МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____ 2022 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 «Кібербезпека»

на тему: **ПІДХОДИ ДО СТВОРЕННЯ ЦЕНТРІВ ОПЕРАТИВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ НА ПІДПРИЄМСТВІ**

Студент групи СЗД-42 Токарєв Ярослав Сергійович _____
(підпис)

Науковий керівник: к.т.н., доц. Шуклін Герман Вікторович _____
(підпис)

Нормоконтроль ст. викл. Гребенніков Асаді Болдхоягович _____
(підпис)

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н., доц. Г.В. Шуклін
«_____»_____ 2022р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Токарєву Ярославу Сергійовичу

1. Тема роботи: Підходи до створення центрів оперативного управління кібербезпекою на підприємствах

Затверджена наказом по університеті від «16» лютого 2022 р. № 16

2. Термін здачі студентом оформленої роботи «____» _____ 2022 р.

3. Об'єкт дослідження: є процеси забезпечення захисту інформації в корпоративних автоматизованих системах.

4. Предмет дослідження: є методи і засоби захисту інформації в каналах зв'язку.

5. Мета роботи: підвищення рівня якості захисту інформації в телекомунікаційних мережах.

6. Перелік питань, які мають бути розроблені:

1. Аналіз загроз та каналів витоку інформації в корпоративних автоматизованих системах.
2. Вимоги до захисту інформації в корпоративних автоматизованих системах.
3. Методи і засоби захисту корпоративних автоматизованих систем від витоку конфіденційної інформації по існуючим каналам.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____2022 р.

Науковий керівник _____ Шуклін Г.В.

Завдання прийняв до виконання _____ Токарєв Я.С.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз загроз та каналів витоку інформації в корпоративних автоматизованих системах	До 25.04.22	Виконано
2	Вимоги до захисту інформації в корпоративних автоматизованих системах	До 06.05.22	Виконано
3	Методи і засоби захисту корпоративних автоматизованих систем від витоку конфіденційної інформації по існуючим каналам	До 13.05.22	Виконано
4	Перевірка роботи на плагіат +передзахист	До 01.06.22	
5	Захист роботи	З 13.06.22 по 21.06.22	

Студент _____ Токарєв Я.С.

(підпис) (прізвище та ініціали)

Керівник бакалаврської роботи _____ Шуклін Г.В.

(підпис) (прізвище та ініціали)

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АРМ - автоматизоване робоче місце

АС - автоматизована система

БД - база даних

ВОЛТ - волоконно-оптичний лінійний тракт

ВОЛЗ - волоконно-оптична лінія зв’язку

ВОСП - волоконно-оптична система передачі

ВТСС - відомчі технічні засоби зв’язку

ЕДС - елементи електрорушійної сили

ЗІ - захист інформації

ІС - інформаційна система

МВ - монітор взаємодії

НСД - несанкціонований доступ

ОВ - оптичне волокно

ОК - оптичний кабель

ОС НЦУ - операційна система національного центру управління

ПД - передача даних

ПО - програмне забезпечення

ПКУ - пункт контролю і управління

СЗІ - система захисту інформації

СЗ - система захисту

СПД - система передачі даних

СУТ - система управління телекомунікаціями

СДС - система діагностики стану

СУ ЦПМ - система управління цифрової первинної мережі

ТК - таблиці комутації

ТМ - таблиці маршрутизації

ТСР	- технічні засоби розвідки
ЦП	- цифровий підпис
ISDN	- цифрові мережі з інтегральними послугами
LAN	- локальна обчислювальна мережа
TMN	- система управління
SMP	- вузол адміністративних послуг
SMTP	- протокол електроної пошти Internet.
SCP	- транспортний протокол
SSP	- транзитна станція комутації
SMS	- нижній рівень системи
UPT	- універсальний персональний зв’язок
СТМ	- бездротовий рухомий зв’язок
TLS	- захист транспортного рівня

ВСТУП

Інформація і її захист є однією з найбільш актуальних і фундаментальних наукових проблем, значення якої важко переоцінити. На всіх етапах розвитку цивілізації люди завжди прагнули до пізнання істини, отримання нової інформації про світ, в якому вони живуть. Інформація виступає як складова частина виробничого процесу, як найважливіша компоненту соціального прогресу. У сучасних умовах захист інформації, нейтралізація інформаційної зброї противника розглядується як найважливіше завдання в забезпеченні національної безпеки кожної держави.

Для захисту інформації слід визначити інформацію, що підлягає захисту, мати чітке уявлення про можливі канали просочування інформації, провести оцінку уразливості інформації, своєчасно прийняти заходи по посиленню програмного захисту, забезпечити нормальне і безперебійне функціонування баз і банків даних, встановити контроль і управління системою захисту. Забезпечити 100-процентний захист на всі випадки життя неможливо, тому основним критерієм її ефективності служить співвідношення фінансових витрат порушника на подолання системи захисту і вартості отриманої інформації. Якщо останнє – менше витрат порушника, то рівень захисту вважається за достатній.

Дослідження проблеми захисту інформації (ЗІ) ведуться як у напрямі розкриття природи явища, що полягає в порушенні збереження інформації, так і у напрямі розробки практичних методів її захисту. Серйозно вивчається статистика порушень, причини їх виникнення, особи порушника, суть вживаних порушником прийомів, обставини, при яких було виявлено порушення Моделювання систем ЗІ (СЗІ) дозволяє визначати необхідні і достатні умови її захищеності.

Особливу увагу для захисту інформації слід звернути на використання антивірусних програм, посилення паролів, зміну алгоритму закриття і тому

подібне. Враховуючи те, що абсолютний ЗІ неможливий, а про обробку інформації вирішено, користувач повинен оцінити ступінь ризику.

Якісні оцінки ЗІ можуть бути комплексом вимог користувача до якості захисту, складу засобів захисту і їх функцій. Кількісні оцінки можуть характеризувати які-небудь небажані для користувача події або якісь конкретні параметри засобів захисту.

1 ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ. АНАЛІЗ ЗАГРОЗ ТА КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

1.1. Правові основи захисту інформації в Україні.

З того часу, як Україна стала суверенною, правовою державою, розширилось її міжнародне співробітництво, реформувалась економіка та оборона, постала необхідність створити принципово нову систему захисту інформації та законодавчого регулювання інформаційних правовідносин у сфері охорони таємниць.

У Конституції України враховані загальносвітові тенденції інформатизації суспільства. Ряд її статей (зокрема ст. 17, 32, 34) визначають забезпечення інформаційної безпеки як одну з найважливіших функцій держави і мають стати основою розвитку інформаційного законодавства.

Ми живемо у світі конкурентної боротьби за сфери впливу на міжнародній арені, світових ринках, за пріоритети у науковій, військово-технічній, економічних галузях. Тому захист інформації, охорона державної таємниці є невід'ємною складовою національної безпеки України. Отже, чинне законодавство повинне забезпечувати саме їх захист, утвердження інформаційного суверенітету України, її права на встановлення особливого порядку користування і розпорядження інформацією з обмеженим доступом.

Всього на сьогодні в Україні існує близько 60 нормативних актів, що стосуються регулювання відносин в інформаційній сфері. Робота з удосконалення нормативної бази проводиться і в даний час.

На сьогодні правову основу забезпечення технічного захисту інформації становлять Концепція національної безпеки України, Закони України

“Про інформацію”, “Про державну таємницю”, “Про захист інформації в автоматизованих системах”, інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин.

1.2. Визначення політики безпеки інформації

Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок передачі обробки інформації і спрямовані на захист інформації від певних загроз.

Термін „політика безпеки” може бути застосований щодо галузі, підприємства (організації), корпорації, системи (комп’ютерна, інформаційна, операційна), мережі та інш., на рівні яких здійснюється регламентація порядку обробки інформації відповідного рівня.

Відповідаючи загалом законам, політика безпеки конкретної системи, зокрема, повинна бути індивідуальною. Вона залежить від технології передачі, обробки інформації, використовуваних програмних і технічних засобів, структури організації т.д.

Політика інформаційної безпеки — набір законів, правил і практичних рекомендацій і практичного досвіду, що визначають управлінські і проектні рішення в області ЗІ. Для конкретної системи політика безпеки повинна бути індивідуальною.

Політика безпеки повинна визначати ресурси системи, установлювати важливість безпеки, категорії та цінність інформації, основні загрози і вимоги захисту від цих загроз, індивідуальну підзвітність персоналу, розподіляє ролі персоналу, установлюючи його обов’язки та відповідальність щодо забезпечення безпеки.

Політика безпеки визначається, як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.

При розробці політики безпеки і проведенні її в життя доцільно керуватися наступними засадами:

1. Неможливість минати захисні засоби.
2. Посилення самої слабкої ланки.
3. Неприпустимість переходу у відкритий стан.
4. Мінімізація привілеїв.
5. Поділ обов'язків.
6. Багаторівневий захист.
7. Розмаїтість захисних засобів.
8. Простота і керованість інформаційної системи.
9. Забезпечення загальної підтримки заходів безпеки.

У загальному виді сукупність заходів, спрямованих на запобігання погроз, визначається в такий спосіб:

- уведення надзаходівності технічних засобів, ПО і масивів даних;
- резервування технічних засобів;
- регулювання доступу до технічних засобів, ПО, масивам інформації;
- регулювання використання програмно-апаратних засобів і масивів інформації;
- криптографічний захист інформації;
- контроль елементів ІС;

Розмаїтість можливих видів захисту інформації визначається способами впливу на дестабілізуючі фактори захищеності інформації. Ці способи можуть бути класифіковані в такий спосіб:

Фізичні засоби — механічні, електричні, електромеханічні, електронні, електронно-механічні й інші пристрої і системи, що функціонують автономно, створюючи різного роду перешкоди дестабілізуючим факторам.

Апаратні засоби — різні електронні, електронно-механічні і подібні пристрої, що вбудовуються в апаратуру ІС чи, сполучаються з нею спеціально для рішення задач захисту інформації.

Програмні засоби — спеціальні пакети чи програм окремі програми, використовувані для рішення задач захисту.

Організаційні заходи — організаційно-технічні заходи, передбачаються спеціально в ІС з метою рішення задач захисту.

Правові заходів — законодавчо-правові акти, що існують у державі, спеціально видавані закони, зв'язані з забезпеченням захисту інформації.

Організаційно-технічні заходи:

– розробка і затвердження функціональних обов'язків посадових осіб служби інформаційної безпеки;

– створення науково-технічних і методологічних основ захисту ІС;

– виключення можливості таємного проникнення в приміщення, установки апаратури, що прослухує, і т.п.;

– перевірка і сертифікація використовуваних у ІС технічних і програмних засобів;

– розробка правил керування доступом до ресурсів системи;

– виявлення найбільш ймовірних погроз для даної ІС, виявлення уразливих місць процесу обробки інформації і каналів доступу до неї;

– оцінка можливого збитку, викликаного порушенням безпеки інформації, розробка адекватних вимог по основних напрямках захисту;

–періодичний аналіз стану й оцінка ефективності заходів захисту інформації;

Для забезпечення ефективності захисту інформації усі використовувані засоби і заходи доцільно об'єднати в систему захисту інформації, що повинна бути функціонально самостійною підсистемою.

СЗІ доцільно будувати у виді взаємозалежних підсистем, а саме:

– підсистема криптографічного захисту;

–підсистема забезпечення юридичної значимості електронних документів;

– підсистема захисту від НСД;

– підсистема організаційно-правового захисту;

– підсистема керування СЗІ.

Побудова системи захисту інформації в такому виді дозволить забезпечити комплексність процесу захисту інформації, керованість процесу і можливість адаптації при зміні умов функціонування

Підсистема криптографічного захисту поєднує засобу такого захисту інформації і по ряду функцій кооперується з підсистемою захисту від НСД. Підсистема забезпечення юридичної значимості електронних документів служить для додання юридичного статусу документам в електронному представленні і є визначальним моментом при переході до без паперової технології документообігу. Дану підсистему зручно і доцільно розглядати як частина підсистеми криптографічного захисту.

Підсистема захисту від НСД запобігає доступу несанкціонованих користувачів до ресурсів ІС.

Підсистема керування СЗІ призначена для керування ключовими структурами підсистеми криптографічного захисту, а також контролю і діагностування програмно-апаратних засобів і забезпечення взаємодії всіх підсистем СЗІ.

Підсистема організаційно-правового захисту призначена для регламентації діяльності користувачів ІС і являє собою упорядковану сукупність ор-

ганізаційних рішень, нормативів, законів і правил, що визначають загальну організацію робіт із захисту інформації.

Система захисту інформації являє собою сукупність автоматизованих робочих місць (АРМ), що входять до складу ІС, і програмно-апаратних засобів, інтегрованих в АРМ користувачів ІС.

1.3. Особливості побудови систем захисту інформації в складних корпоративних інформаційно-телекомунікаційних системах

Нинішня структура управління ІТС потребує безліч різноманітних інформаційних технологій з метою підвищення ефективності та динаміки бізнес-процесів і процесів діяльності тому в основі ІТ-інфраструктури базується на складній інформаційно-телекомунікаційній системі.

Комплекс корпоративних ІТС – це ІТС, побудована на розгалуженій обчислювальній мережі та призначена для автоматизації різних бізнес-процесів великого територіально-розподіленого підприємства.

Враховуючи структуру та склад складних корпоративних ІТС, а також різноманітну інформацію, що обробляється в різних підсистемах, що потребують захисту, інформаційні ресурси (активи) та модель потенційного порушника слід визначати для кожної прикладної підсистеми окремо. Модель потенційного правопорушника повинна поєднувати можливості

порушників, характерних для кожної підсистеми програми.

При виявленні потенційних інформаційних загроз слід враховувати такі характеристики складних корпоративних ІТС, що впливають на безпеку обробленої інформації (в частині використання різних способів реалізації інформаційних загроз):

– територіальний розподіл;

– розподіл інформаційних ресурсів у межах ІТС;

– інтеграція з розподіленими мережами;

– неоднорідність за функціональним призначенням компонентів, що входять до складу ІТС (файлових серверів, серверів додатків (HTTP, FTP та ін.), серверів СУБД, робочих станцій, активного мережевого обладнання – пристроїв маршрутизації, комутації тощо);

– неоднорідність використовуваного ОС і прикладного програмного забезпечення;

– розподіл відповідальності за адміністрування ОС, прикладних систем та інших компонентів ІТС між різними особами.

Ці характеристики призводять до того, що в складних корпоративних ІТС існує висока ймовірність виникнення загроз інформації всіх видів (конфіденційності, цілісності та доступності) різного характеру:

– об'єктивні, наприклад, викликані зміною фізичного середовища або виходом з ладу елементів ІТС;

– суб'єктивні, наприклад, помилки користувачів або дії порушників;

– випадково (ненавмисно);

– навмисні, тобто такі, що є результатом навмисних дій користувачів ІТС

– або сторонні особи для здійснення різних загроз інформації;

– прямі - безпосередньо пов'язані з порушенням встановлених в ІТС правил розмежування доступу;

– непрямі - ті, які безпосередньо не призводять до порушення

– правила розмежування встановлені в ІТС, але в деяких випадках можуть призвести до порушень прийнятої політики безпеки;

– внутрішні, викликані діями користувачів ІТС або іншими внутрішніми факторами;

– зовнішні, викликані діями третіх осіб.

Функціональний профіль інформаційної безпеки в складних корпоративних ІТС слід розробляти з урахуванням специфіки політики впровадження сервісів функціональної безпеки при реалізації комплексу засобів захисту інформації в кожній прикладній підсистемі. Важливим є використання централізованих засобів адміністрування засобів захисту та централізованих засобів контролю за дотриманням політики безпеки, для чого необхідна система управління інформаційною безпекою.

Система управління інформаційною безпекою необхідне для централізованого управління організаційно-технічними заходами та засобами інформаційної безпеки в організації, що дозволяє істотно знизити ризики потенційних загроз для захищених активів.

1.4. Загрози інформації

1.4.1. Аналіз погроз безпеки інформації

Розвиток державної системи захисту інформації неможливо без розробки й практичного освоєння фахівцями методичного забезпечення, що зачіпає такі питання, як комплексна оцінка погроз безпеки інформації, визначення збитку, нанесеного несанкціонованим поширенням інформації, правова й матеріальна відповідальність посадових осіб і фахівців за витік інформації по технічних каналах, і інших аспектів захисту інформації.

Фундаментальними властивостями захищеної інформації є конфіденційність, цілісність, доступність і спостереженість.

Конфіденційність визначається, як властивість інформації, яка полягає в тому, що вона не може бути доступною для ознайомлення користувачам і/або процесам, які не мають на це відповідних повноважень.

Цілісність інформації - це властивість, яка полягає в тому, що інформація не може бути доступною для модифікації користувачам і/або процесам, які не мають на це відповідних повноважень. Цілісність інформації може бути фізичною й/або логічною.

Доступність інформації - це властивість, що полягає в можливості її використання за вимогами користувача, який має відповідні повноваження.

Спостереженість - це властивість інформації, яка полягає в тому, що процес її обробки має безперервно знаходитися під контролем органу, що керує захистом.

Загроза - це потенційно можлива несприятлива дія на інформацію, що призводить до порушень хоча б одної з наведених властивостей.

Основними видами погроз безпеки інформації (погроз інтересам суб'єктів інформаційних відносин) є:

– стихійні лиха й аварії (повінь, ураган, землетрус, пожежа й т.п.);

– збої й відмови устаткування (технічних засобів)

– наслідок помилок проектування й розробки компонентів (апаратних засобів, технології обробки інформації, програм, структур даних)

– помилки експлуатації (користувачів, операторів і іншого персоналу);

– навмисні дії порушників і зловмисників (скривджених осіб із числа персоналу, злочинців, шпигунів, диверсантів і т.п.).

Погрозою може бути будь-яка особа, об'єкт або подія, що, у випадку реалізації, може потенційно стати причиною нанесення шкоди.

1.4.2. Показники політики безпеки

Одним зі складних і трудомістких процесів розробки системи інформаційної безпеки є дослідження можливих погроз і виділення потенційно небезпечних. Даний процес породжує необхідність рішення комплексу питань. У їхньому числі варто виділити основні:

– які цілі переслідує порушник безпеки;

– які умови й фактори сприяють можливості реалізації погроз;

– як дані фактори оцінити;

– яка потенційна небезпека окремих погроз і багато інші.

На розробку й реалізацію погроз впливає величезна кількість факторів (економічних, технічних, технологічних і т.д.). Варто виділити наступні:

–очікуваний порушником "ефект" від реалізації погроз;

–складність розробки й реалізації;

–необхідні витрати;

–можливе покарання у випадку ідентифікації погрози, порушника.

Показники політики безпеки:

– принципи безпеки, що порушують - порушення конфіденційності, цілісності, доступності системи;

–можливість запобігання;

–можливість виявлення погрози нейтралізації / відновлення;

–частота появи;

–потенційна небезпека;

–витрати на проектування й розробку зловживання;

–простота реалізації;

–потенційне покарання в рамках існуючого законодавства.

Всі погрози безпеки й зловживання доцільно розділити на три основні групи: безпечні, небезпечні, дуже небезпечні.

