МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Харківський національний університет внутрішніх справ

Факультет № 6
Кафедра кібербезпеки та DATA-технологій

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ З СЕМІНАРСЬКИХ ЗАНЯТЬ

з дисципліни «Телекомунікаційні системи та мережі нового покоління»

Галузь знань :12 - „Інформаційні технології”

Спеціальність : 125 „ Кібербезпека”

Спеціалізація : протидія кіберзлочинності

Ступень вищої освіти - бакалавр

м. Харків
2023 р.

Передмова

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від _30 .01.23_ № 1 _ _

СХВАЛЕНО
Вченою радою факультету № 6
Протокол від 13 .01.23 №1

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 27 .01.23 № 1

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій
(*протокол від* 13 .01.23 № 1 _ _)

Розробники:
1. *Професор кафедри, д.т.н., професор Семенов С.Г.*
2. *Професор кафедри, д.т.н., проф. Можаєв О.О.*
3. *Завідувач кафедри, к.т.н., Гнусов Ю.В.*

Рецензенти:
Клімушин П.С. доцент кафедри боротьби з кіберзлочинністю ХНУВС, к.т.н., доцент;
Коваленко А.А. д.т.н., професор, завідувач кафедри ЕОМ ХНУРЕ

ЗМІСТ

ВСТУП

Розвиток Інтернету та впровадження цифрових послуг зв’язку (IP телефонія, цифрове телебачення типу DVB-T та IP-TV) привело до докорінної зміни концепцій побудови мереж доступу та транспортних мереж, а також телекомунікаційних систем передачі, що входять до їх складу. З метою надання гнучкості при створенні та наданні послуг, а також для зменшення їх собівартості, сьогодні при побудові нових фрагментів телекомунікаційних мереж широко застосовується концепція мереж наступних поколінь (Next Generation Network, NGN). Вона передбачає розподіл функцій мережі на три групи: транспортування, послуг та управління.

Згідно концепції мереж наступних поколінь, сучасні системи передавання повинні забезпечувати транспортування пакетного трафіка волоконно-оптичними лініями та системами зв’язку. Технологія SDH нової генерації (NG-SDH) відноситься до транспортного рівня NGN і дозволяє ефективно організовувати широкосмугові канали передавання пакетного трафіка. Це дозволяє виконувати побудову нових фрагментів мереж доступу та модернізацію існуючих транспортних мереж SDH із застосуванням даного типу технології.

Головною метою дисципліни “Телекомунікаційні системи мереж наступних поколінь” є формування у студентів системи понять та сукупності знань і умінь, необхідних у практичній роботі напряму “Телекомунікації” зі спеціалізації "Телекомунікаційні системи та мережі" при експлуатації сучасних телекомунікаційних систем зв’язку, що входять до складу мереж, що побудовані згідно концепції побудови мереж наступних поколінь (NGN).

СЕМІНАРСЬКЕ ЗАНЯТТЯ № 1

Тема: Принципи побудови та конфігурування мультиплексорів NG-SDH

Мета: ознайомитися з побудовою, технічними характеристиками та основами конфігурування синхронного мультиплексора NG-SDH на прикладі обладнання uMSPP-155e фірми Hitron Technologies.

Ключові положення

Мультисервісна платформа обслуговування uMSPP-155e (англ. Micro Multi-services Provisioning Platform) є компактним волоконно-оптичним мультиплексором NG-SDH рівня STM-1 з можливістю транспортування пакетного трафіка Ethnernet і застосуванням схеми резервування оптичного тракту 1+1. Оптичні інтерфейси дозволяють використовувати в якості середовища поширення оптичні волокна, що задовольняють рекомендаціям МСЕ-Т G.652, G.653 і G.655 [1]. Сучасна модульна конструкція (рис. 1.1) дозволяє формувати STM-1 з використанням відповідних канальних плат для підключення низькошвидкісних цифрових потоків T1/E1 (G.703 або G.704), трибів V.35 і 10/100M Ethernet. На базі мультиплексора можлива побудова мереж з топологіями "точка-точка " та "кільце". Зазначені особливості дозволяють будувати ефективні мережі доступу з використанням даного типу обладнання.

Рисунок 1.1 – Зовнішній вигляд мультисервісної платформи uMSPP-155e

Обладнання включає наступні елементи:

1) шасі мультиплексора uMSPP-155 з 4 слотами для розміщення канальних плат і двох оптичних модулів;
2) плата QET (канальна плата на 4 потоки T1/E1);
3) плата DQE (канальна плата на 8 потоків T1/E1);
4) плата EOS (плата Ethernet на 4 порти 10/100 Base-T);

5) оптичні модулі для підключення оптичних волокон.

Основні параметри оптичних модулів подані в додатку А.

Подані технічні параметри дозволяють зробити наступний висновок: при використанні чотирьох канальних плат QET і DQE (максимально допустима кількість для шасі MSPP-155), можлива передача всього 16 і 32 цифрових потоків T1/E1 відповідно, що суттєво менше інформаційної ємності STM-1 в 63 потоки E1. Таке неефективне використання ресурсів STM-1 викликане позиціонуванням мультиплексора uMSPP-155e для транспортування пакетного трафіка 10/100M Ethernet. У випадку використання однієї інтерфейсної плати EOS та заповненні інших трьох слотів канальними платами DQE (на 8 потоків T1/E1 кожна) під транспортування пакетного трафіка залишаються доступними 63-3*8=39*VC-12.

Більша частина функціональних блоків розташована усередині шасі uMSPP-155. На лицьовій панелі (рис. 1.2) розташовані необхідні органи управління (клавіатура, інтерфейси RS-232 і RJ-45) та індикації (рідкокристалічний індикатор та індикатори стану трибутарних інтерфейсів), а також два слоти під модулі оптичних інтерфейсів. Задня панель має чотири слоти для встановлення трибутарних плат з відповідними інтерфейсами.

Схема з'єднання функціональних елементів uMSPP-155e між собою показана на рис. 1.3. Шасі мультиплексора містить блок мультиплексування трафіка (згідно рек. MCE-T G.707/Y.1322) і блок управління, що формує відповідні сигнали для елементів мультиплексора. Також є чотири слоти для підключення трибутарних канальних плат (на задній панелі) і два слоти для підключення оптичних модулів (на передній панелі).

Для управління та індикації використовуються наступні елементи:

1) світлодіодні індикатори на передній панелі мультиплексора, які дозволяють контролювати наявність трибутарних сигналів та оперативно діагностувати виникаючі несправності;
2) рідкокристалічний індикатор (РКІ), який у комплекті з 4-х клавішною клавіатурою на передній панелі мультиплексора дозволяє проводити настроювання модулів мультиплексора та моніторинг їх стану;
3) інтерфейсне гніздо RS-232 для підключення персонального комп'ютера (ПК) з термінальною програмою для повноцінного конфігурування мультиплексора;
4) інтерфейсне гніздо RJ-45 для підключення системи управління мережею NMS (англ., Network Management System).

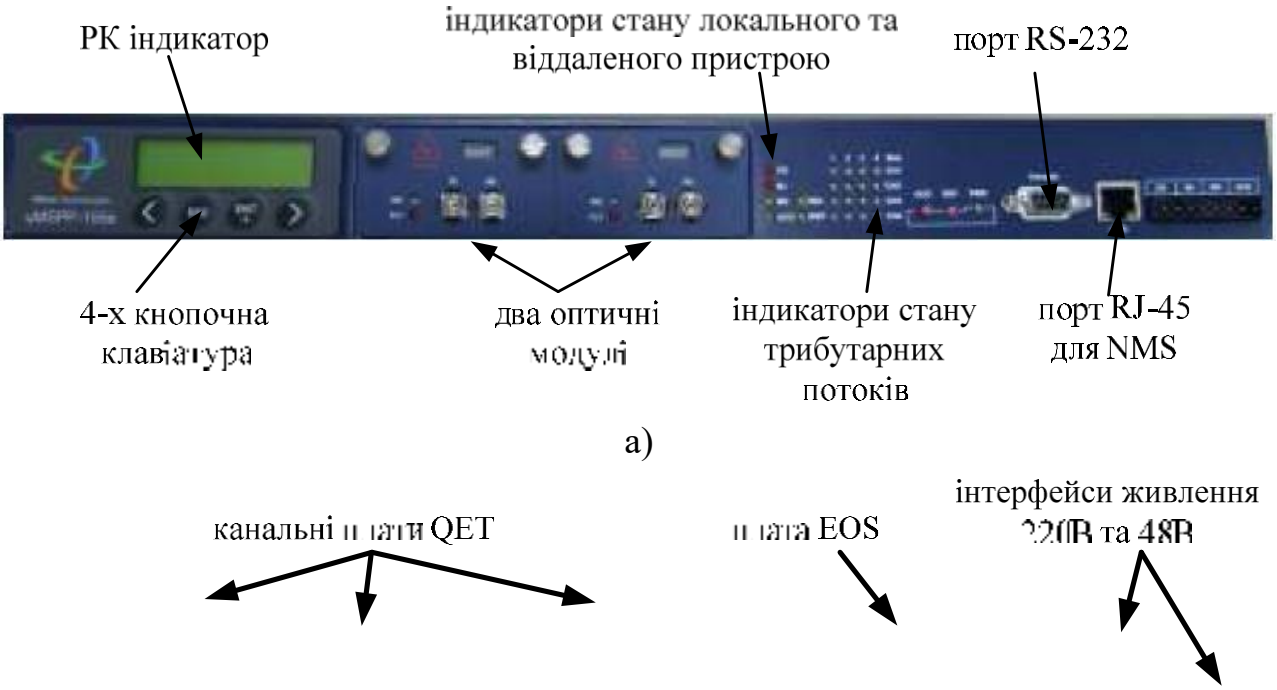


Рисунок 1.2 – Зовнішній вигляд:
а) лицьової панелі мультиплексора;
б) задньої панелі мультиплексора

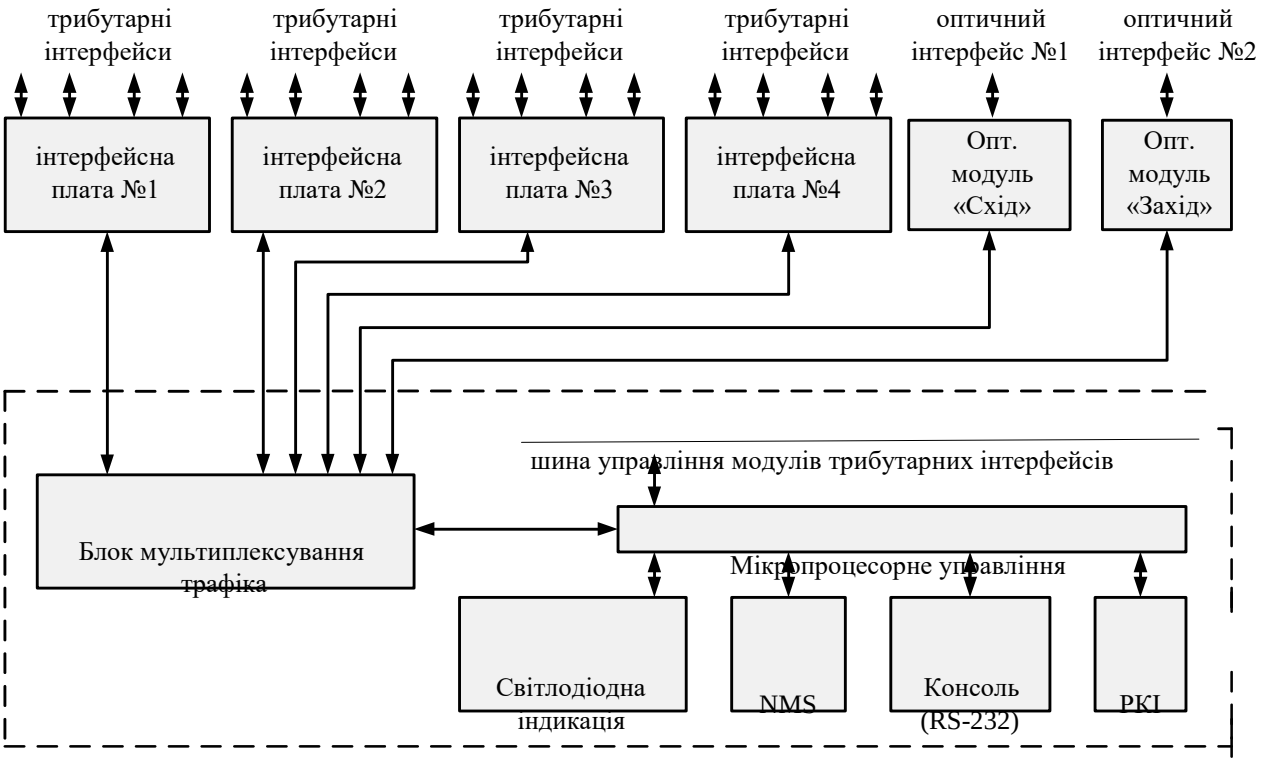


Рисунок 1.3 – Блок-схема мультисервісної платформи обслуговування uMSPP-155e

Моніторинг стану та управління мультиплексором здійснюється трьома способами:

1) за допомогою РКІ та клавіатури на лицьовій панелі мультиплексора;
2) дистанційно за допомогою системи NMS;
3) локальним терміналом, який підключений до інтерфейсу RS-232.

Останній варіант є найбільш зручним і передбачає використання термінальної програми, що виконується на стандартному персональному комп'ютері (рис. 1.4). Мультиплексор, до якого проводиться підключення ПК, називається локальним (англ. *local*), а інший мультиплексор – віддаленим (англ., *remote*). Після виконання стандартної процедури встановлення з'єднання, на екрані ПК виводиться основне меню, що складається із шести пунктів (його загальний вигляд і призначення кожного з пунктів подано у додатку Б).

Рисунок 1.4 – Підключення ПК до мережі NG-SDH з топологією "точка-точка"

Контрольні питання

1. Вкажіть призначення мультиплексора uMSPP-155e.
2. Які варіанти архітектур мереж SDH можливо будувати з використанням мультиплексора uMSPP-155e?
3. Які функціональні блоки входять до складу мультиплексора?
4. Які функції виконують плати QET, DQE та EOS?
5. Перелічіть способи моніторингу стану та управління мультиплексором.

Домашнє завдання

1. Вивчити ключові положення.
2. Ознайомитися із процедурою конфігурування мультиплексора згідно із лабораторним завданням.
3. *Розв'язати завдання.* В мультиплексорі uMSPP-155e для транспортування мовного трафіка використовуються $N_{вар}$×VC-12, де $N_{вар}$ - номер студента за журналом підгрупи ($1 \le N_{вар} \le 16$). Визначити кількість VC-12, які залишаються доступними для транспортування пакетного трафіка Ethernet та відповідну їм кількість інтерфейсних плат QET/DQE.
4. У лабораторному зошиті підготувати бланк протоколу і зарисувати схему мультиплексора.

Завдання

1. Здійснити підключення ПК із встановленою термінальною програмою до мультиплексора uMSPP-155e згідно з рис. 1.5. Тумблером "220 В" увімкнути живлення мультиплексора та дочекатися закінчення процесів самодіагностики, що виконуються після його увімкнення.
2. Підключити перетворювач інтерфейсу RS-232-USB у вільний порт USB робочої станції (PC). Кликнути правою кнопкою миші на іконці "Мій комп'ютер", перейти в меню "Диспетчер пристроїв" і в розділі "Порти (COM і LPT)" знайти пристрій "Prolific Usb-to-Serial Comm Port" (або аналогічний, згідно із вказівками викладача). Записати номер віртуального послідовного порту, який привласнений приєднаному пристрою.
3. Запустити програму "Hyperterminal" або її аналог. Створити нове з'єднання згідно з параметрами з'єднання, поданими в табл. 1.1.

Таблиця 1.1 – Параметри з'єднання

Швидкість, біт/з	Біти даних	Парність	Стопові біти	Управління потоком
115200	8	немає	1	немає

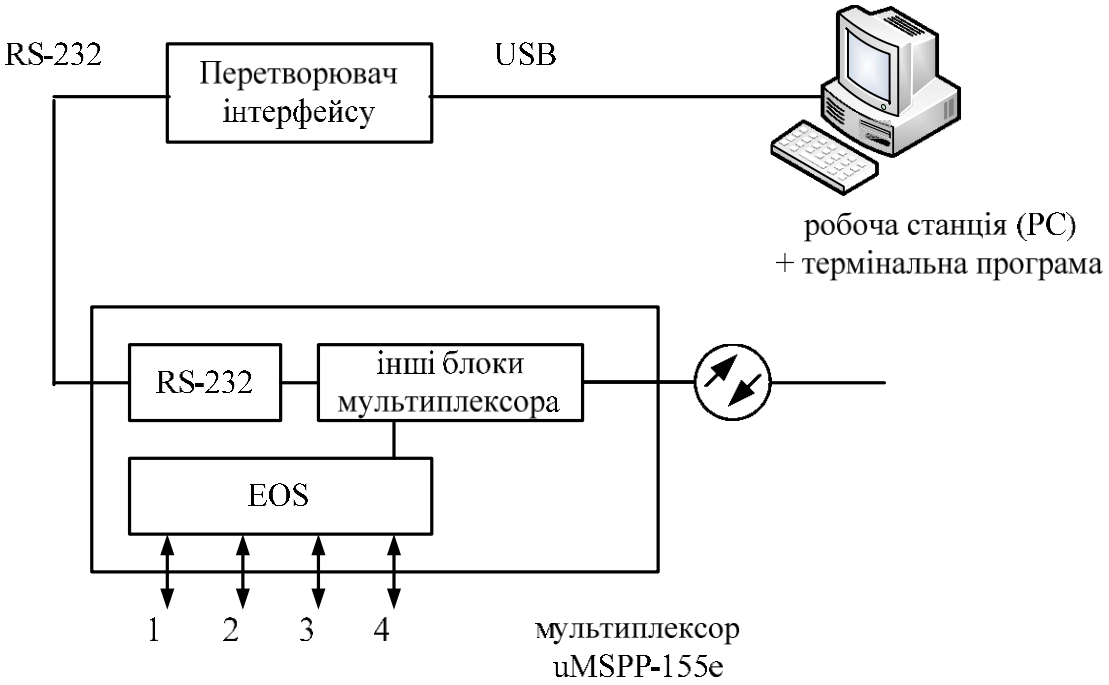


Рисунок 1.5 – Схема підключення терміналу до uMSPP-155e

4. Кілька разів натиснути клавішу "Enter" для появи меню логіна користувача та увести дані згідно з рис. 1.6. Перехід між полями даного меню здійснюється шляхом натискання клавіші "Tab". Після успішного проходження процедури аутентифікації в терміналі відобразиться основне меню мультиплексора зі структурою, зображеною на рис. Б.1 (див. додаток Б). Перехід між пунктами виконується за допомогою клавіш управління курсором "←", "→", "↑" і "↓". Вибір необхідного пункту меню здійснюється натисненням клавіші "Enter".

Рисунок 1.6 – Меню ідентифікації користувача uMSPP-155e

5. Огляд стану та конфігурування плати QET.

5.1 Перейти в пункт головного меню "Config" – "Rtrv Summary" і натиснути клавішу "2" (QET Interface) для відображення конфігурації плати QET. Порівняти її поточні установки з установками за замовчуванням (рис.

1.7) та у випадку їх збігу перейти до пункту 5.3 лабораторного завдання, пропустивши пункт 5.2.

5.2 Перейти в пункт головного меню "Config" – "Agg/Tri Setting" і натиснути клавішу "2" (QET Interface) для переходу в меню редагування параметрів плати QET. Виконати установку параметрів конфігурації плати QET за замовчанням згідно з рис. 1.8. Перехід між параметрами (Slot ID, Channel ID, Mode і т.д.) виконується за допомогою клавіш управляння курсором "←" і "→". Зміна значення параметра виконується за допомогою клавіш "↑" і "↓". Зберегти встановлені параметри в енергонезалежній пам'яті мультиплексора натисканням на клавішу "S".

Type	Slot	Port	Svc	Mode	Code	Frame	Imped	L-Len	Loopback
QET	1	1	IS	E1	HDB3	Unf	120 ohm	*	No LPBK
QET	1	2	IS	E1	HDB3	Unf	120 ohm	*	No LPBK
QET	1	3	IS	E1	HDB3	Unf	120 ohm	*	No LPBK
QET	1	4	IS	E1	HDB3	Unf	120 ohm	*	No LPBK

Press any Key to Exit

Рисунок 1.7 – Установки плати QET за замовчуванням

Tributary Setting: QET (Local)

Slot ID..... 1 Channel ID..... ALL

Mode..... E1 Code..... HDB3

Frame..... Unframe Impedance..... 120 ohm

LBO..... Service State..... IS

<< TCA Threshold (Default) >>

Set All 0

	L.CV	L.ES	L.SES	L.UAS	P.CV	P.ES	P.SES	P.UAS
Qtr	369	180	45	18	415	180	45	18
Hour	1475	720	180	72	1659	720	180	72
Day	35400	17280	4320	1728	39813	17280	4320	1728

Press s:Save, ESC:Exit

Рисунок 1.8 – Меню установки параметрів плати QET

5.3 Перейти в пункт головного меню "Config" – "Agg/Tri Setting" і натиснути клавішу "2" (QET Interface) для переходу в меню редагування параметрів плати QET. Згідно з номером бригади і табл. 1.2 виконати почергове

редагування та збереження параметрів плати QET для кожного порту. Перехід між параметрами (Slot ID, Channel ID, Mode і т.д.) виконується за допомогою клавіш управляння курсором "←" і "→". Зміна значення параметра виконується за допомогою клавіш "↑" і "↓". Збереження встановленого значення параметра в енергонезалежній пам'яті мультиплексора виконується після натиснення на клавішу "S".

5.4 Перейти в пункт головного меню "Config" – "Rtrv Summary" і натиснути клавішу "2" (QET Interface) для відображення конфігурації плати QET. Порівняти поточну конфігурацію плати із заданою в табл. 1.2, записавши в робочий зошит встановлені значення параметрів плати.

Таблиця 1.2 – Варіанти конфігурації плати QET

№ бригади	№ слота (Slot ID)	№ порту (Channel ID)	Режим (Mode)	Код (Code)	Тип циклу (Frame)	Стан порту (Service State)
1	1	1	E1	AMI	Unf	IS IS
	1	2	E1	AMI	Unf	IS IS
	1	3	T1	B8ZS	Unf	IS IS
	1	4	T1	B8ZS	Unf	OOS
2	1	1	E1	AMI	Unf	OOS
	1	2	T1	AMI	Unf	IS
	1	3	T1	B8ZS	Unf	OOS
	1	4	E1	HDB3	Unf	OOS
3	1	1	E1	HDB3	Unf	IS
	1	2	T1	B8ZS	Unf	OOS
	1	3	E1	HDB3	Unf	IS
	1	4	T1	AMI	Unf	OOS
4	1	1	T1	AMI	Unf	IS
	1	2	T1	B8ZS	Unf	
	1	3	E1	HDB3	Unf	
	1	4	E1	AMI	Unf	

6. Огляд стану та конфігурування плати EOS.

6.1 Перейти в пункт головного меню "Config" – "Rtrv Summary" і натиснути клавішу "3" (EOS Interface) для відображення поточної конфігурації плати EOS (рис. 1.9). У випадку наявності одного або декількох відключених трибутарних портів (параметр Service має значення OOS), перейти до пункту 6.2 лабораторного завдання для скидання установок плати у вихідний стан. В іншому випадку перейти до виконання пункту 6.3.

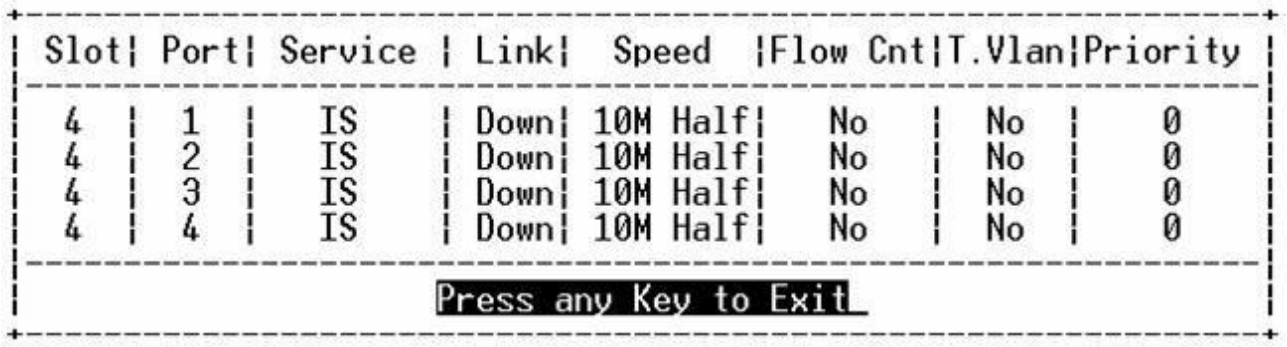


Рисунок 1.9 – Параметри плати EOS за замовчуванням

6.2 Перейти в пункт головного меню "Config" – "Agg/Tri Setting" і натиснути клавішу "3" (EOS Interface) для переходу в меню редагування параметрів плати EOS (рис. 1.10). Натиснути клавішу "b" (Reset to Default) і підтвердити скидання установок плати у вихідний стан.

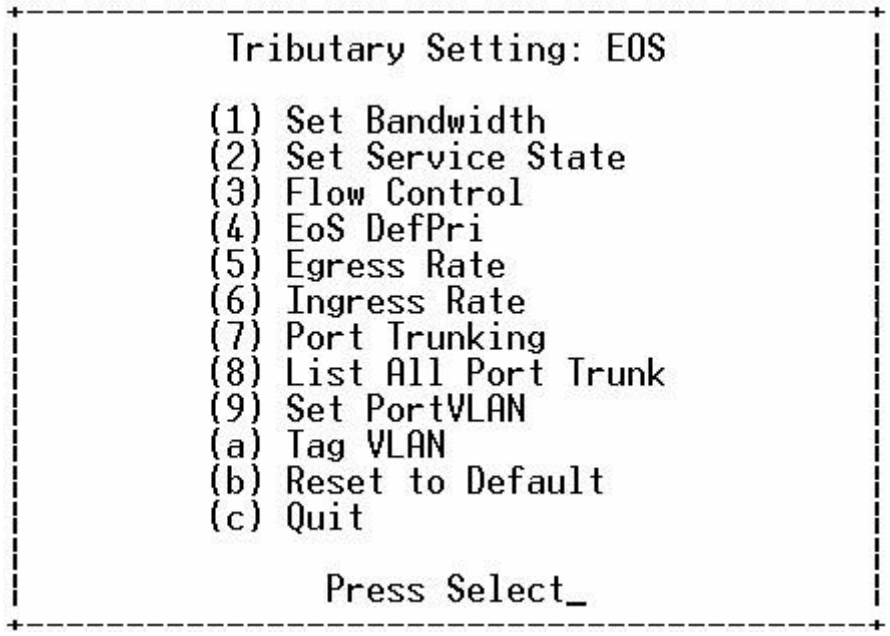


Рисунок 1.10 – Меню редагування параметрів плати EOS

6.3 Вибрати пункт головного меню "Config" – "Agg/Tri Setting" і натиснути клавішу "3" (EOS Interface) для переходу в меню редагування параметрів плати EOS. Натиснути клавішу "2" (Set Service State), вибрати необхідний номер слота (Slot ID) та порту (Port ID), та встановити значення параметра Service State згідно з табл. 1.3. Зміна значення параметра виконується за допомогою клавіш управління курсором "↑" і "↓". Перехід між параметрами здійснюється шляхом натискання клавіші "Enter".

Таблиця 1.3 – Варіанти конфігурації плати EOS

№ бригади	№ слота (Slot ID)	№ порту (Object ID)	Стан порту (Service State)	Пріоритет
1	4	1	IS IS	0
	4	2	OOS	1
	4	3	OOS	2
	4	4	IS	3
2	4	1	OOS	0
	4	2	OOS	0
	4	3	IS	1
	4	4	OOS	1
3	4	1	IS	0
	4	2	OOS	2
	4	3	IS IS	3
	4	4	IS IS	0
4	4	1	IS	2
	4	2		3
	4	3		1
	4	4		0

6.4 Вибрати пункт головного меню "Config" – "Agg/Tri Setting" і натиснути клавішу "3" (EOS Interface) для переходу в меню редагування параметрів плати EOS (рис. 1.10). Натиснути клавішу "4" (EoS DefPri), вибрати необхідний номер слота (Slot ID), порту (Object ID) та встановити значення параметра Default Priority згідно з табл. 1.2.

6.5 Перейти в пункт головного меню "Config" – "Rtrv Summary" і натиснути клавішу "3" (EOS Interface) для відображення поточної конфігурації плати EOS (рис. 1.9). Порівняти поточну конфігурацію плати із заданою в табл. 1.2 і записати в робочий зошит відображувані значення параметрів.

7. Вибрати пункт головного меню "System" – "Log Out" та підтвердити завершення поточного сеансу роботи користувача root.

СЕМІНАРСЬКЕ ЗАНЯТТЯ № 2

Тема: Віртуальна конкатенація в системах NG-SDH

Мета: вивчити особливості реалізації процедури віртуальної конкатенації на прикладі мультисервісної платформи uMSPP-155e

Ключові положення

Технологія SDH, що розроблена в 1988 році для побудови високошвидкісних оптичних мереж є синхронною технологією з комутацією каналів. Вона підтримує транспортування стандартних потоків PDH типу E1, E3 та E4 (2, 34 і 140 Мбіт/с відповідно) та передбачає упаковку вищевказаних потоків у віртуальні контейнери VC-1, VC-3 і VC-4 відповідно. Далі група сформованих VC побайтово мультиплексується в синхронний транспортний модуль рівня *N* (STM-N).

Синхронні мережі нового покоління, що дозволяють додатково транспортувати також і пакетний трафік, одержали умовну назву NG-SDH (New Generation SDH). Структурна схема мультиплексора NG-SDH (рис. 2.1) містить три блоки:

1) попереднього оброблення пакетного трафіка; 2)
формування широкосмугового каналу передачі; 3)
формувач STM-N.

Попереднє оброблення пакетного трафіка необхідне для полегшення процесу упаковки трафіка користувача в STM-N і передбачає використання одного з наступних методів:

1) процедури доступу до ланки передачі SDH (LAPS/X.86);
2) процедури пакетування поверх SDH (Packet over SDH, PoS);
3) основної процедури фреймування (Generic Framing procedure, GFP).

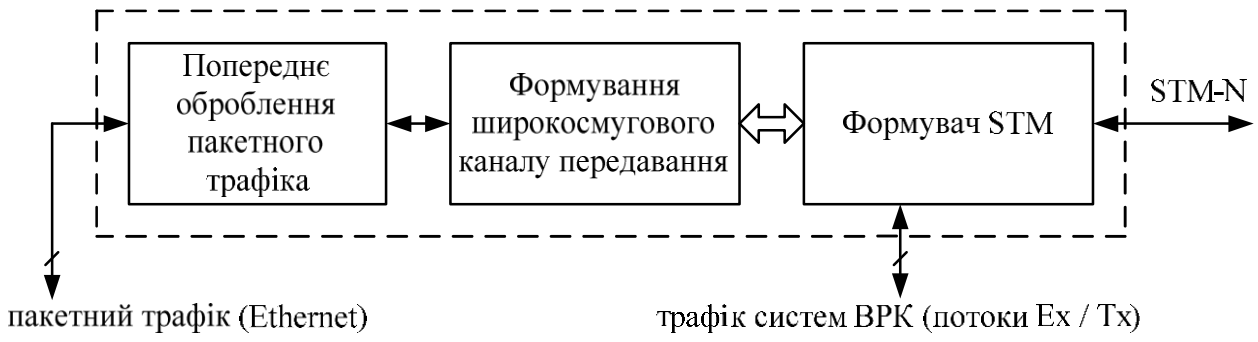


Рисунок 2.1 – Структурна схема мультиплексора NG-SDH

На вході блока попереднього оброблення формується потік, що містить допоміжні інформаційні структури, які згодом будуть розміщені в STM-N. На сьогодні найбільше поширення одержала основна процедура фреймування. У цьому випадку потік на виході блока попереднього оброблення складається з послідовності кадрів GFP. Інкапсуляція трафіка користувача може здійснюватися двома режимами:

1) основна процедура фреймування з відображенням кадрів GFP-F (Frame-mapped GFP);
2) прозора основна процедура фреймування GFP-T (Transparent GFP).

В обладнанні uMSPP-155e використовується режим GFP-F, який продемонстрований на рис. 2.2.

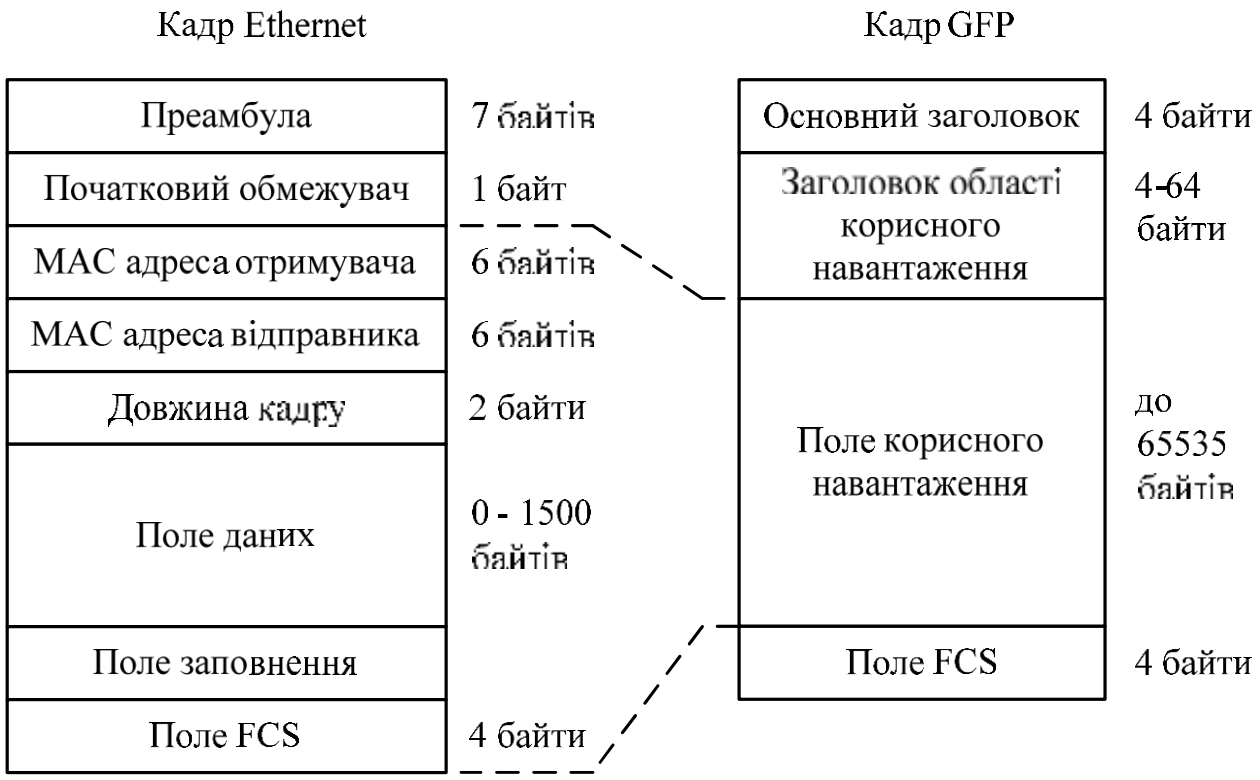


Рисунок 2.2 – Інкапсуляція кадру Ethernet в кадр GFP

Рекомендація ITU-T G.707 дозволяє організувати в STM-N широкосмуговий канал передачі шляхом об'єднання ресурсів (конкатенації) кількох інформаційних структур з низькою пропускною здатністю.

