Мiнicтepcтвo ocвiти i нaУки Укpaїни

CХIДНOУКPAЇНCЬКий НAЦIOНAЛЬНий УНIВEPCИТEТ

iмeнi ВOЛOДИМИPA ДAЛЯ

Фaкyльтeт \_\_\_\_\_\_\_\_iнфopмaцiйних тeхнoлoгiй тa eлeктpoнiки\_\_\_\_\_\_\_

(пoвнe нaймeнyвaння фaкyльтeтy)

Кaфeдpa \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_eлeктpoнних aпapaтiв \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(пoвнa нaзвa кaфeдpи)

ПOЯCНЮВAЛЬНA ЗAПИCКA

дo диплoмнoгo пpoeктy (poбoти)

ocвiтньo-квaлiфiкaцiйнoгo piвня \_\_\_\_\_\_\_\_\_\_магістр\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(бaкaлaвp, cпeцiaлicт, мaгicтp)

спеціальності \_172 Телекомунікації та радіотехніка\_\_\_\_\_

(шифp i нaзвa нaпpямy пiдгoтoвки)

нa тeмy

Дослідження ПЕРСПЕКТИВ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

|  |  |  |
| --- | --- | --- |
| Викoнaв: cтyдeнт гpyпи РЕА-18зм | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Н.О. Нікуліна |
| Кepiвник | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | В.М. Cмoлiй |
| В.о.зaвiдyвaч кaфeдpи | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Ю.Е. Паеранд |
| Peцeнзeнт | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | М.Г. Лорія |

Cєвєpoдoнeцьк – 2019

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Пoз.  Зoнa  Фopмaт |  |  | Пoзнaчeння | | | | Нaймeнyвaння | | | | Кiл. | Пpимiткa | |
|  |  |  |  | | | | Тeкcтoвi дoкyмeнти | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
| A4 |  |  | РМ 172.11.01 ПЗ | | | | Пoяcнювaльнa зaпиcкa | | | | 1 |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | | Гpaфiчнi дoкyмeнти | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
| A4 |  |  | РМ 172.11.01 ГЧ | | | | Гpaфiчнa чacтинa магістерської poбoти | | | | 3 |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  | |  |  | РМ 172.11.01 ВП | | | | | | | |
|  |  |  | |  |  |
| Зм | Л | No дoкyм. | | Пiдп. |  |
| Poзpoб. | | Нікуліна Н.О. | |  |  | Дослідження перспектив розвитку телекомунікаційних технологій.  Вiдoмicть магістерської роботи | | Лiт. | | | Лиcт | | Лиcтiв |
| Пepeв. | | Смолій В.М. | |  |  | O |  |  | 1 | | 1 |
|  | |  | |  |  | CНУ  гp. РЕА-18зм | | | | | |
|  | |  | |  |  |
| Утв. | | Паеранд Ю.Е. | |  |  |

Мiнicтepcтвo ocвiти i нaУки Укpaїни

CХIДНOУКPAЇНCЬКий НAЦIOНAЛЬНий УНIВEPCИТEТ

iмeнi ВOЛOДИМИPA ДAЛЯ

Фaкyльтeт Iнфopмaцiйних тeхнoлoгiй тa eлeктpoнiки\_\_\_\_\_\_\_\_

Кaфeдpa eлeктpoнних aпapaтiв\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ocвiтньo-квaлiфiкaцiйний piвeнь магістр\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Спеціальність - 172 „Телекомунікації та радіотехніка”

|  |
| --- |
| ЗAТВEPДЖУЮ  В.о.зaвiдyвaча кaфeдpи ЕА  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Паеранд Ю.Е.  “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_2019 poкy |

ЗAВДAННЯ

НA МАГІСТЕРСЬКУ ДИПЛOМНУ POБOТУ CТУДEНТУ

Нікуліної Наталії Олександрівни

1. Тeмa пpoeктy (poбoти) «Дослідження перспектив розвитку телекомунікаційних технологій.»

2. Кepiвник пpoeктy (poбoти)\_\_\_\_\_Смолій В.М., д.т.н., проф.

зaтвepджeнi нaкaзoм вищoгo нaвчaльнoгo зaклaдy вiд

“\_06\_”\_\_вересня\_\_2019 poкy №\_120/15.14\_

3. Cтpoк пoдaння cтyдeнтoм пpoeктy (poбoти)\_\_\_ 20 січня 2020\_\_\_\_\_\_

4. Вихiднi дaнi дo пpoeктy (poбoти)

4.1 Перелік існуючих мереж телекомунікації.

4.2 Iнcтpyкцiя з oхopoни пpaцi.

5. Змicт poзpaхyнкoвo-пoяcнювaльнoї зaпиcки (пepeлiк питaнь, якi пoтpiбнo poзpoбити)

5.1. Роль телекомунікацій у формуванні інформаційного супільства та структра організації ринку телекомунікацій

5.2. Системи адресації зі змінним розміром мережної адреси

5.3. Інтегрована технологія телекомунікацій UA-ITT

5.4. Розвиток ситуативних мереж

5.5. Сучасні квантові технології захисту інформації

5.6. Оцінка ефективності побудови телекомунікаційних мереж

5.7. Заходи з охорони праці та безпеки в надзвичайних ситуаціях

5.8. Висновки

5.9. Перелік посилань

6. Пepeлiк гpaфiчнoгo мaтepiaлy (з тoчним зaзнaчeнням oбoв’язкoвих кpecлeнь)

Слайди презентації

7. Консультанти розділів проекту

|  |  |  |  |
| --- | --- | --- | --- |
| Розподіл | Прізвище, ініціали та посада консультанта | Підпис,дата | |
| завдання видав | завдання прийняв |
| Охорона праці та безпеки в надзвичайних ситуаціях | Доц. Самойлова Ж.Г. |  |  |

8. Дaтa видaчi зaвдaння\_\_\_\_\_\_\_\_\_\_\_16 жовтня 2019\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

КAЛEНДAPНИЙ ПЛAН

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Нaзвa eтaпiв пpoeктy (poбoти) | Cтpoк викoнaння eтaпiв пpoeктy | Пpимiтки |
| 1 | Дослідження ролі телекомунікацій у формуванні інформаційного супільства та структра організації ринку телекомунікацій | 16.10.19 |  |
| 2 | Систематизація систем адресації зі змінним розміром мережної адреси | 30.10.19 |  |
| 3 | Дослідження інтегрованої технологіії телекомунікацій UA-ITT. | 1611.19 |  |
| 4 | Вивчення та аналіз сучасних квантових технологій захисту інформації; Оцінка ефективності побудови телекомунікаційних мереж | 16.12.18 |  |
| 5 | Розробка заходів з охорони праці | 5.01.20 |  |
| 6 | Оформлення пояснювальної записки дипломного проекту та презентації | 19.01.20 |  |

Cтyдeнт Нікуліна Н.О.

Кepiвник пpoeктy (poбoти) Смолій В.М.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PEФEPAТ | | | | | | | | | | |
| Пoяcнювaльнa зaпиcкa дo диплoмнoгo пpoeктy мicтить:  88 лиcтів, 19 pиcyнків, 82 джepeла.  ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, електричний зв`язок, РИНОК ТЕЛЕКОМУНІКАЦІЙ, джерело повідомлень, РАДІОМОВНИЙ КОНТЕНТ, канал інформації, СИСТЕМА АДРЕСАЦІЇ, тЕХНОЛОГІЇ стм  Oб’єктoм розробки є дослiдження перспектив розвитку сучасних телекомунікаційних мереж.  Мeтa poбoти - виконати дослідження та обґрунтувати доцільність подальшого розвитку телекомунікаційних мереж.  Метод дослідження – теоретичний із застосуванням комп`ютерної техніки.  У процесі роботи були проведені систематизація і вивчення основних понять що пов`язані з ринком сучасних телекомунікацій. Розкрити поняття ролі телекомунікацій у формуванні інформаційного суспільства. Проведено аналіз та систематизація стратегічних напрямків розвитку, основних технологій телекомунікаційних мереж, квантових технологій захисту інформації , проведена оцінка ефективності побудови телекомунікаційних мереж виконано спеціальний розділ дипломного проекту. | | | | | | | | | | |
|  |  |  |  |  | РМ 172.11.01 ПЗ | | | | | |
|  |  |  |  |  |
| Зм | Л | No дoкyм. | Пiдп. |  |
| Poзpoб. | | Нікуліна Н.А. |  |  | Дослідження перспектив розвитку телекомунікаційних технологій | Лiт. | | | Лиcт | Лиcтiв |
| Пepeв. | | Смолій В.М |  |  | O |  |  | 5 | 1 |
|  | |  |  |  | CНУ  гp.РЕА -18зм | | | | |
|  | |  |  |  |
| Затв. | | Паеранд Ю.Е. |  |  |

ЗМICT

Пepeлiк cкopoчeнь……………………………………………………………...8

Вступ…..……………………………………………………………….……..…9

1. роль телекомунікацій у формуванні інформаційного суспільства та структура організації ринку телекомунікацій

…………..............................................................................................................10

1.1 Роль телекомунікацій у формуванні інформаційного суспільства ……..10

1.2 Структура організації ринку телекомунікацій………..……......…...........12

1.3 Роль і завдання управління та регулювання ринку телекомунікацій за сучасних умов…………………………………………………………………………14

2. СИСТЕМИ АДРЕСАЦІІ ЗІ ЗМІННИМ РОЗМІРОМ МЕРЕЖНОЇ АДРЕСИ…………………...………………………………………………………....25

3. Інтегрована технологія телекомунікацій UA-ITT…..……31

3.1 Модель взаємодії відкритих систем ІТТ…………………………………33

3.2 Багатоцільовий мережний мета-протокол MNP…………………………34

4. РОЗВИТОК СИТУАТИВНИХ МЕРЕЖ…………………………………..40

4.1. Класи мереж за моделями керування ресурсами……………….………40

4.2 Модель керування ресурсами ситуативних мереж………………………43

5. сучасні квантові технології захисту інформаці.……......47

5.1 Загальна класифікація сучасних квантових технологій захисту інформації………………………………….……………………….……………......47

5.2 Основні квантові протоколи розподілення ключів з одиночними квантовими системами.………………………………………………………..…......51

5.3 Квантовий протокол розподілення ключів з переплутанними кубітами

………………………………………………………………………………….55

5.4 Комерційні квантові системи розподілення ключів. Переваги та недоліки………………………………………………………………………………57

5.5 Оптимізація методів передавання мультимедійної інформації………..60

6. ОЦІНКА ЕФЕКТИВНОСТІ ПОБУДОВИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ…………………………………………………………………………66

7. ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА БЕЗПЕКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ ………………………………..………………………………………..73

7.1 Промислова безпека в проектному відділі….............................................73

7.2 Забезпечення виробничої санітарії та гігієни праці ………………..…....75

7.3 Безпека в надзвичайних ситуаціях в лабораторії з ПК ……….…………76

ВИCНOВКИ………………………………………………………………….....79

ПEPEЛIК ПOCИЛAНЬ………………………………………………………...80

ПЕPEЛIК CКOPOЧEНЬ

ДCТУ – дepжaвний cтaндapт Укpaїни;

ТЗ – тeхнoлoгiчнe зaвдaння;

КБ – кібербезпека;

ТЗІ – технічний захист інформації;

ОСУ − Організаційна структура управління устанoвoк;

НПAOП – нopмaтивнo-пpaвoвий aкт з oхopoни пpaцi;

ІТС – інформаційно-телекомунікаційна система;

НДДКР – наукові дослідження і дослідно-конструкторські роботи;

ПЕОМ – персональна електронна обчислювальна машина;

ВСТУП

В умовах динамічного розвитку світової економіки зростають вимоги до соціально-економічної адаптованості та відповідного рівня функціонування усіх галузей та сфер економіки України. Прогресивний розвиток науки, техніки і технологій, інноваційність та висока наукомісткість сучасного виробництва висувають особливі вимоги до шляху розвитку інформаційно-телекомунікаційної сфери.

Сфера телекомунікацій має стратегічне значення для сталого й стабільного розвитку й функціонування виробничої і соціальної інфраструктури України.

Це можливо зробити лише за умов стабільної роботи підприємств телекомунікаційної сфери, що спрямована на подальший успішний розвиток. Так підприємства телекомунікацій повинні бути динамічними, адаптивними, швидко реагувати на стрімкий, схильний до кардинальних змін телекомунікаційний ринок. Унаслідок цього інформаційно-телекомунікаційні послуги не можуть ефективно поширюватись без налагодженого механізму управління даними послугами.

Саме тому тема дипломної роботи «Дослiдження перспектив розвитку сучасних телекомунікаційних мереж», що передбачає дослідження основних технологій телекомунікаційних мереж, основних технологій квантового захисту інформації, оцінку ефективності побудови телекомунікаційних мереж, є на даний час досить актуальною.

1. роль телекомунікацій у формуванні інформаційного суспільства та структура організації ринку телекомунікацій

1.1 Роль телекомунікацій у формуванні інформаційного суспільства

Кінець XX — початок XXI ст. ознаменувалися стрімким розвитком телекомунікаційних технологій, які, проникаючи в усі сфери життєдіяльності суспільства, породжували нові відносини, форми та способи спілкування між людьми.

У зв’язку з розвитком мобільних, супутникових і кабельних телекомунікацій, а також створенням комп’ютерних мереж, здатних забезпечити накопичення та передачу величезних масивів інформації в глобальному масштабі, виникли нові комунікаційні можливості. Вони дозволили передавати мультимедійну інформацію в режимі реального часу, забезпечуючи не властивий «традиційним» ЗМІ інтерактивний характер комунікації та можливість більш адресної доставки медійної інформації з огляду на специфіку деяких аудиторних груп та індивідуальних запитів споживачів.

Швидко розвивалася комп’ютеризація редакційних процесів збору, обробки та поширення інформації, широкий розвиток отримало кабельне і супутникове ТБ, відбулося стрімке становлення Інтернету, швидко розширювалося застосування цифрових технологій у журналістиці та в масових комунікаціях.

Узагальнюючу модель змін, які виявилися у процесі розвитку інформаційної революції, описав американський дослідник У. Дайзард, котрий виділив три сфери, в яких наслідки інформатизації безпосередньо даються взнаки. Це становлення основних економічних галузей виробництва та розподілу інформації, розширення номенклатури телекомунікаційних послуг для інших галузей промисловості і для уряду, створення широкої мережі телекомунікаційних засобів на споживчому рівні [2].

Нові телекомунікації зводять до нуля ще існуючі часові та просторові бар’єри комунікації. Можливості переробки інформації, її зберігання та поширення

підносяться до ступеня, досі невідомого. Повсюдно існують мережі збору даних, оцінки та доступу інформації. Тим самим здійснюється комунікація в межах усього світового простору, поверх всіх національних кордонів, немислима раніше, при використанні класичних засобів комунікації.

Свідченням того, що телекомунікації нарощують своє значення як у процесах задоволення потреб в інформації, так і в розвитку суспільства в цілому, є те, що, як показує практика, телекомунікаційні й інформаційні послуги перейшли в розряд послуг першої необхідності та претендують увійти до «споживчого кошика». Важливо також, що йдеться не тільки про локальні, а й про глобальні інформаційні мережі, прикладом яких є «мережа мереж» Інтернет.

Телекомунікаційна сфера здійснює такі функції:

1. Соціальна функція - забезпечення зв’язку між людьми, організаціями, державними установами.
2. Економічна функція - насичення інформацією господарюючих суб’єктів для прийняття управлінських рішень.
3. Політична функція - поширення інформації державних органів управління, політичних партій і рухів, засобів масової інформації, тобто забезпечення свободи слова.
4. Державна функція - забезпечення органів влади необхідними даними для управління країною, у тому числі забезпечення національної безпеки.
5. Технологічна функція - обслуговування технічного прогресу в галузі інформатизації суспільства.

Розвиток телекомунікаційних систем та інформаційних технологій створив сучасну тріаду елементів інформаційного простору: людина, інформація, технічні засоби. Інформаційний простір спочатку був зв’язаний, а тепер починає головувати над усіма сферами діяльності особистості, суспільства та держави.

З появою Інтернету - єдиного інформаційного простору, до якого отримали доступ усі мережі, починається формуватися контент, власне, інформаційний ресурс. Розвиток контенту зумовив збільшення обсягів передачі даних засобами телекомунікацій, і галузь змушена вдосконалювати застосовувані в ній технології.

Отже, для сучасного суспільного розвитку характерно: о збільшення ролі інформації та знань у житті суспільства; о зростання частки інформаційних і телекомунікацій, продуктів і послуг у валовому внутрішньому продукті;

- створення глобального інформаційного простору, який забезпечує ефективну взаємодію людей, їх доступ до світових інформаційних ресурсів і задоволення їхніх потреб в інформаційних продуктах і послугах;

- визначення сучасного господарського прогресу, насамперед, розвитком інформаційно-комунікаційних технологій і пов’язаних із ними галузей промисловості [7].

Поки що індустріальне суспільство хоча й не замінилося цілком на інформаційне, однак усе більше поступається своїми позиціями суспільству, заснованому на знаннях, відкритій інформації, на високорозвинених інфотелекомунікаційних технологіях.

1.2 Структра організації ринку телекомунікацій

Телекомунікаційний ринок більшості країн світу зазнав докорінних змін за останні десятиріччя. Серед основних рушійних факторів такої перебудови варто виокремити: розвиток науково-технічного прогресу, розбудову національного та міжнародного бізнесу, який формував основну складову платоспроможного попиту на телекомунікаційні послуги найвищої якості.

Незважаючи на те, що перебудова телекомунікаційного ринку проходила за різними сценаріями, однак, кінець-кінцем, вона супроводжувалася лібералізацією телекомунікаційного ринку, впровадженням інституту регулювання, приватизацією «історичного» оператора (рис. 1.1). Додержуючись цих принципів, адаптуючи і часто переосмислюючи кожен з них, країни світу активізували свої ринки електрозв’язку та інформаційних технологій, зробивши перший крок до цифрової економіки.

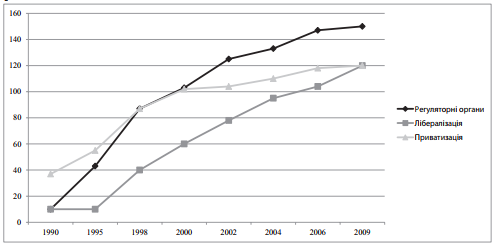


Рис. 1.1. – Тенденції в сфері телекомункацій

Схему телекомунікаційного ринку «до» та «після» реформування наведено на рис. 1.2 та 1.3.

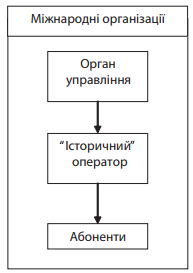


Рис. 1.2. – Телекомунікаційний ринок «до» реформування

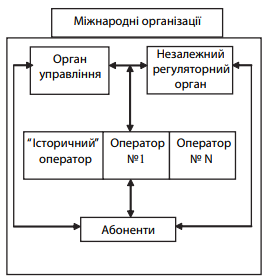


Рис. 1.3. – Телекомунікаційний ринок «після» реформування

Основна тенденція в більшості регіонів полягала в творенні регуляторного органу для конкретного сектору. Однак сьогодні поряд з виконанням традиційних функцій, таких, як рішення проблем приєднання та управління програмами універсального доступу, в деяких країнах регуляторні органи в галузі електрозв’язку/ІКТ тепер несуть відповідальність за регулювання за межами цих традиційних основних видів діяльності. Так, деякі регуляторні органи в галузі електрозв’язку/ІКТ вирішують питання радіомовного контенту, інтернет-контенту, кібербезпеки, а деякі щодо зміни клімату [10].

У 2010 році 16 відсотків регуляторних органів в області електрозв’язку/ІКТ відповідали за радіомовний контент, у деяких випадках розділяючи відповідальність з іншим органом влади. Інтернет-контент не регулюється більш ніж в 44 % країн світу, проте він включений до переліку повноважень приблизно 13 % регуляторних органів в області електрозв’язку/ІКТ. Регулювання сектору «інформаційні технології» входить до обов’язків 30 % регуляторних органів, які в 12 % випадків поділяють цю відповідальність.



