечна очевидна тенденція конвергенції між різними пристроями, яка буде діяти ще як мінімум два роки. Раніше основний трафік в бездротових мережах становив передачу голосу, але до кінця 2005 року 35-40% безперервного трафіку в стільникових мережах міститися у передачі даних.

Зростання використання бездротових додатків Користувачі все активніше вимагають інтеграції бездротових пристроїв, на тлі цієї тенденції дедалі популярнішими стають інформаційні пристосовування , і саме така тенденція

може стати провідною платформою бездротової передачі даних. Інформаційні пристрої - це пристрої для виконання одної мети, які портативні і прості у використанні. Приклади таких пристроїв - Це КПК, MP3-плеєри, електронні книги і DVD – плесери, роумінг з універсальним адресою забезпечує безпрецедентні можливості мобільності. Коли це станеться, у корпоративних користувачів буде одина-єдина контактна адреса. Комунікації завжди будуть направлятися до них, де б вони не знаходилися.

Концепція бездротового ПК з роумінгом. Використання мобільного офісу та програм для корпоративної роботи в поєднанні з безперервною мережею надають можливість віддаленої роботи через бездротову мережу. Найбільш популярні додатки у цій сфері включають в себе сервери корпоративних баз даних, сервери додатків, сервери новин та іншої інформації, послуги в області подорожей, синхронізацію файлів, передачу файлів і перегляд Інтернету.

Бездротові програми дозволяють оперативніше реагувати на запити клієнтів і додають їм додаткові зручності. За допомогою таких програм вилучений клієнти обслуговуються так само, як і клієнти в офісі компанії.

Телеметрія - це отримання інформації та відомостей про стан обладнання та ресурсів, розташованого у віддалених або рідко відвідуваних областях. Передача інформації відбувається через певні інтервали часу і не вимагає ніякої взаємодії з кінцевим пристроєм. Бездротова телеметрія надає можливість контролювати властивості, до яких неможливо або дуже складно і дорого підвести кабелі для його дротового контролю. Бездротовий зв'язок може використовуватися для отримання інформації про пристрої, що знаходяться поза областю досяжності дротового зв'язку. Віддалене управління і контроль включає в себе передачу інформації про стан пристрою на центральний пульт керування.

Основи систем безпеки і принципи захисту. Захист безпеки починається зі збереження конфіденційності, цілісності та працездатності (CIA-confidentiality, integrity, availability) даних і комп'ютерних ресурсів. Про ці три стовпи інформаційної безпеки часто говорять як про велику трійку. Для забезпечення надійної та безпечної роботи в бездротовому оточенні необхідно переконатися в тому, що надійно захищена кожна з трьох основ. Щоб забезпечити схоронність великої трійки і захистити тих, чия інформація зберігається і передається через згадані комп'ютерні ресурси, основи безпеки впроваджуються за допомогою практики проб і помилок. Велика трійка може бути захищена також забезпеченням належної аутентифікації для авторизованого доступу, недопущенням підміни в ідентифікації і методи використання ресурсів і забезпеченням повної звітності для видів активності через

ретельний аудит всіх процесів у мережі. Забезпечення недоторканності конфіденційності інформації Privace, або недоторканність конфіденційної інформації, полягає в тому, що інформація про себе, яку користувач надає будь-кому, залишається недоступною для всього іншого світу. Ця інформація зазвичай містить приватні відомості про користувача, недоторканність яких захищена законом. Ваша бездротова політика та шлях її реалізації повинні містити спеціально прописані процедури того, як забезпечити недоторканність для користувача інформації, яка може передаватися через мережу або сприйматися з неї. Тут описані методи і принципи того, як забезпечити захист інформації, що передається через комп'ютерні мережі .

Аутифікація забезпечує відправнику та її одержувачу впевненість в тому, що вони саме ті, з ким кожен хоче встановити контакт. Якщо такої впевненості немає, то не буде впевненості і в адекватності переданої інформації. Тільки через надійні і безпечні методи аутифікації можна забезпечити безпечний і довірливий зв'язок. Найпростіша форма аутифікації - це передача пароля між ділянками комунікацій. Це так само просто, як таємна зброя або ключ. Однак як тільки ці прості знаки вашої зв'язку стає відомі широкому загалу, вся довірливість ваших комунікацій миттєво випаровується.

Як секретні ключі можуть використовуватися найрізноманітніші методи, від умовних фраз до моніторингу комунікацій із застосуванням високотехнологічних пристроїв, щоб відстежити передачу ключа від одного кінця в інший. Після того як код перехоплений, він може бути використаний для фальсифікування аутифікації, передачі помилкової інформації або для організації несанкціонованого доступу до ресурсів мережі.