Перший варіант об'єднання одержав назву суміжної конкатенації (contiguous concatenation, CAT) і припускає формування мультиконтейнерів типу VC-4-Xc (SDH) або VC-2-Xc (SONET/SDH). На рис. 2.3 показана структура мультиконтейнера типу VC-4-Xc. Він складається з маршрутного заголовка POH (Path Overhead) розміром 9·X байт, у якому використовується

тільки заголовок першого VC-4 (перший стовпець), а інші 9·(X-1) байт у стовпцях (2-X) є фіксованим заповненням розміру. Поле корисного навантаження мультиконтейнера VC-4-Xc містить 260·X байт і містить X адміністративних блоків AU-4 з побайтовим мультиплексуваням. Оскільки структура суміжних полів розглядається як єдине ціле, то для визначення її місця розташування досить одного РОН першого VC-4, розташованого в першому AU-4. Покажчик цього AU-4 визначає позицію байта J1 першого VC-4 у мультиконтейнері VC-4-Xc. Швидкості стандартних мультиконтейнерів для суміжної конкатенації подані в табл. 2.1.

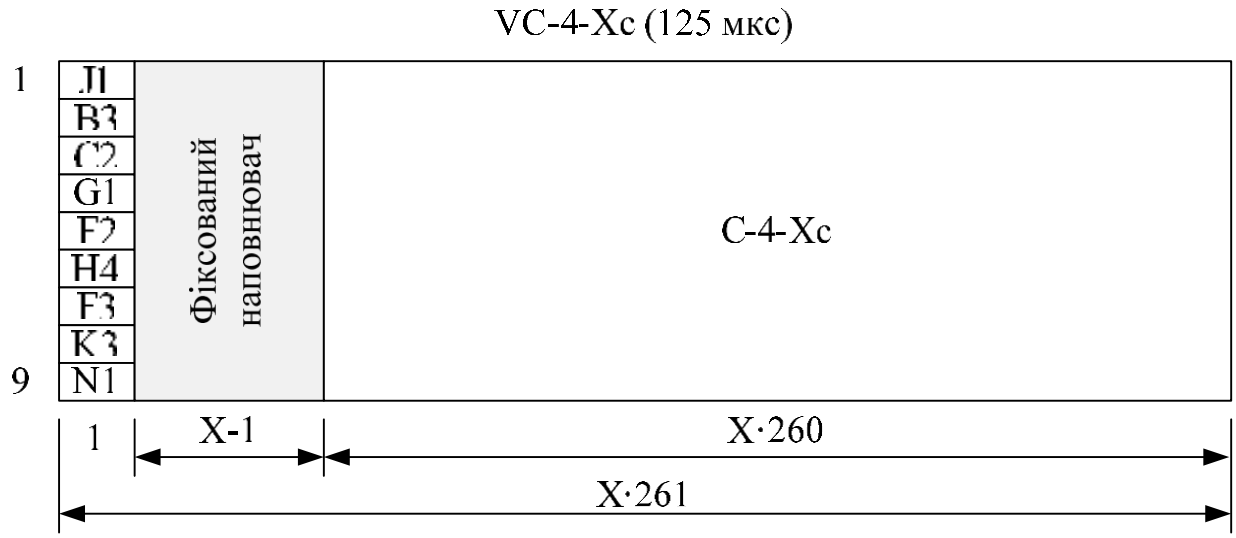


Рисунок 2.3 – Структура мультиконтейнера VC-4-Xc

Таблиця 2.1 – Швидкості мультиконтейнерів при суміжній конкатенації

Рівень STM-N	STM-4	STM-16	STM-64	STM-256
Коефіцієнт X	4	16	64	256
Швидкість VC-4-Xc, Мбіт/с	599,040	2396,160	9584,640	38338,560

Іншим варіантом конкатенації, що найчастіше використовується, є процедура віртуальної конкатенації (Virtual Concatenation, VCAT). Вона дозволяє використовувати всі типи віртуальних контейнерів (VC-1, VC-2, VC-3 та VC-4) з розширеним діапазоном можливих значень коефіцієнта мультиплексування X. Віртуальна конкатенація оперує ємностями окремих VC-*n*, транспортує їх окремо та збирає разом до необхідної суміжної ємності тільки в кінцевій точці маршруту. Таким чином, віртуальна конкатенація вимагає підтримки функціональності мультиконтейнера тільки в рамках обладнання в точці закінчення маршруту. Суміжна конкатенація вимагає підтримки мультиконтейнера кожним мережним елементом маршруту.

Найпростіший варіант процедури віртуальної конкатенації передбачає об'єднання ресурсів контейнерів верхнього рівня VC-3 і VC-4. Сформовані віртуальні мультиконтейнери позначаються відповідно VC-3-Xv і VC-4-Xv (рис. 2.4). Факт об'єднання контейнерів у одну загальну інформаційну структуру та номер послідовності вказується в байті H4 трактового заголовка VC-3/4.

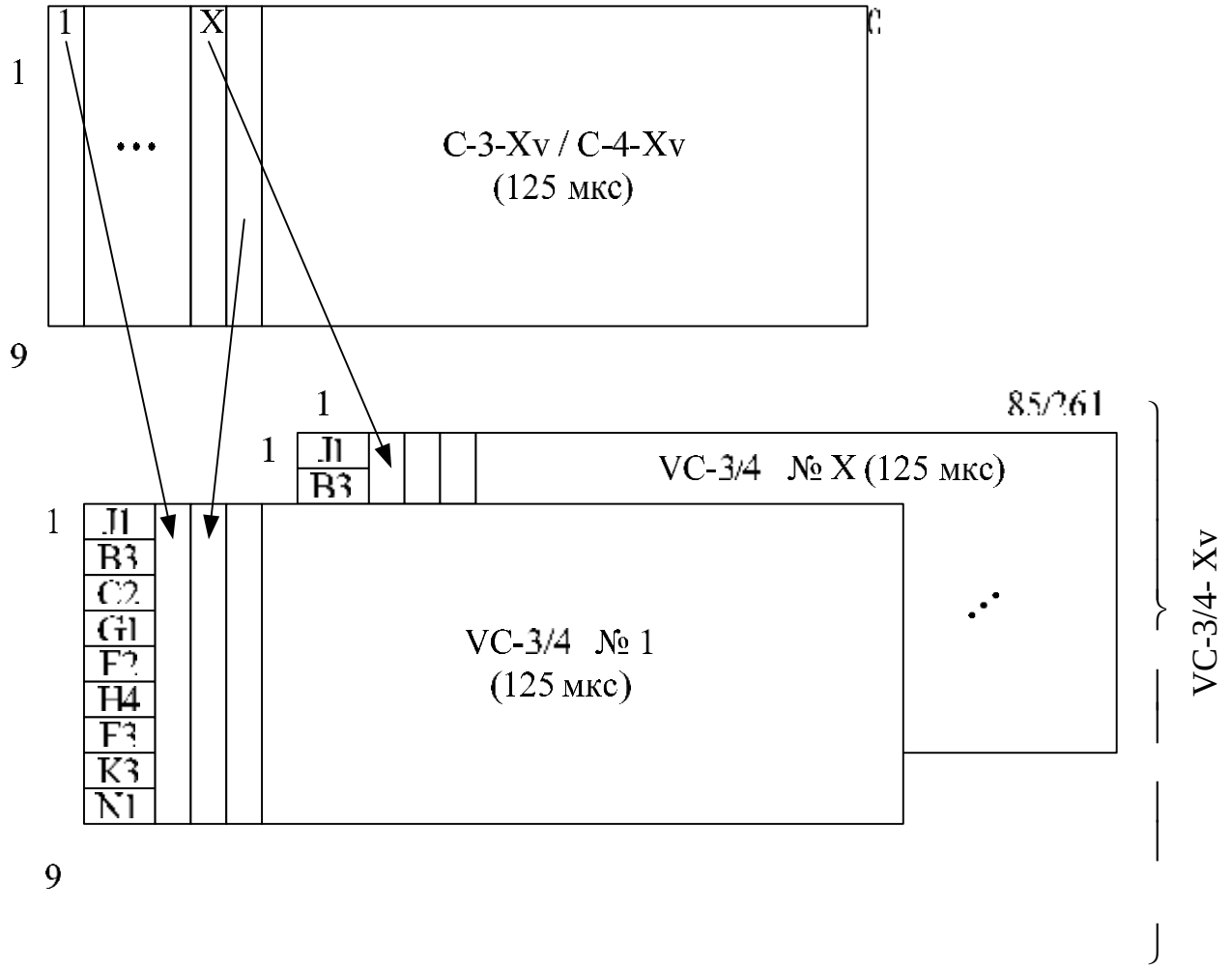


Рисунок 2.4 – Структура віртуального мультиконтейнера верхнього рівня VC-3/4-Xv

Згідно з рис. 2.4 можна розрахувати швидкості передачі одного VC-3 у складі мультиконтейнера VC-3-Xv:

$$B_{VC\text{-}3}=(9\cdot 84)\cdot 8000\cdot 8=48384 \text{ кбіт/с},$$

і одного VC-4 у складі мультиконтейнера VC-4-Xv:

$$B_{VC\text{-}4}=(9\cdot 260)\cdot 8000\cdot 8=149760 \text{ кбіт/с}.$$

Транспортування віртуальних контейнерів, що входять до складу одного мультифрейма, окремими маршрутами приводить до різного часу їх поширення. Це явище повинно бути скомпенсоване в точці закінчення маршрута для формування єдиного поля корисного навантаження мультиконтейнера.

Тепер розглянемо формування віртуальних мультифреймів VC-2-Xv, VC-12-Xv та VC-11-Xv з контейнерів нижнього рівня (рис. 2.5). Факт об'єднання та номер у послідовності контейнерів зазначений у байтах V5 і K4 трактового заголовка POH кожного VC-2/1.

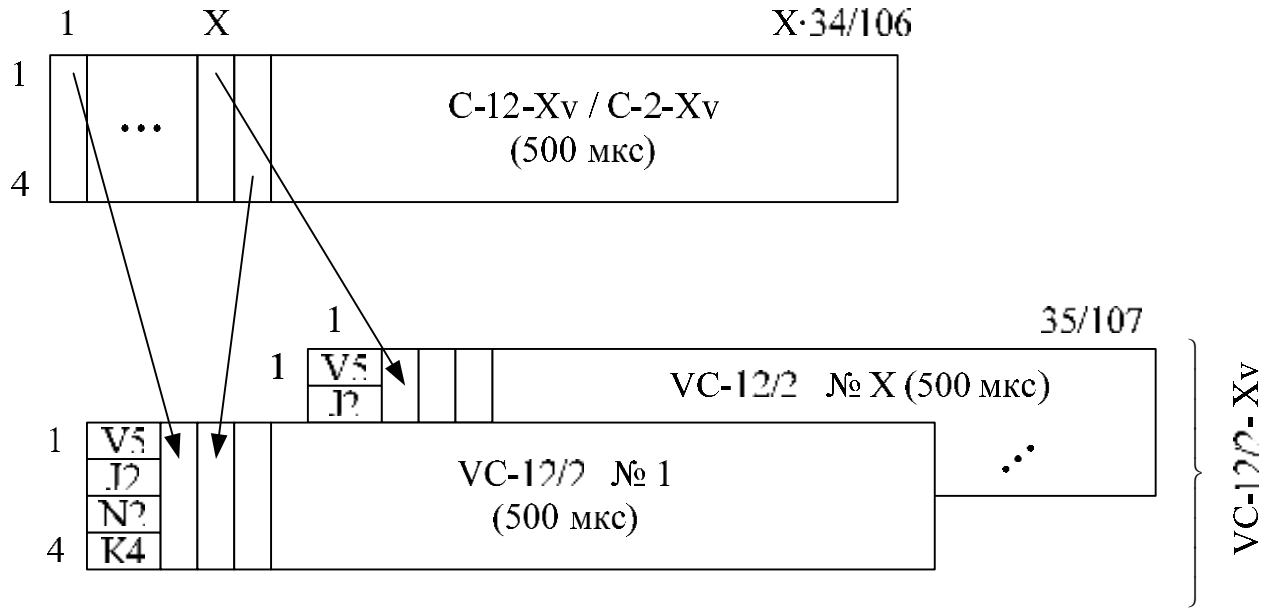


Рисунок 2.5 – Структура віртуального мультиконтейнера нижнього рівня VC-2/1-Xv

Слід зазначити, що у випадку використання VC-12 для передачі пакетного трафіка, використовуються всі 34 байти області корисного навантаження. З урахуванням об'єднання послідовності із чотирьох VC-12 в один мультиконтейнер тривалістю 500 мкс, пропускна здатність одного VC-12 складає

$$B_{VC\text{-}12}=(4\cdot 34)\cdot 8\cdot 8000/4=2176 \text{ кбіт/с}.$$

Швидкості передачі всіх перелічених віртуальних мультиконтейнерів подані в табл. 2.2.

Таблиця 2.2 – Швидкості передачі віртуальних мультиконтейнерів

Тип контейнера	Упакований у модуль STM-N VC-3*	X	Швидкість, Мбіт/с	Крок, Мбіт/с
VC-11-Xv	VC-4 Не визначене	1–28	1,600–44,800	1,600
VC-11-Xv		1–64**	1,600–102,400	1,600
VC-11-Xv	VC-3 VC-4	1–64	1,600–102,400	1,600
VC-12-Xv	Не визначене	1–21	2,176–45,696	2,176
VC-12-Xv	VC-3 VC-4	1–63	2,176–137,088	2,176
VC-12-Xv	Не визначене	1–64	2,176–139,264	2,176
VC-2-Xv	STM-4 STM-16	1–7	6,784–47,448	6,784
VC-2-Xv		1–21	6,784–142,464	6,784
VC-2-Xv	STM-64 STM-256 STM-4 STM-16 STM-64	1–64	6,784–434,176	6,784
VC-3-Xv		1–4	48,384–193,536	48,384
VC-3-Xv		1–16	48,384–774,144	48,384
VC-3-Xv		1–64	48,384–3096,576	48,384
VC-3-Xv		1–256	48,384–12386,304	48,384
VC-4-Xv	STM-256	1–4	149,76–599,04	149,76
VC-4-Xv		1–16	149,76–2396,16	149,76
VC-4-Xv		1–64	149,76–9584,64	149,76
VC-4-Xv		1–256	149,76–38338,56	149,76

Контрольні питання

1. Які функціональні блоки входять до складу мультиплексора NG-SDH?
2. Перелічіть методи упаковки трафіка користувача в STM-N. Який з них реалізовано в мультиплексорі uMSPP-155e?
3. Яким чином організований широкосмуговий канал передачі пакетного трафіка в мультиплексорі NG-SDH?
4. Приведіть порівняльну характеристику методів суміжної та віртуальної конкатенації.
5. Яка структура мультиконтейнера VC-4-Xc та скільки віртуальних контейнерів типу VC-4 він може містити?
6. Опишіть структуру віртуального мультиконтейнера верхнього рівня VC-3/4-Xv та проведіть розрахунки його пропускної здатності.
7. Приведіть структуру віртуального мультиконтейнера нижнього рівня VC-2/1-Xv і проведіть розрахунки його пропускної здатності.

8. Який тип конкатенації віртуальних контейнерів використовується в мультиплексорі uMSPP-155e?

Домашнє завдання

1. Ознайомитися з принципами функціонування мультиплексорів NG-SDH за допомогою ключових положень та додаткової літератури [2-6].
2. У лабораторному зошиті підготувати бланк протоколу: накреслити схеми мультиплексора та проведення вимірювань (рис. 2.1 і 2.6 відповідно), а також табл. 2.5 для запису результатів вимірювань.
3. Розрахувати пропускну здатність каналу Ethernet при використанні процедури віртуальної конкатенації для кількості VC-12, що зазначена у табл. 2.5. У розрахунках враховувати інформаційну ємність VC-12 рівною 34 байти.

Завдання

1. Під'єднати ПК до мультиплексорів uMSPP-155e згідно з рис. 2.6. Тумблером "220 В" увімкнути живлення обох мультиплексорів і дочекатися закінчення процесів самодіагностики, що виконуються під час їх завантаження.
2. Увімкнути живлення робочих станцій PC-1, PC-2 та привласнити їм IP адреси згідно з табл. 2.3.
3. Під'єднати перетворювач інтерфейсу RS-232 - USB до вільного порту USB в PC-1. Кликнути правою кнопкою миші на іконці "Мій комп'ютер", перейти в "Диспетчер пристроїв" і в розділі "Порти (COM і LPT)" знайти пристрій Prolific Usb-to-Serial Comm Port (або аналогічний, згідно вказівкам викладача). Записати номер віртуального послідовного порту, який привласнений приєднаному пристрою.
4. Запустити програму "HyperTerminal" або її аналог. Створити нове з'єднання з параметрами, зазначеними в табл. 2.4.
5. Кілька разів натиснути клавішу "Enter" до появи меню логіна користувача та ввести вихідні дані згідно з рис. 2.7. Перехід між полями даного меню здійснюється шляхом натискання клавіші "Tab".

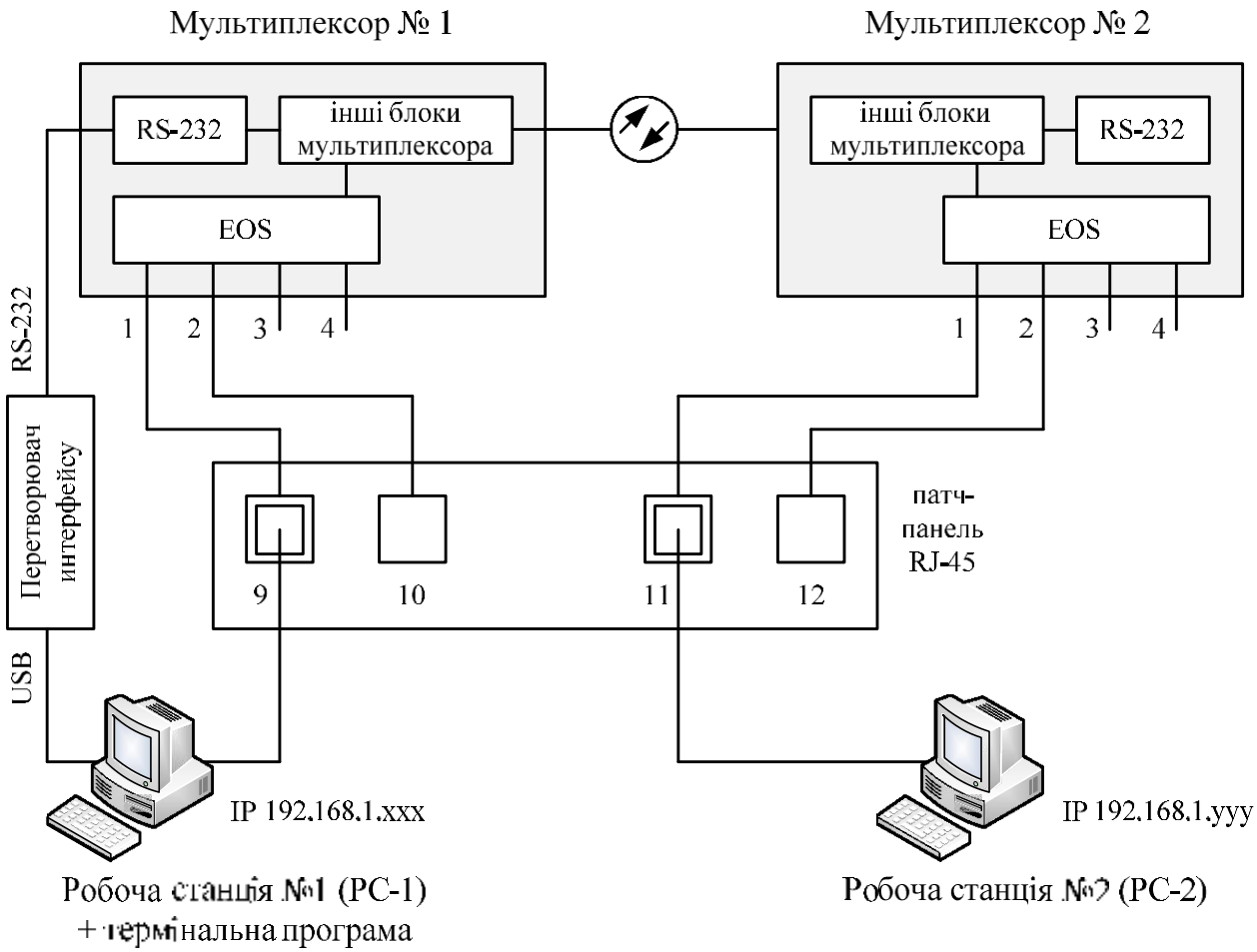


Рисунок 2.6 – Схема проведення вимірювань

Таблиця 2.3 – Конфігурація робочих станцій

№ бригади	PC-1		PC-2	
	IP адреса	режим роботи	IP адреса	режим роботи
1	192.168.1.10	передача	192.168.1.12	приймання
2	192.168.1.14	передача	192.168.1.12	приймання
3	192.168.1.20	приймання	192.168.1.24	передача
4	192.168.1.22	приймання	192.168.1.16	передача

Таблиця 2.4 – Параметри з'єднання

Швидкість, біт/с	Біти даних	Парність	Стопові біти	Управління потоком
115200	8	немає	1	немає

Рисунок 2.7 – Меню ідентифікації користувача мультиплексора uMSPP-155e

6. Огляд стану та попереднє конфігурування плати EOS.
   6.1 Перейти в пункт головного меню "Config" – "Rtrv Summary" і натиснути клавішу "3" (EOS Interface) для відображення конфігурації плати EOS. Порівняти поточні значення параметрів у стовпцях Service (Сервіс), Flow Cnt (Управління потоком), T. Vlan (Віртуальна мережа) та Priority (Пріоритет) з установками за замовчуванням (рис. 2.8). У випадку їх збігу перейти до пункту 7 лабораторного завдання, пропустивши пункт 6.2.
   6.2 Перейти в пункт головного меню "Config" – "Agg/Tri Setting" і натиснути клавішу "3" (EOS Interface) для переходу в меню редагування параметрів плати EOS (рис. 1.10). Натиснути клавішу "b" (Reset to Default) і підтвердити скидання установок плати у вихідний стан.

Slot	Port	Service	Link	Speed	Flow Cnt	T.Vlan	Priority
4	1	IS	Up	100M Full	No	No	0
4	2	IS	Down	10M Half	No	No	0
4	3	IS	Down	10M Half	No	No	0
4	4	IS	Down	10M Half	No	No	0

Press any Key to Exit

Рисунок 2.8 – Установки плати EOS за замовчуванням

7. Користуючись вказівками до лабораторної роботи № 1, програмно відключити трибутарні інтерфейси № 2-4 плат EOS на обох мультиплексорах. Після відключення зазначених інтерфейсів повинні згаснути відповідні світлодіоди на передній панелі мультиплексора.
8. Протестувати пропускну здатність каналу Ethernet між мультиплексорами.

8.1 Перевести відповідну РС в режим приймача тест-сигналу згідно табл. 2.3. Для цього на РС-Приймачі перейти в меню Пуск → Програми → Кафедра ТКС → ТКСМНП і запустити програму "Тест VCAT". У вікні програми ввести цифру "1" для її переводу в режим очікування прийому тест-сигналу з РС-Передавача. Після кожної процедури вимірювання програма виводить результати на екран термінала і автоматично переходить у режим очікування нової тестової послідовності.

8.2 Перейти в меню редагування параметрів плати EOS (рис. 1.10). Натиснути клавішу "1" (Set Bandwidth) і встановити кількість віртуальних контейнерів VC-12 відповідно до одного із стовпців табл. 2.5. Зміна їх кількості виконується за допомогою клавіш управління курсором "↑" і "↓" (рис. 2.9). Запам'ятовування встановленого значення проводиться натисканням клавіші "Enter".

Таблиця 2.5 – Пропускна здатність каналу Ethernet між мультиплексорами NG-SDH

Кількість VCAT VC-12		1	2	5	10	15	20	25	30	35	40	47			
Розрахункова пропускна здатність, Мбіт/с															
Виміряна пропускна здатність, Мбіт/с	з *вимкненим* управлінням потоком передачі даних														
	з *увімкненим* управлінням потоком передачі даних														

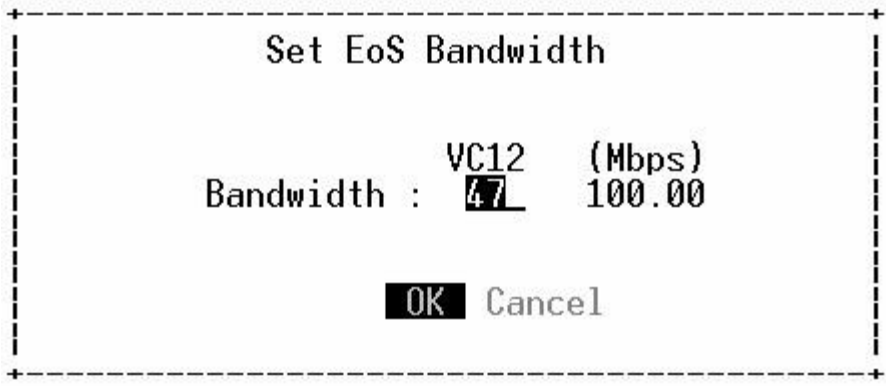


Рисунок 2.9 – Установка кількості елементів віртуального мультиконтейнера VC-12-Xv

8.3 Перевести РС-Передавач у режим передавача тест-сигналу згідно табл. 2.3. На РС- Передавачі перейти в меню Пуск → Програми →

Кафедра ТКС → ТКСМНП і запустити програму "Тест VCAT". У головному меню програми ввести цифру "2" для її переводу в режим передачі тест-сигналу та ввести IP адресу PC-Приймача згідно з табл.2.3. Після завершення процедури тестування каналу на екран виводяться результати тесту мережного з'єднання (рис. 2.10), що складаються із 8 рядків. У процесі процедури вимірювання PC-передавач формує тестову послідовність із 2048 блоків по 8192 байти, що називаються буферами (buffers, англ.). При поточних установках довжина послідовності становить 16777216 байтів. На основі вимірювання проміжку часу, необхідного для передачі всієї тестової послідовності, проводиться розрахунок середньої пропускної здатності каналу. Отримана величина виводиться в сьомому рядку звіту програми (84,52 Мбіт/с на прикладі рис. 2.10). У відповідному стовпці табл. 2.5 робочого зошита записати отриманий результат для поточної кількості конкатенованих віртуальних контейнерів при вимкненому управлінні потоком.

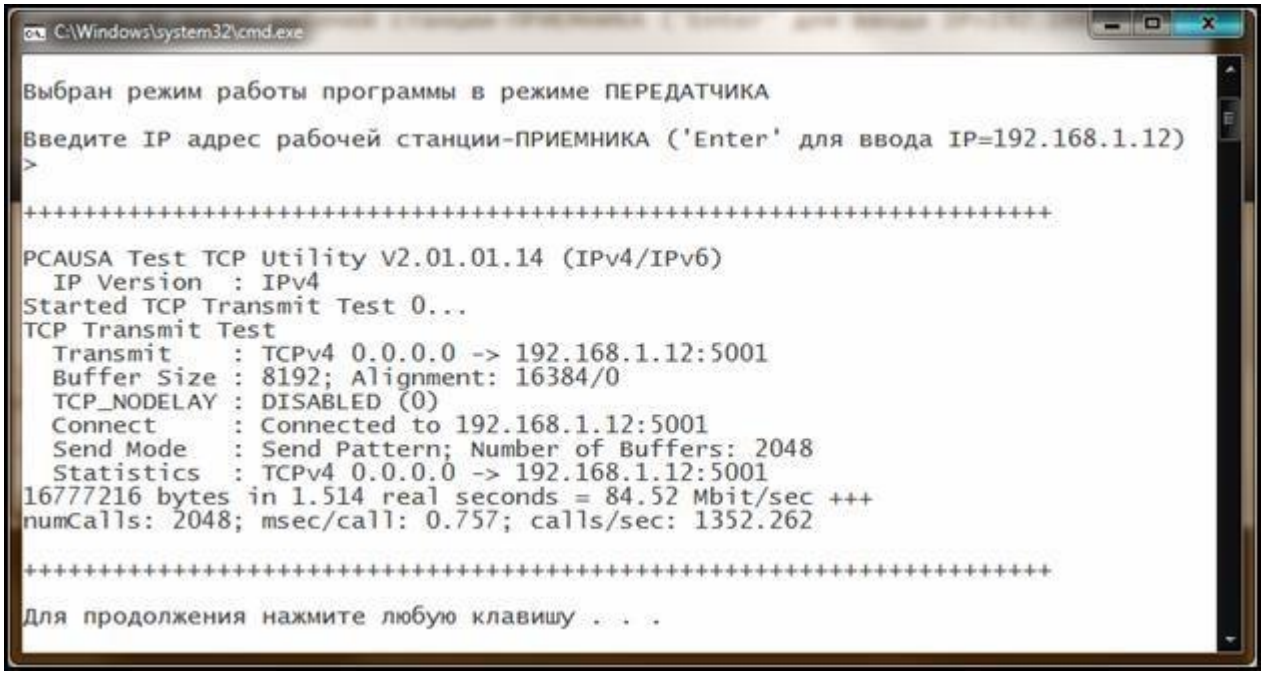


Рисунок 2.10 – Результати тестування мережного з'єднання

8.4 Повторити пункти 8.2 і 8.3 для інших значень кількості конкатенованих віртуальних контейнерів VC-12 згідно з табл. 2.5.

8.5 Перейти в меню редагування параметрів плати EOS . Натиснути клавішу "3" (Flow Control) і встановити параметри плати згідно з рис. 2.11. Повторити п. 8.2-8.4 із записом отриманих результатів для увімкненого режиму управління потоком.

9. Під’єднати патч-корди від мережних карт PC-1 і PC-2 до портів № 1 і № 2 плати EOS одного з мультиплексорів. Програмно увімкнути відповідні інтерфейси на обраному мультиплексорі (див. вказівки до ЛР № 1). За аналогією з пунктом 8 лабораторного завдання провести тестування пропускної здатності вбудованого комутатора Ethernet плати EOS. Записати виміряне значення в робочий зошит та порівняти з отриманою величиною пропускної здатності для 47×VC-12 в табл. 2.5.

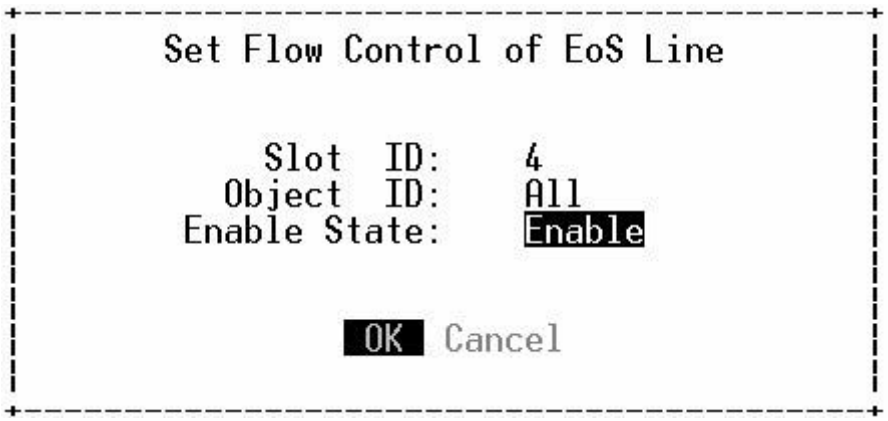


Рисунок 2.11 – Увімкнення режиму управління потоком

Семінарське заняття № 3

Тема: Методи організації віртуальних мереж в системах NG-SDH

Мета: вивчити принципи побудови віртуальних мереж на базі мультисервісної платформи uMSPP-155e

Ключові положення

При необхідності передавання мультиплексором uMSPP-155e пакетного трафіка Ethernet слід використовувати канальну плату EOS. Вона включає наступні елементи (рис. 3.1):

1) чотири трибутарні інтерфейси Ethernet (LAN1 - LAN4) з можливістю програмного відключення кожного з них;
2) керований комутатор другого рівня (Ethernet);
3) блок попереднього оброблення пакетного трафіка з використанням процедури GFP.