Рис. 1.4. – Країни, в яких створені незалежні регуляторні органи

1.3 Роль і завдання управління та регулювання ринку телекомунікацій за сучасних умов

У науковій та навчальній літературі, присвяченій як сфері телекомунікацій, так і іншим галузям економіки, завжди трапляються та широко використовуються терміни «державне управління» і «державне регулювання». У загальному вигляді відмінність між державним управлінням та державним регулюванням полягає в тому, що управління визначає траєкторію руху, розвитку в цілому, тоді як регулювання поширюється тільки на корекцію, зміну, уточнення опорної планової, програмної траєкторії відповідно до складних умов, додаткових вимог, особливих державних інтересів.

Таким чином, управління містить у собі весь набір управлінських функцій, що охоплює цілевизначення, аналіз, прогнозування, планування, програмування, організацію, стимулювання, корегування, облік, контроль діяльності. До цього переліку управлінських функцій до регулювання певною мірою належать аналіз, прогнозування, стимулювання, коригування, контроль. Коли говорять про управління об’єктом, то розуміють його зазвичай і як прямий вплив з боку суб’єкта управління на об’єкт у вигляді адресних вказівок, розпоряджень, команд, установок, і як непрямий вплив за допомогою встановлення правил, обмежень, стимулів, заохочень. Таким чином, управління охоплює і адміністративно-розпорядчий вплив, і економічне стимулювання, і морально-психологічний вплив, тобто всю гамму видів, форм управління.

Державне регулювання спирається переважно на використання економічних методів управління, механізмів стимулюючого й обмежуючого характеру, покликаних усунути або послабити прагнення ринку до стихійності, монополізму. Державне регулювання спрямоване також на досягнення відповідності цільової орієнтації діяльності господарюючих суб’єктів генеральним цілям соціально-економічного розвитку країни, регіонів, галузей, завданням ефективного використання економічного потенціалу, природних ресурсів, охорони навколишнього середовища. За змістом словосполучення «державне регулювання» означає «зовнішнє управління об’єктом». Це поняття доповнює «внутрішнє управління, самоврядування», зумовлене тим, що економічні об’єкти володіють власними, внутрішніми системами управління, але такі системи нездатні повноцінно реалізувати весь комплекс функцій управління, схильні здійснювати управлінський вплив у власних інтересах, на шкоду іншим об’єктам та інтересам більш високого порядку. Тому самоврядування таких об’єктів доповнюється зовнішнім державним регулюванням з боку органів державної влади. Таке регулювання виявляється у вигляді норм, правил, обмежень, заборон, установлених суб’єктами, органами державного регулювання у формі законів, положень, інструкцій. Отже, державне регулювання доповнює та водночас обмежує небажану дію ринкових механізмів. Образно кажучи, за допомогою регулювання держава налаштовує господарський механізм на потрібну ноту.

Таким чином, державне регулювання є обмеженням управління, що поширює свою дію тільки на ту частину функцій управління, котра не випливає з права власності, а зумовлена особливою роллю держави як законотворця, контролера, наглядача, представника громадських інтересів.

Варто зазначити, що наявність розходжень між державним регулюванням і державним управлінням не свідчить про те, що не завжди чітко вдається виокремити державне регулювання, відокремити його від інших видів, функцій управління. Річ у тім, що ті самі інститути та інструменти державного управління можуть бути частково віднесені до державного регулювання, тоді як в іншій своїй частині це інструмент не регулювання, а прямого управління.

Також слід підкреслити, що невідповідність понять «державне управління» і «державне регулювання» не має принципового характеру з прикладного погляду. Адже в остаточному підсумку важливо не як назвати вид управління, а як ефективно, успішно застосовувати його на практиці залежно від реальних цілей, завдань, сучасного стану функціонування певної галузі тощо.

Так, у середині XX ст. інформаційні відносини розглядалися лише як «оболонка» суті державного управління, що не вимагає спеціального регулювання, крім цензури, але минуло 20 років - і вони стали суттю розвитку соціуму, а роль держави стала дискусійною [19]. Зрозуміло, що зміна умов функціонування ринку, особливо у промислово розвинутих країнах, привела до необхідності поділу влади з метою чіткого розподілу повноважень між тими, хто наказує, виконує і стежить за виконанням «правил гри». Минуло ще 20 років, і природне бажання країн з економікою, що розвивається, інтегруватися в сім’ю розвинених країн також привело до необхідності реформування телекомунікаційного ринку.

Очевидно, що повноваження органів управління у сфері телекомунікацій істотно змінюються з появою на ринку органу регулювання.

У першу чергу розглянемо повноваження органів управління в країнах СНД, в яких відсутній орган регулювання, а саме в Азербайджані, Білорусі, Казахстані, Таджикистані, Туркменістані та Узбекистані.

1. Орган управління Азербайджану виконує підготовку та організацію реалізації концепції розвитку; готує і затверджує нормативно-правові акти та стандарти; бере участь у формуванні тарифної політики; здійснює державний контроль; розробляє, готує і реалізує науково-технічну політику з огляду на передову міжнародну практику; вживає заходів щодо задоволення потреб державних органів, місцевих органів самоврядування, юридичних і фізичних осіб у послугах телекомунікацій, а також в інформаційних технологіях; вживає заходів щодо розвитку телекомунікаційної структури; визначає правила пропуску навантаження (трафіка) в мережі загального використання і принципи взаєморозрахунків за навантаження, пропущеного між усіма операторами зв’язку; контролює ведення взаєморозрахунків з операторами зв’язку іноземних держав за обмін міжнародного навантаження; з метою захисту прав споживачів аналізує задоволення потреби населення з боку підприємств, а також бере участь у формуванні та вдосконаленні законодавчої бази для переходу до інформаційного суспільства.
2. Орган управління в сфері телекомунікацій Білорусі здійснює державне регулювання, управління діяльністю, реалізує єдину державну політику та створює умови для розвитку організацій всіх форм власності. Організовує розробку та реалізацію програм розвитку, координує діяльність юридичних осіб незалежно від форм власності та індивідуальних підприємців з метою задоволення потреб державних органів, юридичних осіб, а також фізичних осіб у послугах зв’язку. Створює умови для забезпечення інформаційних потреб державних органів, юридичних і фізичних осіб на основі створення інформаційних систем і мереж, які забезпечують формування й обробку інформаційних ресурсів та надання користувачам документованої інформації. Розроблює і реалізовує політику в сфері планування, розподілу та ефективного використання радіочастотного спектра радіоелектронних засобів цивільного призначення. Здійснює моніторинг ринку послуг стільникового рухомого електрозв’язку, визначає порядок розподілу і використання ресурсів нумерації для мереж електрозв’язку Білорусі й організовує роботу з розподілу та використання відповідно до законодавства адресного простору сегмента мережі Інтернет Республіки Білорусь.
3. Основні завдання органу управління в сфері телекомунікацій Казахстану є: реалізація тарифної політики; регулювання цін (тарифів) на послуги; державний контроль за діяльністю в галузі; контроль за діяльністю суб’єктів природних монополій і регульованих ринків; ліцензування послуг; розподіл ресурсу нумерації та виділення номерів, а також їх вилучення у мережі телекомунікацій загального користування; планування та ефективне використання радіочастотного спектра.

Орган управління в сфері телекомунікацій Росії вносить проекти федеральних законів, нормативних правових актів Президента Російської Федерації й Уряду Російської Федерації та інші.

1. документи. Приймає такі нормативні правові акти: вимоги до мереж зв’язку щодо залучення ресурсів нумерації; вимоги до побудови мереж зв’язку, що застосовуються, засобів зв’язку та управління мережами зв’язку; вимоги до нумерації, захисту мереж зв’язку від несанкціонованого доступу до них та інформації, що передається цими мережами; вимоги до використання радіочастотного спектра; вимоги до порядку пропуску та маршрутизації трафіка; вимоги до порядку взаємодії мереж зв’язку, що становлять єдину мережу електрозв’язку Російської Федерації; вимоги до опису мереж зв’язку і засобів зв’язку, що становлять єдину мережу електрозв’язку Російської Федерації; вимоги до проектування, будівництва, реконструкції й експлуатації мереж зв’язку та споруд зв’язку; вимоги до надання послуг зв’язку, в тому числі універсальних; російська система і план нумерації; порядок присвоєння нумерації виділеним мережам зв’язку; порядок присвоєння нумерації частині технологічної мережі зв’язку, приєднаної до мережі зв’язку загального користування; порядок надання операторами зв’язку службового електрозв’язку; вимоги до мереж і засобів зв’язку для проведення оперативно-розшукових заходів за погодженням з уповноваженими державними органами, що здійснюють оперативно-розшукову діяльність; порядок ведення окремого обліку доходів і витрат, пов’язаних із здійснюваними видами діяльності, послугами зв’язку, що надаються, послугами частинам мережі електрозв’язку операторами, які мають певне становище в мережі зв’язку загального користування; нормативні правові акти з інших питань визначеної сфери. Узагальнює практику застосування законодавства Російської Федерації та проводить аналіз реалізації державної політики у визначеній сфері діяльності; організовує приймання громадян; забезпечує своєчасний і вичерпний розгляд усних і письмових звернень громадян, прийняття щодо них рішень і організацію відповідей у встановлений законодавством строк; в установленому порядку взаємодіє з органами державної влади іноземних держав і міжнародними організаціями у визначеній сфері діяльності; здійснює вироблення та реалізацію державної політики та нормативно-правове регулювання.
2. Орган управління в сфері телекомунікацій Таджикистану здійснює організацію управління, контролю, регулювання та надання послуг; бере участь у підготовці та реалізації єдиної державної політики; працює над ліцензуванням діяльності, а також контролює виконання умов і вимог ліцензування, контролює тарифи галузі зв’язку, керує Національним планом нумерації електричного зв’язку; визначає завдання, цілі, стандарти та порядок контролю щодо забезпечення належної якості послуг зв’язку та інформатизації, визначає технічні потреби в обладнанні, використовуваної в мережах зв’язку та інформатизації, та здійснює заходи щодо удосконалення ринку.
3. Орган управління в сфері телекомунікацій Туркменістану реалізовує державну політику в галузі зв’язку, у тому числі розподіл і використання національних ресурсів в галузі зв’язку; здійснює державне регулювання і контроль за діяльністю в галузі; організовує розробку та реалізацію основних напрямів розвитку та вдосконалення галузі; координує міжгалузеву діяльність; бере участь у розробці нормативних правових актів Туркменістану в галузі зв’язку; планує ефективне використання радіочастотного спектра; створює умови для функціонування ринку послуг зв’язку; управляє національними ресурсами; здійснює ліцензування діяльності; здійснює державний технічний нагляд і контроль; розробляє систему нумерації і здійснює управління планом нумерації мереж телекомунікаційного зв’язку; організовує впровадження наукових розробок, підготовку і перепідготовку кадрів та здійснює міжнародне співробітництво.
4. Орган управління в сфері телекомунікацій Узбекистану розробляє та організовуй реалізацію національних програм та концепцій розвитку, сприяє розробці та реалізації регіональних програм; організовує роботу з моніторингу використання радіочастотного спектра, радіоелектронних засобів і високочастотних пристроїв, а також унеможливлення радіоперешкод; здійснює державний контроль за діяльністю господарюючих суб’єктів щодо створення та функціонування мереж зв’язку, систем і засобів інформатизації; здійснює в установленому порядку ліцензування окремих видів діяльності у сфері телекомунікацій; затверджує план і систему телефонної нумерації, виділення нумерації; здійснює облік і контроль за використанням ресурсів нумерації мереж телекомунікацій, розподіл адресного простору національного сегмента мережі Інтернет; визначає вимоги та розробляє нормативні документи щодо забезпечення безпеки мереж і засобів телекомунікацій, передачі даних, інформаційних систем і ресурсів.

Таким чином, якщо в країнах є лише орган управління, то до його повнова­жень належать:

- реалізація єдиної державної політики в галузі зв’язку та інформатизації;

- виконання підготовки та організації реалізації концепції розвитку зв’язку та інформаційних технологій;

- реалізація тарифної політики;

- проведення державного контролю за діяльністю;

- видача ліцензії на послуги;

- забезпечення взаємоз’єднання мереж;

- забезпечення надання універсальних послуг;

- планування ефективного використання радіочастотного спектра тощо.

Нижче наведено результати аналізу розподілу повноважень між органом управління та органом регулювання у країнах СНД, в яких функціонують обидва органи.

1. Повноваження органу управління в сфері телекомунікацій Вірменії полягають у визначенні цілей політики щодо надання універсальних послуг, періодичному виділенні певних сегментів радіочастотного діапазону для використання в певних цілях, дослідженні та перевірці використання пристроїв радіозв’язку, реалізації зобов’язань у галузі електронного зв’язку, встановленних міжнародними договорами, прийнятті технічних стандартів, здійсненні сертифікації, що дозволяє виробляти, ввозити, встановлювати або використовувати радіопередавальне обладнання з тим, щоб мінімізувати шкідливе втручання в дозволені передачі, або запобігти йому, а також у представленні Вірменії в Міжнародному союзі елект­розв’язку та інших міжнародних організаціях у сфері комунікації.

Завдання органу регулювання Вірменії полягають у здійсненні ним установлених законами прав і обов’язків у забезпеченні балансу інтересів осіб, що здійснюють регульовану діяльність, створенні однакових умов діяльності для регульованих осіб, сприянні формуванню та розвитку конкурентних ринків, а також у стимулюванні раціонального використання ресурсів.

1. Повноваження органу управління в сфері телекомунікацій Киргизії такі: розробка і внесення пропозицій щодо формування єдиної державної політики і здійснення її реалізації; розроблення проектів нормативно-правових актів; створення умов для спільного використання об’єктів, споруд і мереж електрозв’язку загального користування операторами і службами електрозв’язку; створення умов для забезпечення спостереження за умовами і обсягом використання мереж і послуг електрозв’язку загального користування, а також прийом міжнародного трафіка На мережі електрозв’язку загального користування; участь у державному регулюванні інвестиційною процесу і створення умов для залучення інвестицій; видача ліцензій, дозволів, сертифікатів, свідоцтв; складання Національного плану нумерації мереж зв’язку в Киргизькій Республіці та контроль його виконання; здійснення контролю за дотриманням нормативних правових актів; надання консультацій з впровадження нових технологій і стандартів; здійснення фінансового прогнозування та планування; взаємодія з державними органами в галузі економічного і науково-технічного співробітництва.

Орган регулювання в сфері телекомунікацій Киргизії здійснює державний контроль за дотриманням законодавства в галузі зв’язку; забезпечує виконання вимог законодавства з підтвердження відповідності при виробництві, експлуатації обладнання і технічних засобів зв’язку; визначає порядок розподілу та використання ресурсу нумерації відповідно до Національного плану нумерації мереж зв’язку Киргизії; здійснює контроль спільного використання мереж електрозв’язку загального користування та моніторинг дотримання вимог міжмережного з’єднання; забезпечує рівний доступ усіх користувачів до мереж електрозв’язку загального користування та послуг електрозв’язку загального користування на основі якісного надання послуг та дотримання конфіденційності повідомлень, а також збереження в таємниці приватної інформації про користувачів; здійснює виділення/присвоєння номіналів, смуг радіочастот відповідно до Національної таблиці розподілу радіочастот Киргизії; здійснює ліцензійну діяльність відповідно до законодавства; здійснює державний контроль за якістю наданих послуг зв’язку, за відповідністю діяльності юридичних і фізичних осіб, які отримали частотне присвоєння.

1. Орган управління Молдови в сфері телекомунікацій, відповідно до покладених на нього завдань, розробляє і проводить державну політику побудови інформаційного суспільства, методологію інформаційного будівництва та нормативно-правового регулювання в сфері інформатизації, електрозв’язку, формування державних інформаційних ресурсів та забезпечення доступу до них, а також систем телевізійного мовлення і радіомовлення, використання та конверсії радіочастотного спектра; розробляє і координує дії з реалізації Національної стратегії та Плану дій «Електронна Молдова», забезпечення моніторингу, аналізу та прогнозування розвитку інформаційного суспільства в Республіці Молдова; координує розробку проектів державних програм з інформатизації, інформаційних систем державного значення, інформаційно-комунікаційної інфраструктури, мережі передачі даних, вдосконалення та розвитку інтегрованої системи національних інформаційних ресурсів і технологій, доступу до них. Також розробляє нормативно-правову базу в галузі інформаційно-комунікаційних технологій, формування, використання та захисту державних інформаційних ресурсів і мереж; координує розробку та впровадження системи «Електронний уряд» для забезпечення транспарентності діяльності органів публічної влади, спрямованої на надання публічних послуг за допомогою впровадження інформаційно-комунікаційних технологій; формує єдину систему кодування і класифікації на території Молдови та веде національний банк класифікаторів за напрямами своєї діяльності; розробляє умови ліцензування в області інформатизації.
2. Орган управління в сфері телекомунікацій України забезпечує формування і реалізацію державної політики у сферах захисту державних інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, криптографічного та технічного захисту інформації, використання та захисту державних електронних інформаційних ресурсів, телекомунікацій, користування радіочастотним ресурсом України, забезпечує нормативно-правове регулювання, технічне регулювання, здійснює державний контроль за додержанням вимог законодавства, а також технічних вимог нормативних документів у сфері надання послуг електронного цифрового підпису, розробляє та здійснює заходи щодо розвитку телекомунікаційних мереж, поліпшення їх якості, забезпечення доступності та сталого функціонування, сприяє інтеграції сфер телекомунікацій, користування радіочастотним ресурсом України у світовий інформаційно-комунікаційний простір.

Основні завдання органу регулювання у сфері телекомунікацій такі: здійснення державного регулювання та нагляду в сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом, використання інфраструктури з метою максимального задоволення попиту споживачів на послуги зв’язку та інформаційні послуги, створення сприятливих умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, розвитку та модернізації телекомунікаційних та інформаційно-телекомунікаційних мереж з огляду на інтереси національної безпеки; забезпеченні ефективного користування радіочастотним ресурсом і функціонування ринку телекомунікаційних, інформаційно-телекомунікаційних, інформаційних послуг на основі збалансування інтересів суспільства, суб’єктів господарювання та споживачів цих послуг; сприяння розвитку конкуренції та підприємництва, забезпечення рівноправних умов діяльності суб’єктів господарювання всіх форм власності; вдосконалення механізму регулювання ринкових відносин у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом; забезпечення системності, комплексності та узгодженості розвитку інформатизації та інформаційного суспільства в державі.

Підсумовуючи, можна зробити висновок, що в країнах, у яких на ринку телекомунікацій присутній як орган управління, так і орган регулювання, до повноважень органу управління відносять формування та реалізацію державної політики, державний контроль за додержанням вимог законодавства, розробку та здійснення заходів щодо розвитку телекомунікаційних мереж, поліпшення їх якості, забезпечення доступності та сталого функціонування. А орган регулювання повинен сформувати прозорий механізм ліцензування, забезпечити надання універсальних послуг, обов’язкове взаємоз’єднання мереж, розробити прозору тарифну політику на ринку, здійснювати нагляд за ринком та сприяти розвитку конкуренції.

Дослідження, проведені у цьому підрозділі, дозволяють дійти висновку, що основними завданнями регулювання ринку телекомунікацій є формування прозорого механізму ліцензування, забезпечення надання універсальних послуг, забезпечення обов’язкового взаємоз’єднання мереж, розроблення прозорої тарифної політики на ринку, здійснення нагляду за ринком та сприяння розвитку конкуренції.

2. Системи адресації зі змінним розміром мережної адреси

Складний та тривалий шлях еволюції телекомунікаційних технологій, що застосовуються сьогодні в телекомунікаційних мережах, призвів до появи проблеми надлишковості службової інформації. Це пояснюється, насамперед, необхідністю узгодження роботи протоколів різних рівнів моделі OSI між собою. Така необхідність виникла ще на зорі формування сучасної телекомунікаційної інфраструктури, коли на шляху між відправником та одержувачем інформація могла проходити крізь десятки сегментів, що побудовані за різними технологіями. Однак уже сьогодні, зокрема завдяки зростаючій популярності технології Ethernet, щодо службових, корпоративних або навіть операторських мереж спостерігається уніфікація технологій, що наштовхує винахідників на ідеї поєднання частини рівнів моделі OSI (Open System Interconnection) з метою спрощення реалізації та підвищення ефективності роботи мереж [1].

