УДК 004.056.5:004.732 DOI: 10.31673/2412-4338.2022.020412

Гніденко М. П., Сєрих С. О., Захаржевський А. Г.
Державний університет телекомунікацій, Київ.

НАПРЯМКИ ОПТИМІЗАЦІЇ КОМПЛЕКСІВ ЗАХИСТУ КОРПОРАТИВНОЇ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ЗВ'ЯЗКУ

Анотація: *В статті розглянутий комплексний підхід до захисту інформації корпоративної мультисервісної мережі зв'язку, що полягає в використанні технічних, апаратно-програмних та організаційно-правових мір захисту. Визначено, що захист інформації від несанкціонованого доступу та від її витоку технічними каналами ефективніше досягається застосуванням технічних засобів.*

З метою визначення напрямків оптимізації комплексів захисту корпоративної мультисервісної мережі і загальних підходів до її здійснення розглянута модель мережі зв'язку, що побудована по ієрархічному принципу. Визначена місце корпоративної мережі в складі мережі зв'язку. Зазначено, що більш раціональним підходом до забезпечення захисту інформації слід вважати етап проектування, коли можливо передбачити і реалізувати заданий рівень захисту. Запропоновано загальний алгоритм проектування корпоративної мережі, який складається з наведених в статті етапів.

На першому етапі проведено вибір і обґрунтування загальної топології захищеної корпоративної мережі адаптованої до вимог її користувачів. Визначені напрямки комунікаційного трафіку між відправником і одержувачем інформації через мережу.

Оцінка і розрахунок інформаційних потоків з урахуванням масштабування мережі, підвищення інтенсивності та об'ємів трафіку, систематизація функцій захисту з можливістю як узагальнення так і локалізації їх є предметом подальших досліджень.

При виборі типів фізичного обладнання для забезпечення і реалізації заданих класів і функцій захисту розглянута для трьох рівнях мережі: апаратній частині серверів та робочих станціях; комунікаційному обладнання та каналах зв'язку; шлюзах, мостах і тунелях усього діаметра мережі включаючи сегменти і домени.

Визначені напрямками підвищення захисту інформації на рівнях апаратного, канального та мережевого забезпечення.

За результатами досліджень зроблено висновок, що комплексність рішень підвищення захисту інформації досягається крім технічного напрямку апаратно-програмними і організаційно-правовими.

Ключові слова: *корпоративна мультисервісна мережа зв'язку, захист інформації, несанкціонований доступ, витік інформації.*

Gnidenko N. P. Serykh S.A. Zahargevskiy A.GI.
State University of Telecommunications, Kyiv

DIRECTIONS OF OPTIMIZATION OF CORPORATE MULTISERVICE COMMUNICATION NETWORK PROTECTION COMPLEXES

Abstract: *The article considers a comprehensive approach to the protection of information of a corporate multi-service communication network, which consists in the use of technical, hardware-program, and organizational-legal measures of protection. It was determined that the protection of*

information from unauthorized access and its leakage through technical channels is more effectively achieved by the use of technical means.

In order to determine the direction of optimization of the corporate multi-service network protection complexes and general approaches to its implementation, a model of the communication network built according to the hierarchical principle is considered. The place of the corporate network in the communication network is determined. It is noted that a more rational approach to ensuring information protection should be considered the design stage, when it is possible to predict and implement a given level of protection. A general algorithm for designing a corporate network is proposed, which consists of the stages listed in the article. At the first stage, the selection and justification of the general topology of the protected corporate network adapted to the requirements of its users was carried out. The directions of the communication traffic between the sender and the recipient of information through the network are determined.

Evaluation and calculation of information flows taking into account the scaling of the network, increasing the intensity and volume of traffic, the systematization of protection functions with the possibility of both generalization and localization of them are the subject of further research. When choosing the types of physical equipment for the provision and implementation of the specified classes and functions, protection is considered for three levels of the network: the hardware part of servers and workstations; communication equipment and communication channels; gateways, bridges and tunnels of the entire diameter of the network, including segments and domains.

Identified directions for improving information protection at the hardware, channel, and network support levels.

Based on the results of the research, it was concluded that the complexity of solutions to increase information protection is achieved in addition to the technical direction by hardware-software and organizational-legal ones.