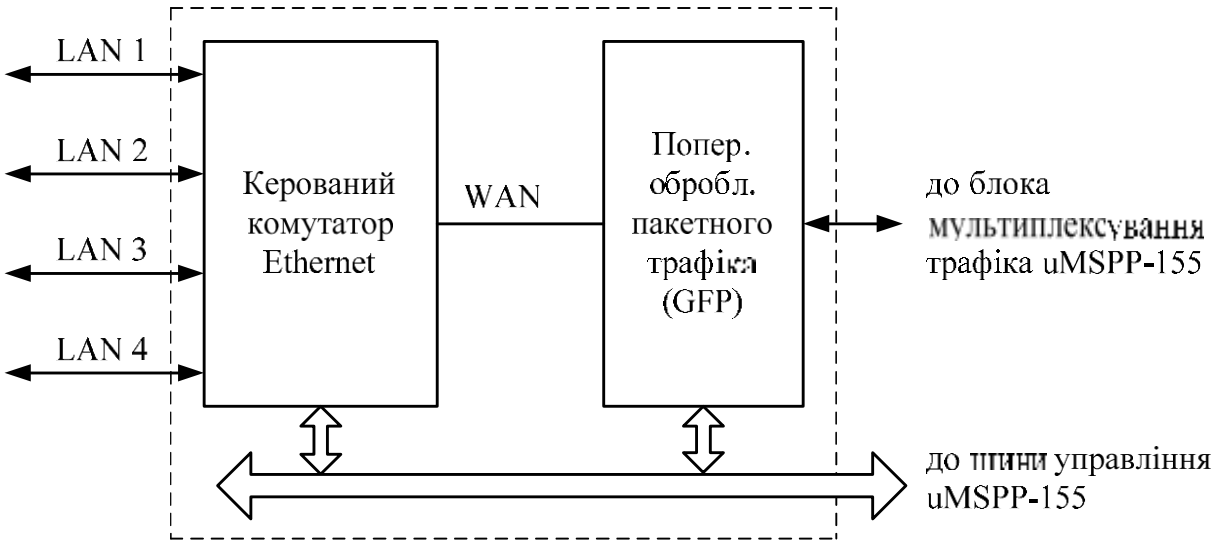


Рисунок 3.1 – Структурна схема плати EOS мультиплексора uMSPP-155e

Важливою властивістю комутатора локальної мережі є здатність контролювати передачу кадрів між сегментами мережі. З різних причин маршрути проходження окремих груп кадрів слід відокремити від інших. Поділ мережі на окремі сегменти дозволяє:

1) підвищити безпеку, оскільки сегменти логічно відділені один від одного, незважаючи на фізичне приєднання до одного комутатора;
2) зменшити навантаження на мережу, оскільки трафік одного сегмента не попадає на станції іншого сегмента. Широкомовні трафіки сегментів також розділені.

З метою зменшення витрат на організацію багатосегментної мережі та її оперативного реконфігурування можлива організація віртуальних мереж на базі загального мережного обладнання.

Віртуальною мережею (Virtual Local Area Network, VLAN) називається група вузлів мережі, трафік якої, у тому числі широкомовний, на канальному рівні повністю ізольований від трафіка інших вузлів мережі (рис. 3.2).

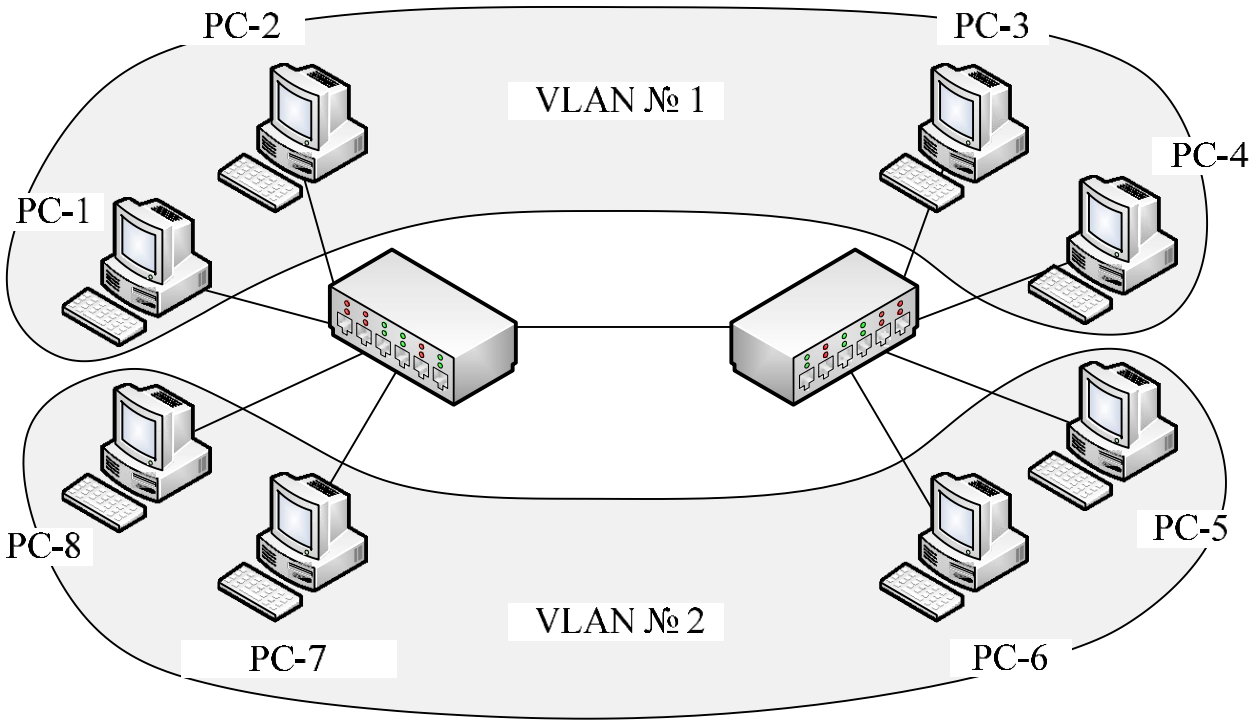


Рисунок 3.2 – Організація двох віртуальних мереж

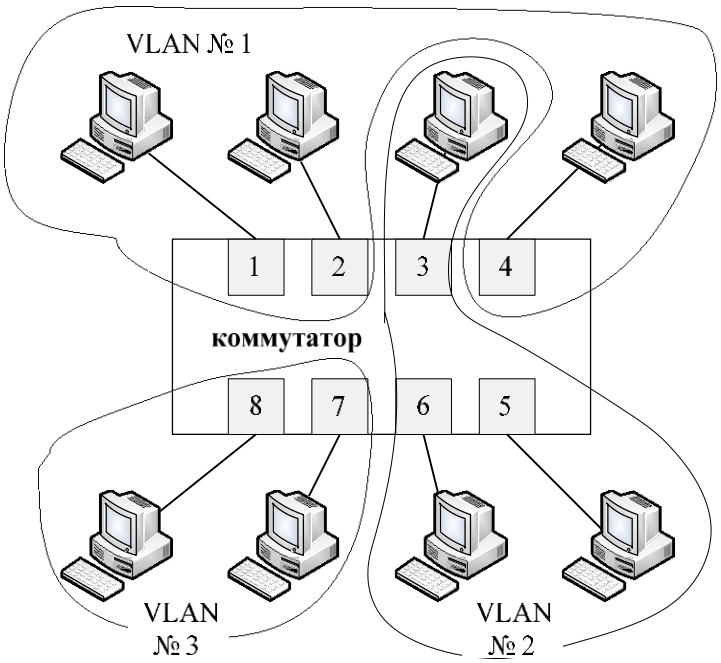
Основне призначення технології VLAN полягає в полегшенні процесу створення ізольованих мереж, які потім з'єднуються між собою за допомогою маршрутизаторів. Така побудова мережі створює потужні бар'єри на шляху небажаного трафіка (в тому числі і широкосмугового) з однієї мережі в іншу.

Базові правила побудови VLAN описуються стандартом IEEE 801.Q. На даний момент існує два основні варіанти організації віртуальних мереж на базі:

1) групування портів комутаторів;

2) тегування кадрів Ethernet.

Перший варіант побудови віртуальних мереж - механізм групування портів комутатора передбачає закріплення портів за тією або іншою віртуальною мережею (рис. 3.3). Кадр, який прийшов до порту, що належить VLAN № 1, не буде переданий порту, який не належить даній мережі. Порт можна прописати кільком віртуальним мережам, хоча при цьому пропадає ефект їх повної ізоляції. Створення мереж даним способом не вимагає від адміністратора великого обсягу роботи – досить кожний порт приписати до однієї з кількох заздалегідь створених віртуальних мереж.



Порт	VLAN № 1	VLAN № 2	VLAN № 3
1	X		
2	X		
3		X	
4	X		
5		X	
6		X	
7			X
8			X

Рисунок 3.3 – Групування портів у комутаторі Ethernet

Альтернативним варіантом побудови VLAN є групування MAC адрес користувачів. У цьому випадку зв'язування портів комутаторів не потрібно, проте потрібне виконання ручної роботи з метою прив'язки MAC адрес користувачів до номерів віртуальних мереж.

Другий варіант побудови віртуальних мереж передбачає доповнення вхідних кадрів Ethernet допоміжним полем з номером VLAN. Стандарт IEEE 802.Q передбачає доповнення кадрів Ethernet додатковим заголовком загальною довжиною 4 байти, який називається тегом (tagg) віртуальної локальної мережі. Кадр, у якого є такий заголовок називається позначеним (tagged frame). Комутатори можуть одночасно працювати як з позначеними, так і непозначеними кадрами. Формати кадрів Ethernet 802.3 і 802.1Q показані на рис. 3.4. Перші два байти тегу містять фіксований ідентифікатор протоколу VLAN зі значенням 0x8100. Оскільки дане число перевищує максимальну довжину поля корисного навантаження (1500 байт), то мережні карти інтерпретують його як поле типу кадру, а не як поле довжини.

Решта (два байти) містять три вкладені поля. Головним з них є 12-бітний ідентифікатор VLAN, що містить номер віртуальної мережі (VID). Номер VLAN може набувати будь-якого значення в діапазоні від 1 до 4094. Номери 0 та 4095 зарезервовані для спеціальних потреб.

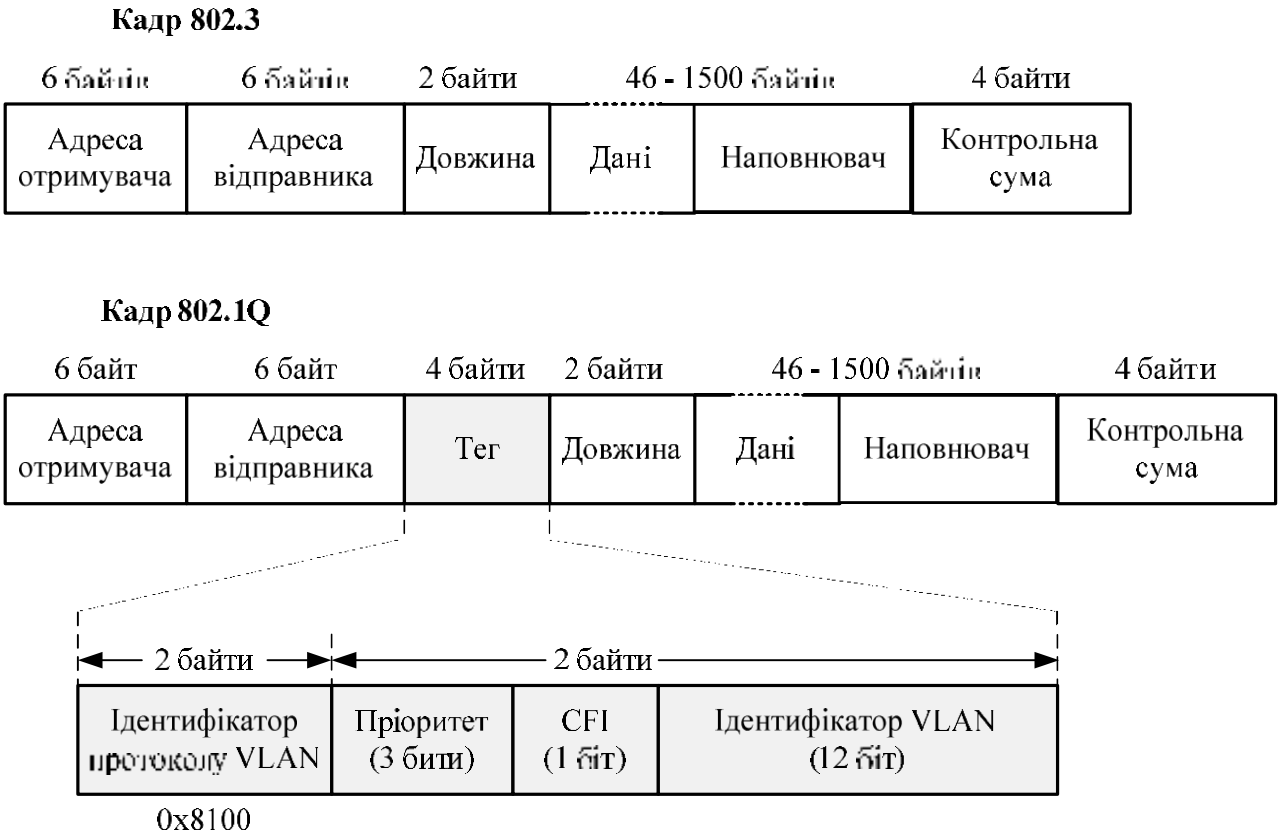


Рисунок 3.4 – Формати кадрів Ethernet 802.3 та 802.1Q

Кодова комбінація пріоритету (PCP), що складається з трьох бітів, указує на черговість оброблення кадру в комутаторі (табл. 3.1).

Таблиця 3.1 – Пріоритети кадрів Ethernet

PCP	Мережний пріоритет	Акронім	Характеристика трафіка
1	0 (найменший)	BK	Фоновий
0	1 2 3 4 5 6	BE	Гарне обслуговування
2	7 (найбільший)	EE	Чудове обслуговування
3		CA	Критичний додаток
4		VI	Відео (затримка <10 мс)
5		VO	Мова (затримка <10 мс)
6		IC	Міжмережне управління
7		NC	Мережне управління

Біт CFI (Canonical Format Indicator) є індикатором канонічного формату MAC адреси і може мати наступні значення: 0 — канонічний, 1 — не канонічний. Біт CFI використовується з метою сумісності мереж Ethernet та Token Ring.

У локальних мережах можливе використання наступних типів кадрів Ethernet:

1) Untagged frame - кадр, у якому не використовується тег 802.1Q;
2) Priority-tagged frame - кадр, що містить тег VLAN, проте поле VID рівне 0. Такий кадр не належить жодній VLAN, у ньому має значення тільки поле пріоритету;
3) VLAN-tagged frame - кадр з тегом 802.1Q та VID якого більше 0.

На рис. 3.5 показана організація двох віртуальних мереж за допомогою двох комутаторів. Робочі станції (PC) A, B, C, D належать VLAN з VID=10, а E, F, G, H – VLAN з VID=15. При надходженні від PC-A на комутатор 1 кадру з MAC адресою PC-D відбувається його передавання до комутатора 2 з метою його наступного транспортування до PC-D. В результаті станції різних віртуальних мереж ізольовані одна від одної.

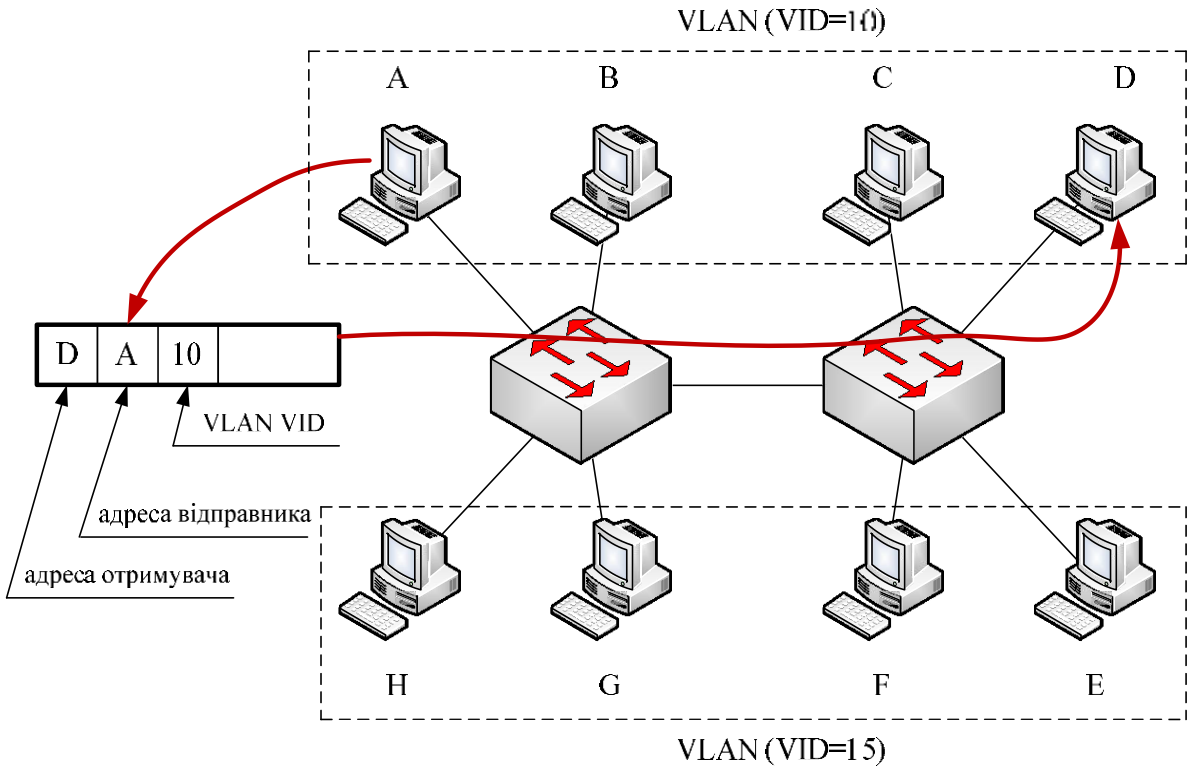


Рисунок 3.5 –Передавання кадру у віртуальній мережі з VID=10

Плата EOS мультиплексора uMSPP-155e дозволяє створювати різні конфігурації віртуальних з'єднань між портами LAN1 - LAN4 і WAN. Він підтримує обидва варіанти організації віртуальних з'єднань: групування портів (Port-based VLAN) та на основі тегування кадрів Ethernet (Tag VLAN). Перший варіант дозволяє забезпечувати віртуальні з'єднання тільки в межах одного мультиплексора, що не дозволяє організовувати незалежні наскрізні логічні канали в оптоволоконній лінії. Разом з тим організація наскрізних незалежних

логічних каналів є досить затребуваним завданням. Організація таких каналів може бути забезпечена за допомогою тегування для помічених та непомічених кадрів Ethernet, що поступають на вхідні порти плати. Помічені кадри можуть надходити на входи портів у разі використання Ethernet комутаторів, що підтримують тегування. Якщо ж використовуються тільки концентратори (Hub), то пакети в таких мережах не помічені. Зокрема, мережні пристрої персональних комп'ютерів не підтримують тегування.

Лабораторне завдання даної роботи передбачає створення двох віртуальних каналів (мереж) з тегуванням кадрів Ethernet між портами 1 і 2 плат EOS двох мультиплексорів NG-SDH та використанням групування портів у межах кожного з мультиплексорів (рис. 3.6).

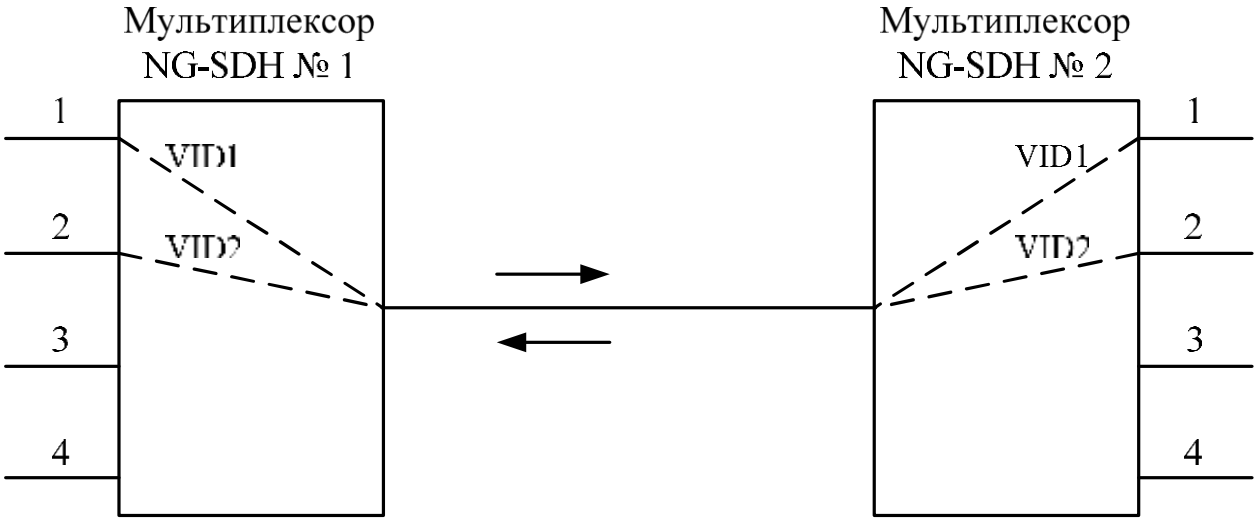


Рисунок 3.6 - Схема організації двох незалежних віртуальних каналів

Контрольні питання

1. У чому полягає призначення віртуальних мереж? У яких випадках доцільно їх використовувати?
2. Перелічіть способи організації віртуальних мереж.
3. Поясніть принцип функціонування віртуальної мережі із групуванням портів комутатора.
4. Поясніть принцип роботи віртуальної мережі з тегуванням кадрів Ethernet.
5. Поясніть призначення складових частин тегу Ethernet стандарту 802.Q.
6. Які варіанти побудови віртуальних мереж підтримуються в обладнанні uMSPP-155e?

Домашнє завдання

1. Вивчити принципи побудови віртуальних мереж згідно літератури [7, стор. 467-475] та [8, стор. 382-391].

2. В робочий зошит зарисувати схеми:
   – плати EOS (рис. 3.1);
   – організації двох незалежних віртуальних каналів (рис. 3.6);
   – проведення вимірювань згідно з лабораторним завданням (рис. 2.6).

Завдання

1. Під'єднати ПК до мультиплексорів uMSPP-155e згідно з Тумблером "220 В" увімкнути живлення обох мультиплексорів та дочекатися закінчення процесів самодіагностики, що виконуються під час їх завантаження.
2. Увімкнути живлення робочих станцій PC-1 та PC-2, привласнити їм IP адреси 192.168.1.10 і 192.168.1.12 відповідно.
3. Керуючись пунктами 1-5 лабораторного завдання до ЛР № 1 або № 2 організувати з'єднання термінальної програми з мультиплексором № 1 через послідовний інтерфейс RS-232.
4. Організація віртуальної мережі з групуванням портів плати EOS.
   4.1 Переключитись на управління локальним мультиплексором (вибрати пункт головного меню "Local" – "Sel Local").
   4.2 Перейти в пункт головного меню "Config" – "Rtrv Summary" і натиснути клавішу "3" (EOS Interface) для відображення конфігурації плати EOS. Переконатися в наявності фізичного під'єднання PC-1 до порту № 1 плати EOS (значення параметра для порту № 1 в стовпці "Link" дорівнює "Up" згідно з рис. 2.8).
   4.3 Перейти в пункт головного меню "Config" – "Agg/Tri Setting" і натиснути клавішу "3" (EOS Interface) для переходу в меню редагування параметрів плати EOS. Натиснути клавішу "b" (Reset to Default) і підтвердити скидання установок плати у вихідний стан.
   4.4 Перебуваючи в меню редагування параметрів плати EOS, натиснути клавішу "9" (Set PortVLAN) для переходу до меню редагування параметрів групування портів. У вікні, що з'явилося, клавішами "↑" і "↓" установити Slot ID (Номер слота) № 4 та підтвердити встановлене значення натисканням клавіші "Enter".
   4.5 Записати в лабораторний зошит вміст вікна "Set Port-Based VLAN".
   4.6 У вікні "Set Port-Based VLAN" встановити параметри заборони комутації трафіка між портами 1-4. За замовчуванням комутація трафіка дозволена між усіма наявними портами (трибутарними портами 1-4 та вихідним портом WAN). Дозвіл на комутацію в матриці на рис. 3.7 позначається символом "V". Для перемикання між дозволом/забороною комутації

необхідно клавішами "←" та "→" встановити курсор на необхідний номер порту, після чого натиснути клавішу "Enter". Для переходу до редагування параметрів наступного порту навести курсор на пункт "next" і натиснути клавішу "Enter". Після редагування параметрів комутації для порту № 4 слід навести курсор на пункт "save" і натиснути клавішу "Enter".

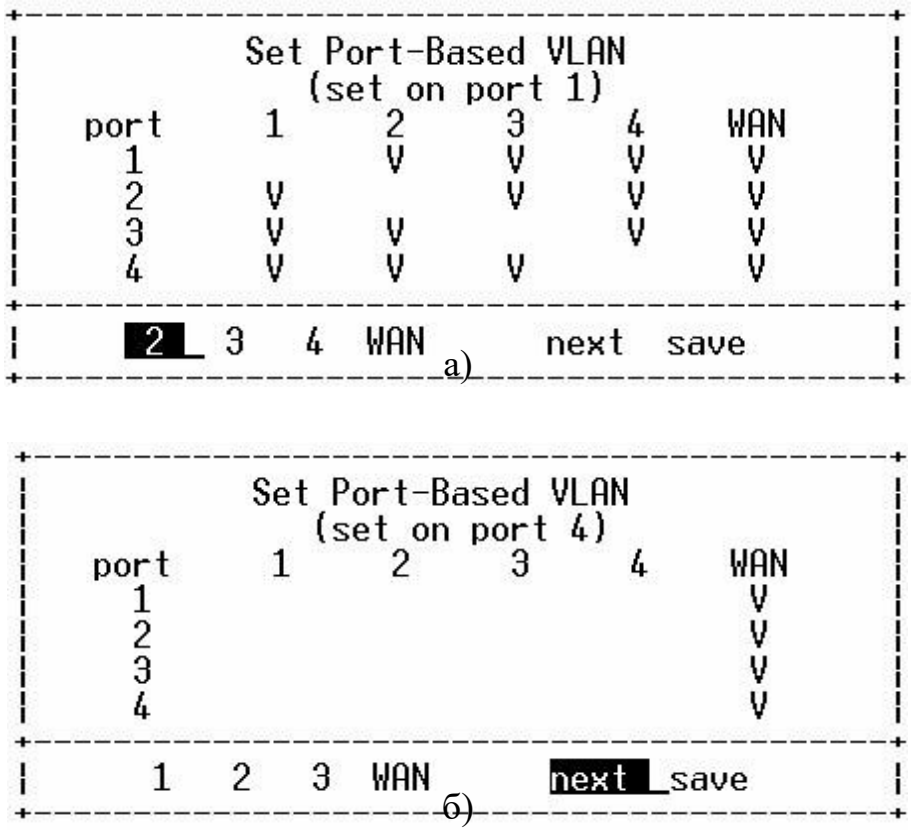


Рисунок 3.7 – Установлення параметрів віртуальної мережі із групуванням портів:

а) вихідні;

б) після редагування

4.7 Переключитися на управління віддаленим мультиплексором (вибрати пункт головного меню "Local" – "Sel Remote") і повторити пункти 4.2 – 4.6 поточного лабораторного завдання. Після виконання всіх процедур конфігурування слід записати в лабораторний зошит вміст вікна "Set Port-Based VLAN".

4.8 На PC-1 в меню "Пуск" операційної системи Windows вибрати пункт "Виконати", ввести команду "cmd" і натиснути клавішу "Enter". У вікні командного рядка виконати команду "ping 192.168.1.12" і переконатися у проходженні пакетів між PC-1 та PC-2.

5. Організація віртуальних мереж з тегуванням кадрів Ethernet.

5.1 Переключитися на управління локальним мультиплексором (вибрати пункт головного меню "Local" – "Sel Local").

5.2 Перебуваючи в меню редагування параметрів плати EOS (рис.1.10), натиснути клавішу "a" (Tag VLAN) для переходу до меню редагування параметрів VLAN с тегуванням кадрів Ethernet (рис. 3.8).

Рисунок 3.8 – Меню редагування параметрів віртуальної мережі з тегуванням кадрів Ethernet

5.3 Натиснути клавішу "1" для вибору пункту " New VLAN Group". У вікні, що з'явилося, вказати ідентифікатор першої мережі VLAN ID (VID) 1, умовну назву (Nickname) та її опис (Description) згідно з рис. 3.9. Встановити значення "Disable" параметра обмеження швидкості (Rate Limit). Аналогічним чином створити другу мережу з VID 2.

Рисунок 3.9 – Параметри віртуальної мережі з VID 1

5.4 Включити порти № 1 і № 2 плати EOS до відповідних VLAN. У меню "Tag VLAN" вибрати пункт "(4) Add Port to VLAN". Для VLAN з VID 1 установити параметри VLAN ID, Slot ID (місце установки плати EOS), Object ID (номер порту) і Egress Tag (маркування вихідних пакетів)

згідно з рис. 3.10. Повторити зазначені дії для другої мережі з VID 2 із заміною значень параметрів VLAN ID та Object ID на 2.

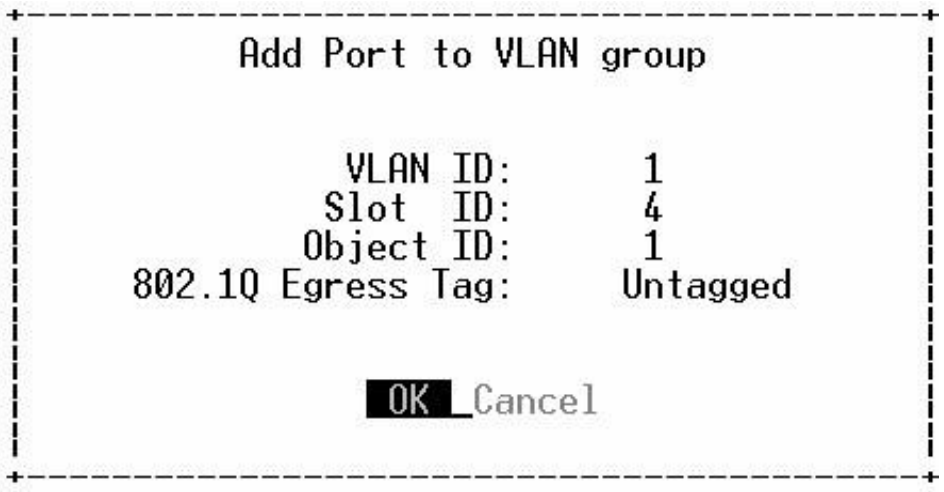


Рисунок 3.10 – Включення порту № 1 до VLAN з VID 1

5.5 Встановити Default VID для кожного з портів VLAN, що необхідно для маркування вхідних кадрів без тегів та їх маршрутизації комутатором у межах відповідної VLAN. Для цього в меню "Tag VLAN" вибрати "(9) Default VID" і вказати параметри Slot ID, Port ID, VLAN ID. При цьому VLAN ID повинен збігатися з номером VLAN, встановленим раніше для цього порту (рис. 3.11). Повторити аналогічні дії для порту № 2 із заміною Port ID і VLAN ID на 2.

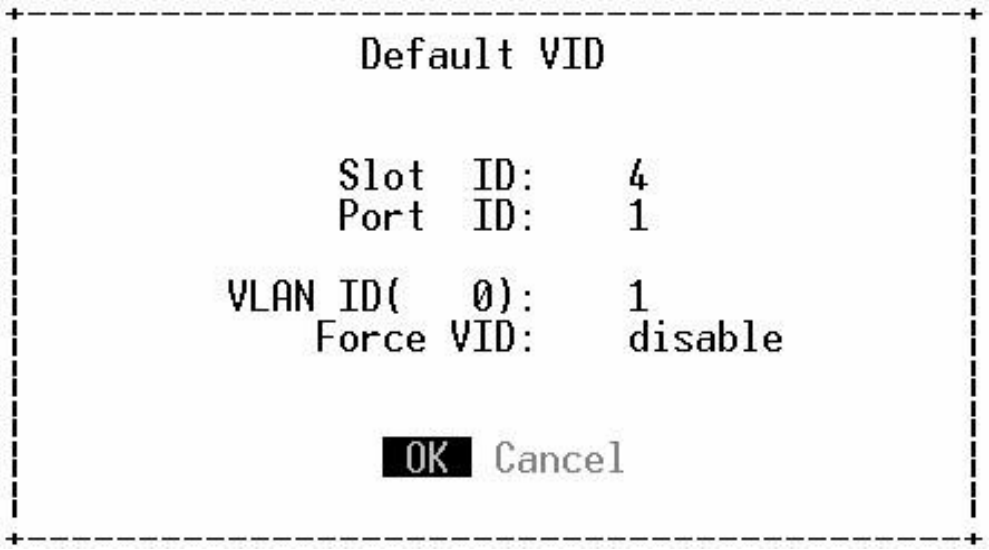


Рисунок 3.11 – Призначення тегів за замовчуванням для вхідних немаркованих пакетів порту №1

5.6Перевірити наявність створених мереж з VID 1 та VID 2. Для цього в меню "Tag VLAN" вибрати пункт "(6) Rtrv VLAN Info" та у вікні "To Retrieve VLAN group" встановити значення "YES" для параметра "Get

All". У результаті на екран буде виведений список із двох створених мереж з тегуванням кадрів.

5.7 Перевірити включення портів № 1 і № 2 до мереж з VID 1 і VID 2 відповідно. Для цього в меню "Tag VLAN" вибрати пункт "(7) Rtrv VLAN Info" і у вікні "Retrieve VLAN port list" встановити значення "YES" для параметра "Get All". Після натискання на кнопку "OK" буде виведений список (рис. 3.12) ідентифікаторів (VID) усіх існуючих мереж VLAN із вказанням закріплених за ними номерів портів (Object ID). Записати в робочий зошит перелік створених мереж та відповідних їм номерів портів.

5.8 У вікні командного рядка на PC-1 виконати команду "ping 192.168.1.12" і переконатися у відсутності проходження пакетів до PC-2, оскільки VLAN з тегуванням кадрів настроєна тільки на мультиплексорі № 1.

5.9 Переключитися на управління віддаленим мультиплексором (вибрати пункт головного меню "Local" – "Sel Remote").

