Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

Студентки *Нікольської Олени Ігорівни*

академічної групи *125м-21з-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *“Розробка організаційно-технічних заходів захисту інформації при використанні цифрової АТС EWSD”*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи				
розділів:	д.т.н., проф. Корнієнко В.І.			
спеціальний	д.т.н., проф. Корнієнко В.І.			
економічний	к.е.н., доц. Романюк Н.М.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Нікольській Олені Ігорівні* **академічної групи** *125м-21з-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему ***"Розробка організаційно-технічних заходів захисту інформації при використанні цифрової АТС EWSD"***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____№ _____

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Аналіз та систематизація матеріалу. Вступ.	30.09.2022
Розділ 2	Дослідження процесів управління і методик оцінки ризиків на ЦАТС. Розробка організаційно-технічних заходів захисту інформації при використанні цифрової АТС EWSD	10.11.2022
Розділ 3	Оцінки витрат на забезпечення інформаційної безпеки цифрової АТС EWSD	30.11.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: 19.12.2022

Прийнято до виконання 05.09.2022

_____ _____
(підпис студента) (прізвище, ініціали

РЕФЕРАТ

Пояснювальна записка: 90 с., 4 рис., 10 табл., 4 додатки, 15 джерел.

Об`єкт дослідження: організаційно-технічні заходи захисту інформації.

Предметом дослідження є захист інформації при використанні цифрової АТС EWSD.

Мета роботи: забезпечення захисту інформації при використанні цифрової АТС EWSD шляхом розробки та впровадження відповідних організаційно-технічних заходів.

Методи розробки: аналіз, опис, математичні та фізичні методи.

У першому розділі проаналізовано загрози для інформації та моделі порушників, організацію та порядок технічного захисту інформації в ЦАТС, сформульовано постановку задачі.

У спеціальній частині розроблено план захисту та політику безпеки інформації на АТС EWSD, розроблено заходи захисту від витоку інформації технічними каналами, розроблено систему захисту в мережі SS7.

В економічному розділі визначено витрати на штатні засоби і механізми інформаційної безпеки. При цьому встановлено, що найбільша частка витрат припадає на ділянки системи захисту від впливів позаштатними програмними і програмно-технічними засобами, які встановлені в процесі її експлуатації (14,20 %) та на систему ліквідації наслідків реалізованих загроз інформації на АТС (15,80%).

Наукова новизна роботи: визначено модель цифрової АТС EWSD з позицій технічного захисту інформації, розроблено план захисту цифрової АТС та політику безпеки інформації на ЦАТС EWSD.

Практичне значення: запропоновані підходи можуть бути використані при розробці, впровадженні, експлуатації чи модифікації цифрових АТС.

Можливі напрямки розвитку цієї роботи пов’язані з використанням інших методів та засобів захисту інформації для вдосконалення інформаційної безпеки цифрових АТС.

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛЬ ПОРУШНИКА, РІВЕНЬ ЗАГРОЗИ

ABSTRACT

Explanatory note: 90 pp., 4 figures, 10 tables, 4 appendices, 15 sources.

Object of research: organizational and technical measures of information protection.

The subject of the study is information protection when using the EWSD digital ATE.

The purpose of the work: ensuring the protection of information when using the EWSD digital ATE by developing and implementing appropriate organizational and technical measures.

Development methods: analysis, description, mathematical and physical methods.

The first chapter analyzes threats to information and models of violators, the organization and procedure of technical protection of information in digital ATE, and formulates the problem statement.

In a special part, a protection plan and information security policy for the EWSD ATE was developed, protection measures against information leakage through technical channels were developed, and a protection system in the SS7 network was developed.

In the economic section was established that the largest share of costs falls on software-technical means, which are installed during its operation (14,20%) and on the system for eliminating the consequences of realized information threats on the automatic transmission system (15,80%).

The scientific novelty of the work: the digital ATE protection plan and the information security policy for the EWSD ATE have been developed.

Practical significance: the proposed approaches can be used in the development, implementation, operation or modification of digital ATE.

Possible areas of development of this work are related to the use of other methods and means of information protection to improve the information security of digital ATE.

INFORMATION SECURITY POLICY, INFORMATION PROTECTION, INFORMATION SECURITY, OFFENDER MODEL, THREAT LEVE

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ATM (Asynchronous Transfer Mode) – асинхронний спосіб передачі даних

EWSD – (Elektronisches Wählsystem Digital - нім., Digital Electronic Switching System) цифрова електронна комутаційна система

ITU – (International Telecommunication Union) Міжнародний союз електрозв'язку

ISDN (Integrated Services Digital Network) інтегрований сервіс цифрової мережі

ISUP – (ISDN User Part) підсистема користувача цифрової мережі з інтеграцією послуг

NGN – (Next Generation Networks) мережі третього покоління

MTP – (Message Transfer Part) підсистема передачі повідомлень

SCCP – (Signaling Connection Control Part) підсистема управління з'єднанням сигналізації

SS7 – (Signaling System) система спільноканальної сигналізації

АКП – абонентські кінцеві прилади (апарати)

АЛ – абонентські лінії

АРМ – автоматизоване робоче місце

АС – автоматизована система

АТС – автоматична телефонна станція

ВОЛЗ – волоконно-оптична лінія зв'язку

ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації

ЕОМ – електронно-обчислювальна машина

ЕОД – електронний обмін даними

ЕЦП – електронний цифровий підпис

ЗМІ – захист мовної інформації

ІБ – інформаційна безпека

ІзОД – інформація з обмеженим доступом

ІКТ – інформаційно-комунікаційні технології

ІР – інформаційні ресурси

ІС – інформаційна система

ІТ – інформаційні технології

КАЗЛ – підсистема комутації абонентських та з'єднувальних ліній

КЗМЗ – комплекс засобів і механізмів захисту

КЗІ – комплексний захист інформації

КМПІ – корпоративна мережа передачі інформації

КСЗІ – комплексна система захисту інформації

КСІБ – комплексна система інформаційної безпеки

ЛОМ – локальна обчислювальна мережа

МПД – мережа передавання даних

МЗК – мережі загального користування

МТЗ – міський телефонний зв'язок

НЦУ – національний центр управління

ОІД – об'єкт інформаційної діяльності

ПЕМВН – побічні електромагнітні випромінювання та наводки

РНБО – Рада національної безпеки та оборони

РСО – режимно-секретний орган

СЗІ – система захисту інформації

СІБ – система інформаційної безпеки

СЦЗІ – соціальний захист інформації

ТЗІ – Технічний захист інформації

ТМЗК – телекомунікаційні мережі загального користування

ТфМЗК – телефонна мережа загального користування

ФВА – функціонально-вартісний аналіз

ФЗП – фонд заробітної плати

ФПЗ – функціональні послуги захисту

ЦАТС – цифрова автоматична телефонна станція

ЦОВ – центр обробки викликів

ЦСК – цифрові системи комутації

ЗМІСТ с.

ВСТУП

Зв'язок є вирішальним чинником прогресу та економічного зростання будь-якої країни. На порозі XXI століття відбулося злиття телекомунікаційних та комп'ютерних технологій, що призвело до зміни структури мереж зв'язку.

Об'єднання традиційно розділених мереж обумовлено як технологічними можливостями, так і бажанням абонента мати єдиний мережевий доступ, що забезпечує простоту звернення до послуг різних мереж - таких, як телефонна, ISDN (Integrated Services Digital Network), Internet, мультимедіа. Незважаючи на те, що в даний час ці мережі диференційовані, надалі намічається їх злиття до певної міри, але без повної взаємозамінності. Водночас ринок послуг зв'язку розвивається у напрямі від вузькосмугових до широкосмугових мереж. Для користувачів стає доступним все більш широкий спектр послуг зв'язку, таких, як послуги, що надаються в режимі on-line, широкосмугові (відеотелефонія, відеоконференція, передача даних та ін), послуги ISDN.

Проблеми зміни структури мереж, збільшення абонентського трафіку зумовлюють створення нових сучасних комутаційних систем із вищими пропускними здібностями.

Цифрова електронна комутаційна система EWSD (нім. Elektronisches Wählsystem Digital, англ. Digital Electronic Switching System) розроблена німецьким концерном Siemens AG для мереж зв'язку загального користування. Цифрова система комутації (ЦСК) EWSD може застосовуватися як міська АТС, сільська контейнерна АТС, в якості комутаційного вузла будь-якого рівня ієрархії (автоматична міжміська телефонна станція (АМТС), вузол автоматичної комутації (ВАК), комп'ютерна телефонія (КТ), комутаційного центру мобільного зв'язку (КЦМЗ), комутаційного центру цифрової мережі інтегрального обслуговування (ЦМІО), центру технічного обслуговування (ЦТО).

Захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах приділяється все більша увага при зростанні ролі інформації в усіх сторонах життя - особи, суспільства, виробництва й держави - та поширенню загроз і ризиків інформаційної, економічної, екологічної,

технологічної тощо, безпеки в рамках національної безпеки України.

Розширення пропускної здатності цифрових мереж в Україні випереджало розвиток систем їх інформаційної безпеки, особливо на перших етапах цифровізації. Перші цифрові телефонні станції (EWSD, 5ESS тощо), цифрові магістралі були побудовані без засобів захисту інформаційних ресурсів, а управління ними обмежувалось національним сегментом. На другому етапі, при розвитку телекомунікацій за технологіями ATM, Frame relay, системи технічного захисту були впроваджені фрагментарно на цифрових вузлах комутації та системах управління телекомунікаціями. На нинішньому етапі розпочато впровадження мереж наступного покоління (Next Generic Network – NGN) і, в першу чергу, мереж за технологією IP/MPLS. Надалі, при будь-якому впровадженні нових технологій, першочергова увага до безпеки стала обов'язковою. При впровадженні нових технологій більш адекватно оцінюються їх загрози інформаційній безпеці та створюються системи інформаційної безпеки з потрібним раціональним рівнем захищеності інформаційних ресурсів і гарантій захисту. В результаті досягається зниження ризиків інформаційної безпеки до прийнятного рівня у телекомунікаційних системах.

Таким чином, розробка організаційно-технічних заходів щодо захисту інформації ЦАТС, у тому числі і на базі EWSD, є актуальним завданням та невід'ємною частиною робіт із створення мереж зв'язку.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

Згідно нормативного документа [1], об'єктом технічного захисту на програмно-керованих АТС, а також на відомчих, корпоративних АТС є конфіденційна, а також відкрита, важлива для особи, суспільства і держави інформація, яка зберігається та циркулює на цих АТС.

Передавання державних інформаційних ресурсів дозволяється тільки через вузли комутації, що мають атестат відповідності комплексної системи захисту інформації вимогам із захисту інформації.

У цьому розділі розкриваються основні принципи й напрямки забезпечення інформаційної безпеки у відповідності з задачами та функціями ЦАТС, які базуються на нормативно-правових документах України, відповідають вимогам щодо забезпечення конституційних прав людини, проведення заходів із захисту даних споживачів при автоматизованій обробці інформації, захисту засобів телекомунікацій і інформації, що передається телекомунікаційними мережами.

Нормативно-правову базу системи захисту інформації в програмно-керованих АТС складають Закони та держстандарти України, комплект НД ТЗІ [2…9].

1.1 Модель цифрового вузла комутації з позицій технічного захисту інформації

Для надання послуг якісного, надійного, безпечного телефонного зв'язку має бути сформована надійна захищена інфраструктура ЦАТС та ліній телекомунікацій з використанням доступних та ефективних засобів і способів інформаційного захисту. Розрізнені заходи щодо інформаційної безпеки, які приймаються при забезпеченні якості послуг, ефективності технічної експлуатації та управління ЦАТС, необхідно привести у єдину керовану комплексну систему інформаційної безпеки, яка має забезпечити:

- стійке функціонування ЦАТС та мережі телекомунікацій;
- попередження загроз їхній безпеці;

- захист законних інтересів підприємства від протиправних посягань;

- недопущення крадіжки фінансових засобів, розголошення, втрати, спотворення й знищення службової, технологічної, управлінської інформації;

- ефективну виробничу діяльність усіх підрозділів;

- підвищення якості наданих послуг та гарантії безпеки майнових прав та інтересів абонентів.

Згідно нормативно-правової бази технічний захист інформації спрямований на забезпечення:

- порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, що є об'єктом державної власності та охороняється згідно із законодавством;

- захисту, спрямованому на недопущення блокування інформації, що є державними інформаційними ресурсами, несанкціонованого ознайомлення з нею та/або її модифікації і, в тому числі, захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

- захисту від несанкціонованого доступу (НСД) до державних інформаційних ресурсів з боку мереж передачі даних, зокрема, глобальних мереж.

- порядку доступу, цілісності та доступності комерційної та відомчої конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в державних органах, підприємствах, установах та організаціях;

- захищеності відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює.

Конфіденційність інформації, яка є державним інформаційним ресурсом, під час передавання мережею забезпечує власник автоматизованої системи або оператор мережі передачі даних за договором із власником автоматизованої системи.

Заходи щодо технічного захисту конфіденційної інформації, що не належить державі, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами державних органів, підприємств, установ і організацій, встановлюються власником інформації або розпорядником.

Узагальнена модель інфраструктури цифрового вузлу комутації з позицій технічного захисту інформації показана на рисунку 1.1.

Обладнання ЦАТС поділяють на станційну частину, блоки абонентських виносів (БАВ) і мережу абонентських, з'єднувальних та міжстанційних цифрових та аналогових ліній, які є для порушника об'єктами несанкціонованого доступу до них, до інформації, що ними передається, і впливу на їх працездатність. На лініях може бути обладнання, встановлене порушником (ОВП).

Станційна частина виконує функції опорної станції або опорно-транзитної станції і з'єднана з іншими станціями міжстанційними з'єднувальними, а з блоками абонентського виносу – з'єднувальними цифровими лініями Е1 з потрібним числом підсилювальних та регенеративних ділянок. БАВ приєднується до опорної станції, як правило, за інтерфейсом V3.1, V3.2.

У якості міжстанційних з'єднувальних ліній можуть використовуватись цифрові канали Е1 з магістральної мережі SDH чи ATM.

Станційна частина цифрового вузла комутації має у своєму складі:

- підсистему комутації абонентських і з'єднувальних ліній (КАЗЛ);

- управляючий комплекс вузла комутації (УК) з автоматизованими робочими місцями операторів (АРМ оператора);

- підсистему технічної експлуатації (ПТЕ) вузла комутації, що дублюється у центрі технічної експлуатації цифрових вузлів комутації, звідки здійснюється віддалений контроль та управління вузлами.

Станційна частина цифрового вузла комутації взаємодіє з наступними технологічними мережами:

АСКР – автоматизована система контролю та розрахунків з абонентами для тарифікації наданих телефонних послуг;

TMN – мережа управління електрозв'язком для технологічного контролю та адміністративно-бізнесового менеджменту послуг;

IN – мережа надання інтелектуальних послуг;

SS7 – система сигналізації для управління процесом з'єднання;

СС – система синхронізації для отримання опорних тактових частот.

У станційній частині можуть бути виявлені програмні закладки та апаратні

закладні пристрої, які виконують не документовані функції і не контролюються системою технічної експлуатації вузла комутації.

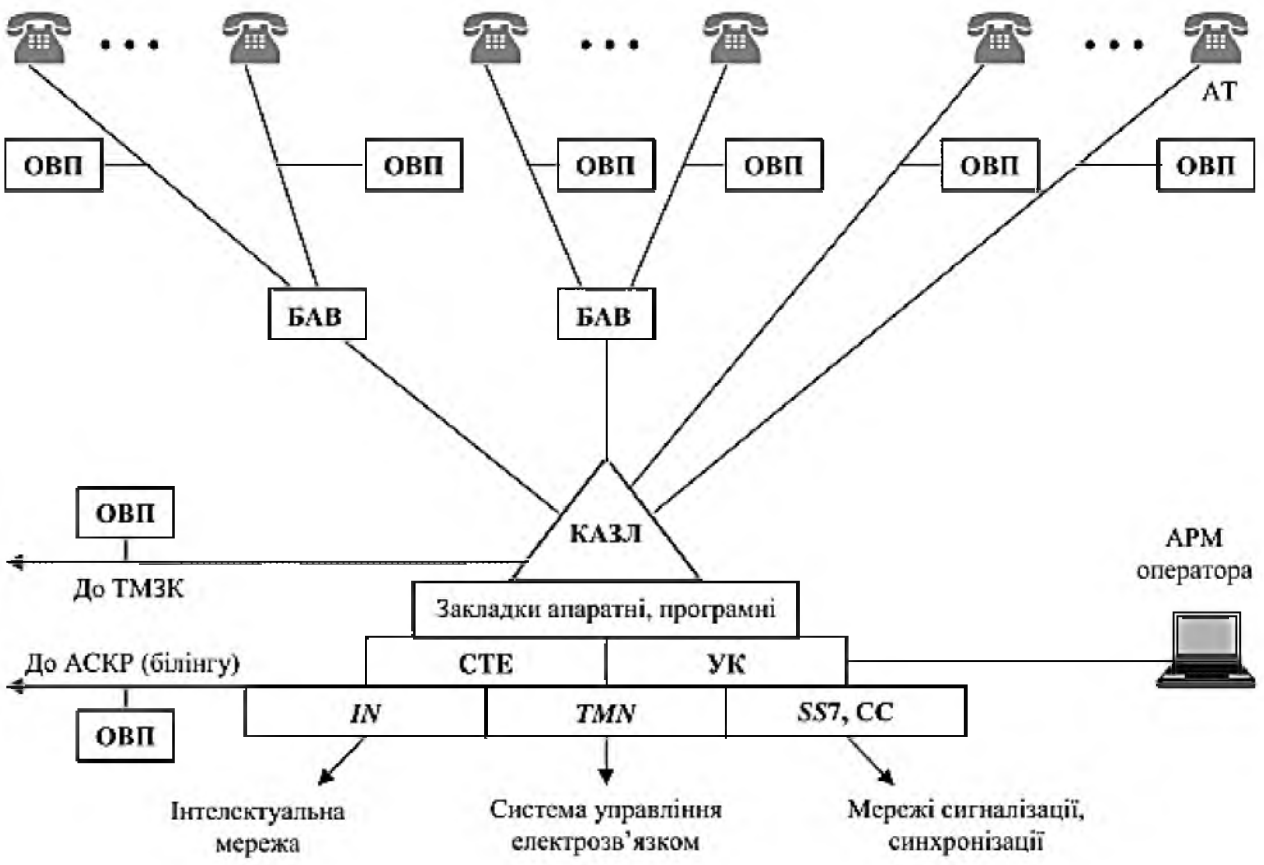

Рисунок 1.1 – Модель інфраструктури цифрового вузла комутації з позицій захисту інформації

Позначення: АРМ – автоматизоване робоче місце; АСКР – автоматизована система комплексних розрахунків з абонентами; АТ – абонентські термінали; БАВ – блок абонентського виносу; КАЗЛ – підсистема комутації абонентських та з'єднувальних ліній; ОВП – обладнання, встановлене порушниками; СС – система синхронізації; СТЕ – система технічної експлуатації; ТМЗК – телекомунікаційна мережа загального користування; УК – управляючий комплекс; IN - інтелектуальна мережа; TMN - мережа управління телекомунікаціями; SS7 – система сигналізації № 7.

