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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Палія Вадима Володимировича*

академічної групи *125м-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка методики оцінки інформаційної безпеки телекомунікаційного комплексу SI3000*

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

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту ***Палію Вадиму Володимировичу*** **академічної групи** ***125м-19-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка методики оцінки інформаційної безпеки телекомунікаційного комплексу SI3000***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Розглянути проблему впровадження та проблеми захисту інформації в мультисервісних мережах, види несанкціонованого доступу персоналу, що складає загрозу інформаційної безпеки в мультисервісних мережах.	10.10.2020
Розділ 2	Реалізувати методику оцінку рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000	20.11.2020
Розділ 3	Обґрунтування економічної доцільності застосування методики оцінки інформаційної безпеки телекомунікаційного комплексу SI3000	05.12.2020

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

Дата видачі: 01.09.2020р.

Дата подання до екзаменаційної комісії: 11.12.2020р.

Прийнято до виконання _____ Палій В.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ___ с., __ рис., __ табл., __ додатки, __ джерел.

Об'єкт дослідження: телекомунікаційний комплекс SI3000 на базі мультисервісної мережі.

Мета роботи: реалізація методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000.

У роботі розглянуто проблеми впровадження та проблеми захисту інформації в мультисервісних мережах (МСМ), види несанкціованого доступу персоналу, що складає загрозу інформаційної безпеки в мультисервісних мережах.

В спеціальній частині проаналізовані атаки на МСМ, складена модель загроз і модель порушника для даної мережі. А також обрано профіль захищеності, який гарантує цілісність, доступність і конфіденційність інформації, що передається по мережі. Реалізовано методику оцінку рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000.

В економічному розділі розраховано експлуатаційні та капітальні затрати, дисконтований період самоокупності телекомунікаційного комплексу SI3000.

Наукова новизна роботи полягає в реалізації процедури оцінювання рівня захищеності, та її адаптації яка виконується на базі телекомунікаційного комплексу SI3000.

МУЛЬТИСЕРВІСНІ МЕРЕЖІ, ЗАХИСТ ІНФОРМАЦІЇ, ТЕЛЕКОМУНІКАЦІЙНИЙ КОМПЛЕКС SI3000, РИЗИК, ЗАГРОЗИ.

РЕФЕРАТ

Пояснительная записка: ___ с., __ рис., __ табл., __ приложений, __ источников.

Объект исследования: телекоммуникационный комплекс SI3000 на базе мультисервисной сети.

Цель работы: реализация методики оценки уровня защищенности информации, обрабатываемой в телекоммуникационном комплексе SI3000.

В работе рассмотрены проблемы внедрения и проблемы защиты информации в мультисервисных сетях (МСМ), виды несанкционированого доступа персонала, что составляет угрозу информационной безопасности в мультисервисных сетях.

В специальной части проанализированы атаки на МСМ, составленна модель угроз и модель нарушителя для данной сети. А также избран профиль защищенности, который гарантирует целостность, доступность и конфиденциальность информации, передаваемой по сети.

Реализовано методику оценку уровня уровня защищенности информации, обрабатываемой в телекоммуникационном комплексе SI3000.

В экономическом разделе рассчитаны эксплуатационные и капитальные затраты, дисконтированный период окупаемости телекоммуникационного комплекса SI3000.

Научная новизна работы заключается в реализации процедуры оценки уровня защищенности, и ее адаптации, которая выполняется на базе телекоммуникационного комплекса SI3000.

МУЛЬТИСЕРВИСНЫЕ СЕТИ, ЗАЩИТА ИНФОРМАЦИИ, ТЕЛЕКОММУНИКАЦИОННЫЙ КОМПЛЕКС SI3000, РИСК, УГРОЗЫ.

ABSTRACT

Explanatory note: ___ p., __ fig., __ tab., __ application, __ sources.

The object of study: telecommunication complex SI3000 based on a multiservice network.

The purpose of work: to put into practice a safety level evaluation technique of information processed in the telecommunication complex SI3000.

In the work, the problems of information input and security in multiservice networks (MSN) are considered, as well as kinds of staff's unauthorized access, which is dangerous for information security in multiservice networks, the influence of the human factor and the authorization problems in a multiservice network.

In the specialty part, attacks on an MSN are analyzed; a model of threats and a model of an intruder for the given network are composed. Besides, such a security profile is chosen that guarantees integrity, accessibility, and privacy of the information transmitted over the network.

In the economics part, the operating and capital costs, and the discounted self-efficiency period of the telecommunication complex SI3000 are calculated.

The practical value of the work is found in a realization of a safety level evaluation procedure and in its adaptation based on of the telecommunication complex SI3000.

MULTISERVICE NETWORKS, INFORMATION SECURITY, THE TELECOMMUNICATION COMPLEX SI3000, HAZARD, THREATS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСТУ – державний стандарт України;

ЕОМ – електронна вимірювальна машина;

ІБ – інформаційна безпека;

ІТ – інформаційні технології;

КЗЗ – комплекс засобів захисту;

КМ – комп'ютерні мережі;

КСЗ – комплексна система захисту;

КСЗІ – комплексна система захисту інформації;

МПД – мультисервісний пристрій доступу;

МСМ – мультисервісна мережа;

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПК – персональний комп'ютер;

ПЗ – програмного забезпечення;

СЗІ – система захисту інформації;

СУБД – система управляння базою даних;

AS – application server;

CS – call server;

DoS – denial of service;

IP – internet protocol;

IPTV – internet protocol television;

ISO – international organization for standardization;

MGCP – media gateway control protocol;

MSAN – multi service access node;

MSCN – multi-Service control node;

MSN - multiservice networks;

OSAP – open service and application plane;

OSI – open systems interconnection;

QoS – open systems interconnection;

SIP – session initiation protocol;

SMG – signaling and media gateway;

TCP / IP – transmission control protocol / internet protoco;

UID – user interface design;

USB – universal serial bus.

ЗМІСТ

с.

ВСТУП

Мультисервісна мережа (МСМ) дозволяє надавати користувачам різноманітні послуги зв'язку, що розрізняються як за якісними, так і за кількісними характеристиками. Саме таке рішення дозволить відмовитися від численних дублюючих одна одну мереж, а в перспективі – впроваджувати нові послуги, забезпечуючи виконання їх специфічних вимог по швидкості і якості передачі інформації.

Теоретично в МСМ не повинно бути розходжень між користувачами. Будь-який її абонент зможе користуватися будь-яким типом послуг, обмеженнями будуть лише платоспроможність абонента, умови контракту та наявність відповідного кінцевого обладнання. Необхідно, щоб у будь-який момент він міг потребувати ту чи іншу послугу і в будь-який момент відмовитися від неї, перейшовши на роботу в більш економічному режимі. Саме в задоволенні цих вимог полягає одна з основних проблем функціонування таких мереж.

Для МСМ потрібна більш складніша система керування, ніж для традиційних комп’ютерних мереж, а також більш складна система захисту інформації, оскільки додаються безліч нових послуг і програмних додатків в єдиному транспортному середовищі, а з цим з’являються нові види атак і загроз.

Оскільки для великих компаній з розрізненими офісами або виробництвами, що займають великі території, мультисервісні мережі дозволяють на порядок збільшити оперативність обміну інформацією, забезпечити доступність даних у будь-який час, влаштовувати між офісами або відділами селекторні наради, відеоконференції, питання захисту конфіденційної і комерційної інформації займає важливу роль у функціонуванні МСМ.

В роботі розглядається побудова МСМ на базі телекомунікаційного комплексу SI3000, який відрізняється високою пропускною здатністю, надійністю та відноситься до найбільш сучасних засобів операторського класу.

Розроблена методика з оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000.

Методика оцінки рівня захищеності інформації розглядається з боку ризиків. В основу методики покладено ідею, що рівень ризиків в захищеній системі повинен бути мінімальний по відношенню до рівня захищеності системи, що без захисту. У даній ситуації можна отримати кількісну оцінку рівня захищеності інформації. Рівень точності оцінки багато в чому залежить від повноти списку висунутих вимог до системи захисту інформації та відповідно до вимог, списку висунутих загроз.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

Актуальність обраної теми

На різних етапах життєвого циклу мультисервісної мережі неминуче постає задача оцінювання її рівня захищеності від методів несанкціонованого доступу до інформації. Дана методика з оцінки рівня захищеності інформації досліджувалась щодо адаптації до конкретної конфігурації телекомунікаційного комплексу SI3000. Тому, тема дослідження є актуальною, новою, а визначений напрям наукових досліджень пріоритетним.

Мета дослідження

Створення методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000, кількісно залежно від вартості інформації, що захищається; ймовірності зламу; вартості самої системи захисту комплексу; продуктивності системи захисту інформації.

Об'єкт дослідження

Телекомунікаційний комплекс SI3000, що реалізується на базі мультисервісної мережі.

Предмет дослідження

Методи та засоби безпеки в мультисервісних мережах передачі даних, що працюють з телекомунікаційним комплексом.

Задачі дослідження

- аналіз та вибір критеріїв оцінювання рівня захищеності телекомунікаційного комплексу SI3000;
- завдання вхідних параметрів для методики оцінювання;
- розробка покрокової методики оцінювання рівня захищеності та алгоритму проведення методики.

1.1 Основні поняття мультисервісних мереж

На сьогодні на ринку інфокомунікаційних послуг мережі перевантажені: вони переповнені численними інтерфейсами клієнтів і контролюються занадто великим числом систем управління. Більше того, кожна служба прагне

створити свою власну мережу, викликаючи експлуатаційні витрати по кожній службі, що не сприяє загальному успіху [1].

Мультисервісна мережа (МСМ) - це мережа зв'язку, яка забезпечує надання необмеженого набору послуг.

Мультисервісність - підтримка безлічі послуг програмно-апаратними засобами однієї мережі.

У концепції МСМ закладена ідея конвергенції існуючих мереж і технологій. Конвергенція - процес поступового зближення різних технологій і служб зв'язку з метою уніфікації обладнання та розширення функціональних можливостей.

МСМ являє собою універсальне багатоцільове середовище, ця мережа призначена для передачі мови, зображень і даних з використанням технології комутації пакетів (IP). МСМ відрізняється надійністю, характерною для телефонних мереж (на противагу негарантованої якості зв'язку через Інтернет), і забезпечує низьку вартість передачі в розрахунку на одиницю об'єму інформації (наближається до вартості передачі даних по Інтернету).

Основне завдання МСМ полягає в тому, щоб забезпечити роботу різнорідних інформаційних і телекомунікаційних систем та програм в єдиному транспортному середовищі, коли для передачі і звичайного трафіку (даних), і трафіку іншої інформації (мови, відео і т. п.) використовується єдина інфраструктура. МСМ відкриває масу можливостей для побудови різноманітних накладених сервісів поверх універсального транспортного середовища - від пакетної телефонії до інтерактивного телебачення і Web-сервісів.

МСМ, використовуючи єдиний канал для передачі даних різних типів, дає можливість зменшити різноманітність типів обладнання, застосовувати єдині стандарти і технології, централізовано керувати комунікаційним середовищем.

Вимоги, яким повинна задовольняти мультисервисна мережа:

- гарантована якість обслуговування (QoS) користувачів;

- доставка інформації, чутливої до затримки, в реальному масштабі часу;

- забезпечення передачі даних з необхідною швидкістю;

- централізоване управління мережею.

Основні відмінності таких мереж полягають у наступному:

- можливість передачі великій кількості користувачів в реальному часі дуже великих обсягів інформації з необхідною синхронізацією і з використанням складних конфігурацій сполук;

- інтелектуальність (управління послугою, викликом і з'єднанням з боку користувача або постачальника сервісу, роздільна тарифікація і керування умовним доступом);

- інваріантність доступу (організація доступу до послуг незалежно від використовуваної технології);

- комплексність послуги (можливість участі декількох провайдерів у наданні послуги і поділ їх відповідальності та доходу згідно з видом діяльності кожного [2].

Переваги МСМ:

- значне підвищення інформативності трафіку всередині підприємства;

- скорочення експлуатаційних витрат за рахунок використання єдиної інфраструктури;

- підвищення продуктивності праці - впровадження нових засобів управління роботою на основі уніфікованих комунікацій;

- скорочення витрат на міжміський телефонний зв'язок, оренду каналів зв'язку, модернізацію обладнання традиційного телефонного зв'язку;

- збільшення конкурентоспроможності організації - надання гнучких можливостей щодо впровадження нових затребуваних сервісів [3];

- надання сучасних високошвидкісних сервісів;

- масштабованість;

- керування трафіком;

- резервування смуги пропускання;

- функції безпеки можуть бути інтегровані в інфраструктуру мережі на всіх рівнях;

- дотримання умов договорів про рівень обслуговування;

- захист, який не впливає на швидкодію мережі в цілому;

- здатність швидко ідентифікувати, класифікувати і відстежувати аномальну поведінку в мережі;

- здатність поширювати контрзаходи на велику кількість вузлів мережі [4].

Залежно від структури територіального розташування організації, МСМ може бути:

- локальна - організація розміщується в одному або декількох досить близько розташованих будівлях і володіє власною мережевою інфраструктурою, яка зв'язує всі структурні підрозділи;

- розподілена - організація має головний офіс і мережу філій, розташованих на значній відстані один від одного, та з'єднуються через мережі та ресурси операторів зв'язку [5].

1.2 Конвергенція мультисервісних мереж

Процес конвергенції став можливим в результаті, з одного боку, технологічного прогресу і, з іншого боку, нових вимог, що пред'являються споживачами послуг.

Конвергенція мереж означає зближення або об'єднання різних мережевих технологій для створення можливостей надати користувачам різнорідні послуги. У результаті цього процесу ми спостерігаємо, наприклад, зникнення відмінностей між телефонними мережами та мережами передачі даних, або між мережами загального користування та корпоративними мережами.

Мультимедіа в МСМ надає інтеграцію декількох інформаційних типів повідомлень, таких як текст, зображення, графіка, анімація і багато іншого.

Сьогодні з багатьох напрямків йде конвергенція різних видів телекомунікаційних мереж [6].

Робимо висновок, що МСМ нового покоління не може бути створена в результаті «перемоги» якої-небудь однієї технології або підходу. Її може породити тільки процес конвергенції, коли від кожної технології буде взято все найкраще і пов'язане в певну нову структуру, яка і дасть необхідну якість для підтримки існуючих та створення нових послуг [7].

1.3 Послуги, які реалізовують мультисервісні мережі

МСМ дозволяє надавати дуже широкий набір послуг і забезпечує гнучкі можливості по їх створенню, управлінню і персоналізації. Ці ж мережі дозволяють автоматизувати отримання інформації з будь-якої кількості датчиків і лічильників, встановлених у квартирах і будинках, до них підключаються системи охоронної сигналізації та контролю.

Проаналізовано нові можливості, які легко реалізуються на базі МСМ поверх стандартних сервісів:

- підключення систем безпеки, відеоспостереження та сигналізації до мережі з виводом в диспетчерські пункти;

- швидка передача великих обсягів графічних, відео-, аудіо-та текстових файлів, потокового відео, аудіоконтенту;

- теленавчання;

- створення в рамках мережі виділених віртуальних мереж з розширенням їх можливостей за рахунок підключення мультимедійних і телевізійних ресурсів;

- диспетчеризація інженерної та іншої інфраструктури підприємств, включаючи підключення систем пожежної безпеки, лічильників енергії, води і тепла, систем контролю та ідентифікації [8].

МСМ підтримують такі види послуг, як телефонний і факсимільний зв'язок; виділені цифрові канали з постійною швидкістю передачі; пакетна передача даних з необхідною якістю сервісу; створення віртуальних корпоративних мереж, комутованих і керованих користувачем [9].

1.4 Архітектура структури мультисервісної мережі

Архітектурно структуру МСМ можна представити у вигляді декількох основних рівнів: рівень послуг, рівень доступу, транспортний рівень.

Рівень послуг визначає склад інформаційного наповнення мережі. Рівень доступу забезпечує доступ користувачів до ресурсів мережі. Транспортний рівень представляє собою основний ресурс мережі, що забезпечує передачу інформації від одного користувача до іншого користувача [10].

Існує безліч методів, алгоритмів, способів, і так само протоколів, що описують і реалізують різні функціональні принципи обміну даними в МСМ. До недавнього часу процеси обробки і передачі даних в МСМ описувалися за допомогою еталонної моделі взаємодії відкритих систем.

Заміна відомих принципів передачі даних в TCP / IP мережах технологіями і протоколами МСМ трансформує семирівневу модель взаємодії відкритих систем в нову трирівневу модель , що представлена на рисунку 1.1.