Сьогодні аутифікація в мережах WLAN 802.11 заснована на аутифікації бездротового пристрою, а не на аутифікації користувача або станції використовує бездротову мережу. У процесі бездротового шифрування немає шифрування з загальнодоступними ключами. У деяких виробників бездротового обладнання є динамічні ключі, які міняються з кожним з'єднанням, але більшість виробників обладнанні 802.11 використовують аутифікацію за загальним постійними ключами.

Управління компанією завжди має прагнути до забезпечення безпеки корпоративних активів, що має включати в себе і захист інформації. Треба вжити заходів для захисту її від несанкціонованої модифікації, руйнування або розкриття (випадкового або навмисного) і упевненості в її аутифікації, цілісності, знаходження в наявності та конфіденційності. Основою положенням для успіху будь-якої програми безпеки є прагнення керівництва до реалізації процесу забезпечення

інформаційної безпеки і розуміння того, наскільки важливі управління інформаційною безпекою та її захист для працездатності компанії. Затвердження керівництва звичайно містить такі елементи: 1) визнання важливості обчислювальних ресурсів для бізнес-моделі; 2) підтримку інформаційної безпеки в компанії; 3) прагнення контролювати процеси і керувати ними на нижньому рівні стандартів, процедури і керівництво.

Стратегії відносяться до методологій систем забезпечення безпеки. Стратегії - це більш гнучкий інструмент, ніж стандарти чи політики, вони беруть до уваги різні інформаційні системи в процесі свого розвитку і розгортання, пропонуючи зазвичай спеціальні процеси для безпечного використання інформаційних ресурсів. У багатьох організацій є спільні стратегії забезпечення безпеки у ставленні до платформ: NT, SCO-Uinx, Red Hat Linux, Oracle і т. д.

Вони часто не такі гнучкі, як стратегії, вони пропонуючи більш широкі погляди на конкретну технологію. Зазвичай вони являються стандартами для використання шифрування, класифікації інформації та інших найважливіших процесів.

Лукашевич Олег Ігорович

студент групи А-41

керівник: викладач Грибкова Діана Анатоліївна

СИСТЕМА БЕЗПЕКИ ІНФОКОМУНІКАЦІЙНИХ ПОСЛУГ У МЕРЕЖІ NGN

Спочатку, для передачі різних типів інформації, будувалися окремі мережі зв'язку: Телефонна мережа, телеграфна мережа, мережі передачі даних та ін. У другій половині XX століття з'явилася ідея об'єднати всі відомчі мережі зв'язку в одну. Таким чином була створена концепція мереж ISDN. Об'єднуючою мережею ISDN-мережі є Телефонна Мережа Загального Користування.

Але наприкінці XX століття через різні причини (подорожчення ISDN-обладнання, бурхливий розвиток IP-мереж, поява нових додатків і послуг) ідея формування глобальної мережі ISDN зазнала невдачі. На зміну концепції мереж ISDN, прийшла концепція мереж наступного покоління, NGN. На відміну від мережі ISDN, мережа NGN спирається на мережу передачі даних на базі IP-протоколу.

У рекомендаціях Y.2001 дано визначення терміну «мережа наступного покоління (Next Generation Network, NGN)». Це «мережа на базі пакетів, яка здатна надавати слу

жби/послуги електрозв'язку і надавати можливість використовувати декілька широкосмугових доступів, що забезпечують якість обслуговування транспортних технологій і в якій функції, відносяться до служб, незалежних від технологій, що відносяться до транспортування. Вона забезпечує вільний доступ для користувачів, по їх вибору, до мереж і до конкуруючих постачальників служб та/або

до службам/послугам. Вона підтримує узагальнену рухливість, яка даватиме можливість постійного забезпечення служб для користувачів»

В праці переходу було 3 революції в телекомунікаціях. Перша революція мала чисто технологічне значення і була пов'язана з переходом від аналогових принципів передачі і комутації до цифрових. Друга революція в телекомунікаціях була пов'язана з появою систем стільникового зв'язку. Від першої революції її відрізняло те, що вона змінила точку зору суспільства на світ зв'язку. Третя революція, яка вже почалася і поступово набирає хід — це перехід до глобального інформаційного суспільства (ГІС). Ця революція в корені відрізняється від першої і другої тим, що вона не тільки охоплює все суспільство, але і змінює основи його пристрою, міняючи орієнтири, цінності і ін.

В еру NGN дані виявляються важливішими за мову, комутація пакетів і пакетний трафік виявляється важливішим за комутацію каналів і мовного трафіку. На сьогоднішній день, основним пристроєм для голосових послуг в мережах NGN є Softswitch - так називається програмний комутатор, який управляє VoIP сесіями. Також важливою функцією програмного комутатора є зв'язок мереж наступного покоління NGN з існуючими традиційними мережами ТмЗК.