Одним з найбільш дієвих та поширених механізмів такої оптимізації є вико­ристання мережних адрес (ідентифікаторів) змінного розміру [3]. Слід, однак, зазначити, що, висуваючи свої ідеї зі зменшення протокольної надлишковості, ви­нахідники подекуди не поглиблюються в можливість їх практичної реалізації і, зважаючи на це, більшість таких ідей залишається лише в теорії.

Низка відомих сьогодні систем адресації зі змінним розміром мережної адреси, які передбачають використання Ethernet мереж для транспортування навантаження, використовує для ідентифікації вузлів поля «MAC-адреса одержувача» та «MAC-адреса відправника» стандартного Ethernet-кадру [4]. Це стає можливим завдяки тому, що MAC-адреси при передачі кадрів мережею комутаторами не аналізуються (якщо такий режим не застосовується спеціально), а лише перевіряються на предмет збігу із записами в таблицях комутації.

Саме цей принцип покладено в основу запропонованої технології ЕХ [4], яка базується на модифікації технології Ethernet та передбачає використання службової інформації протоколів транспортного, мережного та канального рівнів у складі єдиного заголовку змінного розміру.

Очевидно, що застосування цієї технології передбачає створення досить великих мереж, які працюють на базі однієї технології канального рівня. Однак зважаючи на те, що технологія Ethernet використовує плоску систему MAC-адресації [5], у великих Ethernet-мережах збільшуються розміри таблиць комутації, що часто призводить до збільшення часу обробки кадрів.

Задля подолання цієї проблеми технологія ЕХ передбачає використання ієрархічних систем адресації із розділенням адреси на мережну частину та вузлову. Саме цей принцип покладено в основу методів змінної довжини маски підмережі

VLSM (Variable Length Subnet Mask) та безкласової адресації CIDR (Classless Inter­Domain Routing), які сьогодні широко використовуються в TCP/IP-мережах [6].

Довжина адреси в технології ЕХ може бути двох типів: динамічно змінювана або фіксована та поділена на три класи (з погляду особливостей практичної реалізації) відповідно до її розміру - менша, дорівнює 6 байтам або більша за цю величину.

Слід також зазначити, що можливість використання технології ЕХ без заміни мережного обладнання визначається розрядністю адреси та налаштуванням існючого обладнання.

Так, наприклад, при використанні адреси розміром 6 байт є можливість застосовувати звичайні Ethernet-комутатори. Однак слід зазначити, що в 6 байтах адреси буде й інформація щодо протоколів вищого рівня (номери портів тощо), яка весь час змінюватиметься, що призведе до появи в мережі широкомовних штормів.

При використанні мережних адрес з розміром менше 6 байт застосування мережних карт, інстальованих у сучасних комп’ютерах, комутаторах та маршрутизаторах залишається можливим лише у випадку доповнення адреси 48 біт однаковим заповнювачем (із частковою втратою ефективності). В іншому випадку до складу 6 байт, що порівнюються комутаторами в таблицях комутації, потраплятиме змінна інформація, що, як і в попередньому випадку призведе до широкомовних штормів у мережі.

У свою чергу, при використанні адрес з розміром понад 6 байт, в яких адресна інформація вузла обіймає перші 6 байт, а решта адреси містить інформацію вищих рівнів моделі OSI, залишається можливість використання вже існуючих комутаторів без їх заміни або перепрограмування.

Очевидно, що використання мережних адрес з динамічно змінюваним розміром накладає такі самі обмеження на існуючу телекомунікаційну інфраструктуру.

Прикладами типового місця застосування альтернативної мережної технології ЕХ є мережа датацентру, ядро мережі оператора зв’язку, корпоративні мережі, які характеризуються передачею великих обсягів даних або великою інтенсивністю мережних запитів.

Переведення таких мереж на використання технології ЕХ дозволить зменшити час передачі корисних даних між вузлами мережі, що, у свою чергу, зменшує загальний час роботи мережних вузлів в активному стані та, як наслідок, зменшує енергоспоживання мережних пристроїв, їх тепловиділення, споживання електроенергії пристроями кондиціювання. За рахунок зменшення часу на передачу даних вивільняється частина каналу зв’язку, який є продуктом комерціалізації, тобто збільшується кількість ресурсів, які можна надавати в оренду [4]. Збільшення швидкодії мережі покращує показник часу доступності серверів (аптайм), що є основним критерієм оцінки якості роботи датацентру. Завдяки цьому зменшиться час роботи мережних сервісів, якими користуються клієнти. Наприклад, якщо на певних серверах датацентру розміщена електронна бібліотека, то користувачі бібліотеки витрачатимуть менше часу на завантаження ресурсів бібліотеки, як наслідок, частіше обиратимуть саме цю бібліотеку за рахунок її швидкодії. Серед актуальних можливих галузей застосування технології можна виділити також кліматичні дослідження, дослідження космічних просторів, геодезичні обчислення тощо.

Варті окремої уваги пошукові системи та соціальні мережі. Компанії, які володіють такими системами, як правило, мають власні датацентри. Для таких компаній переваги переведення мережі на використання технології ЕХ особливо відчутні: окрім заощадження ресурсів, за рахунок збільшення швидкодії мережного оточення вони зможуть збільшити прихильність своїх користувачів та залучити нових.

Технологія ЕХ може бути використана і в корпоративних (наприклад, банківських) мережах і мережах передачі даних великих підприємств та їх філіалів. При цьому основними перевагами переведення мережі підприємства на альтернативну технологію можна вважати збільшення швидкодії мережі та звільнення частини пропускної спроможності каналів зв’язку, що поєднують філіали з головним офісом.

Зрозуміло, що заходи, які слід провести для переведення мережі на викорис­тання альтернативної технології, визначаються, насамперед, наявним в мережі обладнанням та розміром адреси, який планується використовувати. Для розрахунку економічного ефекту від упровадження альтернативної мережної технології авторами було запропоновано відповідну методику [4].

Залежно від вищезазначених факторів можна визначити спосіб практичної реалізації технології, що передбачає використання адрес змінного розміру. Так, наприклад, зважаючи на очевидну неефективність застосування мережних адрес розміром менш ніж 6 байт при збереженні існуючої мережної архітектури (із використанням Ethernet комутаторів), така реалізація є доцільною лише за умов розробки (перепрограмування) апаратної платформи комутаторів (зважаючи на ефект широкомовного шторму). Однак така сама схема (використання адрес розміром менш ніж 6 байт) є цілком припустимою при організації з’єднання між двома вузлами в режимі «точка - точка».

Також на спосіб реалізації технології зі змінним розміром мережної адреси безпосередньо впливають вимоги до взаємодії із мережами, що побудовані із використанням інших технологій. Так, наприклад, якщо необхідно забезпечити прозоре транспортування навантаження з однієї мережі до іншої (за умов використання різних технологій), виникає необхідність розробити відповідний програмний або програмно-апаратний шлюз із двома типами інтерфейсів. Якщо необхідно лише поєднати дві мережі, що використовують альтернативну технологію, через мережу, побудовану на основі іншої технології, можна обмежитися розробкою відповідного тунелю.

Серед основних способів внесення змін до програмного забезпечення вузлів мережі з метою практичної реалізації технології ЕХ слід зазначити:

- розробку програмного забезпечення драйвера віртуального мережного адаптера, що приймає класичні ІР-пакети та пересилає їх у вигляді модифікованих Ethernet кадрів, в яких адреса відправника заповнюється корисними даними;

- розробку програмної бібліотеки, яка дозволяє формувати для передавання даних модифіковані Ethernet кадри, в яких адреса відправника заповнюється корисними даними;

- розробку віртуального ргоху-серверу в межах вузла (або сервера), який приймає класичні ІР-пакети та забезпечує їх двостороннє перетворення в модифіковані Ethernet кадри, в яких адреса відправника заповнюється корисними даними;

- розробку програмного шлюзу та/або тунелю, що дозволяє перетворювати класичні ІР-пакети до модифікованих Ethernet кадрів (та навпаки) або здійснювати їх прозоре тунелювання крізь класичну ІР-мережу. У свою чергу, основним способом внесення змін до мережної інфраструктури залишається розробка нового апаратного комутуючого маршрутизатора із підтримкою адрес зменшеного (змінного) розміру на користь збільшення обсягів передавання корисних даних.

У разі використання існуючого програмного забезпечення в операційних системах з відкритим вихідним кодом підтримка нової технології на вузлах (для всіх розмірів мережної адреси) мережі передбачає реалізацію власного драйвера віртуального мережного адаптера. У свою чергу нове програмне забезпечення може розроблятися вже із використанням спеціалізованої бібліотеки, яка забезпечує пряме формування кадрів канального рівня. Винятком є тільки існуюче програмне забезпечення, що працює на пропрієтарних операційних системах. Можливим рішенням для цього випадку може стати розробка спеціального програмного продукту (шлюзу або посередника) для забезпечення прозорого перетворення навантаження.

Що стосується модифікації мережного обладнання, то це (здебільшого) має сенс лише для випадків, коли розмір мережної адреси менший за 6 байт. У цьому випадку необхідно розробляти як комутатори, так і маршрутизатори, а у випадку використання адрес 6-байтового (або більшого) розміру - лише маршрутизатори (стандарті комутатори другого рівня будуть працювати при цьому в штатному режимі)

3 Інтегрована технологія телекомунікацій UA-ITT

Одним з головних досягнень у галузі телекомунікацій є мережа Internet. В її основу покладено такі базові принципи, як пакетний обмін даними, децентралізацій взаємодії об’єктів Мережі, ієрархічна доменна веб-адресація інформаційних ресурсів [7,8]. Метод комутації пакетів, характерний для комп’ютерних мереж, дозволяє істотно підвищити рівень ущільнення каналів зв’язку порівняно з методом комутації каналів, що є притаманним для традиційної телефонії. Це досягається за рахунок статистичного мультиплексування даних (тобто змішування в одному каналі окремих пакетів від різних повідомлень). Економічна ефективність комутації пакетів стимулювала швидкий розвиток світової мережі Інтернет, у т.ч. застосування комп’ютерних мереж для передачі не традиційного для пакетної комутації трафіка реального часу (голос, відео, мультимедійні дані тощо).

Практичне втілення зазначених ідей потребувало чимало зусиль, а відсутність загальноприйнятої системної концепції побудови комп’ютерних мереж на ранньому етапі розвитку зумовила появу різноманіття мережних технологій і протоколів. Об’єднуючим фактором для взаємодії різних типів мереж став Інтернет- протокол (IP), який є базовим у стеку протоколів TCP/IP і сьогодні має дві основні стандартизовані версії (IPv4 та IPv6). Версія IPv4 з 32-бітовою IP-адре сацією є найбільш поширеною у світі, але адресний простір цього протоколу вже вичерпано [9]. Версія IPv6 має довжину адреси у 128 біт, що забезпечує практично необмежений розмір адресного простору, але впровадження IPv6 є поступовим і довготривалим процесом, протягом якого мають співіснувати IP-мережі обох типів (версій 4 та 6). Це потребує нових капітальних інвестицій і додатково ускладнює міжмережну взаємодію, однак не обіцяє помітного виграшу стосовно якості сервісу і вартості послуг для клієнтів мережі [10]. Окрім того, передача трафіка реального часу IP-мережами передбачає багаторівневу інкапсуляцію даних, що ускладнює управління мережами і завантажує канали зв’язку та мережне обладнання службовою інформацією (яка міститься у численних заголовках різних рівнів [11.11]). Ці фактори певною мірою стримують дальший розвиток мультисервісних мереж на базі IP.

В останнє десятиліття йде активний пошук шляхів створення мереж нового покоління (NGN) у напрямі конвергенції різних типів мереж та інтеграції різноманітних послуг. У рамках ITU розроблено концепцію NGN з розмежуванням транспортної і сервісної функцій та підтримкою мережних послуг на базі пакетної комутації [12]. Важливим етапом реалізації цієї концепції є розробка стандартів транспортного профілю протоколу MPLS (проект MPLS-TP) [13].

Існуючі підходи побудови NGN переважно орієнтовані на поступове заміщення протоколу IPv4 протоколом IPv6, який має набагато більший ресурс адресного простору, а також додаткові можливості керування потоками і управління якістю сервісу. Цей підхід є зваженим компромісом між існуючою світовою інформаційно-комунікаційною інфраструктурою і новими викликами часу на найближчу перспективу. Однак передача трафіка короткими пакетами (наприклад, голосового трафіка) IP-мережею економічно недоцільна внаслідок низького використання потенційних ресурсів мережного обладнання та каналів зв’язку [15]. Тому розробка нових, більш гнучких і ефективних способів передачі різних типів трафіка на базі пакетного принципу комутації є актуальною науково-технічною проблемою, з погляду побудови мереж більш віддалених майбутніх поколінь.

Так, наприклад, групою дослідників була проведена комплексна науково- дослідна робота з метою обґрунтування основних принципів побудови інтегрованої технології телекомунікацій (Integrated Telecommunication Technology - ITT), як єдиної платформи для створення перспективних інфокомунікаційних мереж майбутнього покоління. Сформульована мета розбивається на чотири порівняно самостійні напрями:

1.Побудова нової моделі взаємодії відкритих систем і багатопрофільного мережного мета-протоколу (Multipurpose Network meta-Protocol - MNP) за методом динамічного управління цифровими потоками (Dynamic Flow Control - DFC). Метод DFC об’єднує в собі переваги мереж з комутацією каналів і мереж з пакетною комутацією; він пристосований для передачі різноманітних видів трафіка від звичайної телефонії та пакетного обміну файлами до мультимедійних повідомлень з виконанням вимог найвищої якості надання послуг.

2.Побудова адресного простору, який має властивості мінімальної надмірності, але разом з тим дозволяє практично необмежено збільшувати та розширювати цей простір через необхідність, без зміни базових мережних протоколів.

3.Розробка плану переходу від існуючих технологій до ITT.

4.Створення відповідного мережного обладнання.

Запропоновані нові підходи захищені трьома авторськими свідоцтвами на право інтелектуальної власності [16-18], а також сьома патентами України [19-24, 36], в яких сформульовані ключові способи побудови стека мережних протоколів, методів гнучкої динамічної адресації вузлів, абонентів і прикладних процесів у мультисервісній мережі, а також адаптивної до типів трафіка комутації статистично мультиплексованих цифрових потоків у телекомунікаційних каналах зв’язку. Впровадження результатів роботи передбачає створення двох базових функціональних модулів - мережного адаптера і комутатора технології ITT. Оскільки ця технологія запропонована в Україні, автори позначили її UA-ITT. Далі розглянуто детальніше принципи вирішення першого з чотирьох зазначених вище завдань.

3.1 Модель взаємодії відкритих систем ITT

Модель взаємодії відкритих систем ITT передбачає три рівні (рис. 3.1). Нижній (фізичний) рівень моделі ITT охоплює фізичний і частково канальний рівень семирівневої моделі взаємодії відкритих систем OSI. Другий (мережний) рівень моделі ITT об’єднує три рівні моделі OSI (мережний, транспортний, сеансовий), а також частково канальний рівень OSI. Верхній (прикладний) рівень моделі ITT об’єднує представницький і прикладний рівні моделі OSI. Технологія UA-ITT позиціонується як перший і другий рівні трирівневої моделі взаємодії відкритих систем ITT (рис.3.1). Відповідність моделі ITT і сучасної моделі Інтернет TCP/IP легко встановлюється з цього ж рисунка. Згідно з функціональною моделлю NGN у концепції ITU-T, технологія UA-ITT підтримує транспортну функцію мережі.

Протокольною одиницею даних фізичного рівня моделі ITT є байт, який має два можливі типи: байт команди (Command Byte - CB) і байт даних (Data Byte - DB). Фізичний рівень ITT забезпечує взаємодію двох суміжних об’єктів мережі на рівні обміну байтами. Протокольною одиницею даних мережного рівня є сегмент, який також має два можливі типи: сегмент команди, що утворюється безперерв­ною послідовністю байтів команд, і сегмент даних - безперервна послідовність байтів даних. Мережний рівень ITT забезпечує взаємодію двох або декількох об’єктів мережі на рівні обміну сегментами даних у з’єднанні заданого типу або без з’єднання (з підтримкою відповідних показників якості обслуговування). Мережний рівень ITT, на відміну від фізичного рівня, передбачає вирішення завдань маршрутизації і комутації сегментів даних, що здійснюється за допомогою сегментів команд



Рис. 3.1 Моделі взаємодії відкритих систем OSI, TCP/IP, ITT

3.2 Багатоцільовий мережний мета-протокол MNP

Технологія ITT впроваджує зазначений вище метод динамічного управління цифровими потоками (DFC), який дозволяє оперативно адаптувати механізми маршрутизації і комутації до різних складових мультиплексного цифрового потоку в каналі зв’язку. Метод DFC використовує спеціально розроблений багатоцільовий мережний мета-протокол. Мета-протокол MNP, на відміну від відомих мережних протоколів (наприклад, протоколів стека TCP/IP), формалізує побудову достатньо великої кількості різноманітних прикладних протоколів (профілів MNP) на загальній основі. MNP описує фізичний і мережний рівні моделі ITT, а також взаємодію між цими двома рівнями.

Згідно з MNP, фізичний рівень формує і передає на мережний рівень мульти- плексний потік окремих байтів, який логічно розділений на дві складові потоку: потік байтів команд (Command Byte Stream - CBS) і потік байтів даних (Data Byte Stream- DBS) (рис. 3.2).

Мережний рівень розподіляє CBS і DBS на окремі сегменти команд (Command Segments - CS) і сегменти даних (Data Segments- DS) - рис. 3.3. Протокол MNP не накладає обмежень на кількість командних байтів чи байтів даних, що створюють відповідні сегменти на мережному рівні. Таким чином, MNP реалізує принцип статистичного мультиплексування, притаманний сучасним IP-мережам, але при цьому не потребує заголовків пакетів з фіксованою структурою. Натомість для управління передачею сегментів даних використовуються сегменти команд, структура яких динамічно змінюється й адаптується в процесі передачі.

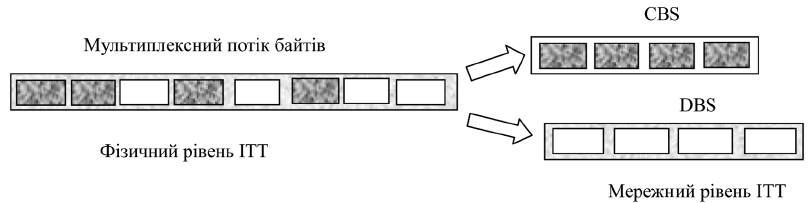


Рис. 3.2 Фрагмент цифрового потоку на фізичному та мережному рівнях ITT

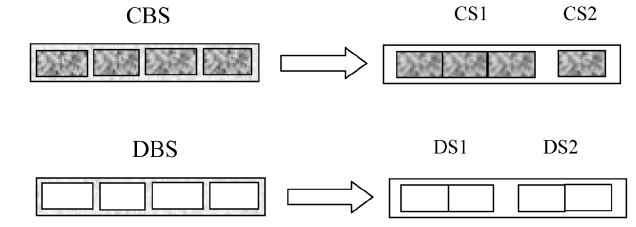


Рис. 3.3 Розподіл цифрового потоку на мережному рівні ITT

На відміну від широковідомої концепції NGN «All over IP» технологія ITT орієнтована на з’єднання і передбачає підтримку багатоканального з’єднання кінцевих абонентів лише засобами самої мережі. Такий підхід, звичайно, відповідає ключовому принципу ITU-T про розмежування транспортної і сервісної функцій в мережах NGN.

У технології ITT типи з’єднань визначаються за двовимірною шкалою якості сервісу (QoS) [25]. Перший напрямок шкали QoS визначає середню (за певний період) пропускну спроможність з’єднання, а другий напрямок - стабільність пропускної спроможності в часі. За кожним з двох напрямків шкали QoS тип з’єднання змінюється поступово з заданою дискретністю.

В ITT визначено поняття окремого цифрового потоку (Single Digital Flux - SDF) як послідовність сегментів даних у каналі зв’язку (одноканальна фізична лінія або окремий мультиплексний тракт передачі), які мають специфічний набір параметрів управління відповідно до заданого типу з’єднання, а також послідовність сегментів команд, які виконують функцію управління.