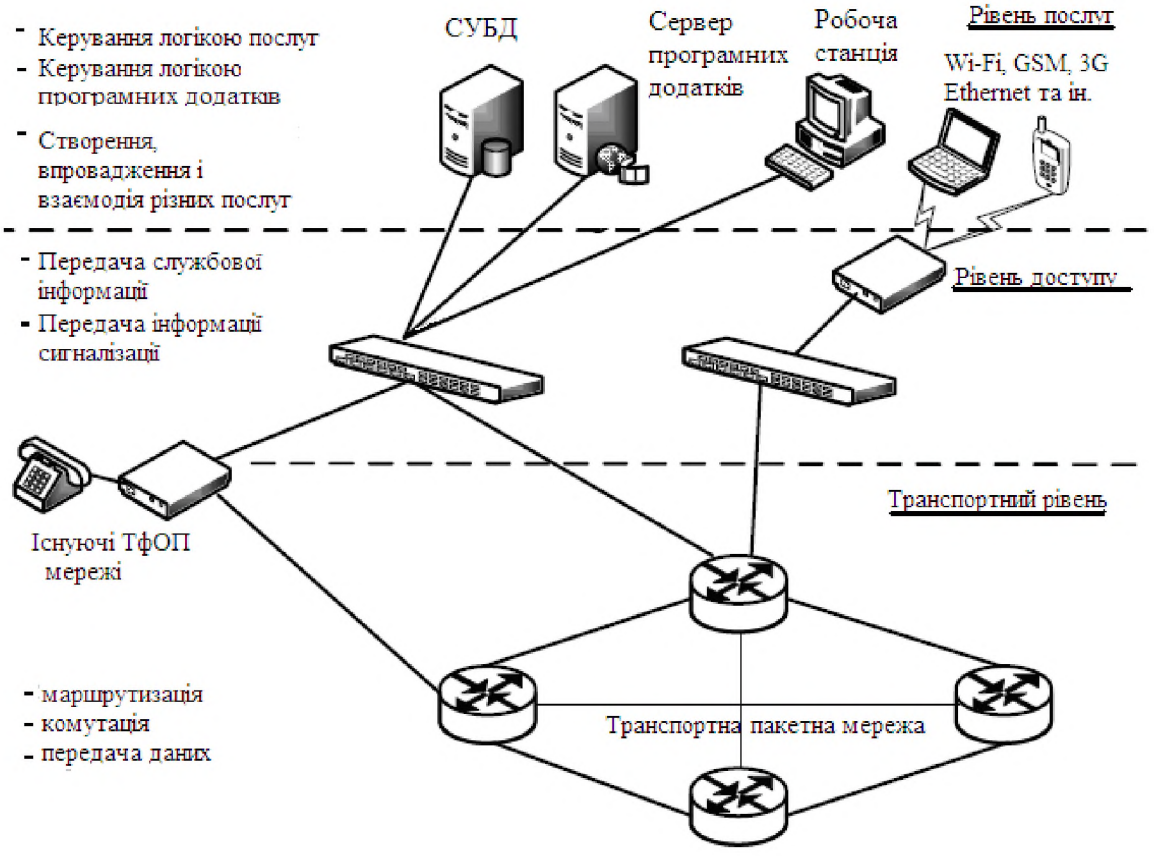

Рисунок 1.1 - Узагальнена схема побудови мережі МСМ

Протоколи керування МСМ:

Протокол H.323. Забезпечує основу для передачі даних, відео та аудіо інформації через IP мережі, включаючи Internet.

Session Initiation Protocol (SIP). Це протокол прикладного рівня, за допомогою якого здійснюються такі операції, як встановлення, модифікація і завершення мультимедійних сесій або викликів по IP-мережі. Сесії SIP можуть включати мультимедійні конференції, дистанційне навчання, Internet-телефонію і інші подібні програми.

Media Gateway Control Protocol (MGCP). Протокол MGCP використовується для управління шлюзами MG. Він розроблений для архітектури, в якій вся логіка обробки викликів розташовується поза шлюзів, і управління виконується зовнішніми пристроями, такими, як MGC або агенти викликів.

MEGACO/H.248. Протокол Media Gateway Control Protocol (MEGACO) повинен замінити MGCP в якості стандарту для управління шлюзами MG. MEGACO служить загальною платформою для шлюзів, пристроїв управління багато точковими з'єднаннями і пристроїв інтерактивної голосової відповіді.

Модель з'єднань, використовувана MEGACO, концептуально більш проста, ніж для протоколу MGCP. MEGACO розглядає шлюзи MG як набір кінцевих пристроїв, які можуть бути співвіднесені один з одним усередині певного контексту. Кінцевий пристрій є джерелом або приймачем медіа-потоків. Як і в MGCP, кінцеві пристрої можуть бути або фізичними, або віртуальними. З'єднання реалізується, коли один кінцевий пристрій поміщається в контекст іншого. Наприклад, переадресація виклику виконується за допомогою переміщення кінцевого пристрою з одного контексту в інший, а відеоконференція буде ініціалізована розміщенням декількох кінцевих пристроїв в загальному контексті.

Протокол Signaling Transport. Цей протокол являє собою набір протоколів для передачі сигнальної інформації по IP-мережі [11].

1.5 Порівняльна характеристика комп'ютерних та мультисервісних мереж

Загрози різного походження в комп'ютерних мережах та в мережах передавання даних усім добре відомі. Більшість організацій витрачають великі кошти та багато часу, захищаючи конфіденційність, цілісність та доступність своїх комп'ютерних інформаційних ресурсів. Проте, аналогічні загрози властиві телекомунікаційним мережам, до яких і відносяться МСМ.

Нехтування тим фактом, що можливий несанкціонований доступ (НСД) і виток конфіденційної інформації у МСМ зв'язку є основою успішних дій зловмисників (викрадення конфіденційної інформації, збитки через оплату чужих міжнародних переговорів, зниження професійної репутації компанії, фінансові втрати, які пов'язані із дефектами в роботі системи зв'язку тощо).

До сьогодні ймовірність виявлення та покарання таких злочинів дуже мала, саме відсутність серйозної статистики свідчить лише про складність виявлення та розслідування злочинів у цій сфері.

Задача знаходиться на перетині двох галузей – телефонії та ІБ. ІБ потребує розроблення нових методів та моделей – вона виникла на базі інформаційних технологій, що активно інтегруються в галузь телефонії. Своєю чергою, розвиток та інтеграція ІТ-рішень призводить до появи нових видів загроз та вразливостей, що потребують застосування нових рішень щодо захисту чи комплексного застосування вже відомих та перевірених.

Схожість МСМ та комп'ютерних систем представлена в таблиці 1.1:

- індивідуальна адресація абонентів (в комп'ютерних системах – мережеві адреса, а в телефонії – телефонний номер мережі);
- великі обсяги передачі інформації;
- наявність каналів з'єднання з телефонною мережею загального користування та глобальною мережею Internet;
- цифрові методи оброблення інформації;
- використання відкритих стандартизованих протоколів взаємодії;
- децентралізоване управління;

- стратегічна важливість безперебійної, високонадійної роботи мережі, дозволяє все вищесказане відносно проблем інформаційної безпеки комп'ютерних систем спроектувати й на сучасні системи телекомунікацій, що побудовані на комп'ютерних платформах.

Але відмінності телекомунікаційних та комп'ютерних систем вимагають індивідуального підходу по захисту МСМ [12].

Таблиця 1.1 – Порівняльна характеристика мультисервісних атак комп'ютерних мереж

Характеристика	Мультисервісні мережі	Комп'ютерні мережі
Особливості	МСМ – це універсальне середовище, призначене для передачі мови, зображення та ін послуг.	КМ - сукупність комп'ютерів, з'єднаних за допомогою каналів зв'язку і засобів комутації в єдину систему для обміну повідомленнями і доступу користувачів.
Основна задача	Забезпечення роботи різнорідних інформаційні та телекомунікаційних систем та програм в єдиному транспортному середовищі.	Надання можливості окремим співробітникам організації взаємодіяти один з одним і звертатися до спільно використовуваних ресурсів.
Переваги	а) масштабування МС; б) скорочення витрат за рахунок використання єдиної інфраструктури;	а) можливість спільного використання периферійних пристроїв;

Продовження таблиці 1.1

Характеристика	Мультисервісні мережі	Комп'ютерні мережі
	г) швидка передача великих обсягів графічних, відео-, аудіо-та текстових файлів, потокового відео, аудіо контенту; д) забезпечення гарантованої якості обслуговування (QoS) користувачів; е) централізоване управління мережею.	б) підвищення ефективності та швидкості обробки інформації в групі співробітників; в) забезпечення спільного доступу до Internet; г) швидке отримання доступу до корпоративних сховищ інформації (бази даних).

1.6 Проблеми захисту інформації мультисервісних мереж

Крім проблем впровадження МСМ існують проблеми переходу до мережі нового покоління. Складність створення мереж нового покоління полягає в тому, що мережі фіксованого, мобільного зв'язку та Internet побудовані за різними стандартами і використовують індивідуальне програмне забезпечення, що гальмує розвиток ринку послуг. Потрібно об'єднати існуючі мережі різних операторів (традиційні мережі, мережі мобільного зв'язку та IP-мережі) в єдину мережу [13].

Разом з тим в МСМ значною проблемою є інформаційна безпека мережі. Донедавна основні зусилля постачальників рішень інформаційної безпеки були зосереджені на захисті інфраструктури: класичні міжмережні екрани, системи виявлення й запобігання вторгнень, так і більш пізні мережні антивірусні системи в першу чергу забезпечували безпечний периметр, захищаючи "ніжні внутрішності" корпоративних мереж від впливу з зовнішніх мереж.

Технології захисту інформаційної інфраструктури сьогодні забезпечують досить високу стійкість до зовнішніх несанкціонованих впливів. Однак це вірно тільки у випадку грамотної побудови системи захисту і її адекватної експлуатації.

Одна з важливих проблем при спробах створити систему захисту сучасної МСМ це фактори, що пов'язані із закритістю більшості сучасних інформаційних систем і з експонентним ростом числа виявлених можливих вторгнень в мережу, однак найбільшу складність представляють проблеми, що випливають із основних тенденцій мережного розвитку.

Наступна проблема це масштабність – найбільш помітна тенденція. Економія на безпеці під час росту ставить під удар самі вразливі вузли мережі. Підтвердженням проблем з ростом служить відсутність масової пропозиції на ринку IP-телефонів з підтримкою шифрування. Дорожнеча, труднощі розгортання й експлуатації систем захисту офісної IP-телефонії затримують масові інсталяції, незважаючи на те, що відповідні технології шифрування трафіка прекрасно себе зарекомендували. У той же час, якщо запитати співробітника служби інформаційної безпеки про потенційні шляхи витоку конфіденційної та комерційної інформації – телефонія буде названа в числі перших. Проблеми масштабності у першу чергу актуальні (отже, вимагають витрат) для мереж, у яких необхідно забезпечувати конфіденційність і цілісність переданої інформації. Згідно діючого законодавства для цих цілей варто використати засоби шифрування, побудовані на нормативних алгоритмах.

Переважна більшість платформ, що реалізують цей механізм, сьогодні являють собою апаратно-програмні або чисто програмні комплекси. Подібні рішення не містять спеціалізованих мікросхем, що прискорюють шифрування трафіка в достатній мірі, щоб закрити одним пристроєм гігабітний канал, а в сучасних мережах уже не рідкість канали із продуктивністю 10 Гбіт/с і більше.

Наступна особливість вітчизняних реалізацій криптографічних засобів – відсутність єдиного набору стандартів на протоколи захищеного обміну даними. Відсутність єдиних стандартів приводить до складності, а іноді просто до неможливості інтеграції систем безпеки мереж, що використають різні вітчизняні засоби забезпечення інформаційної безпеки.

Основні фактори, що впливають на безперервність надання послуг МСМ при впровадженні в ній засобів забезпечення ІБ: додатковий час переходу на резервний пристрій при відмові основного у випадку зміни мережної топології; необхідність у додатковій системі керування засобами забезпечення інформаційної безпеки і в постійному підвищенні кваліфікації персоналу; труднощі поділу трафіка на “корисний” і “шкідливий” в одному потоці даних традиційними засобами [14].

1.7 Загрози персоналу мультисервісної мережі

Загроза ІБ з боку персоналу МСМ має високий пріоритет. Тому робота з персоналом МСМ є одним з основних елементів системи безпеки. Цілеспрямований або випадковий вплив на персонал, що має адміністративні повноваження в системі, може призвести до виникнення суттєвих ризиків.

а) Вмведення в оману. Це основний «компонент» роботи зловмисника з персоналом, який шляхом обману отримує необхідну для своїх дій інформацію. Існує багато прийомів: видача себе за іншу особу, відволікання уваги, нагнітання психологічної напруги і т.д. Інформація, отримана в результаті таких дій зловмисника, необхідна йому для:

- планування несанкціонованого доступу (НСД) до конфіденційної і комерційної інформації;
- маскування несанкціонованих дій під легальні;
- відхід від відповідальності шляхом переведення підозр на іншу особу.

Більш кваліфіковані зловмисники можуть вдатися до обриву ланцюжка вузлів траси. Вони домагаються цього за рахунок знищення та втрати записів у відповідних журналах про проходження пакетів зловмисника в одному з вузлів

магістральної мережі. Кінцевою метою атаки зловмисника може бути інформація:

- про стан рахунку для її модифікації;
- інформація використовувана для ідентифікації, аутентифікації та авторизації доступу, для розкрадання грошових коштів;
- для одержання матеріальних цінностей у вигляді консультацій програмних продуктів, замовних досліджень;
- конфіденційна та комерційна інформація (наприклад, фінансові відомості; списки клієнтів контакти та плани; інформація про маркетинг; договори, пропозиції, квоти; науково-дослідні проекти; конструкторські розробки з виробництва продукції та її технічні параметри; дизайн, ефективність і можливості виробничих методів).

Найбільш ймовірна схема отримання пароля або повного UID (ім'я і користувач) - це дзвінки від імені адміністратора користувачеві (наприклад, проведення роз'яснювальної бесіди і пропозиція змінити пароль у рамках регламентних процедур) або від імені користувача адміністратора з проханням допомогти відновити забутий пароль.

б) Атака на адміністратора системи. У разі, коли пароль роздобути не вдається, і немає можливості підібрати UID, зловмисникові залишається атака на технічні засоби. Для цього йому необхідно локалізувати «діру» в мережевій обороні. При правильно сконфігурованій системі це не тривіальне завдання, що вимагає мережевої розвідки, та загрожує викриттям зловмисника на ранніх стадіях підготовки атаки.

Один з нехитрих способів пробивання «дірок» використовує метод психологічного тиску. Адміністратору по телефону повідомляється про підготовану або про вже виконану атаку. Ніяких деталей, не повідомляється, але вказується передбачуване місцезнаходження загрози. З деякою часткою ймовірності адміністратор спробує підвищити рівень безпеки своєї системи.

Спонтанність його дій і неготовність проаналізувати наслідки незбалансованих дій може призвести до кількох помилок, які спростять атаку.

в) відхід від відповідальності. Найголовніше завдання зловмисника - це не атака на мережу, а замітання слідів, так як загроза бути спійманим, всі його зусилля зводить до нуля.

1.8 Людський фактор і проблеми авторизації в мультисервісній мережі

Зокрема, користувачі не люблять вибирати довгі паролі. Деякі характеристики паролів контролюються системою і «слабкі» паролі не пропускаються. Людська психологія може зіграти в системі безпеки злий жарт при встановленні невірної політики формування UID. Цілком очевидно, що якщо система буде вимагати від користувача не тільки довгий, але і безглуздий пароль, то користувач точно повісить пароль на монітор. Або ще гірше запише його у файл.

а) запит, який вибирається зі спеціального списку за випадковим законом, конфіденційної інформації, відомої тільки тому хто авторизується (наприклад, його переваги або відомості про родичів і друзів: день народження, смаки, характер і т.п).

б) електронні ключі. Всі вони широко застосовуються для зберігання особистих, періодично змінюваних ключів шифрування, інформація про стан особового рахунку або інформації про дозволеня часу проходу в пропускних системах.

в) біометричні параметри людини, вимірювані і оцифровані спеціальними пристроями (сканери відбитків пальців або райдужної оболонки ока, розпізнавачі мови і т.п).

І ці заходи безпеки можуть бути обійдені зловмисниками, але ціна такого рішення зростає в міру зростання числа ліній, що формують ешелони оборони, і сценаріїв розмежування доступу.

В результаті вищевикладеного можна зробити висновок, що оператором МСМ необхідно мати програму навчання своїх співробітників. Така навчальна

програма щодо забезпечення ІБ повинна бути розділена на кілька частин, орієнтованих на: рядових співробітників; адміністраторів та персонал, що відповідають за ІБ підсистем; керівників середньої ланки; вище керівництво з урахуванням специфіки розв'язуваних завдань.

Крім усього іншого навчання це має бути обов'язковим для всіх нових співробітників, прийнятих на роботу, і повинні розглядатися всі аспекти функціональних обов'язків службовця. Необхідно періодично перевіряти, ефективність навчання та готовність службовців до виконання дій, пов'язаних із забезпеченням ІБ, регулярно проводити для всього персоналу заняття з підвищення кваліфікації, що розповідають про нові зміни в стратегії і процедурах безпеки, а також вжити заходів після зафіксованих серйозних інцидентів.