Структурна схема станційної частини програмно-керованої АТС з позицій ТЗІ наведена на рис. 1.2 [1].

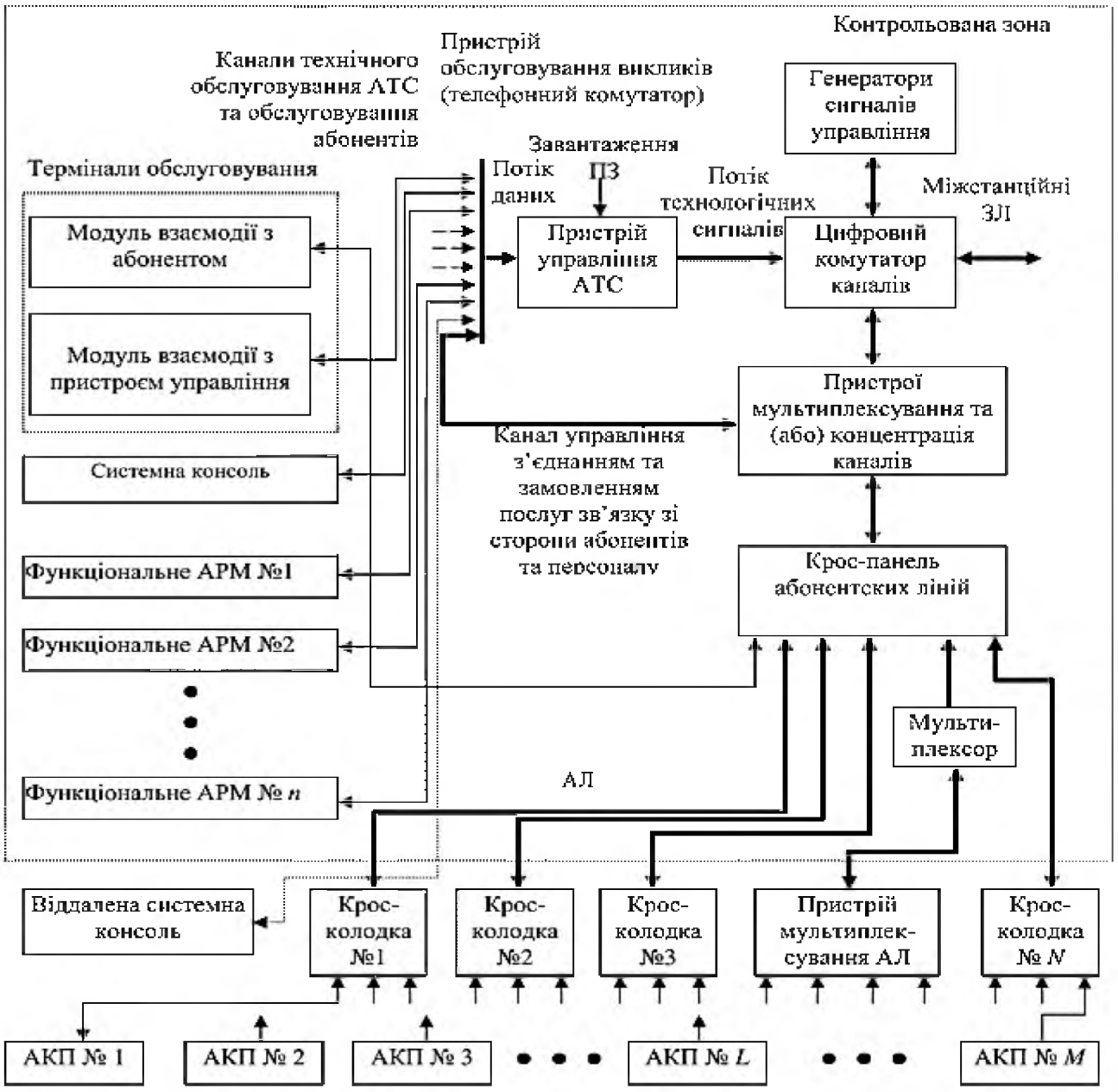

Рисунок 1.2 – Структурна схема станційної частини програмно-керованої АТС з позицій ТЗІ [1]

Позначення: АКП – абонентські кінцеві прилади (апарати); АЛ – абонентські лінії; АРМ – автоматизоване робоче місце; АТС – автоматична телефонна станція; ЗЛ – з'єднувальні (міжстанційні) лінії; ПЗ – програмне забезпечення; L – поточне число АКП; M – загальна кількість АКП (ємність станції); N – кількість кросових колодок; n – кількість АРМ; контрольована зона – територія,

де унеможливлюється присутність сторонніх осіб.

На схемі виділяються ті елементи станції, які мають безпосереднє відношення до процесів захисту інформації.

Станційне обладнання ЦАТС розміщується на об'єкті, який охороняється, де проводиться повний цикл організаційно-технічних заходів з комплексної інформаційної безпеки певного атестованого рівня.

Обладнання програмно-керованих АТС має захищеність базового рівня, яка забезпечується фірмою-виробником даного обладнання.

При встановленні обладнання на мережу рівень захищеності знижується за рахунок можливого впливу на саму систему зі сторони мережі каналами абонентського доступу, сигналізації, синхронізації, тарифікації і системи управління з віддалених терміналів.

Підсистема управління станцією містить у собі:

- спеціалізовані пристрої управління, що реалізують принцип програмного управління і складаються, здебільшого, з процесорів, пристроїв внутрішньої і зовнішньої пам'яті, периферійних пристроїв, спеціалізованих модулів управління сигналізацією, опрацювання викликів, надання послуг і деяких інших програмно-апаратних компонентів, які є характерними для комп'ютерної техніки;

- термінали обслуговування, що приєднані до пристроїв управління через канали технологічного обслуговування АТС і до підсистеми КАЗЛ - через канали інформаційного обслуговування абонентів.

Підсистема КАЗЛ (підсистема комутації абонентських та з'єднувальних ліній) містить у собі пристрої, що реалізують процеси комутації, мультиплексування та концентрації абонентських і міжстанційних з'єднувальних ліній, а також компоненти устаткування абонентських ліній зв'язку - абонентські кінцеві пристрої, фізичні лінії зв'язку, пристрої мультиплексування абонентських ліній, станційні абонентські комплекти тощо.

На виходах підсистеми управління утворюються в реальному часі потоки технологічних сигналів, за допомогою яких має місце процес управління підсистемою КАЗЛ. З іншого боку, абонентські прикінцеві пристрої мають

можливість обмінюватися керуючою інформацією з підсистемою управління станцією через канали управління з'єднаннями й замовлення послуг.

Незалежність підсистем управління станцією і КАЗЛ розуміється в тому сенсі, що підмножина загроз для інформації, яка характерна для підсистеми управління станцією, не перетинається з підмножиною загроз, яка характерна для підсистеми КАЗЛ, за передумовою відсутності механізмів реалізації загроз на підсистемі управління з боку підсистеми КАЗЛ і, навпаки, на підсистемі КАЗЛ з боку підсистеми управління станцією.

Коректність такої декомпозиції структури програмно-керованих АТС обумовлена прийнятими щодо них проектними рішеннями, що не передбачають:

- можливостей штатних впливів на підсистему управління станцією з боку абонентських прикінцевих пристроїв, за винятком можливості запуску абонентом задач із фіксованого набору, що реалізують заздалегідь передбачені функції замовлення абонентом додаткових видів послуг, які надаються станцією;

- можливостей штатних впливів на інформацію в розмовних трактах із боку підсистеми управління станцією, за винятком можливості штатних приєднань до вже встановлених з'єднань (наприклад, із боку телефонного комутатора або абонентських прикінцевих пристроїв у режимі конференцзв'язків), однак з обов'язковим оповіщенням учасників розмови про всі додаткові підключення до їхніх розмовних трактів (зокрема, фоновими тональними сигналами).

Відносність незалежності вищезгаданих підсистем розуміється в тому сенсі, що за певних умов внаслідок помилок або некоректних (зокрема, зловмисних) дій, які були допущені на передексплуатаційних стадіях життєвого циклу АТС (наприклад, при установці програмних закладок або апаратних закладних пристроїв), або внаслідок якісної недостатності АТС, однак, можливі реалізації загроз на підсистемі управління з боку підсистеми КАЗЛ, і, навпаки, на підсистемі КАЗЛ з боку підсистеми управління станцією.

Далі розглянемо загрози інформації та моделі порушників, які їх здійснюють.

1.2 Загрози для інформації та моделі порушників

1.2.1 Основні загрози інформаційним ресурсам вузла комутації

В інформаційній сфері України відокремлені загрози національній безпеці:

- прояви обмеження свободи слова та доступу громадян до інформації;
- комп'ютерної злочинності та комп'ютерного тероризму;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення невірогідної, неповної або упередженої інформації.

Передумовами можливого витоку інформації, порушення її цілісності, блокування та НСД, безконтрольного та неправомочного доступу до інформації та її використання є:

- комунікаційне обладнання іноземного виробництва, використане у мережах зв'язку, яке передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв'язку та змістом повідомлень, які пересилаються. Використання великої кількості засобів зв'язку іноземного виробництва створює можливість втручання іноземних спецслужб в роботу мереж зв'язку шляхом руйнування програмних засобів в певний момент або створення каналів несанкціонованого впливу на інформацію, а також приводить до зростання залежності операторів зв'язку від закордонних виробників програмно-апаратних засобів зв'язку. В закордонній апаратурі можуть бути "закладки" додаткових, не відображених в технічних характеристиках режимів роботи. Активізація таких режимів може здійснюватись як випадково, в процесі роботи оператора, так і дистанційно порушником, що призводить до втрати або зміни даних, помилок у програмному забезпеченні або паралельному підключенні до каналів;

- прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна легко підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо-, радіотехнічної, оптико-електронної, теплової, акустичної, хімічної, магнітометричної та радіаційної розвідок;

- злочинна діяльність, спрямована на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;

- діяльність громадських формувань, політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, спрямована на одержання переваги у політичній боротьбі та конкуренції;

- розміщення на державних та спільних об'єктах зв'язку технологічного обладнання спільних підприємств та представництв інофірм, що вимагає проведення додаткових заходів із забезпечення вимог ТЗІ;

- зростання зацікавленості іноземних розвідок питаннями промислової, комерційної діяльності, ресурсів в Україні;

- відсутність системи атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;

- відсутність політики безпеки систем комутації та телекомунікаційних мереж, де б формулювались вимоги щодо захисту від загроз працездатності, підтримання режиму конфіденційності та відсутності несанкціонованого доступу.

- нелегальне використання ресурсів операторів для несанкціонованого надання послуг зв'язку, що знижує доходи останніх;

- різні фрагменти мережі експлуатуються різними операторами з різними формами власності.

Загрози інформаційній безпеці є при забезпеченні:

1) конфіденційності:

- крадіжка (копіювання) інформації та засобів її обробки;

- утрата (ненавмисна утрата, витік) інформації та засобів її обробки;

2) доступності:

- блокування інформації;

- знищення інформації та засобів її обробки;

3) цілісності:

- модифікація (спотворення) інформації;

- заперечення справжності інформації;

- нав'язування хибної інформації.

4) спостережності:

- блокування;

- модифікація інформації;

- маскування інформації;

5) порядку маршрутизації трафіка:

- крадіжка трафіка;

- несанкціоноване використання послуг та інформаційних ресурсів телекомунікаційних мереж.

Детально загрози інформаційній безпеці, а саме безпеці вузлів комутації, а також перелік інформації, яка захищається, наведені в 1[8].

Джерела загроз інформаційній безпеці поділяють на три групи.

1 Обумовлені зловмисними чи випадковими діями суб'єкта (антропогенні джерела загроз).

2 Обумовлені технічними засобами (техногенні джерела загроз).

3 Обумовлені природними стихійними джерелами.

До антропогенних джерел загроз відносять:

1 Зовнішні антропогенні джерела загроз:

- кримінальні структури;

- потенційні злочинці та хакери;

- недобросовісні партнери, конкуренти, представники сторонніх організацій, відвідувачі;

- технічний персонал постачальників;

- представники організацій нагляду та аварійних служб;

- представники силових структур.

2 Внутрішні антропогенні джерела загроз:

- основний персонал (користувачі-оператори, системні і прикладні програмісти, розробники, оператори баз даних, оператори вводу даних);

- представники служби захисту інформації (системні і мережеві адміністратори, адміністратори безпеки);

- керівництво;

- технічний персонал (життєзабезпечення, експлуатації);

- допоміжний персонал (прибиральники, охорона);

- співробітники, звільнені з роботи.

Особливу групу внутрішніх антропогенних джерел загроз складають особи з порушеною психікою, впроваджені та завербовані агенти (іноземні агенти, що збирають інформацію, корпоративні розвідники) з числа основного, допоміжного та технічного персоналу, представників служби захисту інформації.

До техногенних джерел загроз відносять

1 Зовнішні техногенні джерела загроз:

- засоби службового зв'язку;

- мережі інженерних комунікацій (водопостачання, каналізації, вентиляції);

- засоби пожежної, охоронної сигналізації;

- транспорт;

2 Внутрішні техногенні джерела загроз:

- неякісні технічні засоби комутації та обробки інформації;

- неякісні програмні засоби управління та обробки інформації;

- допоміжні засоби;

- інші технічні засоби, що застосовуються в ЦАТС.

Природними зовнішніми джерелами загроз є пожежі, землетруси, повені, урагани, магнітні бурі, радіоактивне випромінювання, різні непередбачені обставини, не пояснювані явища, інші форс-мажорні обставини: різні рішення вищих державних органів, забастовки, війни, революції тощо.

При складанні окремої моделі порушника орієнтуються на конкретний об'єкт

захисту, враховують мотиви дій і соціально-психологічні аспекти порушення, потенційні можливості доступу до інформаційних ресурсів різних категорій зовнішніх та внутрішніх порушників на різних просторово-часових зрізах об'єкта захисту.

1.2.2 Модель порушника безпеки

Детальну класифікацію моделей порушників антропогенного типу, їх рівні можливостей, основні способи реалізації загроз для інформації програмно-керованих АТС наведено у [8]. Класифікація проводиться за рівнем можливостей, який надається їм штатними засобами. Виокремлено чотири рівні можливостей реалізації НСД:

1 – (найнижчий рівень можливостей) – запускання програм (задач) із фіксованого набору, який реалізує передбачені функції щодо обробки інформації. Це обслуговуючий персонал, котрий забезпечує експлуатацію обладнання ЦАТС. Інженери-електронники ЦАТС, які, користуючись автоматизованим робочим місцем (АРМ) та комутаційною системою, можуть мати доступ до інформації абонента. Вони мають можливість приєднувати до ЦАТС закладні пристрої.

2 – можливість створювання та запускання власних програм з новими функціями щодо обробки інформації. Це оператори даного або інших вузлів комутації. Користуючись комплектом або модулем з'єднувальної лінії, вони мають доступ до програмного забезпечення (ПЗ) АРМ, функціонального й спеціалізованого ПЗ та до баз даних. Типові можливості полягають у передаванні сигналів, як передбачених, так непередбачених у відповідних інтерфейсах.

3 – можливість управління роботою обчислювального комплексу, тобто можливість впливу на базове ПЗ ЦАТС та на склад і конфігурацію обладнання. Це оператори ЦАТС. Користуючись АРМ, вони мають доступ до баз даних, ПЗ АРМ, функціонального й спеціалізованого ПЗ та інформації абонентів. Типові можливості такого порушника: формування штатних команд, запускання задач, не задекларованих у технічній документації, несанкціоноване приєднання до інформаційних трактів.

4 – весь обсяг можливостей суб'єктів, здійснюючих проектування, реалізацію та ремонт технічних засобів, до залучення у склад обладнання власних технічних засобів з новими функціями. Це програмісти, котрі беруть участь у розробленні та виготовленні обчислювальних комплексів. Користуючись АРМ і пристроями управління, вони здатні впливати на функціональне та спеціалізоване ПЗ і на ПЗ АРМ. Типові можливості такі: впровадження програмних закладок, впровадження шкідливих кодів (вірусів), помилки у ПЗ та комутаційній системі.

Якщо на вузлі комутації немає програмних та апаратних закладок, то звичайний абонент мережі практично не має можливості впливати на управляючу систему телефонної станції. Регламентовані для цифрових та аналогових терміналів користувача основні й додаткові послуги не можуть впливати на роботу управляючого комплексу в цілому. Абонент може діяти лише через абонентський комплект. Він здатний активізувати програмне закладення, дістати інформацію інших абонентів через несправності обладнання ЦАТС.

Продовжимо розгляд загроз інформації від зовнішніх, по відношенню до ЦАТС, джерел.

Загрози інформаційній безпеці можут бути різноманітними і довільного походження за часом, тривалістю, факторами та наслідками.

Зрив роботи ЦАТС можливий при зупинці системи електроживлення або виведенні її з ладу порушником.

Можливе впровадження "вірусу" – мікропрограми, здатної самостійно розмножуватись і поширюватись у мережі.

Пристрої обробки інформації, котрі є складовою частиною цифрового вузла комутації, це ЕОМ зі стандартною архітектурою, для яких можна створювати засоби нападу, віруси тощо.

Можливості стосовно здійснення загроз залежать від місцезнаходження порушника. Якщо порушник перебуває поза межами ЦАТС, то його можливості залежать від того, чи є засоби захисту інформації у системі тарифікації (припускається чи не припускається віддалене приєднання легальних користувачів до системи тарифікації), засоби безпеки при виході на мережу SS-7 та TMN, при

приєднанні до Інтернет.

Якщо таких засобів захисту немає, то можливі впливи порушника через зовнішні інтерфейси обладнання, системи сигналізації на абонентських та з'єднувальних лініях.

Загрози стосовно захищеності збільшуються при інтеграції у цифрові комплекси нових функцій, а саме: часткова (приватна) віртуальна мережа (VPN), що забезпечує внутрішній офісний зв'язок та зв'язок з філіалами; функції білінгу на базі локальної мережі; вихід на глобальну мережу – Інтернет, а також використання в мережі імпортних програмно-апаратних комплексів.

Існує небезпечна загроза крадіжки трафіка при сумісному використанні системи зв'язку різними операторами. Захист досягається використанням міжмережевих екранів, шлюзів по каналам управління, синхронізації та сигналізації, здійсненням контролю трафіка і тарифікації.