Keywords: *corporate multi-service communication network, information protection, unauthorized access, information leakage.*

Вступ

На сучасному етапі розвитку і побудови корпоративної мультисервісної мережі зв'язку застосуванню методів захисту приділяється значна увага. Особливість полягає в тому, що крім універсальних і комплексних способів захисту мереж в корпоративних мережах додатково застосовуються специфічні способи, які можуть бути вибірковою частиною комплексних із індивідуалізацією обумовленою самою структурою таких мереж та їх призначенням.

Комплексність захисту пояснюється використанням технічних, апаратно-програмних та організаційно-правових [1] мір захисту. До універсальних способів можна віднести: регламентацію процесу обміну, приховування його або інформації на основі криптографічних методів, обмеження доступу до них, дезінформацію зловмисника та розбиття, сегментацію інформації.

Аналіз літературних даних і постановка проблеми

Одним з найважливіших напрямків захисту інформації в корпоративній мультисервісній мережі вважається технічний захист інформації (ЗІ) [2] перед яким ставляться дві головних задачі - захист інформації від несанкціонованого доступу (НСД) та від її витоку технічними каналами.

При цьому під НСД слід розуміти доступ до інформації, що порушує встановлену в корпоративній мережі політику розмежування доступу, а під витоком технічними каналами розглядається використання зловмисниками побічних електромагнітних випромінювань і наводок, акустичних і оптичних приладів і каналів.

Аналіз літературних даних [3, 4] показує, що проблемам інформаційної і кібернетичної безпеки приділяється значна увага. При цьому напрямок адаптивного управління ризиками інформаційної мережі [4] для інформаційної безпеки систем загальної інфраструктури на основі запропонованої математичні моделі та новітніх технології управління технічними засобами вважаються пріоритетними.

Комплексний підхід до захисту інформації знаходить відображення [5] і в запропонованій концепції створення системи захисту на основі організаційних і програмно-технічних мір і в удосконаленні методів проектування телекомунікаційних систем та мереж в умовах реального трафіку [6] при оцінки характеристик якості обслуговування його [7] в мультисервісних мережах.

Зважаючи, що технічні засоби [4] - це спеціальне обладнання, споруди, додаткові прилади які реалізують захист, оповіщення, спостереження та відеозапис, біологічну ідентифікацію та візуалізацію, вартість їх значна. А додаючи до цього розгортання, модернізацію і регулярне обслуговування витрати стають суттєвими. Але у якості першої і головної межі захисту від зловмисника, самою дієвою. Крім того функціонування решти засобів захисту інформації (ЗІ), так чи інакше, ґрунтується саме на технічних засобах.

Тому головною задачею роботи слід вважати визначення напрямків удосконалення та застосування технічних засобів ЗІ які доцільно використовувати у тієї частини мережі за яку відповідають корпоративні служби.

Мета і задачі дослідження

З метою визначення напрямків оптимізації комплексів захисту корпоративної мультисервісної мережі і загальних підходів до її здійснення доцільно розглянути модель мережі зв’язку, що застосовує ієрархічний принцип побудови.

Задачі дослідження це:

- для розподілу завдань і відповідно обладнання для захисту інформації провести оцінку місця корпоративної мультисервісної мережі у складі загальної мережі зв’язку;
- оскільки на вибір технічних засобів ЗІ впливає топологія мережі – розглянути типову модель корпоративної мультисервісної мережі;
- визначитись із напрямками удосконалення обладнання на кожному рівні моделі і ступенем захисту інформації в мережі.

Основна частина

Сучасні корпоративні мережі обов’язково мають вихід до мереж загального користування і глобальної мережі Internet. Тому їх можна розглядати як деяку складову великої мережі зв’язку із розповсюдженням загальних принципів на окремі складові. Великі мережі за рахунок принципу інтеграції складні, оскільки визначаються безліччю протоколів, конфігураціями та технологіями. За допомогою ієрархії можна впорядкувати всі компоненти в моделі, що полегшує аналіз, а застосовуючи підхід декомпозиції деталізувати вимоги до окремих напрямків таких як захист інформації, що і є метою дослідження.

Модель, яка представлена на рис. 1, визначає характеристики кожного ієрархічного рівня, що допомагає у розробці, впровадженні та обслуговуванні масштабованих, надійних, захищених та ефективних у вартісному виразі об'єднаних мережах. Три ієрархічні рівні моделі передбачають розподіл специфічних мережевих функцій.