1.9 Види НСД персоналу, що складає загрозу ІБ в мультисервісних мережах

Аналіз нештатних ситуацій в МСМ, що виникають в результаті злочинних дій, можна згрупувати в ряд типових сценаріїв:

а) обдурювання з даними. Один з найпоширеніших методів при вчиненні злочинів у галузі інформаційних технологій, так як не вимагає технічних знань і відносно безпечний. Інформація змінюється в процесі її введення в систему або під час її виведення. Наприклад, при введенні мовного з'єднання в точці розгалуження множинного сценарію з'єднання, активується дозволений доступ до непередбачуваної послуги або документи можуть бути замінені фальшивими.

б) сканування. Кваліфікований зловмисник легко може переглядати залишкову інформацію, що залишилася на персональному комп'ютері (ПК) або на носії інформації після виконання співробітником завдання і видалення своїх файлів. Справа в тому, що видалення проводиться тільки зі змісту, інформація про ланцюжок кластерів вилученого файлу зберігається для використання звільненого дискового простору іншим файлом або до дефрагментації дисків.

При цьому не завжди потрібне введення UID для входу терміналу в мережу, тому що інформація, розташована локально, може бути прочитана в багатьох конфігураціях ОС користувачів ПК в обхід паролювання.

в) чорних хід. Цей метод заснований на використанні адміністраторами або розробниками прихованого програмного або апаратного механізму, що дозволяє обійти методи захисту в системі. Іноді пишеться і впроваджується спеціальна програма, що працює таким чином, коли спрацьовує специфічна подія, наприклад, число транзакцій, оброблених в певний день, викличе запуск неавторизованого механізму і відкриє шляхи для НСД.

г) супер відключення. Технологія названа від імені програми, що використовувалася в ряді комп'ютерних центрів, обходячи системні заходи захисту і використовувалася при аварійних ситуаціях. Володіння таким «майстер ключем» дає можливість у будь-який час отримати НСД до ресурсів. Саме тому в структурі оператора МСМ не може бути єдина і централізована структура адміністрування мережевих та інформаційних ресурсів.

1.10 Класифікація віддалених атак на розподілені системи мультисервісних мереж

Основна ціль будь-якої класифікації полягає в тому, щоб запропонувати такі класифікаційні ознаки, використовуючи які можна найбільш точно описати класифіковані явища чи об'єкти. Для опису віддалених атак пропонується класифікація за такими ознаками:

- за характером впливу - пасивний, який практично неможливо виявити, тому що він не надає безпосередній вплив на роботу системи та її політику безпеки, що призводить до змін у системі, які можуть бути виявлені.

- по цілі впливу - порушення конфіденційності інформації або ресурсів системи, наприклад, перехоплення інформації в результаті прослуховування без можливості її модифікації. Порушення цілісності інформації потоком або передачі повідомлень від імені іншого об'єкта, наприклад, створення «помилкового об'єкта» в МСМ. Порушення працездатності або доступності

системи, при якій виводиться з ладу система на атакуємому об'єкті і для всіх інших об'єктів системи доступ до ресурсів атакованого об'єкта стає неможливий, наприклад, «Відмова в обслуговуванні» або DoS-атака.

- за умовою початку здійснення впливу. Атака по запиту від атакує мого об'єкту, коли атакуючий очікує передачу від потенційної цілі атаки запиту певного типу, який і буде умовою початку здійснення впливу. Атака по настанню очікуваної події на атакуємому об'єкті, коли атакуючий здійснює постійне спостереження за станом ОС віддаленої цілі атаки і при виникненні певної події в цій системі починається вплив. Безумовна атака, коли початок здійснення атаки безумовно стосовно цілі атаки, тобто атака здійснюється негайно і безвідносно до стану системи і атакуємого об'єкту.

- по наявності зворотнього зв'язку з атакуємим об'єктом. Зворотній зв'язок, характеризується тим, що на деякі запити, які передані на атакуємий об'єкт, атакуючому потрібно отримати відповідь, і отже, між атакуючим і цілю атаки існує зворотній зв'язок, який дозволяє атакуючому адекватно реагувати на всі зміни, що відбуваються на атакуємому об'єкті. Без зворотнього зв'язку (однонаправлена атака), коли не потрібно реагувати на будь-які зміни, що відбуваються на атакуємому об'єкті, характерний приклад такої атаки «Відмова в обслуговуванні».

- по розташуванню суб'єкту атаки щодо атакуємого об'єкту. Внутрішньосегментна атака, коли суб'єкт і об'єкт атаки знаходиться в одному мережевому сегменті. Міжсегментна, коли об'єкт мережі і безпосередньо атакуючий можуть знаходиться на відстані багатьох тисяч кілометрів один від одного, в різних мережах, що може істотно перешкоджати заходам з відбиття атаки.

Отже розглянемо порівняльну характеристику механізмів реалізації мережевих атак МСМ яка представлена на рисунку 1.2.

Рисунок 1.2 - Характеристика механізмів реалізації мережевих атак МСМ

1.11 Характеристика найбільш поширених способів реалізації загроз інформації, оброблюваної в мультисервісній мережі

Цілеспрямованій атаці завжди передує розвідка або аналіз вразливих місць мережі.

1) Аналіз мережевого трафіку. Атака дозволяє вивчити логіку роботи. Вдається отримати взаємно однозначну відповідність подій, що відбуваються в системі, і команд, що пересилаються один одному її об'єктами, у момент появи цих подій. Це досягається шляхом перехоплення та аналізу пакетів обміну на канальному рівні. Знання логіки роботи розподіленої інформаційної системи дозволяє на практиці моделювати і здійснювати віддалені атаки. Атака даного типу полягає в отриманні на віддаленому об'єкті НСД до інформації, якою обмінюються два мережних абонента. При цьому відсутня можливість модифікації трафіку і сам аналіз можливий тільки всередині одного сегменту мережі.

Прикладом перехопленої за допомогою даної типової віддаленої атаки інформації можуть служити:

- ім'я та пароль користувача, пересилається в незашифрованому вигляді по мережі;

- шифрований інформаційний потік для збереження на ПК зловмисника і подальшого дешифрування;

- «підслуховування» чужих аудіо-або відео потоків, відеоконференцій при недостатньому опрацюванні захисту від шахрайства цих послуг. За характером впливу аналіз мережевого трафіку є пасивним впливом. Здійснення даної атаки без зворотного зв'язку веде до порушення конфіденційності інформації всередині одного сегмента на канальному рівні мережевий моделі OSI. При цьому початок здійснення атаки, безумовно, стосовно мети атаки [15].

2) Несанкціонований доступ. Це найбільш поширений спосіб реалізації загроз інформації в МСМ. Він полягає в отриманні користувачем такого виду доступу до об'єкта, на якого у нього немає дозволу відповідно до прийнятої в організації політики безпеки.

Методика реалізації НСД в значній мірі залежить від організації обробки інформації в МСМ, прийнятої політики безпеки, можливостей використовуваних засобів захисту, а також сумлінності адміністраторів і користувачів. У переважній більшості випадків НСД стає можливим через непродуманий вибір засобів захисту, їх некоректної установки і настройки, контролю їх функціонування, а також при недбалому відношенні до захисту своїх власних даних.

За характером впливу НСД є активним впливом, який використовує будь-яку помилку в системі. НСД відноситься безпосередньо до необхідного інформаційного об'єкта, або впливає на інформацію при санкціонованому доступі з метою легалізації НСД. НСД може бути здійснений як стандартними, так і спеціально розробленими програмними засобами та застосовуватись до інформаційних об'єктів в будь-якому стані.

3) Незаконне використання привілеїв. Практично будь-яка захищена система містить засоби, що використовуються в надзвичайних ситуаціях, або засоби, які здатні функціонувати з порушенням існуючої політики безпеки. У деяких випадках користувач повинен мати можливість доступу до всіх наборів

даних системи (наприклад, при необхідності виконання резервного копіювання). Такі засоби необхідні, але вони можуть бути надзвичайно небезпечними. Зазвичай ці засоби використовуються адміністраторами, операторами, системними програмістами та іншими користувачами, що виконують спеціальні функції.

Для того, щоб зменшити ризик від застосування таких засобів, більшість систем захисту реалізує зазначені функції з використанням спеціальних атрибутів доступу (привілеїв) - для виконання певної функції потрібна певна привілея. У цьому випадку кожен користувач отримує свій набір привілеїв, рядові співробітники - мінімальний, адміністратори безпеки мережі - максимальний.

Таким чином, незаконне захоплення і використання привілеїв можуть призвести до можливості несанкціонованого виконання певної функції. Це може бути НСД (окремий випадок), запуск певних програм і навіть реконфігурація системи. Незаконне захоплення і використання привілеїв можливе або за наявності помилок у самій системі захисту або в випадку недбалості при управлінні системою і привілеями зокрема (наприклад, при призначенні розширеного набору привілеїв всім користувачам).

Порушення шляхом незаконного використання привілеїв, є активним впливом, що використовує будь-яку помилку, вчиненим з метою доступу до якого-небудь пасивного об'єкту, процесу чи системи в цілому.

4) Атаки «Salami». Принцип цих атак побудований на тому факті, що при обробці даних про стан рахунків використовуються цілі одиниці (центи, рублі, копійки), а при обчисленні відсотків нерідко виходять дробові суми, різниця між реальною та округленою сумою надходитимуть на відкритий рахунок зловмисника або зондування системи та підбір паролів проводитимуться з різних місць і з випадковими досить протяжними, паузами між спробами.

Технологія маскує дії зловмисника під звичайні помилки абонентів при виконанні алгоритмів доступу до того чи іншого мережевого інформаційного ресурсу.

Причинами цих атак є, по-перше, похибки обчислень, що дозволяють трактувати правила округлення в ту чи іншу сторону, а по-друге, величезні обсяги обчислень, необхідні для обробки даних про стан рахунків.

Атака «Salami» - активний вплив, з опосередкованим впливом на об'єкт атаки, використовує помилки, допущені на етапі реалізації системи, спеціально розробленого програмного забезпечення.

5) Використання "Прихованих каналів". Даний спосіб отримання інформації за рахунок використання коштів передачі або обробки інформації, існуючих в МСМ, але не керованих КСЗ, або спостереження за існуючими потоками інформації. Наприклад, в МСМ з реалізованим розмежуванням доступу до інформації користувача, який не маючи прав на отримання даних, що його цікавлять, може використовувати для цього обхідні шляхи. Практично будь-яка дія в системі якимось чином зачіпає інші її елементи, які при цьому можуть змінювати свій стан. При знанні цих зв'язків можна хоча б частково відновити першопричину події.

Атаки з використанням прихованих каналів за характером впливу є пасивними: порушення полягає тільки в доступі до переданої або оброблюваної інформації.

Для організації "прихованих каналів" може використовуватися як штатне програмне забезпечення, так і спеціально розроблені програми. Атака зазвичай проводиться програмним засобом.

6) Атака заміни легального користувача нелегальним. Під цією атакою розуміється виконання яких-небудь дій одним користувачем МСМ від імені іншого користувача. При цьому такі дії іншому користувачеві можуть бути дозволені. Порушення полягає у привласненні прав і привілеїв.

Мета заміни легального користувача нелегальним - приховання яких-небудь дій за ім'ям іншого користувача або привласнення прав і привілеїв іншого користувача для доступу до його набору даних або використання його привілеїв.

Прикладом атаки може служити вхід в систему під ім'ям і паролем іншого користувача, при цьому система не зможе розпізнати порушення. У цьому випадку атаки зазвичай передує злом системи або перехоплення пароля.

Інший приклад цієї атаки - присвоєння ідентифікатора іншого користувача в процесі роботи. Це може бути зроблено за допомогою засобів операційної системи (деякі операційні системи дозволяють змінювати код користувача в процесі роботи) або за допомогою програми, яка в певному місці може змінити певні дані, в результаті чого користувач отримає інший ідентифікатор. У цьому випадку "маскараду" може передувати захоплення привілеїв, або він може бути здійсненим з використанням будь-якої помилки в системі.

Атака заміни легального користувача нелегальним - це спосіб активного порушення безпеки системи, він є опосередкованим впливом, тобто впливом, вчиненим з використанням можливостей інших користувачів.

7) Атака типу "Збір сміття". Атака, яка полягає в захопленні і аналізі користувачем або процесом спільно використовуваних ресурсів, звільнених іншим користувачем або процесом, з метою отримання інформації. Після закінчення роботи оброблювана інформація не завжди повністю видаляється з пам'яті. Частина даних може залишатися в оперативній пам'яті, на дисках та інших носіях. Дані зберігаються на носії до перезапису або знищення, при виконанні цих дій на звільненому просторі диска знаходяться їхні залишки. Хоча при спотворенні заголовка файлу їх прочитати важко, однак, використовуючи спеціальні програми і обладнання, все ж можливо. Такий процес прийнято називати "збором сміття". Він може привести до розкриття важливої інформації.

"Збір сміття" – активна атака, безпосередній вплив на об'єкти МСМ при їх зберіганні з використанням доступу.

8) Атака "Злам системи". Умисне проникнення в систему (успішне подолання механізмів захисту системи) з несанкціонованими параметрами входу, тобто псевдонімом користувача і його паролем (паролями) або іншими атрибутами входу.

"Злам системи" - умисний, активний вплив на систему в цілому. Можливість зламу може бути обумовлена помилками адміністративного управління; помилками, які допущені на етапі проектування; помилки, що були допущені на етапі реалізації.

"Злам системи" зазвичай відбувається в інтерактивному режимі. Як правило, "злам системи" здійснюється шляхом підбору або перехоплення атрибутів входу користувачів в систему (паролів і інших даних аутентифікації).

9) використання шкідливих програм. Під шкідливими програмами надалі будемо розуміти такі програми, які прямо або побічно дезорганізують процес обробки інформації або сприяють розкриттю чи спотворенню інформації. Нижче розглянуто деякі (найпоширеніші) види подібних програм: "троянський кінь", комп'ютерний вірус, "жадібна" програма.

"Троянський кінь" - програма, яка, будучи авторизованим процесом, крім виконання документованих функцій, здатна здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми. За характером впливу використання програм типу "троянський кінь" відноситься до активних атак, реалізована спеціально розробленими програмними засобами, працюючими в пакетному режимі. Ця атака може бути спрямована проти будь-якого об'єкта МСМ, як шляхом безпосереднього, так і опосередкованого впливу. Найбільш небезпечним є опосередкований вплив, при якому програма "Троянський кінь" діє в рамках повноважень одного користувача, але в інтересах іншого користувача, встановити якого часом неможливо.

Комп'ютерний вірус - програма, що володіє здатністю до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування МСМ та / або викликати порушення політики безпеки. Як і програми типу "троянський кінь", комп'ютерні віруси відносяться до активних, спеціально розроблених програмних засобів. Вони можуть загрожувати будь-якому об'єкту МСМ, як шляхом безпосереднього, так і опосередкованого впливу.

"Жадібні" програми - це програми, які в процесі свого виконання прагнуть монополізувати (або вивести з ладу) який-небудь ресурс системи, не даючи іншим програмам можливості використовувати його. Природно, атака з використанням таких програм є активним втручанням в роботу системи. Безпосередньо цій атаці зазвичай піддаються такі об'єкти системи як: процесор, оперативна пам'ять, пристрої введення-виведення.

10) Підміна даних. Атака, яка веде до нав'язування помилкових даних, результатом чого є порушення цілісності та достовірності оброблюваної в МСМ інформації. За характером впливу на МСМ - активний вплив; унаслідок появи використовуваної уразливості в МСМ - помилки адміністративного управління; помилки, допущені на етапі проектування; помилки, допущені на етапі реалізації; за способом впливу на об'єкт атаки – з безпосереднім впливом на об'єкт атаки; по використовуваним засобам атаки – стандартне програмне забезпечення; спеціальне розроблене програмне забезпечення; за станом об'єкту атаки - об'єкт атаки, що знаходиться в стані зберігання; об'єкт атаки, що знаходиться в стані передачі.

11) Нав'язування хибного маршруту. Атака, яка веде до такої зміни маршруту передачі повідомлень в МСМ, в результаті якого стає можливим несанкціонований доступ до інформації. За характером впливу на МСМ - активний вплив; унаслідок появи використовуваної уразливості в МСМ - неадекватність реалізованої політики безпеки реальної МСМ; помилки адміністративного управління; помилки, допущені на етапі проектування; помилки, допущені на етапі реалізації; за способом впливу на об'єкт атаки - з

опосередкованим впливом; по використовуваним засобам атаки – стандартне програмне забезпечення та обладнання, спеціально розроблене програмне забезпечення і обладнання; за станом об'єкта атаки - об'єкт атаки, що знаходиться в стані передачі.

12) Перехоплення повідомлень. Спосіб несанкціонованого отримання інформації шляхом доступу до неї в транзитних вузлах МСМ. Перехоплення повідомлень - пасивний вплив, що викликається неадекватністю реалізованої політики безпеки реальної МСМ або помилками на етапі проектування / реалізації системи, за способом впливу - з безпосереднім впливом на об'єкт атаки, з використанням стандартного або спеціально розробленого програмного забезпечення, за станом об'єкта атаки - з впливом на об'єкт атаки, що знаходиться в стані передачі.