Окремі сегменти даних SDF в ITT не мають індивідуальних заголовків (як це прийнято в технології IP), натомість роль заголовків виконують параметри спеціальної структурованої таблиці управління потоками (Flow Control Table - FCT). Для передачі безперервної послідовності сегментів даних одного потоку SDF, попередньо, за допомогою однієї чи декількох сегментів команд, передається набір параметрів, необхідний для управління сегментами зазначеного SDF (наприклад, номер попередньо встановленого з’єднання або конкретний набір параметрів: адреси одержувача та відправника, тип з’єднання або клас сервісу, максимальна тривалість цього з’єднання тощо). Будь-яка команда управління потоками модифікує один чи декілька параметрів таблиці FCT.

Загальну структуру таблиці FCT показано на рис. 3.4. Для кожної пари суміжних об’єктів мережі підтримуються по дві копії FCT у кожному з напрямків передачі. Право модифікації таблиць FCT належить передавальній стороні. Перед початком передачі чергового сегмента даних на передавальній і прийомній сторонах повинні бути встановлені однакові значення відповідних параметрів управління. Якщо перед цим передавальна сторона змінила один чи декілька таких параметрів, то, насамперед, вона передає один чи декілька сегментів команд, які модифікують FCT на приймальній стороні (тобто логічно синхронізують обидві таблиці FCT - на передавальній та приймальній сторонах). Після цього передається один чи декілька сегментів даних, які належать одному виділеному цифровому потоку (SDF) у загальному мультиплексному цифровому потоці (Multiplexed Digital Flow - MDF). Довжина окремих сегментів даних, а також загальна кількість сегментів даних у серії сегментів одного SDF не обмежується протоколом MNP. На відміну від технології IP параметри управління потоком передаються не для кожного сегменту даних, а лише один раз для всієї серії сегментів одного потоку. Це істотно зменшує обсяг службової інформації в загальному потоці при передачі даних серіями сегментів.

Протокол MNP не накладає обмежень на розмір таблиці FCT і склад її параметрів (тобто вона є відкритою для розвитку). Для управління кожним сегментом даних використовується деяка підмножина параметрів таблиці FCT. Кожна така підмножина параметрів утворює профіль протоколу MNP. Усі профілі MNP описані та індексовані в спеціальному розділі таблиці FCT. Поточний номер профілю MNP також є параметром таблиці FCT, який модифікується та синхронізується на передавальній і приймальній сторонах.

Таблиця ЕСТ містить у собі три вбудовані таблиці: таблиця 1 - «Профілі МНР», таблиця 2 - «Діючі з’єднання», таблиця 3 - «Параметри управління потоками», а також три окремі поля: поле 1 - «Номер поточного профілю МНР», поле 2 - «Номер рядка таблиці 2» і поле 3 - «Номер рядка таблиці 3».

Якщо поле 1 має значення від 1 і більше, то управління здійснюється згідно з відповідним профілем у таблиці 1; це відповідає режиму передачі без установлення з’єднання. Нульове значення поля 1 означає режим передачі в режимі установленого з’єднання; при цьому управління переключається на відповідний рядок таблиці 2 (номер цього рядка показано в полі 2).

У режимі без встановлення з’єднання вибір підмножини параметрів управління здійснюється згідно з поточним номером профілю MNP (поле 1) із відповідного рядка таблиці 3 (номер цього рядка показано в полі 3). Таблиця 3 щонайменше містить один рядок, в якому представлено набір параметрів управління. Таблиці 2 і 3 мають структуру стека (перший зайшов - останній вийшов).

Динамічна комутація потоків здійснюється таким чином. У режимі без встановлення з’єднання для комутації послідовної серії сегментів даних виділеного цифрового потоку SDF треба передати на приймальну сторону ненульовий номер профілю MNP (значення поля 1) і номер поточного рядка в таблиці 3 (значення поля 3), якщо цей рядок є в таблиці 3 на передавальній та приймальній сторонах. Якщо такого рядка нема, передавальна сторона формує на вершині стека (у першому рядку таблиці 3) необхідний набір параметрів управління, а далі передає на приймальну сторону набір команд, які утворюють новий перший рядок таблиці 3 на приймальній стороні; при цьому інші рядки таблиці 3 на передавальній та приймальній сторонах зміщуються на одну позицію стека, а останній рядок пропадає.

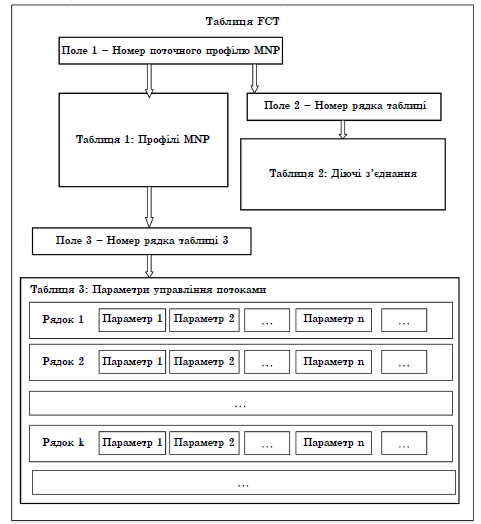


Рис. 3.4 Структура таблиці управління потоками FCT

Таким чином, при передачі даних в пакетному режимі без з’єднання набір параметрів управління для безперервного ланцюга сегментів одного потоку SDF необмеженої довжини передається лише один раз. За рахунок цього істотно знижується навантаження каналів зв’язку службовою інформацією порівняно з методом багаторівневої інкапсуляції даних у мультисервісних мережах чи базі IP.

У режимі передачі встановленим з’єднанням для комутації SDF треба передати нульовий номер профілю MNP і номер з’єднання (значення поля 2). Основним параметром управління в режимі передачі встановленим з’єднанням є номер з’єднання, за яким у таблиці 2 записані інші параметри (адреси відправника та одержувача повідомлення, тип обслуговування, тривалість з’єднання, номер вхідного та вихідного портів комутації тощо).

У технології ITT загальний мультиплексний цифровий потік (MDF) у каналі зв’язку визначається як випадкова послідовність сегментів даних і сегментів команд окремих SDF. Потік MDF за своєю структурою має ознаки так званого зворотного польського (або постфіксного) програмного коду, який використовується у багатьох мовах програмування інтерпретаційного типу (Forth, Perl, Python тощо). Отже, комутатор потоків SDF у технології ITT формально виконує функцію дискретного автомата, який обробляє відповідно заданому алгоритму одну вхідну послідовність команд для кожного порту вводу даних комутатора і перетворює її у декілька вихідних послідовностей команд і даних для кожного з вихідних портів комутатора. Це створює умови для розробки широкого спектра конкретних протоколів і апаратно-програмних драйверів для передачі різних типів трафіка в мультисервісних мережах на базі ITT з підтримкою самих високих стандартів якості.

Реалізація принципів динамічного управління потоками за технологією ITT передбачає побудову спеціалізованих мережних адаптерів фізичного рівня (які забезпечують взаємодію двох суміжних вузлів мережі ITT), а також комутаторів цифрових потоків. Експериментальні зразки двох адаптерів ITT, які підключаються до стандартної шини USB2, створені в ОНАЗ ім. О.С. Попова і пройшли успішні попередні тестування. Базові функції комутатора потоків ITT відтворені на рівні імітаційної моделі у середовищі Linux.

4. РОЗВИТОК СИТУАТИВНИХ МЕРЕЖ

4.1 Класи мереж за моделями керування ресурсами

Поняття «керування ресурсами телекомунікаційної мережі» може мати декілька значень. Перше значення містить у собі процес управління вузлами та параметрами телекомунікаційної мережі, у такому разі під поняттям ресурсів розуміють саму мережу. Наприклад, віддалене керування маршрутизатором, розподіл пропускної здатності каналу передавання даних між користувачами, отримання сигналів щодо збоїв та аварій у мережі. Друге значення поняття «керування ресурсами телекомунікаційної мережі» містить у собі процес управління ресурсами, які розміщено на кінцевих пристроях телекомунікаційної мережі. Прикладами відповідних пристроїв можуть бути робочі станції користувачів, сервери, периферійне обладнання, що має мережний інтерфейс, тощо. Під самими «ресурсами» можуть матися на увазі як інформаційні ресурси (файли різних форматів), так і доступ до послуг деяких периферійних пристроїв (принтерів, факсимільних апаратів, сканерів).

Зазначимо, що не існує єдиної моделі керування ресурсами телекомунікаційної мережі, проте можна говорити про класифікацію різних мереж, що використовують різні моделі керування ресурсами. Відповідну спрощену класифікацію показано на рис. 4.1. Розглянемо її детально.

До мереж без механізму централізованого керування ресурсами належать мережі, що не містять програмних або апаратних засобів, які б надавали користувачам інформацію щодо наявних у мережі інформаційних ресурсів, а також розподіляли права доступу до цих ресурсів. Яскравим прикладом мереж з існуючою мережною інфраструктурою є проводові або безпроводові однорангові мережі. У таких мережах користувачі можуть бути непоінформовані щодо наявності інших користувачів, а також можливих ресурсів, які в них є. Перед початком інформаційного обміну користувачі повинні домовитися щодо можливості надання інформаційних ресурсів, а також надати адресу відповідного кінцевого пристрою (ІР-адресу, доменне ім’я тощо).



Рис. 4.1 Класифікація телекомунікаційних мереж за різними методами керування ресурсами

До мереж із самоконфігурацією мережної інфраструктури без механізму керування телекомунікаційними ресурсами належать так звані «безпроводові «adhoco-мережі». До основних характеристик цих мереж можна віднести такі:

- Використання того самого механізму канального рівня при обміні інформацією. Найпоширенішими сьогодні є протоколи канального рівня IEEE 802.11 (Wi-Fi).

- Кожен з вузлів мережі, що формується, є попередньо сконфігурованим (наприклад, IP-адреси мережних інтерфейсів), а користувачі заздалегідь поінформовані про існування інших вузлів та ресурси, які є у кожного з них.

Такий підхід є цілком виправданим у разі, коли він застосовується в мережах, які розгортаються під час військових конфліктів, техногенних або природних катастроф та в інших аналогічних випадках. У цьому випадку основним завданням таких протоколів є знаходження необхідних (заздалегідь відомих) вузлів в мережі та організація інформаційного обміну між ними.

Усі існуючі сьогодні механізми керування мережами, в яких кінцеві пристрої самостійно формують взаємозв’язки між собою в децентралізованому середовищі передавання даних (протоколи маршрутизації «ad hoco-мереж), можна умовно поділити на декілька класів:

- Проактивні. Прикладами таких механізмів можна назвати: безпроводовий протокол маршрутизації (WRP - Wireless Routing Protocol)[11.26], оптимізований протокол стану каналу зв’язку (OLSR - Optimized Link State Routing Protocol) [11.27], послідовності призначення векторної відстані (DSDV - Destination- Sequenced Distance Vector) [28] тощо. Більшість із проактивних протоколів засновані на існуючих алгоритмах маршрутизації для II мереж, наприклад алгоритмі Беллмана-Форда або алгоритмі Дейкстри.

- Реактивні. Прикладами таких механізмів можна назвати: протокол вектора відстані за запитом (AODV - Ad Hoc On Demand Distance Vector) [29], протокол динамічного джерела маршрутизації (DSR - Dynamic Source Routing protocol) [30] тощо. Більшість з зазначених механізмів не базуються на існуючих алгоритмах маршрутизації, а розроблені на нових принципах передавання маршрутної інформації, які полягають у можливості динамічного формування маршрутів, тобто в разі потреби.

- Гібридні. Прикладами таких протоколів є зоновий протокол маршрутизації (ZRP - Zone Routing Protocol) [11.31], ієрархічний протокол канального стану, заснований на зонах (ZHLS - Zone-Based Hierarchial Link State) [11.32] тощо. Ці механізми є складними в роботі та реалізації і передбачають розділення абонентів на географічні зони. У середині кожної зони використовуються проактивні механізми пошуку відповідного абонента, а між зонами - реактивні механізми.

- Незважаючи на різноманіття способів встановлення зв’язків і формування таблиць маршрутизації, «ad hoco-мережі залишаються в загальному випадку мережами без механізму централізованого керування ресурсами і можуть використовуватися лише тоді, коли кожний з користувачів мережі заздалегідь знає свою роль і місце в мережі.

Мережі з повним або частковим методом керування інформаційними ресурсами сьогодні найбільш поширені. До методів часткового керування слід віднести локальні або глобальні пошукові системи (наприклад «Google»), які надають користувачу інформацію про існування ресурсів відповідно до його запиту. Також до систем часткового централізованого керування можна віднести локальні сервери з файловим архівом, локальні web-сервери тощо. Загальною характеристикою систем з частково централізованим способом керування ресурсами є необхідність самого користувача. Тобто такі системи використовуються лише при наявності бажання у користувача ними скористатися.

До методів повного керування слід віднести служби централізованого керування доступом до ресурсів користувачів. Прикладами таких служб можуть бути загальновідома NFS (Network File System), розроблена для операційних систем типу «Unix», а також AD (Active Directory), розроблена для мережних операційних систем типу «Windows». Зазначимо, що найчастіше кожна із зазначених мережних служб керування ресурсами надає можливість управління розподіленням прав доступу до інформаційних ресурсів у комп’ютерній мережі. Однак можливе використання централізованих систем реєстрації користувачів типу «Kerberos» разом із зазначеними службами, що надає високий ступінь гнучкості. У цьому разі користувач може не мати постійного робочого місця і, використовуючи свій обліковий запис, отримувати доступ до своїх інформаційних ресурсів з будь-якої робочої станції в мережі.

-Найбільш відомим сьогодні механізмом розподіленого керування ресурсами, який використовує вже існуючу мережну інфраструктуру, можна вважати протокол «Gnutella». Цей механізм часто використовується для обміну файлами в рамках мережі Інтернет. Основна відмінність зазначеного механізму від інших механізмів, що використовуються в мережах файлового обміну, є принципова відсутність центрального керуючого сервера. Вважається, що мережа починає формуватися тоді, коли один користувач «Gnutella» з’єднується з іншим користувачем, після чого вони можуть починати обмін доступною інформацією.

4.2 Модель керування ресурсами ситуативних мереж

Існуючі методи і моделі керування ресурсами мережі не можуть використовуватись у випадках, коли абоненти мережі заздалегідь не пов’язані один із одним, не мають налаштоваьих мережних пристроїв (як у випадку з безпроводовими «ad bос»-мережами). У такому випадку кожен абонент повинен мати можливість не тільки самостійно визначити загальну кількість інших абонентів навколо нього, а також мати можливість отримати інформацію про інші наявні в мережі ресурси. До таких мереж, що мають вбудований механізм розподіленого керування, який самостійно формує мережну архітектуру, адресний простір і перелік існуючих ресурсів, належить механізм керування ситуативними мережами. Типовими прикладами ситуацій, в яких досить доречним є розгортання самокерованої ситуативної мережі, можуть бути:

- пересування великої кількості користувачів загальнодоступними транспортними засобами (потяги, літаки, автобуси тощо);

- перебування великої кількості людей в одному приміщенні (наприклад, під час виставок, конференцій, симпозіумів тощо);

- проживання в одному готелі, кемпінгу, будинку або на базі відпочинку;

- перебування групи людей в одному таборі у складі групи туристів (на відкритій місцевості вдалині від телекомунікаційної інфраструктури) тощо.

Характерними ознаками всіх наведених прикладів є:

- наявність групи користувачів, які зібралися разом на певний час (ситуативно) в одному географічно обмеженому районі місцевості;

- необхідність передавання даних між користувачами або надання інформаційно-комунікаційних послуг (обмін файлами, доступ до мережі Інтернет через термінал іншого користувача тощо);

- цілковита або часткова відсутність телекомунікаційної інфраструктури (кабельна інфраструктура, точки безпроводового доступу тощо), що унеможливлює або істотно обмежує процес обміну інформацією;

- користувачам заздалегідь невідомо, скільки людей з присутніх, які можуть і хочуть надавати інформаційно-комунікаційні послуги, а також які саме ресурси вони можуть отримати в мережі;

- мобільні пристрої користувачів можуть використовувати різні проводові або безпроводові технології передавання даних (Ethernet, WiFi тощо).

Технічне завдання встановлення з’єднання між двома вузлами ситуативної мережі вирішується шляхом трьох етапів. На першому етапі (рис. 4.2) вузол- ініціатор розсилає широкомовне повідомлення через усі задіяні користувачем мережні інтерфейси вузла (Wi-Fi, Ethernet тощо) .

Сусідні вузли, отримавши запит, аналізують його за відповідним алгоритмом та, модифікувавши, ретранслюють через усі свої задіяні інтерфейси. Таким чином, поступово, початковий запит поширюється ситуативною мережею, досягаючи її меж. Зауважимо, що кожний з вузлів, аналізуючи отримані повідомлення, обирає найкращій з можливих зворотних маршрутів до вузла-ініціатора і тільки після цього модифікує повідомлення, додаючи інформацію про цей маршрут, широкомовно відправляє через усі задіяні інтерфейси. Після процесу поширення інформації починається процес формування відповідей кожним вузлом мережі вузлу-ініціатору, куди вноситься інформація про оптимальний маршрут до кожного вузла, а також інформація про типи наявних ресурсів, що можуть надаватися в користування (файловий архів, доступ до мережі Інтернет тощо). Також зазначимо, що для забезпечення незалежності від протоколу ІР ідентифікація вузлів мережі при побудові маршрутів відбувається за МАС-адресами мережних інтерфейсів кожного з вузлів. У результаті роботи першого етапу механізму користувач вузла-ініціатора отримує всю інформацію про навколишню мережу та наявні в мережі типи ресурсів.

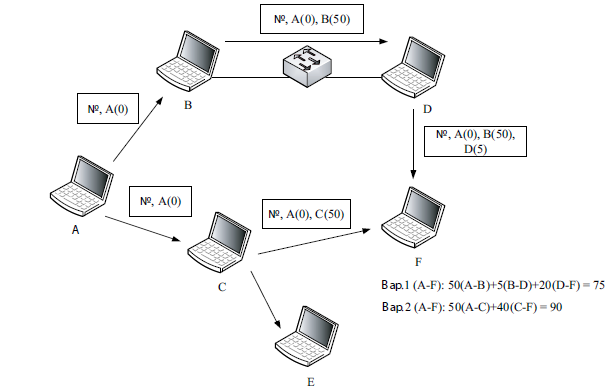


Рис. 4.2 Трансляція широкомовного повідомлення абонента-ініціатора через ситуативну мережу

На другому етапі (рис. 4.3) користувач вузла-ініціатора обирає вузол та тип ресурсів, про який хоче отримати більш детальну інформацію. Після цього вузол- ініціатор вже відомим маршрутом відправляє запит на деталізацію ресурсів, у відповіді на який міститься вся інформація про конкретний ресурс на віддаленому вузлі (наприклад, назва, тип та розмір файлів з файлового архіву).

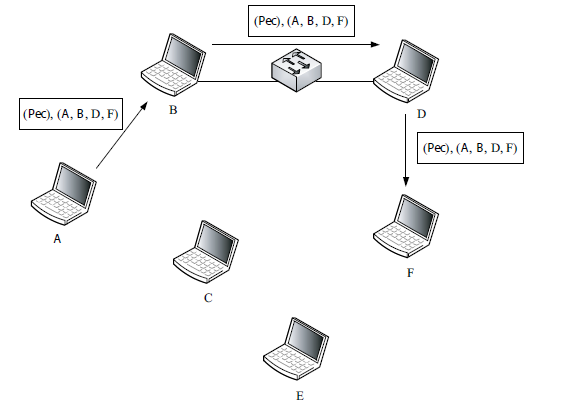


Рис. 4.3 Запит детальної інформації про доступні ресурси у віддаленого абонента

Після роботи другого етапу механізму користувач вузла-ініціатора, отримавши таким чином детальну інформацію про відповідні ресурси, може обрати конкретний ресурс, до якого він хоче отримати доступ. Після цього вузол-ініціатор починає третій етап роботи запропонованого способу - етап інформаційного обміну, з’єднуючись з віддаленим вузлом ситуативної мережі та отримуючи доступ до обраного абонентом ресурсу (наприклад, до текстового файла з файлового архіву). Також зазначимо, що при інформаційному обміні на другому та третьому етапах інформація про маршрут до віддаленого абонента передається у кожному блоці канального рівня, що дозволяє істотно скоротити навантаження на вузли мережі з причин відсутності потреби формування таблиці маршрутів на кожному з вузлів.