Ядро мережі це верхній базовий рівень ієрархії, який відповідає за швидке та надійне пересилання трафіку великого обсягу. Самі дані користувача обробляються на рівні розподілу, який при необхідності пересилає запити до ядра. Тому для забезпечення вимог QoS по швидкості і затримці пакетів перед рівнем ставиться завдання швидкої комутації потоків від

значної кількості користувачів. Помилка або відмова на цьому рівні впливова для усіх користувачів. Для рівня ядра велике значення має його стійкість до відмови, оскільки збій на цьому рівні може призвести до втрати зв'язності мережі.

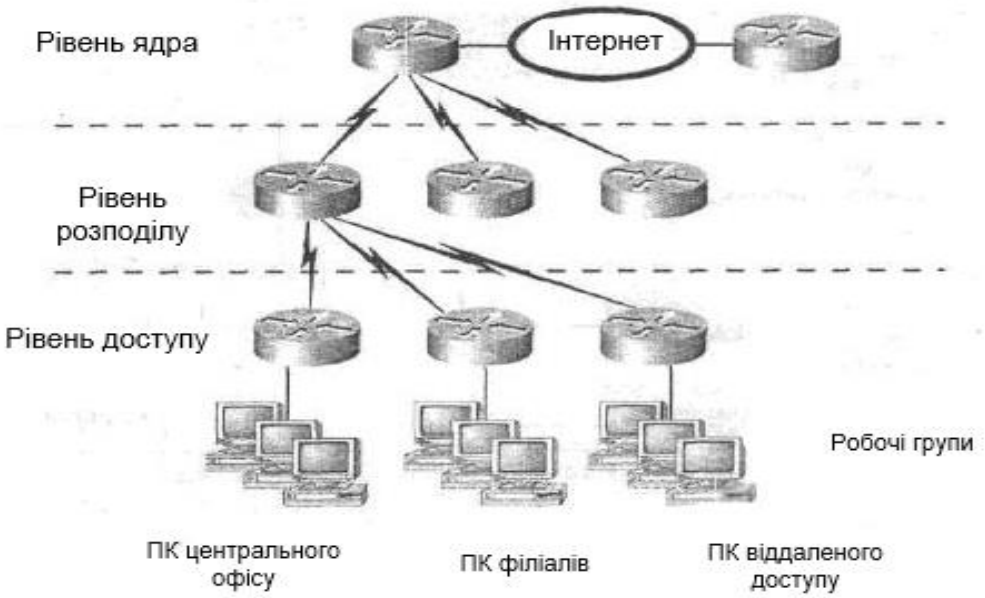

Рис. 1 Трьохрівнева ієрархічна модель мережі зв’язку

Отже, важливо забезпечити високу надійність і захист від перешкод на рівні ядра. Тому особливостями його реалізації слід вважати наступні:

- Ніщо не повинно сповільнювати трафік, включаючи списки доступу, маршрутизацію між віртуальними локальними мережами VLAN та фільтрацію пакетів.
- З метою підвищення захисту функції доступу не повинні розповсюджуватись на всі та всю робочі групи корпоративної мережі.
- У разі необхідності підвищення продуктивності рівня раціонально обирати не розширення, а модернізацію обладнання застосовуючи екстенсивний шлях розвитку мережі,
- Необхідно застосовуючи інженірінг провести оцінку навантаження від користувачів і реалізувати запас за пропускною здатністю рівня щоб забезпечити мінімальну затримку.
- Потрібно використовувати протокол маршрутизації з малим часом конвергенції.

Швидкі та надмірні підключення на канальному рівні не допомагають при некоректних таблицях маршрутизації!

Розташований між рівнем ядра та рівнем доступу рівень розподілу ще називають рівнем робочих груп. Основні функції цього рівня маршрутизація, фільтрація та забезпечення доступу до регіональних мереж. Рівень розподілу повинен встановлювати найшвидший спосіб обробки запитів до служб (наприклад, метод файлового звернення до сервера). Після визначення лише на рівні найкращого шляху доступу, запит може бути переданий на вищій рівень, де реалізований швидкісний транспорт запиту до потрібної службі. Тобто можливо відзначити, що рівні встановлюється політика мережі, а також забезпечуються можливості гнучкого опису мережевих операцій. На рівні поширення виконується кілька функцій:

• Реалізація інструментів, подібних до списків доступу, фільтрації пакетів або механізму запитів.

• Реалізація системи безпеки та мережевих політик, включаючи трансляцію адрес та встановлення брандмауерів.