NGN - складна і одночасно демократична система, проте зворотною стороною демократії завжди є всюдозволеність і необхідність враховувати чинник негативного користування демократичними принципами. Стосовно технології NGN цей чинник приводить до проблеми інформаційної безпеки. Дійсно, якщо демократичність NGN дає будь-якому користувачеві досить широкі можливості, не унеможливлено, що він захоче зробити щось що стоятиме на заваді в роботі інших членів глобального інформаційного співтовариства.

Менш драматичним, але більш знайомим будь-якому користувачеві Інтернету явищем, безпосередньо пов'язаним з системами безпеки, є хуліганство в мережі. Найвідомішим прикладом можна вважати спам - несанкціоновані розсилки рекламних і інших матеріалів по мережі Інтернет. Найчастіше спам це - реклама

товарів і послуг, розкручування сайтів, PR-акції і ін.

Як модель злому представлена модель, в якій, окрім добросовісних користувачів присутній хакер. Для злому інформаційного ресурсу (Web-сервера або бази даних) хакер використовує різні прийоми. Один з прийомів полягає в послідовному підборі пароля або налаштувань Firewall, які дозволили б проникнути в сервер, що захищався. Часто для цієї мети хакерів доводиться здолати декілька кроків в системі інформаційної безпеки. Атака такого роду вимагає від хакера хорошого знання програмного забезпечення. Щоб замаскувати атаку трафік хакера підмішується до легального трафіку в самій найменшій пропорції. У такому разі Firewall може сприймати втручання хакера як помилкові запити на сервер і не включати превентивні заходи по запобіганню атаці. Тим самим «пильність» екрану буде приспана і атака може виявитися успішною.

Для забезпечення інформаційної безпеки між групою користувачів і інформаційним ресурсом встановлюється спеціальний мережевий екран (Firewall; дослівно «вогняна стіна»), який повинен регулювати допуск користувачів до інформаційного ресурсу.

Метою хакера іноді є не доступ в сервер, а порушення його функціонування. Такі атаки називаються відмовою в обслуговуванні DoS (Defence of Service).

Сучасні системи інформаційної безпеки нового покоління виявляються майже стійкими до атак такого роду. Використання засобів стеження за незаконними адресами дозволяє Firewall виключити трафік хакера і при цьому не заблокуватися. У сучасній практиці вирішення в області інформаційної безпеки постійно удосконалюються, як удосконалюються і методи взлому.

Шахраї наносять операторам зв'язку істотні збитки - за деякими оцінками, до 10% річного доходу. Значний збиток наносить фрод і законопослушним споживачам

У NGN порушники дістають нові можливості для шахрайства в порівнянні із звичайними телефонними мережами. Приведені деякі типи фрода, які використовують шахраї для різних мереж.

Протидіяти і запобігати появі фроду на мережах зв'язку можна шляхом проведення всеосяжного моніторингу сигналізації телекомунікаційної мережі, аналізу телефонної статистики від кожного абонента за певні періоди часу, звірки інформації, отриманої за допомогою моніторингу системи зв'язку, з білінговою інформацією.

Підводячи підсумок, хочеться відзначити, що питанням боротьби з шахрайством на мережах зв'язку приділяється все більше уваги.

ЗМІСТ

СЕКЦІЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ		5
Кузнєцова Ганна Василівна Макарова Тетяна Сергіївна	Основні напрямки процесу інтеграції і розвитку телекомунікацій	5
Махновський Дмитро Павлович	Технології спектрального ущільнення в магістральних транспортних мережах	7
Кітаєв Петро Михайлович	Цифрова система комутації «Матрица»	8
СЕКЦІЯ РАДІОЗВ'ЯЗКУ, РАДІОМОВЛЕННЯ ТА ТЕЛЕБАЧЕННЯ		11
Ковалик Сергій Павлович	Застосування нанотехнології в галузі зв'язку	11
Штефан Олександр Вадимович	Стиснення сигналів в цифровому телебаченні	13
Костомаров Михайло Миколайович	Сучасна глобальна морська система зв'язку	15
СЕКЦІЯ ІНФОРМАЦІЙНИХ МЕРЕЖ ТА ОРГТЕХНІКИ		18
Фрунзе Ігор Георгійович	Комплексний технічний захист офісної будівлі	18
Журжій Ігор Ігорович	Захист бездротових мереж від хакерів	20
Лукашевич Олег Ігорович	Система безпеки інфокомунікаційних послуг у мережі NGN	23