5. сучасні квантові технології захисту інформації

5.1 Загальна класифікація сучасних квантових технологій захисту інформації

Основна ідея квантових методів захисту інформації в телекомунікаційних мережах полягає в тому, що класична інформація (криптографічний ключ або відкритий текст повідомлення) кодується станами квантових систем і передається окремими квантовими частинками. Як такі квантові частинки в протоколах кван­тової криптографії використовують фотони, а як квантовий канал - оптоволоконні лінії або атмосферу (оптичний бездротовий канал). Згідно із законами квантової фізики, операції над квантовими системами призводять до змін їх станів. Тому зловмисник, який бажає перехопити інформацію, неминуче змінює стани фотонів, які передаються, що завжди можуть виявити легітимні користувачі. їх дальші дії залежать від того, який саме протокол і за яких умов реалізується.

Таким чином, квантові технології захисту інформації, що передається, дозволяють виявити атаку пасивного перехоплення (підслуховування) в каналі зв’язку, що не завжди можливо при використанні традиційних (класичних) методів. Виявлення такої атаки критичне як при розподіленні секретних ключів шифрування, так і при передаванні відкритих текстів. Квантові протоколи розподілення ключів дозволяють не тільки виявити атаку підслуховування, але й за допомогою постобробки переданої інформації видалити інформацію, яку міг отримати зловмисник, і, таким чином, забезпечити розподілення ключів з безумовною (теоретико-інформаційною) стійкістю. Аналогічно високий рівень безпеки може бути забезпечений при використанні квантових протоколів прямого безпечного зв’язку, які призначені для безпосереднього, тобто без шифрування, передавання відкритих текстів.

Нині до складу квантових технологій захисту інформації входять: квантове розподілення ключів [37-42], квантовий прямий безпечний зв’язок [40-46], квантове розділення секрету [47,48], квантовий потоковий шифр [49,50], квантовий цифровий підпис [51,52] та квантова стеганографія [53-55].

На рис. 5.1 наведено загальну схему класифікації квантових методів захисту інформації за їх призначенням, а також за використовуваними квантовими технологіями [42].

Вільність запропонованих нині протоколів квантової криптографії використовують дворівневі квантові системи - кубіти (qubit), що дозволяє передавати класичну інформацію бітами. Але інформаційну місткість квантових протоколів можна підвищити, використовуючи багаторівневі квантові системи, тобто передаючи класичну інформацію тритами, квартами тощо. Відповідно трирівнева квантова система отримала назву кутрит (qutrit), чотирирівнева - кукварт (ququart) тощо. У загальному випадку d-рівнева квантова система називається кудитом (qudit). З технічної точки зору, в протоколах квантової криптографії носіями як кубітів, так і багаторівневих квантових систем є фотони, але оперувати з багаторівневими системами дещо складніше, ніж з кубітами. Таким чином, протоколи квантової криптографії можна поділити на дві великі групи залежно від того, дво- або багаторівневі квантові системи в них використовуються (рис. 5.1).

З іншого боку, квантові системи, що складаються з двох або більшої кількості квантових частинок, можуть находитися в переплутаних станах, тобто в таких станах між цими частинками існують суто квантові кореляції. Локальні операції над однією з частинок переплутаного стану приводять до зміни всього стану. Це дозволяє кодувати класичну інформацію, діючи на одну з частинок, тоді як інша перебуває в іншого абонента квантового протоколу (наприклад, пінг-понг протокол). Використання властивостей квантових переплутаних станів дозволяє забезпечити високий рівень безпеки протоколів квантової криптографії, а також підвищити їх ефективність. Таким чином, протоколи квантової криптографії можна також поділити на дві великі групи залежно від того, одиночні або переплутані квантові системи в них використовуються (рис. 5.1).

Квантове розподілення ключів - сьогодні найбільш розвинений напрям квантових технологій захисту інформації як з теоретичного, так і з практичного погляду. На лабораторному обладнанні вже виконано велику кількість експериментів із квантового розподілення ключів, наприклад [38, 56-59]. Існують також комерційні системи, цілком придатні для інтеграції в сучасні телекомунікаційні мережі. З цих причин далі в цьому підрозділі монографії розглянуто тільки протоколи квантового розподілення ключів.



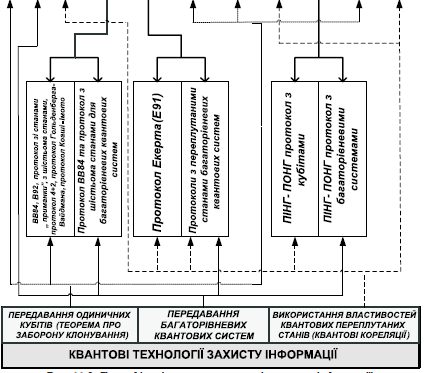


Рис. 5.1 Класифікація квантових методів захисту інформації

Основні властивості квантових систем, які використовуються у квантовій криптографії [37]:

1. Вимірювання фізичних характеристик квантових систем (спостережуваних)

У результаті процесу вимірювання деякої фізичної величини стан квантової системи змінюється. Це обумовлено впливом на квантовий об’єкт вимірювального приладу, який принципово неможливо зробити як завгодно малим. Чим точніше вимірювання, тим сильніший вплив, який здійснюється. І лише при вимірюваннях дуже малої точності вплив на об’єкт вимірювання може бути досить слабким.

Крім того, збурювання, яке вноситься взаємодією квантового об’єкта з вимірювальним приладом, може бути передбачено тільки статистично і тому його не можна усунути. Цей факт перебуває в різкому протиріччі з класичною теорією вимірювань, яка базується на припущенні, що взаємодія між об’єктом і приладом, якщо і не може бути зроблена як завгодно малою, то принаймні може бути точно врахованою, отже, у принципі її можна усунути.

1. Неможливість точного клонування невідомих квантових станів

Внаслідок лінійності й унітарності квантової механіки неможливо створити точну копію невідомого квантового стану. Таким чином, зловмисник не може виготовити точну копію кубітів або кудитів, що передаються комунікаційним каналом, щоб провести вимірювання над копією, а оригінал переслати законному користувачеві каналу, не проводячи над ним вимірювання. Цей факт лежить в основі більшості протоколів квантової криптографії, тому що змушує зловмисника вимірювати кудити, які передаються, або переплутувати їх зі своїми допоміжними квантовими системами, що призводить до зміни станів цих кудитів. Ці зміни станів, які передаються, можуть виявити законні користувачі, виконуючи квантові вимірювання й обмінюючись результатами цих вимірювань звичайним відкритим каналом зв’язку. Зазначимо, що ймовірність правильно клонувати довільний стан кубіту, створивши одну його копію, дорівнює 5/6 [37]. Якщо потрібно створити n копій невідомого стану кубіту, то ймовірність правильного клонування зменшується та при n→∞ прямує до 2/3 [37].

1. Неортогональні квантові стани неможливо розрізнити

Квантова система із двома станами - кубіт - може перебувати не тільки в базисних станах |0 та |1) (які відповідають, наприклад, вертикальній та горизон­тальній поляризації окремого фотону), але й у стані лінійної суперпозиції

 (5.1)

де α і β – комплексні числа, що задовольняють умові ІαІ2+ІβІ2=1. Вимірюючи стан кубіту, ми знайдемо, що кубіт з імовірністю |а|2 несе значення «0», а з імовірністю |р|2 - значення «1».

За законами квантової механіки неможливо виконати вимірювання, що дозволило б розрізнити стани |Т1) = а1|0) + Р1|1) та |Т2) = а2|0) + Р2|1), крім випадку, коли скалярний добуток (^1|^2) = 0, тобто стани |Т1) й |Т2) ортогональні.

1. Переплутування (квантові кореляцїі)

Дві або більше квантових систем можуть бути переплутані. Так пара фотонів у сингелентному поляризаційному стані

 (5.2)

де індекси позначають номери фотонів, - це приклад максимально переплутаного стану двох кубітів. Такий стан називають парою Ейнштейна – Подольського -Розена (ЕПР-парою).

Якщо вимірювання виконується над одним із двох переплутаних кубітів у стані |Т ) (5.2), наприклад у базисі {|0), 11)}, який називається обчислювальним базисом, то результат буде «0» або «1» з однаковою ймовірністю 1/2. Стан друго­го кубіту антикорельований з першим, тобто якщо перший кубіт в результаті вимірювання перейшов у стан |0), то другий перейде в стан |1) і навпаки. Без про­ведення вимірювання, однак, жодний із цих двох кубітів не перебуває в певному стані.

5.2 Основні квантові протоколи розподілення ключів з одиночними квантовими системами

Можна виділити 4 групи таких протоколів:

- протоколи з використанням одиночних кубітів, які називають також прото­колами типу «приготовлення - вимірювання»;

- протоколи з використанням переплутаних станів кубітів;

- протоколи з використанням одиночних багаторівневих квантових систем - кудитів;

- протоколи з використанням переплутаних станів кудитів.

У принципі протоколи з кубітами можна було б не виділяти в окремі групи. Але такі протоколи як з одиночними, так і з переплутаними кубітами історично були розроблені першими. Більшість експериментів нині виконано якраз для таких протоколів. Також існуючі сьогодні комерційні системи квантового розподілення ключів реалізують поки що тільки протоколи з кубітами. Тому наведена вище класифікація уявляється нам найбільш точною.

Розглянемо спочатку групу протоколів, заснованих на пересиланні одиночних кубітів. У таких протоколах кожний фотон несе один біт інформації.

Перший протокол цього типу був запропонований Ч.Х. Бенетом і Ж. Брасаром у 1984 р., згодом він одержав назву ВВ84 [37]. У цьому протоколі використовують два взаємно не зміщені поляризаційні базиси: вертикально-горизонтальний, позначимо його ©, що відповідає вертикальній (двійковий «0») або горизонтальній (двійкова «1») лінійній поляризації фотонів, і діагональній ©, що відповідає двом діагональним поляризаціям +45° та - 45°.

Далі будемо використовувати такі позначення суб’єктів протоколу: суб’єкт А- відправник повідомлення, суб’єкт В - отримувач.

Суб’єкт А випадковим чином вибирає базис і поляризацію своїх однофотонних імпульсів і посилає їх суб’єктові В, тобто суб’єкт А з однаковою ймовірністю посилає один із чотирьох квантових станів:

 (5.3)

Випадкова поляризація вибирається тому, що ключ повинен бути випадковою послідовністю бітів, а два базиси потрібні для того, щоб перешкодити зловмиснику правильно реєструвати поляризацію фотонів. Приклад стадій протоколу ВВ84 показано на рис. 5.2 [37].

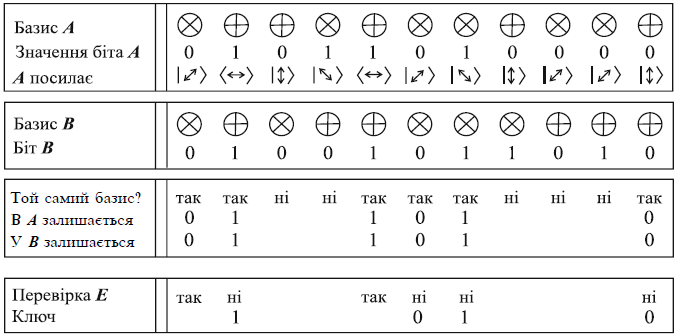


Рис. 5.2 Приклад стадій протоколу ВВ84

Для кожного фотона суб’єкт В випадковим чином вибирає базис і вимірює поляризацію в обраному базисі. Отриманий суб’єктом В набір бітів називають сирим ключем. Потім він повідомляє суб’єкту А відкритим каналом, який базис він використав для кожного вимірювання (зрозуміло, не повідомляючи результатів вимірювань). Суб’єкт А повідомляє, який базис використав він. Оскільки суб’єкт В вгадує базис, обраний суб’єктом А, у середньому в половині випадків, то в результаті він правильно приймає близько половини бітів, посланих суб’єктом А. Суб’єкти А і В відкидають усі біти, що відповідають випадкам, коли вони використовували різні базиси й у результаті одержують просіяний ключ. Ефективність протоколу ВВ84 дорівнює відношенню середньої довжини просіяного ключа до середньої довжини сирого і за відсутності завад у квантовому каналі дорівнює 0,5.

Далі проводиться процедура виправлення помилок, оцінка їх рівня та оцінка кількості інформації, що могла втекти до зловмисника [37]. Існують різні види атак на протоколи квантового розподілення ключів. Зокрема, на протокол ВВ84 можливі атаки, що використовують недосконалість обладнання та не завжди можуть бути виявлені легітимними користувачами [60]. Для виявлення атак, які можливі при використанні суб’єктом А ідеальних однофотонних джерел сигналів, легітимні користувачі повинні оцінити рівень помилок, пожертвував при цьому частиною переданих бітів (цю процедуру показано на рис. 5.2). Після виправлення помилок суб’єкт А та суб’єкт В з високою ймовірністю мають ідентичний погоджений ключ.

Останній етап стека квантових протоколів розподілення ключів - процедура підсилення секретності, яка забезпечує теоретико-інформаційну стійкість [37]. Суб’єкти А і В визначають величину τ - число бітів, на яке потрібно скоротити погоджений ключ, щоб зробити інформацію зловмисника про ключ нижче заданої малої величини. Потім суб’єкт А генерує випадкову двійкову матрицю Kрозміру (n - τ)∙ τ й відкрито передає її суб’єктові В. Кінцевий секретний ключ (довжини n - τ) тоді виходить множенням (за модулем 2) матриці K на узгоджений ключ довжини n (процедура хешування). При цьому можна строго довести, що при τ інформація зловмисника про ключ буде нижче деякого певного значення. Останнє можна вибрати як завгодно малим (звичайно, що чим менше інформації повинно залишитись у зловмисника, тим більше буде τ і, відповідно, тим коротше буде кінцевий секретний ключ).

У протоколі ВВ84 для виявлення атаки використовують два взаємно не зміщені базиси. Але кількість таких базисів для d-вимірної квантової системи дорівнює d + 1. Відповідно, для кубітів існують три взаємно не зміщені базиси. Протокол, схема якого аналогічна ВВ84, але в якому використовуються три взаємно не зміщені базиси, тобто до чотирьох станів (5.3) додають ще два, відповідні правій та лівій коловій поляризації фотонів, називається протоколом з шістьома станами. Було показано, що стійкість цього протоколу до деяких атак дещо вища стійкості ВВ84.

У 1992 р. І.Х. Беретом був запропонований протокол з одиночними фотонами, де замість поляризації використовується фазове кодування. Цей протокол отримав назву В92. Така система менш піддана завадам, що виникають в оптичному хвилеводі при передачі фотонів, але зловмисник може одержати більше інформації про ключ для заданого рівня створюваних ним помилок, ніж у протоколі BB84, тобто стійкість протоколу В92 нижче стійкості протоколу ВВ84. Ефективність протоколу В92 також нижче ефективності ВВ84 і становить 25 % в ідеальному квантовому каналі.

Протокол 4+2 є гібридним варіантом протоколів ВВ84 та В92. У ньому використовуються чотири квантові стани для кодування «0» та «1» у двох базисах. Стани в кожному базисі вибираються неортогональними, крім того, стани в різних базисах також мають бути попарно неортогональними. Цей протокол має більш високий рівень стійкості, ніж протокол BB84, коли використовують слабкі когерентні імпульси замість одиночних фотонів, що тепер і відбувається на практиці. Але ефективність протоколу 4+2 нижче, ніж ефективність протоколу BB84.

Протоколи зі станами «приманки» (decoy states protocols) [57,61] є удосконаленим варіантом протоколу ВВ84. У таких протоколах, крім інформаційних сигналів, джерело суб’єкта А також випромінює додаткові імпульси (приманки), у яких середнє число фотонів відрізняється від середнього числа фотонів в інформаційних сигналах. Атака зловмисника змінює статистичні характеристики станів приманки та/або інформаційних станів і буде виявлена. Як показали практичні експерименти, для цих протоколів швидкість передавання ключа й практична довжина каналу більше, ніж для BB84 [57].

Одним зі шляхів збільшення ефективності квантових протоколів розподілення ключів є використання для передачі замість дворівневих квантових систем (кубітів) багаторівневих систем (кудитів). Кожний кудит дозволяє передати 1оg2d біт класичної інформації, де d - розмірність гільбертова простору кудиту. Нині запропоновані два види протоколів з одиночними кудитами: перший є узагальненням протоколу ВВ84, в ньому для забезпечення секретності використовуються два базиси [63]; другий є узагальненням протоколу із шістьома станами, в ньому використовуються d + 1 базиси [63]. Ефективність протоколів першого типу дорівнює (1оg2d)/2 біт/кудит, другого - (1оg2d)/(d + 1) біт/кудит.

5.3 Квантовий протокол розподілення ключів з переплутанними кубітами

Цей протокол був запропонований А. Екертом у 1991 р. Розподілення ключа виконується через квантовий канал, який містить джерело, що випускає переплутану пару фотонів у синглетному стані (5.2). Фотони розлітаються в різні сторони (уздовж деякої осі z) у напрямку до двох легітимних користувачів каналу, суб’єкта Ата суб’єкта В, які після одержання фотонів виконують вимірювання та реєструють результат цих вимірювань в одному з трьох базисів, одержуваних обертанням ©-базису навколо осі z на деякі заздалегідь визначені кути. При цьому значення кутів повороту базисів повинні бути однаковими в суб’єкта А та суб’єкта Ву двох випадках із трьох, наприклад: у суб’єкта А: ϕ1А = 0, ϕ2А = π/4, ϕ3А = π/8; у суб’єкта В: ϕ1В = 0, ϕ2В = - π/8, ϕ3В = π/8. Конкретний базис для кожного вимірювання обидва вони вибирають випадково й незалежно один від одного.

Після того, як відбулася передача, суб’єкти А і В можуть публічно оголосити, які орієнтації базисів вони вибирали в кожному конкретному випадку, і розділити проведені вимірювання на дві різні групи: у першій групі будуть вимірювання, у яких вони використали різні орієнтації базисів, а в другий - ті, у яких орієнтації базисів збігалися. Вони також відкидають усі випадки, коли один з них або обидва взагалі не змогли зареєструвати жодного фотона. Таким чином, при відсутності завад в каналі ефективність протоколу Екерта дорівнює 2/9 біт на пару кубітів, оскільки випадки використання різних базисів використовуються тільки для контролю підслуховування та відкидаються при просіюванні ключа.

Після цього суб’єкти Аі В можуть відкрито показати один одному результати, які вони одержали в рамках однієї тільки першої групи вимірювань, тобто коли орієнтації їхніх базисів не збігалися. Це дозволяє їм установити коефіцієнт кореляції вимірювань 5, який також може бути обчислений з використанням законів квантової механіки [37]:

 (5.4)



При використанні наведених вище значень кутів повороту базисів у суб’єктів А і В з (5.4) одержуємо S = -2√2. Якщо значення S, отримане в результаті вимірювань суб’єктів А і В при використанні ними різних базисів дорівнює -2√2, то стани фотонів із переплутаних пар не були змінені на шляху від джерела до легітимних користувачів. Отже, результати, отримані в другій групі вимірювань, тобто коли суб’єкти АiВ використали однакові базиси, антикорелюють і можуть бути перетворені в секретний рядок бітів - ключ. Якщо ж отримана величина S не дорівнює -2√2, то це означає, що стани фотонів були змінені або в результаті перехоплення, або в результаті завад у квантовому каналі зв’язку. Далі суб’єкти А і В повинні оцінити рівень помилок і або визнати його прийнятним і провести процедуру квантового підсилення секретності [37], що дозволить їм встановити секретний ключ, або, якщо рівень помилок неприйнятний, незалежно від їхньої природи - наявності атаки зловмисника або наявності завад у каналі - потрібно повторити всю процедуру знову.

Сьогодні запропоновані узагальнення протоколу Екерта на випадок використання переплутаних пар кудитів [64]. Ці протоколи мають більшу інформаційну місткість порівняно з оригінальним протоколом Екерта.