На основі проведеного аналізу представляється можливість опису привабливості погроз для порушника,

B_o - виграш порушника від реалізації погрози;

Со - витрати порушника для підготовки й реалізації погрози.

Отже можна стверджувати, що чим більше значення відношення Во/Со тим більше економічних підстав для реалізації погрози.

Тоді показник привабливості погрози для порушника *(y*) дорівнює:

$$\gamma = \frac{P^U B_o}{C_o}$$

де P^U - визначає середню міру успіху реалізації погрози.

Порушник прагне розробити/інтегрувати погрозу з максимальним зна-

ченням показника привабливості Основним завданням СІБ є мінімізація даного показника.

1.4.3. Аналіз загроз

Аналіз загроз є одним з найбільш важливих питань при побудові захищених систем. Аналіз має виявити можливі загрози інформації, а також показати, з якого боку й у якій точці слід чекати атаки.

Безліч різних потенційних погроз по природі їхнього виникнення розділяється на два класи: природні (об'єктивні) і штучні (суб'єктивні).

Природні погрози - це погрози, викликані впливами на інформаційну систему і її елементи об'єктивних фізичних процесів

Штучні погрози - це погрози , викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити:

– ненавмисні (випадкові) погрози, викликані помилками в проектуванні системи і її елементів

– навмисні погрози, пов'язані з корисливими діями людей (зловмисників).

До ненавмисних погроз відносяться:

– вплив сильних магнітних полів на магнітні носії інформації ;

– збої й помилки в роботі апаратури;

– ненавмисні дії, що приводять до часткової або повної відмови системи або руйнуванню ресурсів системи;

– неправомірне відключення встаткування або зміна режимів роботи пристроїв і програм;

– ненавмисне псування носіїв інформації;

– ненавмисне ушкодження каналів зв'язку.

Навмисні погрози:

– використання відомого способу доступу до системи або її частині з метою нав'язування заборонених дій;

– маскування під законного користувача ;

– фізичне руйнування системи або вивід з ладу найбільш важливих компонентів ;

– відключення або виведення з ладу підсистем забезпечення безпеки ;

– зміна режимів роботи пристроїв або програм;

– розкрадання носіїв інформації й несанкціоноване копіювання носіїв інформації;

– незаконне одержання паролів і інших реквізитів розмежування доступу з наступним маскуванням під законного користувача;

– розкриття шифрів криптозахисту інформації;

– впровадження апаратних і програмних “закладок” і “вірусів”, що дозволяють переборювати систему захисту, потай і незаконно здійснювати

таємний доступ до системних ресурсів ;

–незаконне підключення до ліній зв'язку;

Розглядаючи цілі, переслідувані порушником безпеки, варто звернути увагу на наступному: порушення конфіденційності, цілісності й доступності інформації.

У більшості випадків досягнення наведених цілей прямо пов'язується з порушенням відповідного законодавства, договірних відносин, етичних норм і приводить до відчутних втрат.

1.5. Канали витоку

1.5.1. Структура каналу витоку інформації

Будь-яка система зв'язку (система передачі інформації) складається із джерела інформації, передавача, каналу передачі інформації, приймача й одержувача відомостей. Ці системи використаються в повсякденній практиці у відповідності зі своїм призначенням і є офіційними засобами передачі інформації, робота яких контролюється з метою забезпечення надійної, достовірної й безпечної передачі інформації, що виключає неправомірний доступ до неї з боку конкурентів. Однак існують певні умови, при яких можливе утворення системи передачі інформації з однієї точки в іншу незалежно від бажання об'єкта й джерела. При цьому, природно, такий канал у явному виді не повинен себе проявляти. За аналогією з каналом передачі інформації такий канал називають каналом витоку інформації. Він також складається із джерела сигналу, фізичного середовища його поширення й апаратури що приймає сигнал на стороні зловмисника. Рух інформації в такому каналі здійснюється тільки в одну сторону - від джерела до зловмисника. На рис. 1.1 наведена структура каналу витоку інформації.

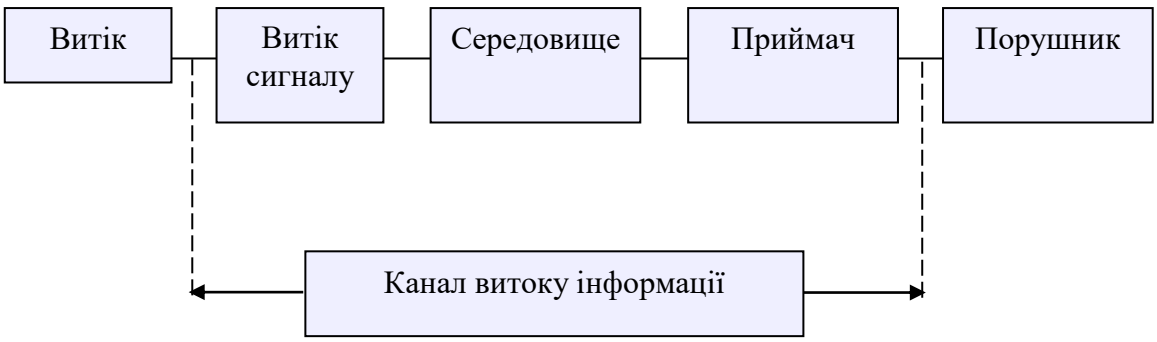


Рис.1.1. Структура каналу витоку інформації

Під каналом витоку інформації будемо розуміти фізичний шлях від джерела конфіденційної інформації до зловмисника, по якому можливий витік або несанкціоноване одержання охоронюваних відомості.

Витік - безконтрольний вихід конфіденційної інформації за межі організації або кола осіб, якою вона була довірена

1.5.2. Класифікація каналів витоку інформації

Всі канали проникнення в систему й витоки інформації розділяють на прямі й непрямі. Під непрямими розуміють такі канали, використання яких не вимагає проникнення в приміщення, де розташовані компоненти системи. Для використання прямих каналів таке проникнення необхідно. Прямі канали можна використати без внесення змін у компоненти системи або зі змінами компонентів.

По способі одержання інформації потенційні канали доступу можна розділити на:

– фізичний;

– електромагнітний (перехоплення випромінювань);

– інформаційний (програмно-математичний).

При контактному НСД (фізичному, програмно-математичному) можливі погрози інформації реалізуються шляхом доступу до елементів ІС, до носіїв інформації), до програмного забезпечення (у тому числі до операційних систем), а також — шляхом підключення до ліній зв'язку.

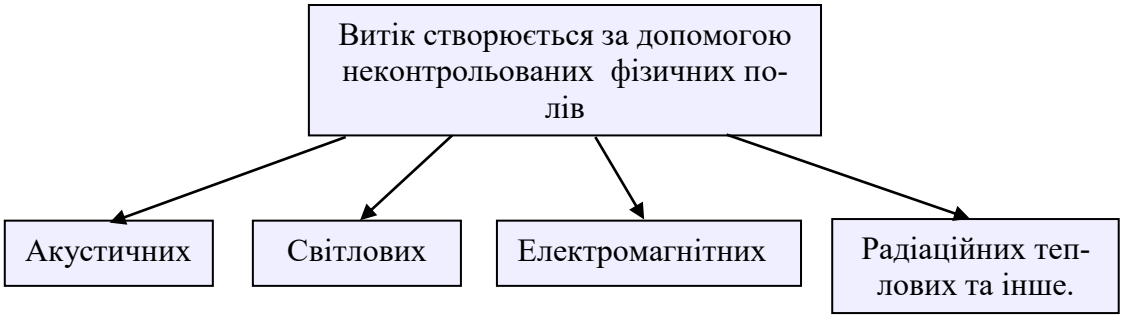


Рис.1.2. Витік інформації

При безконтактному доступі (наприклад, по електромагнітному каналі) можливі погрози інформації реалізуються перехопленням випромінювань апаратури ІС, у тому числі, що наводять у струмопровідних комунікаціях і ланцюгах живлення, перехопленням інформації в лініях зв'язку, уведенням у лінії зв'язку помилкової інформації, візуальним спостереженням (фотографуванням) пристроїв відображення інформації, прослуховуванням переговорів персоналу ІС і користувачів. Все це створює технічні канали витоку інформації

Технічні канали витоку інформації - фізичний шлях від джерела інформації до зловмисника, за допомогою якого може бути здійснений несанкціонований доступ до охоронюваних відомостей.

За фізичною природою технічні канали витоку інформації можна поділити на декілька груп:

– радіоканал (електромагнітні випромінювання в радіодіапазоні);

– акустичний канал (розповсюдження звукових коливань в будь-якому звукопровідному матеріалі);

– електричний канал (напруга та струм в різноманітних токопровідних комунікаціях);

– візуально-оптичний канал (електромагнітні випромінювання в інфрачервоній, видимій та ультрафіолетовій частині спектру);

– матеріально-речовинний канал (папір, фото, магнітні носії, відходи

та. ін.), які в свою чергу можуть бути поділені на групи по способу створення, природі створення середовищі розповсюдження та діапазону (рис.1.3).

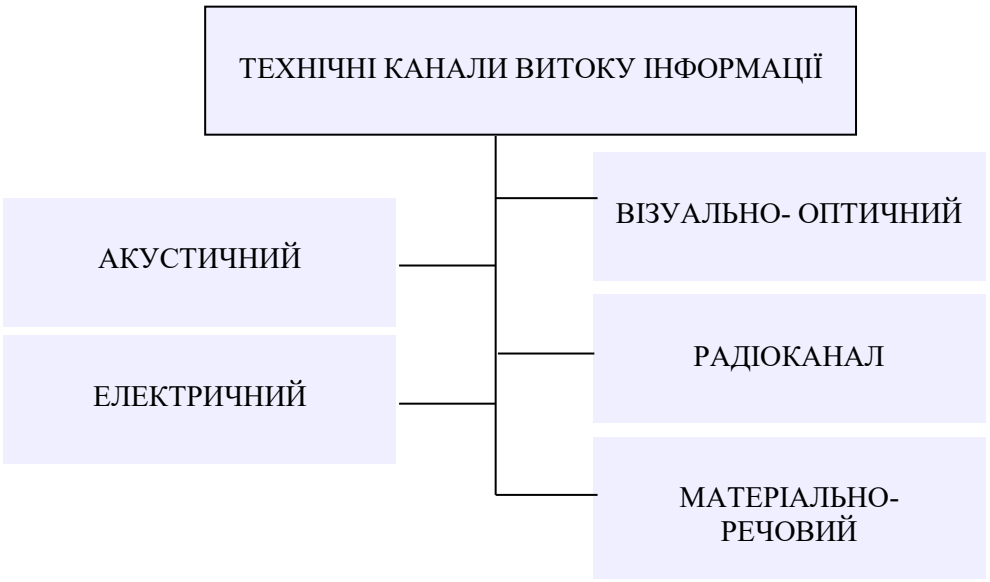


Рис.1.3. Канали витоку інформації

Ґрунтуючись на цьому, можна стверджувати, що по фізичній природі можливі наступні засоби переносу інформації:

- світлові промені;
- звукові хвилі;
- електромагнітні хвилі;
- матеріали й речовини.

2 ЗАХИСТ ІНФОРМАЦІЇ

2.1. Основні визначення

На рис. 2.1 наведена класифікація основних визначень предметної області «Захист інформації».

Рис. 2.1. Основні визначення предметної області „Захист інформації”

Інформація – відомості про осіб, предметах, фактах, подіях, явищах і процесах незалежно від форми їхнього подання.

Інформація, що захищається - інформація, що є предметом власності й підлягає захисту відповідно вимог власника інформації. Власником інформації може бути: держава, юридична особа, група фізичних осіб, окрема фізична особа.

Захист інформації – діяльність, спрямована на запобігання витоку інформації що захищається , несанкціонованих і ненавмисних впливів на інформацію що захищається.

Захист інформації від витоку – діяльність, спрямована на запобігання неконтрольованого поширення захищає інформації, що, у результаті її розголошення, несанкціонованого доступу до інформації й одержання захищає інформації, що, розвідками.

Захист інформації від несанкціонованого впливу – діяльність, спрямована на запобігання впливу на захищаєму інформацію, що, з порушенням установлених прав і (або) правил на зміну інформації, приводить до її перекручування, знищення, блокуванню доступу до інформації, а також до втрати, знищення або збою функціонування носія інформації.

Захист інформації від ненавмисного впливу – діяльність, спрямована на запобігання впливу на захищаєму інформацію, що то, помилок її користувача, збої технічних і програмних засобів інформаційних систем, природних явищ або інших нецілеспрямованих на зміну інформації заходів, що приводять до перекручування, знищення, копіюванню, блокуванню доступу до інформації, а також до втрати, знищення або збою функціонування носія інформації.

Захист інформації від розголошення – діяльність, спрямована на запобігання несанкціонованого доведення інформації що захищається до споживачів, що не мають права доступу до цієї інформації.

Захист інформації від несанкціонованого доступу – діяльність, спрямована на запобігання одержання захищає інформації, що, зацікавленим суб'єктом з порушенням установлених правовими документами або власником, власником інформації прав або правил доступу до інформації що захищається.

2.2. Вимоги до систем телекомунікацій

Приведемо основні вимоги, пропоновані користувачами до систем телекомунікацій з позицій забезпечення захисту переданої інформації. Системи телекомунікацій повинні забезпечити:

– конфіденційність інформації – забезпечення перегляду інформації в прийнятному форматі тільки для користувачів, що мають право доступу до цієї інформації;

– цілісність інформації – забезпечення незмінності інформації при її передачі;

–автентичність інформації – забезпечення надійної ідентифікації джерела повідомлення, а також гарантія того, що джерело не є підробленим.

–доступність інформації – гарантія доступу санкціонованих користувачів до інформації..

2.3. Загальний підхід до побудови системи захисту

Захист інформації телекомунікаційних мереж охоплює дуже широке коло питань. Досить сказати, що під поняттям „телекомунікаційні мережі” кожний, навіть близький до предметної області ” зв’язок”, розуміє все, що відноситься до ліній, засобів зв’язку. Не акцентуючи при цьому увагу на тому, що це можуть бути магістральні мережі, лінії і засоби міських мереж, корпоративні мережі, окремі види зв’язку. Це позиція користувача. І він правий – він хоче мати певну послугу, на певному місці і в певний час, з певною якістю. Забезпечити приведене – це задача зв’язківців.

Проектування системи захисту інформації для різних об’єктів, систем, галузі, видів зв’язку і мереж має масу особливостей і повинне здійснюватися індивідуально. Охопити все це в рамках одного проекту неможливо.

В бакалаврської роботі розглянуті рішення по побудові СЗІ, які можуть бути використані, в певному обсязі, в більшості інформаційних систем різного рівня та призначення. При цьому використані методичні, інформаційні матеріали з побудови аналогічних систем.

У багатьох існуючих системах телекомунікацій для доступу до системи, при підтвердженні ідентифікації, для одержання послуг, а також для керування ними використається тільки Персональний ідентифікаційний номер (PIN) або пароль. Дана "слабка ідентифікація" - украй ненадійна, доцільніше використати механізми захисту, засновані на криптографічних ключах і алгоритмах шифрування.

Однак ідентифікація користувача не є єдиним аспектом захисту мережі. Для мереж загального користування важливо виключити можливість доступу до об'єкта іншої системи. Необхідно запобігти нелегальній реєстрації об'єкта, підслуховування або модифікації переданих даних. Треба, залежно від оцінки ризику, задіяти такі міри захисту, як еквівалентна ідентифікація об'єкта, перевірка схоронності даних, кодування й інших.

Загальний підхід до побудови системи захисту, як показано на рис. 2.1 (з відповідними модифікаціями), успішно використався в багатьох дослідницьких проектах і проектах по стандартизації (наприклад, європейський проект Технологія схоронності механізмів в IBCN у рамках програми RACE, стандарт ETSI для захисту UPT, а також дослідження ITU-T по захисту FPLMTS).

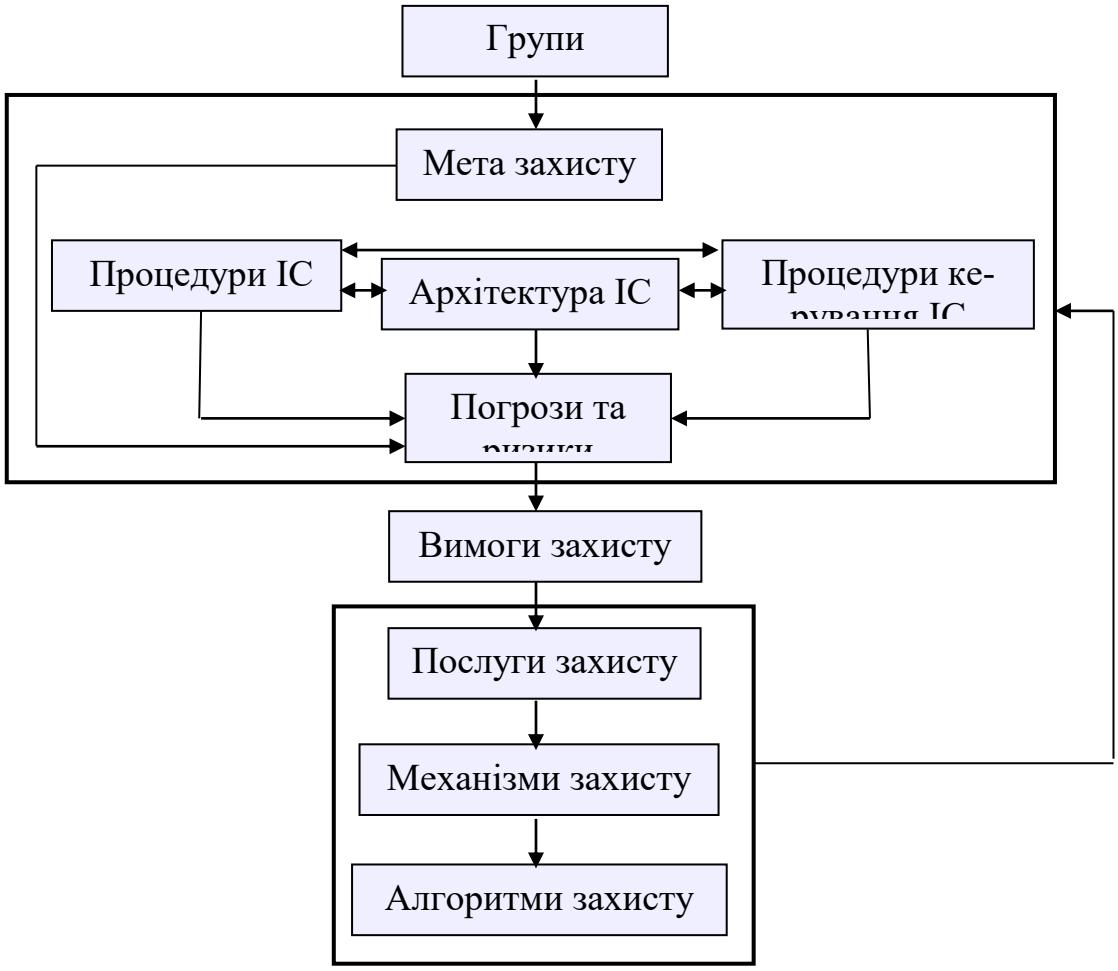


Рис. 2.1. Підхід до побудови системи захисту

Структурна схема на малюнку 2.1. показує логічну послідовність дій при проектуванні системи захисту.