Для розрахунку рівня загроз створено відповідні таблиці (1.1 – 1.6), які дозволили розрахувати ефективний рівень загроз та визначити профілі можливостей порушників усіх категорій (таблиця 1.7).

Таблиця 1.1 - Категорії порушників, що визначені в моделі

Позначення	Визначення категорії	Потенційний рівень загрози
П1	Системний адміністратор ЦАТС EWSD	5
П2	Адміністратор безпеки	5
П3	Користувачі	4
П4	Відвідувачі	2
П5	Технічний персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти ЦАТС EWSD	3
П6	Персонал, який обслуговує технічні засоби (інженери, техніки)	3
П7	Представники організацій, що взаємодіють з питань обслуговування ЦАТС EWSD, технічного забезпечення та підтримки її функціональності	3
П8	Сторонні особи, що знаходяться за межами контрольованої території вузлів ЦАТС EWSD	2

Таблиця 1.2 - Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Ефективний рівень загрози
М1	Безвідповідальність (недбалість)	3
М2	Корислива цілеспрямованість	5

Таблиця 1.3 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ЦАТС EWSD

Позначення	Основні кваліфікаційні ознаки порушення	Ефективний рівень загрози
К1	Не володіє знаннями та інформацією про порядок функціонування ЦАТС EWSD, не має навичок щодо користування штатними засобами системи	1
К2	Має навички щодо користування ПК на рівні користувача	2
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення й операційних систем і практичними навичками роботи із засобами, що реалізовані в ЦАТС EWSD	4
К4	Володіє знаннями щодо функціонування засобів і механізмів захисту, що використовуються у ЦАТС EWSD, і їх недоліків	5

Таблиця 1.4 - Специфікація моделі порушника за показником можливостей використання засобів ЦАТС EWSD для реалізації загроз

Позначення	Основні кваліфікаційні ознаки порушення	Ефективний рівень загрози
З1	Має фізичний доступ до автоматизованого робочого місця ЦАТС EWSD, але не є користувачем ЦАТС EWSD	1
З2	Має можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації	3
З3	Має можливість керування функціонуванням елементів ЦАТС, тобто конфігурує ПЗ та комплекс засобів захисту ЦАТС EWSD.	5
З4	Не має фізичного доступу до ресурсів ЦАТС EWSD	1

Таблиця 1.5 - Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушення	Ефективний рівень загрози
Ч1	Під час бездіяльності компонентів системи (під час планових перерв в роботі)	4
Ч2	Під час функціонування ЦАТС EWSD	5
Ч3	Під час перерв в роботі для обслуговування та ремонту	3

Таблиця 1.6 - Специфікація моделі порушника за місцем дії

Позначення	Характеристика можливостей порушення	Ефективний рівень загрози
Д1	Усередині будівель та приміщень, але без доступу до технічних засобів ЦАТС EWSD	1
Д2	З робочих місць користувачів	5
Д3	З інших об’єктів ЦАТС EWSD, у тому числі каналів зв'язку	2

Ефективний рівень (рейтингова оцінка) загроз: 1 – незначний (низький); 2 – нижчий за середній; 3 – середній; 4 – вищий за середній; 5 – значний (високий). М1, М2 – категорії порушника за мотивами здійснення порушень; К1-К4 - категорії порушника за рівнем кваліфікації ; З1-З4 – категорії порушника за рівнем кваліфікації ; Ч1-Ч3 – категорії порушника за часом дії; Д1-Д3 – категорії порушника за місцем дії

Таблиця 1.7 - Профілі можливостей порушників усіх категорій

Позначення	Визначення категорії	Характер дії порушника					Ефективний рівень загроз
		Мотив порушника	Кваліфікація	Можливості	Час дії	Місце дії	
П1	Системний адміністратор ЦАТС EWSD	М1, М2	К4	З3	Ч1-Ч3	Д2, Д3	5
П2	Адміністратор безпеки ЦАТС EWSD	М1, М2	К4	З3	Ч1-Ч3	Д2, Д3	5
П3	Користувачі	М1, М2	К2-К4	З3	Ч1-Ч3	Д2, Д3	4
П4	Відвідувачі	М1, М2	К1-К4	З1	Ч2	Д2, Д3	3
П5	Технічний персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти ЦАТС EWSD	М1, М2	К1-К4	З2	Ч1-Ч3	Д2	3
П6	Персонал, який обслуговує технічні засоби (інженери, техніки)	М1, М2	К1-К4	З2	Ч1-Ч3	Д2	3
П7	Представники організацій, що взаємодіють з питань обслуговування ЦАТС EWSD, технічного забезпечення та підтримки її функціональності	М1, М2	К1-К4	З3	Ч1-Ч3	Д3	4
П8	Сторонні особи, що знаходяться за межами контрольованої зони вузлів ЦАТС EWSD	М2	К1-К4	З4	Ч1-Ч3	Д3	2

1.2.3 Загрози інформаційним ресурсам ЦАТС від приєднаних технологічних мереж

У межах контрольованої зони ЦАТС може встановлюватись різноманітне устаткування телекомунікаційних мереж. Частина цього обладнання приєднується безпосередньо до обладнання ЦАТС і може впливати на її роботу.

Зокрема, це система сигналізації і синхронізації, система централізованого управління та технічної експлуатації, з'єднувальні та абонентські лінії, системи передавання до АСКР тощо.

Можливі варіанти інформаційного нападу на мережі зв'язку.

Мережа зв'язку складається з вузлів комутації та систем передачі і її можна розглядати, як програмну інформаційну систему з безліччю зовнішніх зв'язків. Розглядають такі загрози:

- загроза атаки через АРМ адміністратора;
- загроза несанкціонованого входу в АРМ адміністратора;
- загроза модифікації системного або програмного забезпечення адміністрування вузла зв'язку;
- загроза зараження файлів комп'ютерними вірусами;
- загроза прослуховування та модифікація трафіка;
- загроза модифікації апаратної частини АРМ, АТС, SS7 і лінійної апаратури (вставка чужого пристрою);
- загроза відмови в обслуговуванні;
- загроза атаки через систему віддаленого програмування та діагностики;
- загроза атаки через систему сигналізації та управління;
- загроза атаки наведеним сигналом;
- загроза атаки абонентськими лініями;
- загроза атаки через мережу електроживлення;
- загроза атаки через системи тарифікації і записи переговорів;

Ці загрози розділяють на загрози на рівні програмного забезпечення, апаратної частини, середовища розробки і середовища експлуатації.

Більшість загроз на системи зв'язку складають атаки на програмному рівні.

Тому необхідно відслідковувати можливість входу у систему програмування або управління системами зв'язку.

Входи в програмне забезпечення АТС і системи передачі можуть бути легальними і нелегальними. До легальних входів відносяться зв'язок з системою віддаленого програмування і діагностики та з локальною системою програмування і тарифікації.

Решта входів - нелегальні. При цьому у сучаснх АТС вхід віддаленого програмування може бути заблоковано парольним захистом або фізичним відключенням. В інтелектуальних мережах вказаний вхід функціонує і відключений бути не може. За рівнем небезпечності ці загрози можна розділити на такі основні рівні:

а) найбільш небезпечним є вхід віддаленого програмування та діагностики АТС, який функціонально призначений для безпосереднього втручання в програмне забезпечення систем зв'язку. Наслідки такого втручання можуть бути будь-якими, навіть до зупинки системи або мережі зв'язку. При цьому неможливо оперативно усунути причин збою системи та усі несправності,оскільки немає можливості здійснити протоколювання усіх дій зі сторони віддаленого доступу в систему управління;

б) вхід локального програмування і тарифікації також небезпечний для програмного забезпечення, але доступ до нього обмежено персоналом станції і безпека може бути забезпечена організаційними заходами. Втручання може бути легко визначене при дотриманні усіх вимог експлуатації: дії обслуговуючого персоналу завжди протоколюються;

в) напад абонентськими та з'єднувальними лініями, а також зі сторони системи сигналізації може бути проведений через активізацію «закладок», що відкривають по кодовому сигналу доступ до ПЗ АТС і систем передачі з вказаних напрямків. Закладки можуть бути створені на програмному та апаратному рівнях;

г) напад наведеним сигналом (наприклад, з космічного об'єкта) може бути здійснено через апаратні «закладки» разом із програмними «закладками». Можуть бути направлені на виведення обладнання з ладу застосуванням потужних

електромагнітних імпульсів;

д) може бути «внутрішній» напад, який забезпечено закладкою у ПЗ, що спрацьовує від лічильника, дати або інших внутрішніх факторів.

Крім того, практично все існуюче ПЗ систем передачі має обмеження за часом. По закінченні часу підтримки даної версії необхідно або купувати нову, або експлуатувати стару на свій страх і ризик.

Загрози, що реалізуються через систему сигналізації. Застосування сигналізації SS7 дозволяє здійснювати певні функції управління окремими вузлами зв'язку, при якому може бути нанесена значна шкода оператором зв'язку.

Системи сигналізації забезпечують передавання різноманітних сигналів управління, в тому числі цифр номера, які через функціональні елементи комутаційної системи надходять для аналізу в управляючий комплекс. В цьому разі можливі різні варіанти використання сигналів управління для активізації програмних закладок, наприклад таких:

- використання режиму типу "додаткова послуга", яка не декларується в документації;

- використання абонентського номера чи коду для активації програмної закладки;

- певні короткочасні маніпуляції з абонентською трубкою.

Система сигналізації SS7, крім вищезазначених можливостей, потенційно надає додаткові можливості організації НСД. У складі SS7 є підсистеми забезпечення можливостей транзакцій (TCAP) та прикладних підсистем, які організуються на них - такі, як підсистема рухомого зв'язку GSM (MAP), підсистема інтелектуальних мереж (INAP), підсистема експлуатації, техобслуговування, адміністрування та управління (OMAP) та інші. До загроз від застосування SS7 також належать:

- інтерфейси, спеціалізовані для нетелефонних функцій (TCAP, OMAP тощо) системи SS7, можуть бути використані для прихованого введення команди, яка реалізує несанкціонований вплив на ЦАТС;

- в SS7 організовується доступ до мережевих баз даних. Виникає загроза

їхнього навмисного спотворення, що може спричинити порушення роботи мережі.

Для захисту від можливого впливу необхідно здійснювати фільтрацію загальноканальної сигналізації та протоколювання повідомлень.

Загрози, що реалізуються за допомогою системи централізованого управління. Якщо порушник перебуває всередині ЦАТС, то, навіть якщо наявні засоби безпеки при реалізації систем тарифікації, засоби безпеки при виході на мережу SS7 та TMN, засоби захисту при приєднанні до Інтернету, то він має багато можливостей для здійснення загроз. Порушник з правами оператора УК може здійснювати НСД шляхом формування штатних команд, запускати програми, нерегламентовані в технічній документації. Порушення доступу відбувається в разі:

- модифікації баз даних (встановлення несанкціонованих режимів технічної експлуатації та видів обслуговування);

- ознайомлення з конфіденційною інформацією баз даних (адресами вхідних та вихідних з'єднань, часом встановлення з'єднання, режимами зв'язку, додатковими використовуваними видами обслуговування);

- зупинки та перезапускання ЦАТС (порушення зв'язку);

- заміни ПЗ (нове інстальоване ПЗ може мати програмні закладення).

Основні можливі варіанти захисту при забезпеченні захисту від впливу через систему управління, як самої критичної ланки, це впровадження жорсткого розмежування прав доступу до інформаційних ресурсів, як на фізичному, так і на програмному рівнях, адміністрування і протоколювання усіх операцій.

Найбільш підпадають під загрози ПЗ АРМ, якщо вони функціонують на базі ПЕОМ і використовують для роботи операційну систему Windows чи MS-DOS. Функціональне та спеціалізоване ПЗ, як правило, зашите у постійні запам'ятовувальні пристрої. Проникнення в операційну систему вузла комутації вважається практично неможливим.

Оскільки найгірший результат нападу - це руйнування системи зв'язку в цілому або окремих її фрагментів, то в цифрових АТС і системах цифрової передачі даних SDH, PDH (радіорелейних, кабельних, волоконно-оптичних)

найбільш вразливим елементом виявляється програмне забезпечення, яке піддається нападу в першу чергу. При цьому, якщо захистити програмне забезпечення від несанкціонованого втручання, з достатньою ймовірністю забезпечується цілісність мережі та її елементів.

Оскільки сучасне обладнання цифрового зв'язку базується на комп'ютерних технологіях, питання забезпечення інформаційної безпеки найбільш ефективніше можуть бути вирішені спеціалістами з обчислювальної техніки, які мають відповідний досвід.

Загрози на абонентських та з'єднувальних лініях. Стосовно абонентських, з'єднувальних та міжстанційних ліній зв'язку виділяють:

- загрози від випадкових дій (впливів) порушників;
- загрози від зловмисних дій порушників;
- загрози безпеці.

Аварії можуть бути викликані впливами техногенного (в результаті земляних та будівельних робіт в районах кабельних трас, розбою та зловмисної диверсійної діяльності) чи природного характеру (промерзання та деформація кабелю у зимовий період). Інформаційна безпека підтримується чіткою стандартною плановою організацією ремонтно-відновлювальних робіт та прогнозуванням ресурсів, необхідних для ліквідації наслідків аварії.

В лінійних трактах, на їх елементах, порушник може успішно здійснювати тривалий, практично не виявляємий, НСД до інформації за допомогою спеціальних засобів доступу до аналогових і цифрових каналів, здійснювати виведення на запис, прослуховування або ретрансляцію несанкціоновано одержаних даних та мови. Захист в такому разі здійснюється плановим патрулюванням (пішим чи моторизованим) кабельних трас та посиленням контролю в періоди вирішення важливих задач. Часто застосовують шифрування інформації.

Загрози інформації в цифрових системах передачі. Цифрові системи передавання мають вразливості на фізичному, канальному та мережевому рівнях стеку протоколів передавання (OSI7).

На фізичному рівні порушник прагне НСД до інформаційної сфери, як правило, шляхом встановлення спеціалізованого обладнання в канали доступу або

в магістральні канали. Можливий НСД через консолі управління або активізацією “закладок”, впроваджених в об’єктах цифрових систем передавання. Закладки можуть бути активізовані за допомогою радіоканалів. Після одержання НСД на фізичному рівні атака порушника може розвиватись на канальному і мережному рівнях стека протоколів.

На канальному рівні порушник може виконувати дії на активізацію вразливості відповідних протоколів. Порушник може одержати доступ до інформації, активізувати “закладку” формуванням спеціальних команд в кадрах (комірках, контейнерах) даних. Команди можуть розміщуватись в заголовку, в полі даних, в полі контрольної суми. Небезпечні атаки блокування передавання повідомлень, що можуть бути реалізовані несанкціонованим формуванням прикмет перевантаження, та які викликають масові повтори передачі.

На мережевому рівні активізуються вразливості протоколів цього рівня. Порушник може отримати НСД до інформації і провести атаки типу блокування передавання, блокування доступу тощо.

1.3 Загальні положення безпеки інформаційних ресурсів у програмно-керованих АТС

Згідно Закону “Про телекомунікації” в ЦАТС та телекомунікаційних мережах повинна бути забезпечена інформаційна безпека телекомунікаційних мереж, тобто здатність телекомунікаційних мереж забезпечувати захист від:

- знищення інформації;
- перекручення інформації;
- блокування інформації;
- несанкціонованого витоку інформації;
- порушення встановленого порядку маршрутизації інформації.

Необхідною умовою для забезпечення інформаційної безпеки є:

- реалізація сталості телекомунікаційної мережі, тобто властивості телекомунікаційної мережі зберігати повністю, або частково, свої функції за умови впливу на неї дестабілізуючих чинників;

- реалізація забезпечення надійності телекомунікаційних мереж;

- захист інформації сигналізації, синхронізації та управління вузлами доступу, вузлами комутації, вузлами надання послуг та телекомунікаційною мережею в цілому, яка містить важливі для підприємства відомості, порушення цілісності, доступності та конфіденційності яких може привести до моральних чи матеріальних збитків.

Реалізація необхідних умов інформаційної безпеки має проводитись з урахуванням їх технологічних особливостей на основі єдиних стандартів, норм та правил, оскільки в інформаційно-телекомунікаційній мережі мають бути визначені ролі суб'єктів служби захисту.

Згідно Законів України "Про основи національної безпеки України", "Про телекомунікації" та інших нормативно-правових документів оператор у сфері діяльності з питань, пов'язаних з формуванням, використанням та захистом національних ресурсів має забезпечити інформаційну безпеку в таких напрямках:

- установлювати спеціальний режим доступу відповідно до законодавства на об'єктах телекомунікацій, а також в окремих структурних підрозділах, де передається, обробляється або зберігається інформація з обмеженим доступом, що є власністю держави;

- вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію й функціонування телекомунікаційних мереж та інформації, що передається цими мережами в інтересах задоволення потреб національної безпеки, оборони та охорони правопорядку;

- забезпечувати готовність телекомунікаційних мереж зв'язку до роботи в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, у тому числі можливість оповіщення своїх споживачів у цих умовах, взаємодіючи при цьому з національним центром оперативно-технічного управління мережами телекомунікацій України в питаннях, віднесених до компетенції оператора;

- встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах

своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення відповідно до діючого законодавства. Оператор телекомунікацій зобов'язаний забезпечувати захист зазначених технічних засобів від несанкціонованого доступу;

- задовольняти вимоги споживачів щодо збереження конфіденційності інформації, яка стосується споживача, забезпечувати та нести відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі номенклатури отримання послуг, їх тривалості, змісту, оплати, маршрутів передавання тощо. Зокрема, під час автоматизованої обробки інформації про абонентів необхідно забезпечувати її захист відповідно до закону;

- забезпечувати під час замовлення та/або надання телекомунікаційних послуг фіксованого телефонного зв'язку безпеку телекомунікаційних послуг та надавати споживачам послуги за встановленими показниками якості та захищеності телекомунікаційних послуг;

- забезпечити таємницю зв'язку згідно із законодавством, охорону таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передається технічними засобами телекомунікацій, та інформаційну безпеку телекомунікаційних мереж;

- додержуватися встановленого нормативно-правовими актами порядку маршрутизації трафіка, забезпечити резервування технічних засобів телекомунікацій, фрагментів телекомунікаційних мереж і альтернативні маршрути в разі пошкодження при надзвичайних ситуаціях у телекомунікаційній мережі загального користування;

- вживати заходів для недопущення несанкціонованого доступу до телекомунікаційних мереж та інформації, що передається цими мережами. Зняття інформації з телекомунікаційних мереж заборонено, окрім випадків, передбачених законом.