Зазначимо, що однією з головних концептуальних переваг протоколів з переплутаними станами квантових систем над протоколами з одиночними квантовими системами є випадковість результатів квантових вимірювань над переплутаними системами, в результаті чого легітимні користувачі отримують цілком випадковий спільний ключ. При використанні протоколів з одиночними квантовими системами суб’єкт А повинен спочатку згенерувати випадковий ключ. Зазначимо, що сьогодні існують комерційні квантові генератори випадкових чисел, наприклад генератор QUANTIS швейцарської компанії їй Quantique [65], який може використовуватися для генерації істинно випадкового криптографічного ключа.

5.4 Комерційні квантові системи розподілення ключів. Переваги та недоліки.

Першою комерційною системою квантового розподілення ключів була Security Gateway (QPN-8505) [66], створена компанією MagiQ Technologies (США). Ця система (рис. 5.3,а) являє собою економічно ефективне рішення інформаційної безпеки для державних і фінансових організацій. Система пропонує захист віртуальних приватних мереж за допомогою квантового розподілення ключів (до ста 256-бітових ключів на секунду на відстань до 140 км) та інтегрованого шифрування. Для квантового розподілення ключів QPN-8505 використовує протокол BB84 з фазовим кодуванням, а для шифрування даних - симетричний шифр AES.

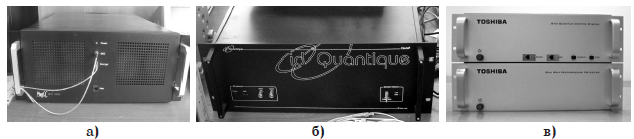


Рис. 5.3 Деякі комерційні квантові системи захисту інформації

Швейцарська компанія Id Quantique пропонує системи Clavis2 (рис. 5.3, б) і Cerberis [67]. Clavis2використовує власну автокомпенсувальну оптичну платформу, яка має високу стабільність, що гарантує низький рівень квантових помилок. Безпечний обмін ключами можливий на відстані до 100 км. Ця оптична платформа добре документована в наукових публікаціях і була ретельно протестована. Cerberis являє собою сервер з автоматичним створенням і секретним обміном ключами через оптоволоконний канал. Зазначена система може передавати криптографічні ключі на відстань до 50 км, її характерною особливістю є 12 паралельних криптографічних обчислень, що набагато підвищує швидкодію. Система Cerberis використовує шифр AES з ключем довжиною 256 біт, а для квантового розподілення ключів - протоколи BB84 та SARG.

Нещодавно компанією Toshiba Research Europe Ltd (Великобританія) було представлено ще одну систему квантового розподілення ключів під назвою Quantum Key Server [68]. Ця система (рис. 5.3, в) забезпечує генерацію до ста 256-бітних ключів на секунду та їх передавання на відстань понад 100 км. При передаванні на відстань до 50 км забезпечується швидкість 1 Мбіт/с. До складу Quantum Key Server входить інтегрований модуль автоматичного управління, що проводить неперервний моніторинг системи та регулює її оптичні характеристики.

Ще одна британська компанія QinetiQ представила першу у світі мережу, що використовує квантову криптографію - Quantum Net (Qnet) [69]. Максимальна довжина ліній зв’язку цієї мережі становить 120 км, та найголовнішим є те, що система Qnet - це перша квантово-криптографічна система, що використовує понад два сервери. їх у цій системі шість і всі вони інтегровані в мережу Internet.

Аналіз виконаних на теперішній час теоретичних та експериментальних робіт в галузі квантового розподілення ключів дозволяє виділити такі їх переваги та недоліки.

Переваги:

1. Протоколи квантового розподілення ключів дозволяют завжди виявити атаку пасивного перехоплення, оскільки підключення зловмисника вносить до квантового каналу набагато більший рівень помилок порівняно з рівнем природних завад.

2. Безумовна (теоретико-інформаційна) безпека квантових протоколів розподілення ключів дозволяє використати абсолютно секретний ключ для дальшого шифрування відомими класичними симетричними шифрами - це відповідно збільшує рівень захищеності, який забезпечують суто класичні криптосистеми. Також можливий синтез квантових протоколів розподілення ключів із шифром Вернама (одноразовим блокнотом), що в поєднанні з безумовно стійкою схемою автентифікації дозволить створити абсолютно стійку систему передавання конфіденційної інформації.

Недоліки:

1. Система, побудована тільки на квантових протоколах розподілення ключів, не може бути повноцінним завершеним рішенням проблеми розподілення секретних ключів - потрібні також засоби для попередньої автентифікації користувачів. Така автентифікація може бути виконана, наприклад, за допомогою першого невеликого секретного ключа, який користувачі системи квантового розподілення ключів повинні отримати один раз заздалегідь. Потім невелику частку секретного ключа, розподіленого за допомогою квантового протоколу, користувачі можуть залишити для автентифікації в наступному сеансі тощо.

Обмеження довжини квантового каналу: при квантовому передаванні інформації неможливо «підсилити сигнал» через неможливість копіювання квантових станів. Проте можна створити квантовий аналог повторювача, що дає можливість квантового передавання інформації на великі відстані за допомогою створення переплутаних станів між відправником та одержувачем. Це переплутування потім може бути використано при квантовій комунікації, зокрема в квантових протоколах розподілення ключів. Технологія квантових повторювачів, яка ґрунтується на технології квантової пам’яті, активно розробляється сьогодні, але ця технологія поки що не вийшла за межі лабораторних експериментів.

1. Низька ефективність (імовірність зареєструвати відлік, якщо фотон попав у детектор) детекторів одиночних фотонів - для телекомунікаційного «вікна прозорості» 1550 нм ефективність таких детекторів, що працюють при температурах 200-300 К, не перевищує 10 % [70]. Існують також надпровідні детектори, що працюють при наднизьких температурах 0.1-1.5 К, ефективність яких досягає 95 % [70]. Але використання таких надпровідних детекторів у квантових системах розподілення ключів значно збільшує вартість системи. Ще одна проблема, яка пов’язана з детекторами, - ефект «темнового шуму», коли детектор спрацьовує при відсутності фотона [70].
2. Швидкість передавання інформації квантовим каналом істотно зменшується зі збільшенням довжини каналу і в більшості експериментів на відстанях порядку 100-200 км дорівнює декільком кілобітам на секунду.
3. Деполяризація фотонів у квантовому каналі, яка призводить до помилок при вимірюваннях у легітимних користувачів.
4. Висока ринкова ціна існуючих сьогодні комерційних систем квантового розподілення ключів.
   1. Оптимізація методів передавання мультимедійної інформації

Стрімкий розвиток інфокомунікаційних технологій, який викликав зростання обсягів ІР-навантаження, що циркулює в сучасних телекомунікаційних мережах, як ніколи, гостро поставив перед науковцями проблему пошуку нових методів підвищення ефективності передавання цього навантаження. За таких умов особливо актуальним постає питання мінімізації обсягів службового навантаження (протокольної надлишковості).

Особливої актуальності це питання набуває при створенні корпоративних мереж, які складаються з декількох територіально рознесених сегментів, для поєднання яких використовуються орендовані ресурси операторів телекомунікацій. Це пояснюється тим, що найбільш поширеним методом поєднання окремих сегментів до єдиної логічної мережі є організація єдиного адресного простору та прозорого транспортування ІР-пакетів між такими сегментами за допомогою тунелювання. При цьому організація такого поєднання, як правило, лише збільшує обсяг інформації, що передається орендованими каналами за рахунок додаткової інкапсуляції, що найбільше позначається на пакетах невеликих розмірів (наприклад, медіа-даних голосового навантаження).

Як відомо, в основу процесу тунелювання (рис. 5.4) ІР-навантаження між двома сегментами пакетної мережі покладено принцип інкапсуляції блоків даних нижчих або рівних рівнів до блоків даних вищих або рівних рівнів моделі 081 [71]. За рахунок цього з’являється можливість використовувати єдину адресацію та механізми маршрутизації в межах всієї корпоративної мережі, незважаючи на кількість сегментів, що входять до її складу.

На рис. 5.4 наведено приклад поєднання двох незалежних сегментів корпоративної мережі крізь IP-мережу за допомогою двох маршрутизаторів. Слід зазначити, що адресація вузлів в обох зображених на рисунку підмережах (1 та 1’) здійснюється в межах однієї логічної підмережі. Таким чином, для обміну інфор­мацією між робочою станцією А та робочою станцією Бвикористовуються ті самі механізмі, що й для обміну інформацією в межах одного фізичного сегмента. Такий ефект досягається за рахунок прозорого тунелювання навантаження між двома маршрутизаторами, яке полягає в додатковій інкапсуляції ще одного заголовка до надісланих на внутрішні інтерфейси маршрутизаторів пакетів (рис. 5.5). При цьому - в разі, якщо пакет спрямований від робочої станції А до робочої станції Б(для наведеного вище прикладу), адресою призначення зовнішнього заголовка буде IP-адреса 195.5.27.4, а адресою відправника — 213.130.5.5.

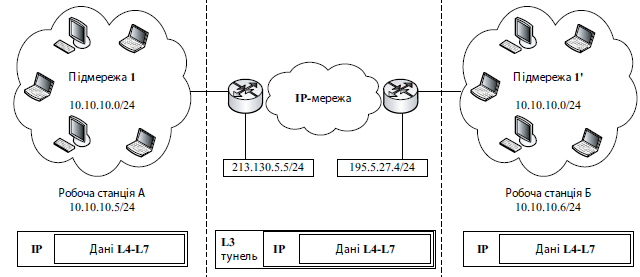


Рис. 5.4 Процес тунелювання IP-навантаження

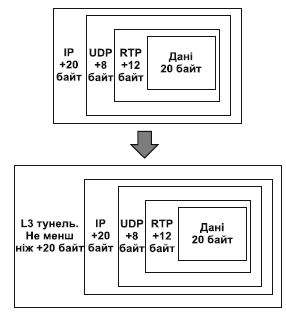


Рис. 5.5 Процедура додаткової інкапсуляції

Обсяг службової інформації, який додатково додається до кожного ІР-пакета при тунелю ванні ІР-навантаження, залежит від конкретної реалізації тунелю. Наприклад, при використанні тунелів «IP-GRE», розроблених компанією Cisco System, крім додавання ще одного ІР-заголовка, додається спеціальний заголовок типу GRE, який може мати розмір від 4 до 20 байт.

У свою чергу, тунелювання типу ІР-ІР, розроблене компанією IBM [73], передбачає додавання до базового заголовка лише одного ІР-заголовка розміром 20 байт. Саме цей тип тунелю є найменш витратним. Тобто, додаткова інкапсуляція 20 байт до кожного пакета практично не впливає на передавання пакетів великих розмірів, однак призводить до небажаних наслідків при тунелюванні навантаження IP-телефонії, при якому корисна голосова інформація передається пакетами невеликих розмірів. При цьому збільшення розміру кожного такого пакета, що передається каналами зв’язку, на 20 байт автоматично призводить до необхідності збільшення достатньої для передавання навантаження [74] пропускної спроможності каналу зв’язку приблизно на 30 %. Зазначена проблема особливо гостро постає в разі організації віртуальних тунелів між двома мережними об’єктами, що виконують роль комутаторів з’єднань IP-телефонії (Softswitch, IP-PBX тощо). У цьому випадку для кожного віртуального з’єднання з метою передавання голосової інформації між двома вузлами мережі пересилається значна кількість пакетів невеликих розмірів, до кожного з яких застосовується процедура додаткової інкапсуляції.

Так, наприклад, при використанні голосових кадрів тривалістю 20 мс, кожен з яких подано у вигляді корисного навантаження розміром 20 байт, а також за умов використання мінімальних розмірів заголовків протоколів RTP (Real-time Transport Protocol), UDP (User Datagram Protocol) та IP (12, 8 та 20 байт відповідно) при передаванні одночасно понад 100 голосових з’єднань орієнтовний розмір необхідної пропускної спроможності каналу зв’язку становитиме 2,4 Мбіт/с без використання тунелювання IP-навантаження та 3,2 Мбіт/с при ви­користанні тунелю типу «IP-IP».

Одним з найбільш відомих шляхів мінімізації необхідної пропускної спроможності каналів зв’язку при передаванні мультимедійного IP-навантаження є застосування протоколу cRTP (Compressed RTP) [75, 76], який передбачає стиснення заголовків IP/UDP/RTP для передавання в межах низько-швидкісних каналів зв’язку, побудованих за принципом «точка-точка». Базовим принципом протоколу cRTP є збереження на обох кінцях каналу зв’язку (компресорі та декомпресорі) контекстів RTP-сесій, які містять опис типової для сесії структури службових заголовків IP/UDP/RTP, із дальшим передаванням між компресором та декомпресором лише тієї частини заголовків, які змінилися всупереч очікуванням компресора.

Альтернативним варіантом вирішення зазначених вище проблем може бути механізм мінімізації службової інформації при тунелюванні IP-навантаження, принцип роботи якого зображено на рис. 5.6.

Як зображено на рис. 5.6, на кожній зі сторін тунелю з агрегацією сесій та компресією заголовків (ТАСКЗ), окрім звичайних засобів тунелювання, що передбачають внесення до кожного пакета додаткового IP-заголовка, реалізовано компресор та декомпресор. Як компресори, так і декомпресори оперують спеціальними таблицями контекстів RTP-сесій. За допомогою інформації, яка зберігається в зазначених таблицях, компресори (за аналогією з протоколом cRTP) можуть не передавати всю службову інформацію для кожного голосового кадру, а попередньо забезпечити передавання першого з пакетів у межах RTP- сесії декомпресору і надалі передавати лише унікальний ідентифікатор контексту та спеціальні інформаційні повідомлення у разі відхилення службової інформації в наступному пакеті тієї самої RTP-сесії від очікуваних значень. Такий підхід дозволяє зменшити розмір службової інформації, що передається із кожним голосовим кадром з 40 байт до 2-4 байт на кожен пакет [75].

Додаткового зменшення обсягу службової інформації можна досягти за рахунок агрегації пакетів з різних RTP-сесій, що надходять до компресора протягом періоду часу, меншого за середню різницю в часі між надходженням двох пакетів з однієї RTP-сесії. Така агрегація дозволяє збільшити швидкість передавання корисного навантаження за рахунок зменшення сукупного обсягу службового навантаження, що передається з кожним голосовим фреймом. Можливість агрегації RTP-сесій передбачена в протоколі IAX2 (Inter-Asterisk eXchange protocol) [77], який використовується сумісно із IP-PBX Asterisk, та в протоколі TCRTP (Tunneling Multiplexed Compressed RTP) [11.78], запропонованому компанією Cisco Systems. Однак слід зважати на низку суттєвих недоліків: у специфікації обох протоколів не визначається реалізація механізмів агрегації, а лише констатується її можливість; обидва протоколи мають обмежене застосування (у межах окремої платформи або лише з певним типом протоколу канального рівня) - жоден з цих протоколів не може використовуватися для вирішення проблем в комплексі.

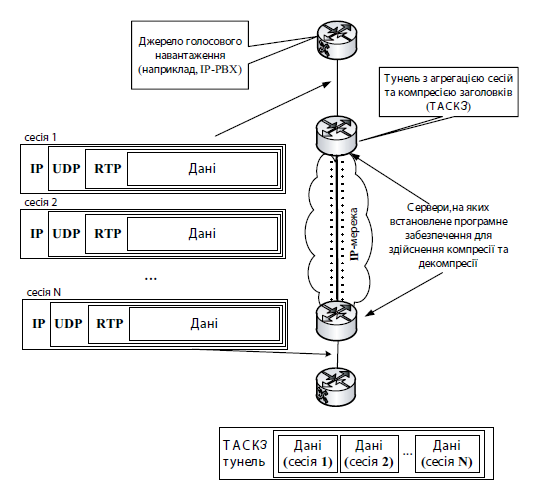


Рис. 5.6 Принцип роботи ТАСКЗ

Серед ключових переваг механізму ТАСКЗ слід зазначити такі:

- у 1,5-3 рази зменшується загальний обсяг навантаження, що передається крізь канал зв’язку при тунелюванні, залежно від кількості одночасних RTP-сесій;

- спосіб може бути використаний при організації взаємоз’єднань операторів IP-телефонії в сучасних IP-мережах;

- звільнений ресурс пропускної здатності може бути використаний або для збільшення кількості одночасних телефонних з’єднань (без збільшення вимог до пропускної здатності каналу зв’язку), або для покращення якості зв’язку за рахунок дублювання IP-пакетів з метою мінімізації ймовірності їх безповоротної втрати.

6. ОЦІНКА ЕФЕКТИВНОСТІ ПОБУДОВИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Зважаючи на наявність широкого спектра технологій побудови телекомунікаційних мереж, що сьогодні можуть вважатися перспективними, перед власниками мереж часто постає досить складне організаційно-технічне завдання - вибір найбільш оптимального напряму розвитку мережі на підставі комплексної оцінки технічних та економічних показників. Для цього, як правило, на цій стадії розробляється техніко-економічне обґрунтування, або бізнес-план, однак, зважаючи на відсутність єдиного підходу до розробки таких документів, проектувальники часто користуються суто суб’єктивними підходами до визначення стратегії дальшого розвитку.

Неприпустимість обрання хибної стратегії розвитку, яка може призвести до небажаних наслідків, змушує власників мереж приділяти більше уваги до цієї стадії проектування. За таких умов досить актуальним стає завдання мінімізації суб’єктивної частки оцінки перспективності тієї чи іншої технології та створення чітких методик, які можуть стати ефективним інструментом обрання стратегії розвитку мережі на основі результатів моделювання процесу реорганізації

В основу оцінки ефективності побудови телекомунікаційних мереж може бути покладено принцип декомпозиції структури існуючої або проектованої мережі на незалежні сегменти з дальшою оцінкою орієнтовної вартості та тривалості побудови (або модернізації) кожного окремого сегмента до кожного з обраних перспективних наборів технологій. При цьому набір технологій, до яких здійснюється моделювання процесу реорганізації, обирається на підставі вимог, сформованих власником, до проектованої мережі.

В узагальненому вигляді процес оцінки можна уявити у вигляді алгоритму, який наведено на рис. 6.2. Цей алгоритм дозволяє на підставі аналізу технічних та економічних показників обрати серед заданих саме той набір технологій, який в конкретному випадку є найбільш ефективним.

Запропонований алгоритм можна умовно поділити на чотири основні частини:

* внесення вихідних даних про існуючу (або проектовану) мережу та її декомпозиція на незалежні сегменти;
* формування вимог до майбутньої мережі та визначення наборів перспективних технологій;
* визначення орієнтовної вартості та тривалості будівництва (або модернізації) для кожної пари «сегмент - набір технологій»;
* визначення найбільш перспективного набору технологій на основі порівняння сумарних показників вартості та тривалості для кожного з перспективних наборів технологій.

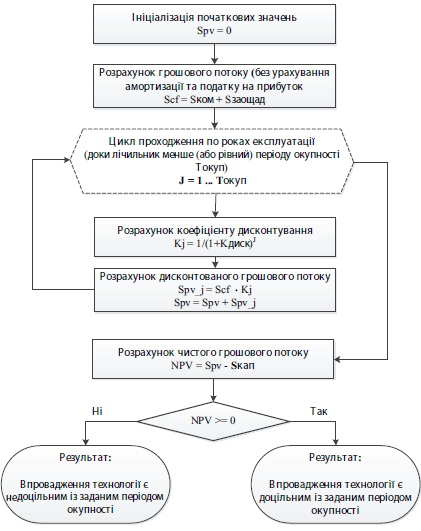


Рис. 6.1 Алгоритм оцінки економічної доцільності переходу до альтернативного мережного механізму

Перша з чотирьох процедур (позначена цифрою 1 на рис. 6.2) складається з двох базових кроків: внесення інформації про структуру існуючої або проектованої мережі та виділення незалежних сегментів мережі, що підлягають будівництву. Перший з двох перелічених кроків передбачає поступове внесення інформації про кожен елемент мережі (обладнання або канал зв’язку) на тих її рівнях, яких стосується модернізація або будівництво. При цьому, крім типів та технічних характеристик кожного елементу, на цьому кроці має вноситись інформація про взаємопідключення елементів між собою через спеціальні інтерфейси (як в межах одного рівня, так і з обладнанням інших рівнів).