1.12 Концепція захисту інформації в мультисервісних мережах

В даний час існує безліч факторів, в тій чи іншій мірі, які впливають на безпеку інформації в МСМ. Найбільш суттєвими з них є фактори, обумовлені складністю архітектури МСМ, різноманітністю і багатозадачністю її структурних і функціональних елементів.

Фактори, що впливають на безпеку МСМ:

1 МСМ є ергатичною (людино-машинною) системою. Даний фактор накладає ряд обмежень на процес проектування і впровадження захищених МСМ. Тому виникає необхідність обліку: вимог політики безпеки організації до персоналу і зовнішнім кореспондентам; ступеню важливості (секретності) циркулюючої в мережі інформації; рівні підготовленості осіб, які обслуговують програмне і апаратне забезпечення МСМ та ін.

2 МСМ є гетерогенними системами, що містять різні компоненти багато з яких самі є складними, багатофункціональними системами. Синтез таких компонентів в єдине ціле являє собою обгрунтований вибір і використання існуючих засобів захисту інформації (як програмних, так і апаратних) з урахуванням вимог якості обслуговування абонентів (QoS).

3 МСМ є багатозв'язними і великомасштабними системами, що охоплюють великі території, що інтегруються у світову систему телекомунікацій. Даний фактор має на увазі можливість проведення різних зловмисних атак і порушення безпеки МСМ на відстані, з використанням як програмних, так і апаратних засобів.

4 МСМ наукомісткі, базуються на перспективних технічних і програмних розробках, перебувають у безперервному розвитку. Облік цього чинника дозволить розробникам і особам, відповідальним за експлуатацію МСМ, постійно шукати шляхи розвитку і вдосконалення засобів захисту інформації

На рисунку 1.3 представлена схема засобів, систем і протоколів забезпечення послуг безпеки трирівневої моделі МСМ.

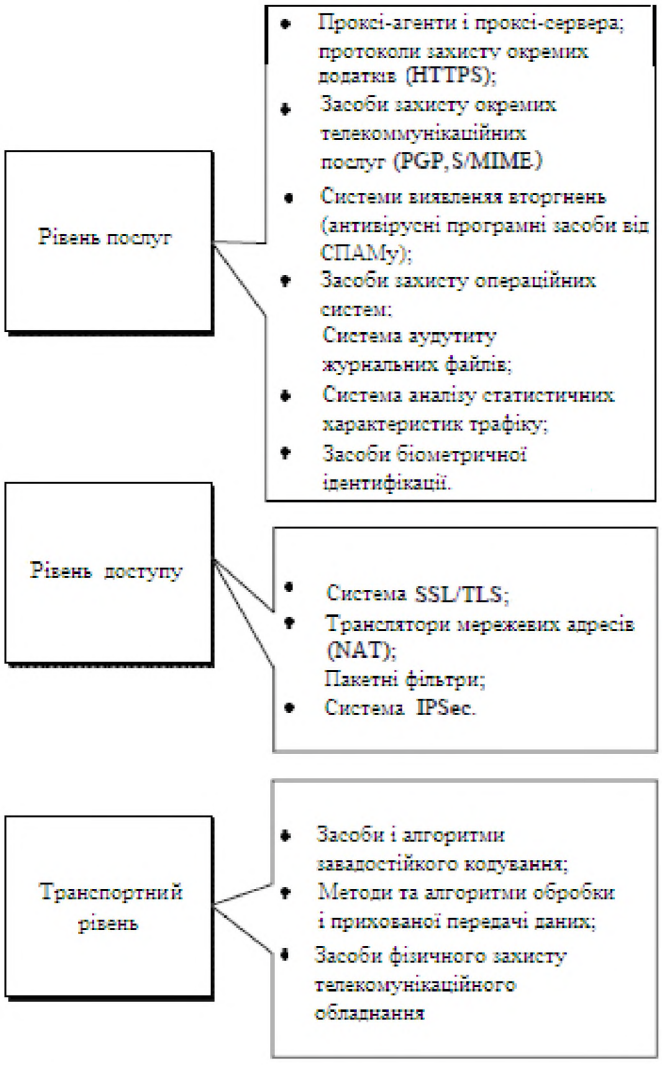

Рисунок 1.3 - Забезпечення послуг безпеки трирівневої моделі МСМ

Структурна схема засобів, систем і протоколів забезпечення послуг безпеки на кожному з рівнів трирівневої моделі МСМ має бути адаптивними.

Головне завдання аналізу захищеності мережі - це профілактика можливих мережевих атак і визначення заходів їх реалізацій. Це здійснюється на підставі пошуку вразливих місць у всій мережі, що складається з власне активного мережного обладнання, фізичних з'єднань, серверів інформаційних додатків і операційних систем. Проаналізовано [15, 17] і встановлено, що виявлення атак - це процес оцінки підозрілих дій в МСМ, який реалізується цілим комплексом дій за допомогою аналізу: log-файлів, мережевого трафіку і профілю абонента. Компоненти системи виявлення атак розміщуються на вузлах або в сегментах мережі, на її прикладних системах або системах зберігання. Система забезпечення безперервності бізнесу є допоміжною системою, яка крім виявлення реалізованих атак і відображення загроз повинна забезпечувати виявлення слідів скоєних атак і їх реєстрацію. Концепцією проектування подібних підсистем повинна стати можливість гарячого і холодного резервування апаратних ресурсів, інформаційних та програмних складових мереж. Керуючий компонент призначений для реалізації політик безпеки в частині автоматизованих засобів аналізу мережі, відбиття атак і відновлення прикладних систем. Адаптивне управління активно використовує тенденції розвитку методів запобігання і відбиття атак, пов'язаних з формуванням системи захисту.

Таким чином фактори, які впливають на безпеку показали, що захист інформації в МСМ є складною структурною і функціональним завданням. У той же час дослідження існуючих механізмів і протоколів захисту інформації показали наявність досить широкого спектру можливих варіантів їх використання при проектуванні МСМ. Саме тому основними напрямками концепції захисту інформації повинні стати: забезпечення основних показників якості послуг (в першу чергу показники безпеки) і основних послуг безпеки, адаптація систем захисту до динамічних змін, що відбуваються в мережі,

забезпечення безперервності функціонування програмних і апаратних засобів [16].

1.13 Завдання системи інформаційної безпеки мультисервісних мереж

Забезпечення захисту інформації в мультисервісних мережах вимагає виконання таких завдань: формування і поступове впровадження законодавчої та нормативно-правової бази технічного та криптографічного захисту інформації, гармонізованої з європейськими та міжнародними стандартами; розроблення сучасних методів захисту інформації для забезпечення комплексного захисту інформації в телекомунікаційних мережах; створення системи легального перехоплення інформації з телекомунікаційних мереж у випадках, передбачених законодавством України; створення державного координаційного центру з питань безпеки в інформаційно-телекомунікаційних мережах загального користування, сприяння створенню державних та недержавних центрів компетенції та реагування на інциденти в телекомунікаційних мережах.

Крім того, має забезпечуватись захист від несанкціонованого втручання в режимі функціонування обладнання мереж, а також вирішення проблеми «непрозорості» впроваджуваних в телекомунікаційних мережах іноземних технічних засобів, програмних продуктів і технологій.

Нові проблеми ІБ є порівняно складними і мають охоплювати декілька рівнів та сфер діяльності: мережне адміністрування, фізичну безпеку, моніторинг, програмне забезпечення телекомунікацій, інструменти забезпечення безпеки, аудит безпеки.

Одними з найбільш вразливих та незахищених елементів телекомунікаційних мереж є фізичні елементи – лінії, канали, засоби комутації тощо. Без їх фізичної безпеки неможливо реалізувати інформаційну та інші види безпеки. Тому проектування відповідних заходів та засобів щодо захисту інформації та фізичної безпеки МСМ є важливою задачею створення комплексної системи безпеки.

Вітчизняні нормативні документи визначають вимоги до проектування, проектної документації та порядку проведення робіт щодо технічного захисту інформації (ТЗІ) [18, 19]. Задачі безпеки повинні розподілятись за всіма елементами МСМ.

Комплексна система безпеки МСМ визначає організаційно-технічну систему, що складається з алгоритмічно об'єднаних та взаємопов'язаних підсистем (фізичної, інформаційної безпеки тощо), які забезпечують захист МСМ від загроз різного походження. Ієрархія підсистем в комплексній системі безпеки МСМ зображена на рисунку 1.4.

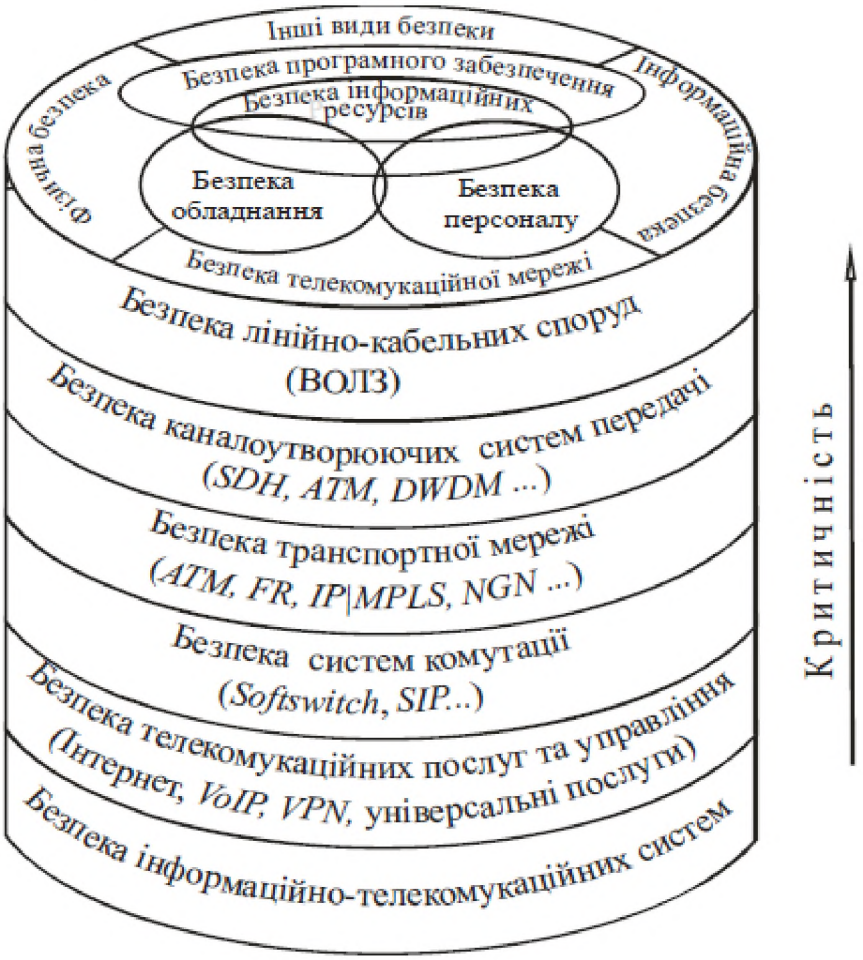

Рисунок 1.4 - Ієрархія підсистем в комплексній системі безпеки МСМ

Зона розмежування відповідальності може проникати на різну глибину та на різні рівні МСМ. Підсистеми безпеки повинні взаємодіяти і функціонувати у МСМ і на усіх рівнях, починаючи з рівня МСМ, каналоутворюючих систем передачі, транспортної мережі, комутації, керування процесами та надання

послуг. Відповідно мають створюватись підсистеми: безпеки лінійно-кабельних споруд; безпеки каналоутворюючих систем передачі; безпеки транспортної мережі; безпеки систем комутації; безпеки послуг; безпеки інформаційних систем.

Згідно [20] захисту в МСМ підлягають усі її складові елементи: лінії, канали, системи передавання, обладнання, програмне забезпечення, інформація та персонал. Кожна з підсистем безпеки, у свою чергу, повинна органічно включати у себе: безпеку інформаційних ресурсів; безпеку програмного забезпечення; безпеку обладнання; безпеку персоналу.

При реалізації проектних процедур щодо створення заходів безпеки МСМ необхідно враховувати їхні особливості: структурну складність, глобально-розподілений характер мереж, велику довжину ліній зв'язку, які знаходяться на неконтрольованій території, тощо. В процесі проектування, створення та експлуатації необхідно узгоджувати методи забезпечення ІБ різних компонентів.

На різних стадіях життєвого циклу МСМ, в різних етапах проектування, створення та експлуатації формуються показники захищеності, гарантій, якості та взаємопов'язані з ними техніко-економічні показники.

Порушення цілісності МСМ на фоні зниження активності їх елементів тягне за собою дезорганізацію управління, одночасне зниження активності елементів та їх живучості – втрату гнучкості, а зниження живучості і порушення цілісності МСМ – втрату найважливіших функцій.

1.14 Порядок виконання робіт із захисту інформації в мультисервісних мережах

Мультисервісну мережа включає велику кількість об'єктів типу вузлів комутації, з'єднаних між собою каналами або сегментами магістралі, які також треба вважати об'єктами, де обробляється, тимчасово зберігається та передається інформація. У такій системі важко точно застосувати всі етапи існуючого порядку виконання робіт з технічного захисту інформації (ТЗІ) та

процедури створення комплексно системи захисту інформації (КСЗІ), які розраховані на захист об'єкта інформаційної діяльності (ОІД).

До існуючого порядку розробки доцільно додати етапи й процедури, які б враховували ієрархічний та розподілений характер телекомунікаційної мережі, а також інтеграцію інформаційних та телекомунікаційних мереж.

Формально можна розбити порядок виконання робіт на три загальних цикли, кожен з яких розділявся б на етапи у відповідності з вимогами ДСТУ 3396.0-96, а етапи виконувались би за стадіями, в порядку, що передбачається ДСТУ 3396.1-96. Цикли виконання робіт:

а) загальний цикл створення технічного завдання (ТЗ) та плану захисту МСМ в цілому як складової інформаційно-телекомунікаційної системи. У цьому циклі проводиться обстеження МСМ та інформаційної системи, в інтересах якої функціонує МСМ, аналізуються загрози інформаційним ресурсам, визначаються вимоги до системи захисту інформації саме в МСМ, обирається мережний функціональний профіль захисту, розробляються засоби реалізації комплексної системи захисту інформаційних ресурсів в МСМ;

б) загальний цикл декомпозиції МСМ на взаємопов'язані об'єкти інформаційної діяльності, раціональної інтерпретації загальних вимог до захищеності інформації за вимогами до системи захисту інформації в ОІД, розробка оптимального розподілу засобів захисту за об'єктами ОІД;

в) загальний цикл виконання робіт з ТЗІ на кожному з телекомунікаційних ОІД відповідно до вимог ДСТУ 3396.0-96 та ДСТУ 3396.1-96.

Але недоліком такого розподілу робіт є те, що не враховується ієрархічний характер МСМ та нерівномірний розподіл механізмів захисту за рівнями ієрархії. Це стосується, перш за все, штатних засобів захисту, які вбудовуються в кожні пристрої, системи, технології, які у сукупності утворюють МСМ.

Діючі нормативно-правові документи сфери захисту інформації рекомендують аналізувати рівень захищеності інформації, виявляти нові загрози й ризики інформаційної безпеки, розробляти ТЗ на вдосконалення й модернізацію КСЗІ повторюючи увесь цикл виконання робіт.

На цьому періоді має значення розвиток штатних засобів захисту, що має призводити до більш ефективного розподілу задач захисту між штатними та додатковими механізмами захисту [21].

1.15 Принцип функціонування мультисервісного телекомунікаційного комплексу SI3000

Концепція побудови мультисервісних мереж на базі комплексу SI3000 можливо реалізувати на основі трьох вузлів устаткування:

- SI3000 MSAN (Мультисервісний вузол абонентського доступу);
- SI3000 MSCN (Мультисервісна площина керування);
- SI3000 OSAP (Відкрита площина послуг і додатків).

Сполучною інфраструктурою цих груп є пакетна комутація на базі IP-протоколу. IP-протокол, дозволяє відокремити програми та послуги від фізичної мережі середовища, використовуючи трафік всіх видів для передачі.

Всі вузли SI3000 управляються з єдиної системи управління MN. Ця система надзвичайно зручна для адміністрування та нагляду за станціями. SI3000 рекомендується використовувати системи живлення - MPS. Можливість використання існуючого обладнання значно знижує розмір необхідних від оператора інвестицій.

Перелічимо основні переваги комплексу SI3000:

- конвергенція мереж стаціонарного та мобільного зв'язку;
- розгляд проблеми побудови мереж як єдиного, цілісного рішення;
- архітектура, що складається з окремих модулів, що дозволяє конфігурувати і налаштувати її для вирішення конкретних завдань користувача;
- високий рівень надійності та готовності кожного вузлу комплексу SI3000;

- керування обробкою відмов, конфігуруванням, тарифікацією, робочими характеристиками і безпекою.