Заходи та засоби захисту телекомунікаційних мереж та інформації, що циркулює ними, мають застосовуватись на всіх, без винятку, етапах їх життєвого

циклу:

- розробки технічного завдання чи технічних умов на створення, техніко-робочого проектування, будівництва, здавання до експлуатації, власне експлуатації, виведення з експлуатації та утилізації;

- на етапах погодження засобів телекомунікацій, які можуть застосовуватися в телекомунікаційних мережах. Одними з критеріїв прийняття рішень є забезпечення надійності та безпеки мереж телекомунікацій. Розвиток та вдосконалення телекомунікаційних мереж має проводитись з урахуванням технологічної цілісності всіх мереж та їх інформаційної безпеки. Договори на постачання телекомунікаційних засобів та обладнання мають включати в себе вимоги щодо інформаційної безпеки ЦАТС;

- етапи будівництва, реконструкції й модернізації телекомунікаційних мереж не повинні призводити до зниження надійності та рівня захищеності ЦАТС. Проекти будівництва, реконструкції та модернізації телекомунікаційних мереж, і в тому числі проекти комплексних систем захисту інформації, підлягають експертизі в порядку, встановленому законодавством;

- на етапі технічної експлуатації телекомунікаційних мереж оператором телекомунікацій ця діяльність повинна здійснюватись тільки за умови наявності проектної документації, розробленої у відповідності до норм технологічного проектування та вимог керівних нормативних документів, зокрема вимог нормативних документів сфери технічного захисту інформації (ТЗІ). Технічне обслуговування технічних засобів телекомунікацій та каналів електрозв'язку повинне забезпечуватись у відповідності до нормативних та технічних документів, чинних у сфері телекомунікацій і, зокрема, нормативних документів сфери ТЗІ.

Згідно законодавства України в телекомунікаційних мережах загального користування, які надаються системі урядового зв'язку, національній системі конфіденційного зв'язку, органам з надзвичайних ситуацій, безпеки, оборони, внутрішніх справ України в інтересах задоволення потреб національної безпеки, оборони, охорони правопорядку, обов'язковий ТЗІ спрямовано на забезпечення конфіденційності, цілісності та доступності інформації, що циркулює в

телекомунікаційній мережі та її системах управління.

Щодо порядку захисту державних інформаційних ресурсів, тобто інформації, яка є власністю держави та (або) необхідність захисту якої визначено законодавством, діють положення нормативно-правових документів:

- в автоматизованих системах повинен забезпечуватися захист від несанкціонованого доступу (НСД) до державних інформаційних ресурсів з боку будь-яких мереж передачі даних;

- конфіденційність інформації, яка є державними інформаційними ресурсами, під час передавання мережею передачі даних забезпечує власник автоматизованої системи або оператор мережі передачі даних за договором із власником автоматизованої системи;

- захист державних інформаційних ресурсів у мережі передачі даних повинен забезпечуватися впровадженням на кожному з її вузлів комутації комплексу технічних, криптографічних, організаційних та інших заходів і засобів захисту інформації, спрямованих на недопущення її блокування та/або модифікації;

- розроблення, виробництво, впровадження та обслуговування комплексної системи захисту інформації (КСЗІ) здійснюється оператором мережі передачі даних самостійно за умови наявності у нього ліцензії на проведення відповідних видів робіт, або сторонньою організацією, яка має ліцензію на проведення даних видів робіт;

- передавання державних інформаційних ресурсів дозволяється тільки через вузли комутації, що мають атестат відповідності КСЗІ вимогам із захисту інформації згідно нормативних документів з ТЗІ;

- під час підключення до глобальних мереж абоненти повинні дотримуватися вимог законодавства щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

Система інформаційної безпеки повинна впорядкувати контроль за критичною, з точки зору підприємства, інформацією, застосуванням нових технологій, попередженням подій, що можуть привести до порушення працездатності телекомунікаційних систем або до збитків внаслідок порушення інформаційної безпеки.

1.4 Організація та порядок технічного захисту інформації в ЦАТС

Для успішної технічної експлуатації КСЗІ на ЦАТС з досягненням заданого рівня захищеності інформаційних ресурсів та рівня гарантій захисту необхідно правильно організувати заходи з ТЗІ на всіх попередніх етапах створення КСЗІ, зокрема на стадіях побудови та здавання в експлуатацію.

1.4.1 Організація ТЗІ на стадії побудови ЦАТС

Заходи та засоби захисту телекомунікаційних мереж та інформації, що циркулює ними, мають застосовуватись на всіх, без винятку, етапах їх життєвого циклу: розробки технічного завдання чи технічних умов на створення, техніко-робочого проектування, будівництва, здавання до експлуатації, власне експлуатації, виведення з експлуатації та утилізації. При цьому:

- на етапах погодження засобів телекомунікацій, які можуть застосовуватися в телекомунікаційних мережах, одними з критеріїв прийняття рішень є забезпечення надійності та безпеки мереж телекомунікацій;

- розвиток та вдосконалення телекомунікаційних мереж має проводитись з урахуванням технологічної цілісності всіх мереж та їх інформаційної безпеки. Договори на постачання телекомунікаційних засобів та обладнання мають включати в себе вимоги щодо інформаційної безпеки;

- будівництво, реконструкція і модернізація телекомунікаційних мереж не повинні призводити до зниження їх надійності та рівня захищеності. Проекти будівництва, реконструкції, модернізації телекомунікаційних мереж, та проекти комплексних систем захисту інформації підлягають експертизі в порядку, встановленому законодавством. Робоча документація має містити детальні рішення щодо реалізації технічного проекту КСЗІ, щодо забезпечення управління КСЗІ і взаємодії її компонентів, а також документацію необхідну для тестування, проведення пусконалагоджувальних робіт, проведення випробувань КСЗІ.

На стадії побудови ЦАТС проводиться обстеження цього об’єкта інформаційної діяльності та створюються документи для побудови КСЗІ

об'єкта:

- технічне завдання на проектування КСЗІ об'єкта;
- робочий або технічно-робочий проект на створення КСЗІ об'єкта.

1.4.2 Організація ТЗІ на стадії вводу в експлуатацію ЦАТС

При проведенні робіт із введення в дію та оцінки захищеності інформації в телекомунікаційній системі виконуються роботи, передбачені НД ТЗІ 3.7-003-05. Порядок проведення робіт з технічного захисту інформації [10], із перевірки КСЗІ на відповідність вимогам нормативних документів з ТЗІ. При підключенні до об'єктів телекомунікаційних мереж та обладнання інших операторів складаються взаємні вимоги до заходів захисту та порядку захисту інформаційних ресурсів у шлюзових точках підключення інших операторів. Взаємні вимоги до інформаційної безпеки телекомунікаційних систем оформляються юридично договорами з іншими операторами у порядку, визначеному законодавством.

1.4.3 Організація ТЗІ на етапі технічної експлуатації ЦАТС

Згідно чинної нормативно-правової бази ТЗІ для організації робіт із створення КСЗІ в ЦАТС (чи для групи ЦАТС) створюється служба захисту інформації та призначаються відповідальні особи.

Організація та забезпечення діяльності в сфері інформаційної безпеки ЦАТС проводиться не відокремлено, а в тісній взаємодії із всіма службами, які мають відношення до технічної експлуатації телекомунікаційних мереж і, зокрема, ЦАТС. Схема взаємодії служб наведена на рис. 1.3 [10].

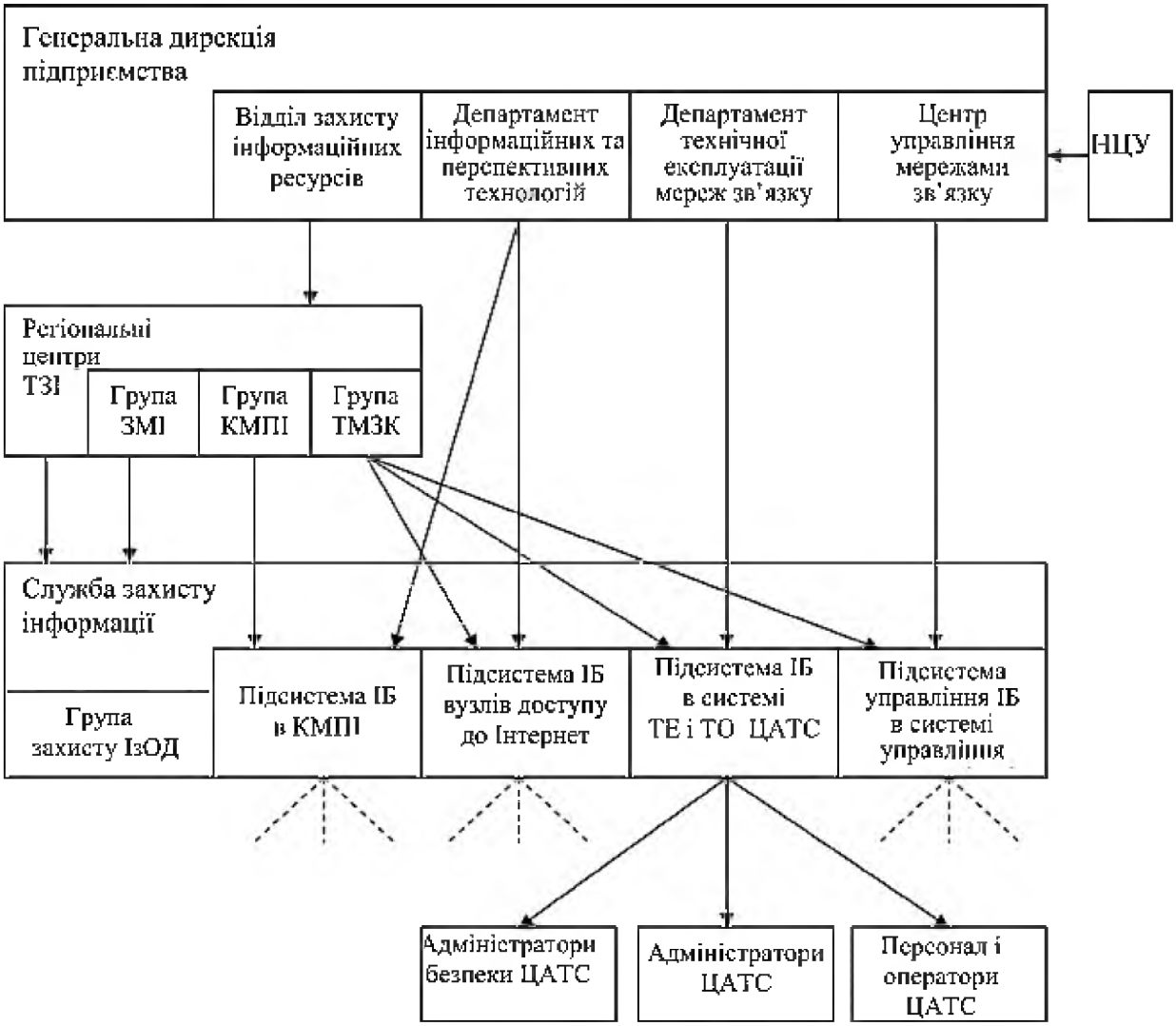

Рисунок 1.3 – Схема організації та забезпечення ТЗІ ЦАТС та мереж

Позначення: ЗМІ – захист мовної інформації; КМПІ – корпоративна мережа передачі інформації; НЦУ – національний центр управління; ІБ – інформаційна безпека; ІзОД – інформація з обмеженим доступом; ТЗІ – технічний захист інформації; ТЕ і ТО – технічна експлуатація і технічне обслуговування; ТМЗК – телекомунікаційна мережа загального користування; ЦАТС – цифрова автоматична телефонна станція.

Схемою передбачається функціонування та взаємодія відповідних служб на рівнях Генеральної дирекції, регіональних центрів ТЗІ, філій та безпосередньо в

ЦАТС. Розглянемо аспекти організації діяльності, які мають бути сформовані додатково або в складі існуючих.

В системі технічної експлуатації і технічного обслуговування (ТЕ і ТО), поряд з підсистемами забезпечення якості, надійності і сталості мереж, створюється підсистема інформаційної безпеки мереж телекомунікацій та ЦАТС. Підсистема виконує такі функції:

- створює і забезпечує використання систем моніторингу телекомунікацій, волоконно-оптичну лінію зв'язку (ВОЛЗ) та центрів мережі для вирішення комплексного контролю телекомунікацій, виявлення несанкціонованого доступу на фізичному рівні, мережному рівні та на рівні надання послуг, локалізації порушень у найкоротші строки;

- створює і підтримує функціонування КСЗІ в ЦАТС у відповідності до державних і галузевих нормативних документів.

Група ТЗІ у складі Служби захисту інформації координує і контролює роботи із забезпечення інформаційної безпеки ЦАТС та телекомунікаційних мереж, керує роботою адміністраторів безпеки ЦАТС, надає методичну, інструментальну і технічну допомогу у забезпеченні захисту комерційної таємниці підприємства, готує ЦАТС до державної експертизи та атестації на відповідність вимогам з інформаційної безпеки.

В ЦАТС обов'язки забезпечення інформаційної безпеки на робочих місцях покладаються на всіх, без винятку, працівників в межах означених у їх посадових інструкціях:

- адміністратори безпеки забезпечують функціонування КСЗІ ЦАТС та контролюють стан інформаційної безпеки і роботу адміністраторів мереж і систем та експлуатаційного персоналу. У питаннях інформаційної безпеки адміністратори безпеки підпорядковані і звітують Службі захисту інформації. У технологічних і виробничих питаннях адміністратори безпеки підпорядковані керівництву ЦАТС.

Адміністратори безпеки, в залежності від обсягу роботи, призначаються штатними або суміщають ці обов'язки з іншими обов'язками. Заборонено суміщати функції адміністратора безпеки і адміністратора мережі чи системи, бо

це може суттєво знизити рівень інформаційної безпеки ЦАТС;

- адміністратори мереж та систем забезпечують працездатність обладнання ЦАТС та інформаційної безпеки в межах своїх повноважень.

Штатний експлуатаційний персонал додатково до своїх функцій виконує заходи і роботи із підтримання інформаційної безпеки на своїх робочих місцях і в закріпленому за ними обладнанні. Ці функції відмічаються у посадових інструкціях і у окремих інструкціях з інформаційної безпеки.

1.4.4 Організація управління інформаційною безпекою

Для безпосередньої організації роботи із забезпечення інформаційної безпеки (та/або захисту інформації) в структурі управління мережами телекомунікацій має бути створена служба управління інформаційною безпекою, яка повинна забезпечити виконання всього комплексу завдань захисту телекомунікаційних мереж та інформації. Вказаній службі підпорядковуються групи інформаційної безпеки, що створюються на ЦАТС (і/або в структурі місцевої телефонної мережі загального користування), в задачу яких входить комплексне забезпечення інформаційної безпеки.

Управління інформаційною безпекою проводиться на всіх етапах життєвого циклу: планування, створення та експлуатації системи інформаційної безпеки. На стадії технічної експлуатації системи метою процесу управління інформаційною безпекою є оцінювання ефективності створеної системи захисту інформації й розроблення додаткових уточнюючих вимог для доопрацювання системи захисту з метою забезпечування її адекватності за зміни умов функціонування: характеристик системи, опрацьовуваної інформації, фізичного середовища, персоналу, призначення системи, політики безпеки тощо. Управління інформаційною безпекою базується на практичних правилах, котрі групуються в такі складові:

1) загальні положення з управління інформаційною безпекою:

- політика безпеки;

- організація захисту;

- класифікація ресурсів та їх контроль;

2) безпека персоналу, фізична безпека й безпека навколишнього середовища;

3) адміністрування комп'ютерних систем та обчислювальних мереж;

4) управління доступом до систем;

5) розробка й супроводження інформаційних систем;

6) планування захисту:

- планування безперебійної роботи підприємства;

- виконання вимог.

Завдання управління інформаційною безпекою розв'язуються із застосовуванням засобів контролю. Ключовими є такі засоби контролю:

- документ про політику інформаційної безпеки;

- розподіл обов'язків щодо забезпечування інформаційної безпеки;

- навчання й підготовка персоналу до підтримування режиму інформаційної безпеки;

- повідомлення про випадки порушення захисту чи інциденти в системі безпеки;

- засоби захисту від вірусів;

- процес планування безперебійної роботи підприємства;

- контроль за копіюванням програмного забезпечення, захищеного законом про авторське право;

- захист документації підприємства;

- захист даних;

- відповідність політиці безпеки.

Реалізація засобів управління безпекою в інформаційній інфраструктурі не повинна заважати іншій виробничій діяльності. Витрати на систему захисту інформації слід привести у відповідність з цінністю інформації, яка захищається, та інших інформаційних ресурсів, які піддаються ризикам, а також зі збитками, що їх може бути нанесено підприємству через збої в системі захисту. Тому в процесі управління мають оцінюватись ризики порушення безпеки. Для оцінювання ризиків слід:

- визначати й аналізувати потенційні загрози, яким піддаються комп'ютерні

системи, та їхні вразливості;

- розглядати збитки, котрі можуть нанести діяльності підприємства серйозне порушення інформаційної безпеки, з урахуванням можливих наслідків порушення конфіденційності, цілісності та доступності інформації;

- розглядати реальну ймовірність такого порушення захисту від суттєвих загроз за наявності засобів контролю.

Оцінка ризику залежить від таких чинників:

- характеру виробничої інформації та систем;

- виробничої мети, для якої інформація використовується;

- середовища, в якому система використовується й скеровується;

- захисту, забезпечуваного існуючими засобами контролю.

Успішне здійснення системи інформаційної безпеки визначається таким:

- забезпечення безпеки має ґрунтуватися на виробничих цілях і вимогах;

- функції управління безпекою має взяти на себе керівництво підприємства;

- оцінювання ризиків порушення безпеки, загроз і слабкостей інформаційних ресурсів та рівня їхньої захищеності має ґрунтуватися на цінності й важливості цих ресурсів;

- ознайомлення з системою безпеки всіх керівників та рядових співробітників підприємства;

- вивчання співробітниками політики та стандартів інформаційної безпеки;

- врахування конкретних інформаційних технологій, функцій підприємства та виробничого чи обчислювального середовища.

Згідно зі схемою маршрутизації викликів необхідно передбачити можливість альтернативного виходу до ТМЗК інших операторів, контролювати правильність маршрутизації трафіка, оперативно інформувати Національний центр оперативно-технічного управління мережами телекомунікацій (НЦУ), інших операторів телекомунікацій взаємоприєднаних мереж стосовно ситуацій, які призвели або можуть призвести до припинення обслуговування трафіка та про надзвичайні ситуації, у тому числі спричинені аваріями, пожежами тощо, використовувати технічні засоби та обладнання телекомунікацій, у тому числі ті, які призначені для обліку обсягів та проведення розрахунків наданих

телекомунікаційних послуг, які мають документ про підтвердження відповідності вимогам нормативних документів у сфері телекомунікацій та інформаційної безпеки, дотримуватися технічних вимог та вимог з інформаційної безпеки.