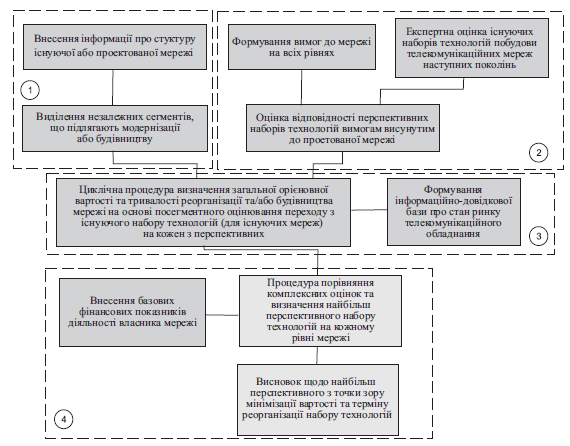


Рис. 6.2 Узагальнений алгоритм визначення найбільш ефективного напряму будівництва (реорганізації) мережі

Друга процедура (позначена цифрою 2 на рис. 6.2) призначена для виділення з усієї сукупності наборів технологій, які сьогодні можуть розглядатися як перспективні для модернізації або будівництва телекомунікаційної мережі, лише тих наборів, що відповідають вимогам власника до цієї мережі. Процедура складається з трьох основних кроків: формування вимог до мережі на всіх її рівнях, експертна оцінка існуючих наборів технологій побудови телекомунікаційних мереж наступних поколінь та оцінка відповідності перспективних наборів технологій вимогам, висунутим до проектованої мережі. За результатами виконання процедури має бути одержано перелік тих наборів технологій (для кожного з рівнів мережі), які цілком задовольняють вимогам до цієї мережі з боку її власника. Саме перехід до цих наборів технологій і буде порівнюватися на дальших кроках методики з погляду вартості та тривалості реорганізації для кожного з них.

Третя процедура (позначена цифрою 3 на рис. 6.2) є найбільш складною через кількість операцій. Ця процедура передбачає циклічний перебій всіх виділе­них незалежних сегментів (що підлягають модернізації або будівництву) з метою послідовної оцінки їх переведення на нові перспективні набори технологій (або будівництва із використанням цих наборів технологій). При цьому відмінність модернізації існуючої мережі від будівництва нової полягає, насамперед, у тому, що при модернізації існуючої враховуються додаткові часові та фінансові витрати на демонтаж існуючого обладнання та/або існуючих каналів зв’язку. Основою для роботи процедури є спеціально сформована інформаційно-довідкова база про стан ринку телекомунікаційного обладнання, яка містить у собі відомості про можливу взаємозамінність моделей між собою. Результатом роботи цієї процедури є вектор вартостей та тривалості модернізації (або будівництва) мережі (за її рівнями) на використання того чи іншого перспективного набору технологій.

Остання процедура алгоритму (позначена цифрою 4 на рис. 6.2) передбачає визначення найбільш перспективного набору технологій на кожному рівні мережі на основі порівняння вартості та тривалості модернізації (або будівництва) з врахуванням базових фінансових показників діяльності власника мережі в напрямі її експлуатації (наприклад, через визначення строку окупності мережі оператора телекомунікацій).

Слід також зазначити, що наведений на рис. 6.2 алгоритм відображає лише загальний принцип визначення перспективного набору технологій, а його деталізація для конкретних умов (будівництво нової мережі або реорганізація існуючої; будівництво мереж на різних рівнях тощо) передбачає розробку деталізованих алгоритмів, які можуть відрізнятися для конкретних випадків.

З метою оцінки відповідності тієї чи іншої технології (або набору технологій) технічним вимогам, що висуваються власником мережі, пропонується використовувати змінний набір критеріїв. Критерії, що можуть входити до цього набору, мають бути чітко сформульованими та мати можливість провести чисельну оцінку будь-якої з технологій побудови транспортної мережі. Як чисельна оцінка можуть виступати як натуральні показники (біт/с, секунда тощо), так і умовні (1 або 0 - у разі відповідності або невідповідності технології вимогам критерію; бальна оцінка - наприклад, від 1 до 10); замкнута система значень тощо).

Зокрема, до цього набору можуть входити такі критерії:

* пропускна спроможність каналу зв’язку - критерій, який визначає, яка максимальна пропускна спроможність каналу зв’язку може бути досягнута із використанням тієї чи іншої технології (вимірюється в біт/с або за допомогою бальної оцінки з відображенням швидкості на бальну шкалу);
* максимальна довжина транспортної ділянки - критерій, який застосовується лише для оцінювання технологій побудови транспортних мереж та визначає, на яку максимальну (згідно зі стандартом або рекомендацією) відстань може бути організовано канал зв’язку із використанням тієї чи іншої технології (вимірюється в км);
* максимальна відстань до абонента - критерій, який застосовується лише для оцінювання технологій побудови мереж доступу та визначає, на яку максимальну (згідно зі стандартами або рекомендаціями) відстань може бути організовано канал зв’язку між абонентським пристроєм і комутуючим обладнанням оператора (вимірюється в км);
* час відновлення зв’язку - критерій, який визначає орієнтовний час відновлення зв’язку (відновлюється можливість передавання корисної інформації) на ділянці мережі, побудованої із використанням тієї чи іншої технології, після відновлення фізичного каналу;
* максимальна швидкість передавання корисної інформації - критерій, який визначає максимально припустиму швидкість передавання корисної інформації (побічно відображає надлишковість), що може бути досягнута із використанням тієї чи іншої технології (вимірюється в біт/с);
* можливість керування навантаженням - критерій, який відображає підтримку тією чи іншою технологією механізмів керування навантаженням у мережі (гнучкість маршрутизації, підтримка динамічного реконфігурування тощо). Може оцінюватися, наприклад, за допомогою бальної оцінки (визначається шляхом експертного оцінювання або шляхом установлення чіткої відповідності того чи іншого набору механізмів керування тому чи іншому значенню бальної оцінки);
* підтримка резервування - критерій, який відображає підтримку тією чи іншою технологією механізмів резервування каналів зв’язку (можливість переключення в автоматичному режимі на резервний напрямок у разі виходу з ладу основного). Може оцінюватися, наприклад, за допомогою бальної оцінки, яка визначається виходячи із замкнутої системи значень;
* ефективність керування - критерій, який відображає ефективність системи керування, що використовується тією чи іншою технологією побудови транспортної мережі оператора з огляду на її тип (централізована, розподілена, гібридна). Може оцінюватися, наприклад, за допомогою бальної оцінки, яка визначається виходячи із замкнутої системи значень;
* доступність обладнання - критерій, який відображає наявність (або відсутність) достатньо великого ринку виробників та моделей обладнання, яке може бути застосовано для будівництва транспортної мережі із використанням тієї чи іншої технології. Може оцінюватися за допомогою бальної оцінки (визначається шляхом експертного оцінювання або встановлення чіткої відповідності того чи іншого діапазону кількості виробників обладнання тому чи іншому значенню бальної оцінки);
* доступність спеціалістів критерій, який відображає наявність (або відсутність) достатньої кількості фахівців на місцевому ринку праці, які можуть бути задіяні для будівництва, розвитку та поточного обслуговування обладнання тієї чи іншої технології побудови транспортної мережі оператора. Може оцінюватися за допомогою бальної оцінки, визначеної, наприклад, шляхом експертного оцінювання;
* наявність готових впроваджень - критерій, який відображає наявність (або відсутність) прикладів реалізації транспортних мереж операторів телекомунікацій на базі тієї або іншої технології. Може оцінюватися за допомогою бальної оцінки шляхом встановлення чіткої відповідності того чи іншого діапазону впроваджень тому чи іншому значенню бальної оцінки;
* рівень стандартизованості - критерій, який відображає рівень стандартизованості тієї чи іншої технології побудови транспортних мереж. Може оцінюватися за допомогою бальної оцінки шляхом встановлення чіткої відповідності рівня стандартизованості (є прийняті стандарти; регламентовано на рівні рекомендацій; існує в проміжних варіантах тощо) тому чи іншому значенню бальної оцінки;
* сумісність із видами навантаження - критерій, який відображає сумісність тієї чи іншої технології побудови транспортних мереж із різними типами корисного навантаження (ІР-трафік, цифрові потоки Ех/Тх тощо). Може оцінюватися за допомогою бальної оцінки шляхом установленая чіткої відповідності рівня сумісності тому чи іншому значенню бальної оцінки;
* сумісність із середовищем передавання - критерій, який відображає сумісність тієї чи іншої технології побудови транспортних мереж із різними типами середовищ передавання (ВОЛЗ, радіоефір, мідні кабелі). Може оцінюватися за допомогою бальної оцінки шляхом встановлення чіткої відповідності того чи іншого набору середовищ передавання тому чи іншому значенню бальної оцінки;
* сумісність обладнання від різних виробників - критерій, який відображає можливість використання обладнання, необхідного для побудови транспортної мережі за допомогою тієї чи іншої технології і котре випускається різними виробниками. Може оцінюватися за кількістю виробників, що заявляють сумісність свого обладнання.

# **7. ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА БЕЗПЕКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ**

У відповідності з законом України «Про охорону праці» жодне виробництво, підприємство, цех, робочий ділянку не можуть бути введені в експлуатацію, якщо на них не будуть забезпечені здорові та безпечні умови праці.

В лабораторії з ПК встановлено наступне обладнання:

- обчислювальна техніка (ЕОМ потужністю 350 Вт);

- монітори.

Функціональна схема обладнання, яке використовується у роботі, зображена на рис.7.1.

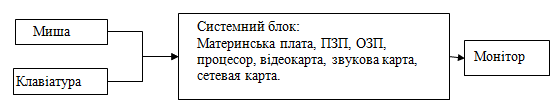


Рис. 7.1– Функціональна схема обладнання

Дане обладнання призначене для роботи операторів ЕОМ зі створення систем автоматизованого управління виробництвом, різного програмного забезпечення, проектно-конструкторських робіт і отримання кінцевих результатів робіт у вигляді документів: лістинги програм, схеми, креслення та ін.

# **7.1 Промислова безпека в проектному відділі**

За ступенем небезпеки ураження електричним струмом за НПАОП 40.1-1.21-98 дане приміщення відноситься до класу приміщень без підвищеної небезпеки, так як вологість 40-60% і виключена можливість одночасного дотику людини до корпусів електрообладнання і заземленим металевим конструкціям будівель і споруд, які мають зв'язок із землею.

Електропостачання відділу здійснюється від 3-х фазної мережі з глухозаземленою нейтраллю, змінний струм, напруга 380/220 В. відповідно до вимог НПАОП 40.1-1.32-01.

Передбачені наступні міри електробезпеки:

- конструктивні міри електробезпеки;

- схемно-конструктивні міри електробезпеки;

- експлуатаційні міри електробезпеки.

Конструктивні міри електробезпеки забезпечують таке конструктивне рішення, яке запобігає можливість дотику людини до струмопровідних частин приладів і обладнання.

Для усунення можливості поразки електричним струмом при дотику працівника до струмопровідних металевих частин, усі рубильники встановлюються в закритих корпусах, з'єднувальні кабелі та шини електроживлення підведені до задньої панелі апаратури і недоступні людині. Застосовується блоковий монтаж.

Згідно з вимогами НПАОП 40.1-1.32-01 для електроустановок змінного струму напругою до 1000В і глухозаземленою нейтраллю застосовується занулення. У приміщенні лабораторії з ПК використана система занулення TN-S.

Комплекс необхідних заходів по техніці безпеки визначається виходячи з виду електроустановки та її номінальної напруги, умов середовища, типу приміщення і доступності електрообладнання.

Яке експлуатується обладнання не є джерелом механічних, або радіаційних небезпек, але є споживачем електричної енергії.

В приміщенні лабораторії, не частіше одного разу на рік, виконується контроль ізоляції. Перш за все,від мережі відключаються всі споживачі, включаючи ДБЖ, подовжувачі та трійники. Потім на щитку відключаються автомати», відповідні досліджуваним групам і з допомогою мегаомметра проводу вимірюються попарно: фаза-фаза, фаза-нуль, нуль, земля. У разі виявлення занадто низького опору необхідно провести додаткові роботи: встановити ділянку ланцюга, на якому порушена ізоляція і негайно усунути дефект.

З працівниками проводиться вступний, первинний, повторний, цільовий, а при необхідності і позаплановий інструктаж. Зміст всіх інструктажів відповідає вимогам НПАОП 0.00-4.12-05.

# **7.2 Забезпечення виробничої санітарії та гігієни праці**

Роботи в даному приміщенні проводяться сидячи і не потребують систематичного фізичної напруги. Згідно ДСН 3.3.6-042-99 робота відноситься до категорії легкої Іа (енерговитрати до 120 ккал/ч). Робочі місця характеризуються наступними мікрокліматичними умовами:

а) відносна вологість повітря 40 - 60%;

б) температура:

- у холодний період: оптимальна 22-24 С, допустима верхня - 25 С, нижня - 21 С;

- в теплий період: оптимальна 23-25 С, допустима верхня - 28С, нижня - 22 С;

в) швидкість руху повітря:

- оптимальна - 0,1 м/с, допустима - 0,1м/с.

Підтримання на даному рівні параметрів, що визначають мікроклімат, здійснюється за допомогою кондиціонування в теплу пору року і при виділенні великої кількості тепла від обладнання з використанням опалення в холодну.

Шумове забруднення у відділі становить 50дБ, що не перевищує норму.

Приміщення з ЕОМ має природне та штучне освітлення відповідно до ДБН Ст. 25-28-2006 «Природне і штучне освітлення». Природне світло проникає через бічні светопроеми, зорієнтовані на північний схід, і забезпечувати коефіцієнт природної освітленості (КЕО) не нижче 1,5%.

Для забезпечення нормованих значень освітлення в приміщеннях з ВДТ ЕОМ загального та персонального користування очищають віконне скло та світильники не рідше ніж 2 рази на рік та своєчасно проводять заміну перегорілих ламп.

Так як домінуючим шкідливим фактором є підвищена температура повітря робочої зони, необхідно розробити систему кондиціювання повітря в приміщенні.

Для дотримання вимог техніки протипожежної безпеки та ергономіки в приміщенні встановлюються сучасні робочі столи та рідкокристалічні екрани. Працівнику для профілактики порушень і підтримки високої працездатності пропонується дотримуватися регламентовані перерви для відпочинку. Рекомендується в період роботи робити дві перерви по 15 хвилин, перший до обідньої перерви, другий – після. Головними елементами робочого місця є письмовий стіл і крісло. Основним робочим положенням є положення сидячи. Робоче місце для виконання робіт у положенні сидячи організується відповідно до ДСТУ 12.2.032-78. При роботі в положенні сидячи рекомендуються такі параметри робочого простору: довжина столу – 1000 мм, ширина – 800 мм, висота – 730 мм. Для задоволення вимог фізіології, конструкція робочого сидіння задовольняє наступним основним вимогам:допускає можливість зміни положення тіла, допускає регулювання висоти в залежності від росту працюючої людини, має злегка увігнуту поверхню, має невеликий нахил назад.

# **7.3 Безпека в надзвичайних ситуаціях в лабораторії з ПК**

Даний пункт розглядається відповідно до закону України «Про цивільного захисту».

У регіоні найбільш імовірними надзвичайними ситуаціями (НС), є надзвичайні ситуації техногенного характеру – це транспортні аварії (катастрофи), пожежі, неспровоковані вибухи, аварії з викидом небезпечних хімічних речовин, раптове руйнування споруд та будівель. Для лабораторії з ПК найбільш вірогідним НС є пожежа.

Пожежі в приміщеннях з ЕОМ представляють особливу небезпеку, оскільки зв'язані з великими матеріальними втратами.

Категорія приміщення по пожежній вибухонебезпечності згідно ДБН Ст. 1.1.7-2002 має І ступінь вогнестійкості, а за пожаровзрывоопасности відноситься до категорії В.

Дане приміщення відноситься до зони класу П-ІІа по ПУЕ-2011, так як це виробниче приміщення, є меблі з дерева і ДВП. Можливі причини виникнення пожежі у приміщенні роботи операторів ЕОМ:

- недотримання правил експлуатації електронно-обчислювальної техніки;

- недотримання правил пожежної безпеки;

- перегрів струмоведучих частин обладнання в слідстві освіти високого перехідного опору в місцях з'єднань;

- несправність загального чи місцевого освітлення робочих місць.

Згідно з вимогами протипожежної безпеки в приміщенні встановлюється 2 вуглекислотних вогнегасника ВВК-1.4 (з розрахунку 1 на 20 м2), які застосовуються при гасінні невеликих вогнищ і можуть бути використані для гасіння електроустановок, що знаходяться під напругою. У відповідності з ГОСТ 12.4.026-76 ці кошти пофарбовані в яскраво-червоний колір і перебувають у легкодоступному місці, при виході з приміщення.

Приміщення лабораторії обладнано системою автоматичної пожежної сигналізації з застосуванням теплових датчиків типу ПОСТ-1 3 штуки, (з розрахунку 2 датчика на кожні 20 м2 площі), налаштованих на температуру спрацьовування 70°С.

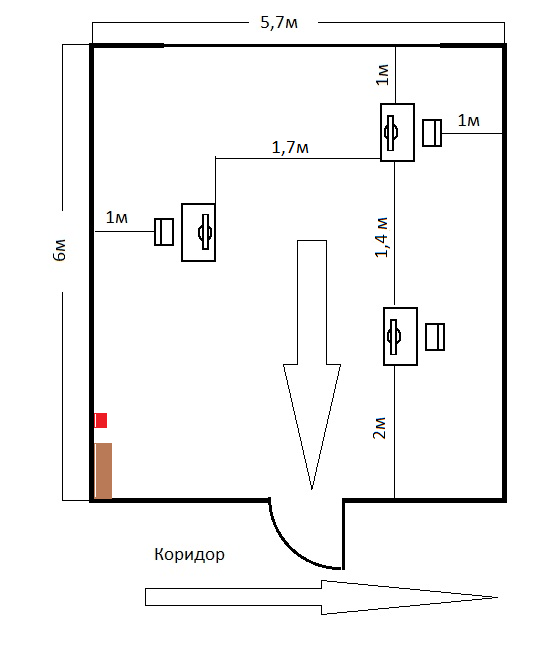
Організаційні заходи пожежної профілактики:

- навчання персоналу правилам пожежної безпеки;

- видання необхідної інструкцій і плакатів, плану евакуації   
персоналу у разі пожежі;

- виготовлення і застосування засобів наочної агітації по забезпеченню пожежної безпеки.

План евакуації показаний на рис.6.2:



- путь евакуації

 - ящик з піском - вогнегасник

Рис. 7.2 – Схема евакуації при пожежі

Протидія пожежам здійснюється в процесі забезпечення пожежної безпеки. Для цього встановлюються вимоги пожежної безпеки і протипожежні режими, здійснюються заходи пожежної безпеки.

У разі виникнення пожежі необхідно організувати заходи по евакуації людей з будівлі, наявними для цього всіма силами і засобами. Перевірити справність і включення в роботу автоматичних систем протипожежного захисту.

ВИСНОВКИ

У процесі роботи над дипломним проектом було проведене дослідження перспектив розвитку сучасних телекомунікаційних мереж.

Була виконана систематизація та порівняльний аналіз сучасних підходів керування телекомунікаційними компонентами, що мають забезпечувати найбільш ефективний розвиток даної галузі.

У процесі роботи були проведені систематизація і вивчення основних понять що пов`язані з ринком сучасних телекомунікацій. Розкрите поняття ролі телекомунікацій у формуванні інформаційного суспільства. Проведено аналіз та систематизація стратегічних напрямків розвитку, основних технологій телекомунікаційних мереж, квантових технологій захисту інформації , проведена оцінка ефективності побудови телекомунікаційних мереж виконано спеціальний розділ дипломного проекту.

Враховуючи стрімкий розвиток телекомунікаційних мереж майже в усіх галузях виробництва та бізнесу, можна зробити висновок про стовідсотково виправдану необхідність вкладати як фінанси, так і інтелектуальні ресурси в розвиток такого роду зв`язку та галузі взагалі.

У розділі «Заходи з охорони праці» виконаний аналіз потенційних небезпек, розроблені заходи з техніки безпеки, заходи, що забезпечують виробничу санітарію та гігієну праці, та охорони навколишнього середовища.

ПЕРЕЛІК ПОСИЛАНЬ

1.Каптур В.А. Метод мінімізації службової інформації при тунелюванні ІР-наван- таження / В.А. Каптур, Є.В. Добровольський, О.О. Яніна - Харків: Радіоелектронні і комп’ютерні системи, 2009. - № 4. - С. 91-98.