Необхідно особливо підкреслити, що як основу необхідно мати загальний вигляд побудови системи, характеристик і процесів, що ставляться до системи захисту. Крім того, необхідно враховувати цілі системи захисту всіх задіяних груп.

На наступному етапі необхідно провести ретельний аналіз всіх погроз, включаючи оцінку ризику. Даний аналіз погроз повинен ураховувати всі представлені послуги , задіяні групи й елементи системи, певні в області си-

стеми захисти. Тільки на основі даного аналізу погроз можуть бути визначені вимоги до системи захисту, а потім послуги, механізми й алгоритми.

Процедуру необхідно повторити щоб уникнути неврахованих погроз. Після цього враховуються загальні цілі системи захисту й загальних умов погрози й захисту.

Для ІС загалом, обговорюються рішення, прийняті на основі існуючої технології по безпечній комунікації й захисту комп'ютера. Окремо розглядається рішення по захисту доступу користувача, засноване на використанні ІС-карт і завантаженню відповідного програмного забезпечення на термінали.

Цілі, що впливають на захист, виходять із вимог різних суб'єктів, а саме:

– користувачів,

– провайдерів послуг і провайдерів мережі,

– органів керування ІС.

Цілі користувачів послуг є аспекти, пов'язані із правильним функціонуванням і конфіденційністю, провайдерів послуг - одержання гарного річного доходу при роботі в системі органів керування ІС- певні вимоги, пов'язані з конфіденційністю, гарним захистом інформації й інфраструктури, обмеженням використання криптографічних методів і виправданістю дій.

Перераховане вище може бути зведено до однієї або до комбінації наступних основних цілей, що стосуються послуг ІС або керування ІС:

– конфіденційність даних;

– схоронність даних;

– ураховуваність;

– доступність.

Рішення для системи захисту керування ІС, представлені на рис.2.3. ґрунтуються на наступних припущеннях:

–SMP, SCP і OS (Operation System) уводяться в дію на стандартній платформі UNIX з елементами захисту UNIX.

–На використовуваних лініях передачі (через LAN, ISDN, Інтернет) не були реалізовані послуги конфіденційності й схоронності інформації.

Для забезпечення безпечного зв'язку між передплатниками провайдерами послуг і SMP, можна використати існуючі криптоблоки.

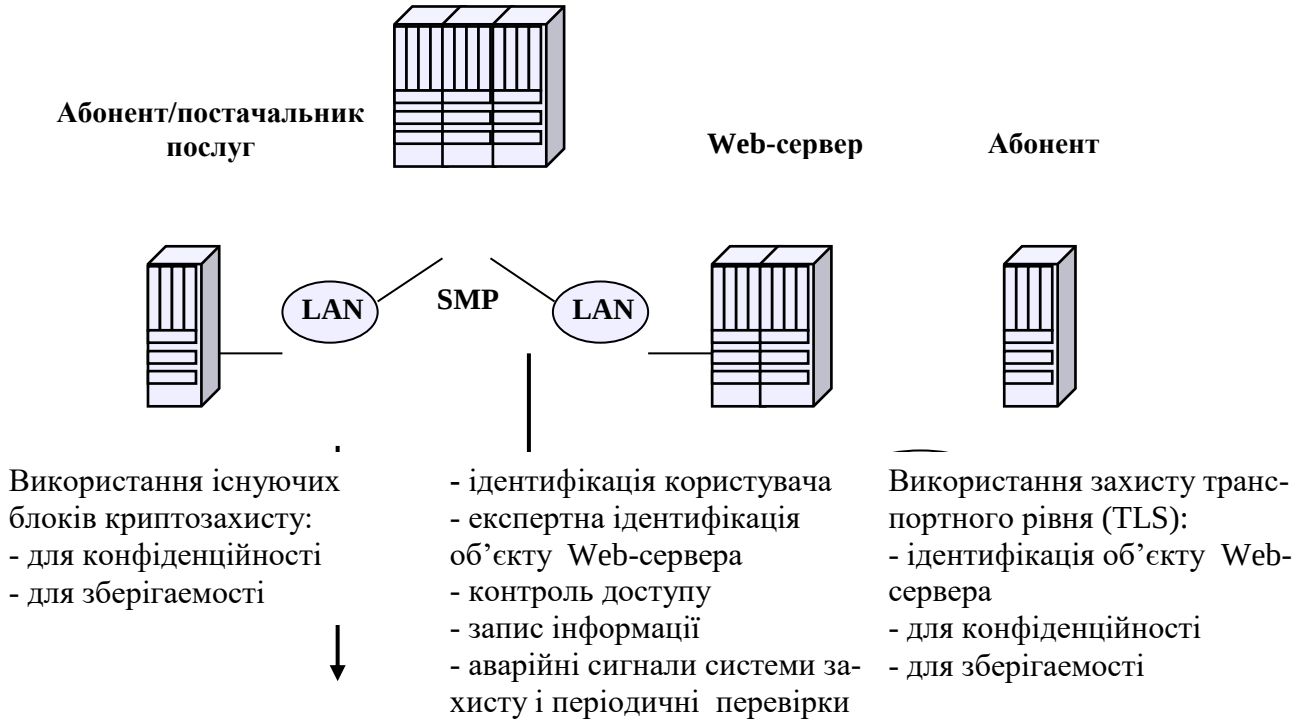


Рис. 2.3. Рішення системи захисту для керування ІС

Вибір механізмів захисту може залежати від індивідуальної послуги ІС, уведення в роботу системи ІС, фізичного оточення, у якому перебувають елементи системи, а також від взаємної довіри й відносин між задіяними організаціями

У таблиці 2.1 представлена залежність між погрозами й функціональними вимогами до СЗ. Вона складена на основі результатів Групи захисту ETSI TMN.

Таблиця 2.1.

Погрози й вимоги до системи захисту

Вимоги до системи захисту	Види погроз						
	Погрози елементам ІС					Погрози під час передачі	
	Нелегальне проникнення	Несанкціонований доступ	Відмова підтвердження	ах ай тво	Відмова від виконання послуг	Підслухо вування	аль-сифі-кація
Підтвердження ідентифікації	*	*	*		*		
Гарантія конфіденційності ЗД		*			*		
Гарантія зберігаемості ЗД и ПО		*			*		
Не відмова від дій	*		*				
Визначення спроб порушення захисту	*	*	*		*	*	»
Гарантія схоронності КД						*	
Гарантія конфіденційності КД							»

Примітка: ЗД – Зберігаемі данні, КД - комунікаційні данні

На основі певних цілей, описаних погроз і варіантів ризику, функціональні вимоги до системи захисту представлені для тих елементів і з'єднань, потенційний ризик яких оцінюється як найбільш високий. Дані вимоги показані в таблиці 2.2.

Таблиця 2.2

Вимоги до системи захисту

Для елементів ІС	Для ліній зв'язку
Підтвердження ідентифікації користувача передплатника (якщо можливо)	Гарантія конфіденційності даних
Підтвердження ідентифікації комунікаційного партнера	Гарантія схоронності даних
Гарантія конфіденційності даних	****
Гарантія схоронності ПО й даних	****
Не відмова від дій	****
Визначення спроб порушення захисту	****

Кожна вимога до СЗ повинне бути виконана за допомогою однієї послуги захисту, з позначених у таблиці 2.3.

Кожна послуга здійснюється за рахунок одного з механізмів СЗ. Наприклад, механізми експертної ідентифікації об'єкта можуть бути засновані на заміні захищеного пароля, секретного ключа, загальнодоступного ключа або хешированих технологій. Механізм індивідуальної ідентифікації застосуємо до однобічної й взаємної ідентифікації. Однобічна ідентифікація означає, що тільки одна із двох взаємодіючих сторін (активна сторона) ідентифікована для іншої сторони (приймаючої сторони). При взаємній ідентифікації обидві сторони ідентифікують один одного.

Таблиця 2.3

Послуги захисту

Для елементів ІС	Для ліній зв'язку
Ідентифікація користувача для провайдерів послуг і передплатників	Конфіденційність
Експертна ідентифікація комунікаційного партнера	Схоронність
Контроль доступу до ПО й даним	
Безвідмовність	
Запис дій	
Реєстрація аварійних сигналів СЗ	
Періодична перевірка СЗ	

Кожний механізм СЗ може використати певний алгоритм. Наприклад, механізм ідентифікації, заснований на секретних ключах, може використати один з наступних алгоритмів: DES, потрійний DES або алгоритм FEAL і т.д.

Крім того, можуть бути корисними чисто організаційні міри, наприклад, керування якістю, контрольована вхід у приміщення, відповідальність сторін, обговорена в контракті. Якщо ризик продовжує становити більшу небезпеку, кількість послуг повинне бути зменшене, а платежі обмежені певними сумами.

2.4. Захист каналів зв'язку

2.4.1. Контроль телефонних розмов

Контроль телефонних розмов є одним з найпоширеніших видів промислового шпигунства й дій злочинних елементів. Це пов'язане з незначними витратами й ризиком, необов'язковістю заходу в контрольоване приміщення, розмаїтістю способів і місць знімання інформації.

У числі засобів перехоплення телефонних переговорів різноманітні пристрої контактного й безконтактного підключення до телефонних ліній, спеціальні телефонні «жучки» і т.д. Сучасні засоби й методи захисту телефонних переговорів від перехоплення протидіють практично всій розмаїтості засобів їхньої реалізації.

Фахівці виділяють два основні технічні різновиди протидій:

– засобу фізичного захисту інформації, що включають у себе постановники загороджувальних перешкод, нейтралізатори, фільтри й засоби пошуку каналів витоку інформації;

– засобу значеннєвий (криптографічної) захисту інформації.

Нові технічні рішення дозволяють комплексно вирішувати питання й виявлення факту підслуховування телефонних переговорів і гарантованого придушення багатьох видів техніки перехоплення.

Для забезпечення фільтрації сигналів, що виникають у телефонній лінії при покладеній трубці за рахунок мікрофонного ефекту або ВЧ- нав’язування розроблені й випускаються серійно недорогі прилади. В Україні випускаються прилади серії «Рікас» і «Базальт». Нейтралізатори призначені для виведення з ладу (пропалювання) пристроїв, гальванічні підключених до теле-

фонної лінії. Це такі прилади, як «КС-1303», «Кобра». На виході цих приладів створюється короткочасна високовольтна напруга (до 1500 вольтів), подаване в лінію. Пристроїв захисту телефонних переговорів, що створюють загороджувальні перешкоди, безліч, але найбільш ефективними є такі, як «Цикада-М», «Прокруст», «Акорд-200», «Бар'єр-3», «Грім», що забезпечують захист від телефонного апарата до АТС. Принцип захисту, організований цими пристроями полягає в тому, що в лінію видається шумова перешкода поза смугою мовного сигналу й перевищує його номінальний рівень на один-два порядків. Наявність інтенсивної перешкоди виводить із лінійного режиму пристрою, як гальванічно підключених до лінії, так і індуктивних. Зловмисник через свій пристрій чує сильний шум, що забиває мовний сигнал. Абоненти, що ведуть переговори чують незначний шум, що не заважає розмові, завдяки попередній високочастотній фільтрації вихідного сигналу.

Окремо слід зазначити маскувальники мови серії «Туман», що використають зовсім нову технологію захисту. Особливість у тім, що шумова перешкода, що діє за межами мовного діапазону частот, замінена на перешкоду в мовному діапазоні. Така перешкода формується за псевдовипадковим законом і міняється від сеансу до сеансу.

Природно такий детермінований підхід дає можливість компенсувати перешкоду на своєму кінці

Недоліки однобічних маскувальників :

– неможливість закриття вихідних повідомлень.

–наявність сильного шуму в трубці абонента, що передає повідомлення.

Відсутність у приладах такого класу протидії перехопленню мовної інформації із приміщення, по якому проходить телефонна лінія, у режимі відбою лінії.

Криптографічний захист телефонних розмов уважається найбільш гарантованим захистом від перехоплення по будь-яких видах зв'язку. Пристрої

криптографічного захисту телефонних переговорів звуться скремблери. Найпоширенішими є скремблери серії SCR і «Горіх». Для організації захисту необхідно мати скремблери в обох абонентів і встановити систему уведення ключів.

Скремблери реалізують криптографічне перетворення як для аналогових телефонних повідомлень, так і для цифрових (вакодеры). Необхідно відзначити, що мова при цьому зберігає прийнятну розбірливість, але пізнати абонента по тембрі голосу буває важко.

Робота таких систем ділиться на кілька етапів. На першому етапі мовне повідомлення абонента обробляється по якому-небудь алгоритмі (кодується) так, щоб зловмисник, що перехопив оброблений сигнал, не зміг розібрати значеннєвий зміст вихідного повідомлення. Потім оброблений сигнал направляється в телефонну лінію. На останньому етапі сигнал, отриманий іншим абонентом, перетвориться по зворотному алгоритмі (декодується) у мовний сигнал з неминучою втратою якості.

Для того, щоб розкрити зміст захищеної криптографічним способом телефонної розмови, зловмисникові буде потрібно:

– наявність криптоаналітика;

– дороге устаткування;

–якийсь час для проведення криптоаналізу.

Останній фактор може звести нанівець всі зусилля, оскільки до моменту розкриття повідомлення висока ймовірність того, що воно вже застаріло. Крім того, момент розкриття може взагалі не наступити. .До достоїнств криптографічних систем варто віднести те, що захист відбувається на всьому протязі лінії зв'язку й байдуже якими апаратурами перехоплення користується зловмисник, він однаково не зможе в режимі реального часу розшифрувати повідомлення.

2.4.2. Конфіденційність електронної переписки

У цей час конфіденційність електронної переписки можна забезпечити декількома способами. Всі вони опираються на потужні засоби шифрування, ідентифікації й фіксації авторства для гарантії того, що відправляють і одержувані повідомлення відповідають оригіналу й надходять дійсно від зазначених осіб.

Розроблений RSA в 1996 році, S/MIME став досить розповсюдженим і широко визнаним стандартом обміну повідомленнями. Технологія опирається на стандарт шифрування з відкритими ключами, і, таким чином, її реалізаціям гарантована сумісність на криптографічному рівні. Двома основними відмітними рисами S/MIME є цифровий підпис і цифровий конверт. Цифровий підпис гарантує, що повідомлення не було змінено в процесі передачі. Крім того, її наявність не дозволить відправникові відмовитися від свого авторства.

Підпис являє собою зашифроване за допомогою особистого ключа відправника резюме повідомлення (саме резюме обчислюється з використанням алгоритму хешування). Для перевірки цілісності повідомлення одержувач розшифровує підпис за допомогою відкритого ключа відправника. Якщо резюме, що вийшло, не збігається з обчисленим, це означає, що повідомлення було змінено в процесі передачі.

Однак цифровий підпис не гарантує конфіденційність повідомлення. В S/MIME цю функцію виконує цифровий конверт. Шифрування здійснюється за допомогою симетричного алгоритму типу DES, Triple DES або RS2.

Симетричний ключ шифрується за допомогою відкритого ключа одержувача, а зашифроване повідомлення й ключ передаються разом. Крім забезпечення захисту повідомлення й гарантії його незміни під час передачі S/MIME ідентифікує власника конкретного відкритого ключа за допо-

могою цифрових сертифікатів X.509. Цифровий сертифікат засвідчує, що відкритий ключ дійсно належить тому, від чийого імені він публікується.

2.4.3. Міжмережеві екрани

Часто міжмережеві екрани використаються для створення захищеного від перегляду каналу між декількома сегментами мережі Internet. Ця функція дозволяє дуже ефективно використати можливості Internet для корпоративних цілей. Для створення таких каналів застосовуються спеціальні протоколи шифрування інформації. Алгоритми шифрування з відкритим ключем звичайно працюють повільно, тому для шифрування більших потоків інформації задіються алгоритми, у яких для шифрування й дешифрації використається однаковий секретний ключ. Складність використання симетричного шифрування полягає в тім, що відправник і одержувач повідомлень повинні знати однаковий секретний ключ. Це означає, що передавати по мережі такий ключ незашифрованим не можна. Але передавати його потрібно. Найбільш перспективне рішення цієї проблеми - шифрувати секретні ключі по несиметричному алгоритмі, а основний текст повідомлення - по симетричному із застосуванням секретних ключів. При цьому знову виникає потреба в розвитий системі сертифікатів для передачі повідомлень за допомогою алгоритму відкритих ключів.

2.4.4. Захист потоків маршрутизатором

Маршрутизатори Advanced Remote Node (ARN), Access Stack Node 2 (ASN2) і BackBone Node (BN)мають можливість керування доступом, протоколювання переданих потоків, шифрування даних при передачі пакетів і інші властивості, необхідні для побудови між мережевого екрана. Їх можна використати для побудови всієї мережі підприємства, що дозволяє створити кілька рівнів захисту для різних сегментів мережі.

2.4.5. Захист від перехоплення

Від нього можна захиститися за допомогою шифрування вмісту повідомлення або каналу, по якому він передається. Якщо канал зв'язку зашифрований, то системні адміністратори на обох його кінцях все-таки можуть читати або змінювати повідомлення. Було запропоновано багато різних схем шифрування електронної пошти, але жодна з них не стала масовою.

2.4.6. Захист електронної пошти

Електронна пошта (ЕП) у цей час широкий використається завдяки своїй дешевині й оперативності. Питання захисту повідомлень, забезпечення

їхньої цілісності й дійсності, а іноді й конфіденційності, важливі навіть при передачі особистої пошти.

Використається кілька протоколів передачі й прийому ЕП. Основними протоколами є протоколи SMTP, POP3. Як показує аналіз цих протоколів можливо підміна окремих частин листа, їхнє видалення або вставка нової інформації. Можна навіть створювати нові листи, минаючи поштовий клієнт і «одержувати» листи, які не відправляв сервер. Тому проблема захисту ЕП є актуальною.

Існуючі засоби захисту убудовані в клієнтські програми роботи. Ці засоби забезпечують цифровий підпис (ЦП) і шифрування, але надійність цих засобів дуже мала, довжина ключа в 40 біт не забезпечує достатнього рівня захищеності.

Останнім часом великою популярністю користується алгоритм RSA с ключами довжиною до 4096 біт (починаючи з версії 5.0) і симетричний алгоритм шифрування (IDEA) с довжиною ключа 128 біт.

Збільшення довжини ключа істотно збільшує час, необхідний для ЦП, тому що формування ЦП зводиться до виконання операції модульного зведення в ступінь. Незважаючи на численні методи прискорення цієї операції, час виконання залишається істотним при обробці поштових повідомлень. Є й інші підходи до рішення проблеми злому RSA алгоритмів, засновані на зміні зашифрованого особистого ключа й аналізі підпису, зробленої зміненим ключем. Тому застосування убудованих засобів захисту для передачі важливої інформації з ЕП неможливо.