Особливості кожного вузла комплексу SI3000:

а) SI3000 MSAN (Мультисервісний вузол абонентського доступу)

SI3000 MSAN забезпечує будь-які комбінації доставки високошвидкісних, мультимедійних або мовних послуг за фіксованим та бездротовим з'єднанням. Вузол SI3000 MSAN забезпечує реалізацію мультимедійних послуг, послуг передачі мови та даних з використанням різних інтерфейсів користувача. Він є оптимальним рішенням для плавного впровадження послуг Triple Play або розширення їх спектру для абонентів квартирного сектору і бізнес-абонентів. В даному вузлі гарантується резервування і постійна експлуатаційна готовність елементів.. Уніфікована система керування забезпечує повний набір функцій дистанційного керування і контролю для кожного мережевого елемента, та знижуються витрати на конфігурацію і контроль за рахунок всебічного керування обробкою відмов, конфігуруванням, тарифікацією, робочими характеристиками і безпекою.

SI3000 включає в себе доступ: DSL, Fiber, WiMAX, POTS, та Metro Ethernet.

Модульність продукту забезпечується вдосконаленою мультисервісною платформою на базі технології Gigabit Ethernet (GE). Канали GE використовуються для забезпечення зв'язку між платами і для встановлення зовнішніх з'єднань.

Реалізована на мультисервісній платформі здвоєна зіркоподібна топологія дозволяє максимально ефективно використовувати з'єднання між платами, забезпечуючи при цьому високий рівень надійності та готовності.

SI3000 MSAN розміщується в мережі доступу і забезпечує для користувачів можливість отримання індивідуальних персоналізованих послуг незалежно від їх типу. Деяким абонентам можуть надаватися всі мультисервісні

послуги (triple-play) на базі широкосмугового доступу, іншим - тільки послуги передачі даних або відео.

Безпека SI3000 MSAN забезпечується безпосереднім та індивідуальним підходом при призначенні прав користувачам. Оператор з правами адміністративного користувача створює права доступу і призначає їх користувачам на всіх рівнях конкретних мережевих елементів і підключених до них абонентів [22].

б) SI3000 MSCN (Мультисервісна площина керування)

SI3000 MSCN являє собою інтегроване рішення, яке призначене для управління викликами, конфігурування послуг і забезпечення взаємодії між IP-мережею і телефонними мережами загального користування.

Складові окремих компонентів SI3000 MSCN зображено на рисунку 1.5.

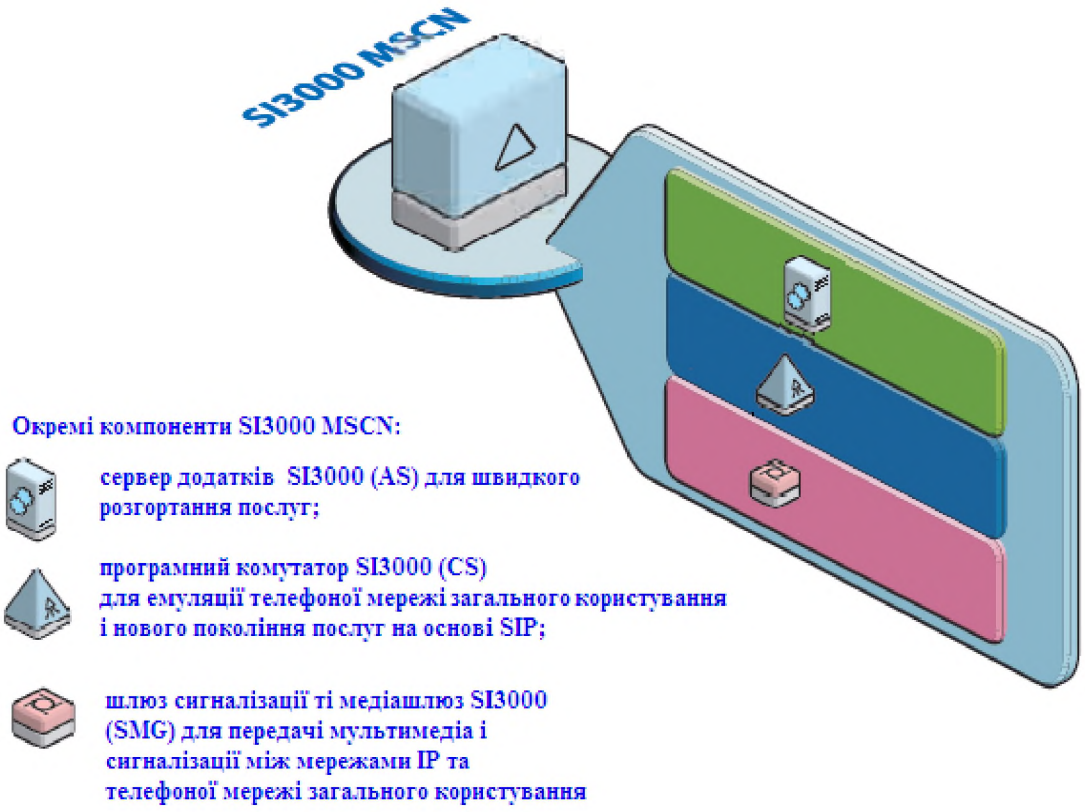

Рисунок 1.5 - Складові окремих компонентів SI3000 MSCN

SI3000 CS виконує у вирішенні функцію управління викликами для голосової частини рішення. Сервіси сервера додатків забезпечують стороннє керування викликами і надають локальним абонентам повний спектр розширених голосових IP-послуг.

SI3000 CS включає інтерфейс додатків та забезпечує управління: послугами, викликами, сигналізацією, медіа.

SI3000 AS реалізує розгортання удосконалених, конвергентних послуг, тобто конвергенцію голосового зв'язку з миттєвим обміном повідомленнями, IPTV і з веб-технологіями.

SI3000 AS включає рішення з обміну повідомленнями та рішення з управління викликами.

Шлюз сигналізації та медіашлюзи SI3000 додає широко масштабовану і гнучку функцію перетворення голосу та сигналізації на ділянці телефонної мережі загального користування та IP, і включає в себе медіа сервер [23].

Головні переваги SI3000 MSCN надійні, безпечні та зручні для користувача вузли [24].

в) SI3000 OSAP (Відкрита площина послуг і додатків)

SI3000 OSAP і вхідні в нього продукти налаштовані таким чином, щоб забезпечувати виконання завдань, що стоять як перед операторами.

Цей вузол дозволяє представити користувачам такі сервіси, як: інформаційний портал, автосекретар, маршрутизація за часом, система сповіщення, багатоканальний запис голосу, зміна тону, голосова пошта та ін. [25].

Загальна транспортна інфраструктура MCM зображена на рисунку 1.6.

Рисунок 1.6 - Загальна транспортна інфраструктура на базі мультисервісної мережі

1.2 Постановка задачі

Побудова МСМ на базі комплексу SI3000, є досить актуальною на даний час, оскільки відбувається розгляд проблеми побудови мереж як єдиного, цілісного рішення.

Завдання МСМ полягає в тому, щоб забезпечити роботу різнорідних інформаційних і телекомунікаційних систем та програм в єдиному транспортному середовищі, а це накладає певні вимоги на заходи захищеності інформації.

Постає питання з оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000. Важливим являється аналіз та вибір критеріїв оцінювання рівня захищеності.

1.3 Висновок

Інтеграція трафіку різнорідних даних і мови дозволяє якісно підвищити ефективність інформаційної підтримки керування глобальною інформаційно-

телекомунікаційною структурою, при цьому використання інтегрованого транспортного середовища знижує витрати на створення й експлуатацію мережі.

МСМ використовуючи єдиний канал для передачі даних різних типів, дає можливість зменшити різноманітність типів устаткування, застосовувати стандарти й технології, централізовано управляти комунікаційним середовищем.

Проведений аналіз чинників, які впливають на безпеку, показав, що захист інформації в МСМ є складною структурою. У той же час дослідження існуючих механізмів і протоколів захисту інформації показали наявність достатнього широкого спектру можливих варіантів їх використання при проектуванні МСМ різного рівня та призначення.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Модель загроз мультисервісних мереж

Ідентифікація загроз (визначення безлічі загроз, реалізація яких можлива в конкретнії МСМ , в даному випадку для мультисервісної мережі) передбачає розгляд джерел впливів і наслідків реалізації загроз, а також їх класифікацію.

Всі джерела загроз інформації, що обробляється в конкретній МСМ, можна розділити на три основні групи:

- загрози, зумовлені діями суб'єкта (антропогенні);
- загрози, зумовлені технічними засобами (техногенні);
- загрози, зумовлені стихійними джерелами.

Антропогені загрози найобширніші, і становлять найбільший інтерес з точки зору організації захисту від загроз даного типу, так як дії суб'єкта завжди можна оцінити, спрогнозувати і вжити адекватних заходів. Методи і заходи протидії цим загрозам (контрзаходи) керовані і безпосередньо залежать від розробників СЗІ.

Суб'єкти, дії яких можуть призвести до порушення захищеності інформації, можуть бути як зовнішні:

- кримінальні структури;
- несумлінні партнери;
- конкуренти;
- політичні супротивники;

так і внутрішні:

- персонал організації.

За результатами міжнародного та вітчизняного досвіду, дії суб'єктів можуть привести до ряду небажаних наслідків, серед яких можна виділити:

1 Крадіжка:

- технічних засобів МСМ;
- носіїв інформації;
- інформації;

- засобів доступу до інформації.

2 Підміна (модифікація):

- операційних систем;

- систем управління базами даних;

- прикладних програм;

- інформації (даних), заперечення фактів відправки повідомлень;

- паролів і атрибутів доступу.

3 Знищення (руйнування):

- технічних засобів МСМ;

- носіїв інформації;

- програмного забезпечення;

- інформації;

- паролів і ключової інформації.

4 Порушення нормальної роботи:

- зниження швидкості обробки інформації;

- зниження пропускної здатності каналів зв'язку;

- зменшення обсягів вільної оперативної пам'яті;

- зменшення обсягів вільного дискового простору;

- порушення електроживлення технічних засобів.

5 Помилки:

- при інсталяції програмного забезпечення (ПО), ОС, СУБД;

- при написанні прикладного ПЗ;

- при експлуатації ПЗ;

- при експлуатації технічних засобів.

6 Перехоплення інформації:

- за рахунок побічного електромагнітного випромінювання від технічних засобів;

- за рахунок наведень по лініях електроживлення;

- за рахунок наведень по стороннім провідникам;

- по акустичному каналу від засобів виводу;

- по акустичному каналу при обговоренні питань;

- при підключенні до каналів передачі інформації;

- за рахунок порушення встановлених правил доступу (злом).

Техногенні загрози, менш прогнозовані, безпосередньо залежать від властивостей техніки і тому вимагають особливої уваги. Технічні засоби, що містять канали реалізації потенційних загроз захищеності інформації, також можуть бути внутрішніми:

- неякісні технічні засоби обробки інформації;

- неякісні програмні засоби обробки інформації;

- допоміжні засоби (охорони, сигналізації, телефонії);

- інші технічні засоби, що застосовуються в організації;

і зовнішніми:

- засоби зв'язку;

- близько розташовані небезпечні виробництва;

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

- транспорт.

Наслідками застосування таких технічних засобів, що безпосередньо впливають на захищеність інформації, можуть бути:

1 Порушення нормальної роботи:

- порушення працездатності засобів обробки інформації;

- порушення працездатності каналів передачі даних;

- старіння носіїв інформації та засобів її обробки;

- порушення встановлених правил доступу;

- електромагнітний вплив на технічні засоби.

2 Знищення (руйнування):

- програмного забезпечення, ОС, СУБД;

- засобів обробки інформації;

- приміщень;

- інформації;

- персоналу.

3 Модифікація (зміна):

- програмного забезпечення, ОС, СУБД;

- інформації при передачі по каналах передачі даних.

Стихійні загрози, які абсолютно не піддаються прогнозуванню і тому заходи для їх запобігання повинні застосовуватися, по можливості, завжди, але необов'язково до МСМ як до об'єкта захисту, а ширше, до всіх елементів технічної інфраструктури підприємства чи організації.

Стихійні джерела, є складовими потенційних загроз захищеності інформації, як правило, являються зовнішніми по відношенню до даного об'єкту, під ними розуміються, перш за все, природні катаклізми:

- пожежі;

- землетруси;

- повені;

- урагани;

- інші форс-мажорні обставини;

- різні непередбачені обставини;

- нез'ясовні явища.

Ці природні та нез'ясовні явища також впливають на захищеність інформації, небезпечні для всіх елементів МСМ і можуть призвести до таких наслідків:

1 Знищення (руйнування):

- технічних засобів обробки інформації;

- носіїв інформації;

- програмного забезпечення;

- інформації (файлів даних);

- приміщень;

- персоналу.

2 Зникнення (пропажа):

- інформації в засобах обробки;

- інформації при передачі по каналах передачі даних;

- носіїв інформації;

- персоналу [26].

На рисунку 2.1 представлені види загроз, що впливають на безпеку інформації та стійкість функціонування МСМ [27].

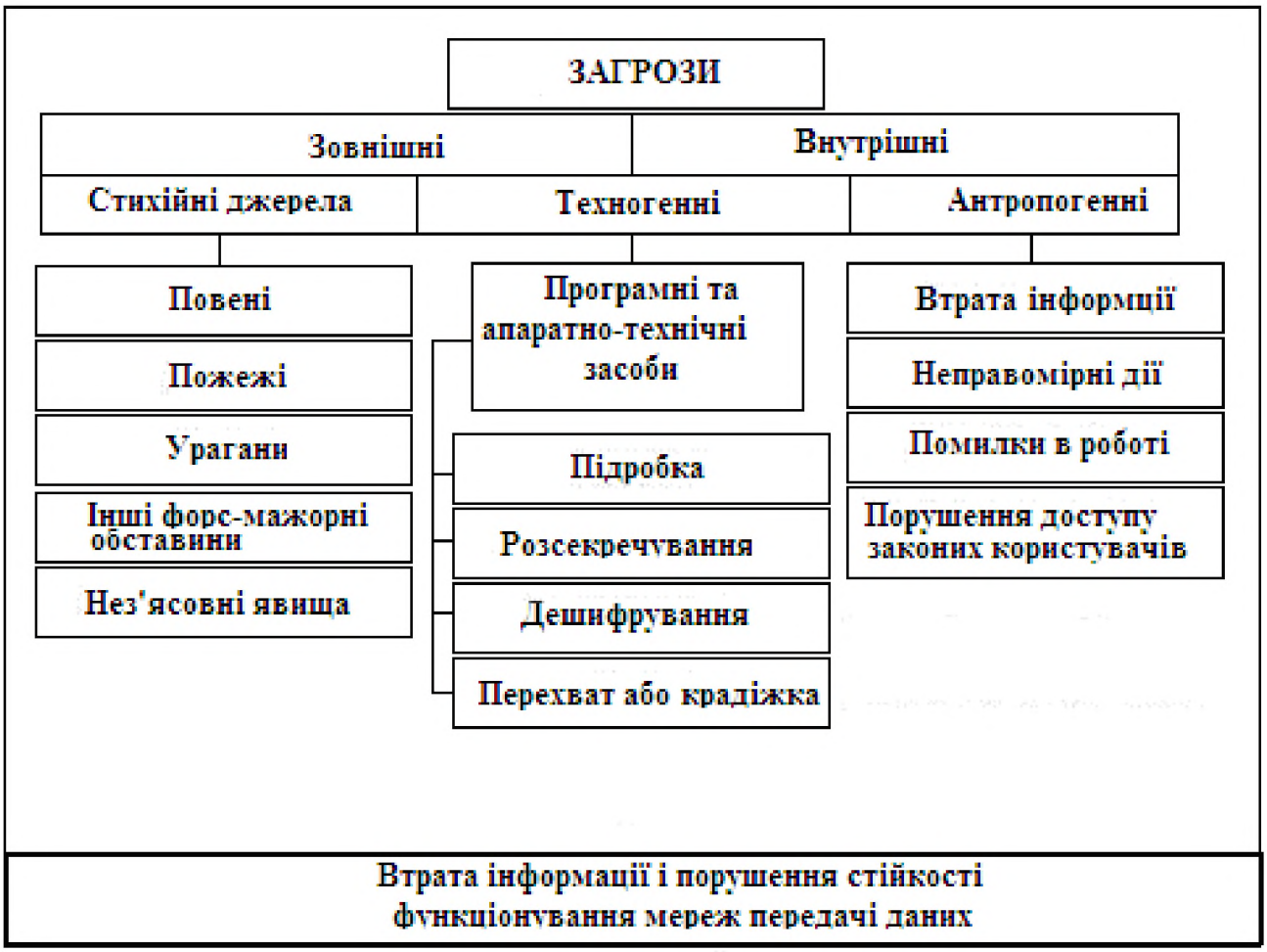

Рисунок - 2.1 Види загроз МСМ

В таблиці 2.1 представлена модель загроз для мережевих атак МСМ.