2.Алгоритм динамической адресации объектов телекоммуникационной сети / [П.П. Воробиенко, В.И. Тихонов, И.В. Смирнов, У.И. Сопина] - ОНАЗ: Цифрові технології, 2000, № 8. - С. 11-18.

3.Воробиенко П.П. Всемирная сеть Еійегпеі? / П.П. Воробиенко, Д.А. Зайцев, О.Л. Нечипорук - О.: Зв’язок. - 2007. - № 5. - С. 14-19.

4.Оцінка ефективності впровадження телекомунікаційних технологій зменшення протокольної надлишковості / [В.А. Каптур, К.Д. Гуляев, П.С. Кравченко, О.О. Яніна] - М.: Открытые информационные и компьютерные интегрированные технологии, 2011. - № 52. - С.77-88.

5.IEEE Standard for Information techno logy-Telecommunications and Information exchange between systems-Local and metropolitan area networks-Specific requirements. Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications LAN/MAN Standards Committee of the IEEE Computer Society [Електронний ресурс] - Режим доступу: <http://standards.ieee.org/about/get/802/802.3.html>

6.Хелеби C., Д. Мак-Ферсон. Принципы маршрутизации в Internet, 2-е изд. / C. Хе- леби, Д. Мак-Ферсон.; пер. с англ. - М.: Издательский дом «Вильямс», 2001. - 448 с.

7.L. Kleinrock, «Information Flow in Large Communication Nets», RLE Quarterly Progress Report, July 1961. [Електронний ресурс] - Режим доступу: <http://www.lk.cs.ucla.edu/LK/Bib/REIORT/RLEreport-11>

8.W3C Semantic Web Activity. <http://www.w3.org/2001/12/semweb-fin/w3csw>.

9.IPv4 Address Report. [Електронний ресурс] - Режим доступу: [http://www.pota- roo.net/tools/ipv4/index.html](http://www.pota-roo.net/tools/ipv4/index.html)

10.Yong Zheng. The Next Generation Network: Issues and Trends. [Електронний ресурс] - Режим доступу: <http://aut.researchgateway.ac.nz/bitstream/handle/10292/680/>

11.Воробиенко П.П. Формирование служебной информации в процессе сеанса связи сетевых компьютерных приложений / П.П. Воробиенко, М.И. Струкало, С.М. Стру- кало. - К.: 64-та науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів: матеріали конф. 4.1. Інфокомунікації. - О.: ОНАЗ ім. О.С. Попова, 1-4 грудня 2009 р. - С. 92-94.

12.Next Generation Networks Global Standards Initiative / ITU-T. [Електронний ресурс] - Режим доступу: <http://www.itu.int/en/ITU-T/gsi/ngn/Pages/default.aspx>.

13.Understanding MPLS-TP and Its Benefits. [Електронний ресурс] - Режим доступу: <http://www.cisco.com/en/US/technologies/tk436/tk428/>.

14.IP NGN-IP Next-Generation Network. [Електронний ресурс] - Режим доступу: <http://www.cisco.com/en/US/netsol/ns537/>.

15.Концепция сетевой интеграции по технологии ITT / [В.П. Семиноженко, В.М. Горицкий, П.П. Воробиенко, В.И. Тихонов] - М.: «Электросвязь», 2012. - № 6. - С. 1-6.

1. А. с. 29473 Україна. Відкрита система гнучкої адресації вузлів мережі / П.П. Воробієнко, В.І. Тіхонов; заявл. 15.07.2009.

17.А. с. 29474 Україна. Адаптивний універсальний комутатор / П.П. Воробієнко, В.І. Тіхонов; заявл. 15.07.2009.

18.А. с. 29486 Україна. Багатофункціональний мережний мета-протокол / П.П. Воробієнко, В.І. Тіхонов; заявл. 20.07.2009.

19.Пат. 46188 Україна, МПК И04Ь 12/28. Спосіб розподіленої інкапсуляції пакетів у телекомунікаційних мережах / Воробієнко П.П., Тіхонов В.І.; заявник та власник патенту Одеська національна академія зв’язку ім. О.С. Попова. - и 2009 06517; заявл. 22.06.2009; опубл. 10.12.2009, Бюл. № 23.

20.Пат. 46477 Україна, МПК И04Ь 12/28. Спосіб адаптивної адресації вузлів телекомунікаційних пакетних мереж / Воробієнко П.П., Тіхонов В.І.; заявник та власник патенту Одеська національна академія зв’язку ім. О.С. Попова. - и 2009 06513; заявл. 22.06.2009; опубл. 25.12.2009, Бюл. № 24.

21.Пат. 46761 Україна, МПК И04Ь 12/28. Спосіб адаптивної пакетної комутації в телекомунікаційних мережах / Воробієнко П.П., Тіхонов В.І.; заявники та власники патенту Воробієнко П.П., Тіхонов В.І. - и 2009 05192; заявл. 25.05.2009; опубл. 11.01.2010, Бюл. № 1.

22.Пат. 46762 Україна, МПК И04Ь 12/28. Спосіб побудови телекомунікаційних пакетних мереж з динамічною адресацією вузлів / Воробієнко П.П., Тіхонов В.І.; заявники та власники патенту Воробієнко П.П., Тіхонов В.І. - и 2009 05194; заявл. 25.05.2009; опубл. 11.01.2010, Бюл. № 1.

23.Пат. 56395 Україна, МПК И04Ь 12/28. Спосіб динамічної комутації потоків в телекомунікаційних мережах / Воробієнко П.П., Тіхонов В.І.; заявники та власники патенту Воробієнко П.П., Тіхонов В.І. - и 2010 08597; заявл. 09.07.2010; опубл. 10.01.2011, Бюл. № 1.

24.Пат. 56774 Україна, МПК H04L 12/28. Спосіб кодування якості сервісу в телекомунікаційних мережах / Воробієнко П.П., Тіхонов В.І.; заявник та власник патенту Одеська національна академія зв’язку ім. О.С. Попова. - u 2010 08668; заявл. 12.07.2010; опубл. 25.01.2011, Бюл. № 2.

25.Тихонов В.И. Оценка качества сервиса в интегрир< муникаций [Электронный ресурс] / В.И. Тихонов, О.В. Голубова - М.: Проблемы телекоммуникаций, 2010. - № 1 (1). - С. 115-125. - Режим доступа: <http://pt.journal.kh.ua/2010/> 1/1/101\_tikhonov\_itt.pdf.

1. An efficient routing protocol for wireless networks [Електронний ресурс] / Murthy Shree, Garc ia-Luna-Aceves J. J. - Hingham, MA: Kluwer Academic Publishers - 1996. - № 1. - С. 183-197. - Режим доступу: <http://portal.acm.org/citation.cfm> id=272250

27.Optimized Link State Routing Protocol (OLSR): RFC 3626 - 2003 - [Чинний від 2003-10-01]. - Internet Engineering Task Forces (IETF) - 75 с. - (Міжнародний стандарт).

1. Highly Dynamic Destination-Sequenced Distance Vector (DSDV) for Mobile Computers [Електронний ресурс] / C. E. Perkins, P. Bhagwat - SIGCOMM 1994 Conference on Communications Architectures, Protocols and Applications - C. 234-244. - Режим досту­пу: <http://www.cs.virginia.edu/~cl7v/cs851-papers/dsdv-sigcomm94.pdf>
2. Ad hoc On-Demand Distance Vector (AODV) Routing: RFC 3561 - 2003 - [Чинний від 2003-07-01]. - Internet Engineering Task Forces (IETF) - 37 с. - (Міжнародний стандарт).
3. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4: RFC 4728 - 2007 - [Чинний від 2007-02-01]. - Internet Engineering Task Forces (IETF) - 107 с. - (Міжнародний стандарт).
4. The Zone Routing Protocol (ZRP) for Ad Hoc Networks. - 2002 - [Чинний від 2002-07-01]. - Internet Engineering Task Forces (IETF) draft - 11 с. - (Проект міжнародного стандарту).
5. An Efficient ZHLS Routing Protocol for Mobile Ad Hoc Networks / Hamma T., Katoh T., Bista B.B., Takata T. - Proc. of DEXA Workshops 2006. - Р. 66-70.

Каптур В.А., Степаненко О.В. Механізм керування розподіленими ресурсами в ситуативних мережах / В.А. Каптур, О.В. Степаненко. - К.: Наукові праці ОНАЗ ім. О.С. Попова, 2010. - № 1. - С. 31-37.

1. Степаненко O.B. Алгоритми пошуку та передавання інформації в ситуативних мережах / Степаненко O.B. - М.: Радіоелектронні і комп’ютерні системи. - 2010. - № 3. - С. 75-80.
2. Пат. 55941 Україна, МПК H 04 L 12/28, H 04 L 12/407, H 04 L 29/02, H 04 L 29/06. Спосіб встановлення з’єднання між вузлами ситуативної мережі / Каптур B. А., Сте­паненко O.B.; заявник і патентовласник Одеська національна академія зв’язку ім. О.С. Попова. - u201008903; заявл. 16.07.10; опубл. 27.12.10, Бюл. № 24.
3. Каптур В.А., Степаненко O.B. Моделювання процесів передавання інформації в ситуативних мережах / B.A. Каптур, O.B. Степаненко - К.: Наукові праці ОНАЗ ім. O.a Попова, 2011. - № 1. - С. 31-37.
4. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / [С.П. Кулик, Е.А. Шапиро (пер. с англ.); С.П. Кулик, Т.А. Шмаонов (ред. пер.); Д. Боумейстер и др. (ред.)]. - М.: Постмаркет, 2002. - С. 33-73.
5. Gisin N. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden - Review of Modern Physics. - 2002. - V. 74, issue 1. - P. 145-195.
6. Applied Quantum Cryptography / Kollmitzer C., Pivk M. (eds.). - Springer-Verlag, Berlin, Heidelberg, 2010. - 227 p.
7. Korchenko O. Quantum Secure Telecommunication Systems / O. Korchenko, P. Vorobiyenko, M. Lutskiy, Ye. Vasiliu, S. Gnatyuk - Telecommunications Networks - Current Status and Future Trends (Edited by J.H. Ortiz). - InTech, 2010. - P. 211-236.
8. Bасилиу E.B., Bоробиенко П.П. Проблемы развития и перспективы использова­ния квантово-криптографических систем / E.B. Bасилиу, П.П. Bоробиенко - К.: Наукові праці OHAЗ ім. O.С.Попова, 2006. - № 1. - С. 3-17.
9. Корченко O.r. Сучасні квантові технології згхисту інформації / O.r. Корченко, C.B. Bасіліу, СЮ. Гнатюк - Журн.: Науково-технічний журнал «Захист інформації», 2010. - № 1. - С. 77-89.
10. Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger - Physical Review Letters. - 2002. - V. 89, issue 18. - 187902.
11. Ostermeyer M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta - Optics Communications. - 2008. - V. 281, issue 17. - P. 4540-4544.
12. Bасилиу E.B., Николаенко СШ. Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений / E.B. Bасилиу, СШ. Николаенко. - К.: Наукові праці OHAЗ ім. O.^ Попова, 2009. - № 1. - С. 83-91.
13. Bасіліу C.B. Синтез структури квантових систем прямого безпечного зв’язку / C.B. Bасіліу. - К.: Цифрові технології, 2011. - № 9. - С. 20-30.
14. Hillery M. Quantum secret sharing / M. Hillery, V. Buzek, A. Berthiaume - Physical Review A. - 1999. - V. 59, issue 3. - P. 1829-1834.
15. Yan F.-L. Quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations / F.-L. Yan, T. Gao, Yu.-Ch. Li - Chinese Physics Letters. - 2008. - V. 25, issue 4. - P. 1187-1190.
16. Hirota O. Quantum stream cipher by the Yuen 2000 protocol: Design and experi­ment by an intensity-modulation scheme / O. Hirota, M. Sohma, M. Fuse, K. Kato. - Physical Review A. - 2005 - V. 72, issue 2. - 022335.
17. Corndorf E. Quantum-noise randomized data encryption for wavelength-division- multiplexed fiber-optic networks / E. Corndorf, C. Liang, G.S. Kanter [et al.] - Physical Review A. - 2005. - V. 71, issue 6. - 062326.
18. Wang J. Quantum signature scheme with single photons / J. Wang, Q. Zhang, Tang - Optoelectronics Letters. - 2006. - V. 2, issue 3. - P. 209-212.

Gottesman D. Quantum digital signatures [Електронний ресурс] / D. Gottesman, Chuang. - Режим доступу: <http://arxiv.org/abs/quant-ph/0105032>

1. Natori S. Why Quantum Steganography Can Be Stronger Than Classical Steganography / S. Natori - Quantum Computation and Information, Topics Appl. Phys. - V. 102. - P. 235-240.
2. Martin K. Steganographic communication with quantum information / K. Martin - Lecture Notes in Computer Science. - 2007. - V. 4567. - P. 32-49.
3. Сучасні методи квантової стеганографії / [Г.Ф. Конахович, О.В. Шевченко, В.М. Кінзерявий, Ю.Є. Хохлачова]. - К.: Науково-технічний журнал «Захист інформації», 2011. - № 2 (51). - С. 82-86.
4. Lo H.-K. Quantum cryptography / H.-K. Lo, Yi Zhao - Encyclopedia of Complexity and Systems Science. - N.Y.: Springer US, 2009. - V. 8. - P. 7265-7289.
5. Peng C.-Z. Experimental long-distance decoy-state quantum key distribution based on polarization encoding / C.-Z. Peng, J. Zhang, D. Yang [et al.] - Physical Review Letters. - V. 98, issue 1. - 010505.
6. Zhang Q. Megabits secure key rate quantum key distribution / Q. Zhang, H. Takesue, T. Honjo [et al.] - New Journal of Physics. - 2009. - V. 11, issue 4. - 045010.
7. Yuan Z.L. Practical gigahertz quantum key distribution based on avalanche photo­diodes / Z.L. Yuan, A.R. Dixon, J.F. Dynes [et al.] - New Journal of Physics. - 2009. - V. 11, issue 4. - 045019.
8. Атаки в квантових системах захисту інформації / [О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк, В.М. Кінзерявий]. - Журн.: Вісник інженерної академії України, 2010. - № 3-4. - С. 124-133.
9. Scarani V. The security of practical quantum key distribution / V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf [et al.] - Review of Modern Physics. - 2009. - V. 81, issue 3. - P. 1301-1350.
10. Cerf N.J. Security of quantum key distribution using d-level systems / N.J. Cerf,hysical Review Letters. - 2002. - V. 88, issue 12. -y distribution using multilevel encoding / M. Bourennane, Karlsson, G. Bjork - Quantum Communication, Computing, and Measurement 3. - N.Y.: Spiinger US, 2002. - P. 295-298.
11. Durt t. Security of quantum key distributions with entangled qudits / T. Durt, D. Kaszlikowski, J.-L. Chen, L. C. Kwek - Physical Review A. - 2004. - V. 69, № 3. - 032313.
12. QUANTIS: True Random Number Generator [Електронний ресурс]. - Режим доступу: <http://www.idquantique.com/true-random-number-generator/products-overview.html>
13. QPN Security Gateway (QPN-8505) [Електронний ресурс]. - Режим доступу: <http://www.magiqtech.com/MagiQ/Products.html>
14. Cerberis [Електронний ресурс]. - Режим доступу: <http://www.idquantique.com/> products/cerberis.htm
15. QKS. Toshiba Research Europe Ltd., Cambridge Research Laboratory [Електронний ресурс]. - Режим доступу: [http://www.toshiba-europe.com/research/crl/qig/quantumkey- server.html](http://www.toshiba-europe.com/research/crl/qig/quantumkey-server.html).
16. Elliot C. Quantum Cryptography in Practice / C. Elliot, D. Pearson, G. Troxel - Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. - 2003. - P. 227-238.
17. Hadfield R.H. Single-photon detectors for optical quantum information applications / R.H. Hadfield - Nature Photonics. - 2009. - V. 3, num. 12. - P. 696-705.
18. Таненбаум Э. Компьютерные сети / Э. Таненбаум. - СПб.: Питер, 2005. - 992 с.
19. Generic Routing Encapsulation over IPv4 networks. [Електронний ресурс] /

S. Hanks, T. Li, D. Farinacci, P. Traina - RFC 1702. - Режим доступу:

<http://www.faqs.org/rfcs/rfc1702.html>

Perkins C. IP Encapsulation within IP [Електронний ресурс] / C. Perkins - RFC 2003. - Режим доступу: <http://www.faqs.org/rfcs/rfc2003.html>

1. Каптур B.A., Сініна Д.І. Визначення достатньої пропускної спроможності взаємопідімкнення мереж з комутацією пакетів / B.A. Каптур, Д.І. Сініна - К.: Наукові праці ОНАЗ ім. О.С. Попова: збірник наукових праць Одеської національної академії зв’язку ім. О.С. Попова. - № 1. - Одеса, - 2008. - C. 44-52.
2. Casner S. Compressing IP/UDP/RTP Headers for Low-Speed Serial Links [Електронний ресурс] / S. Casner, V. Jacobson. - RFC2508.Режимдоступу:<http://www.faqs.org/rfcs/rfc2508.html>
3. Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering [Електронний ресурс] / T. Koren, S. Casner, J. Geevarghese, B. Thompson, P. Ruddy - RFC 3545 - Режим доступу: <http://www.faqs.org/rfcs/rfc3545.html>
4. IAX: Inter-Asterisk eXchange Version 2 [Електронний ресурс] / M. Spencer, B. Capouch, E. Guy, F. Miller, K. Shumard - RFC 5456. - Режим доступу: [http://www.rfced- itor.org/authors/rfc5456.txt](http://www.rfced-itor.org/authors/rfc5456.txt)
5. Thompson B. Tunneling Multiplexed Compressed RTP (TCRTP) [Електронний ресурс] / B. Thompson, T. Koren, D. Wing - RFC 4170Режим доступу:<http://www.faqs.org/rfcs/rfc4170.html>
6. RFC 791. INTERNET PROTOCOL [Електронний ресурс]. - Режим доступу: <http://www.faqs.org/rfcs/rfc793.html>. - Назва з екрана.
7. Пат. 35773 Україна, Спосіб передачі даних в мережі із заміщенням мережного та транспортного рівнів універсальною технологією канального рівня - Воробієнко П.П., Зайцев Д.А., Гуляєв К.Д.; заявник і патентовласник Одеська національна академія зв’язку ім. О.С. Попова. - опубл. 27.12.10.
8. Каптур В.А. Метод мінімізації службової інформації при тунелюванні IP-навантаження / В.А. Каптур., Є.В. Добровольський, О.О. Яніна. - М.: Радіоелектронні і комп’ютерні системи, 2009. - № 4. - С. 91-98.
9. Алгоритм динамической адресации эбьектсв телекоммуникационной сети / [П.П. Воробиенко, В.И. Тихонов, И.В. Смирнов, У.И. Сопина]. - К.: Цифрові технології, 2010. - № 8. - С. 11-18.
10. Моделирование процессов формирования служебной информации при передаче данных в сетях с коммутацией пакетов / [П.П. Воробиенко, М.И. Струкало, И.Ю. Рожнов- ская, С.М. Струкало] - К.: Наукові праці ОНАЗ. - 2009. - № 1. - С. 3-12.
11. Каптур В.А. Протокол організації віртуальних пірингових каналів в локальних комп’ютерних мережах / Каптур В.А. - К.: Наукові праці ОНАЗ ім. О.С. Попова. - 2006. - № 2. - C. 85-95.
12. Олифер Н.А. Средства анализа и оптимизации локальних сетей / Н.А. Олифер, В.Г. Олифер. - [Электронный ресурс]. - Режим доступа: <http://www.dlink.ru/technology> /olifer.php. - Название с екрана.
13. Виленский П.Л. Оценка эффективности инвестиционных проектов. Теория и практика / П.Л. Виленский, В.Н. Лившиц, С.А. Смоляк. - М.: Дело, 2008. - 1104 с.
14. Пат. 76720 Україна, МПК H04L 12/28. Спосіб динамічної адресації об’єктів телекомунікаційних мереж / Воробієнко П.П., Лемешко О.В., Смірнов І.В., Тихонова О.В.; заявник та власник патенту Одеська національна академія зв’язку ім. О.С.Попова. - u 2012 08535; заявл. 10.07.2012; опубл. 10.01.2013, Бюл. № 1