Розглянемо вимоги до системи захисту ЕП.

–Вона повинна забезпечувати всі послуги безпеки, які визначаються ISO 7498-2 з допомогою національних криптографічних алгоритмів, а саме: конфіденційність інформації, цілісності інформації, причасність, автентифікація, управління доступом.

– Вона повинна підтримувати роботу з основним поштовим клієнтом, такими як OUTLOOK EXPRESS, MS OUTLOOK, The Bat!

– Вона повинна бути прозорою для користувача

– Вона повинна бути кросплатформеною.

Помітимо, що перша вимога обов'язково, всі інші – бажані. Як криптографічні алгоритми будемо використати алгоритми, прийняті як стандарти на Україні. Для ЦП використаються алгоритми ДЕРЖСТАНДАРТ 34.310-95, ДЕРЖСТАНДАРТ 34.311-95, для шифрування ДЕРЖСТАНДАРТ 28147-89.

Розгортання інфраструктури з відкритими ключами має важливе значення не тільки для організації захищеного обміну повідомленнями, але й для створення захищеної системи ідентифікації в мережі, і для надання користувачам прав доступу до баз даних, каталогам і іншим мережним компонентам. Захищений обмін повідомленнями, надійна ідентифікація й електронна комерція неможливі без інфраструктури з відкритими ключами (Public Key Infrastucture, PKI).

2.5. Захист інформації в волоконно-оптичних лініях зв'язку

Останнім часом одним з найбільш перспективних напрямків побудови мережі зв'язку в Україні й у світі є волоконно-оптичні лінії зв'язку (ВОЛЗ).

Вони значно перевершують провідні за такими показниками, як пропускна здатність, довжина регенераційної ділянки, а також перешкодозахищеність.

Уважається, що ВОЛЗ, у силу особливостей поширення електромагнітної енергії в оптичному волокні (ОВ), мають підвищену скритність. Оптичне випромінювання, що є носієм інформації, поширюється в ОВ відповідно до

закону повного внутрішнього відбиття, а за ОВ електромагнітне випромінювання експоненціально спадає.

Але, не зважаючи на технічну складність НСД до інформації, яка передається по волоконно-оптичних мережах зв'язку, можливість такого випадку завжди треба враховувати Існує можливість знімання інформації з волоконно-оптичного тракту (ОТ) шляхом фізичного доступу до ОВ ОТ і відводу частини оптичного сигналу, що поширюється по ОВ .Таким чином, при НСД необхідно вивести із ОВ оптичний сигнал і зібрати його. При локальному виводі сигналу, тією чи іншою мірою змінюються параметри ОТ, фіксація яких дозволяє фіксувати НСД й забезпечувати захист інформації шляхом переривання її передачі.

2.5.1. Оцінка впливу на параметри ОТ знімання інформації при НСД

Уведемо наступні позначення: P_s, $P_г$, $P_х$ – потужності оптичних сигналів, відповідно на початку ОТ, наприкінці ОТ і в місці знімання інформації. $\Delta\alpha$ [дБ/км] – загасання ОТ, Е - енергетичний потенціал приймально-передавачів ВОСП.

При НСД в результаті впливу на ОВ виникає неоднорідність, із ОВ випливає оптичний сигнал $\Delta P_к$, частина якого збирається на фотоприймачі системи НСД – $P_к$, при цьому в ОТ вноситься додаткове загасання $\Delta\alpha_к$.

Уведемо наступні коефіцієнти:

ДО=$P_к / P_х$ – коефіцієнт зв'язку пристрою НСД;

N= $P_к / \Delta P_к$ – коефіцієнт збору пристрою НСД;

$К_{зч}=P_{го}/P_{ко}$ – коефіцієнт запасу чутливості пристрою НСД, де $P_{го}$, $P_{ко}$ – чутливість відповідно фотоприймачів ВОСП і пристрою НСД.

З умови $P_к \geq P_{ко}$ можна одержати умови працездатності пристрою НСД:

$\alpha_x \leq E + K_{зч} + ДО$, дБ

При цьому внесене загасання дорівнює

$\Delta\alpha_{до} = 10 \lg(1-\Delta P_к / P_x)$

У цей час експерименти дозволяють оцінювати мінімально внесене додаткове загасання ОТ при НСД в 0,1-0,5 дБ, що приводить до флуктуації $P_г$ порядку 0,02.

Таким чином, реалізація пристрою НСД приводить до досить малих змін параметрів ОТ, необхідності проектування систем захисту ВОСП від несанкціонованого знімання інформації.

2.5.2. Способи знімання

Способи знімання, які можуть бути використані для перехоплення інформації з ВОЛС, можна умовно розділити на кілька груп.

1. По способі приєднання:
   - безрозривний;
   - розривний;
   - локальний;
   - протяжний.

2. По способі реєстрації й посилення:

– пасивні - реєстрація випромінювання з бічної поверхні ОВ;

– активні - реєстрація випромінювання, виведеного через бічну поверхню ОВ за допомогою спеціальних засобів, що міняють параметри сигналу у ВОЛТ;

– компенсаційні - реєстрація випромінювання, виведеного через бічну поверхню ОВ за допомогою спеціальних засобів з наступним формуванням і уведенням в ОВ випромінювання, що компенсує втрати потужності при висновку випромінювання;

Основним і найбільш популярним способом безрозривного локального НСД є спосіб лінзового фокусування сингулярних (витікаючих) мод на вигині волокна.

Пристрої розривного НСД дозволяють здійснювати більше надійне знімання інформації. Однак розривне підключення вимагає тимчасового вимикання лінії, що може сигналізувати про наявність самого доступу. Імовірно, “для маскування”, паралельно з підключенням можуть бути здійснені й навмисні ушкодження кабелю.

Пасивні способи мають високу скритність, тому що практично не міняють параметри поширення по ОВ випромінювання, але мають низьку чутливість. Тому для перехоплення інформації використовують ділянки, на яких рівень бічного випромінювання підвищений. Навіть після формування стаціонарного розподілу поля у волокні невелика частина випромінювання все-таки проникає за межі оболонки й може бути каналом витоку переданої інформації. Можливість існування побічних оптичних випромінювань із бічної поверхні ОВ обумовлена низкою фізичних, конструктивних і технологічних факторів (рис.2.4):

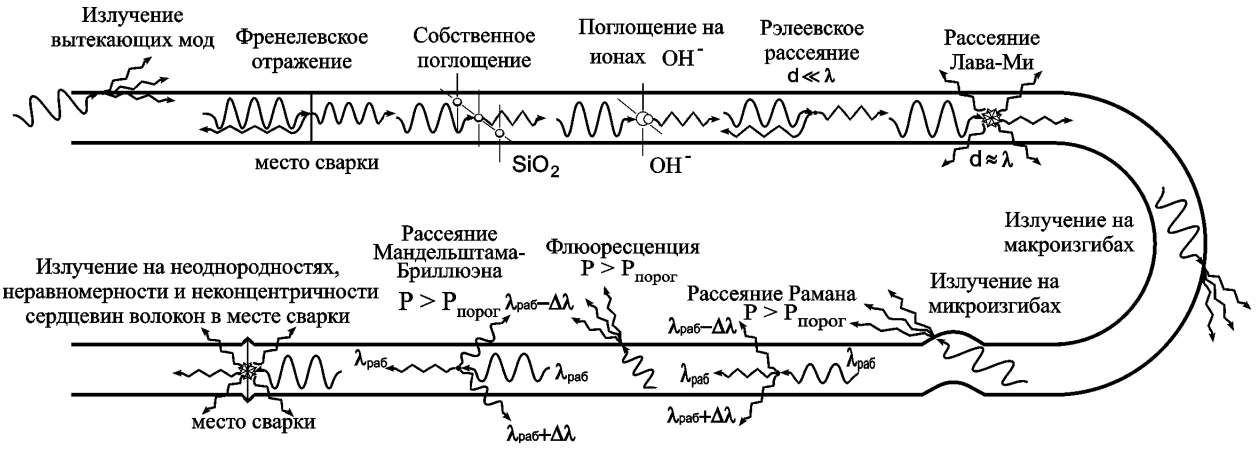


Рис. 2.4. Причини випромінювання й розсіювання в ОВ

– існування мод, що випливають, на початковій ділянці волокна, обумовлена порушенням його джерелом випромінювання із просторовим розподілом, що перевищує апертуру волокна;

– випромінювання що випливають і випромінювальних мод на всьому протязі ОВ за рахунок релеевского розсіювання на структурних неоднорідно-

стях матеріалу ОВ, характерні розміри яких істотно менше довжини хвилі випромінювання;

– перетворення мод, що направляють, в, що випливають за рахунок локальних змін хвилеподібного параметра на хвилеподібних нерегулярностях волокна: мікровигинах (радіус вигину зрівняємо з діаметром ОВ) і макровигинах (радіус вигину набагато більше діаметра ОВ);

– виникнення розподілених і локальних тисків на ОВ.

Волоконно-оптичні лінії зв'язку мають оптичні канали витоку інформації з акусто-оптичним ефектом, що також утворить канал витоку акустичної інформації.

Причинами виникнення випромінювання (витік світлової інформації) у рознімних з'єднаннях волоконних світловодів є:

– радіальна непогодженість волокон що стикуються;

– кутова непогодженість осей світловодів;

– наявність зазору між торцями світловоду;

– наявність взаємної непаралельності поверхонь торців волокон;

– різниця в діаметрах сердечників волокон що стикуються;

Всі ці причини приводять до випромінювання світлових сигналів у навколишній простір.

Використання мод, що випливають, у місцях стикування ОВ становить достатню небезпеку з погляду захисту інформації, тому що є можливість організувати режим «прозорості» НСИ, коли ВОЛЗ «не зауважує» відбір досить великого оптичного сигналу з ВОЛТ. У цьому випадку забезпечення захисту інформації відносно просто досягається організаційно-технічними заходами (охорона, спостереження таких ділянок).

Активні способи дозволяють вивести через бічну поверхню ОВ випромінювання значно більшої потужності. Однак при цьому відбувається зміна параметрів поширюється по ОВ випромінювання (рівень потужності в каналі, модова структура випромінювання), що може бути легко виявлено. До спо-

собів цієї групи ставляться: механічний вигин ОВ, вдавлення зондів в оболонку, безконтактне з'єднання ОВ, шліфування й розчинення оболонки, підключення до ОВ фотоприймача за допомогою спрямованого ответвителя, термічне деформування геометричних параметрів ОВ і формування неоднорідностей в ОВ.

Компенсаційні способи принципово сполучать у собі переваги перших двох груп - скритність і ефективність, але сполучені з технічними труднощами при їхній реалізації.

Практичні пристрої, що реалізують компенсаційні способи знімання інформації з бічної поверхні ОВ, у цей час невідомі.

Слід зазначити, що захисні оболонки й елементи конструкції кабелю істотно послабляють бічне випромінювання.

Можна значно зменшити чутливість волоконно -оптичного кабелю до дії акустичного поля, якщо волокно перед його закладенням у кабель покрити шаром речовини з високим значенням об'ємного модуля пружності. Це може бути досягнуто, наприклад, нанесенням безпосередньо на поверхню оптичного волокна шаруючи нікелю товщиною близько 13 мкм, алюмінію товщиною близько 95 мкм або скла, що містить алюмінат кальцію, товщиною близько 70 мкм.

Застосовуючи метод гальванічного покриття, можна одержувати на оптичному волокні відносно товсту й міцну плівку.

Тому перехоплення інформації кожним з перерахованих вище способів можливий тільки при порушенні цілісності зовнішньої захисної оболонки кабелю й безпосередньому доступі до оптичних волокон.

Протяжний без розривний знімання інформації, можна здійснити або на пологому вигині волокна або на прямому волокні під впливом низьких температур. Справа в тому, що при низьких температурах відбувається зміна ко-

ефіцієнтів переломлення скла, у результаті чого в серцевині може підвищитися рівень розсіювання.

2.5.3. Конфіденційність інформації

Конфіденційність переданої по ВОЛЗ інформації може бути забезпечена застосуванням спеціальних методів і засобів захисту лінійного тракту від НСД. До основних достоїнств застосування захищених ВОЛС ставляться:

- незалежність від структури переданих цифрових сигналів;
- незалежність від швидкості передачі цифрових сигналів;
- відносно низька вартість;
- універсальність застосування в локальних, абонентських або зонових мережах зв'язку.

В останні час проводяться інтенсивні роботи зі створення ВОЛС, що забезпечують захист переданої інформації від НСД Можна виділити три основних напрямки цих робіт:

- розробка технічних засобів захисту від НСД до інформаційних сигналів, переданим по ОВ;
- розробка технічних засобів контролю НСД до інформаційного сигналу, переданому по ОВ;
- розробка технічних засобів захисту інформації, переданої по ОВ, що реалізує принципи маскування , додавання перешкод, оптичної й квантової криптографії.

Системи захисту переданої інформації у ВОСП повинні затрудняти НСД, а також фіксувати знімання оптичного сигналу з ОТ.

Основою системи фіксації НСД є система діагностики стану (СДС) ВОЛТ. СДС можна побудувати з аналізом або минулого через ВОЛТ сигналу, або відбитого сигналу (рефлектометричні СДС).

СДС із аналізом минулого сигналу є найбільш простою діагностичною системою. На прийомної частини ВОЛС аналізується минулий сигнал. При НД відбувається зміна сигналу, ця зміна фіксується й передається в блок керування ВОЛЗ.

При використанні аналізатора коефіцієнта помилок на прийомному модулі ВОЛЗ (рис. 2.5). СДС реалізується при мінімальних змінах апаратур ВОЛЗ, тому що практично всі необхідні модулі є в складі апаратур ВОЛЗ. Недоліком є відносно низька чутливість до змін сигналу.

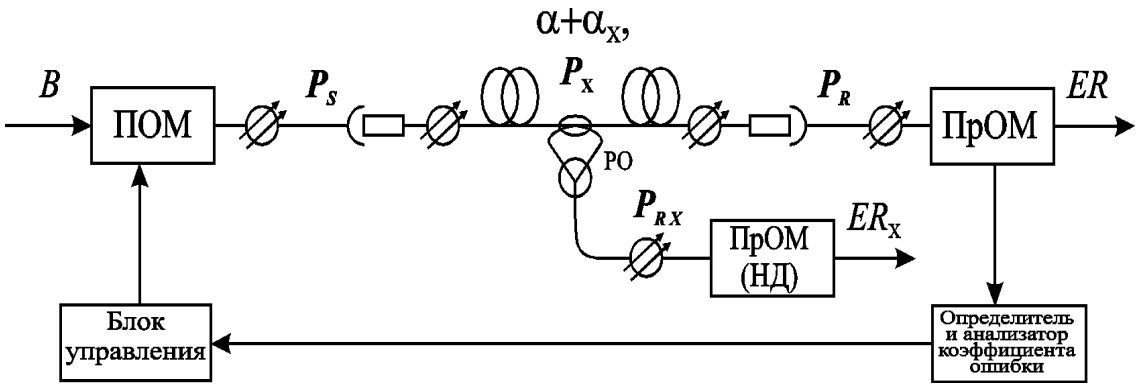


Рис. 2.5. ВОЛЗ із системою діагностики по аналізі коефіцієнта помилок

Основним недоліком СДС із аналізом минулого сигналу є відсутність інформації про координату неоднорідності, що з'явилася, що не дозволяє проводити більше тонкий аналіз змін режимів роботи ВОЛЗ (для зняття помилкових спрацьовувань системи фіксації НСД).

СДС із аналізом відбитого сигналу (рефлектометричні СДС) дозволяють найбільшою мірою підвищити надійність ВОЛЗ.

Для контролю величини потужності сигналу зворотного розсіювання в ОВ у цей час використається метод імпульсного зондування (рис.2.6).

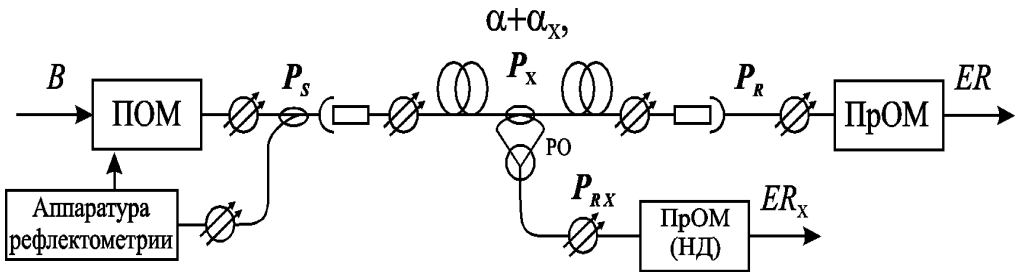


Рис. 2.6. ВОЛЗ із рефлектометричними системами діагностики стану ВОЛТ

Суть його полягає в тому, що в досліджуване ОВ уводиться потужний короткий імпульс, і потім на цьому ж кінці реєструється випромінювання, неуважне у зворотному напрямку на різних неоднорідностях, по інтенсивності якого можна судити про втрати в ОВ, розподілених по його довжині на відстані до 100 - 120 км. Початкові рефлектограми лінії фіксуються при різних динамічних параметрах зондувального сигналу в пам'яті комп'ютера й рівняються з відповідними поточними рефлектограми. Локальне відхилення рефлектограми більш ніж на 0,1 дб свідчить про ймовірності спроби несанкціонованого доступу до ОВ.

Основними недоліками СДС із аналізом відбитого сигналу на основі методу імпульсної рефлектометрії є наступні:

– при високому дозволі по довжині ВОЛТ (що має важливе значення для виявлення локальних неоднорідностей при фіксації НСД) значно знижується динамічний діапазон рефлектометрів і зменшується контрольована ділянка ВОЛТ;

– потужні зондувальні імпульси утрудняють проведення контролю ВОЛТ під час передачі інформації, що знижує можливості СДС, або ускладнює й здорожує систему діагностики;

– джерела потужних зондувальних імпульсів мають ресурс, недостат-

ній для тривалого безперервного контролю ВОЛЗ;

– спеціалізовані джерела зондувального оптичного випромінювання, широкосмугова й швидкодіюча апаратури прийомного блоку рефлектометрів значно здорожує СДС.

СДС із аналізом відбитого сигналу на основі методу частотно-модульованого зондування (ЧМЗ) є найбільш перспективною. Це, в основному, обумовлено наступними особливостями подібних систем:

– забезпечується найбільша чутливість прийомного блоку ЧМЗ рефлектометра; виграш у чутливості тим більше, чим краще просторовий дозвіл рефлектометра;

– є можливість використати для зондувального випромінювання СДС серійний, зв'язковий джерело випромінювання;

– є можливість проводити діагностику ОТ під час передачі інформації;

– використання щодо дешевих компонентів у СДС дозволяє реалізувати системи значно більше дешеві, чим на основі імпульсних рефлектометрів.

Методи цієї групи добре сполучаються з багатьма іншими методами захисту.