Знак «+» відображає, що дана властивість інформації втрачена, знак «-» відображає, що дана властивість збережена.

Таблиця 2.1 - Модель загроз для мережевих атак МСМ

Мережева атака	Порушення		
	Конфіденційності	Цілісності	Доступності
З використанням НСД	+	+	+
Незаконне використання привілеїв	+	+	+
«Salami»	-	+	-
«Прихованих каналів»	+	-	-
Заміна легального користувача нелегальним	+	+	-
«Збір сміття»	+	-	-
«Злам системи»	+	+	+
Зловмисні програми	+	+	+
Заміна даних	-	+	-
Нав'язування хибного маршруту	+	+	+
Перехоплення повідомлень	+	-	-

2.2 Модель порушника для мультисервісних мереж

Загрози інформації в МСМ реалізуються порушниками з використанням різних вразливостей системи. Вразливість системи - нездатність системи протистояти спробам реалізації певної загрози або сукупності загроз (атакам). Для обмеження безлічі потенційно можливих загроз і способів їх реалізації (вибору тих із них, які можуть бути реалізовані в умовах конкретної МСМ) важливо коректно визначити модель потенційного порушника.

Модель порушника - абстрактний формалізований або неформалізований опис порушника. При визначенні моделі порушника необхідно класифікувати

всіх потенційних порушників в МСМ на категорії за їх можливостями доступу до системи і, отже, по можливостям використання тих чи інших вразливостей системи та наносимому збитку.

У чинних НД ТЗІ в якості порушника розглядається особа, яка може отримати доступ до роботи з усіма включеними до складу МСМ засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами МСМ. Виділяється чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей ведення діалогу в МСМ, це можливість запуску фіксованого набору завдань (програм), які реалізують заздалегідь передбачені функції з обробки інформації;

- другий рівень визначається можливістю створення і запуску власних програм з новими функціями з обробки інформації;

- третій рівень визначається можливістю управління функціонуванням МСМ, тобто впливом на базове програмне забезпечення системи, а також на склад і конфігурацію її устаткування;

- четвертий рівень визначається всім обсягом можливостей осіб, які здійснюють проектування, реалізацію і ремонт апаратних компонентів МСМ, аж до включення в склад МСМ власних коштів з новими функціями з обробки інформації. Передбачається, що в своєму рівні порушник - це фахівець вищої кваліфікації, який має повну інформацію про МСМ та КСЗ. Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу уразливості системи, ефективності існуючих і планованих заходів захисту. На її основі можна (при необхідності, з уточненнями, які враховують специфіку конкретної МСМ) обмежити коло потенційних порушників та їх можливостей [26].

Категорії порушників, що визначені у моделі загроз МСМ представлені в таблиці 2.2.

Таблиця 2.2 - Категорії порушників моделі загроз МСМ

Позначення	Визначення категорії	Рівень загрози
	Внутрішні по відношенню до мережі	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, сантехніки, прибиральники тощо), в яких розташовані компоненти АС	2
ПВ2	Рядові співробітники	3
ПВ3	Адміністратор ІБ	2
ПВ4	Керівники середньої ланки	2
ПВ5	Вище керівництво	2
	Зовнішні по відношенню до мережі	
ПЗ1	Відвідувачі (запрошені з деякого приводу)	3
ПЗ2	Представники організацій, які взаємодіють з питаннями технічного обслуговування (енерго-, водного-, теплопостачання і т.п.)	4

Специфікація моделі порушника МСМ за мотивами здійснення порушень наведена в таблиці 2.3.

Таблиця 2.3 - Модель порушника МСМ за мотивами здійснення порушень

Позначення	Характеристика можливостей порушника	Рівень загрози
Ч1	До впровадження МСМ або її окремих компонентів	3
Ч2	Під час бездіяльності компонентів системи (в неробочій час, під час планових перерв у роботі.	2

Продовження таблиці 2.3

Позначення	Характеристика можливостей порушника	Рівень загрози
Ч3	Під час функціонування МСМ (або компонентів системи)	3
Ч4	Як у процесі функціонування МСМ, так і під час призупинки компонентів системи	4

Специфікація моделі порушника МСМ за часом дії представлена в таблиці 2.4.

Таблиця 2.4 - Модель порушника МСМ за часом дії

Позначення	Мотив порушення	Рівень загрози
М1	Безвідповідальність	1
М2	Самозатвердження	3
М3	Корисливий інтерес	4
М4	Професійний обов’язок	2

Специфікація моделі порушника МСМ за рівнем кваліфікації та обізнаності представлена в таблиці 2.5.

Таблиця 2.5 - Модель порушника МСМ за рівнем кваліфікації

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К1	Знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи	1
К2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування	2
К3	Високий рівнем знань у галузі програмування та проектування та експлуатації МСМ.	3

Продовження таблиці 2.5

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К4	Знає структуру, функції й механізми дії засобів захисту МСМ, їх недоліки	3
К5	Знає недоліки та “вади” механізмів захисту, які вбудовані у системне ПЗ та його недокументовані можливості	3
К6	Є розробником програмних та програмно-апаратних засобів захисту або системного ПЗ.	4

Специфікація моделі порушника МСМ за показником можливостей використання засобів та методів подолання системи захисту представлена в таблиці 2.6.

Таблиця 2.6 - Модель порушника МСМ за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загрози
З1	Використовує лише агентурні методи одержання відомостей	1
З2	Використовує пасивні засоби (технічні засоби перейманння без модифікації компонентів системи)	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання, а також компактні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Застосовує методи та засоби дистанційного упровадження програмних закладок та спеціальних резидентних програм збору, пересилання або блокування даних.	3

Продовження таблиці 2.6

Позначення	Характеристика можливостей порушника	Рівень загрози
З5	Застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передачі даних).	4

Специфікація моделі порушника МСМ за місцем дії представлена 2.7.

Таблиця 2.7 - Модель порушника МСМ за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загрози
Д1	Без доступу на контрольовану територію організації	1
Д2	З контрольованої території без доступу у будинки та споруди	1
Д3	Усередині приміщень, але без доступу до технічних засобів МСМ	3
Д4	З робочих станцій (операторів)	3
Д5	З доступом у зони даних (баз даних, архівів й т.ін.)	3
Д6	З доступом у зону керування засобами забезпечення безпеки МСМ	4

Використовувані позначення:

1 - рівень загрози малий, практично неможливий (ймовірність в 0-30% випадків);

2 - рівень загрози невеликий, але в окремих випадках можливий (ймовірність в 30-50% випадків);

3 - загроза можлива в 50% випадків;

4 - дуже велика ймовірність загрози (ймовірність в 50-80% випадків);

5 - загроза неминуча (ймовірність в 80-90% випадків).

В таблиці 2.8 представлена модель порушника МСМ.

Таблиця 2.8 - Модель порушника МСМ

Порушник	ПВ1	ПВ2	ПВ3	ПВ4	ПВ5	ПЗ1	ПЗ2
Мотив	М1, М2	М2, М3	М3, М4	М1, М3	М3, М4	М3	М1, М4
Час дії	Ч1, Ч2	Ч2, Ч3	Ч1, Ч4	Ч3	Ч4	Ч2	Ч2
Порушник	ПВ1	ПВ2	ПВ3	ПВ4	ПВ5	ПЗ1	ПЗ2
Використання засобів подолання системи захисту	З3, З4, З5	З2, З3	З4, З5	З1, З2, З3	З3	З3, З4	З5
Кваліфікація	К1	К1, К2, К3	К4, К5, К6	К2, К3	К2, К3	К1	К1
Місце дії	Д3	Д4	Д6	Д4	Д5	Д2	Д3

2.3 Функціональний профіль захищеності для мультисервісної мережі

МСМ відносяться до 3 класу автоматизованих систем. АС в МС представляє собою розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності, а також існує необхідність передачі інформації через незахищену середу. Для АС обрані стандартні функціональні профілі захищеності в МСМ, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації:

3.КЦД.1 = {КД-2, КО-1, КВ-1,
ЦД-1, ЦО-1, ЦВ-1,
ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

Згідно з [28] експертним висновком №130 держспецзв'язку в телекомунікаційному комплексі SI3000 сертифікований мультисервісний пристрій доступу SI-3000 (МПД SI-3000). Призначення засобу: забезпечення захисту інформаційних ресурсів МПД SI-3000. Відповідає вимогам НД з ТЗІ в

обсязі функцій, зазначених у Технічному завданні, сукупність яких визначається функціональним профілем КА-2, ЦА-1, ЦА-2, ЦО-1, ДР-1, ДВ-1, ДЗ-1, ДС-1, НР-2, НИ-2, НК-1, НО-2, НЦ-1, НТ-2 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99.

Далі наведено функціональний профіль для МСМ, а також критерії профілю який забезпечує МПД SI-3000.

Мультисервісна мережа:

3.КЦД.1 = {КД-2, КО-1, КВ-1,
ЦД-1, ЦО-1, ЦВ-1,
ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1} ;

МПД SI3000 забезпечує критерії : ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НТ-2.

КД-2. Базова довірча конфіденційність

Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта КЗЗ, повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

Для реалізації послуги повинні використовуватися такі механізми:

а) керування доступом (на основі списків управління доступом - перелік користувачів та / або процесів із зазначенням їх прав доступу до інформаційного об'єкту МСМ, з яким пов'язаний цей перелік. Забезпечує дуже виборчу настройку прав доступу);

б) система обліку і контролю доступу абонентів до серверів програмних додатків вбудовано в загальний комплекс структурованої ІБ МСМ . В такій системі ні жодна людина навіть легальний адміністратор, не має контроль над декількома життєво важливими програмними додатками, там активно використовуються клієнтські профілі, що містять finger - & voice- print досьє, контролюється маршрутизація трафіку, тобто є відповідність клієнтської адреси і доступних йому сегментів мережі.

в) отримуючи доступ к тому чи іншому ресурсу для підключення пакету послуг, що йому надаються, абонент МСМ включається в групу спеціальних користувачів, яким дозволено лише певний сценарій взаємодії, який передбачає відповідний ланцюжок, що активує процеси на сервері програмних додатків.

КО-1. Повторне використання об'єктів

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Для реалізації послуги повинні використовуватися такі механізми:

а) очищення дискової пам’яті, видалення файлів перед наданням відповідному ресурсу іншому клієнту.

б) очищення дискової пам’яті, і оперативної пам’яті після видалення інформації про об'єкт перед наданням пам’яті під розміщення інших об'єктів;

в) видалення атрибутів доступу (списків керування доступом) при видалені об'єкту.

КВ-1. Повторне використання об'єктів Мінімальна конфіденційність при обміні

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Для реалізації послуги повинні використовуватися такі механізми:

Найбільш популярними стеками протоколів, що забезпечують захищений обмін даними в МСМ, є протоколи IPsec, TLS, L2TP і PPTP. Реалізуючи функції, визначені в стеку, стає можливим формування криптографічного захищеного каналу (узгодження параметрів і виділення ресурсів для з'єднання типу «точка-точка»), реалізації взаємної аутентифікації об'єктів, а також конфіденційності і цілісності даних.

ЦД-1. Мінімальна довірча цілісність

Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. Права доступу до кожного

захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

Для реалізації послуги повинні використовуватися такі механізми:

Керування доступом (на основі списків управління доступом - на основі списків управління доступом - перелік користувачів та / або процесів із зазначенням їх прав доступу до інформаційного об'єкту МСМ, з яким пов'язаний цей перелік. Забезпечує дуже виборчу настройку прав доступу).

ЦО-1. Обмежений відкат

Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Реалізовується МПД SI-3000, для реалізації послуги використовуються такі механізми:

а) забезпечення цілісності шляхом реплікації даних (механізму забезпечення цілісності даних з відновленням, що передбачає: наявність зроблених заздалегідь декількох копій даних, рознесених на різних серверах; виявлення порушення цілісності шляхом виконання порівняння даних з різних джерел);

б) забезпечення цілісності шляхом повтору повідомлень (механізм забезпечення цілісності даних з відновленням, що включає: виявлення порушення цілісності з використанням механізмів контролю цілісності; оповіщення джерела даних про порушення і повтор повідомлення доти, поки цілісність даних не буде забезпечена);

в) контроль цілісності по коду контроля цілісності (механізм перевірки / підтвердження цілісності повідомлення з використанням спеціальної контрольної величини, що є функцією переданих в повідомленні даних);

г) контроль цілісності по контексту (механізм перевірки / підтвердження цілісності повідомлення, що передбачає перевірку наявності в певній частині повідомлення певних, наперед відомих даних (наприклад, тимчасової мітки або номера пакета). використовується для перевірки цілісності потоку даних (повідомлень).

ЦВ-1: Мінімальна цілісність при обміні

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається.

Для реалізації послуги повинні використовуватися такі механізми:

а) контроль цілісності і незмінності даних при передачі базується на використанні криптографічних контрольних сум (підписів) .

б) кожна послуга, яка надається абоненту повинна розглядатися як окрема транзакція, що потребує процедур ідентифікації і аутентифікації клієнту, а також авторизації отриманих послуг. Ці процедури,які розділені по різноманітним сегментам мережі, дозволяють знизити вірогідність одночасної модифікації всіх інформаційних потоків, що забезпечують кожну клієнтську транзакцію.

ДР-1. Квоти

Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

Реалізовується МПД SI-3000, для реалізації послуги використовуються такі механізми: управління доступом (на основі списків управління доступом - перелік користувачів та / або процесів із зазначенням їх прав доступу до інформаційного об'єкту МСМ, з яким пов'язаний цей перелік. Забезпечує дуже виборчу настройку прав доступу) з контролем використовуваного об’єму ресурсів.

ДВ-1. Ручне відновлення

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС . Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Реалізовується МПД SI-3000, для реалізації послуги використовуються такі механізми: резервування програмних засобів та інформації з можливістю ручного відновлення.

НР-2. Захищений журнал

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Реалізовується МПД SI-3000, для реалізації послуги використовуються такі механізми: реєстрація та аудит (механізми, використовувані для реалізації контролю дій об'єкта (сутності) на підставі зареєстрованої інформації. включають:

а) контроль поведінки на основі заздалегідь певного «профілю»;

б) контроль на наявність деяких типів подій протягом певного періоду часу;

в) контроль на відсутність деяких типів подій протягом певного періоду часу.

НИ-2. Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

Реалізовується МПД SI-3000, для реалізації послуги використовуються такі механізми: ідентифікація абонента виконується на підставі введеного ним з клавіатури імені (псевдоніма). Автентифікація абонента виконується на підставі введеного з клавіатури пароля і висунутого носія даних аутентифікації. Таким чином, реалізована автентифікація користувача одночасно за двома принципами: «володію чимось» - носій даних аутентифікації і «знаю щось» - пароль (двофакторна автентифікація). В якості носія даних аутентифікації виступає пристрій USB flash drive.

У разі якщо надана користувачем інформація аутентифікації не відповідає еталону, доступ користувача в систему блокується. Крім того, МПД SI-3000

веде контроль за закінченням терміну дії повноважень користувача і його пароля.

НК-1. Однонаправлений достовірний канал

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

Реалізовується МПД SI-3000, для реалізації послуги використовуються такі механізми: організація каналу безпосередньої взаємодії користувача з КСЗ.

НО-2. Розподіл обов'язків адміністраторів

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

Реалізовується МПД SI-3000, для реалізації послуги використовуються такі механізми: управління доступом (на основі ролей, повноважень).

НЦ-2. КЗЗ з гарантованою цілісністю

Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Для реалізації послуги повинні використовуватися такі механізми: контроль цілісності по коду контроля цілісності (механізм перевірки / підтвердження цілісності повідомлення з використанням спеціальної контрольної величини, що є функцією переданих в повідомленні даних. Використання даного механізму передбачає виконання операцій вироблення і перевірки контроля цілісності коду контролю цілісності), керування доступом.

НТ-2. Самотестування при старті

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

Реалізовується МПД SI-3000, для реалізації послуги використовуються такі механізми: кожен раз в процесі старту МПД SI-3000 здійснює контроль цілісності свого програмного забезпечення, тестування його базових механізмів. У разі виявлення порушення цілісності користувачеві видається відповідне повідомлення і подальша робота блокується. У такій ситуації необхідне втручання системного адміністратора для відновлення цілісності.

Додатково для забезпечення цілісності МПД SI-3000 обмежується доступ до серверів програмних додатків, в якому містяться файли ПО, і налаштувань ОС по запису. Доступ по запису до цього серверу, в якому містяться файли ПО, системний адміністратор може отримати тільки через програму керування адміністратора КСЗ, яка дозволяє модифікувати файли програмного забезпечення МПД SI-3000.

НВ-1: Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ.

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму.

Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації [29].