1.4.5 Повноваження та відповідальність суб'єктів взаємовідносин при реалізації задач забезпечення інформаційної безпеки в ЦАТС

Суб'єкти взаємовідносин при реалізації задач інформаційної безпеки в ЦАТС, права та повноваження посадових осіб, відповідальність суб'єктів взаємовідносин і ЦАТС при реалізації задач інформаційної безпеки мають відповідати чинним нормативно-правовим документам.

Функції та порядок роботи "Служби захисту інформації" в підрозділах підприємства слід визначати згідно НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі [11].

Права і обов'язки адміністраторів безпеки визначаються наказом та інструкціями, затвердженими керівником підприємства.

1.5 Постановка задачі

Метою даної роботи є забезпечення захисту інформації при використанні цифрової АТС EWSD шляхом розробки та впровадження відповідних організаційно-технічних заходів.

Для реалізації поставленої мети необхідно вирішити такі задачі:

1 Розробити модель АТС EWSD з позицій технічного захисту інформації та виконати аналіз загроз для інформації і моделі порушника

2 Розробити політику безпеки інформації та вимоги до календарного плану робіт із захисту інформації АТС EWSD

3 Розробити заходи захисту від витоку інформації технічними каналами та виконати розрахунок границь ближньої та дальньої зон при вимірах ПЕМВ

4 Розробити заходи щодо захисту мережі сигналізації SS7

5 Сформулювати рекомендації щодо обмеження фізичного доступу до обладнання зв'язку в абонентській мережі

1.6 Висновки

У даному розділі:

1 Розроблено модель цифрового вузла комутації з позицій технічного захисту інформації.

2 Виконано аналіз загроз для інформації та моделі порушника.

3 Сформульовано загальні положення безпеки інформаційних ресурсів у програмно-керованих АТС.

4 Розглянуто організацію та порядок технічного захисту інформації в ЦАТС.

5 Виконано постановку завдання дослідження.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Розробка плану захисту АТС EWSD

2.1.1 Загальні положення

План захисту інформації на ЦАТС визначає зміст робіт відповідно до вимог НД ТЗІ 1.4-001-2000 „Типове положення про службу захисту інформації в автоматизованій системі" [11] .

План захисту розробляється на підставі проведеного аналізу технології обробки інформації, аналізу ризиків, сформульованих тимчасових положень політики безпеки інформації.

Безпека інформації – це стан стійкості інформації до випадкових та зловмисних дій, що виключає недопустимі ризики її знищення, спотворення та розкриття, які можуть привести матеріальні втрати власнику або користувачу інформації.

Цифрова АТС класифікується згідно НД ТЗІ 2.5-003.99 „Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту" [4] як автоматизована система класу "3" – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

2.1.2 Основні об'єкти захисту:

1 Відомості, віднесені до інформації з обмеженим доступом (ІзОД) або інших видів інформації, що підлягають захисту, обробка яких здійснюється на АТС EWSD і які можуть знаходитись на паперових, магнітних, оптичних та інших носіях.

2 Інформаційні масиви та бази даних, програмне забезпечення, інші інформаційні ресурси.

3 Обладнання вузла комутації та інші матеріальні ресурси, включаючи

технічні засоби та системи, які не обробляють ІзОД, але знаходяться у контрольованій зоні, носії інформації, процеси і технології її обробки. Технічні області, в яких необхідно захищати інформаційне та програмне забезпечення – робоча станція, фізична мережа та комутаційне обладнання.

4 Засоби та системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту.

5 Користувачі АТС EWSD.

2.1.3 Загрози інформації в АТС EWSD та моделі порушників

Опис загроз інформації та моделі порушників в АТС EWSD наведено у розділі 1.2.

2.1.4 Політика безпеки інформації на АТС EWSD

Політика безпеки (ПБ) інформації АТС EWSD базується на таких документах:

- Закон України „Про захист інформації в автоматизованих системах" від 03.07.94 р.;

- НД ТЗІ 1.1-001-99 „Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення" [1].

Під політикою безпеки інформації розуміється набір вимог, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

Політика безпеки визначає інформаційні ресурси, які потребують захисту, та категорії інформації.

Формулюються загрози для ЦАТС, персоналу, інформації різних категорій та вимоги до захисту від цих загроз. ПБ включає в себе вимоги до забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється.

Політика безпеки визначає такі аспекти забезпечення захищеності інформаційних ресурсів у технологічному середовищі АТС EWSD:

- гарантії безпеки середовища персоналу;

- гарантії стандартизації технологічного середовища;

- гарантії забезпечення спостереження та керованості технологічного середовища;

- гарантії забезпечення конфіденційності і цілісності інформаційних ресурсів технологічного середовища;

- гарантії якості документації.

Нормальне функціонування АТС EWSD на всіх стадіях її життєвого циклу забезпечує персонал, тому необхідно забезпечити захищеність інформаційних ресурсів від їх помилкових і зловмисних дій.

Вимоги до персоналу включають у себе:

- вимоги до системи організації праці – забезпечення відповідності кваліфікації персоналу складу виконуваних робіт, система підвищення кваліфікації тощо;

- вимоги до контролю системи організації праці – контроль кваліфікації персоналу, аналіз і контроль системи підвищення кваліфікації, аналіз системи підбору кадрів, аналіз розподілу повноважень, аналіз системи оцінки якості праці тощо;

- вимоги до поведінки персоналу в робочий час – підтримання загальної дисципліни праці, виконання правил роботи з секретною інформацією та інше;

- вимоги до контролю поведінки персоналу в робочий час – контроль виконання технологічної дисципліни і поведінка персоналу у робочий час тощо;

- вимоги до поведінки персоналу в неробочий час – відсутність фактів антигромадської діяльності, аномалій у психофізичному стані організму і таке інше;

- вимоги до контролю поведінки персоналу у неробочий час – контроль достовірності даних про персонал, перевірка стану здоров'я персоналу.

Для забезпечення гарантій якості стандартизації технологічного середовища необхідно виконати вимоги: до повноти обхвату нормативними документами (НД) елементів середовища, до повного обхвату НД елементів технологій роботи в середовищі та до рівня відповідності НД.

Забезпечення спостережності та керованості технологічного середовища

залежить від виконання вимог: до ефективності аудиту технологічного середовища, до автентифікації суб'єктів та ідентифікації об'єктів (процесів, ресурсів), до сертифікованих шляхів керованості технологічним середовищем.

Вимоги до забезпечення конфіденційності та цілісності інформаційних ресурсів технологічного середовища включають в себе: вимоги до реалізації правил розмежування доступу (ПРД), до реалізації послуг повторного використання об'єктів, до захищеності від таємних каналів витоку та каналів спеціального впливу на елементи АТС, до фізичної цілісності, розмежування обов'язків та самотестуванню об'єктів.

Для забезпечення гарантій якості документації необхідно виконати вимоги: до повноти документації, до рівня деталізації опису середовища та/або технології, достовірності інформації в документації, до якості оформлення документації.

Політика безпеки має бути завершена планом захисту інформації, у якому відображаються основні вимоги і положення інформаційної безпеки.

2.1.5 Календарний план робіт із захисту інформації на АТС EWSD

На підставі НД ТЗІ 1.4-001-2000 „Типове положення про службу захисту інформації в автоматизованій системі" [11] складається календарний план робіт із захисту інформації на АТС EWSD.

Він може мати такі розділи:

- організаційні заходи;
- контрольно-правові заходи;
- профілактичні заходи;
- робота з кадрами;
- інженерно-технічні заходи.

Організаційні заходи захисту інформації – це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне розв'язання задач захисту шляхом регламентації діяльності персоналу і порядку функціонування систем забезпечення інформаційної діяльності та засобів забезпечення ТЗІ.

До контрольно-правових заходів можуть бути віднесені:

- контроль за виконанням персоналом (користувачами) вимог, відповідних інструкцій, розпоряджень, наказів;

- контроль за виконанням заходів, розроблених за результатами попередніх перевірок;

- контроль за станом зберігання та обігу носіїв інформації на робочих місцях.

До профілактичних слід відносити заходи, спрямовані на формування у персоналу та користувачів мотивів поведінки, які спонукають їх до безумовного виконання у повному обсязі вимог режиму, правил проведення робіт тощо.

Планування роботи з кадрами включає заходи з підбору та навчання персоналу і користувачів встановленим правилам безпеки інформації, новим методам захисту, підвищення їхньої кваліфікації.

До інженерно-технічних слід відносити заходи, спрямовані на налагодження, випробовування і введення в експлуатацію, супроводження й технічне обслуговування апаратних і програмних засобів захисту інформації від НСД, комплексів захисту інформації від загроз технічними каналами та каналами спеціального впливу, інженерного обладнання споруд і приміщень, в яких розміщуються засоби обробки інформації тощо.

Політика безпеки та комплексний план її реалізації є основою для побудови та функціонування системи безпеки.

2.2 Розробка заходів захисту від витоку інформації технічними каналами

Під витоком інформації розуміється неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

Витік інформації відбувається відповідним каналом витоку. Оскільки засоби розвідки противника, як правило, технічні, то і канали витоку також називають технічними.

Технічний канал витоку інформації (ТКВІ) – сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засобу

технічної розвідки (рис. 2.1) [2, 4-6].

Також враховуються завади, що діють на вході засобу технічної розвідки.

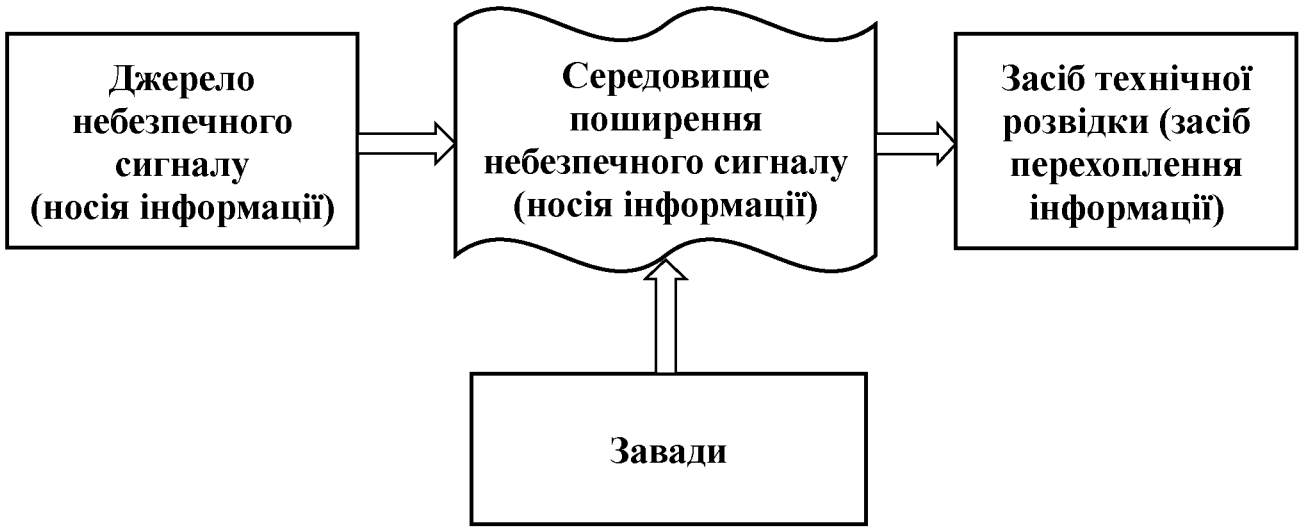

Рисунок 2.1 – Технічний канал витоку інформації

Збереження інформаційних ресурсів АТС EWSD визначається умовами забезпечення їх захищеності на станції та в мережі. Для рішення цієї задачі розробляється система безпеки, основними функціями якої є захист інформації при її обробці та передачі каналами зв'язку від НСД до неї, від різноманітних програмно-технічних впливів, а також від витоку технічними каналами за рахунок побічних електромагнітних випромінювань та наводок (ПЕМВН).

Розглянемо можливість витоку інформації. Припустимо, що на ОІД передбачаються всі види робіт з інформацією: зберігання носіїв інформації, озвучування інформації, обробка інформації технічними засобами та системами (ТЗС), візуалізація інформації. Схематично можливість витоку інформації наведена на рис. 2.2.

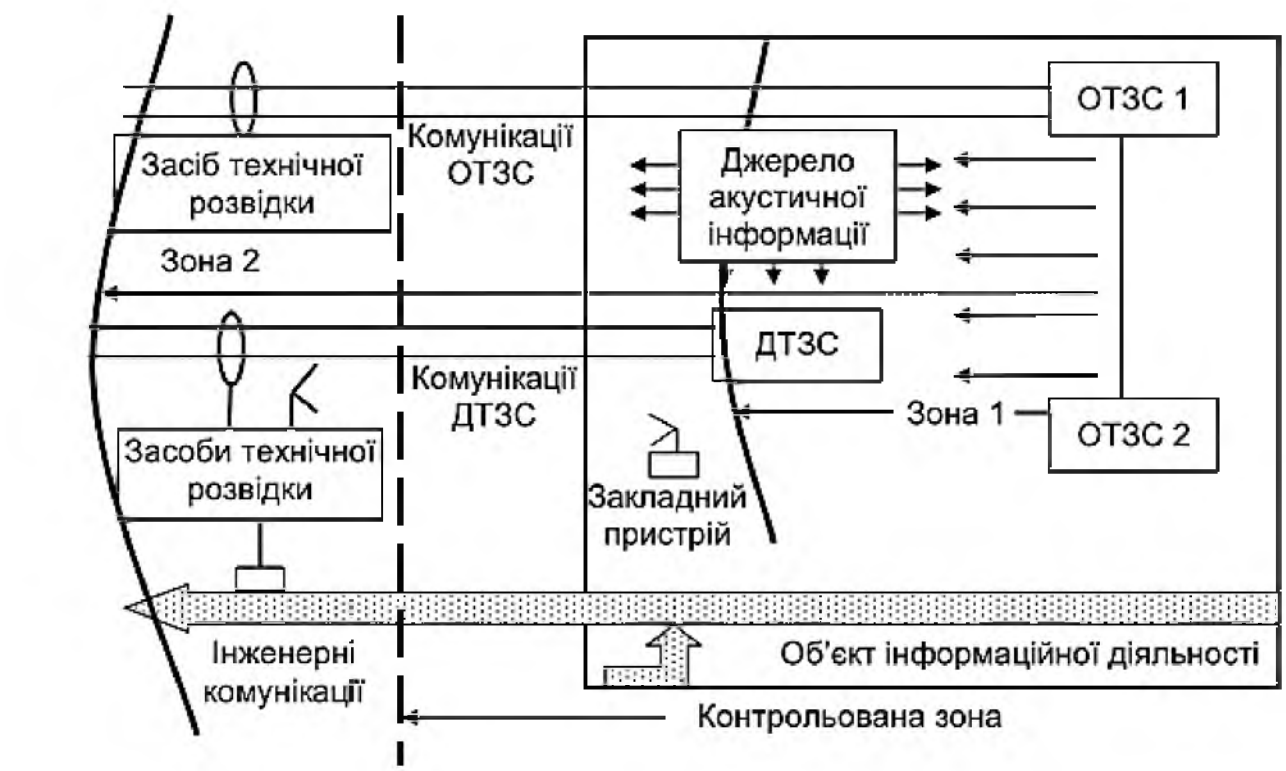

Рисунок 2.2 – Схема витоку інформації: ДТЗС – допоміжні технічні засоби і системи, ОТЗС – основні технічні засоби і системи

Відповідно до інформаційної діяльності на ОІД можна виділити такі первинні джерела небезпечного сигналу:

- людина, що озвучує інформацію, засоби відтворення або підсилення звуку;
- технічні засоби та системи, що обробляють інформацію;
- монітори засобів електронно-обчислювальної техніки, екрани, секретні документи з надрукованим текстом, на яких візуалізується інформація.

Також можна виділити такі середовища поширення небезпечного сигналу:

- вільний простір;
- комунікації ОТЗС та ДТЗС, які виходять за межі контрольованої зони;
- інженерні комунікації (жорсткі пружні поверхні), які виходять за межі контрольованої зони.

За межами контрольованої зони можливе застосування засобів технічної розвідки, які перехоплюють небезпечний сигнал у вільному просторі, або знімають

небезпечний сигнал, безпосередньо підключившись до комунікацій ОТЗ, комунікацій ДТЗС або до інженерних комунікацій.

Таким чином, наявні усі три складові технічних каналів витоку інформації, що уможливлює створення певних технічних каналів витоку інформації.

На ОІД одні ТЗС використовуються для обробки і передачі секретної інформації, а інші – для інших завдань, не пов'язаних з обробкою секретної інформації, але необхідних для виробничої діяльності об'єкту. В залежності від того, обробляють технічні засоби секретну інформацію або не обробляють її, вони розділяються на основі та допоміжні. До допоміжних ТЗС можуть належать засоби міського зв'язку, охоронної та пожежної сигналізації та ін.

Основні технічні засоби та системи (ОТЗС) – розташовані на об'єкті інформаційної діяльності технічні засоби та їх комунікації, які здійснюють обробку секретної інформації.

Допоміжні технічні засоби та системи (ДТЗС) – розташовані на об'єкті інформаційної діяльності технічні засоби та системи і їх комунікації, які не здійснюють обробку секретної інформації, але перебувають під впливом небезпечних сигналів основних технічних засобів або небезпечних акустичних полів.

Основні технічні засоби та системи є джерелом небезпечного сигналу, який може розповсюджуватись в просторі на досить великі відстані і може бути перехопленим (знятим) засобами технічної розвідки противника поза межами контрольованої зони.

Однак поля (акустичні, вібраційні, електричні, магнітні, електромагнітні) при їх розповсюдженні мають властивість загасати. При цьому знайдеться така відстань від джерела небезпечного сигналу, на якій перехоплення (зняття) небезпечного сигналу та відтворення інформації стане неможливим. Для ОТЗС визначають небезпечні зони 1 та 2.

Зона 2 – територія (сфера) навколо технічних засобів обробки інформації, за межами якої вважається неможливим перехоплення небезпечного сигналу з метою відтворення інформації, характеризується радіусом $R2$, що визначає найбільшу відстань від технічних засобів обробки інформації до межі, за якою напруженості

електричного та магнітного полів небезпечного сигналу відносно шумових завад не перевищують нормованого значення (рис. 2.2).

В Зоні 2 можливе перехоплення інформації, а за її межами – ні.

Зона 1 – територія (сфера) навколо основних технічних засобів, в межах якої здійснюється наведення небезпечних сигналів на інші технічні засоби, системи та їх комунікації, характеризується радіусом $R1$, що визначає граничну відстань від основних технічних засобів до межі, за якою вважається неможливим наведення небезпечних сигналів на технічні засоби (рис. 2.2).