• Перерозподіл між протоколами маршрутизації, включаючи використання статичних шляхів.

• Маршрутизація між мережами VLAN та іншими функціями підтримки робочих груп.

• Визначення доменів широкомовних та багатоадресних розсилок.

На рівні розподілу не слід покладати ті функції, які властиві двом іншим рівням. Ніщо не повинно сповільнювати трафік, включаючи списки доступу, маршрутизацію між віртуальними локальними мережами VLAN та фільтрацію пакетів.

• Для захисту використовувати функції доступу для робочої групи недоцільно.

• При зростанні розмірів об'єднаної мережі (наприклад, при додаванні маршрутизаторів) необхідно вимкнути розширення рівня ядра.

На рівні доступу реалізовано управління користувачами та робочими групами під час звернення до ресурсів об'єднаної мережі. Іноді рівень доступу називають рівнем настільних систем або ПК. Найбільша частина необхідних користувачам мережевих ресурсів має бути доступна локально. На рівні розподілу виконується перенаправлення трафіку до віддалених служб. Для рівня доступу характерні такі функції:

- керування доступом користувачів, фільтрація трафіку, забезпечення якості обслуговування (QoS);
- підключення робочих груп до рівня розподілу та сегментація мережі;
- постійний контроль (з рівня розподілу) за доступом та політиками захисту.
- формування незалежних доменів конфліктів;
- використання технології комутованих локальних мереж.

Рівень доступу керує доступом користувачів та робочих груп до ресурсів об'єднаної мережі. Основним завданням рівня доступу є створення точок входу/виходу користувачів у мережу.

Зазвичай на рівні доступу використовуються технології Dialon-Demand Routing (DDR)– маршрутизація з викликом у міру необхідності) і Ethernet. Не слід додавати нові маршрутизатори нижче рівня доступу. Такі дії призводять до збільшення діаметра мережі, що порушить передбачуваність топології. Тут можна побачити статичну маршрутизацію (замість протоколів динамічної маршрутизації).

Три окремих рівня пов'язані з трьома спеціальними типами маршрутизаторів. Цих пристроїв може бути менше або більше, але завжди потрібно пам'ятати про розділення мережевих функцій за рівнями моделі.

Три рівні необов'язково припускають наявність трьох різних пристроїв. Якщо провести аналогію з ієрархічною моделлю OSI, то окремий протокол не завжди відповідає одному з семи рівнів. Іноді протокол відповідає більш ніж одному рівню моделі OSI, інколи ж кілька протоколів реалізовані в рамках одного рівня. Так і при побудові ієрархічних мереж, на одному рівні може бути як кілька пристроїв, так і один пристрій, що виконує всі функції, визначені двох сусідніх рівнях.

Із аналізу цієї моделі доцільно визначити, що корпоративна мультисервісна мережа зазвичай забезпечує рівень доступу і у багатьох випадках перехоплює початкові функції рівня розподілу бо є невід'ємною частиною мережі зв’язку.

Разом з тим задача забезпечення комплексного ЗІ розмежована. Частина її покладається на загальну мережу зв’язку, а інша є завданням корпоративної мережі, що і представляє предмет дослідження. При цьому впливовим фактором на розв’язання завдання захисту стає топологія мережі. Більш раціональним підходом до забезпечення ЗІ слід вважати етап проектування, коли можливо передбачити і реалізувати заданий рівень захисту. Тоді алгоритм проектування корпоративної мережі доцільно розділити на декілька етапів.

- Вибір і обґрунтування загальної топології захищено корпоративної мережі адаптованої до вимог її користувачів.
- Оцінка і розрахунок інформаційних потоків з урахуванням масштабування мережі, підвищення інтенсивності та об’ємів трафіку.
- Систематизація функцій захисту з можливістю як узагальнення так і локалізації їх.
- Введення і моніторинг класів захищеності корпоративної мультисервісної мережі.
- Вибір фізичного обладнання для забезпечення і реалізації заданих класів і функцій захисту.