Для реалізації послуги повинні використовуватися такі механізми:

а) інфраструктура клієнтського доступу МСМ має лиш одну точку входу для доступу клієнта до будь-якого ресурсу мережі через портал, що включає в себе центр ідентифікації і аутентифікації. Кожний із рівнів аутентифікації дозволяє легальному клієнту доступ до відповідної групи серверів програмних додатків.

б) перехід абонента від ресурсу до ресурсу можливий тільки після повернення портальної сесії абонента і повторної процедури ідентифікації і авторизації.

в) політика безпеки на основі ролей для аутентифікації і авторизації, з використанням функції єдиної реєстрації (Single Sign-On).

2.4 Методика оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000

Критерії оцінювання рівня захищеності. В якості параметрів, на підставі яких і робиться вибір методики для оцінки рівня захищеності телекомунікаційного комплексу SI3000, можна виділити наступні: продуктивність, вартість, керованість, сумісність, захищеність.

Із зростанням рівня захищеності, наприклад, зростає вартість, складність налагодження комплексу, в той же час падає продуктивність його роботи. Тому в даній методиці проводитиметься оцінка ефективності системи за параметром захищеності, як основного показника, що характеризує рівень забезпечуваного захисту телекомунікаційного комплексу SI3000, а на інші характеристики вводяться обмеження. Будемо оцінювати захищеність телекомунікаційного комплексу SI3000 кількісно формула (2.1) залежно від вартості інформації, що

захищається; ймовірності зламу; вартості самої системи захисту комплексу; продуктивності системи захисту інформації:

$$Z = f(B_{зк}, P_{зл}, B_{зі}, П_{сзі}), \tag{2.1}$$

де Z - кількісний параметр оцінювання захищеності;

$B_{зк}$ - вартість системи захисту комплексу;

$P_{зл}$ - ймовірності зламу;

$B_{зі}$, - вартість захисту інформації;

$П_{сзі}$ - продуктивності системи захисту інформації.

Для спрощення розрахунків необхідно звести задачу шляхом початкового завдання ряду параметрів. Для цього потрібно встановити обмеження на вартість захисту Взі ≤ Взад, де Взі – вартість інформації, що захищається, в телекомунікаційному комплексі SI3000; Взад - задані обмеження на вартість системи захисту.

Обмеження на продуктивність: Псзі ≥ Пзад, де Псзі – продуктивність системи захисту інформації, Пзад – задані обмеження на продуктивність системи захисту інформації.

При цьому, крім забезпечуваного рівня захищеності, повині враховувати ще ряд найважливіших характеристик системи захисту комплексу. Наприклад, обов'язково має враховуватися вплив системи захисту на завантаження обчислювального ресурсу, що захищається. У загальному випадку завантаження обчислювального ресурсу визначається кількістю прикладних завдань, що вирішуються об'єктом в одиницю часу [30].

Критерії по яким розробляється методика для оцінки рівня захищеності телекомунікаційного комплексу SI3000 проілюстровані на рисунку 2.2.

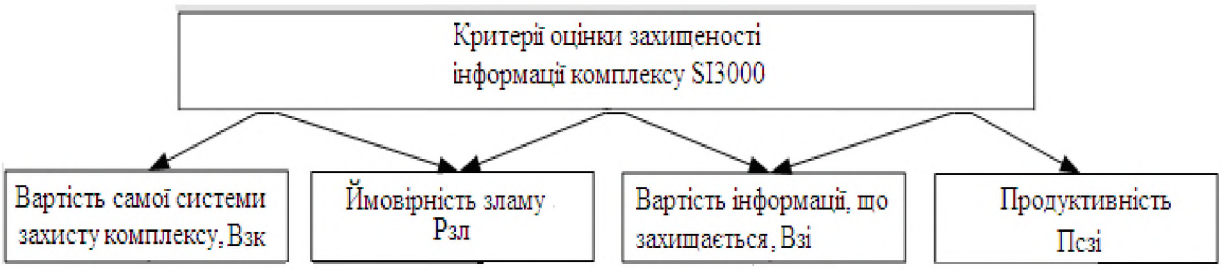

Рисунок - 2.2 Критерії оцінки захищеності

2.4.1 Захищеність з точки зору ризику

В даний час на практиці використання теорії ризиків для оцінки рівня захищеності на сьогодні є найбільш використовуваним методом.

Ризик - функція ймовірності реалізації певної загрози, виду і величини завданих збитків [31]. Ризик обчислюємо по формулі (2.2):

$$R(p) = (B_{зі} * P_{зл});\ R(\alpha) = (B_{зі} * \alpha_{зл}), \qquad (2.2)$$

де $R(p), R(\alpha)$ - ризик;

$B_{зі}$, - вартість захисту інформації;

$P_{зл}$ - ймовірності зламу;

$\alpha_{зл}$ - інтенсивність потоку зломів;

В якості основного критерія захищеності будемо використовувати коєфіцієнт захищеності D, що показує відносне зменшення ризику в захищеному (Rзах) телекомунікаційному комплексі SI3000 в порівнянні з незахищеним (Rнез) телекомунікаційним комплексом SI3000. В формулі (2.3) представлено розрахунок коефіцієнту захищеності D.

В формулі (2.4) обчислювання коефіцієнту D відбувається, з точки зору Інтенсивності потоків зламів системи захисту SI3000.

$$D = (1 - \frac{R_{зах}}{R_{незах}}) * 100\%, \qquad (2.3)$$

де $R_{зах}$ - ризик в захищеному телекомунікаційному комплексі SI3000;

$R_{незах}$ - ризик в незахищеному телекомунікаційному комплексі SI3000.

$$D = 1 - \frac{\sum_{1}^{w} C_i * \alpha_i (1 - p_i)}{\sum_{1}^{w} C_i * \alpha_i}, \quad (2.4)$$

де C_i - вартість втрати від злому;

α_i - інтенсивність потоків зламів;

p_i - ймовірність відбиття загроз і-го виду системи захисту;

w - кількість видів загроз, що впливають на систему.

Якщо розраховане значення коєфіцієнту захищеності (D), що приведено в формулі (2.4) не задовольняє вимогам по захисту інформації, то в допустимих значеннях можливо міняти задані обмеження. При цьому задається прирощення вартості та зниження продуктивності. У такому вигляді задача вирішується в результаті реалізації ітераційної процедури шляхом відсіювання варіантів, що не задовольняють обмеженим умовам, і подальшого вибору з решти варіантів з максимальним коефіцієнтом захищеності.

2.4.2 Завдання вхідних параметрів системи для методики

Способи завдання інтенсивностей і ймовірностей загроз. Основною проблемою проведення кількісної оцінки рівня захищеності є завдання вхідних параметрів для захисту інформації - ймовірностей і інтенсивностей загроз. Розглянемо можливі способи завдання ймовірностей і інтенсивностей загроз

1 Метод статистичної оцінки li (Qi) та pi. Основним засобом завдання інтенсивностей потоків загроз li (ймовірностей загроз Qi) і ймовірностей зломів pi є отримання цих значень на основі наявної статистики загроз безпеки телекомунікаційних систем, в яких реалізується система захисту. Якщо існує статистика для аналогічного телекомунікаційного обладнання, то задавати вихідні параметри для оцінки захищеності можна на її основі. При цьому

бажано, щоб подібне телекомунікаційне обладнання експлуатувалося на підприємствах з подібною специфікою діяльності. Однак при практичній реалізації такого підходу виникають наступні складності. По-перше повинен бути зібраний досить великий матеріал про події в даній області. По-друге даний підхід не завжди виправдано. Якщо телекомунікаційний комплекс досить великий (містить багато елементів, розташований на великій території) має давню історію, то подібний підхід, швидше за все, застосуємо. Якщо ж комплекс порівняно невеликий і експлуатує новітні елементи технології (для яких поки немає достовірної статистики) оцінки загроз можуть виявитися недостовірними. Статистика загроз періодично публікується досить авторитетними виданнями, тобто завжди існують вихідні дані для використання даного підходу для більшості додатків засобів захисту інформації.

Даний телекомунікаційний комплекс використовує нові технології та програмні додатки, оскільки необхідна статистика по загрозам безпеки відсутня, тому скористаємось наступним методом – методом експертної оцінки.

2 Метод експертної оцінки. Метод експертної оцінки застосовується на етапах формулювання проблеми і оцінки різних способів її вирішення. Група експертів, створена з метою збору інформації з певних джерел з певної проблеми.

Експерт оцінює ефективність (імовірність) відображення загроз елементами захисту pi та ймовірність появи загроз Qi.

Ймовірності експерт задає лінгвістичними оцінками: відмінно, добре, задовільно, погано, не відображає, ймовірно, близько до нуля, близько до одиниці, досить імовірно і т.п. Потім ці лінгвістичні оцінки за допомогою словника переводяться в числа pi і в діапазоні Qi [0, 1]. Після розрахунку загальної оцінки всієї групи розраховується узгодженість відповідей, яка може використовуватися для оцінки достовірності результатів. Узгодженість розраховується за допомогою середньоквадратичного відхилення і виражається у відсотках. Максимальна узгодженість досягається при однакових значеннях

оцінок експертів і в цьому випадку дорівнює 100%. Мінімальна узгодженість досяжна при максимальному розкиді оцінок експертів [30].

2.4.3 Способи завдання вартості інформаційних ресурсів

Найважливішою характеристикою телекомунікаційного комплексу,що захищається (як наслідок, і системи захисту) є вартість втрат від злому. Розглянемо можливі способи завдання вартості втрат. Метод дозволяє встановити цінність телекомунікаційного обладнання. Цінність телекомунікаційного обладнання у даному методі залежить від ціни їх відновлення у разі руйнування. Цінність даних та програмного забезпечення визначається в наступних ситуаціях:

- недоступність телекомунікаційних вузлів протягом певного періоду часу;

- руйнування ресурсу - втрата інформації, отриманої з часу останнього резервного копіювання, або її повне руйнування;

- порушення конфіденційності у випадках несанкціонованого доступу штатних співробітників або сторонніх осіб;

- модифікація даних - розглядається для випадків дрібних помилок персоналу (помилки вводу), програмних помилок, навмисних помилок;

- наявність помилок, пов'язаних з передачею інформації.

Для оцінки можливого збитку рекомендується скористатися деякими з перерахованих критеріїв: шкода репутації організації; порушення чинного законодавства; збиток, пов'язаний з розголошенням персональних даних; фінансові втрати від розголошення інформації; фінансові втрати, пов'язані з відновленням ресурсів; дезорганізація діяльності.

а) Вартість викраденої / спотвореної / втраченої інформації складатиме формула (2.5):

$$C_i = \min(c_i \cdot V \cdot T \cdot V_i), \tag{2.5}$$

де c_i - [грн./біт] - питома ціна інформації;

V - [біт /с] - швидкість отримання / спотворення / знищення інформації;

T - [с]... час знаходження інформації в системі;

V_i - [біт] об'єм інформації.

б) Витрати від неможливості отримання доступу до інформації складатиме формула (2.6):

$$C_i = c_i \cdot T, \tag{2.6}$$

де c_i [грн./біт] - питома ціна недоступності інформації;

T [с] - час відновлення системи [30].

Щоб точніше визначити збиток в результаті реалізації загроз інформації необхідно вдатися до деякої класифікації загроз і виділити той принцип класифікації який більшою мірою характеризує вартість втрат. Існують різні класифікації загроз: за принципами і характером впливу на систему; по використовуваним технічним засобам; по цілям атаки і т.п.

Очевидно, що вартість втрат Сі зручніше задавати для загроз, класифікованих за цілями атаки. Що стосується характеристики інтенсивності загроз, то вона визначається за допомогою засобів аудиту та мережевого моніторингу, які розрізняють загрози за принципами і характером впливу на телекомунікаційний комплекс (механізму атаки, способом проникнення). Ймовірність віддзеркалення загрози засобами захисту рі визначається у відповідності з тими механізмами, які реалізовані в кожному вузлі телекомунікаційного комплексу SI3000. Причому кожен з механізмів у загальному випадку може відображати кілька видів атак.

Для успішного приведення у відповідність різних параметрів оцінки захищеності необхідна коректна побудова моделі порушника, де відображено практичні та теоретичні можливості порушника, його апріорні знання, час і місце дії порушника.

Завдання відповідності між вартістю втрат і інтенсивністю погроз здійснюється за допомогою статистичного підходу, що є основним, який володіє більшою вірогідністю. З аналізу статистики можна виявити ймовірності нанесення певних видів збитку при певних видах зломів.

2.4.4 Опис покрокової методики

Оцінка захищеності рівня телекомунікаційнного комплексу SI3000 складається з кроків:

1 Розрахунок параметрів: вартості втрат, інтенсивності потоків загроз, ймовірності відображення загроз елементами захисту телекомунікаційнного комплексу SI3000. Для оцінки захищеності за вихідними даними використовують метод експертної оцінки.

2 Розрахунок критеріїв захищеності: коефіцієнта захищеності, вартості системи захисту інформації, зниження продуктивності телекомунікаційнного комплексу від установки системи захисту для кожного набору механізмів захисту.

У тому випадку коли загрози і потенційний збиток зрозумілі, то зрозумілі і рамки бюджету на систему ІБ. Істотно, що при цьому стає можливим притягнути керівництво компанії до усвідомлення проблем ІБ і побудови системи захисту інформації і заручитися його підтримкою. В якості такого підходу для оцінки вартості системи захисту може використовуватися дана методика без введення обмежень на параметр вартості системи захисту інформації, а орієнтуватися тільки на необхідний рівень захищеності.

3 Оцінка набору механізмів захисту телекомунікаційнного комплексу SI3000 з максимальним коефіцієнтом захищеності D, що задовольняє обмеженням по вартості системи захисту інформації та продуктивності системи захисту інформації комплексу SI3000.

4 Оцінка рівня захищеності по максимальному коєфіцієнту захищеності D по трьохбальній процентній шкалі.

На рисунку 2.3 представлена схема покрокової методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000.

Рисунок 2.3 Схема покрокової методики

При оцінці [32] вартості захисту інформації телекомунікаційного комплексу SI3000 використовується підхід, який полягає в тому, щоб освоїти, а потім застосувати на практиці необхідний інструментарій отримання метрики і заходів безпеки, а для цього залучити керівництво компанії (як її власника) до оцінки вартості захищаємої інформації, визначенню ймовірностей потенційних загроз і вразливостей, а також потенційного збитку.

На рисунку 2.4 представлений алгоритм проведення методики.

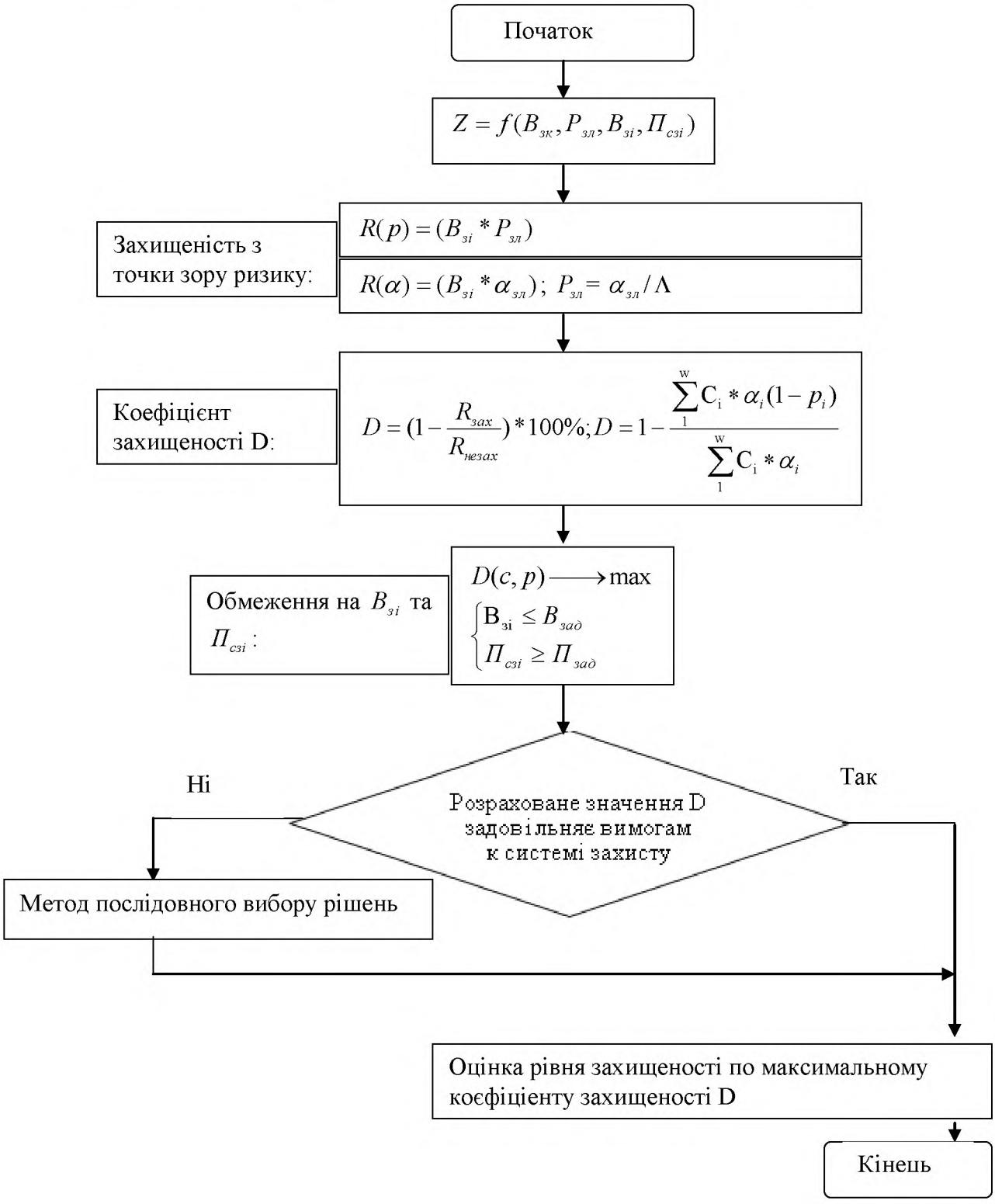

Рисунок 2.4 – Алгоритм проведення методики, оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000

Для отримання більш точних даних наближених до реальності і більшою мірою, що відповідають специфіці організації, на першому етапі (підготовчому), попередньому етапу розрахунку параметрів, потрібно провести ретельний опис телекомунікаційнного комплексу SI3000. Цей пункт є невід'ємною частиною багатьох міжнародних стандартів у галузі інформаційної безпеки. Його значимість очевидна, тому чим краще фахівець знає об'єкт котрий йому належить захищати, тим більш точну оцінку він зможе отримати [33].