В межах Зони 1 на ОІД під впливом небезпечного сигналу від ОТЗС знаходяться ДТЗС, лінії яких можуть виходити за межі ОІД або за межі контрольованої зони, або знаходяться сторонні провідники (наприклад – стара електропроводка, тощо), які виходять за межі контрольованої зони. Допоміжні технічні засобі та системи, а також сторонні провідники можуть виступати в ролі випадкових антен або середовищ поширення небезпечного сигналу. Цілком природно, що ДТЗС або сторонні провідники не будуть достатньо ефективними антенами, однак достатньо близьке розташування засобів технічної розвідки може призвести до витоку інформації. Тому технічні засоби та системи, а також сторонні провідники мають розташовуватися на ОІД поза Зоною 1.

Зона 1 та Зона 2 є фізичними характеристиками (показниками) ОТЗС та визначаються експериментально-розрахунковим методом при спеціальних дослідженнях ОТЗС.

Як правило, радіус Зони 1 менший, ніж радіус Зони 2.

2.2.1 Оцінка долі технічних каналів витоку у загальній безпеці

В АТС EWSD основна увага приділяється питанням захисту інформації від НСД. Заходи захисту інформації від ПЕМВН зустрічаються рідко і застосовуються у особливо відповідальних випадках. Це пояснюється тим, що здійснення різних видів НСД, як всередині АТС EWSD, так і зовні з мереж, не потребує великих витрат, оскільки виконується з використанням штатних технічних засобів самої АТС EWSD. Організація перехоплення інформаційних

сигналів каналами ПЕМВН потребує високих витрат, так як пов'язана з використанням спеціальних комплексів перехвату. Крім того, проведення таких атак можливе лише при умові розташування апаратури перехоплення в безпосередній близькості від об'єкта, у відношенні до якого проводиться атака.

Але недооцінка загроз витоку інформації каналами ПЕМВН призводить до того, що вони можуть стати самим вразливим місцем в системі інформаційної безпеки.

2.2.2 Організація захисту інформації від витоку за рахунок ПЕМВН

Захист інформації від витоку за рахунок ПЕМВН повинен бути реалізований або у всій АТС EWSD, або в тих сегментах, де обробляється найбільш важлива інформація. Такого захисту на АТС EWSD, в першу чергу, потребують приміщення центру технічної експлуатації, оскільки там обробляється технологічна інформація. В загальному випадку всередині контрольованої зони АТС можуть бути виділені внутрішні зони безпеки, в яких повинен бути реалізований захист від ПЕМВН.

Рівні ПЕМВН залежать від параметрів (амплітуди, форми, тактової частоти) сигналів, які обробляються, а також від конструктивного виконання обладнання. Ці ж фактори визначають характер затухання випромінювань з відстанню та радіус Зони 2 (мінімально необхідної контрольованої зони) навколо обладнання. Найбільш потужні випромінювання ідуть від моніторів ПЕОМ, а також фізичними лініями. Інші технічні засоби ЦАТС утворюють більш низькі рівні випромінювання. Окрім випромінювань, канали витоку виникають в результаті електромагнітних наводок на кола, які виходять за межі контрольованої зони (електроживлення та заземлення, охоронна та пожежна сигналізації) та інших факторів.

Як правило, на ЦАТС більшу частину каналів ПЕМВН намагаються закрити організаційно-технічними рішеннями. Проблему випромінювань фізичних ліній можна зняти використанням криптографічного захисту чи використанням ВОЛЗ. Системи електроживлення, заземлення та сигналізації можна розмістити у

контрольованій зоні. Використання таких заходів знижує ймовірність витоку, але не вирішує повністю проблеми ПЕМВН, так як залишаються випромінювання моніторів та фізичних ліній (на неохоплених захистом ділянках), і необхідно використовувати додаткові заходи захисту.

В загальному випадку потрібно вибрати комплекс технічних засобів захисту. При цьому необхідно враховувати ряд загальних вимог, які пред'являють до такого комплексу: ефективність, економічність, відповідність основним характеристикам систем, надійність і т. д.

Комплекс може включати активні та пасивні технічні міри захисту. Активні заходи полягають у маскуванні (зашумленні) побічних випромінювань та наводок поблизу технічних засобів широкосмугових шумових сигналів, які перевищують за рівнем сигнали ПЕМВН. До них відносяться, в основному, генератори шуму. Пасивні заходи захисту спрямовані на ослаблення побічних випромінювань та наводок. До них відносяться екранування, фільтрація, схемно-конструктивна доробка та ін. Які саме заходи потрібно реалізувати, в кожному конкретному випадку розглядається окремо.

Незалежно від того, які засоби захисту на АТС EWSD будуть прийняті, потрібно правильно розрахувати радіус Зони 2, який характеризує мінімальну відстань від технічного засобу, на границі та за межами якої відношення сигнал/шум не перевищує нормованого значення.

2.2.3 Розрахунок границь ближньої, дальньої та перехідної зон при вимірах ПЕМВН

Для вибору належного рівня захисту технічних засобів обробки інформації необхідно виміряти рівень побічних електромагнітних випромінювань та розрахувати радіус Зони 2, на границі та за межами якої відношення сигнал/шум не перевищить нормованого значення. В загальному випадку ця відстань може знаходитись в ближній, перехідній чи дальній зоні. В межах кожної з зон загасання електромагнітної хвилі описується різними аналітичними залежностями. Уміння вірно визначити границі зон необхідне для одержання об'єктивної оцінки величини

Зони 2.

В даний час границі зон визначаються умовно без достатнього математичного або електродинамічного обґрунтування. Таким чином, при розрахунку радіусу Зони 2 допускаються методичні похибки, що неприпустимо при організації захисту інформації обмеженого поширення від витоку за рахунок ПЕМВН. Для багатьох технічних засобів обробки інформації, наприклад персональних ЕОМ, характерна велика величина амплітуди напруги небезпечного сигналу і мала величина амплітуди струму. Такі джерела відносять до електричних випромінювачів.

Будемо вважати ПЕОМ точковим електричним випромінювачем, тому що його розміри істотно менші відстані до точки можливого перехоплення інформації. Представимо його у вигляді диполя, розміщеного в точці O сферичної системи координат.

Математичні вирази для визначення параметрів поля джерела ПЕМВН можна одержати з класичної теорії технічної електродинаміки, використовуючи вирази для векторного потенціалу [12]. Наведені формули відображають електромагнітні процеси, які описують теорію електромагнітного поля та дозволяють виконати оцінку границь ближньої та дальньої зони при відповідних припущеннях та обмеженнях.

Відомо, що вектори напруженості магнітного H та електричного E полів пов'язані з векторним потенціалом залежностями:

$$H = (1/\mu) rot A_a, \quad E = (1/i\bar{\omega}\varepsilon_a\mu_a) rot rot A_a,$$

де ε_a – абсолютна комплексна діелектрична проникність; μ_a – абсолютна магнітна проникність середовища; I – струм в провіднику; l – довжина провідника; r – відстань від випромінювача до вимірювальної антени (точки спостереження); k – хвильове число.

Розкладемо векторний потенціал на радіальну (A_r), кутову (A_θ) та азимутальну (A_ϕ) складові:

$$A_r = \frac{\mu_a}{4\pi} Il \frac{e^{-jkr}}{r} \cos\Theta, \; A_\Theta = \frac{\mu_a}{4\pi} Il \frac{e^{-jkr}}{r} \sin\Theta, \; A_\varphi = 0$$

В сферичній системі координат складові вектора напруженості електричного поля описуються наступними виразами:

$$E_r = -i \frac{Il}{2\pi\omega\varepsilon_a} e^{-ikr} \left(\frac{1}{r^3} + \frac{ik}{r^2}\right) \cos\Theta \tag{2.1}$$

$$E_\Theta = -i \frac{Il}{4\pi\omega\varepsilon_a} e^{-ikr} \left(\frac{1}{r^3} + \frac{ik}{r^2} - \frac{k^2}{r}\right) \sin\Theta \tag{2.2}$$

$$E_\varphi = 0.$$

Вектор напруженості електричного поля має вигляд $E = rE_\text{г} + \theta E_\theta$. Силові лінії вектора E проходять у меридіальних площинах. Складова E_θ досягає максимального значення при $\theta = \pi/2$ в екваторіальній площині та рівна нулю на осі диполя. Тому вимірювання ПЕМВ потрібно здійснювати в напрямі максимального випромінювання ПЕОМ при $\theta = \pi/2$. Складова $E_\text{г}$ пропорційна cos θ та досягає максимуму на осі диполя, а в екваторіальній площині рівна нулю.

З урахуванням хвильового опору середовища без втрат $\rho_0 = (\mu_\text{а} / \varepsilon_a)^{1/2}$, швидкості поширення $v_0 = (\mu_\text{а} / \varepsilon)^{-1/2}$ та довжини хвилі $\lambda = v / f$, вираз (2.2) для E_θ можна представити у вигляді:

$$E_\Theta = \rho_0 Il \left[\frac{1}{8\pi r^2} - i \left(\frac{\lambda}{8\pi^2 r^3} - \frac{1}{2\lambda r} \right) e^{-jkr} \right]. \tag{2.3}$$

При вимірюванні напруженості електричної складової поля за допомогою селективних мікровольтметрів використовується режим пікового або квазіпікового детектування. В цьому випадку амплітуда напруженості електричної складової поля може бути виражена наступним чином:

$$E_m = \sqrt{\left(E_{m1} - E_{m3}\right)^2 + E_{m2}^2} \tag{2.4}$$

де:

$$E_{m1} = \rho_0 \frac{Il\lambda}{8\pi^2} \frac{1}{r^3}, \quad E_{m2} = \rho_0 \frac{Il}{4\pi} \frac{1}{r^2}, \quad E_{m3} = \rho_0 \frac{Il}{2\pi} \frac{1}{r}.$$

Простір навколо випромінювача умовно розділяється на 3 зони – ближню, перехідну та дальню. Характер залежності амплітуди електричної складової від дальності залежить від того, в якій зоні знаходиться точка спостереження.

Розглянемо залежності амплітуди електричної складової в ближній, перехідній та дальній зонах.

Ближня зона. Під ближньою зоною розуміється область навколо випромінювача, для якої $|kr| << 1$, де k = $2\pi / \lambda$ – хвильове число. Відповідно, $r << \lambda/(2\pi)$. Враховуючи, що $|kr| << 1$, приймемо $|kr| = 0$. В цьому випадку вирази (2.1) та (2.2) можна привести до виду:

$$E_r = -i \frac{Il}{2\pi\varpi\varepsilon_a} \frac{1}{r^3} \cos\Theta, \quad E_\Theta = -i \frac{Il}{4\pi\varpi\varepsilon_a} \frac{1}{r^2} \sin\Theta, \tag{2.5}$$

Дальня зона. Під дальньою зоною розуміється область простору навколо випромінювача, для якої $|kr| >> 1$ чи $r >> \lambda/(2\pi)$. Нехтуючи доданками з більш високими ступенями r в знаменнику, отримуємо:

$$E_\Theta = i \frac{k^2 Il}{4\pi\varpi\varepsilon_a} \frac{e^{-ikr}}{r} \sin\Theta \tag{2.6}$$

Перехідна зона. Під перехідною зоною розуміється область простору навколо випромінювача, в якому відстань r від випромінювача до вимірювальної антени порівняно з довжиною хвилі λ. Це значить, що жодним з доданків в (2.3) нехтувати не можна. В даній зоні формула для розрахунку електричної складової поля має вигляд:

$$E_\Theta = A\sqrt{\left[\left(\frac{\lambda}{4\pi^2 r^3} - \frac{1}{\lambda r}\right)^2 + \left(\frac{1}{2\pi r^2}\right)^2\right]}, \tag{2.7}$$

де $A = \rho_0 Il/2$ - енергетичний коефіцієнт.

Взаємне порівняння внеску кожної зі складових в амплітуду напруженості електричного поля дозволяє визначити границі зон з достатньою для практики точністю.

Відстанню до границі ближньої зони $r_{áë}$ назвемо відстань від джерела ПЕМВ, на якій максимальна складова E_{m1} у ξ разів перевищує внесок складової E_{m2}. У межах даної відстані можна зневажити складовими E_{m2} і E_{m3} і вважати, що результуюча амплітуда електричної складової поля дорівнює складовій E_{m1}.

З рівняння $E_{m1} = \xi E_{m2}$ можна одержати шуканий вираз до границі ближньої зони $r_{áë} = \lambda/(2\pi\xi)$. Аналогічно, для границі дальньої зони отримуємо $r_{ä} = \xi\lambda/(2\pi)$.

Величина прийнятого граничного внеску складових поля ξ залежить від необхідної точності і для практичних розрахунків може складати величину від 3 до 10. На границі ближньої (дальньої) зони можна обмежитися значенням $\xi = 3$, при якому у виразі (2.4), з урахуванням зведення членів у квадрат, величинами E_{m2} і E_{m3} (E_{m1} і E_{m2}) можна зневажити в порівнянні з E_{m1} (E_{m3}). Так, для $\xi = 3$ границя ближньої зони складає $r_{áë} = \lambda/(6\pi)$, а границя дальньої зони – $r_{ä} = 3\lambda/(2\pi)$.

Ширина перехідної зони залежить від довжини хвилі ПЕМВН та обраної точності розрахунків і дорівнює $D = \lambda(\xi^2 - 1)/(2\pi\xi)$. При $\xi \geq 3$ ширину перехідної зони можна визначити виразом $D \approx \xi\lambda/(2\pi)$. Таким чином, на фіксованій частоті ширина перехідної зони залежить тільки від обраної точності розрахунків. У граничному випадку при великих значеннях ξ ширина смуги необмежено зростає, що призводить до необхідності враховувати всі члени у виразі (2.4) незалежно від відстані до джерела ПЕМВ.

Розрахуємо радіус Зони 2 у випадку, коли ПЕМВ є персональна ЕОМ на АТС EWSD. Середня частота роботи ПЕОМ 110 МГц. Звідси маємо, що довжина хвилі становить:

$$\lambda = \frac{3*10^8}{110*10^6} = 2,73(м)$$

Тоді границя ближньої зони становить:

$$r_{аё} = \frac{2,73}{6*3,14} = 0,15(м)$$

Границя дальньої зони

$$r_{ä} = \frac{3*2,73}{2*3,14} = 1,30(м)$$

Ширина перехідної зони

$$D = \frac{2,73*(3^2-1)}{2*3*3,14} = 1,15(м)$$

Як видно з розрахунків, границя дальньої зони при частоті ПЕОМ 110 МГц становить 1,30 м. Віддалення границь від джерела ПЕМВ визначається довжиною хвилі та із збільшенням частоти переміщується в сторону джерела. Тому при виборі ПЕОМ для робочого місця оператора з точки зору системи технічного захисту потрібно вибирати ПЕОМ з якнайменшою робочою частотою, аби радіус зони, на границі та за межами якої відношення сигнал/шум не перевищить нормованого значення, теж був мінімальним.

2.3 Організація та реалізація системи захисту системи сигналізації SS7

2.3.1 Структура та організація системи сигналізації SS7

Система спільноканальної сигналізації (SS7) служить для передачі інформації між ЦАТС (АМТС) з програмним управлінням. SS7 використовується для інформаційного обміну сигнальною інформацією в процесі встановлення з'єднання, управління процесами встановлення з'єднання, маршрутизацією та трафіком, організації інтеграції та надання послуг, контролю, технічної діагностики, технічного обслуговування, конфігурації та реконфігурації мережі, її агрегатних засобів та інших застосувань. У відповідності з цим „Національна версія України" передбачає в SS7:

- підсистему передачі повідомлень (MTP – Message Transfer Part);
- підсистему управління з'єднанням сигналізації (SCCP – Signaling Connection Control Part);
- підсистему користувача цифрової мережі з інтеграцією послуг (ISUP –

ISDN User Part);

- підсистему використання можливостей транзакції;

- підсистему експлуатації та технічного обслуговування SS7;

- підсистему користувача технічної експлуатації мережі зв'язку.

Основною властивістю SS7 є те, що один канал (16-ий часовий інтервал 30-канальних цифрових з'єднувальних ліній) використовується для переносу повідомлень сигналізації, які відносяться до кількох розмовних каналів. Також цей канал використовується для переносу повідомлень управління розмовними каналами та управління мережею сигналізації. Мітка, яка присутня в кожному сигнальному повідомленні, використовується для однозначного визначення розмовного каналу, до якого відноситься дане повідомлення.

Система SS7 забезпечує надійну та достовірну передачу сигнальної інформації як наземними, так і супутниковими каналами зв'язку. Вона може застосовуватись на міжнародній, міжміській, внутрішньозоновій та місцевих мережах.

Система SS7 ТМЗК України може працювати у двох режимах: спільному та квазіспільному, що дозволяє будувати мережу сигналізації з високим ступенем використанням ланок. За спільного режиму роботи для кожного маршруту робочих каналів відводяться сигнальні канали SS7 у тому ж маршруті.

За квазіспільного режиму роботи маршрут проходження інформації сигналізації на комутаційній ділянці може не співпадати з розмовними каналами. В цьому випадку маршрут SS7 проходить через один або кілька транзитних пунктів сигналізації (ТПнС).

При передаванні інформації SS7 основним маршрутом використовується спільний режим роботи. При передачі інформації SS7 обхідними маршрутами можуть використовуватись спільний або квазіспільний режим роботи.

SS7 ТМЗК України організується на базі стандартних цифрових каналів зі швидкістю 64 кбіт/с. Сигнали каналами SS7 передаються методом послідовної передачі по ділянках (ланках сигналізації), з однієї ділянки на іншу, після їх обробки у пунктах сигналізації (ПнС) або ТПнС.

Підсистема передачі повідомлень (MTP - Media Transfer Protocol) утворена

трьома функціональними рівнями:

- перший рівень визначає фізичні електричні та функціональні характеристики ланки даних сигналізації та засоби доступу до неї. Елемент першого рівня є каналом зв'язку для ланки сигналізації;

- другий рівень визначає функції та процедури, що належать до передачі сигнальних повідомлень окремою ланкою даних сигналізації. Із сигнальних повідомлень, які надходять з верхніх рівнів, на другому рівні формуються сигнальні одиниці, які мають, окрім сигнальної інформації, ще і інформацію для управління передачею. Перший та другий рівні утворюють ланку сигналізації.

- третій рівень вміщує в себе функції та процедури обміну сигнальними повідомленнями між вузлами мереж сигналізації (пунктами сигналізації), які зв'язані ланками сигналізації. Ці функції діляться на дві категорії: обробка повідомлень сигналізації та управління мережею сигналізації.