Становить інтерес метод, заснований на використанні кодового зашумлення переданих сигналів. При реалізації цього методу застосовуються спеціально підібрані відповідно до необхідної швидкості передачі коди, що розмножують помилки. Навіть при невеликому зниженні оптичної потужності, викликаному підключенням пристрою знімання інформації до ОВ, у цифровому сигналі на виході ВОЛЗ різко зростає коефіцієнт помилок, що досить просто зареєструвати засобами контролю ВОЛЗ. Цікавим також є метод, заснований на використанні пари різно знакових компенсаторів дисперсії на ВОЛЗ.

При використанні маскування інформаційного сигналу може застосо-

вуватися система, що використає спектральний поділ каналів.

З розвитком науки й техніки назріла необхідність і з'явилася можливість з'єднати досягнення криптографічної науки із квантовою механікою й квантовою статистикою. На цьому стику виникло й інтенсивно розвивається новий перспективний напрямок - квантова криптографія.

Методи квантової криптографії потенційно забезпечують високий ступінь захисту від перехоплення інформації на лінії зв'язку за рахунок передачі даних у вигляді окремих фотонів, оскільки не руйнуючий вимір їхніх квантових станів у каналі зв'язку перехоплювачем неможливо, а факт перехоплення фотонів з каналу може бути виявлений по зміні імовірнісних характеристик послідовності фотонів.

Основним недоліком СДС із аналізом минулого сигналу є відсутність інформації про координату неоднорідності, що з'явилася, що не дозволяє проводити більше тонкий аналіз змін режимів роботи ВОЛЗ (для зняття помилкових спрацьовувань системи фіксації НСД).

СДС із аналізом відбитого сигналу (рефлектометричні СДС) дозволяють найбільшою мірою підвищити надійність ВОЛЗ.

З розвитком науки й техніки назріла необхідність і з'явилася можливість з'єднати досягнення криптографічної науки із квантовою механікою й квантовою статистикою. На цьому стику виникло й інтенсивно розвивається новий перспективний напрямок - квантова криптографія.

Методи квантової криптографії потенційно забезпечують високий ступінь захисту від перехоплення інформації на лінії зв'язку за рахунок передачі даних у вигляді окремих фотонів, оскільки не руйнуючий вимір їхніх квантових станів у каналі зв'язку перехоплювачем неможливо, а факт перехоплення фотонів з каналу може бути виявлений по зміні імовірнісних характеристик послідовності фотонів.

– безпекою;
– використання надійних і доступних засобів аудиту для полегшення

виявлення порушень безпеки;

– надання допомоги при визначенні джерела зловмисного програмного забезпечення і зони його поширення.

3 СИСТЕМА УПРАВЛІННЯ ЦИФРОВОЮ ПЕРВИННОЮ МЕРЕЖЕЮ ЗВ'ЯЗКУ УКРАЇНИ

3.1. Аспекти політики безпеки інформації в системі управління мережами

Політика безпеки СУТ є частиною загальної політики безпеки галузі і успадковує її принципи.

Політика визначає важливість (цінність) інформації, встановлює для усіх працівників важливість безпеки в середовищі СУТ, розподіляє їх ролі, встановлює обов'язки та відповідальність щодо забезпечення безпеки як даних і інформації, так і самої СУТ. Політика повинна встановлювати: відповідальність за захист інформації в СУТ та обов'язки підрозділів.

План захисту інформації СУТ полягає в тому, щоб гарантувати цілісність, доступність та конфіденційність даних, що мають бути достатньо повними, точними, і своєчасними, щоб задовольняти потреби СУТ. Необхідно гарантувати:

– забезпечення відповідного рівня безпеки;

– забезпечення відповідної підтримки захисту даних

– індивідуальну підзвітність щодо даних, інформації та інших комп'ютерних ресурсів, до яких є доступ;

– можливість перевірки середовища функціонування СУТ;

– забезпечення користувачів достатньо повними інструкціями;

– відповідність планів забезпечення безупинної роботи критично важливих функцій СУТ, планів відновлення роботи при стихійних лихах;

– виконання усіх відповідних законів, указів тощо.

За впровадження і досягнення цілей політики безпеки відповідають

такі групи співробітників:

– функціональне керівництво відповідає за інформування співробітників щодо політики, взаємодіє з усіма службовцями в питаннях з проблем безпеки;

– адміністратори СУТ здійснюють щоденне керування і підтримку працездатності СУТ, відповідають за забезпечення безупинного функціонування СУТ та за здійсненням заходів захисту в СУТ відповідно до варіантів політики безпеки СУТ;

– місцеві адміністратори відповідають за надання кінцевим користувачам доступу до необхідних ресурсів СУТ, що розміщені на серверах, і відповідають за забезпечення захисту своїх серверів;

– користувачі-оператори – це працівники, що мають доступ до СУТ.

Порушення політики може піддати інформацію неприпустимому ризику втрати конфіденційності, цілісності або доступності при її зберіганні, обробці або передачі в межах СУТ.

Передбачається система правил розмежування доступу

– кожний ПК (автоматизоване робоче місце – АРМ) повинен мати свого відповідального за працездатність, безпеку комп'ютера та за дотриманням політик і процедур при використанні АРМ. усі механізми захисту серверів СУТ повинні знаходитися під монопольним керуванням місцевого адміністратора і місцевого персоналу адміністраторів СУТ;

– користувачі повинні гарантувати, що їхнє програмне забезпечення має належні ліцензії і є безпечним.

– за всі зміни на серверах відповідають адміністратори СУТ;

– користувачу призначається унікальний ідентифікатор користувача і початковий пароль;

– користувачі проходять процедуру автентифікації в СУТ перед зверненням до ресурсів СУТ;

– ідентифікатор користувача має періодично змінюватись;

– використання апаратних засобів СУТ типу моніторів чи реєстраторів (аналізаторів) трафіку і маршрутизаторів має бути авторизованим і проводитись під контролем адміністраторів СУТ;

Користувачі цілком відповідають за власну поведінку. Зокрема, користувачі відповідають за:

– дотримання відповідних законів, політики безпеки, процедур і пов’язаних з ними наслідків для СУТ;

– використання доступних механізмів безпеки для захисту конфіденційності і цілісності власної інформації;

– вибір і використання відповідних паролів;

– допомогу іншим користувачам;

– сповіщення місцевого адміністратора або керівника щодо порушень захисту або виявлених відмов;

– невикористання слабких місць СУТ;

– надання правильної інформації для ідентифікації й автентифікації, недопущення спроб вгадування подібної інформації для потреб інших користувачів;

– гарантування виконання резервного копіювання даних і програмного забезпечення;

– знання і використання відповідних політик і процедур для запобігання, виявлення і видалення зловмисного програмного забезпечення.

Функціональні керівники відповідають за розробку і виконання ефективних варіантів політики безпеки, що відображають специфічні цілі СУТ. Задача захисту інформації і ліній зв'язку є важливою і критичною метою у повсякденній діяльності. Зокрема функціональні керівники відповідають за:

– проведення ефективного керування;

– реалізацію програми навчання користувачів основам безпеки;

– гарантування того, що весь персонал у межах операційної одиниці організації знає політику безпеки і програми навчання;

– інформування місцевого адміністратора й адміністраторів СУТ про зміни.

Передбачається, що адміністратори СУТ (або підготований для цього персонал) реалізують місцеві варіанти політики безпеки. Цей процес пов'язаний із застосуванням програмно-апаратних засобів захисту, архівацією кри-

тичних програм і даних, керуванням доступом і захистом устаткування СУТ. Зокрема, адміністратори СУТ несуть відповідальність за:

– коректне застосування доступних механізмів захисту;

– захищеність середовища СУТ та інтерфейсів із глобальними мережами;

– оперативне й ефективне улагоджування подій із комп'ютерною безпекою;

– використання надійних і доступних засобів аудиту для полегшення виявлення порушень безпеки;

надання допомоги при визначенні джерела зловмисного програмного забезпечення і зони його поширення.

Місцеві адміністратори використовують доступні служби і механізми захисту СУТ на сервері, що знаходиться в їхній зоні відповідальності, щоб підтримувати і впроваджувати варіанти і процедури політики безпеки. Зокрема, місцеві адміністратори відповідають за:

– керування доступу всіх користувачів

– контроль всіх пов'язаних з захистом подій і за розслідуванням будь-яких реальних або підозрюваних порушень

– підтримку і захист програмного забезпечення.

– сканування серверу СУТ антивірусним програмним забезпеченням

– призначення унікального ідентифікатора користувача і початкового паролю.

– забезпечення допомоги при виявленні джерела зловмисного програмного забезпечення і зони його поширення.

Інцидент із комп'ютерною безпекою – це будь-який несприятливий випадок, у ході якого може опинитися під загрозою деякий аспект безпеки: втрата конфіденційності даних, цілісності даних або цілісності системи, руйнація або відмова в обслуговуванні. В середовищі СУТ поняття інциденту з безпеки може бути поширене на усю область СУТ. Плани відновлення в се-

редовищі СУТ мають бути розроблені із найменшим впливом на функціональні можливості управління телекомунікаційними мережами і дії з відновлення.

Мета дій полягає в тому, щоб зменшити потенційно небезпечні наслідки проблеми, пов’язаної з безпекою СУТ.

Плани відновлення створюються, щоб забезпечити плавне, швидке відновлення середовища СУТ після перерви в її роботі.

3.2. Захист інформації в системі керування

Система управління цифровою первинною мережею зв'язку України (СУ ЦПМЗ) служить для автоматизації цифрової магістральної первинної мережі зв'язку. Національне значення цієї мережі зв'язку вимагає особливої уваги до забезпечення захисту інформації, тому що порушення її роботи або витік конфіденційної інформації спричинили б величезний збиток як для окремих користувачів мережі, так і для держави.

Функціонально СУ складається із трьох рівнів, взаємодія між якими здійснюється через мережу передачі даних (СПД). На нижньому рівні системи (SMS) здійснюється керування елементами мережі. Цей рівень є вже сформованим і істотним змінам піддатися не може. Верхній рівень являє собою операційну систему національного центра керування (ОС НЦУ), головною метою якої служить координація дій всієї системи в цілому й керування її конфігурацією. Для організації взаємодії між верхнім і нижнім рівнем використається середній рівень - пункт контролю й керування (ПКУ), у завдання якого входить фільтрація, обробка й передача інформації про стан цифрових трактів по інтерфейсі Q3, а також прийом команд керування від рівня керування мережею. На першому етапі створення системи функціональність рівня

ПКУ буде забезпечувати оператор робочої станції SMS, що переносить інформацію зі свого термінала на монітор взаємодії з ОС НЦУ.

Таким чином, СУ являє собою складну розподілену обчислювальну систему, що включає в себе різнорідні технічні засоби. Для рішення завдання захисту інформації в такій системі виберемо модель, що з однієї сторони адекватно відображала б погрози на різних рівнях системи, а з іншого боку - не була б перевантажена зайвими деталями. Візьмемо за основу модель, у якій інформація буде ставитися до однієї із трьох категорій (табл.5.2.1):

– дані, що зберігаються на сервері або робочій станції (бази даних, текстові документи, графічні файли й т.д.);

– дані, переміщувані між серверами й робочими станціями за допомогою середовища передачі;

– програмне забезпечення (ПО).

Розглянемо ситуації, що приводять до виконання наведених погроз і надають пропозиції що до захисту.

Доступ сторонніх осіб до даних робочої станції

СУ проектується таким чином, щоб у нормальному режимі роботи сервери не мали власних терміналів, а керування здійснювалося винятково віддалено. Для того, щоб робоча станція могла користуватися системою, вона (у фазі підключення) посилає на сервер своя адреса. Система з'ясовує у своїй базі даних, чи має дана станція на цей дозвіл. Якщо це так, то процес установлення з'єднання триває. Користувач уводить свій пароль, що посилає на сервер. Якщо пароль дійсний, система порівнює дані користувача з даними користувачів, що мають дозвіл працювати на даній робочій станції. Якщо перевірка закінчується позитивно, починається нормальна робота із системою з вилученого термінала.

Таблиця 3.1

Втручання сторонніх осіб через вилучений доступ

Категорії інформації	Погрози
Дані на робочій станції	знищення - навмисна або випадкова втрата даних; перекручування - несанкціонована зміна даних, викликана дією випадкових причин; фальсифікація - навмисна зміна даних з метою ввести в оману власника інформації; витік - поширення конфіденційної інформації внаслідок несанкціонованого доступу до системи;
Дані в СПД	несанкціонований доступ на незахищеній ділянці мережі; перекручування й втрати, викликані природними перешкодами в СПД; погрози, пов'язані з нечесністю відправника або одержувача інформації (наприклад, відправник відправив одне повідомлення, а затверджує, що послав інше);
Програмне забезпечення	наслідки несанкціонованого доступу; дії вірусів;

У якості СПД у системі використаються лінії передач мереж електрозв'язку, тобто телефонні лінії. Тому що ці лінії є дуже протяжними, то здійснення повного контролю над доступом до них неможливо. Отже, у зловмисника завжди є можливість незаконного підключення до СПД, що він може використати для проникнення в систему. У загальному випадку найбільш складним є подолання первинної ідентифікації користувача, без успішного проведення якої неможливий доступ до ресурсів системи. Із цією метою застосовується прослуховування каналів зв'язку для визначення паролів, обсягу трафіку й адрес відправників і одержувачів. На базі цієї інформації фахівець може розробити програму, що перехоплює запити легальних користувачів на

входження в систему й процедуру, що імітує, упізнавання. Укравши секретний пароль, програма імітує відмову в доступі. При цьому користувач не підозрює, що його пароль розкритий.

Як показала практика, єдиним надійним методом захисту в цій ситуації є криптографічний захист. Щоб запобігти можливості “підбудуватися” під робочу станцію всі дані, що пересилають по мережі, шифруються.

Рекомендується передбачити адміністративні міри, що обмежують доступ у приміщення, де перебувають сервери системи. У цьому випадку особа, що не має повноважень, не зможе підключитися до системи через мережу.

Таким чином, надійність системи захисту від несанкціонованого доступу багато в чому визначається якістю використовуваних криптографічних алгоритмів.

Дії персоналу.

Користувач системи може повідомити свій пароль сторонній особі. Для захисту від подібних випадків кожному користувачеві призначений список робочих станцій, на яких він може працювати. Спроби доступу із чужої робочої станції системою припиняються й доводять до відомості адміністратора.

У випадку спроби користувача перевищити свої повноваження, автоматично повинен запускатися алгоритм обслуговування виниклої ситуації (наприклад, запис рапорту, що інформує адміністратора про спробу несанкціонованого доступу). Зміст такого способу захисту полягає в тім, що кожній удалій спробі несанкціонованого доступу часто передує якась серія невдалих спроб, і інформація про це може сприяти своєчасному виявленню порушника.

Система автоматичного спостереження повинна дозволяти вести записи про всі дії користувачів. У випадку помилкових дій при роботі, наприклад, з базами даних ця система дозволить довідатися, які саме зміни були внесені в

систему і як дані були змінені. Якщо велося резервне копіювання даних, то можливо відновити змінені дані в досить великому обсязі.

Високий відсоток помилок можна чекати серед операторів ПКУ, що займаються переносом інформації з одного термінала на інший. У зв'язку із цим необхідно розробити ПО, що виконує перевірку переданої інформації за допомогою контрольних сум.

Несанкціонований доступ, заснований на дослідженні електромагнітних випромінювань

Останнім часом широко поширилися технічні засоби, що дозволяють зчитати інформацію із працюючого комп'ютера, перебуваючи на значній відстані від нього. Ця можливість пов'язана з тим, що всякий електронний прилад є джерелом електромагнітного випромінювання. У комп'ютерах характер випромінювання залежить від оброблюваних даних, а отже може служити джерелом інформації.

Захист інформації від витоку по каналах побічних електромагнітних випромінювань і наведень (ПЭМіН) є важливим аспектом захисту конфіденційної й секретної інформації в ЕОМ від несанкціонованого доступу з боку сторонніх осіб. Даний вид захисту спрямований на запобігання можливості витоку інформативних електромагнітних сигналів за межі охоронюваної території. При цьому передбачається, що усередині охоронюваної території застосовуються ефективні режимні міри, що виключають можливість безконтрольного використання спеціальних апаратур перехоплення, реєстрації й відображення електромагнітних сигналів. Для захисту від ПЭМіН широко застосовується екранування приміщень, призначених для розміщення засобів обчислювальної техніки, а також технічні міри, що дозволяють знизити інтенсивність інформативних випромінювань самого встаткування ЕОМ і зв'язку.

Іншим видом інформаційного випромінювання є акустичне випромінювання (наприклад, від працюючого принтера). Не рекомендується використа-

ти техніку, зібрану в країнах третього миру, тому що вона є особливо сильним джерелом випромінювань.

Збої й помилки в роботі апаратного й програмного забезпечення.

Збої в роботі апаратур можуть бути викликані стрибками напруги в мережі харчування, несправностями енергопостачання, тимчасовими або постійними помилками в її схемах. Помилки в роботі апаратур досить рідкі, тому що в ЕОМ є достатня кількість схем, що забезпечують виявлення й локалізацію помилок.

Операційна система як у перших, так і у своїх наступних версіях містить, як правило, не виявлені помилки. Момент їхнього прояву визначається набором факторів, і у звичайних умовах ці помилки не приводять до відмов у роботі ЕОМ.

Помилки в програмах користувачів уважаються особливо небезпечними, здатними привести до самих серйозних наслідків. Наприклад, неправильне керування уведенням даних приведе до запису в масив даних перекрученої інформації, а неправильне керування висновком даних - до печатки документів з помилками. Програми користувачів, що працюють у мультипрограмному режимі й містять не виявлені помилки, являють загрозу для правильно працюючих програм, тому що в певних умовах вони можуть уважати або записати інформацію в не приналежні їм області пам'яті.

Вплив вірусів.

Вірус - це програма, здатна мимовільно створювати свої копії й модифікуватися в інші програми, записані у файлах або системних областях, для наступного одержання керування й відтворення нової копії. Необхідне застосування спеціальних програм-аналізаторів, що здійснюють постійний контроль виникнення "аномалій" у діяльності прикладних програм, періодичну перевірку наявності інших можливих слідів вірусної активності (наприклад, виявлення порушень цілісності програмного забезпечення), а також "вхід-

ний" контроль нових програм перед їхнім використанням (по характерних ознаках наявності в їхньому тілі вірусних утворень).

3.3. Система захисту інформації в автоматизованих системах

3.3.1. Принципи побудови системи захисту

Сучасний етап розвитку інформатизації характеризується необхідністю переходу до створення глобальних територіально розподілених автоматизованих інформаційно-аналітичних систем.

Одним із найважливіших показників надійності автоматизованої системи є забезпечення цілісності та конфіденційності інформації. Основні вимоги до інформаційної безпеки автоматизованої системи визначені Законом України “Про захист інформації в автоматизованих системах”. Комплексне вирішення проблеми технічного захисту інформації в автоматизованій системі потребує глибокого аналізу архітектури системи, методів і технологій обробки інформації з метою визначення максимально повного складу потенційних загроз інформаційної безпеки, побудови ефективної моделі стратегії захисту інформації і способів її реалізації.