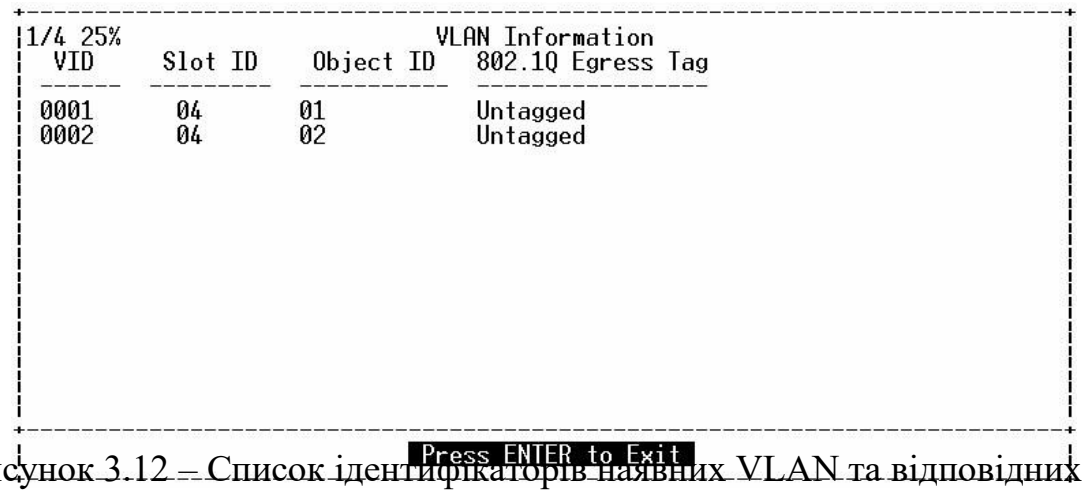


Рисунок 3.12 – Список ідентифікаторів наявних VLAN та відповідних їм номерів портів

5.10 Перейти до меню редагування параметрів плати EOS і повторити пункти 5.2 - 5.7 лабораторного завдання для мультиплексора № 2.

5.11 Перевірити функціонування створених мереж. У вікні командного рядка виконати команду "ping 192.168.1.12" і переконатися в працездатності каналу зв'язку між портами № 1 мультиплексорів. Під'єднати PC-1 і PC-2 до портів № 2 мультиплексорів і пересвідчитись у проходженні пакетів каналом мережі з VID 2.

Семінарське заняття № 4
ПОСТАНОВКА ПРОБЛЕМИ КІБЕРБЕЗПЕКИ МЕРЕЖ НАСТУПНИХ ПОКОЛІНЬ

4.1 Принципи та визначення кібербезпеки

Принципи забезпечення кібербезпеки знаходяться в руслі загальних принципів побудови *NGN*, серед яких розглядаються загальні принципи інформаційної й кібербезпеки, взаємозв'язок з іншими функціональними можливостями, безпека за рівнями, елементами мережі та безпека «з кінця в кінець» [22, 23]. Кібербезпека *NGN* є специфічною проблемою, яка ще повинна бути вирішена поряд і у взаємозв'язку з проблемами впровадження голосових послуг у інфраструктурі *NGN*, якості обслуговування – *QoS*, при наданні голосових послуг у реальному часі (гарантованою смугою пропускання, гарантована затримка голосових пакетів, гарантована невтрата пакетів тощо). Питання забезпечення кібербезпеки в *NGN* основним аспектом і стратегічною задачею. Забезпеченість безпекою взаємно залежить і розповсюджується на архітектуру, *QoS,* менеджмент мережі, білінг і платежі.

Потрібна для *NGN* безпека повинна включати:

- розробку вичерпної архітектури безпеки для мереж *NGN*;
- підготовку керівництв з експлуатаційного захисту *NGN*;
- розвиток стратегії й удосконалення експлуатаційного захисту *NGN*;
- відповідні протоколи й інтерфейси *API* для безпеки *NGN*.

NGN повинна бути забезпечена механізмами безпеки для:

- захисту обміну вразливою інформацією в її інфраструктурі;
- захисту проти шахрайського використання послуг, які надаються провайдерами;
- захисту власної інфраструктури від зовнішніх атак.

На сьогодні подібні послуги пропонуються користувачам як фіксованого доступу так і мобільних мереж. Але ці послуги все ще розглядаються розрізнено, з різними конфігураціями послуг і без можливих взаємозв'язків між різними послугами [16, 17] (службами).

Одним із найсуттєвіших фактів є те, що мережі більше не є монолітними системами з відомими інтерфейсами. Робота по забезпеченню кібербезпеки повинна здійснюватись так, щоб безпечна мережа могла бути побудована з даного вибору певних визначених *NGN* компонентів. Безпека входить до складу послуг менеджменту мережі, поряд із задоволенням вимог до *NGN*:

– надійності (*faultless*), сталості (*configuration*);
– підзвітності, спостережності (*accounting/charging*);
– експлуатаційних властивостей (*performance*);
– безпеки (*security*);
– адміністрування клієнта (*customer administration*);
– навантаження (трафік – *traffic*);
– менеджмент маршрутизації (*routing management*).

Як мережа загального користування, *NGN* повинна відповідати вимогам надійності, цілісності, захищеності та суверенності. Дані щодо найменувань і нумерації мережі є важливими даними, які можуть безпосередньо впливати на функціонування мережі. Вони є також уразливими комерційними даними, які відображають структуру та політику функціонування мережі. Безпека є складовою частиною вимог до системи вибору (розподілу) імен і нумерації.

Система вибору (розподілу) імен і нумерації безпосередньо зв'язана з функціонуванням мереж загального користування. Тому важливо, щоб системи вибору (розподілу) імен і нумерації не приводили до протиріч. Повні бази даних для переведення найменування в номер повинні мати дійсні та надійні дані, так щоб результат переводу не порушував цілісність бази в умовах розподіленого використання.

Відповідно, система вибору (розподілу) імен і нумерації має бути використана лише цією мережею та повинна мати перевірені (надійні) засоби безпеки. Безпека, головним чином, підтримується засобами автентифікації доступу користувачів, безпеки (захисту) даних, безпеки (захисту) приватності, синхронізації даних мережі й відновлення після збоїв (пошкоджень і помилок).

Термінологія в галузі кібербезпеки. Архітектура безпеки – це вимоги, які відносяться в контексті безпеки викликів [16, 17] *NGN* до мережі та провайдерів послуг, підприємств і споживачів. Архітектура безпеки направлена на безпеку менеджменту, сигналізації (управління) та використання інфраструктури мережі, послуг і застосувань, щоб виявляти, передбачати й усувати вразливі моменти в захисті. Архітектура безпеки в *NGN* повинна забезпечити всеохоплюючу, зверху-вниз, з кінця в кінець перспективу безпеки мережі та може бути застосована до елементів мережі, послуг і застосувань для виявлення, прогнозування та коригування вразливостей безпеки.

У галузі технічного захисту інформації чинні терміни та визначення, що відповідають установленим державним стандартом України ДСТУ 3396.2-97 [32], нормативним документом ТЗІ 1.1-003-99 [33]. Термінологія в галузі кібербезпеки телекомунікацій може бути встановлена згідно з Рекомендацією МСЕ-Т серії *Y*. Дамо визначення основних термінів кібербезпеки та кіберсередовища, що не визначені у вітчизняних нормативних документах.

Кіберсередовище (*cyber environment*) – включає у себе користувачів, мережі, пристрої, все програмне забезпечення, процеси, зберігану чи транзитну інформацію, застосування, послуги та системи, які можуть бути прямо чи посередньо приєднані до мереж для забезпечення інформаційних і телекомунікаційних послуг користувачам.

Кібербезпека (*cybersecurity*) – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до менеджмент ризиків, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути застосовані для захисту кіберсередовища, ресурсів організацій будь-якого рівня та користувача. Кібербезпека полягає у спробі досягнення та збереження властивостей безпеки ресурсів організації або користувача, спрямованих проти відповідних загроз безпеки в кіберсередовищі. Загальні задачі забезпечення безпеки включають:

– доступність;

– цілісність, яка може включати автентичність і невідмовність;

– конфіденційність.

Ресурси (*assets*) підприємства, організації або користувача включають у себе приєднані комп'ютерні пристрої, персонал, інфраструктуру, застосування, послуги, системи зв'язку та всю сукупність переданої та/або інформації, що зберігається в кіберсередовищі.

Інші визначення термінів сфери кібербезпеки телекомунікацій наведено в Додатку 1.

Природа середовища кібербезпеки телекомунікацій. Підприємства, установи та організації (далі – організації) всіх форм власності повинні розробити всебічний план кібербезпеки. План кібербезпеки повинен бути індивідуальним для кожної організації. Кібербезпеку неможливо забезпечити за допомогою апаратних модулів, об'єднаних разом. Рекомендується розглядати кібербезпеку як процес або спосіб безперервного вдосконалення засобів захисту мереж, застосувань і послуг, що надаються мережею.

Кібербезпека повинна бути всебічною на всіх рівнях мереж. Рівневий підхід до проблеми кібербезпеки, разом із сильним менеджментом політики кібербезпеки та забезпечення її виконання забезпечує модульні, гнучкі та розширювані рішення з кібербезпеки.

Кібербезпеку важко перевірити, передбачити та реалізувати. Вимоги до безпеки та рекомендована стратегія кібербезпеки в кожній організації унікальна та різна. Кожне підприємство – оператор зв'язку, оператор мережі, провайдер послуг – володіє своїм унікальним набором вимог, може створити своє мережне середовище, що відповідає цим вимогам. Використовуються цифрові чи фізичні канали для надання доступу, віддалений доступ надається тим, хто працює дома, послуги надаються провайдером послуг, який відповідає за встановлення безпечного середовища. Використовується внутрішня електронна пошта, а також місцеві безпроводові локальні мережі. Оператор мережі або провайдер послуг можуть забезпечувати доступ через мережі *IP VPN* або надавати можливість здійснення високошвидкісних з'єднань. Може здійснюватись доступ для взаємодії внутрішніх систем електронної пошти із зовнішнім світом.

Для кібербезпеки необхідне управління ризиками. Процес менеджмент ризиків включає у себе задачу ідентифікації сукупного набору компонентів, що підлягають захисту. Для аналізу ризиків корисно розглядати спроби порушення захисту таких типів:

– порушення захисту в вигляді переривання обслуговування. Цей тип зламу відключає доступ користувача до потрібних йому послуг тимчасово чи постійно;

– несанкціонований доступ до інформаційних ресурсів. Ці типи зламів включають у себе крадіжку або неправильне використання інфраструктури. Вони небезпечні, якщо кіберзлочинність досягає великих масштабів;

– захоплення компонентів. Ці типи зламів включають у себе захоплення контролю над деякими пристроями, а потім використання їх для запуску нових зламів, спрямованих проти інших компонентів кіберсередовища.

Будь-який елемент кіберсередовища може розглядатися як ризик безпеки, який у загальному випадку сприймається як комбінована оцінка загрози.

До аналізу загрози входить задача опису типу можливих зламів, типових нападників та їх методи здійснення спроб порушення захисту та наслідки в випадку успішних зламів.

Спроби порушення захисту можуть виходити із кіберсередовища, такі як злами за допомогою «червів» та інших шкодоносних програм, можуть бути здійснені прямими спробами порушення захисту важливої інфраструктури, таких як кабелі телекомунікацій, або злами, що викликані діями довіреної добре обізнаної людини. Можлива комбінація цих спроб порушення захисту. Зазвичай, ризики характеризуються як високі, середні та низькі. Рівень ризику змінюється серед різних компонентів середовища.

Забезпечення кібербезпеки включає у себе менеджмент ризиків. Для менеджменту ризиків можуть бути використані різні технології. Наприклад, до технології входять такі складові. Розробка стратегії захисту, яка визначає заходи протидії, що можуть бути запроваджені при можливих спробах порушення захисту. Виявлення, до якого входить ідентифікація зламу в момент його виникнення та розвитку. Формування реагування на спробу порушення захисту, в якому визначаються сукупність заходів протидії цій спробі для того, щоб її зупинити або знизити її вплив. Формулювання стратегії відновлення, яка дає можливість мережі відновити роботу з відомого стану.

4.2 *NGN* як об’єкт кібербезпеки

Механізми безпеки мають розподілятись за елементами об’єкта захисту. Розглянемо *NGN*, як об’єкт інформаційної безпеки. Вимоги до системи кібербезпеки повинні враховувати особливості телекомунікаційних мереж наступних поколінь. Архітектура кібербезпеки повинна бути узгоджена з архітектурою головних архітектурних рішень.

Поділ функцій між *обслуговуванням* і *транспортом* представлено двома різними блоками або стратами (рівнями) функціональних можливостей у *NGN*. Транспортні функції належать до транспортної страти, а функції обслуговування (надання послуг), які відносяться до застосувань, розміщуються у страті обслуговування (надання послуг).

Сукупність транспортних функцій займається виключно передаванням цифрової інформації будь-якого виду, між будь-якими географічно окремими пунктами. Транспортні функції забезпечують можливість з’єднання. Функції транспортної страти використовують для з’єднання об’єкти та функції мережного, канального та фізичного рівнів, визначені в основній семирівневій моделі *OSI*. Щоб взаємодіяти, мережа більш високого рівня запитує послуги від мережі більш низького рівня. Зокрема, транспортна страта дає можливість:

– з’єднання користувач-користувач;

– з’єднання платформи користувача з послугами;

– з’єднання платформи послуг із платформою послуг.

У транспортній страті можуть бути розгорнуті будь-які мережні технології, зокрема, орієнтовані на з'єднання комутація каналів, комутація пакетів, не орієнтована на з'єднання комутація пакетів. Для надання послуг *NGN* і підтримки успадкованих послуг віддають перевагу застосуванню *IP* (*Internet Protocol*). Але існуюча четверта версія цього протоколу розроблялась без урахування вимог до інформаційної безпеки. Тому ймовірно, що буде застосована більш захищена шоста версія цього протоколу.

Сервісні платформи забезпечують використання послуг, таких як телефонне обслуговування, *WEB*-послуги тощо. Послуги забезпечуються сукупністю модулів прикладних функцій, які можуть бути викликані. У страті послуг можуть бути: голосові послуги, зокрема телефонні послуги, аудіо, факс тощо; послуги передачі даних, зокрема *WWW, E-mail* тощо; відео послуги, зокрема без обмежень, кіно, телебачення тощо; комбінація послуг, наприклад, мультимедійні послуги типу відеотелефон та ігри. Послуги можуть надаватись у реальному часі та не в реальному часі, як однонаправлені, широкомовні та радіомовні.

В кожній страті незалежно виділяються площини *користувача* (або *даних*), *сигналізації* та *контролю* та *менеджменту* Тобто, передбачається, що в кожній страті застосовуються функції для передачі даних, функції управління (і контролю) діями об'єктів, які залучені до передавання цих даних, і функції менеджмента об'єктами в межах страти (рис. 5.1).

Площина *користувача* (синонім – площина даних) – це сукупність функцій, які використовуються для передачі даних у страті або рівні.

Площина *сигналізації та контролю* (управління) – це сукупність функцій, які керують діями об'єктів у страті або рівні, плюс функції, необхідні для підтримки цього управління.

Площина *менеджменту* – це сукупність функцій, які використовуються для менеджменту об'єктами, плюс функції, необхідні для підтримки цього менеджменту.

Страта послуг – це та частина *NGN*, яка забезпечує функції користувача, що передають зв'язані з послугами дані та функції, які виконують управління (сигналізацію та контроль) і менеджмент ресурсів послуг і ресурсів мережі, щоб забезпечити послуги користувачів і застосування. Послуги користувачів (обслуговування користувачів) можуть бути здійснені рекурсією багаторазових шарів (рівнів) послуги всередині страти.

У страті послуг *NGN* розглядаються ті застосування та їх послуги, які функціонують між взаємодіючими (рівними за положенням) об'єктами. Наприклад, послуги можуть відноситись до голосу, даних, або відео застосувань, установлених окремо або в деякій комбінації у випадку мультимедіа застосувань. З точки зору архітектури передбачається, що кожен шар (рівень) страти послуг включає у себе свої площини користувача (даних), сигналізації та контролю та менеджменту.

Страта транспорту – це та частина *NGN*, яка забезпечує функції користувача, що передають дані та функції, які виконують управління та менеджмент транспорту ресурсів для перенесення цих даних між прикінцевими

об’єктами. Дані, які переносяться, можуть бути даними користувача, управління (сигналізації та контролю) і/або менеджменту. Динамічно чи статично може бути встановлене управління (контроль) і/або управління (менеджмент) передачі інформації між певними об’єктами.

Рисунок 4.1 – Структурна модель *NGN* з позицій кібербезпеки

З точки зору архітектури передбачається, що кожна страта послуг включає у себе свої площини користувача (даних), сигналізації та контролю та менеджменту.

На практиці, для певного рівня площини користувача (даних) або сигналізації та контролю, або менеджменту можуть бути пустими. Функції для всіх площин можуть оброблятися одним протоколом.

Ролі, гравці (учасники гри), організація в підприємницькій моделі, послуги й застосування у структурній моделі, функції та інтерфейси у функціональній моделі є складовими частинами, які будуть застосовані у моделі реалізації.

У структурній моделі описані окремо послуги й компоненти послуг. Це забезпечує:

– підприємницьку модель, яка визначає гравців і ролі, тобто ділову діяльність згідно з цільовими цінностями, такими як структурні й інфраструктурні ролі;

– модель реалізації, в якій можуть розглядатись розподіл і реалізація функцій у обладнанні, визначатись протоколи передачі через інтерфейси обладнання й інші засоби фізичної реалізації.

Далі описана модель реалізації в загальній високорівневій формі. Аналіз послуг і функцій проводиться роздільно.

4.3 Загальні положення щодо кібербезпеки *NGN*

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження та вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів. Впливи, які призводять до зниження цінності інформаційних ресурсів, називаються *несприятливими*. Потенційно можливий несприятливий вплив називається *загрозою*.

Телекомунікаційна мережа являє собою організаційно-технічну систему, що об'єднує систему надання послуг, систему управління (менеджменту), транспортну систему, мережу доступу, фізичне середовище, персонал та оброблювану інформацію. Прийнято розрізняти два основних напрями ТЗІ в *NGN* – це захист *NGN* і оброблюваної інформації від несанкціонованого доступу та захист інформації від витоку технічними каналами (оптичними, акустичними, захист від витоку каналами побічних електромагнітних випромінювань і наведень).

Захист інформації, що передається й обробляється в *NGN*, полягає у створенні та підтримці в дієздатному стані системи заходів як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Іншими словами, захист інформації спрямовано на забезпечення кібербезпеки оброблюваної інформації та *NGN* у цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації та *NGN*. Система зазначених заходів, що забезпечує захист інформації в *NGN*, називається *комплексною системою захисту інформації*.

Істотна частина проблем забезпечення захисту інформації в *NGN* може бути вирішена організаційними заходами. Проте, з розвитком інформаційних технологій спостерігається тенденція зростання потреби застосування технічних заходів і засобів захисту.

Організаційні та фізичні заходи захисту, включаючи захист від фізичного НСД до компонентів системи телекомунікацій, як і захист від витоку технічними каналами, не є предметом розгляду. Незважаючи на це, при викладі матеріалу увага приділяється також і деяким нетехнічним аспектам, але тільки там, де це впливає на оцінку технічної захищеності.

Правовою основою забезпечення технічного захисту інформації в Україні є Конституція України, Закони України "Про інформацію", "Про основи національної безпеки України", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про державну таємницю", "Про науково-технічну інформацію", "Про телекомунікації", "Про захист персональних даних", "Про доступ до публічної інформації", "Концепція технічного захисту

інформації в Україні", "Положення про порядок здійснення криптографічного захисту інформації в Україні", "Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин.

Архітектура кібербезпеки з кінця в кінець. Незалежно від базової технології мережі архітектура забезпечення кібербезпеки передбачає структуру реалізації наскрізної безпеки зв'язку. Наскрізному зв'язку відповідає англомовні терміни «point-to-point», «end-to-end», які мають смисл для одно точкових з'єднань. Архітектура кібербезпеки призначена для вирішення глобальної складної задачі безпеки провайдерів послуг, підприємств і користувачів, вона застосовується для конвертованої безпроводової, оптичної та проводної мережі, мереж передачі мови й даних. Архітектура торкається безпеки управління, менеджменту, контролю та використання мережної інфраструктури, послуг і застосувань. Передбачається забезпечення можливості активно діючої системи виявлення вразливих місць у безпеці та пом'якшення пов'язаних з ними наслідків відносно відомих загроз. Архітектура безпеки логічно поділяє складний набір функцій, зв'язаний із наскрізною безпекою зв'язку на окремі архітектурні компоненти. Цей поділ дає можливість системного підходу до наскрізної безпеки зв'язку та оцінки безпеки існуючих мереж.

Кібербезпека забезпечується сукупністю засобів безпеки, які захищають від усіх основних загроз. Засоби безпеки розроблені для всіх типів мереж, а також розповсюджуються на всі типи користувачів та інформаційні застосування користувача. Ці засоби застосовуються для провайдерів послуг або підприємств, що пропонують послуги безпеки своїм споживачам. Засобами безпеки є:

- контроль доступу;
- автентифікація;
- невідмовність (від факту приймання чи передавання);
- конфіденційність даних;
- безпека комунікацій;
- цілісність даних;
- готовність; -

приватність.

Для того, щоб забезпечити вирішення питань наскрізної безпеки, телекомунікацій засоби кібербезпеки повинні бути застосовані до ієрархії мережного обладнання й угрупування засобів, які розглядаються як рівні безпеки. Розрізняють три рівні:

– рівень кібербезпеки інфраструктури;
– рівень безпеки послуг;
– рівень безпеки застосувань.

На рис. 5.2 наведено архітектуру безпеки та показано, яким чином засоби безпеки застосовуються до рівнів безпеки та площин для того щоб зменшити кількість уразливих місць, які присутні на кожному з рівнів взаємодії відкритих

систем. Спочатку звертається увага на вразливі місця рівня інфраструктури, потім рівня послуг і рівня застосувань.

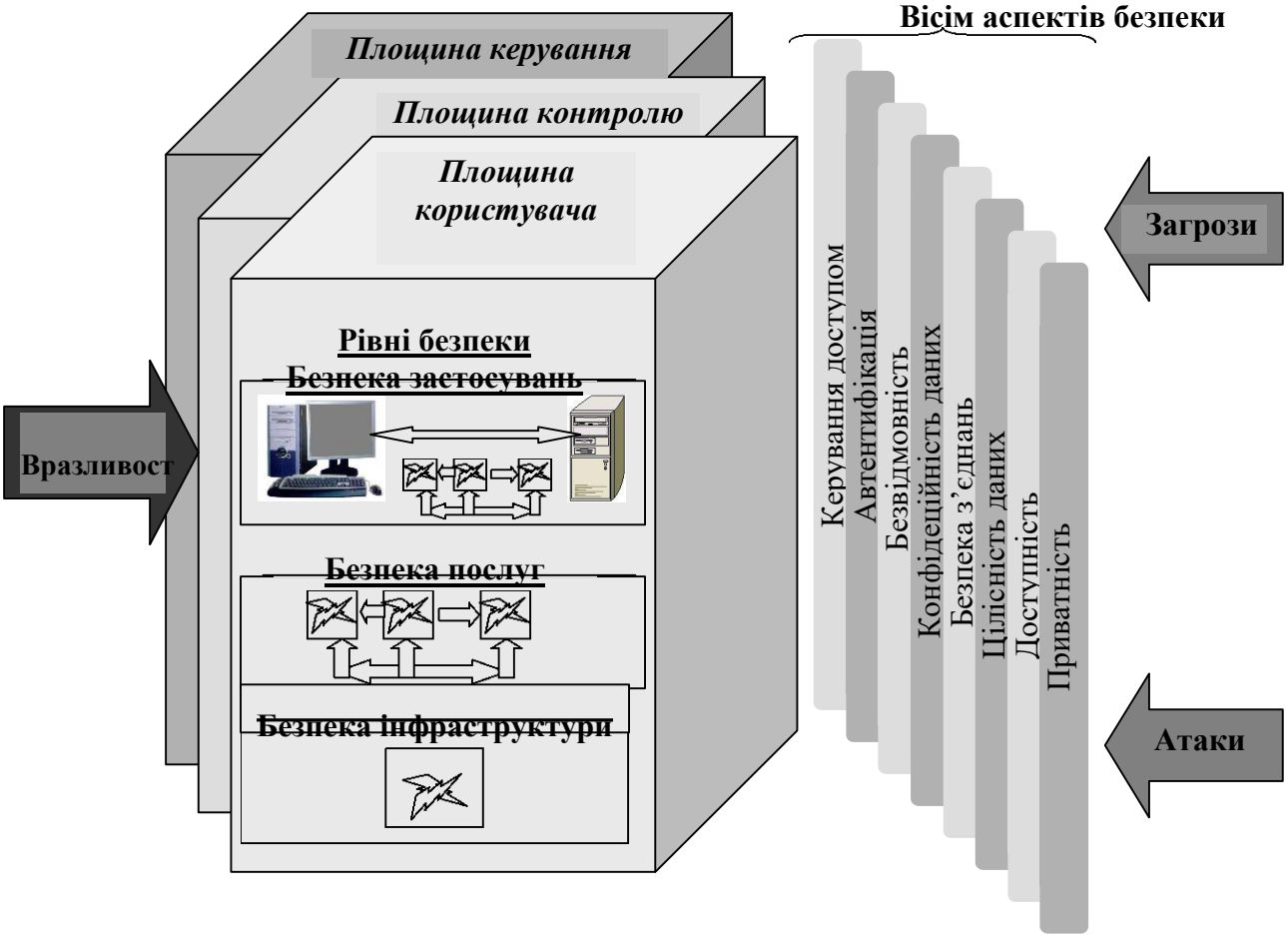


Рисунок 4.2 – Застосування засобів кібербезпеки до рівнів і площин мережі для різних типів діяльності з кібербезпеки (рисунок запозичено з Рекомендації МСТ-Т X.805)

Площина безпеки – це певний тип функціонування мережі, захищений за допомогою засобів безпеки. Визначено три площини безпеки для представлення трьох типів подій, що відбуваються в мережі. Площинами безпеки є: площина менеджменту, площина управління (сигналізації), площина користувача.

Ці площини призначені для конкретних потреб безпеки, пов'язаних із функціонуванням менеджменту мережі, контролю мережі та передачі сигналів і діяльністю користувача, відповідно. Мережі розробляються таким чином, щоб події в одній площині безпеки відбувались незалежно від інших площин безпеки.

Наприклад, потік запитів (викликів) у площині користувача до серверів не повинен блокувати інтерфейс управління, адміністрування, технічного обслуговування й експлуатації (OAM&P) у площині менеджменту. А, наприклад, задача безпеки менеджменту послуги має бути незалежна від задачі

безпеки контролю цієї послуги та від задачі безпеки даних, які передаються за допомогою цієї послуги.

Безпека охоплює всі архітектурні рівні мережі. Такий підхід дозволяє розробити гнучкі масштабовані рішення по всьому мережному рівню, рівню застосувань і рівню менеджменту для всіх типів організацій.

Система кібербезпеки вбудовується в функціональну архітектуру телекомунікаційних мереж за принципом інтегрування її із системою управління та менеджменту.

4.4 Модель довіри кібербезпеки

У функціональній архітектурі телекомунікаційних мереж (ТМ) визначаються функціональні об'єкти – ФО (фізичні та віртуальні). Засоби забезпечення кібербезпеки залежать від способу, за допомогою якого ФО взаємозв'язуються один з одним. Архітектура безпеки ТМ базується, в решті решт, на фізичних мережних елементах (МЕ), тобто на матеріальних модулях, які містять один або декілька ФО, що об'єднані один з одним.

У ТМ виділяються три зони безпеки:

- довірена;
- довірена, але вразлива;
- недовірена, які залежать від системи технічної експлуатації й управління, місцеположення та можливостей з'єднання з іншими пристроями/елементами мережі. Ці три зони довіри кібербезпеки показані на рис. 5.3.

Довірена зона кібербезпеки мережі, або коротко «довірена зона» – це область, де розміщені елементи та системи ТМ, які ніколи не зв'язуються напряму з обладнанням користувача або іншими доменами/мережевими елементами телекомунікаційної мережі – МЕ. ТМ у даній зоні повністю управляються провайдером ТМ, що розташовані в домені провайдера ТМ і зв'язуються лише з елементами в «довіреній зоні» та з елементами у «довіреній але вразливій зоні». Довірена зона захищається поєднанням різних методів. Наприклад, фізична безпека елементів ТМ, загальне укріплення мережі, використання безпечної сигналізації, безпечність для повідомлень системи *OAMP* окремої мережі *VPN* у межах мережі *MPLS*/*IP* для зв'язку в межах «довіреної» зони.

Довірена, але вразлива зона кібербезпеки мережі, або коротко «довірена, але вразлива зона» представляє собою зону, в якій працюють і обслуговуються МЕ провайдера ТМ. Обладнання може знаходитись під управлінням або користувача/абонента, або провайдера ТМ. Обладнання може знаходитись як на об'єктах провайдера ТМ, так і в інших місцях. Воно зв'язується з елементами як у довіреній зоні, так і в недовіреній зоні, і тому, є «вразливим». Головна функція кібербезпеки полягає в захисті елементів ТМ у довіреній зоні від атак на кібербезпеку, що ініційовані в недовіреній зоні. Елементи, що розташовані в домені провайдера ТМ, які мають можливість з'єднання з елементами, що знаходяться поза довіреної зони, називаються *приграничними мережними елементами* (ПМЕ).

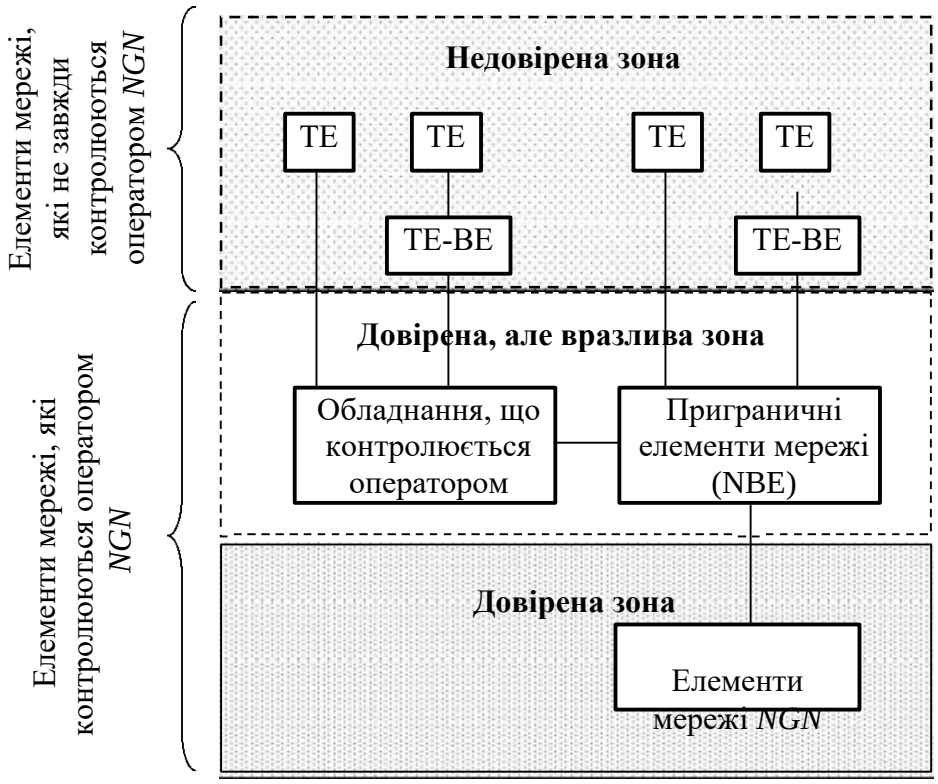


Рисунок 4.3 – Модель довіри кібербезпеки

Прикладами таких елементів є:

– пригранічний мережний елемент (ПМЕ) на інтерфейсі *UNI*, який служить засобом зв'язку зі службою управління або транспортними елементами провайдера ТМ у довіреній зоні для забезпечення доступу користувача/абонента до мережі провайдера ТМ з метою отримання послуг та/або транспортування даних;

– пригранічний доменний елемент (ПДЕ), що є тим самим видом обладнання, що й ПМЕ, але знаходиться на кордоні домена;

– пригранічний мережний елемент (ПМЕ) конфігурації пристроїв і початкового завантаження служить для зв'язку із системою конфігурації пристроїв провайдера в довіреній зоні та дозволяє конфігурувати пристрої користувача/абонента та обладнання провайдера, що знаходиться поза приміщень провайдера;

– пригранічний мережний елемент (ПМЕ) *OAMP*-ПМЕ служить засобом зв'язку із системами технічної експлуатації та обслуговування (*OAMP*) провайдера ТМ у довіреній зоні та служить для обслуговування та підтримки пристроїв користувача/абонента й обладнання провайдера ТМ, що знаходиться поза приміщень провайдера;

– пригранічний мережний елемент (ПМЕ) сервера застосувань/веб-сервера, який служить засобом зв'язку із серверами провайдера ТМ у довіреній зоні та служить для надання користувачу/абоненту доступу до веб-послуг.

Прикладом пристроїв/елементів, які управляються провайдером ТМ і можуть не бути розташованими в приміщеннях провайдера ТМ і можуть належати або не належати провайдеру ТМ, відносяться:

– обладнання зовнішніх пристроїв/технології доступу;

– маршрутизатор базової станції – елемент мережі, що об'єднує базову станцію, контролер радіомережі та функціональні можливості маршрутизатора;

– оптичні блоки в межах місцеположення користувача/абонента.

Захист «довіреної, але вразливої зони», що складається з МЕ, буде здійснюватись поєднанням різних методів. Прикладами є: фізичний захист елементів ТМ, загальне укріплення мережі, присвоєння кожному елементу ТМ унікального сертифіката, використання безпечної сигналізації для всіх повідомлень сигналізації, що відправляються елементам ТМ у довіреній зоні, безпечність для повідомлень системи *OAMP*, а також за необхідністю, модульні фільтри пакетів і брандмауери (міжмережні екрани).

«Недовірена зона» включає у себе всі елементи мережі абонентних мереж або мереж чи доменів інших провайдерів ТМ, що знаходяться за межами основного домена, які зв'язані з приграничними елементами провайдера ТМ. Провайдери ТМ можуть не мати можливості управляти прикінцевим обладнанням користувача, яке розміщене у «недовіреній зоні», та не мати можливості нав'язати користувачеві політику безпеки провайдера. Проте бажано, застосовувати деякі заходи кібербезпеки. Для цього рекомендується, щоб сигналізація, середовище передачі й *OAM&P* були б захищені. Але через недостатній фізичний захист ці заходи не можуть вважатися абсолютно безпечними..

Коли ТМ з'єднується з іншою мережею, довіра залежить від:

– фізичного з'єднання, яке може бути безпосереднім усередині захищеної будівлі або через сумісно використаний пристрій;

– типу обміну трафіком, який може проходити безпосередньо між двома провайдерами послуг *NGN* або через одного чи декількох провайдерів транспортних мереж;

– ділових відносин, до яких можуть відноситись пункти щодо штрафів в угодах *SLA* та/або довіри до політики безпеки іншого провайдера ТМ;

– як правило, провайдери ТМ повинні вважати інших провайдерів недовіреними.