- четвертий рівень є набором підсистем користувачів, в кожній з яких реалізовані функції, які характерні для користувачів даної підсистеми.

Одним з основних користувачів є підсистема користувача цифрової мережі з інтеграцією послуг (ISUP). На цьому рівні обробляються сигнальні повідомлення, які управляють телефонними з'єднаннями у відповідності з міткою маршрутизації та інформацією користувача.

Мережа сигналізації може бути поділена на рівні з метою оптимального адміністрування.

Специфікація SS7 дозволяє поділити мережу на ієрархічні рівні, які відповідають традиційному принципу побудови телефонної мережі: міжнародний, національний та місцевий (регіональний) (рис. 2.3).

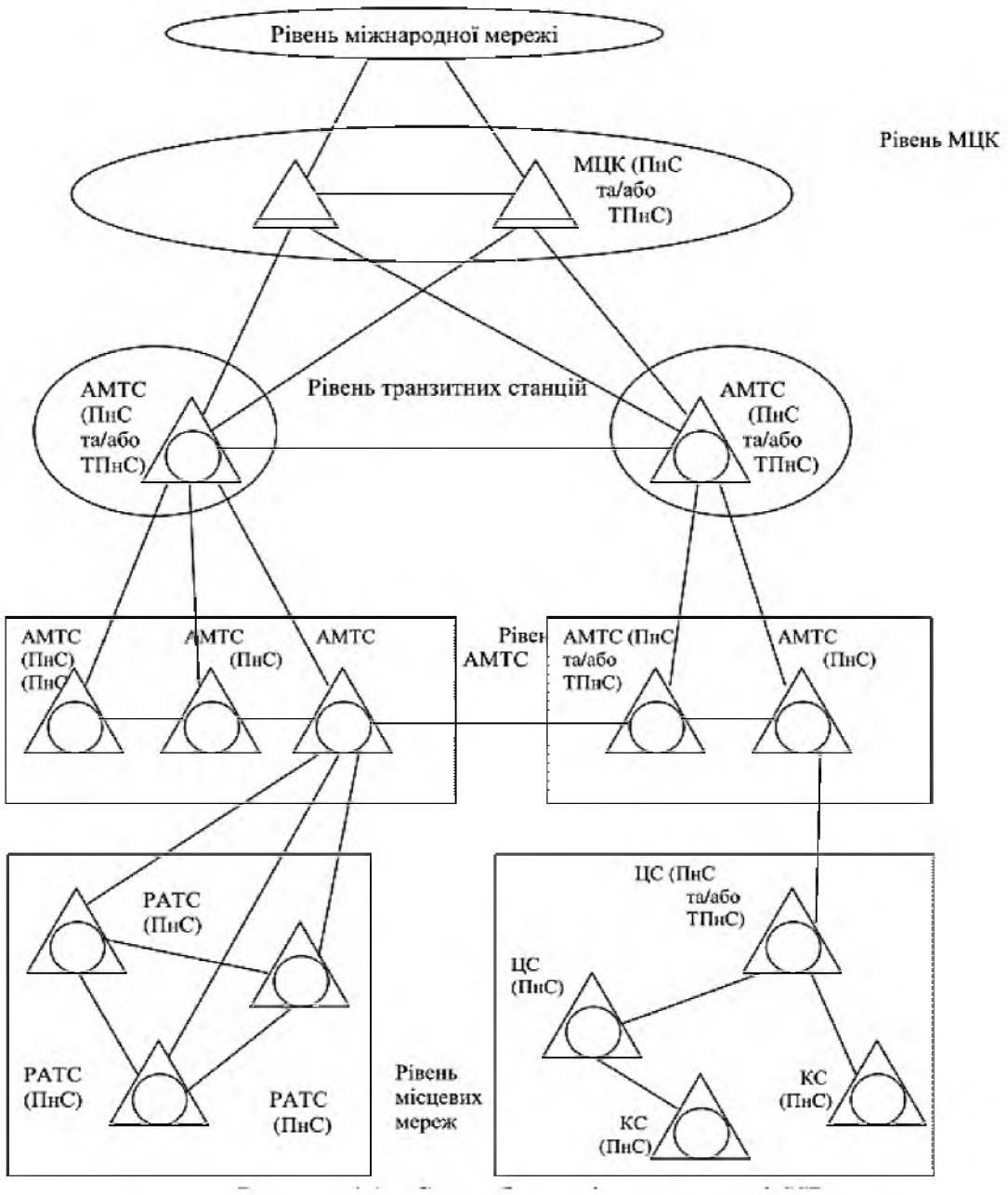

Рисунок 2.3 – Схема багаторівневої мережі SS7

При використанні системи SS7 в процесі установлення і з'єднання розмовний тракт не перевіряється, тому що лінійні сигнали ним не передаються. Щоб виключити можливість передачі абонентам зіпсованого розмовного тракту, у системі може передбачатися шлейфна перевірка розмовних каналів. Шлейфна перевірка полягає у підключенні до тракту приймально-передавального пристрою на вихідній станції та організації шлейфа на вхідній станції. Перевірка повинна проводитися за ділянками.

Нумерація пунктів сигналізації всередині кожного рівня – незалежна, значення мережного індикатора визначає, до якої мережі відноситься дане повідомлення. Основними перевагами SS7 є: - швидкість – у більшості час встановлення з'єднання менше 1 секунди; - один канал сигналізації здатний одночасно керувати 2 - 4 тисячами розмовних каналів;

- економність – у порівнянні з іншими системами сигналізації зменшує кількість обладнання на ЦАТС;

- гнучкість – система передає будь-які дані – не лише дані телефонії, але й дані цифрових систем з інтеграцією служб, мереж рухомого зв'язку, інтелектуальних мереж тощо;

- надійність – досягається за рахунок можливості альтернативної маршрутизації у мережі сигналізації.

У період створення та становлення мереж SS7 проблеми захисту інформації від різноманітних загроз були не такі актуальні. Головна увага приділялась питанням забезпечення надійності мережі та достовірності передачі даних мережею (цілісності даних та цілісності мережі). Захищеність даних від несанкціонованого втручання виявилась порівняно низькою.

2.3.2 Система захисту у мережі SS7

Спочатку мережа SS7 створювалася в припущенні, що невелика кількість магістральних мереж будуть взаємодіяти з обмеженою кількістю місцевих, і дані будуть передаватися в замкнутому середовищі – між комутаторами і базами даних (БД) – з мінімальним втручанням людини. У такому випадку вважалося, що всі дані надходять з надійних джерел. Тому протоколи SS7 на відміну від IP-протоколів не підтримують функції шифрування й автентифікації. Акцент у ТфМЗК було зроблено на захисті обладнання, а не протоколів.

Відносно принципів роботи мережі сигналізації були прийняті наступні заходи безпеки. Шлюз у складі транзитного пункту сигналізації маршрутизатора мережі SS7 виконує сканування повідомлень, що надходять у мережу, щоб запобігти надходженню повідомлень з неавторизованих внутрішніх і зовнішніх

вузлів мережі.

Оскільки зараз зв'язок розвивається дуже швидко, мережа SS7 використовується в широкому діапазоні застосувань і тому більше не є закритою мережею. Доступ до неї має велика кількість користувачів інших мереж. Кожна точка взаємодії мереж різних типів – це потенційна загроза безпеки.

Як уже говорилося вище, мережі сигналізації не підтримують функції шифрування й автентифікації, за допомогою яких можна гарантувати достовірність вузлів зовнішньої мережі, що посилають повідомлення.

Наприклад, сервер, що посилає спеціальні руйнуючі повідомлення, може порушити роботу сигнальної мережі і перервати обслуговування клієнтів. Елементи самої мережі сигналізації також не захищені. Якщо зловмисник зможе відправити на деякий вузол мережі SS7 трафік, що перевищує той, на який цей вузол розрахований, останній вийде з ладу, і управління викликами в цьому секторі мережі буде порушено.

Сучасні підходи до захисту мережі SS7 припускають надання їй додаткових інтелектуальних властивостей. Спеціальні програми, установлені на транзитних пунктах, дозволяють операторам ідентифікувати повідомлення, що випадають із загального контексту або виявляють себе нетиповим поводженням.

Одним з важливих способів підвищення безпеки мережі є побудова правильної архітектури на стику ТфМЗК – IP-мережі. Кількість вузлів з'єднання цих мереж повинне бути мінімальним, повідомлення з мережі SS7 повинні надходити на IP-шлюзи централізовано. Замість численних шлюзів використовується єдиний високопродуктивний шлюз. Тоді за рахунок скорочення точок взаємодії між різнорідними частинами мережі підвищується загальна безпека мережі.

Ще одне питання захисту мережі SS7 пов'язане з тим, що на сучасних мережах широко використовується централізована обробка і управління мережею SS7. У зв'язку з цим використовуються спеціальні функції, розроблені для дистанційного експлуатаційного управління АТС EWSD, заміни версії програмного забезпечення тощо. Вони також являють собою загрозу

інформаційної безпеки, тому що дані функції можуть збігатися з цілями зловмисника. У зв'язку з цим для процедур віддаленого доступу необхідний моніторинг міжстанційної і міжмережної інформації, захист від загрози пересилання по мережі сигналізації спеціальних директив шляхом їх фільтрування при вході у фрагмент мережі, що захищається.

Як правило, доступ до спеціальних функцій АТС, створюваних виробником, реалізується за допомогою не задокументованої адреси джерела і спрямований до інструментів експлуатаційного управління ЦАТС. Наведемо деякі не задокументовані функції:

- функція завантаження/розвантаження станційної БД. Така утиліта дозволяє завантажувати у виробника і досліджувати БД на предмет її функціонування, а також завантажувати нову БД. Існування утиліти може дозволити зловмисникові вивантажити БД системи, модифікувати її або вставити програмну закладку;

- функція перевірки/модифікації станційної БД. Утиліта дозволяє дистанційно досліджувати і модифікувати БД системи для усунення несправностей через неправильну конфігурацію, помилки конструкції тощо. Ця утиліта дає можливість модифікувати БД для одержання доступу до спеціальних функцій;

- функція наладчика/відновлення ПЗ. Така утиліта дозволяє дистанційно налагоджувати несправну систему в умовах, у яких вона несправно працює. Функція також дає можливість дистанційно обновляти системи з виявленими дефектами. Це місце найбільш вразливе, тому що доступ зловмисника до ПЗ дає практично необмежений доступ до ЦАТС і мережі.

Описані загрози можна вважати первинними або безпосередніми через розуміння загрози не тільки як деякої потенційної небезпеки, що наносить збиток інформаційній системі, але і як безпосереднього впливу на АТС EWSD, SS7 і на мережу в цілому. Нормальна робота мережі багато в чому також залежить від навантаження, створюваного на мережі SS7, тому таке навантаження необхідно контролювати.

2.4 Розрахунок надійності системи управління АТС EWSD

Обробка технологічної інформації на АТС EWSD, її зберігання та контроль за роботою системи в цілому проводиться оператором за допомогою персональної ЕОМ. Оскільки повна чи часткова втрата цієї інформації може привести до порушення роботи ЦАТС та збоїв в системі, то важливо знати, наскільки надійним є обладнання, яке використовується оператором при роботі.

Стандартом (ГОСТ 13377-75) дається таке визначення терміну «надійність»: надійність – це властивість об'єкта виконувати задані функції, збереження у часі значень встановлених експлуатаційних показників у заданих межах, які відповідають заданим режимам та умовам використання, технічного обслуговування, ремонтів, зберігання й транспортування.

Кількісною оцінкою надійності найчастіше є ймовірність безвідмовної роботи, тобто ймовірність того, що при роботі у заданих умовах система буде задовільно виконувати необхідні функції протягом встановленого проміжку часу. Така модель справедлива при умовах:

- допущення, що надійність має ймовірнісний характер за можливості появи відмовлення;
- система працює задовільно за повільного погіршення її параметрів у часі;
- система працює у незмінних умовах навколишнього середовища.

Ймовірність є величина безрозмірна, яка може приймати значення у інтервалі від 0 до 1. Якщо функції системи і критерії відмовлення точно задані, то надійність може бути точно виражена кількісно через ймовірності.

При розрахунку надійності, в залежності від призначення обладнання, на перший план висувається її безвідмовність, довговічність та ремонтопридатність.

Безвідмовність – це властивість пристрою безперервно зберігати працездатність.

Довговічність – це властивість заданий строк зберігати працездатність до руйнування або іншого граничного стану.

Ремонтопридатність – це можливість ремонту та технічного обслуговування обладнання.

Виходячи з цього, під надійністю розуміють властивість апаратури, обумовлену її безвідмовністю, довговічністю та ремонтопридатністю за умови виконання заданих функцій, тобто це здатність виконувати визначені задачі у визначених умовах експлуатації.

Велике значення в теорії та практиці надійності має поняття відмовлення. Під відмовленням розуміють подію, яка полягає в порушенні працездатності пристрою.

Оскільки відмовлення є випадковою подією, то для визначення надійності обладнання використовуються ймовірнісні характеристики – ймовірності відмовлення та безвідмовної роботи.

Ймовірністю безвідмовної роботи називається ймовірність того, що в заданому інтервалі часу t при заданих режимах і умовах роботи не відбудеться жодного відмовлення. Час t безвідмовної роботи приладу є випадковою величиною із середнім значенням T_{m}. Ймовірність безвідмовної роботи визначається з виразу:

$$P(t) = p(T_m \geq t), \tag{2.8}$$

де $p(T_{\text{m}} \geq t)$ - ймовірність того, що відмовлення не відбудеться протягом часу t, який не перевищує значення T_{m}.

При розрахунках ймовірності безвідмовної роботи використовується наступна формула:

$$P(t) = e^{-\lambda t}, \tag{2.9}$$

де λ - інтенсивність відмовлень.

Ймовірністю відмовлення $Q(t)$ називається ймовірність його, що в даному інтервалі часу відбудеться хоча б одне відмовлення:

$$Q(t) = q(T_m < t), \tag{2.10}$$

де $q(T_m < t)$ - ймовірність того, що відмовлення відбудеться в інтервалі часу t.

Оскільки несправна та безвідмовна робота є протилежними несумісними подіями, то справедлива наступна рівність:

$$Q(t) = 1 - P(t), \tag{2.11}$$

Інтенсивністю відмовлень $\lambda(t)$ називається ймовірність відмовлень не відновлюваного пристрою в одиницю часу після даного моменту часу t за умови, що до цього моменту відмовлення не виникло. Кількісно інтенсивність відмовлень виражається в числі відмовлень, що приходяться на одну годину роботи.

Наробітком на відмовлення називається середнє значення часу роботи T_m відновлюваного елемента між відмовленнями і визначається за формулою:

$$T_m = \frac{1}{\lambda} \tag{2.12}$$

При розрахунку ймовірності безвідмовної роботи пристрою інтенсивність відмовлень цього пристрою визначається за формулою:

$$\lambda = \sum_{i=1}^{n} \lambda_i \tag{2.13}$$

де n – кількість видів елементів, що складають необхідний пристрій; λ_i – загальна інтенсивність відмовлень елементів одного виду.

Розрахуємо надійність обладнання на робочому місці оператора центру технічної експлуатації. Для цього в табл. 2.1 приведемо дані про елементи, що складають ПЕОМ – їх кількість та інтенсивність відмовлень.

Розрахуємо за формулою (4.13) сумарну інтенсивність відмовлень ПЕОМ:

$\lambda = \lambda_{мон} + \lambda_{мп} + \lambda_{в} + \lambda_{д} + \lambda_{сд} + \lambda_{з} + \lambda_{пр} + \lambda_{кл} + \lambda_{м} + \lambda_{зк} = (2,6 + 3,5 + 0,2 +$ 0,19+ + 0,19 + 3 + 0,2 + 9,09 + 0,25 + 0,075) $\times 10^{-6} = 19,295 \times 10^{-6}$ 1/ч.

Тепер за формулою (2.12) розрахуємо середній час наробітку на відмовлення:

$$T_m = \frac{1}{\lambda} = \frac{1}{19,295*10^{-6}} = 51826,8(години)$$

Таблиця 2.1 – Інтенсивність відмовлень елементів персональної ЕОМ

Найменування елемента	Кількість елементів одного виду в ПЕОМ, n	Інтенсивність відмовлень одного елемента, $\lambda*10^{-6}$, 1/год.	Сумарна інтенсивність відмовлень елементів одного виду, $n*\lambda*10^{-6}$, 1/год.
Монітор	1	2,6	2,6
Системний блок: - материнська плата	1	3,5	3,5
- вінчестер	1	0,2	0,2
- дисковод 3‘5“	1	0,19	0,19
- флеш-пам'ять	1	0,14	0,14
- CD-ROM	1	0,19	0,19
- звукова плата	1	3	3
Прінтер	1	0,2	0,2
Клавіатура (клавіші)	101	0,09	9,09
Мишка	1	0,25	0,25
З‘єднувальний кабель	5	0,015	0,075

Середній час наробітку на відмовлення ПЕОМ з даною інтенсивністю відмовлень дорівнює 51826,8 години, що складає майже 6 років.

Це не означає, що ПЕОМ виходить із ладу через кожні шість років. Це означає, що у великій партії ПЕОМ, кожна з них має випадковий час наробітку на відмовлення T_i.

Якщо знайти середнє значення часу наробітку на відмовлення ПЕОМ даної партії, тобто знайти суму наробітків на відмову кожної з ПЕОМ і поділити цю суму на кількість ПЕОМ у партії, то одержимо вказані значення T_m. Якщо процеси

виникнення відмов мають властивість ергодичності, тоді середнє за ансамблем (тобто середнє значення T_i за всією партією) можна замінити середнім за часом. Тобто можна спостерігати довгий час за одним комп'ютером.

Щоб показати це наглядно, розрахуємо за формулою (2.9) ймовірність безвідмовної роботи ПЕОМ протягом цих шести років. Результати цього розрахунку зведемо в табл. 2.2. Фізичний смисл даних цієї таблиці полягає у тому, що за час роботи ПЕОМ - t ймовірність її безвідмовної роботи складає величину $P(t)$.

За результатами табл. 2.2 побудуємо графік залежності ймовірності безвідмовної роботи від часу (рис. 2.4).