Серед проблем забезпечення захисту інформації можна виділити питання організації та інженерних рішень, які потребують специфічного підходу вже на стадії попереднього проектування автоматизованої системи.

З метою забезпечення принципів відкритої архітектури система захисту інформації має:

– будуватися на основі штатних вмонтованих механізмів захисту інформації базового програмного забезпечення;

– мати модульну структуру;

– підтримувати централізоване адміністрування в неоднорідному середовищі робочих станцій та серверів.

Для здійснення управління доступом і захистом інформації в різнорідних автоматичних системах обрана доменна організація системи захисту інформації. Домен системи захисту інформації від несанкціонованого доступу – це програмно-апаратний комплекс, що здійснює захист територіально відокремленої частини автоматизованої системи. Взаємодія між доменами системи захисту полягає в передачі команд віддаленого управління від одних доменів до інших і поверненні інформації про результати виконання цих команд. Обмін інформацією між доменами здійснюється через обчислювальну мережу.

Для забезпечення централізованого управління системою захисту інформації використовується ієрархічна організація доменів. Між доменами існує відношення підпорядкування, тобто можливості віддаленого управління одних доменів іншими. Причому, ці домени мають бути пов’язані обчислювальною мережею чи безпосередньо, чи через домени проміжних рівнів ієрархії.

Процес інформаційного обміну системи захисту інформації задовольняє наступним вимогам:

– взаємна автентифікація компонент, що приймають участь у процесі;

– розпізнається коректне та некоректне (внаслідок розриву зв’язку) припинення процесу інформаційного обміну;

– захист інформації, інформація передається по каналах зв’язку в криптографічною захищеному вигляді;

– контроль цілісності інформації;

– забезпечує гарантовану доставку інформації;

Основною програмно-апаратною компонентою домену є монітор безпеки.

Монітор безпеки складається з наступних основних функціональних компонент:

–засоби опису моделі об’єкта управління;

–засоби опису параметрів функціонування монітора безпеки. Забезпечують вказування загальних параметрів функціонування монітора; параметрів зв’язку з суміжними доменами та АРМами адміністратора системи захисту;

–засоби аудита. Забезпечують вибірку інформації про події, що були зареєстровані в процесі роботи монітора безпеки, та генерацію звітів про ці події. Наявність механізму селекції подій дозволяє вибирати тільки ті події, що задовольняють заданим критеріям.

–засоби інтерфейсу з суміжними доменами. Забезпечують можливість віддаленого управління доменами нижчих рівнів ієрархії та прийняття команд віддаленого управління від доменів вищих рівнів ієрархії.

–засоби інтерфейсу з АРМами адміністратора безпеки. Забезпечують з’єднання з монітором безпеки довільної кількості АРМів адміністратора безпеки, з яких здійснюється управління засобами безпеки.

–засоби забезпечення процесів захисту. Здійснюють загальне управління функціонуванням системи захисту інформації, забезпечують процеси автентифікації користувачів, санкціонування та блокування доступу користувачів до ресурсів, реєстрації подій, які впливають на безпеку об’єкта управління, управління засобами оперативного реагування. До функцій засобів забезпечення процесів захисту також належить контроль цілісності ресурсів системи захисту інформації, її тестування та діагностика.

–база даних системи захисту. Виконує функції зберігання моделі автоматизованої системи, правил розмежування доступу, параметрів функціонування монітора безпеки та журналу реєстрації подій. Також являє собою буфер передачі інформації між доменами, між монітором безпеки та проблемно-орієнтованими засобами захисту в разі, коли зв'язок встановлюється у певні моменти часу чи за запитами адміністратора безпеки.

Монітор підсистеми безпеки, як основна програмно-апаратна компонента системи захисту інформації, може функціонувати в трьох режимах.

–мережевий режим. Забезпечує функціонування монітора безпеки на центральному, регіональному, та місцевому рівнях ієрархії, пов'язаних обчислювальною мережею.

–автономний режим. За умови відсутності зв'язку з іншими рівнями ієрархії монітор безпеки здатний функціонувати в автономному режимі. Автономний режим роботи також використовується при немережевому варіанті функціонування монітора безпеки.

–режим гарячого резерву. З метою підвищення надійності системи захисту інформації передбачається режим дублювання функцій її основних компонент. У цьому випадку до підсистеми безпеки включається резервний монітор, до функцій якого входить підтримка бази даних гарячого резерву. У випадку відмови основного монітора безпеки, його функції бере на себе резервний монітор, забезпечуючи таким чином неперервність роботи системи захисту інформації в цілому.

Наведені принципи не можуть відображати всієї повноти проблем, що виникають при побудові системи захисту інформації в різнорідних автоматизованих системах.

3.3.2. Деякі проблеми захисту інформації в автоматизованих системах

Для вирішення окремих питань управління АС прикладного рівня об'єднуються в автоматизовані функціонально спрямовані комплекси, які можуть з'єднуватись з використанням будь-якої системи зв'язку. Доцільно вважати системи зв'язку зовнішніми елементами АС , які не можуть контролюватись і нести відповідальність за пошкодження або зникнення інформації.

З цієї позиції проблеми захисту інформації, можна поділити на дві частини: внутрішню і зовнішню. У внутрішній частині системи захисту здійснюється, в повному обсязі, контроль за несанкціонованим доступом (НСД) шляхом складної ієрархічної організації ідентифікації та автентифікації користувача окремо при доступі до інформаційної системи – локальної обчислювальної мережі (ЛОМ), та при використанні внутрішніх процесів на робочих станціях.

Безпека інформації в зовнішній частині АС, забезпечується посиленою схемою автентифікації з використанням криптографічних методів.

Часто відсутність єдиного концептуального погляду на проблеми забезпечення безпеки інформації, як об'єднаному комплексі різних за призначенням АС обробки зв'язку накладає свій відбиток на питання комплексної безпеки. Серцевинним питанням при створенні системи є забезпечення безпеки інформації від НСД. Головною проблемою системи захисту є перекриття можливих напрямків НСД до захищених даних. При цьому, головна увага повинна бути звернута на дотриманні таких положень:

–комплексність системи захисту;

–сувора регламентація прав користувачів до доступу до інформації;

–контроль та реєстрація інформації;

–контроль за функціонуванням системи захисту;

–відкритість проектування, тобто забезпечення ефективного захисту при відомій структурі та принципах функціонування системи захисту.

Механізм реалізації визначених положень об’єднує комплекс організаційних, нормативно-правових та програмно-технічних заходів (не відокремлюючи криптографічні), які встановлюють передбачений надійний кордон каналам НСД.

Треба звернути увагу ще на одну недостатньо вирішену загальну проблему для усіх систем захисту інформації в АС різного призначення. Йдеться про об’єктивну комплексну оцінку ефективності систем забезпечення безпеки інформації в цілому АС обробки зв’язку. На цей час така оцінка отримується здебільшого експортним шляхом, за відсутності строгого обґрунтування критеріїв та показників.

Під захистом інформації розуміється використання в ній засобів та методів, прийняття мір та здійснення заходів з метою забезпечення передбаченої захищеності інформації. Під захищеністю інформації розуміється підтримка на належному рівні тих параметрів інформації, які характеризують встановлений статут її зберігання, обробки та використання в АС. Поняття "захист інформації" передбачає використання заходів у двох сполучених напрямках: безпека інформації та цілісність даних. Зауважимо, що під словом "інформація" тут і далі вважається власна інформація користувачів (власників) та інформація про використовувані інформаційні технології, тобто захисту підлягає:

–загальна інформація, яка призначена для використання кінцевим користувачам АС;

–інформаційно-програмне забезпечення АС;

–службова інформація з адміністративного управління АС;

–інформаційно-програмне забезпечення адміністративного управління;

–власну інформацію про АС (склад, архітектура, технічне забезпечення тощо).

Крім того, захисту підлягають технічні засоби АС:

Системна класифікація погроз безпеки інформації в АС може бути здійснена на підставі таких критеріїв:

а) розташування захищеної інформації відносно процесів автоматизованої обробки:

- погрози, що не пов’язані з обробкою;
- погрози, що з’являються тільки при обробці;

б) розташування джерела дестабілізуючого впливу відносно компонентів АС:

- за кордонами АС та її елементів;
- в межах АС та її елементів.

В останньому випадку джерело дестабілізуючого впливу може нічого не змінювати в АС та її елементах або навпаки, випадково або зосереджено вносити зміни в технічні засоби, програми, масиви та таке інше.

Так, в умовах інтегрованої інформаційної системи, цілком ймовірно виникає поява погроз:

– непередбаченого і небажаного впливу різних функціональних процесів один на одного;

– несанкціонованого доступу авторизованих або неавторизованих користувачів до локальних чи віддалених БД та функціонального програмного забезпечення;

– зміна маршруту передачі інформації;

– несанкціоноване використання локальних та мережних інформаційно-програмних ресурсів;

– несанкціонована зміна елементів ЛОМ або режимів їх роботи;

– можливість широкого розповсюдження комп’ютерних вірусів;

– помилки та неузгодженість дій відповідальних осіб АС;

– підвищення загрози порушення цілісності інформації тощо.

Щоб запобігти цим загрозам та порушенням, необхідно реалізувати систематизований захист інформації на рівні:

- локальних ресурсів робочих станцій;
- ресурсів мережі кожної ЛОМ;
- ресурсів мережі зв'язку між складовими частинами АС.

На рис. 3.1 приведено наближений склад функціональних підсистем системи забезпечення безпеки інформації.

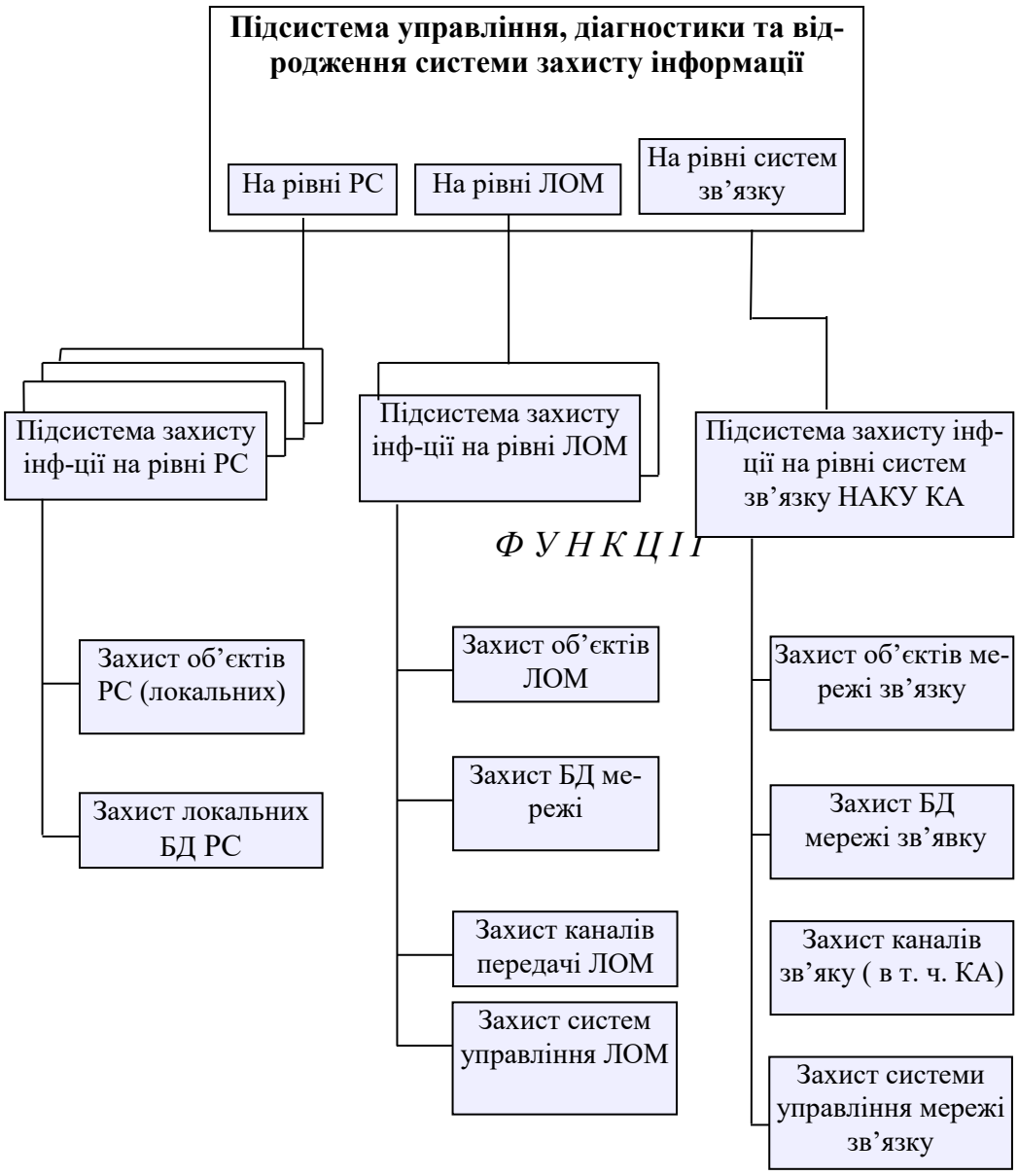


Рис.3.1. Склад функціональних підсистем системи забезпечення безпеки інформації

3.4. Захист інформації в мережах з технологією АТМ

3.4.1. Класифікація порушень передачі інформації

Нормальна передача інформації (рис. 3.2а) у мережах з гарантованою якістю обслуговування користувачів має на увазі виконання трьох етапів (рис. 3.2б).

– у площині менеджменту - формування й коректування баз даних (БД) про стан елементів мережі. Кінцевим результатом функціонування даного етапу є формування плану розподілу інформації на мережі - розрахунок таблиць маршрутизації (ТМ) у всіх вузлах для кожної служби електрозв'язку.

– у площині керування (стек протоколів сигналізації) - організацію маршруту між вузлом - джерелом (ВД) і вузлом - одержувачем (ВО) у вигляді віртуального що комутирує або постійного з'єднання (каналу або тракту). Кінцевим результатом функціонування даного етапу є заповнення й обнуління таблиць комутації (ТК).

– у площині користувача - безпосередня передача користувальницької інформації.

При цьому передача всіх видів інформації в мережі (службової - для формування БД і ТК; користувальницької) здійснюється по своїм окремо виділених віртуальних з'єднаннях (каналам і трактам).

Під порушенням передачі інформації будемо розуміти одну із ситуацій, які можуть бути організовані порушником (рис. 3.3).

– переривання або роз'єднання (рис.3.3.а). Інформація знищується або стає недоступної або непридатної для використання. У цьому випадку порушується доступність інформації. Прикладом таких порушень може бути вплив порушника на елементи мережі (лінії зв'язку (ЛС), вузли комутації

(КК), пристрою керування, БД і так далі) з метою їхнього знищення або приведення в неробочий стан.

– перехват (рис. 3.3 б). До інформації відкривається несанкціонований доступ. Порушується конфіденційність переданої інформації. Прикладом такого типу порушень є несанкціоноване підключення до каналу зв'язку.

– модифікація (рис. 3.3 в). До інформації відкривається несанкціонований доступ з метою зміни інформації. При цьому порушується конфіденційність переданої інформації і її цілісність. Метою такого типу порушень є зміна інформації, переданої по мережі.

– фальсифікація (рис. 3.3 г). Порушник видає себе за джерело інформації. При цьому порушується автентичність інформації. Прикладом такого типу порушень є відправлення підроблених повідомлень по мережі.

–

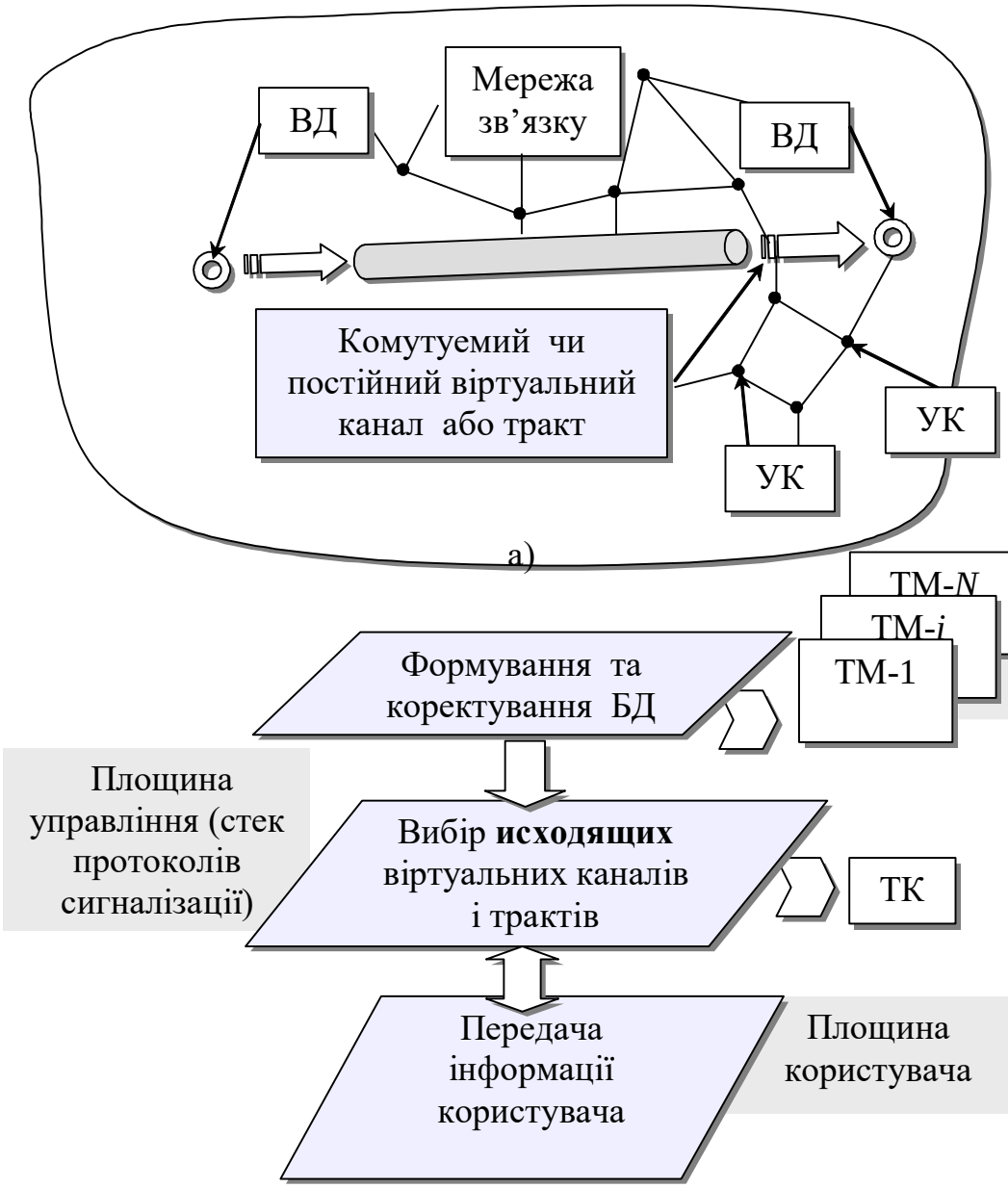
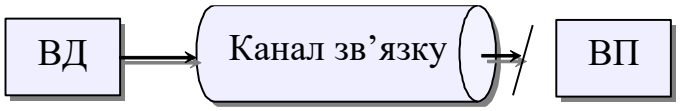
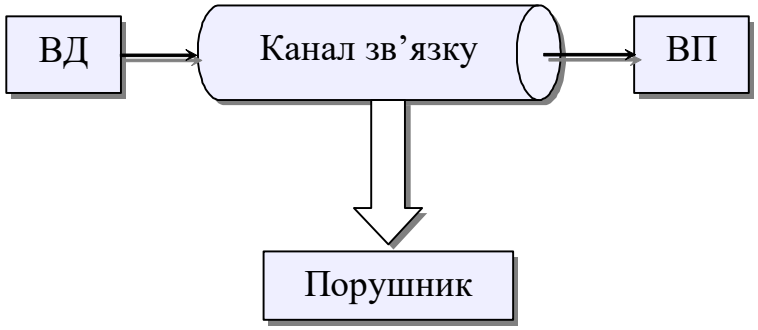