Питання для самоконтролю

1. Поясніть визначення кібербезпеки та кіберсередовища.
2. Яка природа середовища кібербезпеки?
3. Охарактеризуйте структурну модель *NGN* з позицій кібербезпеки.
4. Дайте перелік цілей проектування мереж майбутнього.
5. Яка модель довіри щодо кібербезпеки *NGN*?
6. Яка функціональна гнучкість проектується реалізувати в мережах майбутнього?
7. Поясніть головні інтерфейси взаємодії телекомунікаційних мереж.
8. Яка функціональна архітектура *NGN* з позицій кібербезпеки?
9. Які ресурси підлягають захисту та цілі захисту в мережах майбутнього?
10. Цілі та задачі захисту цінностей, ресурсів та інтерфейсів *NGN*, пов'язаних з *UNI*.

11. Цілі та задачі захисту цінностей, ресурсів, інформації та інтерфейсів, пов’язаних із транспортним рівнем.

12. Цілі та задачі захисту цінностей, ресурсів, інформації та інтерфейсів, пов’язаних з рівнем послуг у частині менеджменту послугами.

13. Цілі та задачі захисту цінностей, ресурсів, інформації та інтерфейсів, пов’язаних з рівнем послуг у частині підтримки застосувань і послуг.

14. Цілі та задачі захисту цінностей, ресурсів, інформації та інтерфейсів, пов’язаних з адмініструванням.

15. Якими методами й засобами буде розвинена ідентифікація в мережах майбутнього?

Семінарське заняття №5
ЗАГАЛЬНІ ВИМОГИ ДО КІБЕРБЕЗПЕКИ МЕРЕЖ НАСТУПНИХ ПОКОЛІНЬ

5.1 Політика кібербезпеки інформації та модель порушника

Під *політикою кібербезпеки* інформації слід розуміти набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації та спрямовані на захист інформації від певних загроз. Термін "політика кібербезпеки" може бути застосовано щодо організації, мережі, операційної системи, послуги, що реалізується системою (набору функцій) тощо. Чим дрібніше об’єкт, відносно якого застосовується даний термін, тим конкретнішими та формальнішими стають правила.

Політика кібербезпеки інформації в *NGN* є частиною загальної політики кібербезпеки підприємства та має успадкувати, зокрема, положення державної політики в галузі захисту інформації. Для кожної *NGN* політика кібербезпеки інформації може бути індивідуальною та може залежати від технології обробки інформації, що реалізується, особливостей програмного забезпечення, фізичного середовища та від багатьох інших факторів. Тоді політика кібербезпеки інформації в такій *NGN* буде складеною, а її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси *NGN*, що потребують захисту, зокрема установлювати категорії інформації в *NGN*. Мають бути сформульовані основні загрози для *NGN*, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Як складові частини загальної політики кібербезпеки інформації в *NGN* мають існувати політики забезпечення конфіденційності, цілісності та доступності оброблюваної інформації. Відповідальність персоналу за виконання положень політики кібербезпеки має бути персоніфікована.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів *NGN*, складає правила розмежування доступу.

Модель порушника. Модель порушника надана в НД ТЗІ 1.1-002-99. Як порушник розглядається особа, яка може отримати доступ до роботи з включеними до складу *NGN* засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами *NGN*. Виділяються чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожен наступний рівень включає у себе функціональні можливості попереднього:

– перший рівень визначає найнижчий рівень можливостей проведення діалогу з *NGN* – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– другий рівень визначається можливістю створення та запуску власних програм з новими функціями обробки інформації;

– третій рівень визначається можливістю управління функціонуванням *NGN*, тобто впливом на базове програмне забезпечення системи та на склад, і конфігурацію її обладнання;

– четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію та ремонт апаратних компонентів *NGN*, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

Припускається, що на своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію щодо *NGN* і системи кібербезпеки.

Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

5.2 Загальні задачі системи кібербезпеки

Основними задачами системи кібербезпеки є:

– функції кібербезпеки *NGN* повинні бути розширюваними та досить гнучкими для задоволення різних потреб;

– вимоги безпеки повинні врахувати якісні показники, зручність в експлуатації, розширюваність і вартість *NGN*;

– за можливості методи безпеки повинні базуватись на існуючих і добре зрозумілих стандартах безпеки;

– архітектура безпеки *NGN* повинна бути універсально масштабована в межах домена провайдера мережі, у доменах декількох провайдерів мережі, при наданні послуг безпеки;

– архітектура безпеки *NGN* повинна врахувати логічний і фізичний розподіл трафіка сигналізації та контролю, трафіка користувача та трафіка управління (менеджменту);

– безпека мереж *NGN* повинна безпечно забезпечуватись і безпечно управлятись;

– мережа *NGN* повинна забезпечувати безпеку з усіх точок зору: служб, провайдера мережі та користувача;

– методи безпеки не повинні впливати на якість послуг, що надаються;

– безпека повинна забезпечувати абонентам і провайдерам можливість простої конфігурації та безпечної роботи (включай і працюй);

– відповідні рівні захисту повинні підтримуватись навіть, якщо використовується функція багатоадресного зв’язку;

– функція послуги виявлення повинна мати множину критеріїв огляду (вибору), наприклад, місцезнаходження, вартість тощо, для забезпечення необхідного масштабування з необхідними механізмами забезпечення безпеки та приватності;

– система розпізнавання адреси повинна бути спеціальною системою, яка використовується лише даною мережею та вимагає застосування певних заходів безпеки. Дана система може використовувати бази даних, що знаходяться в межах чи поза домену;

- повинні дотримуватись принципи та загальні задачі безпеки для безпечного управління системою менеджменту телекомунікаціями (у тому вигляді, як вони наведені в розділі 7 Рекомендації МСЕ-Т М.3016.0).

Загальні задачі забезпечення кібербезпеки для менеджменту NGN. Задачі кібербезпеки повинні бути визначені виходячи з інтересів, ділових зв'язків, законодавчих і регламентуючих обмежень, договірних обмежень і вимог щодо оператора та інших діючих об'єктів. Загальні задачі формулюються в відповідності з видом і мовою менеджменту *NGN*.

Задачами кібербезпеки для менеджменту *NGN* є:

– можливість доступу та роботи з наявними засобами менеджменту *NGN* повинні мати лише легально діючі об'єкти. Термін «доступ до наявних засобів» розуміється як можливість виконання функцій, а також зчитування інформації;

– легально діючі об'єкти повинні мати можливість доступу та роботи з наявними засобами, якщо вони санкціоновані для доступу;

– всі діючі об'єкти повинні бути підзвітні за свої й лише за свої дії в менеджменті *NGN*;

– доступність менеджменту *NGN* повинна бути захищена від не запитуваного доступу або не запитуваних операцій;

– повинна бути забезпечена можливість пошуку в менеджменті *NGN* інформації, що пов'язана з безпекою;

– у випадку виявлення порушення безпеки обробка відбувається контрольованим способом, мінімізуючи тим самим нанесений збиток;

– повинна бути забезпечена можливість відновлення нормальних рівнів безпеки після виявлення «злому» в системі безпеки;

– архітектура безпеки менеджменту *NGN* повинна мати певну гнучкість для можливості підтримки різних стратегій безпеки, наприклад, застосування механізмів безпеки з різним ступенем надійності.

Можна показати, що неодмінною та достатньою умовою реалізації перших п'яти вище зазначених задач є забезпечення послуг:

– конфіденційності (конфіденційності інформації, що передається та зберігається);

– цілісності даних (захист інформації, що передається та зберігається);

– підзвітності (будь-який об'єкт повинен нести відповідальність за будь-яку подію, яка ним ініційована);

– доступності (всі легітимні об'єкти повинні мати можливість правильного доступу до обладнання менеджменту *NGN*).

Інші вище згадані задачі вимагають додаткових засобів і засобів захисту.

Задачі кібербезпеки, що охоплюють домени декількох провайдерів мережних послуг. Головною задачею є забезпечення безпеки на основі мережі для наскрізних систем зв'язку в умовах існування множини доменів провайдерів.

Це досягається за допомогою забезпечення наскрізної безпеки системи комунікацій, що заснована на можливості ретрансляції через домени різних провайдерів.

На рис. 5.1 показані основні принципи побудови мережі, яка забезпечує зв'язок між конечними користувачами через множину мережних доменів.

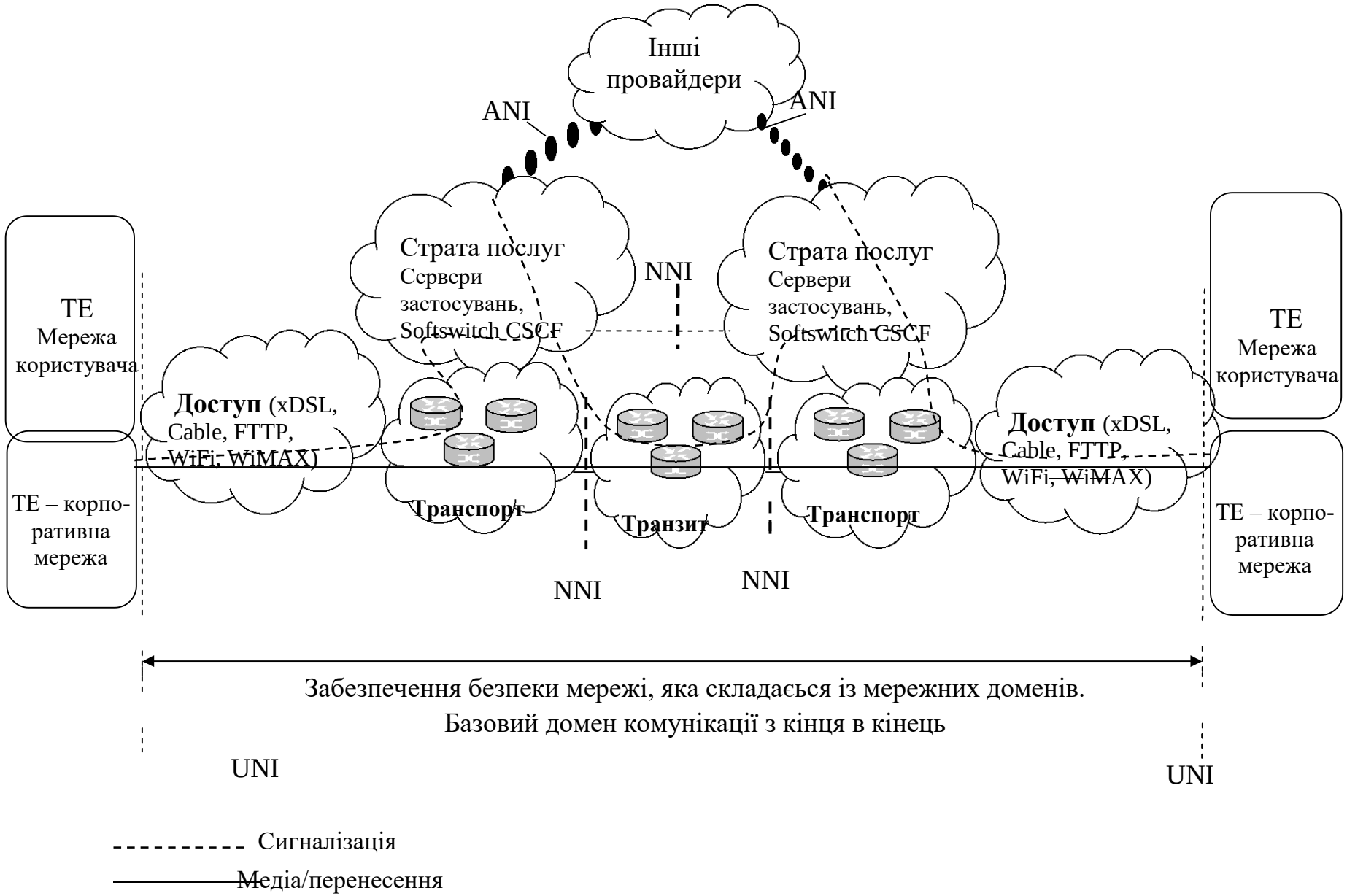


Рисунок 5.1 – Безпека комунікацій у мультимережі

Кожна ланка мережі несе відповідальність за безпеку в межах свого домена безпеки для полегшення безпеки та доступності системи комунікацій *NGN* в умовах множини мереж.

Довірена модель між взаємозв'язаними мережами *NGN* залежить від декількох аспектів, таких як фізичний взаємозв'язок, моделі однорангових мереж і ділове співробітництво.

Задачі, що характерні складовим безпеки. Задачі, що описані в даному пункті, є характерними для більшості певних складових (аспектів) безпеки. Вони є загальними для всіх інтерфейсів.

***Контроль доступу*.** Провайдери *NGN* повинні надавати доступ лише авторизованим абонентам.

Авторизація може надаватись провайдером, що надає доступ, або іншими провайдерами після підтвердження автентичності в процесі автентифікації та контролю доступу.

Мережа *NGN* повинна запобігати несанкціонованому доступу, наприклад, порушників, що маскуються під авторизованих користувачів.

***Автентифікація*.** Провайдер *NGN* повинен підтримувати можливість автентифікації абонентів, обладнання, елементів мережі й інших провайдерів. Автентифікація включає у себе, але не обмежується лише наступним:

– можливостей автентифікувати користувачів для доступу до транспортної мережі, наприклад, автентифікація та авторизація пристрою користувача, шлюзу, шлюзу мережі користувача або шлюзу корпоративної мережі для отримання доступу або приєднання до доступу до транспортної мережі:

– можливостей автентифікувати користувачів для доступу до послуг на початку та під час доставки послуги, наприклад, автентифікувати користувача, пристрій або комбінації користувач/пристрій, коли автентифікація застосовується для доступу до послуг/застосувань *NGN*;

– можливості для абонента автентифікувати провайдера *NGN* на кожному рівні, наприклад, автентифікація користувачем ідентичності провайдера приєднаної мережі *NGN* або провайдера послуг, якщо це потрібно політиці безпеки;

– можливостей, що дозволяють користувачу автентифікувати рівноправні з ним об'єкти, наприклад, користувача, який викликається, об'єкт, який ініціює виклик або джерело даних, як послуг або можливостей мережі;

– можливостей, що дозволяють двохсторонню автентифікацію між двома провайдерами *NGN* на кожному з рівнів обміну трафіком сигналізації, управління, менеджменту та інформації/каналу передавання, наприклад, автентифікація мереж, приєднаних безпосередньо чи опосередковано через інтерфейси *NNI*:

– можливості автентифікації інших провайдерів послуг через інтерфейси *ANI*. Повинні підтримуватися методи на основі *SIM* чи на іншій основі.

Зауважимо, що автентифікація об'єкта не означає позитивного підтвердження фізичної особи.

Підзвітність (невідмовність від участі). Будь-який об'єкт повинен нести відповідальність за будь-яку ініційовану ним дію.

Всі мережні елементи повинні забезпечувати можливість того, щоб об'єкт не міг заперечити свою відповідальність за будь-які виконані ним дії, а також за їх результати. Все програмне забезпечення, що поставляється провайдеру послуг, повинно містити, коли це необхідно, криптографічну автентифікацію та механізми захисту цілісності, а саме: цифрові підписи або симетричну автентифікацію повідомлень

Конфіденційність даних. Провайдери *NGN* повинні захищати конфіденційність трафіка абонента за допомогою криптографії або іншими способами.

Провайдери *NGN* повинні захищати конфіденційність повідомлень контролю за допомогою криптографії або іншими способами, якщо цього вимагає політика безпеки.

Провайдери *NGN* повинні захищати конфіденційність за допомогою криптографії або іншими способами.

Безпека комунікації. Провайдери *NGN* повинні мати можливість надавати механізми забезпечення того, що інформація не піддається незаконному пере направленню або перехопленню.

Цілісність даних. Провайдери *NGN* повинні захищати цілісність трафіка абонента за допомогою криптографії або іншими способами.

Провайдери *NGN* повинні захищати цілісність повідомлень контролю за допомогою криптографії або іншими способами, якщо цього вимагає політика безпеки.

Провайдери *NGN* повинні захищати цілісність за допомогою криптографії або іншими способами.

Доступність. Для запобігання атак відмови в обслуговуванні (*DoS*), розповсюдження вірусів і червів, а також інших атак, провайдер *NGN* повинен мати можливість підтримувати надання заходів безпеки для запобігання або завершення з'єднань з невідповідним обладнанням користувача. Дія даних можливостей може призупинятися для забезпечення зв'язку в надзвичайних ситуаціях.

Елементи зовнішньої мережі *NGN* також можуть бути сприйнятливі до вірусів, червів й інших атак. Також необхідні аналогічні заходи для карантину мережних компонентів.

Мережа *NGN* повинна надавати можливості забезпечення безпеки, для того щоб провайдер *NGN* міг відфільтрувати пакети та трафік, які вважаються шкідливими з точки зору політики безпеки.

Мережа *NGN* повинна надавати можливості для підтримки функцій і процедур відновлення після лиха.

***Приватність* (*захист персональних даних*).** Мережа *NGN* повинна забезпечувати можливість захисту персональної інформації абонента, наприклад, даних щодо місцеположення, ідентичність, телефонні номери, мережні адреси або дані обліку викликів, згідно з національним правилам і законам.

Ці спеціальні вимоги здійснюються у відповідності до Закону України «Про захист персональних даних».

6.3 Технології забезпечення кібербезпеки

Існуючі системи захисту інформації в Україні описує модель, що описана у навчальному поссібнику [34, с. 56 - 59]. Логіка забезпечення безпеки інформації описується ієрархічною послідовністю: “загрози безпеки → послуги безпеки → механізми безпеки”. Служби безпеки будуються за ієрархічним багаторівневим модульним принципом: служба безпеки – послуги безпеки – функції безпеки – механізми безпеки. Служба безпеки реалізує сервіси безпеки, розподілені за рівнями. Кожен сервіс – це набір функціональних послуг безпеки, які надаються певним рівнем. Кожна функціональна послуга безпеки реалізується одним чи більш механізмами безпеки. Одні й ті ж самі механізми можуть бути використані для реалізації кількох функціональних послуг. Це забезпечує універсальність, гнучкість та економічність системи захисту інформації та ресурсів мереж.

У сучасних складних телекомунікаційних системах системи безпеки «з кінця в кінець» своїми спеціальними механізмами безпеки та частково загальними механізмами безпеки інтегровані в телекомунікаційну систему та розподілені за складовими мережі та рівнями й площинами її архітектури. З іншого боку механізми та послуги безпеки розвиваючись ускладнились і самі перетворились в технології.

Бурхливий розвиток телекомунікаційних технологій, зростання кіберзлочинності, ускладнення мереж вимагають розвитку від засобів і заходів кібербезпеки до технологій кібербезпеки. Складність і ефективність технологій нападу на інформаційні ресурси користувачів і підприємств весь час удосконалюються. Зловмисники можуть швидко розробляти атаки з проникненням і розкриттям інформації. При цьому використовуються вразливі місця, які виявляються в інформаційних технологіях підприємств, призначені до зламу. Нападники можуть автоматизувати атаки проникнення та зламу й при цьому зробити їх доступними для широкої публіки.

У процесі свого розвитку послуги та механізми безпеки переросли в закінчені технології, тобто сукупність методів, процесів, засобів і заходів, що використовуються для забезпечення кібербезпеки. Логіку забезпечення безпеки доцільно доповнити технологіями кібербезпеки, які зручно описувати ієрархічною послідовністю: “техніка кібербезпеки (*technique* – технічні прийоми) → категорії (*category*) технологій кібербезпеки → технології (*technology*) кібербезпеки” [див. 35, с. 26, 27]. На рис. 6.2 показана модель класифікації технологій кібербезпеки.

Технологія (від грец. *techne* – мистецтво, майстерність, уміння + *logos* – поняття, вчення, думка, причина, методика, спосіб виробництва) – у широкому смислі – сукупність методів, процесів і матеріалів, що використовується в певній області виробництва; сукупність знань щодо способів і засобів проведення виробництва товарів і послуг із економічних ресурсів разом з процесами, за яких відбувається якісні зміни об’єктів, що обробляються; а також наукове описання способів технічного виробництва.

Рисунок 5.2 – Модель класифікації технологій кібербезпеки

У вузькому смислі, *технологія* – це комплекс організаційних заходів, операцій і прийомів, способів перетворення речовини, енергії, інформації, спрямованих на виготовлення, обслуговування та експлуатацію виробу з контролем якості та оптимальними витратами й обумовленим поточним рівнем розвитку науки, техніки та суспільства.

Перехід до високих технологій і відповідної їм техніки є найважливішою ланкою науково-технічної революції на сучасному етапі.

Стосовно галузі кібербезпеки можна дати таке визначення.

Технологія кібербезпеки – у широкому смислі – це комплекс організаційних заходів, послуг, програмних і апаратних функцій, механізмів, засобів, методів і прийомів, режимів роботи, послідовності операцій і процедур, обладнання, а також самі процеси проектування, побудови, експлуатації, управління та менеджменту комплексу забезпечення кібербезпеки із заданим рівнем безпеки, гарантій рівня безпеки та оптимальними витратами. У вузькому смислі, *технологія кібербезпеки* – це описування процесів забезпечення кібербезпеки, інструкції з їх виконання, технологічні вимоги до кібербезпеки тощо, а також операції проектування, створення, експлуатації, менеджменту та управління системи кібербезпеки, які є основою процесу забезпечення кібербезпеки.

Технологія кібербезпеки служить для створення віртуального продукту – безпеки з високими техніко-економічними параметрами та гарантії безпеки.

У своїй класифікації технології кібербезпеки групуються за *категоріями,* за *ознаками цілей*, які ними досягаються. За методами досягнення цілей сукупності категорій технології кібербезпеки об’єднуються в технічні прийоми.

Виділяються такі категорії технологій кібербезпеки:

– сертифікати й архітектура відкритих ключів (*Certificate and public key architecture*);

– гарантії (*Assuranse*);

– захист периметра (*Perimeter protection*);

– автентифікація (*Authentification*);

– авторизація, надання прав (*Authorization*);

– антивірусний захист (*Antivirus*);

– цілісність даних, ресурсів, обладнання (*Integrity*);

– виявлення порушень, атак (*Detection*);

– запобігання порушень, атак (*Prevention*);

– реєстрація подій кібербезпеки (*Logging*),

– менеджмент мережі (*Network management*),

– політика кібербезпеки (*Policy*).

За методами досягнення цілей сукупності *категорій* технології кібербезпеки об’єднуються в технічні прийоми – *техніки*. Термін «техніка» застосовується тут в одному зі своїх значень, а саме: *техніка* – це сукупність прийомів, способів, а також володіння цими прийомами, у даному разі, забезпечення кібербезпеки.

Виділяються такі техніки кібербезпеки:

– криптографія (*Cryptography*);

– контроль доступу (*Access control*);

– цілісність системи (*System integrity*);
– аудит і моніторинг (*Audit and Monitoring*);
– менеджмент (*Management*);

Техніки кібербезпеки можуть бути використані для гарантування готовності систем, цілісності, автентичності, конфіденційності та невідмовності від виконаних дій. Техніки кібербезпеки можуть бути використані для гарантій захисту персональних даних користувача. Техніки кібербезпеки можуть бути використані для встановлення достовірності користувача.

Опишемо детальніше приклади доступних технологій кібербезпеки.

5.3.1 *Технології криптографії*

Однією з ефективних технологій захисту інформаційних ресурсів є застосування криптографічних методів. Технології *криптографії* – це застосування операцій перетворення до даних у простому вигляді для того, щоб забезпечити ***шифрування*** (*Encryption*) їх таємним кодом. До технологій криптографії відносяться: цифрові підписи, шифрування, розподіл ключів. Технології криптографії розподіляють за двома категоріями: сертифікати й архітектура відкритих ключів, гарантії. Дешифрування таємних даних дозволяє відновити початковий текст. Метою шифрування є засекречування даних під час передачі та зберігання.

Для шифрування/дешифрування даних можуть бути застосовані сучасні розвинені методи криптографії, що дозволені до використання нормативними документами у сфері захисту інформації в Україні. Дана технологія може бути використана для автентифікації відправника повідомлення та його невідмовнсті в наданні/отриманні послуг. Криптографія відіграє важливу роль у захисті інформації під час зберігання її в запам’ятовуючих пристроях або на носії даних і під час її передачі лініями зв’язку. Методи криптографії поділяють на два основних типи: симетричного ключа та асиметричного ключа.

Криптографія симетричного ключа використовує алгоритми, в яких ключ шифрування та ключ дешифрування один і той самий. Сторони, що обмінюються інформацією, повинні домовлятися щодо ключа та тримати ключ у таємниці.

Криптографія асиметричного ключа використовує два ключі: один ключ для шифрування даних і другий – для дешифрування закодованого тексту. У користувача є свій приватний таємний ключ, відомий лише йому, й відкритий ключ, відомий іншим. Відкритим ключем користуються всі інші для шифрування відкритого тексту. Але лише власник приватного таємного ключа може розшифрувати зашифрований текст. Методи криптографії симетричного ключа в загальному випадку більш швидкодіючі, ніж методи асиметричного ключа. Безпека таких методів залежить від складності розгадування ключа. Розвиток квантових комп’ютерів може звести нанівець ефективність таких методів. Вони дозволять розкривати ключі методом прямого перебору.

Головні труднощі в мережах для криптографії симетричного ключа полягають у проблемі розподілу ключів. Система ***розподілу ключів*** (*Key*

exchange) має мету встановлення або сеансового ключа, або ключа менеджменту інформаційним обміном, щоб його використати для безпечного з'єднання. Криптографія відкритого ключа використовує цифрові сертифікати для вирішення питань менеджменту відкритих ключів і відкликання ключів.

Цифрові підписи (*Digital signatures*) є прикладом практичної реалізації криптографії відкритого ключа. Мета цифрового підпису полягає в тому, щоб забезпечити видавання, зберігання та підтримання сертифікатів, які будуть використані у цифрових комунікаціях.

Сертифікат цифрового підпису забезпечує гарантію зв'язаності між відкритим ключем і власником сертифікату. При гарантуванні використовується ***шифрування*** (*Encryption*) із метою страхування автентичності даних.

Цифрові підписи можуть забезпечити автентифікацію, цілісність даних і невідмовність для транзакцій. Цифрові підписи можуть бути використані для підтвердження доказу заявленого ідентифікатора відправника повідомлення. Цифрові підписи часто використовуються в поєднанні з цифровим сертифікатом.

Сертифікати цифрового підпису використовуються як транспортний засіб, що переносить інформацію, яка необхідна в криптографії відкритого ключа із застосуванням цифрового підпису. Сертифікати цифрового підпису можуть видаватись користувачам з підтвердженими або довіреними повноваженнями.

5.3.2 *Технології контролю доступу*

Контроль доступу спрямовано на гарантування того факту, що лише санкціонований користувач може отримати доступ до пристрою мережі або до підключеної системи. Контроль доступу дає можливість спеціалістам контролю мережі краще проаналізувати та зрозуміти природу атак, які відбуваються в мережі. Існує багато методів, що можуть бути використані для реалізації контролю доступу: міжмережні екрани, менеджмент контента, одно- та багатофакторна автентифікація, смарт-маркери, визначення ролей, визначення правил доступу. Технології контролю доступу поділяються на категорії: захист периметра, автентифікація, авторизація.

Захист периметра. При технічному захисті інформації виникають питання захисту периметра. Технології захисту периметра попереджують доступ до мережі або комп'ютеру з боку неперевірених або несанкціонованих зовнішніх користувачів. Технології захисту периметра встановлюють логічні або фізичні границі між зонами, що захищаються, та зонами, відкритими для загального користування та неперевірених зовнішніх користувачів. Технології захисту периметра можуть бути застосовані для захисту мережі та окремого пристрою. До технологій захисту периметра відносяться: міжмережні екрани та менеджмент контента.

Міжмережні екрани (*Firewalls*). Мета застосування технології міжмережних екранів полягає в контролі доступу до мережі та з мережі. Технологію міжмережних екранів можна поділити на такі типи: фільтри

пакетів, шлюзи канального рівня (рівня маршрутів), шлюзи рівня застосувань, повно функціональний міжмережний екран із багаторівневою перевіркою.

Міжмережний екран фільтрації пакетів працює на рівні *IP*. Звичайно вони є частиною міжмережного екрана маршрутизатора. Вони порівнюють кожен пакет IP з певним набором правил до того, як переадресувати його наступним маршрутом або в його кінцевий пункт призначення. У залежності від результатів перевірки, міжмережний екран може видалити даний пакет, переадресувати його або відправити повідомлення автору. До правил може входити *IP*-адреса або пункт призначення, номер порту джерела або місця призначення, використаний протокол. Маршрутизатори протоколу трансляції мережних адрес (*NAT*) мають переваги міжмережного екрану фільтрації пакетів та додатково можуть приховати *IP*-адреси пристроїв за цим міжмережним екраном. Міжмережні екрани фільтрації пакетів мають незначний вплив на роботу мережі та надають певну степінь захисту на мережному рівні.

Шлюзи канального рівня працюють на рівні протоколу управління передачі (*TCP*) протоколів *TCP*/*IP* для того, щоб здійснювати моніторинг квітування *TCP* між пакетами для з'ясування того, чи є запитуваний сеанс законним чи ні. Більше того, запити, що виходять для віддаленого комп'ютера, виглядають перед отримувачем так, ніби він був створений у цьому шлюзі. Цей метод допомагає приховати інформацію щодо мережі, яка захищається. Шлюзи канального рівня не фільтрують індивідуальні пакети.

Проксі-сервери або шлюзи рівня застосувань можуть фільтрувати пакети на рівні застосувань. Вхідні чи вихідні запити не можуть отримати доступ до послуг, в яких нема проксі-серверів. Проксі-сервери перевіряють пакети на рівні застосувань, а саме *HTTP POST*. Проксі-сервер не допустить, щоб не конфігурований потік дійшов до застосування. Проксі-сервери можуть також бути використані для реєстрації діяльності користувача та реєстраційних імен. Проксі-сервери можуть надати високий рівень безпеки визнаному впливу на роботу мережі.

Повнофункціональні міжмережні екрани з багаторівневою перевіркою об'єднують властивості всіх вищеописаних типів міжмережних екранів. Багаторівневі міжмережні екрани фільтрують пакети на мережному рівні, встановлюють, чи є пакети сеансу дійсними та фільтрують зміст пакетів на рівні застосувань. Багаторівневі міжмережні екрани є прозорими для з'єднань між відправником і отримувачем.

Фільтрація контента (*Content management*) або програмне забезпечення ***менеджменту контента***, з обмеженням типу даних, які можуть бути доступні або поширені в мережі. Мета менеджменту контента полягає в проведенні поточного спостереження за потоком несумісної інформації. Менеджмент контента обмежує можливість користувачів отримувати доступ до контента за його межами. Це мінімізує можливості скачувати віруси та інші зловмисні коди з неперевірених місць. Менеджмент контента може приймати форму фільтрів *URL*. За його допомогою може бути відмовлено в доступі користувачам веб-сторінок із сумнівним контентом. Менеджмент контента може бути

використано для сканування повідомлень застосувань, таких як електронна пошта на предмет вірусів, спаму або незатвердженого контента.

Протокол трансляції мережних адрес (*NAT*) – це технологія, що надає можливість приховати схему адресації мережі за середовищем міжмережного екрану. У *NAT IP*-адреса системи у внутрішній мережі відображається на іншу, відповідну їй, зовнішню маршрутизовану *IP*-адресу. У *NAT* багато систем за міжмережним екраном мають можливість сумісно використати одну й ту саму зовнішню *IP*-адресу. Ресурси за міжмережним екраном залишаються доступними для зовнішніх користувачів за допомогою переадресації вхідних з'єднань на певні номери портів.

Шлюзи рівня застосувань складаються з апаратної та програмної частин базового пристрою або набору пристроїв. Вони розробляються для того, щоб обмежити доступ між двома окремими мережами. У цих системах використовуються повнофункціональні перевірки пакетів і застосувань проксі-серевера для того, щоб обмежити доступ мжємережами. Можна також застосувати поєднання та варіації цих методів. Протокол *NAT* може виконуватись за допомогою шлюзів рівня застосувань.

Проксі-застосування забезпечує розуміння прикладного рівня зроблених з'єднань, перевіряючи пакети на найвищому рівні стека протоколу. У проксі-застосувань є повний огляд обміну даними на рівні застосувань. Ця можливість дозволяє їм без труднощів розглянути найдрібніші подробиці кожної спроби підключення та реалізувати політику безпеки. У проксі-застосувань може бути можливість припинення підключень клієнта та ініціації нового підключення до внутрішньої захищеної мережі. Ця можливість надає додаткову безпеку, бо вона розподіляє внутрішні та зовнішні системи.

Автентифікація. До методів автентифікації входять: паролі, одноразовий пропуск, біометричні методи, смарт-карти та сертифікати. Автентифікація на основі паролів повинна використовувати сильні паролі. Пароль має складатись, що найменше, з восьми символів і мати, як мінімум, один буквений, один числовий та один спеціальний символ. Автентифікація на одному паролі може виявитись недостатньою. Опираючись на оцінку вразливості, можливі поєднання автентифікації на основі паролю з іншим процесом автентифікації та авторизації, таким як сертифікати, полегшений протокол доступу до мережних каталогів (*LDAP*), служба віддаленої автентифікації користувачів по комутованих лініях (*RADIUS*), *Kerberos* та інфраструктура відкритого ключа (*PKI*). Системи автентифікації можуть бути на категорії в залежності від кількості необхідних факторів ідентифікації.

Однофакторна автентифікація (*Single factor*) відноситься до системи, яка використовує один фактор, наприклад, поєднання ідентифікатора користувача та пароля. Метою цієї технології є використання комбінації ідентифікатора користувача та пароля для перевірки ідентифікатора.

Двофакторна автентифікація (*Two factor*) описує процес, в якому необхідно два компоненти, для досягнення своєї мети – для того, щоб надати доступ до системи, такі як володіння фізичним маркером, плюс знання секрету: наприклад, паролю.

Трифакторна автентифікація (*Three factor*) для досягнення своєї мети додає ще один фактор ідентифікації, такий як біометричний план або виміряну характеристику тіла людини. Використання значної кількості факторів автентифікації приводить до більш гарантованої автентифікації, але й додає складність, вартість і витрати на менеджмент. Відшукання оптимального співвідношення вигод і втрат між простотою та безпечністю є основною задачею в будь-якій системі автентифікації.

Однофакторна автентифікація на основі ідентифікатора користувача та пароля на сьогодні є самою розповсюдженою застосованою системою автентифікації. Системи автентифікації на основі пароля прості, легкі в управлінні та добре знайомі користувачам. При використанні сильних паролів однофакторні системи автентифікації можуть забезпечити високий рівень безпеки. Але в діючих систем паролів є деякі проблеми, тому що сильні паролі зі складною структурою важкі для запам'ятовування користувачами. Ці недоліки можна звести до мінімуму наданням оптимального рішення за допомогою системи «єдиного сильного пароля».