Таблиця 2.2 – Ймовірність безвідмовної роботи ПЕОМ у залежності від часу

Час роботи t, ч	Ймовірність безвідмовної роботи, P(t)
0	1
10000	0,79
20000	0,63
30000	0,55
40000	0,40
50000	0,32
60000	0,25

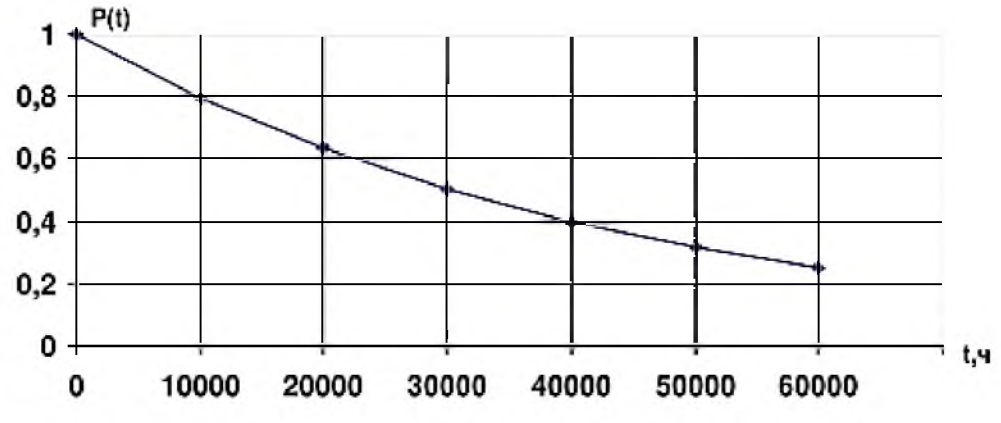

Рисунок 2.4 – Графік залежності ймовірності безвідмовної роботи ПЕОМ у залежності від часу роботи

Як видно з графіка, ймовірність безвідмовної роботи ПЕОМ за 60000 годин падає практично до нуля. А це значить, що для того, щоб попередити

пошкодження чи втрату технологічної інформації на ЦАТС внаслідок виходу з ладу ПЕОМ на робочому місці оператора, під кінець цього строку комп'ютер бажано замінити на новий.

Наведену методику розрахунку надійності можна застосовувати для широкого кола технічних пристроїв.

2.5 Рекомендації щодо обмеження фізичного доступу до устаткування зв'язку в абонентській мережі

Метод обмеження фізичного доступу до устаткування зв'язку спрямований на те, щоб унеможливити для зловмисника фізичне сприйняття інформативних сигналів, які існують у лінії зв'язку, колах апаратури та навколишньому просторі. Для досягнення такої мети слід застосовувати апаратуру, перевірену на відсутність упроваджених «закладок», пломбувати експлуатовану апаратуру, ремонт апаратури робити лише з залученням довірених фахівців під контролем власника чи співробітника служби безпеки підприємства.

Необхідно виключити будь-які ініціативні переробки впровадженої до експлуатації апаратури обслуговуючим персоналом чи ремонтниками. Особливу увагу слід звертати на легко замінювані елементи. Наприклад, кабель, що з'єднує телефонний апарат з апаратом захисту (скремблером, шифратором), може бути замінено за кілька секунд, а його конструкція й габарити припускають установлення закладки. Такі елементи слід додатково закріплювати й маркувати. Додаткове кріплення й маркування повинні бути непомітні для стороннього спостерігача, але легко перевірятися власником термінала чи допущеним обслуговуючим персоналом.

Прокладання проводів, які несуть сигнали незахищеної інформації, повинне виконуватися приховано, за можливості без роз'ємних з'єднань. Функційно необхідні роз'єми повинні додатково фіксуватися чи пломбуватися.

Для унеможливлення перехоплення інформації з електромагнітних полів бажано застосовувати сертифіковану апаратуру, виконуючи вказівки щодо її розміщення. За використання іншої апаратури бажано провести інструментальну

перевірку можливості приймання сигналів захищеної інформації у безпосередній близькості (10….15 см) від апаратури.

Кола, що відходять, повинні бути максимально віддалені від апаратури опрацьовування інформації. Кабелі, шнури, що несуть сигнал захищеної інформації, повинні бути екрановані. Оскільки застосування сертифікованої апаратури й рекомендоване розташування апаратури та кабелів в умовах комерційного підприємства часто є нездійсненні, корисним може бути розташування в складі абонентського термінала генераторів електромагнітного шуму. При цьому випромінювальні системи (антени) генераторів повинні бути максимально сполучені в просторі з випромінювальними елементами апаратури.

У цілому при організації робочого місця абонента захищеного зв'язку слід дотримуватися правил:

- на робочому місці має бути мінімум апаратури та устаткування;

- встановлення всього устаткування та елементів інтер'єра має утруднювати їхнє переміщення та заміну чи впровадження сторонніх предметів;

- на випадок, якщо відбудуться порушення розташування, заміна чи впровадження нового предмета, тоді слід вжити заходів задля виявлення й знешкодження певних дій;

- повинно бути максимально утруднене для зловмисника спостерігання за робочим процесом зв'язку й ознайомлення з системою та апаратурою захисту інформації.

Слід зазначити, що за всієї простоти пропонованих заходів, їхня реалізація й, головне, оцінювання ефективності потребують глибокого аналізу конкретної апаратури зв'язку, її розташування та приміщення, в якому встановлено термінал. Це пов'язано з тим, що більшість процесів, які призводять до витоку інформації (за винятком безпосереднього приєднання зловмисника до лінії зв'язку), мають паразитний характер, не нормуються документацією на апаратуру, не виявляються в головному робочому процесі. Багато параметрів цих процесів істотно змінюються від екземпляра до екземпляра апаратури зв'язку та сполучених з нею виробів, істотно залежать від впливів, що не впливають на головний робочий процес (наприклад, від переміщення кабелів

електроживлення).

Оцінювання значимості тих чи інших паразитних процесів у конкретній ситуації, вибір раціональних заходів щодо придушення, формування правил експлуатації термінала в частині підтримування на необхідному рівні його інформаційної захищеності вимагають високої кваліфікації та якісно можуть бути виконані лише із залученням спеціалізованої організації.

2.6 Висновки

У даному розділі:

1 Розроблено план захисту АТС EWSD.

2 Розроблено заходи захисту від витоку інформації технічними каналами.

3 Розроблено систему захисту в мережі SS7.

4 Виконано розрахунок надійності системи управління АТС EWSD.

5 Сформульовано рекомендації щодо обмеження фізичного доступу до обладнання зв'язку в абонентській мережі.

3 ЕКОНОМІЧНА ЧАСТИНА

3.1 Розрахунок собівартості послуг міської цифрової АТС EWSD

Розрахуємо собівартість послуг міського телефонного зв'язку, сформовану на основі чинної нормативно-правової бази з урахуванням системи управлінського обліку вітчизняних операторів телекомунікацій [13, 14, 15].

Критерієм для розподілення усіх статей витрат пропонується взяти частку $ФЗП_{АТС}$ (фонд заробітної плати працівників штату АТС EWSD):

$$d_{фзпАТС} = ФЗП_{АТС} / ФЗП \quad (3.1)$$

Річний фонд заробітної плати за кожною j-ою ділянкою робіт визначається:

$$ФЗП_{АТСj} = З*Шj* (1 + Н_{ФЗП})*12 , \quad (3.2)$$

де З – середньомісячна заробітна плата працівника цифрової АТС;

$Ш_j$ – штат за j-ою ділянкою робіт;

$Н_{фзп}$ – норматив відрахувань на соціальні заходи.

Частка фонду заробітної плати для кожної j-ої ділянки робіт розраховується за формулою:

$$d_{фзпАТСj} = ФЗП_{АТСj} / ФЗП_{АТС} \quad (3.3)$$

Амортизаційні відрахування за кожною j-ою ділянкою робіт обчислюються за формулою:

$$A_{АТСj} = d_{фзпАТС} * A_{АТС} \quad (3.4)$$

де $A_{АТС}$ – амортизаційні відрахування по АТС.

Матеріальні витрати за кожною j-ою ділянкою робіт подаються у вигляді:

$$M_{АТСj} = d_{фзпАТС} * M_{АТС} \quad (3.5)$$

де $M_{АТСj}$ – матеріальні витрати по АТС EWSD.

Інші операційні витрати за кожною j-ою ділянкою робіт визначаються за

формулою:

$$E_{ATCj} = d_{фзпATC} * E_{ATC} \quad (3.6)$$

де $E_{ATCін}$ – інші витрати по АТС.

Приклад розподілення витрат АТС EWSD за функціональними послугами захисту наведений у вигляді табл. 3.1.

Таблиця 3.1 – Розподілення витрат АТС EWSD за функціональними послугами захисту

Статті витрат	Номер j-ої ділянки роботи (ФПЗ)												
	Виробничий штат												Адміністративний штат
	1	2	3	4	5	6	7	8	9	10	11	12	13
1. Оплата праці з відрахуваннями ($ФЗП_{ATCj}$)	Визначається відповідно до нормативного штату АТС та середньої заробітної плати												
2. Амортизаційні відрахування (А АТСj)	Визначається відповідно до частки амортизаційних відрахувань у сумі витрат оператора або до частки амортизаційних відрахувань оператора у витратах на оплату праці оператора; за ділянками робіт розподіляється пропорційно до ФЗП для кожної з ділянок робіт												
3. Матеріальні витрати ($М_{ATCj}$)	Визначається відповідно до частки доходів від надання послуг АТС у сумі доходів оператора; або до частки матеріальних виплат оператора у витратах на оплату праці оператора; за ділянками робіт розподіляється пропорційно до ФЗП для кожної з ділянок робіт												
4. Інші операційні витрати ($Е_{ATCj}$)													
5. Усього витрат													
6. Структура витрат ($dФЗП_{ATCj}$), %													

Вихідні дані :

А. Розмір витрат ФПЗ (функціональні послуги захисту) за статтями, грн.:

- оплата праці з відрахуваннями ФЗП – 138087600,00;
- амортизаційні відрахування $А_{АТС}$ – 630000,00;
- матеріальні витрати $М_{АТС}$ – 460000,00;
- інші операційні витрати $Е_{АТС}$ – 355000,00.

Б. Штат оператора телекомунікацій, який залучено до надання ФПЗ, розраховано за нормативами чисельності штату, за ділянками робіт, осіб [15]:

1 Система захисту від впливів суб'єктів доступу через штатні термінали обслуговування і штатні прикінцеві пристрої – 0,45.

2 Система захисту від позаштатних впливів через штатні, або основні або штатні додаткові програми, і (або) технічні засоби – 0,3.

3 Системи захисту від позаштатних впливів на параметри середовища функціонування АТС – 0,3.

4 Система захисту від впливів позаштатними технічними і (або) програмно-технічними засобами на елементи устаткування в процесі експлуатації АТС – 0,7.

5 Система захисту від впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на АТС, які встановлені в процесі її експлуатації – 1,1.

6 Система захисту від впливів програмних закладок і (або) технічних закладних пристроїв, що установлені на передексплуатаційних стадіях життєвого циклу АТС – 0,3.

7 Система захисту від витоків інформації через канали ПЕМВН – 0,3.

8 Система захисту від витоків інформації через канали побічних акусто-електричних перетворень – 0,3.

9 Система захисту від якісної недостатності інформаційно вразливих режимів, функцій і послуг, що надаються АТС – 0,7.

10 Система захисту від збоїв та відмов у роботі АТС – 0,9986.

11 Система захисту від загроз у системах збереження інформації на фізичних носіях – 0,3.

12 Система ліквідації наслідків реалізованих загроз інформації – 1,1.

13 Система керування засобами ТЗІ – 1,0.

В. Середньомісячна заробітна плата – 8390 грн.

Сукупністю всіх наведених ФПЗ створена множина засобів та механізмів захисту, які забезпечують ефективний та коректний захист.

При цьому під ефективністю засобу або механізму захисту розуміється його спроможність протистояти як прямим атакам, так і всіляким лазівкам, що пов'язані з роботою засобу або механізму захисту в конкретних умовах застосування (зокрема, спроможність протистояти відключенням, обходам, ушкодженням, обманам, провокуванням тощо).

Під коректністю засобу або механізму захисту розуміється його спроможність правильно реалізувати визначену ФПЗ.

Результати розрахунків витрат за ділянками робіт занесені у табл. 3.2, де наведено функціонально повний набір механізмів захисту інформації, необхідних та достатніх, для забезпечення заданого рівня захищеності АТС EWSD.

Таблиця 3.2 - Розподілення витрат АТС за функціональними послугами захисту

Статті витрат	Номер j-ої ділянки роботи													
	Виробничий штат												Адмін.штат	Усього
	1	2	3	4	5	6	7	8	9	10	11	12	13	
1. Охорона праці з відрахуваннями ($ФЗП_{АТСj}$), грн.	6243	4162	4162	9711	15261	4162	4162	4162	9711	13854	4162	15261	13873	
2. Амортизаційні відрахування ($А_{АТСj}$), грн.	2835	1890	1890	4410	6961	1890	1890	1890	4410	6300	1890	6961	6325	
3. Матеріальні витрати ($М_{АТСj}$), грн.	2070	1380	1380	3220	5083	1380	1380	1380	3220	4600	1380	5083	4618	
4. Інші операційні витрати ($Е_{АТСj}$),грн.	1597	1065	1065	2485	3922	1065	1065	1065	2485	3550	1065	3922	3564	
5. Усього витрат, грн.	112745	8497	8497	19826	31228	8497	8497	8497	19826	28304	8497	31228	28381	222523
6. Структура витрат ($dФЗП_{АТСj}$), %.	5,73	3,82	3,82	8,91	14,20	3,82	3,82	3,82	8,91	12,72	3,82	15,80	12,75	100

3.1 Висновки

1 Витрати на штатні засоби і механізми інформаційної безпеки АТС EWSD на стадії її проектування і створення складають невелику частку загальних витрат. Вони включені у вартість систем, що постачаються, або у вартість будівництва об'єкта зв'язку.

2 Витрати на інформаційну безпеку на стадії технічної експлуатації АТС EWSD можуть досягати 20...25% загальних витрат на цій стадії. Значна їхня частина вже врахована в існуючій системі технічної експлуатації АТС EWSD.

3 Додаткові заходи і механізми забезпечення інформаційної безпеки, як правило, необхідні при досягненні високого рівня захищеності інформаційних ресурсів АТС EWSD. Для базового рівня захищеності частка витрат на додаткові засоби і механізми захисту може бути незначною.

4 Найбільша частка витрат припадає на ділянки системи захисту від впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на АТС EWSD, які установлені в процесі її експлуатації (14,20 %) та на систему ліквідації наслідків реалізованих загроз інформації на АТС EWSD (15,80%). Доцільність їх визначається при оцінках захищеності інформації та атестації КЗМЗ на відповідність вимогам системи ТЗІ.

ВИСНОВКИ

1 Визначено модель цифрової АТС EWSD з позицій технічного захисту інформації

2 Виконано аналіз загроз інформаційної безпеки АТС EWSD

3 Розроблено модель порушника

4 Розроблено політику безпеки інформації та план захисту цифрової АТС EWSD

5 Розроблено заходи захисту від витоку інформації технічними каналами

6 Виконано розрахунок границь ближньої та дальньої зон при вимірах ПЕМВН. Показано, що коли ПЕОМ є персональна ЕОМ, а середня частота її роботи - 110 МГц, границя ближньої зони становить 0,15 м, границя дальньої зони – 1,30 м

7 Розроблено заходи щодо захисту мережі сигналізації SS7

8 Сформульовано рекомендації щодо обмеження фізичного доступу до обладнання зв'язку в абонентській мережі

9 Встановлено, що найбільша частка витрат припадає на ділянки системи захисту від впливів позаштатними програмними та (або) програмно-технічними засобами на програми, дані та процеси на АТС EWSD, які встановлено в процесі її експлуатації (14,20%) та на систему ліквідації наслідків реалізованих загроз інформації на АТС EWSD (15,80%).

ПЕРЕЛІК ПОСИЛАНЬ

1 НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. – Режим доступу: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-1.1-001-99.pdf

2 НД ТЗІ 2.5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту. – Режим доступу: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-2.5-001-99.pdf

3 НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту. – Режим доступу: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-2.5-002-99.pdf

4 НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту. – Режим доступу: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-2.5-003-99.pdf

5 НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. – Режим доступу: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-2.7-001-99.pdf

6 НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінювання захищеності інформації (базова). – Режим доступу: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-3.7-002-99.pdf

7 НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. – Режим доступу: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-2.1-001-2001.pdf

8 Будько М. Методика оцінки загроз для інформації автоматизованих систем. - Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 10 вип., 2005 р.

9 ISO/IEC 15408:2000 Части 1–3. “Информационные технологии. Общие критерии оценки безопасности информационных технологий (ИТ – безопасности)”, ISO/IEC 13335:1997 «Руководство по управлению ИТ –

безопасностью», ИСО/МЭК 17799:2000 “Практические рекомендации по управлению ИТ-безопасностью”.

10 НД ТЗІ 3.7-003-05. Режим доступу: https://tzi.com.ua/downloads/3.7-003-2005.pdf

11 Типове положення про службу захисту інформації в автоматизованій системі НД ТЗІ 1.4-001-2000. Режим доступу: https://tzi.com.ua/downloads/1.4-001-2000.pdf

12 Теорія електромагнітного поля і основи техніки НВЧ: навч. Т 59 посіб. / С.В. Соколов, Л.Д. Писаренко, В.О. Журба; за заг. ред. Г.С. Воробйова. – Суми : Сумський державний університет, 2011. – 393 с.

13 Інтерактивна бухгалтерія. – Газета № 89/2020. Режим доступу: https://interbuh.com.ua/ua/documents/oneanalytics/138487.

14 Журнал Дебет-кредит. – «ДК» № 50/2011. Режим доступу: https://online.dtkt.ua/2011/50/63671

15 «Телекомунікації (електрозв’язок)». Порядок надання телекомунікаційних послуг. Режим доступу: https://i.factor.ua/ukr/journals/nibu/2014/june/issue-45/article-65762.html

ДОДАТОК А. Відомість матеріалів дипломної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	2	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	36	
6	А4	Спеціальна частина	30	
7	А4	Економічний розділ	6	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А. Відомість матеріалів дипломної роботи	1	
11	Матеріали дипломної роботи на оптичному носії	Додаток Б		Оптичний диск
12	А4	Додаток В. Відгук керівника економічного розділу	1	
13	А4	Додаток Г. Відгук керівника дипломної роботи	2	

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу

_____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г Відгук керівника дипломної роботи

ВІДГУК
на магістерську дипломну роботу

Студента(ки) _____ гр.
(прізвище, ім'я)

_____

на тему: _____

_____

_____

Актуальність теми _____

_____

_____

Повнота розкриття теми _____

_____

_____

_____

Теоретичний рівень _____

_____

_____

Практична значущість _____

_____

_____

Самостійність виконання роботи _____

_____

_____

_____

Якість оформлення, загальна та спеціальна грамотність _____

_____

_____

Переваги та недоліки роботи _____

_____

_____

_____

Загальна оцінка роботи та висновок щодо рекомендації до захисту в ДЕК

Науковий керівник

Д.т.н., професор Корнієнко В.І.

(посада) (підпис) (ініціали, прізвище)

«____»_____2022 р.