Рис. 3.2. Нормальна передача інформації в мережі з гарантованою якістю обслуговування користувачів

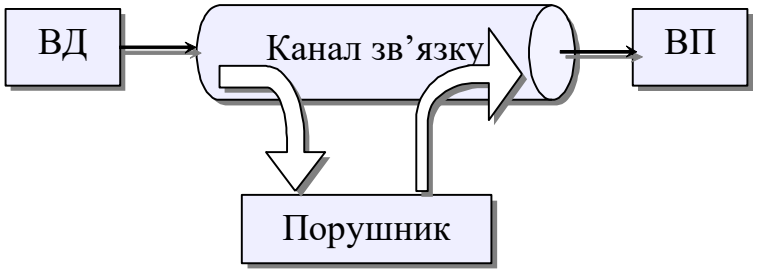
–



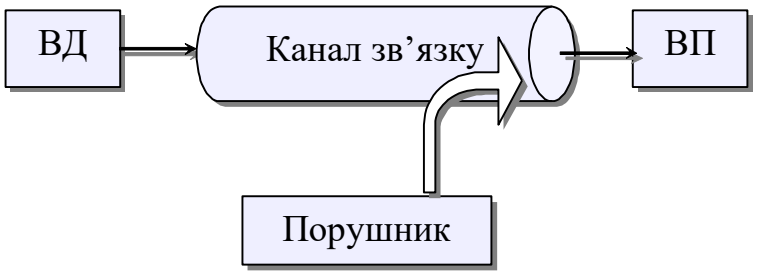
а) Переривання передачі інформації



б) Перехват інформації, що передається



в) Модифікація інформації, що передається



г) Фальсифікація інформації, що передається

Рис. 3.3. Види порушення інформації, що передається

Наведені вище типи порушень можна розділити на дві групи:

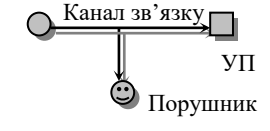
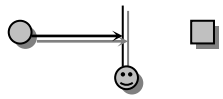
– активні;
– пасивні.

До першої групи ставляться:

– переривання - порушення доступності й конфіденційності;
– модифікація - порушення цілісності;
– фальсифікація - порушення автентичності.

Таблиця 3.2

Класифікація порушень захисту інформації

Види порушень	Активність порушень	Графічне представлення порушень	Порушення властивості інформації
Перехват інформації, що передається	Пасивне		Конфіденційність інформації, що передається
Переривання інформації, що передається	Активні		Доступність інформації
Модифікація інформації, що передається			Конфіденційність та цілісність інформації, що передається
Фальсифікація інформації, що передається			Автентифікація інформації, що передається

Даний тип порушень має активний характер впливу на елементи мережі й передану інформацію. Основна мета цих порушень складається в зміні або знищенні потоків інформації на мережі.

До пасивних порушень ставиться перехоплення з метою одержання переданої інформації, її аналізу й використання в певних цілях.

Досить упевнено можна затверджувати, що пасивні порушення ставлять своєю кінцевою метою перехід у групу активних порушень.

Наведена вище класифікація порушень захисту інформації представлена в таблиці 3.2.

Перераховані види порушень можуть мати місце, як у площині користувача, так і в площинах керування й менеджменту рис. (3.2 б). Причому, ак-

тивні види порушень (переривання, модифікація й фальсифікація) у площині менеджменту ведуть до порушень або знищення інформації, збереженої в базах даних КК. У результаті порушуються таблиці маршрутизації і як результат - неможливість нормального функціонування площин керування (сигналізації) і користувача.

3.4.2. Сервісні служби, профіль захисту і з'єднання захисту інформації

Сервісні служби захисту інформації (рис.3.4) є відповідальними за забезпечення основних вимог користувачів, пропонованих до телекомунікаційних систем (з погляду її надійності). Причому дані служби повинні функціонувати у всіх трьох площинах: менеджменту, керування й користувальницької.

Рис. 3.4 Сервісні служби захисту інформації

Сукупність сервісних служб захисту інформації, що забезпечують вимоги користувачів, утворять профіль захисту.

За установку й припинення дії тієї або іншої служби відповідають агенти захисту (Security Agent , SA). Узгодження служб захисту між агентами відбувається через з'єднання захисту. По цих з'єднаннях виробляється обмін інформацією захисту.

Рис. 3.5 демонструє найпростіший варіант організації з'єднання захисту - агенти захисти розміщені в межах кінцевих систем користувачів. У цьому випадку кінцеві системи й агенти захисту взаємодіють із мережею через інтерфейс «користувач - мережа + захист» (UNI+Sec).

Агенти захисту для віртуального з'єднання (каналу або тракту), що встановлений між кінцевими системами користувачів, послідовно виконують наступні дії:

– визначають вид сервісних служб захисту, які повинні бути застосовані до даного віртуального з'єднання;
– погоджують служби захисту між собою;
– застосовують необхідні служби захисту до даного віртуального з'єднання.

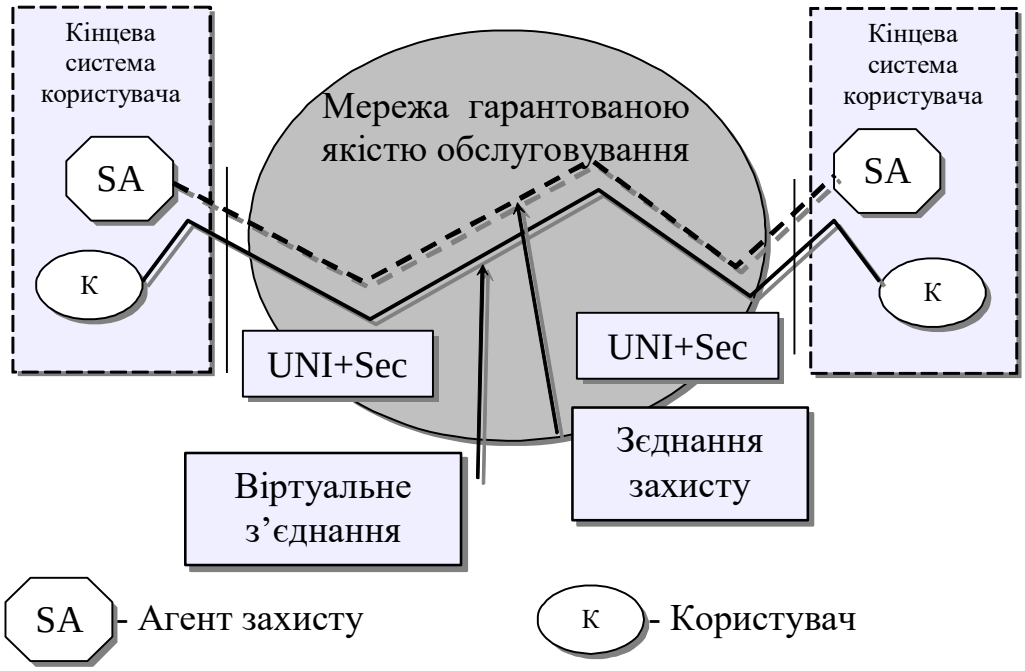


Рис. 3.5 Варіант організації з’єднання захисту між агентами захисту

За установку й припинення дії тієї або іншої служби відповідають агенти захисту (Security Agent , SA). Узгодження служб захисту між агентами відбувається через з'єднання захисту. По цих з'єднаннях виробляється обмін інформацією захисту.

Рис. 3.6 демонструє найпростіший варіант організації з'єднання захисту - агенти захисти розміщені в межах кінцевих систем користувачів. У цьому випадку кінцеві системи й агенти захисту взаємодіють із мережею через інтерфейс «користувач - мережа + захист» (UNI+Sec).

Агенти захисту для віртуального з'єднання (каналу або тракту), що встановлений між кінцевими системами користувачів, послідовно виконують наступні дії:

– визначають вид сервісних служб захисту, які повинні бути застосовані до даного віртуального з'єднання;

– погоджують служби захисту між собою;

– застосовують необхідні служби захисту до даного віртуального з'єднання.

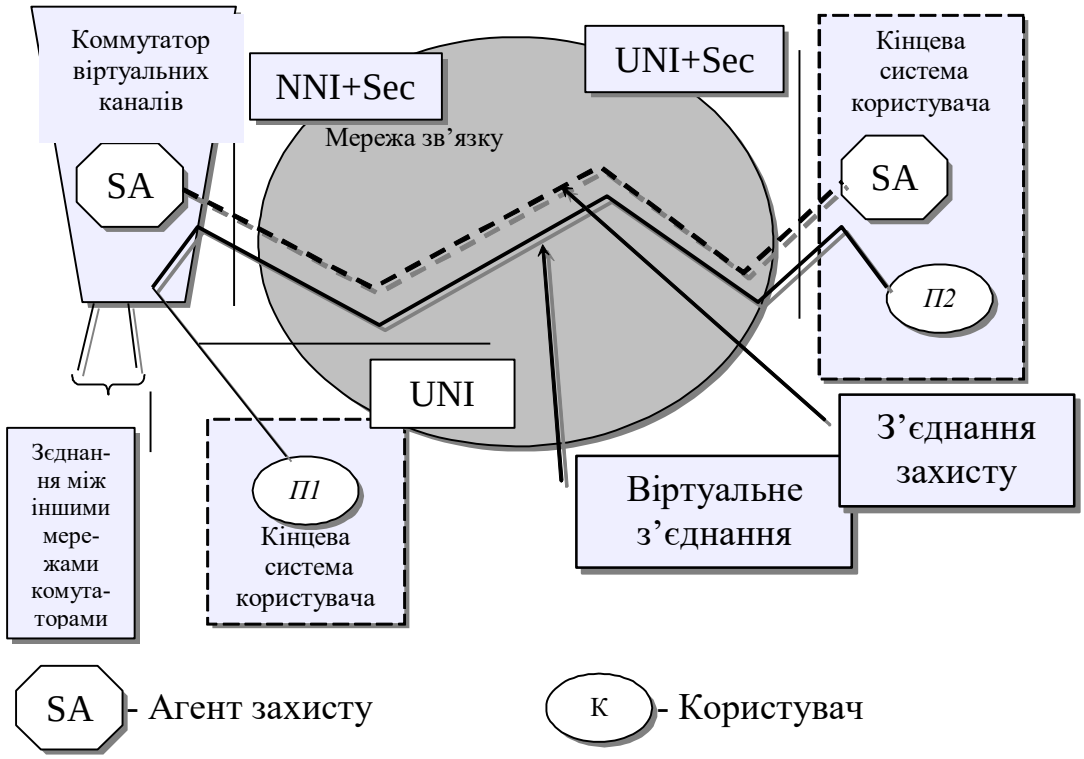


Рис. 3.6 Варіант організації з'єднання захисту між агентами захисту

Кількість з'єднань захисту повинне бути дорівнює кількості встановлених служб захисту. Тобто, якщо для даного віртуального з'єднання одночасно потрібно автентифікація, конфіденційність і вірогідність даних, то встановлюється три самостійних з'єднання захисту.

Рис. 3.6 показує інший варіант організації з'єднання захисту. У цьому випадку один агент захисту розміщається на кінцевій системі користувача, а іншої на комутаторі віртуальних каналів. Відповідно, користувачі й агенти захисту взаємодіють із мережею зв'язку через інтерфейси «користувач – мережа» (UNI) або UNI+Sec; комутатор віртуальних каналів через інтерфейс «вузол – мережа + захист» (NNI+Sec). У цьому випадку агент захисту, розміщений у межах комутатора віртуальних каналів, має можливість забезпечувати служби захисту не тільки для користувача *П*2, але й для інших вузлів і мереж, які приєднуються до даного комутатора віртуальних каналів. Часто таких агентів захисту називають брандмауерами. Фактично брандмауер - це

шлюз, що виконує функції захисту мережі від несанкціонованого доступу з поза (наприклад, з іншої мережі).

Розрізняють три типи брандмауерів (рис.3. 7).

Шлюз рівня додатків часто називають проксі – сервером (proxy server) - виконує функції ретранслятора даних для обмеженого числа додатків користувача. Тобто, якщо в шлюзі не організована підтримка того або іншого додатка, те відповідний сервіс не надається, і дані відповідного типу не можуть пройти через брандмауера.

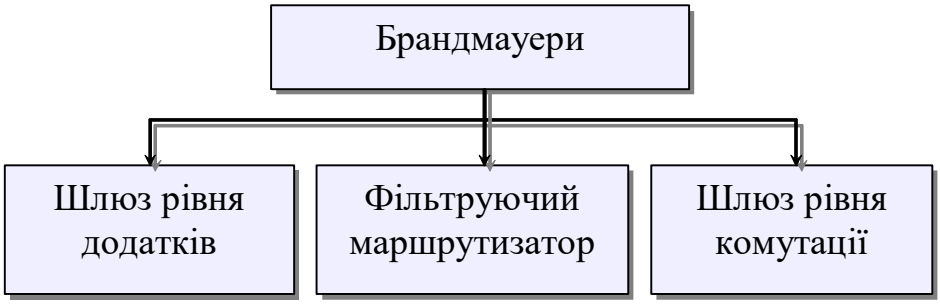


Рис. 3.7 Типи брандмауерів

Фільтруючий маршрутизатор. Точніше це маршрутизатор, у додаткові функції якого входить фільтрування пакетів (packet-filtering router). Використається на мережах з комутацією пакетів у режимі дейтаграм. Тобто, у тих технологіях передачі інформації на мережах зв'язку, у яких площина сигналізації (попереднього встановлення з'єднання між УИ й УП) відсутній (наприклад, IP V 4). У цьому випадку ухвалення рішення про передачу по мережі пакета, що надійшов, даних ґрунтується на значеннях його полів заголовка транспортного рівня. Тому брандмауери такого типу звичайно реалізуються у вигляді списку правил, застосовуваних до значень полів заголовка транспортного рівня.

Шлюз рівня комутації – захист реалізується в площині керування (на рівні сигналізації) шляхом дозволу або заборони тих або інших з'єднань.

Для збільшення надійності захисту віртуальних з'єднань (каналів і трактів) можливе використання більше однієї пари агентів захисту й більше одного з'єднання захисту. У цьому випадку формується топологія з'єднань захисту, в основі якої закладений принцип вкладення й не перетинання з'єднань захисту уздовж усього маршруту між УІ й УП (або кінцевими системами користувачів). Приклад принципу вкладення й не перетинання з'єднань захисту наведений на рис. 3.8. У цьому випадку захист віртуального каналу, організованого між кінцевими системами, здійснюється чотирма з'єднаннями захисту й вісьма агентами захисту (*SA*1 – *SA*8). Причому, кожне з'єднання не знає про існування інших з'єднань і не піклується про те, яку службу захисту останні забезпечують. Тобто, з'єднання захисту абсолютно незалежний друг від друга. Даний підхід дозволяє застосовувати численні стратегії й тактики захисту різних ділянок мережі. Наприклад, з'єднання захисту між агентами *SA*1 і *SA*8 забезпечує автентифікацію між кінцевими системами. Незалежно від даного з'єднання між *SA*2 і *SA*7 забезпечує конфіденційність, а *SA*2, *SA*3, *SA*4 і *SA*4, *SA*5, *SA*6 вірогідність даних.

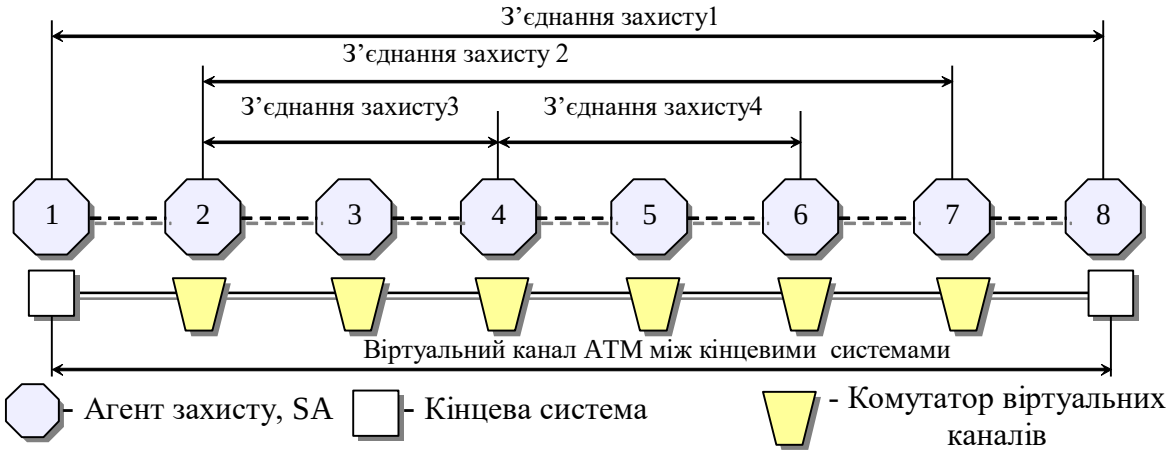


Рис. 3.8. Приклад організації топології з'єднання захисту з використанням принципу вкладання і не перетинання

Кожне з'єднання захисту можна представити у вигляді сегмента

$$S_k = \lfloor SA_i, SA_j \rfloor,$$

де *k* – порядковий номер з'єднання захисту; *i, j* – порядкові номери агентів захисту.

Для рис. 3.8 з'єднання захисту можна записати відповідними сегментами:

$$S_1 = [SA_1, SA_8];$$
$$S_2 = [SA_2, SA_7];$$
$$S_3 = [SA_2, S_3, SA_4];$$
$$S_4 = [SA_4, S_5, SA_6].$$

У свою чергу другий сегмент виявляється вкладеним у перший. Тобто, у символьній формі це виглядає в такий спосіб:

$$S_2 \subset S_1.$$

Не перетинання сегментів S_3 і S_4 можна представити у вигляді:

$$S_3 \not\subset S_4.$$

З огляду на, що $S_3 \not\subset S_4$ вкладено в S_2,то одержимо:

$$[[S_3 \not\subset S_4] \subset S_2].$$

Остаточний символьний запис топології з'єднань захисту, представлений на рис. 3.8, виглядає в такий спосіб:

$$[[S_3 \not\subset S_4] \subset S_2] \subset S_1.$$

З рис. 3.8. і отриманого виразу видно, що дана топологія з'єднань захисту віртуального каналу між кінцевими системами має три рівні вкладення.