Смарт-картки (*Smart tokens*).У багатьох системах автентифікації як другий фактор додаються маркери, такі як смарт-картки. Маркери надають додаткову гарантію автентифікації. Користувач повинен підтвердити фізичне володіння таким маркером, для того щоб підтвердити свою справжність. Атакуючому також потрібне володіння маркером користувача для того, щоб отримати доступ до системи. Але більш високий рівень автентифікації супроводжується подорожчанням системи через необхідність маркерів і пристроїв, що зчитують маркери. До того ж маркери легко губляться, а це означає високі адміністративно-господарські витрати на повторний випуск маркерів.

Сильна автентифікація, заснована на шифруванні, може бути представлена при використанні цифрових сертифікатів, які випускаються для користувачів і зберігаються на маркерах або в пам'яті комп'ютера користувача. Для гарантії того, що конкретний сертифікат випущено для конкретного користувача законним чином. Використовуються криптографічні алгоритми. Для гарантій випуску та супроводження цифрових сертифікатів використовується інфраструктура відкритого ключа. Системи на основі сильного шифрування надають дуже сильну автентифікацію, але такі системи дуже дорогі та, як наслідок, необхідні додаткові витрати на менеджмент. Такі системи знаходять місце лише в середовищах із дуже сильною охороною.

Авторизація (говорять, також, санкціонування). Після однократної автентифікації, механізми авторизації контролюють доступ користувача до відповідних ресурсів системи. Авторизація може бути поділена на категорії в залежності від глибини деталізації контролю, тобто, у залежності від того, наскільки детально проведено розподіл між ресурсами системи. При дрібно модульній авторизації контролюється доступ до індивідуальних застосувань та послуг. Авторизація як категорія включає у себе дві технології: технологія на рольовій основі та технологія на основі правил.

*Авторизація **«на рольовій основі»*** (*Role based*) має метою реалізацію механізмів авторизації, які управляють доступом користувача до відповідних

ресурсів системи, заснованій на присвоєній ролі. Доступ до ресурсів системи заснованій на ролі, що призначена для особи в організації. Для ролі системного адміністратора може надаватися доступ високого рівня до всіх ресурсів системи. Ролі звичайного користувача буде дозволено доступ лише до підмножини цих ресурсів. Для ролі адміністратора трудових ресурсів може надаватися необмежений доступ до надто таємних баз даних трудових ресурсів. Для ролі облікової діяльності може надаватися необмежений доступ до баз даних систем бухгалтерського обліку

Авторизація ***«на основі правил»*** (*Rule based*) має метою реалізацію механізмів авторизації, які управляють доступом користувача до відповідних ресурсів системи, заснованій на конкретних правилах, пов'язаних із кожним користувачем, незалежно від його ролі в організації. Наприклад, правила можуть установлюватись лише для доступу до зчитування або доступу до зчитування/запису всіх або деяких файлів у середині системи.

Протоколи автентифікації та авторизації. Декілька протоколів були адаптовані для служб автентифікації. Протокол *RADIUS* (служба віддаленої автентифікації користувачів комутованими лініями) широко використовується для централізації служб автентифікації паролів. Спочатку задуманий для автентифікації віддалених користувачів, що застосовують наборні пристрої, протокол *RADIUS* було адаптовано для служб автентифікації звичайних користувачів.

Полегшений протокол доступу до мережних каталогів (*LDAP*) знаходить широке застосування в системах автентифікації та авторизації. Протокол *LDAP* надає зручний метод для зберігання автентифікації користувача та мандатів авторизації. Часто сервери автентифікації *RADIUS* застосовуються в парі для зберігання мандатів у каталогах *LDAP*, для надання централізованої системи автентифікації та авторизації. Коли користувач робить спробу отримати доступ до якогось конкретного застосування в такій системі, застосування генерує запит щодо мандату автентифікації в цього користувача та вони відправляються до централізованої системи. У сервері *RADIUS* буде проведена перевірка представлених мандатів на предмет їх збігу з мандатами, що зберігаються в базі даних *LDAP*, а буде зроблено запит до бази даних *LDAP* щодо інформації про правила авторизації. Результати автентифікації повертаються до застосування з інформацією щодо правил авторизації для конкретного користувача. Правила авторизації будуть потім виконані в застосуванні для того, щоб надати користувачеві доступ до конкретних даних чи послуг. З точки зору користувача, ці системи автентифікації та авторизації є автоматичними та простими у використанні.

5.3.3 *Технології антивірусів і цілісності системи*

Черви, зловмисні коди, віруси та троянські коні можуть змінити систему й її дані. Таким чином, важливе значення набуває використання технологій, які проводять сканування на наявність вірусів і гарантують збереження цілісності системи. Черви – це програми, які відтворюється за допомогою тиражування

самих себе з однієї системи в іншу без втручання людини. Віруси можуть прикріплятися до файлів користувача та відроджуватися до життя, тиражуючи себе в інші файли, якщо нічого не підозрюючий користувач зробить якісь події, такі як відкриття інфікованого файла. «Троянський кінь», в якому вкладено шкідливий код, поводиться інакше, представляючи себе звичайно нічого не підозрюючому користувачу, як корисна програма,

Антивірусні технології допомагають захистити системи від атак червів, зловмисних кодів і «троянських коней». Це програмне забезпечення може бути встановлено в пристрої користувача або надано, як послуга, мережею або провайдером Інтернет послуг. Технології цілісності систем використовують програмне забезпечення, яке перевіряє той факт, що лише санкціоновані оновлення застосовуються до важливих файлів системи

У антивірусному програмному продукті можуть бути використані методи сигнатур кодів для ідентифікації вірусів і зловмисних кодів і метод перевірки поведінки виконуваних програм.

Технологія «***метод сигнатур***» (*Signature methods*) призначена для захисту від зловмисного комп'ютерного коду, такого як віруси, черви, троянські коні, використовуючи їх сигнатури. Для цієї технології потрібне попереднє знання зловмисного коду, до того, як антивірусна програма зможе його розпізнати. По суті, для ефективного захисту потрібні поточні значення їх сигнатур у базі даних.

Технологія захисту ***методом*** перевірки ***поведінки*** (*Behavior methods*) має своєю метою перевірку поточних програм на несанкціоновану поведінку. Перевірка подій за допомогою сканерів на наявність дозволених дій здійснюється за допомогою поточного коду. Програмне забезпечення повідомляє користувача про підозрілі події. Активні сканери не завжди успішно діють проти вірусів, але можуть бути ефективнішими проти червів і троянських коней. Статичні евристичні сканери сканують код для того, щоб спробувати ідентифікувати події, які можуть бути пов'язані з поведінкою, що нагадує поведінку вірусів.

Технологія «***виявлення вторгнень»*** (*Intrusion detection*) має своєю метою застереження системних адміністраторів щодо можливості подій, які пов'язані з безпекою, таких як дискредитація файлів на сервері. Методи забезпечення цілісності системи використовують програмне забезпечення, яке веде поточний нагляд за змінами, які проводяться відносно важливих файлів системи. Ці методи можуть бути використані адміністраторами для виконання перевірок системи й визначення того факту, чи вдалося хакерам проникнути у систему, при цьому завжди необхідно врахувати, що в хакерів є схильність залишати таємні пастки.

6.3.4 *Технології аудиту та моніторингу*

Методи (техніки) аудиту та моніторингу дають можливість адміністраторам мереж оцінити безпеку системи в цілому, включаючи інструкції по виявленню та програмне забезпечення для запобігання вторгненням. Адміністратори

мережі можуть використати цей метод для виконання аналізу системи з метою виявлення її слабких місць після атаки. у деяких випадках аналіз системи може бути виконаний під час активної атаки на систему.

Техніки аудиту та моніторингу за їх функціями поділяють на категорії: виявлення, запобігання та реєстрації. За метою кожній з категорій відповідають технології аудиту та моніторингу: виявлення вторгнень, попередження вторгнень, інструменти реєстрації.

Технологія ***виявлення вторгнень*** (*Intrusion detection*) має своєю метою порівняння потоків мережі та елементів реєстрації для підбирання даних щодо сигнатур, які вказують на хакерів.

Технологія ***запобігання вторгнень*** (*Intrusion prevention*) має своєю метою виявлення атак на мережу та проведення заходів, передбачених політикою безпеки підприємства, для пом'якшення наслідків цих атак. Підозрілі події запускають сигнали тривоги адміністратора й інші передбачені реагування.

Технологія ***інструментів реєстрації*** (*Logging tools*) має своєю метою ведення поточного спостереження та порівняння потоків мережі та елементів реєстрації на вузлі для підбирання даних щодо сигнатур і профілів адрес на вузлі, які вказують на хакерів.

Система виявлення вторгнень (IDS) може бути використана для поточного нагляду за мережею для гарантій того, що жоден несанкціонований користувач не має доступу до мережі. У більшості застосувань IDS порівнюється мережний потік з реєстраційними записами хоста для того, щоб порівняти сигнатури даних і профілі адрес хоста, що вказують на хакерів. Система виявлення вторгнень ідентифікує моделі потоку, які вказують на присутність несанкціонованих користувачів. Підозрілі події запускають сигнали тривоги адміністратора й інші передбачені реагування. Система виявлення вторгнень (IDS) може бути в загальних рисах поділена на категорії, відповідно до наступних критеріїв:

– часові рамки виявлення інциденту: У реальному часі або в режимі відключеної лінії, залежно від того, чи проводиться аналіз облікових записів системи та мережного потоку в момент часу, коли ця подія відбувається, або в пакетному режимі протягом неробочого часу;

– місце встановлення: у мережі або в хості (мереже-базовані та хост-базовані). у мереже-базованих *IDS*, як правило, включена множина пристроїв поточного контролю (часто заздалегідь конфігурованих застосувань), які встановлюються в пунктах фільтрації в мережі (де можна спостерігати весь потік між двома пунктами). Для *IDS*, що встановлено в хості, необхідно, щоб програмне забезпечення було встановлене безпосередньо на сервери, що захищаються. З його допомогою ведеться поточний нагляд за мережними комунікаціями та за діяльністю користувача на цих серверах;

– тип реакції на інцидент: або *IDS* втручається активним чином для запобігання атакам (наприклад, за допомогою зміни правил для брандмауера або для фільтрів маршрутизатора) або просто повідомляє персонал, або інші мережні системи щодо проблеми, яка виникла.

Більшість комерційних продуктів *IDS* надає поєднання можливостей моніторингу: мереже-базованих та хост-базованих, в яких хост центрального менеджменту отримує повідомлення від різних пристроїв спостереження та подає сигнал тривоги для персоналу підтримки мережі. Використання програм мереже-базованих *IDS* рекомендується для більшості мережних установок, залежно від конкретних потреб споживачів.

5.3.5 *Технології менеджменту*

Техніки менеджменту поділяють на категорії: мережний менеджменту та політика безпеки. Категорії мережного менеджменту об'єднують у собі технології менеджменту конфігурації та менеджменту внесення змін у систему. Категорії політики безпеки відповідає технологія примушування, яка її забезпечує.

Технологія ***менеджменту конфігурації*** (*Configuration management*) має своєю метою взяття до уваги контроль та конфігурацію мереж і менеджмент аварій та інцидентів.

Технологія ***менеджменту внесення змін (патчів)*** (*Patch management*) має своєю метою встановлення самих останніх оновлень, налаштування до пристроїв мережі.

Технологія ***примушування*** (*Enforcement*) має своєю метою дати можливість адміністраторам вести моніторинг і примусово проводити політику безпеки.

Методи моніторингу конфігурації дають можливість адміністраторам мережі встановлювати та перевіряти настановні параметри безпеки на пристроях у своїх мережах. Менеджмент політики дозволяє адміністраторам мереж визначати безпеку менеджменту бізнесу та політику якості обслуговування *QoS*, здійснювати їх у організації безумовне розуміння всіх правил, що відносяться до конкретних пристроїв, і настановних параметрів, які необхідні для здійснення необхідних політик. Технічно, політики є набором правил для адміністрування, менеджменту та управління доступом до ресурсів мережі. Вони повинні бути виведені з конкретних політик, визначених організацією або корпорацією. У просторі безпеки менеджмент політики призначено для вирішення заплутаних проблем і труднощів процесу навчання, пов'язаних із цими методами (наприклад, брандмауерами, IDS, таблицями доступу та фільтрами доступу, методами автентифікації), і відсутністю системного нагляду за різними частинами мережі (центр обробки даних, віддалений офіс, комплекс офісних будівель).

У той час, як існують численні вирішення частини проблем, остаточна система менеджменту політики надає централізовану мережну конфігурацію, що гарантує злагоджену установку параметрів безпеки в численних вузлах, що знижує ризик уразливості мережі. Це не означає, що існує лише одна система політики. У мережі більшого розміру з численними адміністративними доменами, може виникнути необхідність у множині систем політики, кожна з яких відповідає за управління підмножиною пристроїв і узгодженість між доменами.

Еталонна модель менеджменту політики. На рис. 5.3 зображена архітектурна структура менеджменту політики безпеки мережі. Ця еталонна модель використовується як зразок для менеджменту політики, як безпеки, так і менеджменту *QoS*. Таким чином, якщо менеджмент політики, засновано на цій моделі, буде реалізовано в мережі та на всіх рівнях даної архітектури, то він буде доступний для всіх типів користувачів і застосувань, включаючи фахівців обслуговування мережі, технічних партнерів і навіть споживачів.

До компонентів даної моделі належать:

1. *Пункт примусового застосування політики* (*PEP*). Пристрій мережі або системи безпеки, який приймає політику (правила конфігурації) з пункту вибору політики та примусово застосовує її відносно мережного потоку, що проходить через цей пристрій. Це примушення вигідно використовує мережні та допоміжні для мережі механізми безпеки належним чином.

2. *Пункт вибору політики* (*PDP*). Пункти *PDP* або сервери політики видають абстрактні мережні стратегії в повідомленнях управління конкретними пристроями, які потім слідують до пунктів проведення політики. Ці сервери політики часто є автономними системами, які управляють усіма комутаторами та маршрутизаторами всередині конкретного адміністративного домена; вони сполучаються з цими пристроями, використовуючи протокол управління (наприклад, *COPS*, набір команд *SNMP*, протокол *Telnet* або, що відноситься до конкретного пристрою, інтерфейс командного рядка *CLI*).

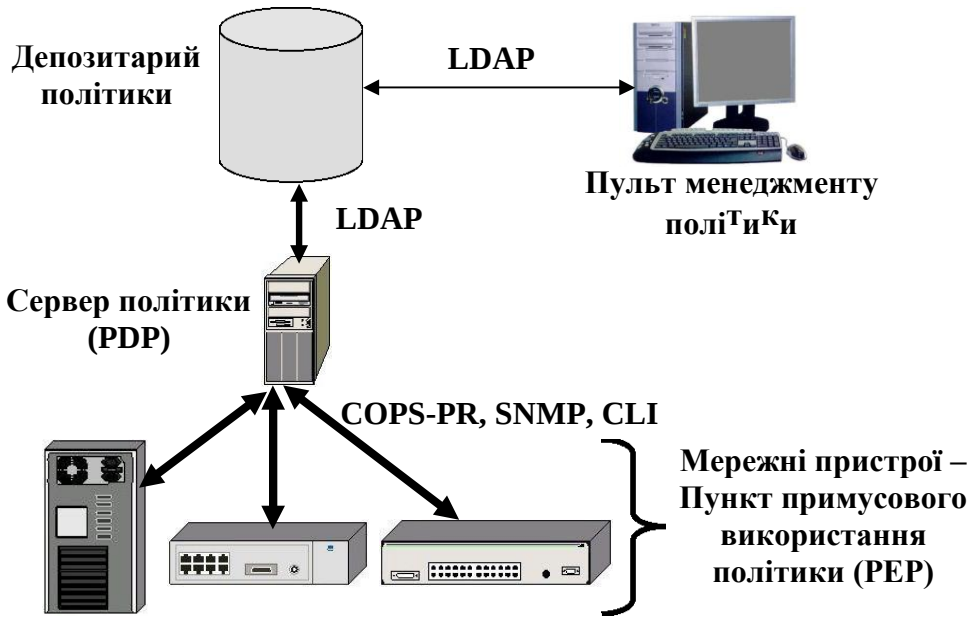


Рисунок 5.3 – Еталонна модель менеджменту політики безпеки

5.4 Базові принципи системи кібербезпеки мереж наступних поколінь

При створенні системи інформаційної безпеки в мережі *NGN* і надання послуг наступного покоління операторам телекомунікацій слід реалізувати наступні базові принципи:

– захищати власну інфраструктуру оператора телекомунікацій: загрози можуть приходити звідусіль – від абонентів, інсайдерів, взаємозв'язаних операторів або будь-яких інших віддалених джерел, які мають доступ до мережі *NGN*;

– гарантувати, що оператор телекомунікацій не є джерелом виникнення «зламів» і «слабких місць» у системі безпеки для взаємозв'язаних доменів – інших операторів і провайдерів послуг;

– надавати абонентам безпечні послуги, оскільки користувачі чекають таку ж якість обслуговування для голосових або мультимедійних послуг на основі *NGN*, яку вони мали в телефонній мережі загального користування;

– оскільки створення системи безпеки в цілому засновано на захищеності окремих мережних елементів, необхідно використати для побудови мережі продукти й обладнання, які мають інтегровані функції захисту, що дозволяє забезпечувати базовий рівень безпеки мережі;

– не слід вважати, що прикінцеве абонентне обладнання завжди працює в «дружньому» режимі;

– зовнішні границі (з публічним Інтернетом, операторами пірінгових мереж *NGN*, сторонніми провайдерами застосувань) слід захищати за допомогою посилених механізмів фільтрації, міжмережевих екранів;

– системи управління ключами та сервери управління, будучи особливо сприйнятливими системами, також повинні бути захищені за допомогою міжмережевих екранів;

– управляючий трафік між станціями управління та мережними елементами повинен бути захищений, хоча б за допомогою механізмів автентифікації/цілісності;

– базові механізми безпеки повинні бути застосовані для кожного мережного елементу (особливо в площинах контролю й управління);

– інфраструктура мережі повинна бути сегментована так, щоб сервери, доступні для трафіка кінцевих користувачів, були повністю відокремлені від особливо сприйнятливих серверів, які, у свою чергу, ізольовані від систем експлуатаційної підтримки операторів;

– успіх реалізації системи інформаційної безпеки полягає в постійному моніторингу мережної безпеки, який дозволяє бути в курсі еволюціонуючих загроз і постійно удосконалювати технології боротьби з ними.

Питання для самоконтролю

1. Поясніть політику кібербезпеки інформації.
2. Опишіть модель порушника кібербезпеки.
3. Дайте перелік основних задач системи кібербезпеки.
4. Які загальні задачі забезпечення кібербезпеки для менеджменту *NGN*?
5. Задачі кібербезпеки, що охоплюють домени декількох провайдерів мережних послуг?
6. Які задачі характерні складовим кібербезпеки? Дайте перелік складових.
7. Поясніть модель класифікації технологій кібербезпеки.
8. Яку логіку забезпечення безпеки доцільно доповнити технологіями кібербезпеки?
9. Як дати визначення технології, категорії та техніки кібербезпеки?
10. Дайте перелік технологій, категорій і технік кібербезпеки.

11. Опишіть технології криптографії, контролю доступу, антивірусів і цілісності системи, аудиту й моніторингу, менеджменту.

18. Які плануються технології реалізації вимог до мереж майбутнього?

19. Дайте пояснення еталонній моделі менеджменту політики кібербезпеки.

20. Поясніть базові принципи системи кібербезпеки *NGN*.

Семінарське заняття № 6
СПЕЦІАЛЬНІ ВИМОГИ ДО КІБЕРБЕЗПЕКИ ЕЛЕМЕНТІВ ТЕЛЕКОМУНІКАЦІЙ

6.1 Спеціальні вимоги до кібербезпеки елементів телекомунікацій

У даному розділі визначаються спеціальні вимоги безпеки для кожного елемента мережі в межах архітектури *NGN*. Оскільки багато зі складових безпеки будуть однаковими для різних типів елементів мережі, то спочатку визначаються типові вимоги безпеки.

6.1.1 *Типові вимоги до безпеки елементів телекомунікаційної мережі*

Дані вимоги застосовуються до елементів мережі *NGN* у довіреній зоні та в довіреній, але вразливій області. Бажано, щоб даним вимогам відповідали також пристрої в недовіреній зоні.

До загальних вимог безпеки відносяться:

– взаємодія повинна підтримуватись різними елементами *NGN*, зокрема, між різними механізмами безпеки *NGN*. Мінімальні стандартизовані можливості безпеки повинні бути доступними всім у ТМЗК;

– необхідно, щоб автентифікація й авторизація (користувач – мережа, мережа – користувач, мережа – мережа) були застосовані на транспортному рівні та рівні послуг. Автентифікація повинна бути можливою також при трансляції мережних адрес і портів;

– елемент мережі *NGN* повинен застосовувати заходи безпеки проти несанкціонованого доступу до мережних ресурсів, пристроїв, послуг і даних абонента (профілю), наприклад, шляхом блокування неавторизованого трафіка;

– мережна інфраструктура *NGN* повинна дозволяти провайдерам забезпечувати видимість топології та ресурсів мережі лише авторизованим об’єктам;

– необхідно, щоб інфраструктура *NGN* підтримувала множинні зони безпеки. З метою забезпечення безпеки може знадобитись ізоляція між різними зонами безпеки;

– необхідно, щоб інфраструктура *NGN* гарантувала конфіденційність і цілісність потоків сигналізації/контролю та потоків менеджменту, що передаються через неї;

– інфраструктура *NGN* повинна гарантувати конфіденційність, цілісність потоків інформації, що передаються нею;

– *NGN* повинна точно гарантувати безпеку елементів мережі, пов’язаних із ресурсами менеджменту (*OSS*, бази даних тощо) та ресурсів послуг;

– вимоги до безпеки для безпечного управління системою менеджменту телекомунікацій викладено у спеціальному навчальному посібнику;

– необхідно, щоб функціональні можливості системи безпеки були застосовані для пригранічних елементів мережі (*NBE* або *TE-BE*, тобто для елементів *NE* у довіреній, але вразливій зоні). Вони включають у себе такі

функції, як контроль доступу до пакетів даних та інформації сигналізації в відповідності з певними правилами, наприклад, відмова передавати трафік від певних застосувань або користувачів;

– чутливі елементи *NGN*, особливо пригранічні елементи мережі, можуть здійснювати логічний та/або фізичний розподіл потоків управління та/або менеджменту від інформаційних потоків, використовуючи логічно різні інтерфейси або різні адресні плани та за допомогою фізично різних реальних або віртуальних транспортних мереж (наприклад, віртуальні мережі *VPN* і *VLAN*);

– необхідно, щоб *NGN* забезпечувала безпечне зберігання даних щодо безпеки, наприклад, щодо ідентичності та повноважень. Необхідно, щоб таке зберігання здійснювалось окремо від спільного сховища даних, яке містить інформацію, що відноситься до послуг для абонентів;

– необхідно, щоб у *NGN* забезпечувалась політика безпеки, що включає набір правил, які визначають, який трафік повинен бути захищений на основі, наприклад, контрактів, який вид захисту використовується, як часто змінюються ключі сеансів зв'язку та правила, що визначають відповідність безпеки пристрою;

– необхідно, щоб *NGN* підтримувала можливість моніторингу мережного трафіка та визначала базові дані того, що повинно вважатись звичайними подіями в мережі;

– необхідно, щоб *NGN* мала можливість виявляти випадки аномальних подій мережі, повідомляти про них і протистояти їм.

6.1.2 *Політика безпеки інформаційних ресурсів*

Поняття політики безпеки було надане у розд. 6.1. Повторимо, що під *політикою безпеки інформації* розуміють набір правил, обмежень, рекомендацій тощо, визначених органом безпеки, який регулює використання та надавання послуг і функцій безпеки, порядок обробки інформації, що спрямована на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо організації, мережі, домена, ОС, послуги, що реалізується системою, набору функцій тощо. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими стають правила.

Політика безпеки інформації в ТМЗК є частиною загальної політики безпеки організації та має успадкувати, зокрема, положення державної політики в галузі захисту інформації. Для кожної *NGN* політика безпеки інформації може бути індивідуальною та може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища та від багатьох інших факторів. Тим більше, одна й та ж сама *NGN* може реалізувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій *NGN* буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси *NGN*, що потребують захисту, зокрема встановлювати категорії інформації, оброблюваної в *NGN*. Мають бути

сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Політика безпеки інформації, що реалізуються різними *NGN* будуть відрізнятися не тільки тим, що реалізовані в них функції захисту можуть забезпечувати захист від різних типів загроз, але і в зв'язку з тим, що ресурси *NGN* можуть істотно відрізнятись.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступу.

Провайдери *NGN* повинні підготувати відповідну (придатну) політику безпеки та повинні нести відповідальність за її застосування до всіх елементів *NE* та пристроїв, що знаходяться під їх контролем.

6.1.3 *Закріплення та позбавлення прав на обслуговування*

Всі елементи мережі *NGN* повинні мати здатність до конфігурування для мінімальних послуг, необхідних для підтримки інфраструктури *NGN* провайдера *NGN*. В усіх системах та елементах мережі необхідно відключити будь-який порт рівня послуг або транспорту, які не потрібні для правильної роботи елементів *NGN*.

Крім того, необхідно, щоб застосування працювали з мінімальними привілеями, наприклад, на платформах «*UNIX*/*Linux*» застосування не повинні запускатись як кореневі, якщо їм не потрібні кореневі привілеї. Необхідно, щоб операційна система, що підтримує будь-який елемент *NGN*, могла бути зконфігурована спеціальним чином для забезпечення безпеки та відповідно закріплена. Недопустимі ніякі «чорні ходи» (доступ до програмного забезпечення, яке може обійти звичайні механізми контролю доступу) до будь-якого елемента *NGN*.

Додатково до закріплення повинні бути застосовані фізичні та логічні схеми контролю доступом, які реалізують найліпші практичні методи в телекомунікаційній індустрії.

6.1.4 *Журнал виявлення, реєстрації й обліку подій*

Всі елементи *NGN* повинні мати можливість створення та ведення журналу реєстрації подій, який містить реєстр подій, що пов'язані з безпекою, у відповідності до політики безпеки провайдера *NGN*. Необхідні механізми для запобігання несанкціонованого змінення журналу, які не моги б бути виявлені.

Повинна існувати можливість менеджменту журналами реєстрації подій, а також можливість переміщення старих даних із журналу реєстрації подій на інші носії інформації, наприклад, на змінні носії для довготривалого зберігання. Даний інтерфейс повинен дозволяти авторизованим адміністраторам переміщати старі дані з журналу реєстрації подій на змінні носії (і навпаки з носіїв для порівняльного аналізу).

Необхідно, щоб дана можливість вимагала спеціальної авторизації для менеджменту та була захищена за допомогою певної авторизації для менеджменту журналом реєстрації подій.

Аудит безпеки. Повинна забезпечуватись можливість аналізу зареєстрованих даних щодо подій, які відносяться до забезпечення безпеки, для контролю їх на наявність порушень політики безпеки. Перевірка повинна являти собою незалежний аналіз і вивчення записів і дій системи для тестування адекватності засобів управління системою, для забезпечення відповідності прийнятої політики безпеки робочим процедурам і для виявлення порушень безпеки.

У результаті перевірки виявляються зміни в управлінні, менеджменті, політиках і процедурах.

У табл. 6.1 наведено взаємозв'язок між основними стандартними вимогами до безпеки та послугами безпеки.

Таблиця 6.1 – Відповідність між вимогами до безпеки та послугами безпеки

Функціональні вимоги до безпеки	Послуги безпеки
Перевірка ідентичності	Автентифікація користувача Автентифікація рівноправного об'єкта Автентифікація джерела даних
Управляний доступ та авторизація	Контроль доступу
Захист конфіденційності запам'ятованих даних	Контроль доступу, конфіденційність
Захист конфіденційності переданиих даних	Конфіденційність
Захист цілісності запам'ятованих даних	Контроль доступу
Захист переданих даних	Цілісність
Підзвітність	Невідмовність від участі
Реєстрація подій	Дані журналу реєстрації
Звіти щодо сигналів порушення безпеки	Сигнали порушення безпеки
Аудит безпеки	Дані журналу реєстрації
Захист DCN	Перевірка пакетів

Реєстрація подій безпеки. Важливо забезпечити кожен мережний елемент (ME) адекватними можливостями, що дозволяють виконувати дії з дослідження, перевірки, визначення реального часу, аналізу та захисту з тим, щоб могли бути розпочаті належні коригуючі дії.

Дії щодо вивчення, аналізу суперечливих ситуацій можуть включати у себе повідомлення *OAM&P*, а також інформацію, що занесена до реєстраційних записів журналу реєстрації. Реєстрація непов'язаних з безпекою повідомлень *OAM&P*, що називають *повідомленнями* «*щодо останніх змін*», необхідна за будь-яких доступних для перевірки подій. Мають виконуватись такі рекомендації:

– мережний елемент має бути здатним реєструвати будь-яку подію, яка змінює атрибути та послуги безпеки, налаштування безпеки, параметри конфігурації пристроїв;

– мережний елемент повинен забезпечувати здатність конфігурувати ті невідкладні дії з адміністративного забезпечення безпеки, які будуть включені до реєстраційних записів безпеки;

– мережний елемент має бути здатним реєструвати кожну спробу та її результат; кожну відміну реєстрації або завершення сеансу та кожну спробу реєстрації та її результат, які викликають активізацію системного таймера неактивності. Рекомендується відправляти реєстраційні записи на постійний сервер перевірки після виконання мережним елементом присвоєння послідовної позначки та криптографічної автентифікації (цифрового підпису);

– мережний елемент повинен мати здатність дистанційної реєстрації захищеним маршрутом;

– кожен реєстраційний запис має містити таку інформацію:

– опис події, що реєструється;

– рівень ідентичності та безпеки користувача або процесу, який ініціював дану подію;

– дата та час події, що сталася;

– мережне джерело й інформація щодо пункту призначення, якщо вона застосована (наприклад, коли виконується входження до системи);

– індикація успіху чи невдачі дії.

Звіти щодо аварійних сигналів безпеки. Має бути складено перелік подій, для яких необхідно складати звіт щодо аварійних сигналів безпеки. Повинні бути виконані такі вимоги:

– всі мережні елементи повинні забезпечувати можливість генерування повідомлення щодо аварійних сигналів для обраних подій;

– всі мережні елементи повинні забезпечувати можливість, яка дозволяє користувачеві визначати критерій вибору для подій, що генерують повідомлення щодо аварійних сигналів.

Нанесення позначок (міток) часу та датчик часу (система синхронізації).

Необхідно, щоб елементи *NGN* підтримували використання довірених датчиків часу (мережі синхронізації) для системного часу й запису в журналі реєстрації. Довірене джерело часу в даному випадку означає джерело часу, який може бути перевірений на предмет стійкості до несанкціонованого змінення. Перехідна довіра також можлива – тобто джерело часу, яке покладається на довірене джерело часу, саме є довіреним джерелом часу.

Розподіл ресурсів й обробка критичних ситуацій. Необхідно, щоб кожен елемент *NGN* мав можливість обмежувати кількість своїх важливих ресурсів, наприклад, розподіл пам’яті запитам на обслуговування. Ці обмеження можуть зменшити негативні наслідки атак «відмова в обслуговуванні». Запити на обслуговування конкурують у системі з іншими запитами на ресурси. Крім того, кожне окреме застосування *NGN* повинне мати можливість обмежувати використання у себе важливих ресурсів, виділених для виконання запитів.

Метою даної вимоги є обмеження впливу спалахів активності так, щоб вони не впливали на інші запити на обслуговування. Це також дасть/залишить застосуванню й операційній системі можливість повідомити системі

моніторингу про те, що застосування та/або його платформа можуть потерпати атаку *DoS* або *DDoS*. Необхідно, щоб елемент *NGN* забезпечував інтерфейс для спостереження за використанням ресурсів.

Елемент *NGN* повинен безумовно відхиляти будь-які пакети, які не відповідають очікуваному протоколу чи формату, та, засновуючись на політиці безпеки, повинен мати можливість створювати в журналі запис для кожної подібної події. «Безумовне відхилення» означає перехоплення та реєстрацію прийнятого пакета, а також відкидання прийнятого пакета, без повідомлення про відкидання, наприклад, без передачі про помилку.

Мета полягає в тому, щоб обмежити можливі атаки з боку шкодоносних або неправильних пакетів. Але, якщо використання дій реєстрації таке велике, що воно пересікається з іншими діями елемента, очевидним рішенням буде припинення реєстрації до того часу, поки використання ресурсів не повернеться на прийнятний рівень.

Моніторинг і цілісність коду та системи. Елемент мережі повинен мати засновані на політиці безпеки можливості моніторингу 1) своєї конфігурації та програмного забезпечення та 2) будь - яких змін для виявлення несанкціонованих змін. Будь-які несанкціоновані зміни повинні приводити до створення запису в журналі реєстрації та генерування сигналу тривоги. Елемент повинен періодично сканувати свої ресурси та програмне забезпечення на предмет шкодоносних програм, наприклад, вірусу. Елемент повинен генерувати сигнал тривоги, якщо в процесі сканування виявляється шкодоносні програми.

Необхідно, щоб управління моніторингом відбувалось таким чином, щоб воно не впливало на передачу в реальному часі. Така передача чутлива до затримок зв’язку або з’єднання може бути розірвано без необхідності.

Цілісність. Для гарантування надійності функцій у реальному середовищі, необхідно, щоб апаратне та програмне середовище реалізованих функцій безпеки підтримували потрібний рівень безпеки. Це включає у себе правильну конфігурацію операційних систем і виключення системних дефектів.

1. Поясніть політику кібербезпеки інформації.
2. Опишіть модель порушника кібербезпеки.
3. Дайте характеристику типовим вимогам телекомунікаційної мережі.
4. Дайте характеристику вимогам до безпеки «довіреній» зоні.
5. Дайте характеристику вимогам до безпеки «довіреній», але вразливій зоні.
6. Дайте характеристику вимогам до безпеки «недовіреній» зоні.

Семінарське заняття №7
КІБЕРБЕЗПЕКА МЕРЕЖ НАСТУПНИХ ПОКОЛІНЬ У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

7.1 Природа надзвичайних ситуацій

Телекомунікаційним службам у надзвичайних ситуаціях приділяється значна увага в національному законодавстві та рекомендаціях міжнародних організацій [35,…, 38]. Лихо часто приходить раптово та призводить до колосальних пошкоджень, втрат і руйнувань. Вони можуть мати величезну руйнівну силу (енергію), можуть тривати дуже довго й охоплювати суттєві географічні території. Від лиха не застрахований ніхто. Кожне лихо приносить горе, фінансові втрати та соціальні наслідки.