На даному кроці описуються цілі створення телекомунікаційного комплексу, його межу, інформаційні ресурси, вимоги в галузі ІБ і компонентів управління телекомунікаційним комплексом і режимом ІБ.

Опис телекомунікаційного комплексу SI3000 рекомендується виконувати у відповідності з наступним планом:

- апаратні засоби комплексу SI3000, їх конфігурація;
- використовуване ПЗ та системне забезпечення;
- інтерфейси комплексу, тобто зовнішні та внутрішні зв'язки з позиції інформаційної технології;
- типи даних та інформація;
- персонал, що працює на даному телекомунікаційному комплексі (обов'язки);
- послуги і сервіси які надаються (основні цілі по впровадженню і створенню телекомунікаційнного комплексу);
- критичні типи даних та інформаційні процеси;
- функціональні вимоги до телекомунікаційного комплексу SI3000;
- категорії обслуговуючого персоналу;
- формальні вимоги в області ІБ, застосовні до даного телекомунікаційному комплексу SI3000 (законодавство, міжнародні стандарти і т.д.);
- архітектура підсистеми ІБ;

- топологія мультисервісної мережі;

- програмно-технічні засоби забезпечення ІБ;

- вхідні та вихідні потоки даних;

- система управління в даному телекомунікаційному комплексі (посадові інструкції, система планування у сфері забезпечення ІБ);

- існуюча система управління в області ІБ (резервне копіювання, процедури реагування на нештатні ситуації, інструкції з ІБ, контроль підтримання режиму ІБ і т.д.).

- організація фізичної безпеки;

- управління і контроль зовнішнім середовищем по відношенню до телекомунікаційного комплексу (кліматичними параметрами, електроживленням, захистом від затоплень, агресивного середовища і т.д.).

2.5 Висновок

Встановлено, що МСМ відносяться до 3 класу автоматизованих систем, тому для забезпечення конфіденційності, цілісності та доступності обрано стандартний функціональний профіль 3.КДЦ.1 з рівнем гарантій Г-2.

Реалізовано методику оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000. Приведена покрокова оцінка захищеності телекомунікаційного комплексу SI3000 кількісно залежно від вартості інформації, що захищається; ймовірності зламу; вартості самої системи захисту комплексу; продуктивності системи захисту інформації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є обґрунтування економічної доцільності розробки методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000, кількісно залежно від вартості інформації, що захищається; ймовірності зламу; вартості самої системи захисту комплексу. Для чого необхідно розрахувати величину капітальних та експлуатаційних витрат, визначити величину економічного ефекту, а також показники економічної ефективності щодо запропонованих рішень із забезпечення інформаційної безпеки

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні (фіксовані) витрати відображаються величину коштів, призначених для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу;

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1. Визначення витрат на підвищення рівня інформаційної безпеки підприємства шляхом розробки методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000

3.1.1.1 Визначення трудомісткості розробки методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000

Трудомісткість розробки визначається тривалістю кожної робочої операції:

$$t = t_{тз} + t_в + t_а + t_р + t_д, \text{ годин,}$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000, $t_{тз}=80$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в=30$;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а=40$;

$t_р$ – тривалість розробки методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000, $t_м=126$;

$t_д$ – тривалість підготовки технічної документації, $t_д=20$.

Отже,

$$t = 80+30+40+126+20 = 296 \text{ годин.}$$

3.1.1.2. Розрахунок витрат на підвищення рівня інформаційної безпеки підприємства шляхом розробки методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000

Витрати на розробку заходів безпеки Кпз складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки *Ззп* і вартості витрат машинного часу *Змч*:

$$К_{пз} = З_{зп} + З_{мч} = 97680 + 2516 = 100196 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 296*330 = 97680 \text{ грн.}$$

де t – загальна тривалість операцій, годин;

Зпр – средньогодинна заробітна плата спеціаліста с інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{Мч} = t \cdot С_{Мч} = 296 \cdot 8{,}5 = 2516 \text{ грн.}$$

де t – трудомісткість операцій із побудови ефективної системи доступу персоналу, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{Мч} = 0{,}8 \cdot 4 \cdot 1{,}55 + \frac{6200 \cdot 0{,}6}{1920} + \frac{7700 \cdot 0{,}4}{1920} = 8{,}5 \text{ грн.}$$

При застосуванні заходів із оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000 планується його закупівля. Вартість телекомунікаційного комплексу SI3000 визначається його специфікацією і складає 301320 грн.

Для управління телекомунікаційним комплексом SI3000 оператором МСМ необхідно пройти відповідне навчання. Вартість навчання складе

20000 ($К_{навч}$=20000 грн.). Також необхідне здійснення налагодження системи інформаційної безпеки, витрати на яке складуть 15000 грн. . ($К_н$=15000 грн.).

Таким чином, капітальні (фіксовані) витрати на підвищення рівня інформаційної безпеки підприємства шляхом розробки методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000 складуть:

$$К = 100196 + 301320 + 20000 + 15000 = 436516 \text{ грн.}$$

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad \text{грн.}$$

де $С_в$ - вартість відновлення й модернізації системи;

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки).

При застосуванні методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000, вартість модернізації системи складає 5000 грн. щорічно.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Річний фонд амортизаційних відрахувань ($С_а$) визначається прямолінійним методом, виходячи з вартості активів та строку їх корисного використання. Вартість телекомунікаційного комплексу SI3000 складає 301320 грн. Строк корисного використання – 5 років. Отже,

C_a=301320/5=60264 грн.

Віповідно до специфіки застосування телекомунікаційного комплексу SI3000 операторам МСМ необхідно мати програму навчання своїх співробітників. Така навчальна програма щодо забезпечення ІБ повинна бути розділена на кілька частин, орієнтованих на: рядових співробітників; адміністраторів та персонал, що відповідають за ІБ підсистем; керівників середньої ланки; вище керівництво з урахуванням специфіки розв'язуваних завдань. Сумарно витрати на навчання співробітників на рік складають 42000 грн.

Крім усього іншого навчання це має бути обов'язковим для всіх нових співробітників, прийнятих на роботу, і повинні розглядатися всі аспекти функціональних обов'язків службовця. Планується здійснення таких витрат на рівні 3000 грн.

Необхідно періодично перевіряти, ефективність навчання та готовність службовців до виконання дій, пов'язаних із забезпеченням ІБ, регулярно проводити для всього персоналу заняття з підвищення кваліфікації, що розповідають про нові зміни в стратегії і процедурах безпеки, а також вжити заходів після зафіксованих серйозних інцидентів. На зазначене навчання плануються витрати на рівні 6600 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 20000 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Отже,

$$С_з = 22000*12 + 22000*12*0,08= 285120 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.09.2020 р. складає 22%.

$$С_{єв} = 259200*0,22 = 62726,4 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=7,4 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,55 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 7,4*1920*1,55 = 22022,4 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% ($С_{тос}$ = 436516*0,01=4353,16 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 60264 + 42000+3000 +6600 +285120 +62726,4 +22022,4 + 4353,16 =$$
$$= 486086 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С =5000+ 486086 = 491086 \text{ грн.}$$

3.2 Оцінка можливого збитку

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 8 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 5 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 18 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 17000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 18000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 11 осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 20 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 900 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 2;

N – середнє число атак на рік, 45.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_n = \frac{18000 \cdot 20}{176} \cdot 8 = 16363{,}64 \quad \text{грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{18000 \cdot 20}{176} \cdot 18 = 36818{,}18 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{17000 \cdot 11}{176} \cdot 5 = 5312{,}5 \text{ грн.}$$

Таким чином, витрати на відновлення працездатності вузла або сегмента корпоративної мережі складають:

$$П_в = 36818{,}18 + 5312{,}5 = 42130{,}68 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{О}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{900000}{2080} \cdot (8 + 5 + 18) = 13413{,}46 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 16363,64 + 42130,68 + 13413,46 = 71907,78 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_2 \sum_{45} 71907,78 = 6471700,2 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (R=0,2);

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 6471700,2*0,2 - 491086 = 803254,04 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{\text{E}}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{803254{,}04}{436516} = 1{,}84, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (\text{N}_{\text{деп}} - \text{N}_{\text{інф}})/100),$$

де $\text{N}_{\text{деп}}$ – річна депозитна ставка, (5,5 %);

$\text{N}_{\text{інф}}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1{,}84 > (5{,}5 - 5)/100 = 1{,}84 > 0{,}005.$$

Термін окупності капітальних інвестицій T_{o} показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від

впровадження системи інформаційної безпеки. Відповідно термін окупності розробки методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{1{,}84} = 0{,}54, \quad \text{років (6,5 місяців).}$$

3.4 Висновок

Згідно з наведеними розрахунками можна дійти висновку, що розробка методики оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000, можна вважати економічно доцільною. Оскільки при капітальних витратах на рівні 436516 грн та експлуатаційних витратах на рівні 491086 на рік, можливо отримати економічний ефект у розмірі 803254,04 грн. при вірогідності реалізації загроз 20%. Термін окупності складе 0,54 року або 6,5 місяців. Коефіцієнт повернення інвестицій ROSI складає 1,84 (ROSI=1,84).

ВИСНОВКИ

В роботі розглянуто проблеми впровадження та проблеми захисту інформації в мультисервісних мережах (МСМ), види несанкціонованого доступу персоналу, що складає загрозу інформаційної безпеки в мультисервісних мережах, вплив людського фактору і проблеми авторизації в мультисервісній мережі. Наведена характеристика найбільш поширених способів реалізації загроз інформації, оброблюваної в телекомунікаційному комплексі SI3000.

В спеціальній частині реалізовано методику оцінки рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000. Приведена покрокова оцінка захищеності телекомунікаційного комплексу SI3000 кількісно залежно від вартості інформації, що захищається; ймовірності зламу; вартості самої системи захисту комплексу; продуктивності системи захисту інформації.

ПЕРЛІК ПОСИЛАНЬ

1 Журнал ИКС. Мультисервисные сети следующего поколения, 2008.

2 Владислав Шаров. Базовые технологии мультисервисных сетей / Сети и телекоммуникации, июнь 2006, №6 (94).

3 Дмитрий Чижиков. Журнал ИКС: Мультисервисные сети следующего поколения: потребности рынка, принципы, мониторинг, 2008.

4 Технический обзор Cisco “Безопасность IP-сетей нового поколения для провайдеров услуг”, 2012.

5 Електронний ресурс / Спосіб доступу: URL: http://www.tts.kiev.ua?conception.- Концепция систем NGN.

6 Телекоммуникационніе сети (Електронний ресурс).// Спосіб доступу: URL: http://rt-sit. narod.ru/ lections/11/11.html.- Конвергенция компьютерных и телекоммуникационных сетей.

7 В.Г.Аверин. Компьютерные сети и телекоммуникации - Екатеринбург, 2009.

8 Петр Чачин. NGN и пакетные мультисервисные услуги / PC Week Review, октябрь 2007, №4.

9 Владислав Шаров. Инфраструктурные технологии, июнь 2006.

10 Бакланов И.Г. NGN: принципи построения и организации / Под.ред. Ю.Н. Чернышова. – М.: Эко-Трендз, 2008. – 400с.

11 Леонид Бараш. Архитектура мультисервисных сетей / Компьютерное Обозрение 2002г, №4.

12 Дудикевич В.Б., Гарасим Ю.Р., Метод створення профілів захисту для мереж зв’язку та систем комутації, 2009.

13 Сергей Головин. Мультисервисные сети в России: поворот неизбежен / «CIO» август 2005, №39.

14 Толюпа С.В., д. т. н.; Кунах Н. І., д.т.н.. Побудова мультисервісних мереж на концепції NGN та проблеми захисту / Наукові записки УНДІЗ, 2011, №3(19).

15 Гургенидзе А.Т., Кореш В.И. Мультисервисные сети и услуги широкополосного доступа.- М.: Наука и Техника, 2003. - 400 с.

16 В.В. Босько, И.А. Березюк, Е.В. Мелешко, С.Г. Семенов. Концепция защиты информации в NGN-сетях / Системи управління, навігації та зв'язку, 2011, випуск 4(20).

17 Кузнецов О.О. Протоколи захисту інформації у комп'ютерних системах та мережах: навчальний посібник / О.О. Кузнецов, С.Г. Семенов. – Х.: ХНУРЕ, 2009. – 184 с.

18 ДБН А.2.2-2-96. Державні будівельні норми України. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва. - Держкоммістобудування України. – Київ. – 1996.

19 ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт.

20 ITU-T Recommendation X.805. Security architecture for system providing end-to-end communications. – Geneva: 2003. – 28 с.

21 КОНОНОВИЧ В.Г. Система інформаційної безпеки мультисервісних мереж / Цифрові технології , 2009, № 6.

22 SI3000 MSAN. Мультисервисный узел абонентского доступа. Разнообразие доступа / Iskratel, 2013.

23 SI3000 MSCN. Мультисервисный узел управления / Iskratel, 2013.

24 Technology. IT msan. (Електронний ресурс).// Спосіб доступу: URL: http.//fixtoolz.ru/iskratel-linejka-produktov-si3000-msan-mscp-osap.- IT Information Technology.

25 Інструкція користувача Iskratel OSAP / Голосові послуги, 2013.

26 А.А.Тимошенко. Защита информации в специализированных информационно – телекоммуникационных системах. Киев, 2010.

27 В.Г. Грибунин. Безопасность сетей NGN / Information Security, 2006.

28 Відомості про засоби забезпечення технічного захисту.(Електронний ресурс).// Спосіб доступу URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish

/article?art_id=78384&cat_id=39181&mustWords=BBO+S&searchPublishing=1.-
Відомості про засоби забезпечення технічного захисту інформації загального призначення.

29 НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”.

30 Щеглов А.Ю Защита компьютерной информации от несанкционированного доступа. – С.- Пб.: Наука и техника, 2004.- 384с.

31 НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

32 Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. — М.: Компания Айти; ДМКПресс, 2004.

33 NIST 800-30 стандарт США «Предотвращение и мониторинг инцидентов связанных с вредоносным ПО».

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	2	
3	А4	Зміст	3	
4	А4	Вступ	2	
5	А4	1 Розділ	37	
6	А4	2 Розділ	33	
7	А4	3 Розділ	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу магістра на тему:
Розробка методики оцінки інформаційної безпеки телекомунікаційного комплексу SI3000
студента групи 125м-19-2
Палія Вадима Володимировича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерела та __ додатка.

Новизна роботи полягає в реалізації процедури оцінювання рівня захищеності, та її адаптації яка виконується на базі телекомунікаційного комплексу SI3000.

Зміст та структура роботи дозволяють розкрити поставлену тему повністю.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. У роботі розглянуто проблеми впровадження та проблеми захисту інформації в мультисервісних мережах (МСМ), види несанкціонованого доступу персоналу, що складає загрозу інформаційної безпеки в мультисервісних мережах.

В спеціальній частині проаналізовані атаки на МСМ, складена модель загроз і модель порушника для даної мережі. А також обрано профіль захищеності, який гарантує цілісність, доступність і конфіденційність інформації, що передається по мережі. Реалізовано методику оцінку рівня захищеності інформації, що обробляється в телекомунікаційному комплексі SI3000.

Це підтверджує самостійність обробки даних, практичні рекомендації та висновки.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор Палій Вадим Володимирович заслуговує на оцінку «_____».

Керівник роботи

д.т.н., проф. Корнієнко В.І.