У такий спосіб:

– принцип вкладення й не перетинання з'єднань захисту;

– гранична кількість рівнів вкладення (для технології АТМ до 16 рівнів);

є єдиними обмеженнями організації топології з'єднань захисту для одного віртуального з'єднання (каналу або тракту).

У теж час, для топології захисту, зображеної на рисунку 7.6 з'єднання між агентами *SA*3 і *SA*5 не можливо, тому що порушується принцип не перетинання.

Таким чином, топологія з'єднань захисту реалізує профіль захисту користувача, що є розподіленим по мережі.

Вибір топології з'єднань захисту багато в чому визначається вимогами користувачів до ступеня захищеності переданої інформації й ресурсних можливостей самої мережі забезпечити дані вимоги.

3.4.3. Обмін інформацією між агентами захисту

Установлення й підтримка з'єднань захисту на мережах АТМ досить складний і відповідальний процес, що складається із двох етапів і базується на протоколі обміну повідомленнями захисту (Security Message Exchange, SME) і передачі спеціальних осередків захисту OAM (рис. 3.10).

Рис. 3.10. Етапи встановлення и підтримки з’єднань захисту

Протокол обміну повідомленнями захисту SME використається для:

– автентифікації агентів між собою;

– узгодження служб захисту між агентами захисту;

– установлення з'єднання захисту.

Можливо два варіанти реалізації протоколу SME:

– у площині керування (з використанням каналу сигналізації).

– у площині користувача (з використанням каналу даних, установленого сигналізацією раніше).

У першому випадку агенти захисту додають до сигнального повідомлення інформаційний елемент служб захисту (Security Services Information Element, SSIE).

У другому випадку протокол SME реалізується через установлене з'єднання між користувачами мережі АТМ. При цьому на час дії протоколу обміну повідомленнями захисту передача даних користувачів блокується.

У випадку якщо частина елементів мережі не підтримує протокол SME з використанням сигналізації, то допускається комбіноване застосування обох варіантів. Тобто, частина мережі застосовує протокол SME у площині керування (сигналізації), а інша в площині користувачів.

Передача осередків захисту OAM використається тільки для підтримки з'єднань захисту й застосовується після завершення протоколу SME.

3.4.4. Захист інформації в площині користувача

Автентифікація площини користувача або автентифікація об'єкта – ця служба відповідає за визначення ідентичності зухвалого й/або викликуваного користувачів оригіналу. Автентифікація є основною для встановлення надійних з'єднань. Дана служба є базовою для інших служб захисту.

Автентифікація може бути як взаємної (симетричної), так і однобічної (асиметричної). У першому випадку обоє користувача автентифікують один одного. При однобічної автентифікації тільки один користувач аутентифікується для іншого.

Автентифікація забезпечується через обмін інформацією між агентами безпеки, які обмінюються між собою повідомленнями безпеки (Security Message Exchange, SAsme). У свою чергу, обмін повідомленнями безпеки можливий або в площині сигналізації, або в площині користувача.

Конфіденційність площини користувача забезпечується криптографічними механізмами, які захищають дані «користувача» у віртуальних каналах і трактах від несанкціонованого розкриття. Дана служба функціонує на рівні

осередків АТМ. При цьому шифрується тільки користувальницька частина осередку АТМ. Заголовок осередку передається незашифрованим.

Вірогідність даних або «оригінальна автентифікація даних» площини користувача забезпечується механізмом, що дозволяє визначати навмисну модифікацію даних. Дана служба функціонує між користувачами на рівні AAL (для AAL S і AAL 5) і може бути реалізована у двох варіантах:

– вірогідність даних без захисту від повторної модифікації;
– вірогідність даних із захистом від повторної модифікації.

У першому випадку джерело перед передачею додає криптографічну характеристику наприкінці кожної AAL SDU. Ця характеристика обчислюється по всім AAL SDU. Цей варіант реалізації вірогідності даних корисний для протоколів верхнього рівня, які забезпечують свою власну нумерацію послідовності (наприклад TCP), без додавання заголовка, необхідного для дублювання даної функції на рівні AAL.

Другий варіант реалізації вірогідності даних деректує і відбраковує «старі» або «з» AAL-SDU. Це досягається спочатку додаванням номера послідовності наприкінці кожної AAL-SDU, а потім обчисленням характеристики для сукупності AAL-SDU, включаючи номера послідовності. Це характеристика, що захищає й AAL-SDU і номер послідовності, потім додається д загального AAL-SDU (якого включає номер послідовності). Цей метод забезпечує захист додатків АТМ, які не здійснюють свою власну нумерацію послідовності.

Контроль доступу площини користувача – це застосування набору правил для запиту послуги. Ці правила можуть залежати від атрибутів зухвалого об'єкта, таких як ідентичність, атрибутів відповідних параметрів, таких як цільова адреса, системних атрибутів, таких як час і історія попередніх запитів даним або іншим об'єктам клієнта. Правила контролю доступу можуть бути предикатом, сформованим всіма цими атрибутами. Якщо предикат удоволе-

ний, то запитувана служба (послуга) надається, якщо предикат не вдоволений, те запитувана служба не надається.

Контроль доступу площини користувача вимагає механізмів для транспортування інформації контролю доступу, використовуваної під час установлення з'єднання, тому що механізми усередині компонентів АТМ використають цю інформацію, щоб визначити потрібно чи надавати доступ до з'єднання. Контроль доступу площини користувача може ґрунтуватися на мітках захисту (наприклад, стандартні мітки захисту [10]), ідентичності джерела або одержувача, часу дня, типі служби, полях протоколу вищого рівнем (наприклад, протокол Інтернет), або на інших параметрах, які можуть бути визначені під час установлення з'єднання.

Контроль доступу площини користувача забезпечується на рівні АТМ.

3.4.5. Служби підтримки

Перераховані служби захисту інформації, які часто називають базисом служб захисту. Крім даного базису існують також служби підтримки, які необхідні для забезпечення масштабованості й підвищення ефективності базису служб захисту (рис. 3.11):

– обмін повідомленнями захисту й узгодження опцій захисту

– обмін ключами

– відновлення ключів

– інфраструктура сертифікації.

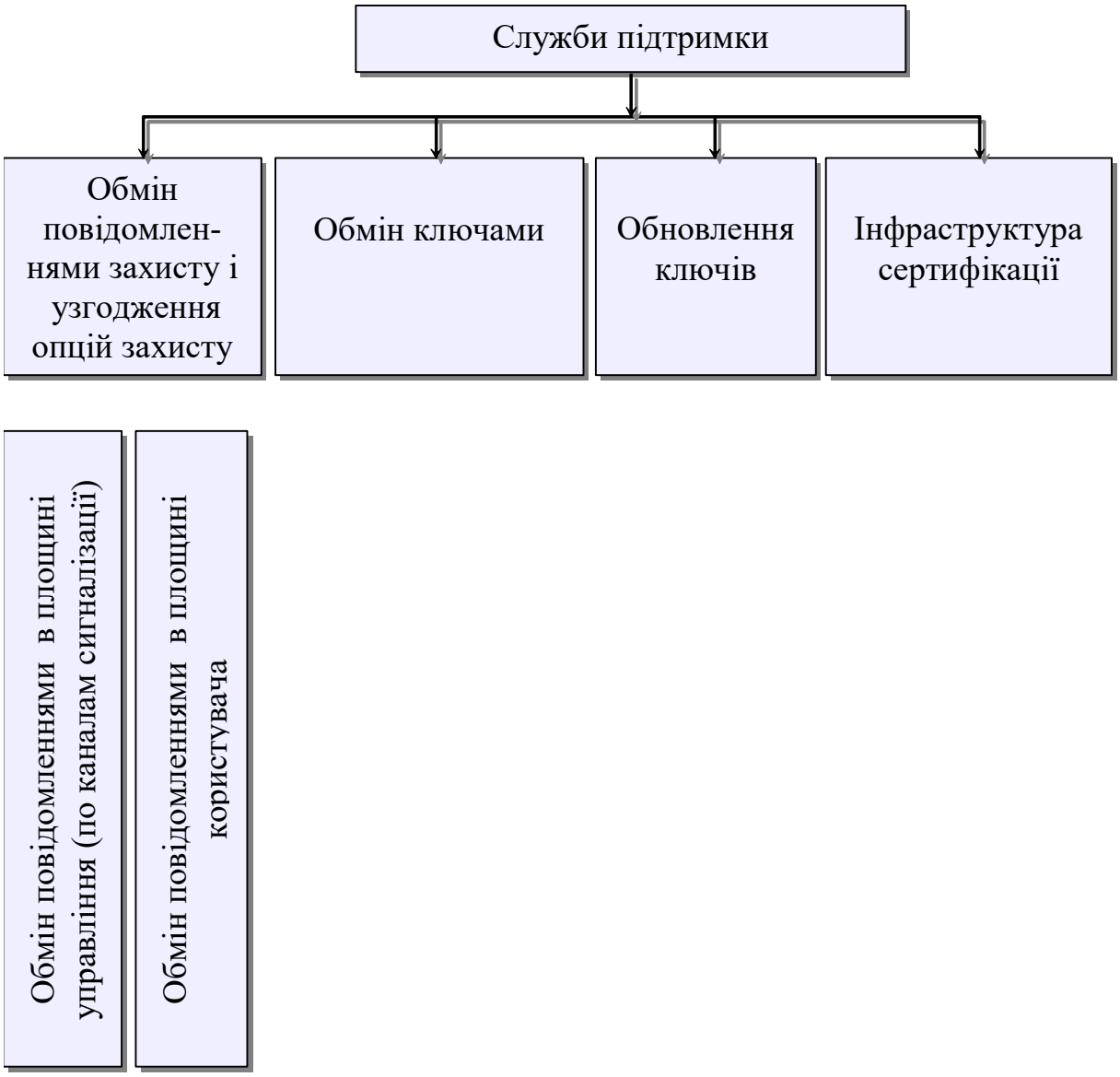


Рис.3.11. Служби підтримки базису служб захисту в площині користувача

Обмін повідомленнями захисту й узгодження. Для того щоб надати більшість служб, описаних вище, повинні передаватися повідомлення між залученими агентами захисту (SA). Дана специфікація описує два методи обміну повідомленнями захисту - обмін повідомленнями по сигналізації UNI 4.0 і

обмін повідомленнями in-band (тобто обмін повідомленнями захисту по доречному віртуальному каналі площини користувача).

Ці методи обміну повідомленнями також забезпечують механізм для узгодження опцій захисту. Для вимоги захисту різні для різних організацій, важливо забезпечити асортименти служб захисту, алгоритмів і терміновості ключів, які відповідають широкій області потреб захисту. Крім того, закони експорту й/або імпорту деяких країн накладають обмеження, через які зашифровані продукти можуть імпортуватися/експортуватися. Із цих причин механізми захисту АТМ підтримують множинні служби захисту, алгоритми й тривалості ключів. Для того щоб агент захисту відповідав загальним параметрам захисту (таким як алгоритми й тривалості ключів), ці методи обміну повідомленнями захисту забезпечують узгодження цих параметрів як частина процедури встановлення захисту для VC.

Обмін ключами – це механізм, за допомогою якого два агенти захисту обмінюються секретними ключами для служб конфіденційності й/або вірогідності. Для того щоб протистояти атакам типу «людина в середині», обмін ключем звичайно зв'язаний зі службою автентифікації. Це може бути здійснене шляхом включення «конфіденційного» ключа усередині параметрів обміну потоків автентифікації.

Також як автентифікація, обмін ключем представлений і для симетричних (секретний ключ) і для асиметричних (публічний ключ) алгоритмів. Крім того, обмін ключем може бути двунаправленним (два шляхи) і односпрямованим (один шлях).

Відновлення ключа сеансу. Ключі сеансу - це ключі, використовувані прямо для забезпечення служб конфіденційності й вірогідності площини користувача через віртуальні канали АТМ. Тому що швидкість даних може бути високої в VC, конче потрібно періодично міняти ключі, щоб уникнути «повторного використання ключа». Дана специфікація визначає службу відновлення ключа сеансу, що забезпечує цю можливість.

Ця служба представлена у двох фазах - фаза обміну ключем сеансу й фаза зміни ключа сеансу. Фаза обміну ключем сеансу використає «майстер ключ», яким обмінюються при встановленні з'єднання (використовуючи службу обміну ключем), щоб зашифрувати новий ключ сеансу. При прийманні зашифрованого ключа сеансу, приймач розшифровує ключ сеансу, використовуючи загальний майстер ключ, і зберігає його для другої фази - зміни ключа.

Інфраструктура сертифікації. У криптосистемі публічного ключа кожна сторона (агент захисту) X має пари ключів: один – привселюдно відомий – «публічний ключ» X ($РК_X$), і інший, відомий тільки X – «приватний ключ» X (SK_X). Для того, щоб сторона A послала секретну інформацію стороні B (або щоб сторона могла перевірити характеристику, передану стороною B), A повинна одержить публічний ключ B, $РК_B$. Хоча $РК_B$ – публічний, по визначенню, ніяка сторона X не повинна мати можливість замінити $РК_B$ на іншій (наприклад $РК_X$). Щоб запобігти такого роду впливи, публічним ключем можна обмінюватися у формі «сертифіката».

Сертифікат містить ім'я сторони, її публічний ключ і деяка додаткова інформація й позначається стороною, що довіряє, «орган сертифікації» (CA). Ця характеристика жорстко зв'язує публічний ключ із предметною стороною. Будь-яка сторона, що має доступ до публічного ключа CA може перевіряти дійсність сертифіката (шляхом перевірки характеристики CA в сертифікаті) і використати публічний ключ, що сертифікований. Один раз відзначені сертифікати можуть передаватися через комутатори повідомлень не підтримуючий захист.

ВИСНОВКИ

В бакалаврської роботі розглянуто політику безпеки, основні її засади, загрози інформації та їх класифікацію канали витоку інформації, канали зв'язку та їх захист .

Розглянуто побудову систем захисту, на прикладі побудови СЗІ ІС визначені задіяні групи та елементи системи.

Детально розглянуті:

- система захисту телефонних каналів;
- захист інформації на ВОЛЗ;
- захист інформації в системі управління ЦПМЗ України;
- проблеми захисту інформації в АС;
- захист інформації в мережах АТМ, IP.

Поняття Управління інформації в телекомунікаційних системах слід відносити до усіх її дільниць, розуміючи під „управлінням" обов'язкове виконання вимог політики безпеки, гнучке реагування на зміну ситуації.

Виходячи з приведеного маємо:

1. Магістральна і внутрішньо зонова частини мережі зв'язку України побудовані на базі ВОЛЗ.
2. Зняти інформацію з ВОЛЗ, на її лінійній і станційній дільницях практично неможливо.
3. Разом з тим, існуюча мережа в структурному плані себе вичерпала.
4. Створення кабелю з довільною будівельною довжиною, з надзвичайно низьким загасанням, покращення технології зварювання, випуск ВОК без металу , впровадження новітніх систем та технологій передачі дозволяє ставити питання про зміну принципів побудови мережі.
5. Найбільш незахищеною є місцева дільниця. Виходячи з інтересів захисту інформації доцільно кодеки ставити безпосередньо у абонентів, на скрізній дільниці „абонент-абонент" використовувати захищені канали (криптографічний захист).

ПЕРЕЛІК ПОСИЛАНЬ

1. Хорошко В.А., ЧекатковА.А. Методи и средства защитi информации / Под ред. Ю.С. Ковтанюка – К.: Издательство Юниор, 2003.-504., с, ил. ISBN 966-7323 – 29-3.
2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты
3. Защита информации в компьютерных системах и сетях / Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.; Под ред. В.Ф.Шаньгина. - М.: Радио и связь, 1999. - 328с.
4. С.Н. Новиков. Защита информации в сетях связи с гарантированным качеством обслуживания / Учебное пособие. — Новосибирск: 2003.— 84 с.: ил.
5. Герасименко В.А. «Защита информации в автоматизированных системах обработки данных» Москва, Энергоатомиздат 1994 г.
6. Гордиенко В.Н., Ксенофонтов С.Н., Кунегин С.В., Цыбулин М.К. Современные высокоскоростные цифровые телекоммуникационные системы. Ч. 2. Основы технологии АТМ: Учебное пособие / МТУСИ. - М., 1998. - 65 с.
7. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографических преобразований
8. ГОСТ 34.310-95. МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ. Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. Киев. Госстандарт Украины. 1998

9. Принципи побудови системи захисту інформації в різнорідних автоматизованих системах Будько М. М., Волков О. М., Короленко М. П. ВАТ “КП ОТІ”, м. Київ.
10. Проблеми захисту інформації в автоматизованих системах інформації в автоматизованих системах обробки даних та зв’язку Макаренко Б. І., Трощило О. С.Акціонерне товариство Науково-дослідний інститут радіотехнічних вимірювань, м. Харків.
11. Аспекти політики безпеки системи управління телекомунікаційними мережами. Микола Тардаскін, Володимир Кононович Одеський регіональний центр технічного захисту інформації ВАТ “УКРТЕЛЕКОМ”.
12. Защита информации в системе управления цифровой первичной сетью связи Украины Кононович В. Г., Голобородько Д. В. Украинская государственная академия связи, г. Одесса.
13. Принципи побудови системи захисту інформації в різнорідних автоматизованих системах Будько М. М., Волков О. М., Короленко М. П. ВАТ “КП ОТІ”, м. Київ.
14. Проблеми захисту інформації в автоматизованих системах обробки даних та зв’язку Макаренко Б. І., Трощило О. С. Акціонерне товариство Науково-дослідний інститут радіотехнічних вимірювань, м. Харків.
15. Один из аспектов технической защиты информации в телекоммуникационных системах Олег Степанов Военный институт Национального технического университета Украины «КПИ».
16. ВОСП и защита информации Свинцов А. Г. “Прогноз+”, г. Москва.
17. Захист інформації у волоконно-оптичних мережах звязку Михайло Задорожній, Віктор Каток, Олександр Манько Науково-інженерний центр лінійно-кабельних споруд при Державному комітеті зв’язку та інформатизації України, м. Київ.
18. Защита информации на волоконно-оптических линиях связи от несанкционированного доступа Александр Манько, Виктор Каток, Михаил

Задорожний Научно-инженерный центр линейно-кабельных сооружений Киевского института связи при Государственном комитете связи и информатизации Украины, г. Киев.

19. Загрози інформації і канали витоку Анатолій Антонюк, Віктор Жора Інститут програмних систем Національної Академії наук України,Національний технічний університет України «КПІ».
20. Закон України "Про інформацію"
21. Закон України "Про захист інформації в автоматизованих системах"
22. Закон України "Про державну таємницю"