Джерела надзвичайних ситуацій. Лихо є результатом дії природних сил або виникає внаслідок дії чи втручання людини. Джерелом стихійних лих можуть бути:

– *урагани*, *тайфуни* (циклони) охоплюють великі географічні простори і є найбільш руйнівними несприятливими погодними умовами на землі;

– *сильні повені*, *сильні грози*, *бурі*, *торнадо* є результатом штормів, ураганів різної сили та викликають широкомасштабні та важковідновлювані пошкодження. Кліматичні явища можуть бути передбаченими короткостроковими прогнозами погоди, що дає шанс на врятування людей, але руйнування будівель і землі неминучі;

– *засуха, лісові пожежі, сильна жара, холоднеча, сніг, лід* також приводять до значних втрат;

– *грязеві зсуви* та *снігові лавини* можуть бути результатом сильних опадів чи землетрусів;

– *землетруси, виверження вулканів* не можна поки що передбачити і вони приносять значні руйнування та людські втрати, особливо в густо населених районах світу. Як правило, одні стихійні лиха тягнуть за собою інші додаткові природні явища;

– *цунамі*, *сейсмічні хвилі*, можуть виникати внаслідок землетрусів і приносити додаткові руйнування;

– *епідемії, голод* можуть супроводжувати стихійні лиха.

Зі стихійними природними лихами конкурують антропогенні лиха – надзвичайні події, причиною яких є дії людей. До антропогенних катастроф відносяться: вибухи, руйнування промислових або житлових будівель; підпал, пожежі; ядерні вибухи, радіація, прориви трубопроводів; витоки газу, розливи хімічних речовин; аварії літаків/вимушені посадки, зіткнення поїздів/сход-ження з рейок на транспорті та в метро; тероризм, паніка/панічна втеча, отруєння, нещасні випадки на воді.

Зв’язок необхідний для ефективного проведення аварійно-рятувальних робіт і врятування життя поза залежності від типу лиха. Телекомунікаційна служба в надзвичайних ситуаціях забезпечує пріоритетне надання телекомунікаційних послуг авторизованим користувачам під час лиха та надзвичайних ситуацій. Це

дає можливість підтримки надання під час лиха та надзвичайних ситуацій пріоритетних телекомунікаційних послуг, наприклад, голос, повідомлення, відео та дані в рамках надзвичайної служби. При цьому мають виконуватись задачі та вимоги безпеки, має підтримуватись безпека при роботі з різними видами реалізації мереж загального користування. Основною задачею є забезпечення безпеки послуг, які надаються мережею, тобто безпечної та пріоритетної передачі голосу, відео, даних і повідомлень.

Невідкладні заходи у випадку надзвичайних ситуацій. Всі типи лих, будь вони стихійними чи викликані діями людей, можуть відбутися в будь-якому місці та в будь-який час. Ліквідація наслідків надзвичайних ситуацій проводиться поетапно. Головна задача рятівників, що першими з'являються на місці лиха, полягає в тому, щоб мати доступ до району руйнувань і попередження подальших руйнувань. Інші етапи швидко змінюють один одного. На другому етапі пріоритетом є лікування поранених і рятування життя. До робіт третього етапу залучаються додатковий персонал, що займається ліквідацією наслідків надзвичайних ситуацій, обладнання та матеріальні ресурси, можливо зарезервовані раніше. Четвертий етап – це розчищення та відновлення.

Ключовим засобом полегшення аварійно-рятувальних робіт на всіх етапах є використання швидкого, надійного, зручного зв'язку, який організовується прийняттям технічних рішень та/або реалізації адміністративної політики.

8.2 Цілі та функціональні вимоги до телекомунікаційних служб у надзвичайних ситуаціях

Гарантовані телекомунікації. До зв'язку в надзвичайних ситуаціях (включаючи підтримку та раннє попередження) входять:

- зв'язок від окремого суб'єкта до органу влади, наприклад, виклик екстрених служб;
- зв'язок між органами влади, наприклад, зв'язок для надання допомоги при лихах (TDR);
- зв'язок від органу влади до окремого суб'єкта, наприклад, послуги масового сповіщення.

У Рекомендаціях МСЕ ITU-T Y.1271, ITU-T E.106, ITU-T E.107 [37 – 41] представлені «Структура вимог до мереж і функцій зв'язку в надзвичайних ситуаціях у мережах, що розвиваються, з комутацією каналів і з комутацією пакетів», «Міжнародна схема пріоритетів надання допомоги в надзвичайних ситуаціях (IEPS) для дій з надання допомоги при лихах» і «Служба зв'язку в надзвичайних ситуаціях, і структура взаємодії для державної реалізації ETS» відповідно.

Метою є забезпечення гарантованого зв'язку протягом існування надзвичайних ситуацій. При виникненні лиха інфраструктура телекомунікацій може бути зруйнована. Мережі перенавантажуються. Може виникнути необхідність створення нових або розширення існуючих ліній зв'язку, щоб

досягти нових географічних районів. Попит на телекомунікаційні послуги зростає.

Призначення учасників рятувальних операцій може виконуватись задовго до виникнення реальної надзвичайної операції. Тоді можуть бути відомі паролі , які дозволяють отримати дозвіл на першочергове надання телекомунікаційних послуг. Для надання права на переважне та пріоритетне користування телекомунікаціями, її користувачі повинні мати відповідні дозволи. Бажана також авторизація, інакше користувачі, що не мають дозволу, можуть зловживати правом переважного користування телекомунікаціями.

У мережах різного типу пріоритети призначаються та реалізуються різним чином. У мережах комутації каналів реакція на перенавантаження виражається у відмові надання зв'язку. Тоді способом забезпечення екстреного зв'язку є попередження користувачів про те, що зв'язок потрібен санкціонованому учаснику рятувальних операцій. У мережах з очікуванням додаткове навантаження приводить до погіршення якості роботи всієї мережі, бо інформація з однаковим пріоритетом просто вишукується в чергу до тих пір, поки є доступні ресурси мережі.

Для забезпечення гарантованих можливостей застосовують надання режиму переважного доступу до засобів телекомунікацій і створення відмово-стійких мереж. Таким, наприклад, є мережі передачі пакетів (з пакетною комутацією). В усякому разі, оператори мереж повинні мати плани відновлення для ремонту мереж у випадку несправності.

Вимоги та функції забезпечення зв'язку в надзвичайних ситуаціях. Повномасштабний зв'язок у надзвичайних ситуаціях повинен забезпечувати виконання різноманітних експлуатаційних вимог до засобів аварійно-рятувальних робіт. Реалізація цих вимог суттєво спрощує ефективне та своєчасне виконання відновлювальних операцій під час лиха. Наведемо перелік конкретних цілей, функціональних вимог і можливостей, які здатні спростити забезпечення зв'язку для робіт з ліквідації наслідків надзвичайних ситуацій:

– реалізація пріоритету та вдосконалений пріоритетний режим. Для передачі трафіка зв'язку в надзвичайних ситуаціях потрібні гарантовані можливості передачі незалежно від того, якими мережами він передається (обов'язково);

– захищені мережі. Мережі повинні мати захист від спотворення (фальсифікації) трафіка або сигналів управління, а також від несанкціонованого доступу до них, включаючи необхідні методи шифрування й автентифікації користувача (реалізується обов'язково);

– конфіденційність даних щодо місцеположення. Для обмеженої кількості керівників вищої ланки може бути потрібний особливий зв'язок у надзвичайних ситуаціях із метою керівництва й організації аварійно-рятувальних робіт без ризику розкриття відомостей щодо їх місцеположення (бажано);

– відновлюваність. Незалежно від виду руйнувань, певні засоби мережі зв'язку повинні бути такими, щоб їх можна було легко поповнити, відремонтувати або відновити до такого ступеня, щоб забезпечувався пріоритетний зв'язок необхідних рівнів (бажано);

– функція міжмережних з'єднань. Мережі, що забезпечують зв'язок у надзвичайних ситуаціях, повинні передбачати міжнародні та міжміські з'єднання скрізь, де це можливо (реалізується обов'язково);

– функція міжмережної взаємодії. Повинні забезпечувати взаємні з'єднання та міжмережеву взаємодію всіх мереж, існуючих і тих, що будуть впроваджені (реалізується обов'язково);

– мобільність. Інфраструктура зв'язку повинна підтримувати рухливість користувача та терміналу, включаючи зв'язок швидкого розгортання та рухомий зв'язок (бажано);

– повсюдне покриття. Ресурси інфраструктури зв'язку загального користування на великих географічних площах повинні утворювати основу для повсюдного проникнення екстреного зв'язку (реалізується обов'язково);

– живучість/довговічність (життєспроможність/працездатність). Засоби зв'язку повинні бути достатньо стійкими, щоб надавати зв'язок користувачам, що вижили у широкому діапазоні зовнішніх умов (реалізується обов'язково);

– передача в реальному часі: голос/текст у реальному часі та відео/зображення (якщо дозволяє смуга пропускання). Мережі з комутацією каналів та *IP*-мережі повинні забезпечити користувачам зв'язку в надзвичайних ситуаціях необхідний рівень якості передачі мови (реалізується обов'язково);

– аналогічно передача не в реальному часі: повідомлення/потоки даних (аудіо/відео) не в реальному часі (реалізується обов'язково);

– функція розширення смуги пропускання. Санкціоновані користувачі повинні мати можливість обирати параметри екстреного зв'язку для того, щоб виконувалися різні вимоги за шириною смуги пропускання (бажано);

– надійність/доступність (/експлуатаційна готовність). Зв'язок повинен функціонувати погоджено та в точній відповідності з проектними вимогами та специфікаціями, і повинна бути можливість використання з високим рівнем таємності (реалізується обов'язково).

Мета полягає в тому, щоб забезпечити високий ступінь упевненості та ймовірності того, що критично важливі комунікації (зв'язок) доступні авторизованим користувачам, наприклад, тим, хто має безпосереднє відношення до телекомунікаційної служби в надзвичайних ситуаціях.

Розглянемо ці функціональні можливості докладніше.

Реалізація пріоритету, пріоритетний режим. У цілому, пріоритетний режим є основним елементом забезпечення телекомунікацій у надзвичайних ситуаціях, який за визначенням має вважатись більш важливим, ніж звичайні телекомунікаційні послуги. Засобами надання екстреним службам пріоритетного режиму є:

– розпізнавання й авторизація користувачів телекомунікацій у надзвичайних ситуаціях;

– надання авторизованим користувачам телекомунікацій у надзвичайних ситуаціях пріоритету в обслуговуванні.

В архітектурі *NGN* визначено індикатор пріоритету, який передається функцією управління обслуговуванням (*SCF*) функції управління ресурсами та допуском (*RACF*). Індикатор пріоритету повинен бути здатним вказувати

категорії пріоритетів, що надаються користувачам, з тим щоб застосувати різні правила та встановлювати різницю між багатьма видами пріоритетних застосувань. Наприклад, координаторам служби швидкої допомоги надаються більш високий пріоритет, ніж персоналу лікарні.

У мережах комутації каналів (з встановленням з'єднання) метод забезпечення пріоритетності полягає в призначенні трафіку позначки надзвичайної ситуації, а потім стосовно цього трафіка реалізувати особливу мережну політику з метою досягнення бажаного рівня обслуговування. У мережах із встановленням з'єднання, як тільки з'єднання встановлено, виклик стає «чітко прив'язаним», потрібна якість гарантується та подальшого підтвердження переважного статусу не потрібно.

У мережах із комутацією пакетів (у мережах без встановлення з'єднання) може бути потрібним передавати в кожному пакеті позначку екстреного зв'язку, щоб давати їй пріоритетний статус.

На час аварійно-рятувальних робіт новим тимчасовим користувачам необхідно надавати, на переважній основі, лінію доступу та швидко ініціювати зв'язок.

Переважний доступ до телекомунікаційних засобів. Необхідно значно прискорити надання зв'язку в надзвичайних ситуаціях на пріоритетній чи переважній основі. Способами доступу до телекомунікаційних ресурсів для використання можливостей телекомунікацій у надзвичайних ситуаціях є: аналогова абонентна лінія, безпроводова, супутникова, кабельна, цифрова абонентна лінія (*DSL*) й оптоволокно.

Традиційна мережа комутації каналів, як правило, не передбачає позначення пріоритетних викликів. Але режим переважного доступу може бути забезпечено за допомогою помічених ліній або постійно підключених ліній.

На сьогодні нема можливості обробки пріоритетного виклику або ініціації послуги екстреного зв'язку при доступі зі звичайного телефону. Виклик приходить у режимі запиту з обмеженого числа портів. Якщо всі порти зайняті, з'єднання може бути затримане.

Переважне встановлення з'єднань, використання доступних ресурсів і завершення трафіка зв'язку в надзвичайних ситуаціях. у надзвичайних ситуаціях потрібно відрізняти звичайний трафік від трафіка надзвичайної ситуації. У традиційній мережі комутації каналів, розрізнити два типи трафіка дозволяє лише протокол сигналізації. У мережі комутації пакетів це простіше – можна провести ідентифікацію трафіка за допомогою позначок, які розміщені в елементах сигнальної посилки елемента даних (пакета). Позначки можуть розміщуватись на різних рівнях і підрівнях.

Після того, як трафік зв'язку в надзвичайних ситуаціях ідентифіковано, для його пріоритетного проходження повинні бути застосовані правила та методи політики мережі. Така політика повинна забезпечувати високу ймовірність успішної маршрутизації та доставки порівняно зі звичайним трафіком. Вкрай бажано, щоб існувало декілька запасних маршрутів або можливих запасних шляхів, які можна було б використати під час перенавантаження або несправності мережі.

Можливе попереднє видалення трафіка неекстреного зв'язку. У мережі комутації каналів метод попереднього видалення неекстреного трафіка застосовується широко. У мережі з комутацією пакетів цей метод не є обов'язковим.

Допустиме погіршення якості QoS за недоступності ресурсів інфраструктури. Якість обслуговування екстреного зв'язку визначається як найкращою для розбірливого беззавадового зв'язку та передачі важливої інформації. Але коли телекомунікаційні ресурси працюють у стресовій ситуації допустиме погіршення *QoS* може бути прийнятним. Це можливо, коли мережа не спроможна підтримувати передачу звичайного трафіка та відсутня достатня пропускна здатність і ресурс для підтримка рівня *QoS* нормально прийнятного для передачі трафіка екстреного зв'язку.

Для виконання аварійно-рятувальних робіт необхідно не втратити можливість зв'язку та продовжувати передачу важливої інформації, нехай навіть з обмеженнями. У тих випадках, коли це виправдано, коли ресурси інфраструктури практично вичерпані, може бути необхідним забезпечити пріоритет екстреного зв'язку перед звичайним. Звичайний зв'язок може погіршитись або перериватися.

Захищені мережі (див. також розд. 7.5). Забезпечення безпеки необхідне для запобігання можливості використання несанкціонованими користувачами дефіцитних телекомунікаційних ресурсів, що потрібні для забезпечення операцій з ліквідації наслідків надзвичайних ситуацій.

Прискорена автентифікація санкціонованих користувачів у надзвичайних ситуаціях. Зв'язок у надзвичайних ситуаціях призначено лише для санкціонованих користувачів, що беруть участь у аварійно-рятувальних операціях. Цих користувачів визначає відповідний компетентний орган. Бажано впровадити новітній метод потокової прискореної автентифікації користувачів, який перевіряє ідентифікаційну інформацію користувача для захисту телекомунікаційних ресурсів від інтенсивного використання та зловживання під час надзвичайних ситуацій. Після того, як автентифікація підтверджена та в мережі передається трафік екстреного зв'язку, така автентифікаційна інформація може бути асоційована з позначками, які потім повинні передаватись протягом всього часу від ініціалізації виклику до його завершення. Може виявитись необхідним продовжити передачу цієї позначки протягом усієї розмови.

Забезпечення безпеки трафіка екстреного зв'язку. Додатково до автентифікації й авторизації, для зв'язку в надзвичайних ситуаціях необхідні інші аспекти безпеки, наприклад, заходи проти зловмисного спотворення інформації, проникнення та відмови в обслуговуванні. Дуже бажано гарантувати виявлення несанкціонованої зміни інформації для екстреного (і звичайного) зв'язку. Мережі повинні мати захист від спотворення (фальсифікації) трафіка або сигналів управління, а також від несанкціонованого доступу до них, включаючи необхідні методи шифрування й автентифікації користувача.

Таємність місцеположення. Для деяких типів зв'язку в надзвичайних ситуаціях можуть бути застосовані спеціальні додаткові методи безпеки. Наприклад, потрібно попередити спроби перешкодити роботам з ліквідації наслідків надзвичайних ситуацій. Необхідно забезпечити захист екстреного зв'язку певних користувачів, через важливість й екстреність цього зв'язку, від підроблення, перехоплення або постановки завад з боку зловмисних користувачів.

Для попередження розкриття місцеположення певних санкціонованих користувачів засобів екстреного зв'язку іншими несанкціонованими сторонами повинні бути застосовані спеціальні механізми захисту даних про те, де розташовані санкціоновані користувачі. Обмеженому числу керівників вищої ланки може знадобитись особливий зв'язок у надзвичайних ситуаціях із метою керівництва й організації аварійно-рятувальних робіт без ризику розкриття відомостей щодо їх знаходження.

Відновлюваність. Якщо ресурси мережі, що є ключовими для аварійно-рятувальних робіт, їх необхідно своєчасно відновити. Коли фізичні лінії доступу пошкоджені, оператори відновлюють їх працездатність, але час відсутності доступу може бути значним.

Для забезпечення відновлення необхідна можливість швидкого початку функціонування екстреного зв'язку для користувачів із переважним доступом. Певні засоби телекомунікаційної мережі повинні бути такими, щоб їх можна було легко поповнити, відремонтувати та відновити до такого ступеня, щоб забезпечити пріоритетний зв'язок потрібного рівня.

Міжмережні з'єднання. Бажано, щоб мережі, які забезпечують зв'язок у надзвичайних ситуаціях, були з'єднані з іншими мережами, дозволяючи отримати широке охоплення. Надзвичайні ситуації часто бувають регіональними, але можуть охопити декілька країн. Необхідно розглянути можливість з'єднання мереж декількох операторів в одній країні або оператора, чия мережа охоплює декілька країн, для забезпечення зв'язку в надзвичайних ситуаціях.

Міжмережна взаємодія. У схемах взаємодії мереж існує необхідність організованого та прозорого виконання основних положень [40] з надання екстреного зв'язку режиму переваги. Мають бути розглянуті переважні методи організації взаємодії в гетерогенних мережах. Проблемою міжмережної взаємодії часто буває проблема конфігурації. Найбільш зручною була б єдина конфігурація всіх систем для забезпечення можливості взаємодії з мережами різних операторів, які надають засоби зв'язку в надзвичайних ситуаціях.

Передбачається, що перехід на потрібну конфігурацію буде виконуватись у відповідних місцях входу/виходу, а не на внутрішніх мережах. Цей метод дозволяє забезпечити повсюдний зв'язок, оскільки будь-яким доступним провайдером може бути організована будь-яка послуга зв'язку в надзвичайних ситуаціях без зміни конфігурації засобів зв'язку. Метою цієї вимоги являється забезпечення взаємного з'єднання та міжмережної взаємодії всіх існуючих і нових мереж.

Мобільність. Мобільність вимагає, щоб до інфраструктури зв'язку були включені рухомі, швидкорозгортувані та повністю рухомі засоби. Телекомунікаційна інфраструктура повинна підтримувати рухомість користувача та термінала, включаючи зв'язок швидкого розгортання та рухомий зв'язок. Цим вимогам найбільшою мірою відповідає мережа *NGN*.

Повсюдність покриття. Повсюдна доступність телекомунікаційних ресурсів, які забезпечують реалізацію телекомунікаційних послуг для населення, може слугувати базисом для легко доступних засобів екстреного зв'язку. Аварійно-рятувальні роботи не будуть затримані до розгортання спеціальних засобів зв'язку, коли користувачі екстреного зв'язку використають засоби зв'язку загального користування. Тому ресурси телекомунікаційної інфраструктури загального користування на широких географічних площинах повинні утворювати основу для повсюдного проникнення екстреного зв'язку.

Життєздатність/працездатність. Основна мережна інфраструктура, яка підтримує зв'язок у екстрених ситуаціях, повинна бути максимально стійкою для того, щоб вистояти в разі лиха. Засоби зв'язку повинні бути досить стійкими, щоб підтримувати зв'язок із «вижившими» користувачами в широкому діапазоні зовнішніх умов, що виникли внаслідок стихійного лиха або антропогенних катастроф.

Передача мови. Основним способом зв'язку в ході аварійно-рятувальних робіт була й продовжує бути передача мови. Мережі з комутацією каналів виконують цю вимогу. У мережі з комутацією пакетів, для забезпечення нормального телефонного спілкування в реальному часі необхідно забезпечити: мале фазове тремтіння, малі втрати та малу затримку передачі. Телекомунікаційні мережі повинні забезпечити користувачам у надзвичайних ситуаціях потрібний рівень передачі мови.

Розширювана смуга пропускання. У тих випадках, коли це виправдано, під час оголошених надзвичайних ситуацій, коли ресурси інфраструктури практично вичерпані, може бути потрібним забезпечити пріоритетність зв'язку в надзвичайних ситуаціях порівняно зі звичайним зв'язком. Одним зі способів досягнення цього є надання розширюваної смуги пропускання для передачі трафіка екстреного зв'язку. Для звичайного зв'язку виділяється більш вузька смуга пропускання, що знижує якість встановлених з'єднань, або зв'язок може взагалі перерватись. Ширина смуги пропускання визначається потребами користувача. Вона може визначатись у ході отримання телекомунікаційних послуг у надзвичайних ситуаціях. Санкціоновані користувачі повинні мати можливість обирати параметри екстреного зв'язку для того, щоб виконувати різні вимоги по ширині смуги пропускання.

Надійність/експлуатаційна готовність. Для того, щоб бути максимально корисним, зв'язок у надзвичайних ситуаціях має бути як надійним, так і доступним. Скрізь, де це можливо, доступ до менеджменту мережі або її політики може підвищити ймовірність успішного з'єднання за рахунок надання режиму переважного зв'язку в надзвичайних ситуаціях. Телекомунікації повинні функціонувати узгоджено в точній відповідності з проектними

вимогами та повинні мати можливість її використання з високим рівнем таємності.

7.3 Механізми та функції забезпечення зв'язку в надзвичайних ситуаціях у *NGN*

7.3.1 *Загальні відомості щодо механізмів та функцій*

У *NGN* менеджмент надання послуг/застосуваннями відділено від транспортування в вигляді двох роздільних страт функціональних можливостей: страти транспортування та страти обслуговування. Це дає можливість роздільно пропонувати прикладні послуги та транспортні послуги і забезпечувати їх незалежний розвиток. Кожна страта має свій незалежний набір ролей, учасників та адміністративних доменів. Функції управління ресурсами та допуском (*RACF*) виконують роль арбітра для цих страт при виконанні їх взаємодії та резервування, пов'язаних із *QoS*.

Рішення, що приймаються *RACF* та пов'язані з *QoS*, опираються на *SLA*, пріоритет обслуговування, профілі користувача, правила роботи оператора мережі, а також наявність ресурсів як для мережі доступу, так і для базових мереж. Необхідно, щоб користувачі зв'язку в надзвичайних ситуаціях були ідентифіковані та щоб після того, як вони пройшли автентифікацію та авторизацію, *RACF* надала їм пріоритет в управлінні доступом.

Якщо в *NGN* необхідно відрізняти трафік зв'язку в надзвичайних ситуаціях від звичайного трафіка, то необхідно, щоб були доступні відповідні позначки, які називають *маркерами*. У наскрізній (тобто через сегменти мережі доступу та базової мережі) багаторівневій (тобто через страти транспортування й обслуговування) архітектурі *NGN* можливе існування різних позначок на різних рівнях протоколу, як вертикальних (тобто за взаємодії між різними рівнями протоколів), так і горизонтальних (тобто за взаємодії міжмережними елементами, між якими встановлюється зв'язок).

Позначки можуть передаватися в пакетах сигналізації та/або вставлятися в заголовок пакетів даних для ідентифікації та маркування викликів/сеансів зв'язку в надзвичайних ситуаціях. Позначки, що використовуються для ідентифікації та маркування викликів/сеансів або трафіка зв'язку в надзвичайних ситуаціях, залежать від протоколу.

Для отримання спеціалізованого (наприклад, переважного/пріоритетного) режиму, що є наскрізним для всіх аспектів виклику/сеансу зв'язку в надзвичайних ситуаціях (наприклад, управління викликом/сеансом, трафіком і управління носійною), вимагається забезпечити відповідне перетворення позначок, що використовуються в різних протоколах, і взаємодію між цими позначками.

У страті обслуговування послугами звичайно використовуються конкретні задані набори протоколів. Отже, методи, які можуть бути ефективно використані для конкретних послуг зв'язку в надзвичайних ситуаціях,

змінюватимуться залежно від даних послуг і можливостей конкретного протоколу (протоколів), щодо якого йде мова, пов’язаного з послугою.

У площині транспортування може бути використано протокол Інтернет (*IP*). Точний склад базового стека протоколу *IP*, ймовірно, змінюватиметься залежно від постачальника.

Крім того, протоколи, що використовуються в інфраструктурі локального (остання миля) доступу, можуть відрізнятися від протоколів, що використовуються в базовій інфраструктурі. Інфраструктура локального доступу може будуватися з використанням проводових (тобто фіксований доступ) технологій, безпроводових технологій, або на основі їх поєднання.

Таким чином, для організації заданого наскрізного маршруту даних виклику/сеансу зв’язку в надзвичайних ситуаціях може бути використано широкий діапазон технологій транспортування.

У *NGN*, де страти обслуговування та транспортування незалежні, наступні фактори впливають на успішне забезпечення зв’язку в надзвичайних ситуаціях:

– ідентифікація та маркування трафіка зв’язку в надзвичайних ситуаціях;

– політика управління допуском;

– політика розподілу смуги пропускання;

– автентифікація й авторизація справжніх користувачів зв’язку в надзвичайних ситуаціях.

Реалізацію пріоритетного режиму див. у розд. 8.2.

7.3.2 *Ідентифікація, автентифікація, авторизація й управління доступом*

Необхідно запобігати неавторизованому доступу до послуг і ресурсів зв’язку в надзвичайних ситуаціях, наприклад, з боку зловмисників, що маскуються під авторизованих користувачів. Отже, повинні забезпечуватися механізми та можливості автентифікації користувачів або пристроїв зв’язку в надзвичайних ситуаціях, або тих, й інших, залежно від випадку, а також авторизації доступу, на основі політики, застосовуваної до конкретної служби.

Необхідно ідентифікувати виклик/сеанс зв’язку в надзвичайних ситуаціях (наприклад, за допомогою спеціального набору номера, вхідних даних, профілів користувача або підписки).

Провайдери послуг *NGN* повинні прискорювати автентифікацію авторизованих користувачів зв’язку в надзвичайних ситуаціях. Вимагається використати конкретні механізми та методи для автентифікації й авторизації, засновані на політиці, застосовуваній до конкретних видів зв’язку в надзвичайних ситуаціях (наприклад, використати персональний ідентифікаційний номер (*PIN*), а також профілі користувача та підписки). Після того, як користувач або пристрій, або обидва, автентифіковані й авторизовані на основі застосованої політики, трафік виклику/сеансу зв’язку в надзвичайних ситуаціях повинен бути маркований і спрямрваний у прямо до подальших мереж. Також після проходження автентифікації й авторизації вимагається, щоб пріоритет надався за всіма аспектами виклику/сесії зв’язку в надзвичайних

ситуаціях, сигналізації/управлінні, трафіка носійної та будь-якому застосовуваному управлінні.

Необхідно врахувати автентифікацію й авторизацію за естафетним передаванням та прийманням викликів/сеансів зв'язку в надзвичайних ситуаціях між провайдерами послуг *NGN*, з урахуванням наявності багатьох провайдерів послуг і розподілу менеджменту обслуговування і транспортування. Автентифікація й авторизація провайдерів послуг *NGN* для естафетного передавання та приймання викликів/сеансів і трафіка зв'язку в надзвичайних ситуаціях повинна ґрунтуватися на *SLA* і застосовуваній політиці.

7.3.3 *Заходи щодо забезпечення вищої ймовірності допуску за управління доступом*

Однією із задач функції управління ресурсами та допуском (*RACF*) є забезпечення управління *QoS*, включаючи допуск до ресурсів і резервування ресурсів, якщо побажає провайдер послуги. У зв'язку з цим у періоди високої потреби в обслуговуванні з боку користувачів, у деяких запитах на обслуговування, можливо, доведеться відмовити. Якщо такі відмови не відбуваються, то *NGN* не може повністю гарантувати якість обслуговування в надзвичайних ситуаціях. Процеси *RACF*, пов'язані з *QoS*, включають авторизацію на основі профілів користувача, *SLA*, правил роботи оператора мережі, пріоритету обслуговування та наявності ресурсів для доступу та базового транспортування. Пріоритет обслуговування є фактором першорядної ваги, який має бути врахованим у методах планування для ухвалення рішення щодо розподілу ресурсів стосовно допуску з очікуванням/загальним допуском.

Високорівневі вимоги *RACF* полягають у роботі над авторизованими запитами відносно *QoS* із використанням профілів і пріоритету користувача. Одна конкретна вимога полягає в тому, щоб за управління допуском для пріоритетної обробки була використана інформація щодо пріоритету обслуговування. Існують різні методи, які можуть бути використані для пріоритету обслуговування при управлінні допуском на основі ресурсів.

Один із можливих методів полягає в тому, щоб для трафіка зв'язку в надзвичайних ситуаціях було використано вищі пороги допуску і, таким чином, забезпечувалася можливість деякого додаткового допуску для пріоритетних запитів, коли звичним запитам видається відмова. При застосуванні даного методу тимчасово підвищується використання ресурсів мережі. Проте внаслідок великого обсягу ресурсів *NGN*, пропускна здатність системи відновиться до свого встановленого робочого поточного рівня. Більш того, якщо припустити, що обсяг пріоритетного трафіка відносно невеликий і що мережа рідко або майже ніколи не працює з повною 100-стовідсотковою пропускною здатністю, стає очевидним, що вищий поріг рішення про допуск для пріоритетного трафіка не повинен створювати ніякої загрози загальній працездатності мережі або *QoS* іншого трафіка.

Існують системи управління допуском на основі резервування, які дозволяють запити на обслуговування тільки в тому випадку, якщо запит

відносно необхідної смуги пропускання є успішним. У цьому випадку в методі обслуговування механізму планування, як першочергова задача, повинен бути врахованим пріоритет обслуговування.

Управління допуском виклику є набором дій/правил, що використовуються мережею на етапі встановлення виклику/сеансу, для того, щоб приймати або відхиляти обслуговування на основі запрошуваної інформації та критеріїв пріоритету, а також наявності необхідних ресурсів.

У традиційній телекомунікаційній мережі загального користування (ТМЗК) управління допуском виклику означає те, що канал або надається, або не надається на основі авторизації. Більше того, надання каналу за визначенням має на увазі наявність маршруту з необхідною смугою пропускання. У зв'язку з тим що є інформація щодо стану мережі, яка стосується статусу окремих каналів (мовних каналів), мережа ТМЗК може:

– спрямовувати екстрені виклики на спеціально зарезервовані для екстреного трафіка маршрути (якщо є);

– чекати, поки звільниться канал (постановка до черги).

Оскільки в мережах на основі протоколу *IP* відсутня інформація щодо стану окремих маршрутів або каналу, з допомогою лише автентифікації й авторизації при вході до мережі не можна гарантувати наявність наскрізного маршруту або достатньої наскрізної смуги пропускання для даного виклику/сеансу. У мережі на основі протоколу IP вхідний мережний елемент не має або майже не має відомостей про переважаючі стани мережі за межами свого домена. Отже, управління допуском виклику у вхідному мережному елементі є недостатнім для того, щоб гарантувати наявність наскрізного маршруту, якщо його не було розширено за допомогою додаткових засобів.

З цього далі випливає, що вихідний мережний елемент ніяким чином не управляє віддаленим вхідним мережним елементом, який може намагатися встановити з ним виклик/сеанс, бо не має про цей елемент ніяких відомостей. Проте в мережах ТМЗК вихідний мережний елемент здатний управляти можливим вхідним мережним елементом, який намагається встановити виклик/сеанс за допомогою механізмів зв'язаної сигналізації.

Рекомендовано три рівні пріоритету управління допуском для сигналів служб, що вимагають входження в *NGN*. Рівень пріоритету 1 (найбільший) рекомендований для зв'язку в надзвичайних ситуаціях по *NGN*. Трафік із цим рівнем пріоритету отримує найбільшу гарантію допуску в *NGN*.

7.3.4 *Страта обслуговування*

Можуть виникати кризові ситуації, за яких важливо, щоб користувач міг зв'язатися з будь-якими доступними користувачами в тій же чи іншій країні. У цьому випадку важливо, щоб виклик/сеанс, що виходить з будь-якої країни, отримав наскрізний пріоритетний режим. Для цього потрібна взаємодія двох мереж, в яких або надається можливість пріоритетного режиму, або забезпечується прозора передача пріоритету між обома мережами.

Пріоритет ресурсів для SIP. До *SIP* додано два поля заголовків, а саме поле "пріоритет ресурсу" (*Resource-Priority*) і поле "прийняти пріоритет ресурсу" (*Accept-Resource-Priority*), а також визначаються процедури їх використання. Поле заголовка "пріоритет ресурсу" може використано агентами користувача *SIP*, шлюзовими станціями та кінцевим обладнанням телекомунікаційної мережі загального користування (ТМЗК), а також серверами-посередниками *SIP* з метою дії на оброблення ними запитів *SIP*.

IEPS. У Рекомендації ITU-T E.106 [40] описуються функціональні вимоги до міжнародної системи переваг при надзвичайних ситуаціях (*IEPS*), її властивості, доступ до *IEPS* і оперативне управління системою. *IEPS* дає можливість взаємодії різних систем пріоритетів/переваг, реалізованих на національному рівні. Тим самим забезпечується наскрізний переважний режим для авторизованих вузькосмугових голосових виклик і викликів для передачі даних. Сфера застосування *IEPS* сформульована для випадків телефонної мережі загального користування або мережі сухопутного рухомого зв'язку загального користування (*PLMN*). *IEPS* надає авторизованим користувачам пріоритетний режим для служби міжнародного телефонного зв'язку на телекомунікаційних мережах зі встановленням з'єднання. Отже, на основі двосторонніх/багатобічних угод між країнами/адміністраціями можна б було використати *IEPS* за такого сценарію для забезпечення взаємодії реалізованих на національному рівні *ETS*.

***Протоколи управління у системі H.*323.** У Рекомендації ITU-T H.460.4 [41] визначається позначення пріоритету виклику й ідентифікація мережі країни/міжнародної мережі походження виклику для пріоритетних викликів у системі H.323. Параметр для позначення пріоритету виклику в системі H.460.4 підтримує індикатор пріоритетного виклику та п'ять рівнів пріоритету.

У Рекомендації ITU-T H.248.1 визначаються протоколи, що використовуються між елементами фізично розподіленого мультимедійного шлюзу, який застосовується відповідно до архітектури, вказаної в Рекомендації ITU-T H.323. Для санкціонованих урядом екстрених служб визначаються індикатор виклику й індикатор пріоритету *IEPS*. В індикаторі виклику *IEPS* передається вказівка на пріоритет між функціями контролера та шлюзу. В індикаторі пріоритету передаються рівні пріоритету між функціями контролера та шлюзу. Індикатор пріоритету підтримує 16 рівнів пріоритету. Для служб суспільної безпеки визначаються індикатори екстреного виклику для передачі вказівки на пріоритет між функціями контролера і шлюзу.

7.3.5 *Страта транспортування*

У основі спеціальних угод, таких як *SLA*, для обробки сигналів *NGN* лежить припущення про те, що коли мережні ресурси недостатні для того обсягу трафіка, який надходить до мережі, то за таких умов трафік зв'язку в надзвичайних ситуаціях міг бути істотно затриманим та/або перерваним, або нижчим за той рівень, за якого його можна використати. У випадку якщо обсяг трафіка, що приймається, передбачений у моделі з максимально можливим

рівнем обслуговування, перевищує пропускну здатність даного мережного елемента (наприклад, *IP*-маршрутизатора), то єдиною можливістю, доступною для даного мережного елемента є припинення передачі надмірного трафіка. Це означає, що якщо не дозволені спеціальні заходи переважної обробки, передача трафіка зв'язку в надзвичайних ситуаціях була б припинена разом з іншим трафіком, що не є трафіком зв'язку в надзвичайних ситуаціях.

Як рішення іноді пропонуються методи надмірного забезпечення ресурсами. Проте в багатьох випадках надмірне забезпечення може виявитися неможливим або недоцільним. Деякі види надзвичайних ситуацій можуть виникати в результаті навмисного або випадкового руйнування/пошкодження ділянок мережі. Якщо *NGN* спроможна буде справитися з усіма видами надзвичайних ситуацій за несприятливих обставин, то буде необхідно забезпечити наявність конкретних засобів для надання трафіка зв'язку в надзвичайних ситуаціях переважного режиму.

Управління смугою пропускання. Однією з можливих характеристик *IP*-мережі, за рахунок якої забезпечується певна (груба) відповідність розподіленій смузі пропускання в мережах з комутацією каналів, є використання механізму розподілу та резервування смуги пропускання на основі протоколу *IP*. Даний механізм є процедурою в протоколі резервування ресурсів (*RSVP*), який описано в RFC 2205. Параметри управління ресурсами, які необхідні для протоколу ініціації сеансу (*SIP*) у страті обслуговування, повинні бути використані спільно з протоколом у страті транспортування. Дані параметри дозволяють використати процедури сигналізації *RSVP* до процедури сигналізації *SIP*, під час їх та/або разом з ними.

Управління чергові стю з використанням диференційованого обслуговування. Рекомендується перетворення класів обслуговування в указники коду диференційованого обслуговування (*DSCP*). У таблицях перетворення виділяється клас термінового пересилання даних (*EF*). Це дозволяє включати у пакети протоколу *IP* значення *DSCP*, виділених для класу термінового пересилання даних.

Рекомендується також, щоб голосовий трафік у пакетах протоколу IP маркувався (позначався) з використанням *DSCP*, відповідного терміновому пересиланню даних. При отриманні пакетів, маркованих як *EF*, мережні елементи (маршрутизатори) у страті транспортування забезпечать своєчасну доставку трафіка, що вимагає негайної обробки, порівняно з трафіком, що не вимагає негайної обробки, з використанням правил термінового пересилання даних, які визначені для показника коду *EF*.

Але код *EF* використовується для звичного телефонного трафіка. Отже, як і раніше може існувати необхідність у тому, щоб якимось чином розрізняти трафік телефонного зв'язку в надзвичайних ситуаціях від трафіка зв'язку в надзвичайних ситуаціях.

EF DSCP для трафіку, що має допуск до пропускної здатності. Рекомендується здійснювати розподіл *EF DSCP* для трафіка, що має допуск до пропускної здатності. Це дає можливість передавати трафік у реальному часі, відповідно до правил поведінки на кожному кроці за термінового пересилання

даних, з використанням процедури, передбачає автентифікацію, яка авторизацію та допуск до пропускної здатності.

7.3.6 *Доступ до NGN*

Існує багато методів доступу до *NGN*, залежних від технології. Мережа доступу включає функції, залежні від поєднання методу доступу та технології. Наприклад, для технології *W-CDMA* та доступу по *xDSL*. Залежно від технології, що використовується для доступу до послуг *NGN*, мережа доступу включає функції, що відносяться до:

1) кабельного доступу;

2) доступу по *xDSL*;

3) безпроводовому доступу (наприклад, з використанням технологій IEEE 802.11 та 802.16, а також доступу по 3*G RAN*);

4) оптичного доступу.

Для забезпечення зв'язку в надзвичайних ситуаціях у сегменті доступу до *NGN* також необхідні спеціальні угоди. В основі необхідності у спеціальних угодах лежить припущення того, що ресурси доступу обмежені точно так, як і ресурси базової мережі. Отже, залежно від обсягу трафіка, який надходить у сегмент мережі доступу, на трафік зв'язку в надзвичайних ситуаціях може бути вплив. Наприклад, він міг би виявитися затриманим та/або перерваним, нижчим за той рівень, за якого його може бути використано.

Отже, якщо *NGN* спроможна бути справитися з усіма видами надзвичайних ситуацій за несприятливих обставин, то у сегменті доступу *NGN* повинна бути забезпечена наявність конкретних засобів для надання трафіка зв'язку в надзвичайних ситуаціях переважного режиму. Це включає, крім іншого, механізми та функції для:

– розпізнавання трафіка зв'язку в надзвичайних ситуаціях;

– переважного/пріоритетного доступу до ресурсів/засобів;

– переважної/пріоритетної маршрутизації трафіка зв'язку в надзвичайних ситуаціях;

– переважного/пріоритетного встановлення сеансів/викликів зв'язку в надзвичайних ситуаціях.

Безпроводовий радіодоступ. Вимагається, щоб мережі безпроводового радіодоступу забезпечували конкретні механізми та можливості надання авторизованим сеансам/викликам зв'язку в надзвичайних ситуаціях переважного/пріоритетного режиму. Для надання такого режиму можуть бути використані механізми та функції, залежні від технології. Це включає, крім іншого, механізми та функції для:

– розпізнавання трафіка зв'язку в надзвичайних ситуаціях: таке розпізнавання включає ідентифікацію та маркування авторизованого трафіка зв'язку в надзвичайних ситуаціях;

– переважного/пріоритетного доступу до ресурсів/засобів: це полегшує доставку в *NGN* запиту на зв'язок у надзвичайних ситуаціях, якщо наявні ресурси доступу обмежені;

– переважної/пріоритетної маршрутизації трафіка зв’язку в надзвичайних ситуаціях: це може припускати такі властивості, як поставлення до черги на наявні ресурси, виключення з певних обмежувальних функцій управління мережею та резервування деяких маршрутів/шляхів для трафіка зв’язку в надзвичайних ситуаціях;

– переважного/пріоритетного встановлення сеансів/викликів зв’язку в надзвичайних ситуаціях.

Наприклад, у стандарті 3*GPP* визначається пріоритетне обслуговування або пріоритетне обслуговування мультимедійного трафіка у системах 3*GPP*. Пріоритетне обслуговування та пріоритетне обслуговування мультимедійного трафіка дозволяє авторизованим користувачам отримувати пріоритетний доступ до найближчих наявних радіоканалів (для голосового трафіка або трафіка даних) порівняно з іншими користувачами у ситуаціях, коли перевантаження приводить до блокування спроб виклику.

За пріоритетного обслуговування підтримується пріоритетне проходження та завершення виклику, що забезпечує "наскрізний" пріоритетний виклик між мережами рухомого зв’язку, між мережами рухомого та фіксованого зв’язку та між мережами фіксованого та рухомого зв’язку. За пріоритетного обслуговування мультимедійного трафіка забезпечується пріоритетне проходження та завершення мультимедійних сеансів, що забезпечує "наскрізні" пріоритетні мультимедійні сеанси, зокрема між мережами рухомого зв’язку, між мережами рухомого та фіксованого зв’язку та між мережами фіксованого та рухомого зв’язку.

Фіксований доступ. Вимагається, щоб мережі фіксованого доступу забезпечували конкретні механізми та можливості надання авторизованим викликам/сеансам зв’язку в надзвичайних ситуаціях переважного/пріоритетного режиму. Для надання такого режиму можуть бути використані механізми та функції, залежні від технології. Це включає, крім іншого, механізми та функції для:

– розпізнавання трафіка зв’язку в надзвичайних ситуаціях: таке розпізнавання включає ідентифікацію та маркування авторизованого трафіка зв’язку в надзвичайних ситуаціях;

– переважного/пріоритетного доступу до ресурсів/засобів: це полегшує доставку в *NGN* запиту на зв’язок у надзвичайних ситуаціях, якщо наявні ресурси доступу обмежені;

– переважної/пріоритетної маршрутизації трафіка зв’язку в надзвичайних ситуаціях: це може припускати такі властивості, як постановлення до черги на наявні ресурси, виключення з певних обмежувальних функцій менеджменту мережею та резервування деяких маршрутів/шляхів для трафіка зв’язку в надзвичайних ситуаціях;

– переважного/пріоритетного встановлення сеансів/викликів зв’язку в надзвичайних ситуаціях.

Наприклад, істотні аспекти переважного зв’язку мережами *IPCablecom* групуються за двома напрямами: встановлення пріоритету й автентифікації. Ці два напрями включають можливості забезпечення зв’язку в *IPCablecom*, для

якого можливо потрібний переважний режим. Реалізація пріоритету й автентифікації необхідні для забезпечення переважного зв'язку в мережах *IPCablecom.*

7.4 Задачі кібербезпеки та принципи приєднання служб зв'язку в надзвичайних ситуаціях

7.4.1 *Вихідні дані й основні задачі*

Зв'язок у надзвичайних ситуаціях повинен користуватися переважним режимом порівняно із звичними послугами мереж загального користування. Ідея пріоритетного зв'язку, що використовується в надзвичайних ситуаціях, не нова; протягом багатьох років мережі з комутацією каналів забезпечували роботу таких систем, здебільшого, для голосових викликів [39]. Що стосується технічних методів, що використовуються для забезпечення виконання цих основоположних вимог до зв'язку в надзвичайних ситуаціях у середовищі *NGN*, то вони розвиваються. Традиційні методи встановлення пріоритету, що використовуються при комутації каналів, не можуть бути застосовані в *NGN* унаслідок відмінностей, властивих зв'язку з комутацією каналів і з комутацією пакетів. У зв'язку з тим, що *NGN* засновані на технології комутації пакетів, яка принципово відрізняється від технології комутації каналів, вимагається розглянути технічні питання та можливі рішення, які можуть бути використані для реалізації можливостей зв'язку в надзвичайних ситуаціях у *NGN*.

Мережні елементи, системи, ресурси, дані та служби, що використовуються для забезпечення зв'язку в надзвичайних ситуаціях, можуть піддаватися кібератакам. Цілісність, конфіденційність і доступність зв'язку в надзвичайних ситуаціях, особливо в разі атаки, залежатиме від мережних засобів захисту та практичних заходів безпеки, реалізованих у *NGN*, а також від можливостей у області забезпечення безпеки (наприклад, функцій автентифікації й авторизації), які виконуються в рамках прикладної послуги для зв'язку в надзвичайних ситуаціях. Загальні керівні вказівки для розгляду питань планування безпеки в області зв'язку в надзвичайних ситуаціях включають, крім іншого, наступне.

Всі аспекти зв'язку в надзвичайних ситуаціях, включаючи менеджмент, сигналізацію та контроль, канал передачі/середовища, а також дані й інформацію, що стосуються менеджменту (наприклад, інформація щодо профілю користувача) вимагається захищати від загроз безпеки. Загрози безпеки зв'язку в надзвичайних ситуаціях можуть виникати на різних рівнях (наприклад, транспорт, менеджмент обслуговування, забезпечення обслуговування) та в різних мережних сегментах (наприклад, доступ, базова мережа та міжмережеві інтерфейси).

Встановлення та забезпечення виконання стратегії та практики в області безпеки, характерні для послуг зв'язку в надзвичайних ситуаціях. Слід визначити та реалізувати можливості послаблення впливу для забезпечення захисту від різних загроз безпеки. Конкретно, для послуг зв'язку в

надзвичайних ситуаціях слід визначити та реалізувати можливості послаблення впливу та практичні заходи безпеки, крім тих, які потрібні для загальних прикладних послуг. До них відносяться стратегія безпеки для захисту даних менеджменту, управління та накопичення інформації (наприклад, інформації щодо профілю користувача), що відноситься до зв'язку в надзвичайних ситуаціях.

Реалізація та застосування процедур для автентифікації й авторизації користувачів, пристроїв, з тим щоб забезпечити захист від неавторизованого доступу до послуг, ресурсів та інформації (наприклад, інформації користувачів у серверах автентифікації та системах управління), що відноситься до зв'язку в надзвичайних ситуаціях. Наприклад, слід реалізувати функції автентифікації й авторизації, щоб не допустити використання неавторизованими користувачами ресурсів, виділених для зв'язку в надзвичайних ситуаціях, і запобігти атакам типу відмова в обслуговуванні (*DoS*) та інші види атак.

Відповідальність у рамках кожної мережі за безпеку повідомлень у межах свого домена, які перетинають множину доменів провайдерів мережних послуг, для того, щоб можна було забезпечити безпеку наскрізної передачі. У зв'язку з тим, що у зв'язку в надзвичайних ситуаціях можуть бути використані повідомлення, які перетинають різні домени провайдерів мережних послуг на національних і міжнародних мережах, вимагається встановити та реалізувати стратегію безпеки, довірчі відносини, методи та процедури ідентифікації трафіка зв'язку в надзвичайних ситуаціях, менеджмент ідентичності й автентифікацію користувачів і мереж у межах багатьох доменів адміністративного управління мережею.

При плануванні безпеки зв'язку в надзвичайних ситуаціях слід урахувати рекомендації з безпеки *NGN*, що містяться в розд.6. Крім того, слід також урахувати концепцію безпеки, в основі якої лежать наступні сфери діяльності в області безпеки, які визначені в Рекомендації ITU-T X.805: управління доступом; автентифікація; невідновність; конфіденційність даних; безпека з'єднань; цілісність даних; готовність; приватність. Здійснення пріоритетного зв'язку може привести до створення нових механізмів, а також до взаємодії/повторного використання існуючих механізмів.

Послуги зв'язку в надзвичайних ситуаціях (*ETS*) між різними національними мережами, тобто країнами/адміністраціями, повинні бути захищені від загроз безпеки. Щоб дати можливість мережі забезпечувати безпеку наскрізних послуг зв'язку *ETS* між різними національними мережами, тобто країнами/адміністраціями, необхідні рекомендації та загальні задачі та вимоги безпеки. Безпека та доступність послуг зв'язку *ETS* залежатимуть від безпеки кожної мережі, що бере участь у створенні наскрізного зв'язку.

Основна задача полягає в тому, щоб дати мережам можливість забезпечити безпеку послуг зв'язку *ETS*, наприклад, безпечної та пріоритетної передачі голосу, відео, даних і повідомлень, через різні національні мережі, тобто країни/адміністрації, та захист доступності *ETS*. Вона включає безпеку наскрізних з'єднань, які можуть проходити через домени різних провайдерів мережних послуг у національних і міжнародних мережах, тобто

країнах/адміністраціях, де кожна мережа несе відповідальність за безпеку в межах свого домену.

7.4.2 *Загальні положення та планування безпеки зв'язку в надзвичайних ситуаціях*

У системах пріоритетної передачі голосу, відео або повідомлень, між двома різними національними мережами, наскрізні пріоритетні системи зв'язку в надзвичайних ситуаціях можуть складатися з багатьох мережних сегментів і адміністративних доменів, наприклад, мережа доступу, мережа походження, мережа провайдера зв'язку в надзвичайних ситуаціях, мережа міжнародного провайдера, проміжна мережа та прикінцева мережа.

Кожен сегмент мережі несе певну відповідальність за безпеку в межах свого домена для забезпечення наскрізної безпеки та доступності послуг зв'язку в надзвичайних ситуаціях.

Мінімальний набір основних положень і планів безпеки для захисту сигналізації, каналу передачі та даних, а також даних й інформації, пов'язаної з менеджментом зв'язку в надзвичайних ситуаціях, наприклад, інформації щодо профілю користувача.

Кожен домен мережі повинен встановити та застосувати стратегії безпеки, а також реалізувати можливості придушення атак на зв'язок у надзвичайних ситуаціях у межах свого домена. Зокрема, рекомендується, щоб для пріоритетних з'єднань зв'язку в надзвичайних ситуаціях були визначені та застосовані можливості придушення атак і практичні застосування з безпеки крім тих, які необхідні для служб загального користування. Наприклад, повинні розроблятися дані можливості та практичні застосування для запобігання використанню ресурсів зв'язку в надзвичайних ситуаціях неавторизованими користувачами, а також для запобігання атакам типу "відмова в обслуговуванні" й атак інших типів.

Кожен домен мережі повинен встановлювати відносини довіри, методики та процедури для визначення послуг зв'язку в надзвичайних ситуаціях, а також для менеджменту ідентичності й автентифікації користувачів і мереж через множину мережних доменів. Наприклад, угоди щодо рівня обслуговування (*SLA*) повинні встановлювати політику безпеки для автентифікації кожного домена при обробці й отриманні послуг зв'язку в надзвичайних ситуаціях.

Кожен адміністративний домен мережі повинен встановити та застосувати стратегії безпеки для захисту даних менеджменту й інформації зв'язку в надзвичайних ситуаціях, наприклад, інформації щодо профілю користувача.

Основні функції безпеки. Рекомендується, щоб для зв'язку в надзвичайних ситуаціях виконувалися наступні основні вимоги до безпеки:

– функції безпеки із захисту наскрізних послуг зв'язку в надзвичайних ситуаціях за передавання через домени множини мереж;

– функції безпеки із захисту доступності послуг зв'язку в надзвичайних ситуаціях за передавання через домени множини мереж;

– функції безпеки із забезпечення менеджменту ідентичності й автентифікації користувачів і мереж за передавання через множину адміністративних доменів. Бажано, щоб користувач взаємодіяв зі службою зв'язку в надзвичайних ситуаціях тільки один раз, а повноваження користувача передавалися від одного адміністративного домена до іншого за допомогою механізмів безпеки.

Автентифікація, авторизація та контроль доступу. Рекомендується, щоб для зв'язку в надзвичайних ситуаціях підтримувався наступний мінімальний набір функцій автентифікації, авторизації й управління доступом:

– функції безпеки із захисту механізмів, що використовуються при автентифікації й авторизації користувачів і пристроїв зв'язку в надзвичайних ситуаціях;

– функції безпеки із захисту механізмів, що використовуються при з'єднанні користувача зв'язку в надзвичайних ситуаціях із відповідними пристроями;

– функції безпеки із захисту механізмів, що використовуються при сумісному використанні інформації автентифікації, наприклад, підтвердження того, що користувач був автентифікований, за передаванні через домени множини мереж;

– функції безпеки із захисту механізмів, що використовуються при двосторонній автентифікації користувача й об'єктів. Включає механізми для користувача зв'язку в надзвичайних ситуаціях з автентифікації взаємодіючих об'єктів, наприклад, інтернет-сайта, сервера контента тощо, що викликаються;

– функції безпеки із захисту механізмів, що використовуються однією мережею при автентифікації іншої мережі. Включає механізми, що використовуються при автентифікації мережі, що обробляє послуги зв'язку в надзвичайних ситуаціях, наприклад, мережі походження виклику, й автентифікації мережі, що отримує послуги зв'язку в надзвичайних ситуаціях, наприклад, проміжної або кінцевої мереж.

– функції безпеки із захисту від несанкціонованого доступу до інформації та ресурсів зв'язку в надзвичайних ситуаціях, наприклад, інформації користувачів на серверах автентифікації та у системах менеджменту.

Конфіденційність і приватність. Рекомендується, щоб підтримувався наступний мінімальний набір функцій конфіденційності:

– функції безпеки із забезпечення захисту конфіденційності для сигналізації, управління та менеджменту зв'язку в надзвичайних ситуаціях;

– функції безпеки із забезпечення захисту конфіденційності каналу передачі та даних трафіка зв'язку в надзвичайних ситуаціях, наприклад, голосу, відео або даних;

– функції безпеки із забезпечення захисту конфіденційності користувача зв'язку в надзвичайних ситуаціях та ідентичності взаємодіючих об'єктів, а також інформації щодо умов підписки;

– функції безпеки із забезпечення захисту конфіденційності місцеположення користувача зв'язку в надзвичайних ситуаціях.

Рекомендується, щоб підтримувався наступний мінімальний набір функцій приватності:

– функції безпеки із забезпечення захисту приватності інформації зв’язку в надзвичайних ситуаціях, наприклад, інформації, отримуваної зі спостереження за діяльністю мережі, такої як інтернет-сайти, які відвідав користувач, географічне положення користувача, *IP*-адреса й імена *DNS* пристроїв у мережі провайдера мережних послуг;

– функції безпеки із забезпечення захисту приватності від несанкціо-нованого спостереження за інформацією використання зв’язку в надзвичайних ситуаціях, наприклад, таких особливостей використання, як обсяг трафіка зв’язку в надзвичайних ситуаціях, місцеположення, час, частота тощо.

Цілісність даних. Рекомендується, щоб підтримувався наступний мінімальний набір функцій забезпечення цілісності даних:

– функції безпеки із забезпечення захисту цілісності послуг зв’язку в надзвичайних ситуаціях, наприклад, захист від несанкціонованої зміни, видалення, вставки або заміщення;

– включає функції надання повідомлень щодо фальсифікації або зміну інформації;

– функції безпеки із забезпечення захисту цілісності інформації зв’язку в надзвичайних ситуаціях, наприклад, позначення пріоритету, голосу, даних і відео;

– функції безпеки із забезпечення захисту цілісності особливих даних із конфігурації зв’язку в надзвичайних ситуаціях, наприклад, інформації про пріоритети, що зберігається в функціях стратегічних рішень, рівень пріоритету користувача тощо.

Комунікації. Рекомендується, щоб підтримувалися мінімальні функції безпеки із захисту послуг зв’язку в надзвичайних ситуаціях від вторгнень проти авторизованих користувачів зв’язку в надзвичайних ситуаціях, наприклад, механізми для запобігання перехопленню, захопленню або заміщенню сигналізації або каналу передачі/трафіка даних зв’язків у надзвичайних ситуаціях.

Доступність. Рекомендується, щоб підтримувався наступний мінімальний набір функцій:

– функції безпеки із захисту доступності послуг зв’язку в надзвичайних ситуаціях, наприклад, захист сигналізації та контролю зв’язку в надзвичайних ситуаціях, а також каналу передачі/трафіка даних від атак типу "відмова в обслуговуванні" (*DoS*) й атак іншого типу;

– функції безпеки із захисту доступності особливих ресурсів та інформації зв’язку в надзвичайних ситуаціях, наприклад, баз даних автентифікації/авторизації, інформації про пріоритети, що зберігається в функції стратегічних рішень, а також спеціальних мережних ресурсів від атак типу "відмова в обслуговуванні" (*DoS*) й атак іншого типу.

Питання для самоконтролю

1 Поясніть природу та джерела надзвичайних ситуацій.

2 Опишіть цілі та функціональні вимоги до телекомунікаційних служб у надзвичайних ситуаціях.

3 Дайте перелік основних функцій забезпечення зв’язку в надзвичайних ситуаціях.

4 Як реалізується пріоритети та пріоритетний режим?

5 Поясніть функцію конфіденційності даних щодо місцеположення.

6 Поясніть функцію захищені мережі.

7 Поясніть функцію відновлюваності.

8 Поясніть функцію міжмережних з'єднань.

9 Поясніть функцію міжмережної взаємодії.

10 Поясніть функцію мобільності.

11 Поясніть функцію повсюдного покриття.

12 Поясніть функцію розширення смуги пропускання.

13 Як реалізуються ідентифікація, автентифікація, авторизація та управління доступом?

14 Опишіть заходи щодо забезпечення вищої ймовірності допуску за управління доступом.

15 Безпека методів доступу до *NGN*.

16 Опишіть задачі кібербезпеки та принципи приєднання служб зв'язку в надзвичайних ситуаціях.

17 Опишіть технології менеджменту.

18 Опишіть менеджмент персональної інформації.

19 Опишіть механізми та функції забезпечення раннього попередження. 20 Дайте характеристику протоколу загального сповіщення.

Додаток А

Основні технічні характеристики uMSPP-155e

Таблиця А.1 – Технічні характеристики модулів мультиплексора uMSPP -155e

Параметр	Значення
Оптичний Інтерфейс	
Швидкість передачі	155,52 Мбіт/с (STM-1)
Довжина хвилі	1310 / 1550 нм
Тип лазера	SLM (одномодовий)
Тип оптоволокна	Одномодове
Підсилення системи	Більше 26 дБ з АРУ при $K_{пом} = 10^{-10}$
Чутливість приймача	-34 дБм
Тип лінійного кодування	Без переходу в нуль (NRZ) зі скремблюванням
Тип з'єднувача	FC/SC/WDM
Резервування	1+1 автоматичне або 1+0 (без резерву)
Інтерфейс E1	
Швидкість передачі, кбіт/с	2048
Лінійний код	HDB3
Режим роботи	Прозорий або структурований
Структура циклу	G.704
Параметри інтерфейсу	G703, симетричний / несиметричний
Вхідний / вихідний опір, Ом	120 / 75
Допустимі прямі втрати з'єднувальної лінії	Не менш 6 дБ на частоті 1024 кГц
Допустимі втрати за рахунок відбиття сигналу на вході каналу	12 дБ в діапазоні 51…102 Гц 18 дБ в діапазоні 102… 2048 Гц 14 дБ в діапазоні 2048… 3072 Гц
Інтерфейс 10/100 Base-T плати EOS	
Сумарна швидкість передачі всіх портів	До 100 Мбіт/с
Параметри інтерфейсу	10 / 100Base-T
З'єднувач	4×RJ-45
Електроживлення	
Джерело постійного струму	36-72 В
Джерело змінного струму	90-264 В із частотою 47…63 Гц
Споживана потужність	до 15 Вт

Таблиця А.2 – Характеристики оптичних модулів

Тип модуля	Лазер	Довжина хвилі, нм	Вихідна потужність, дБм	Чутливість, дБм	Дальність, км
S-1.1	MLM	1310	-15 ... -8	-34	30
S-1.2	MLM	1550	-15 ... -8	-34	40
L-1.1	MLM	1310	-5 ... 0	-35	50
L-1.2	SLM	1550	-5 ... 0	-35	80
Примітка. MLM- багатомодовий лазер; SLM- одномодовий лазер.					

Додаток Б

Основне меню мультиплексора uMSPP-155e

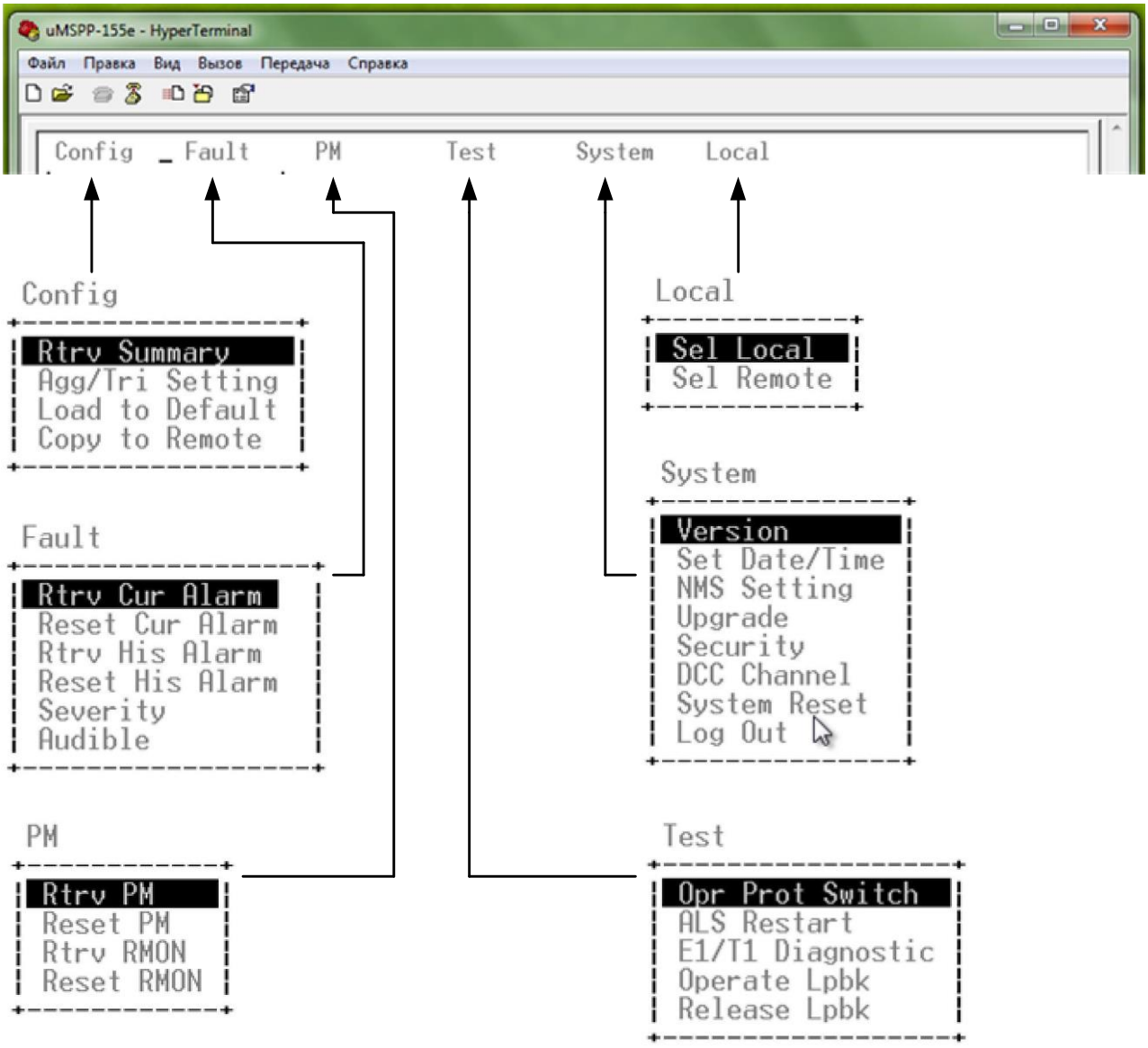


Рисунок Б.1 – Ієрархія основного меню

Таблиця Б.1 – Призначення пунктів основного меню мультиплексора

Пункт меню	Підпункт меню	Призначення
Config (конфігурування мультиплексора)	Rtrv Summary (перегляд загальної інформації)	Контроль установок і стан: оптичного модуля, трибутарных плат (QET і DQE) і плати Ethernet (EOS); номер плати вибирається в новому вікні
	Agg/Tri Setting (агрегатні та трибутарні установки)	Установка параметрів плати; її назва та номер вибирається надалі у спливаючому вікні
	Load to Default (установка вихідних значень)	Установка вихідних значень параметрів плат мультиплексора
	Copy to Remote (копіювати у віддалений мультиплекор)	Копіювання поточної конфігурації локального мультиплексора на віддалений
Fault (аварії)	Rtrv Cur Alarm	Перегляд поточних аварійних повідомлень; номер плати вибирається у новому вікні
	Reset Cur Alarm	Очищення інформації про поточні аварійні повідомлення
	Rtrv His Alarm	Перегляд журналу аварійних повідомлень
	Reset His Alarm	Очищення журналу аварійних повідомлень
	Severity	Перегляд і установка рівня критичності сигналу аварії для кожної плати
	Audible	Тимчасове або повне вимкнення, ввімкнення звукової аварійної сигналізації
PM (вимірювання характеристик)	Retrieve PM	Перегляд журналу вимірювань
	Reset PM	Очищення журналу вимірювань
	Rtrv RMON	Перегляд статистики протоколу віддаленого управління мережею (RMON)
	Reset RMON	Очищення зібраної статистики протоколу віддаленого управління мережею (RMON)
Test (тест)	Opr Prot Switch	Управління оптичним захисним перемиканням

Продовження таблиці Б.1

	ALS Restart	Перезапуск системи автоматичного гасіння лазера (ALS) при проведенні вимірювань
	E1/T1 Diagnostic	Запуск тесту самодіагностики інтерфейсу E1/T1 шляхом передачі псевдовипадкової послідовності з періодом 2^{15}-1
	Operate Lpbk	Управління функцією організації шлейфів на вході або виході оптичного модуля або плат QET / DQE
	Release Lpbk	Видалення раніше організованих шлейфів на вході або виході оптичного модуля або плат QET / DQE
System (системні установки)	Version	Перегляд інформації про версію програмного та апаратного забезпечення
	Set Date/Time	Установка поточної дати і часу
	NMS Setting	Установка параметрів системи управління мережею (NMS)
	Upgrade	Поновлення програмного забезпечення на локальному або віддаленому мультиплексорі
	Security	Управління обліковими записами користувачів (додавання, видалення, редагування або перегляд)
	Timming Src	Вибір джерела синхронізації мультиплексора
	DCC Channel	Вибір інформаційних ресурсів SDH для організації каналу службового зв'язку DCC (D1-D12 або VC -12)
	System Reset	Скидання параметрів системи до заводських значень
	Logout	Завершення сеансу авторизації поточного користувача
Local / Remote (локальний / віддалений мультиплексор)	Sel Local	Підключення до локального мультиплексора для його подальшого конфігурування
	Sel Remote	Підключення до віддаленого мультиплексора для його подальшого конфігурування