Узагальнену топологічну модель мультисервісної корпоративної мережі можливо представити так - рис. 2. В моделі показані декілька робочих груп, що відповідають територіальному розподілу за дислокацією користувачів поширюючи діаметр мережі. До складу доменів мережі входять сервери контролери доменів (СКД), поштові сервери (ПС) як складові рівня розподілу, FTP-сервер з комп'ютерним програмним забезпеченням, що складається з однієї або декількох програм, які можуть виконувати команди, транслювати дані віддаленим клієнтом, такі як отримання, відправлення, видалення файлів, створення або видалення каталогів, SQL сервери як система управління реляційними базами даних, яка використовується для роботи з базами даних розміром від персональних до великих баз даних масштабу корпорації і відповідають рівню доступу. У якості кінцевого обладнання представлені персональні комп’ютери (ПК) або робочі місця користувачів послугами мережі, мобільні пристрої користувачів для підтримання технології BYOD. Між мережевий екран є межею доступу до ядра і відповідно розподілу функцій ЗІ.

Аналіз моделі дозволяє визначитись із містом використання обладнання яке на фізичному рівні дозволяє забезпечити захист інформації та визначитись із потоками її для подальшого аналізу протидії НСД і витоку технічними каналами.

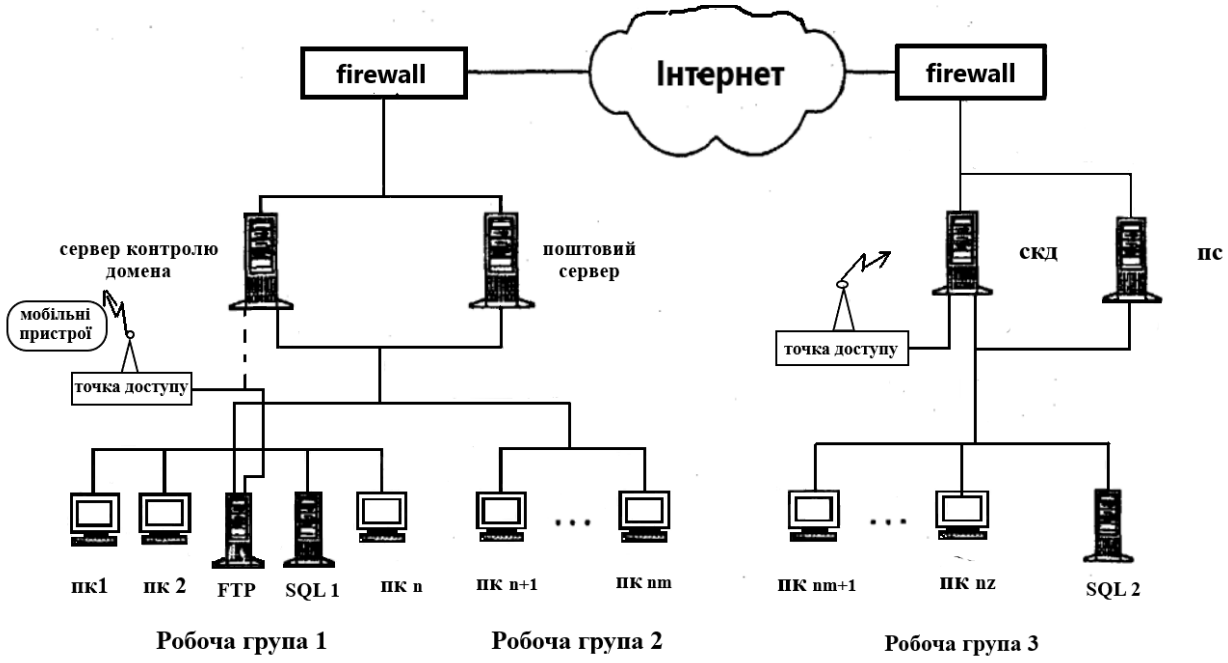

Рис. 2 Топологічна модель мультисервісної корпоративної мережі

Комунікаційний трафік між відправником і одержувачем інформації через мережу може бути наступним.

1. Внутрішній інформаційний потік в робочої групи.
2. Інформаційний потік між робочими групами в нутрі домену.

3. Інформаційний потік між робочими групами із використанням незахищеної зовнішньої мережі,
4. Зовнішній вхідний потік до користувачів корпоративної мережі.

В умовах реалізації достатнього рівня ЗІ корпоративної мережі загрозу можуть представляти два останніх шляхи, коли задіяна зовнішня мережа. Напрямками підвищення ЗІ перших двох слід вважати реалізацію видів функцій захисту: ідентифікація, аутентифікація, аудит, контроль цілісності, проксі-технологія та трансляція мережевих адрес і шифрування інформації. Використання тих чи інших функцій з цього набору залежить від рівня захищеності системи і обраної топології мережі.

На фізичному рівні захист від НСД повинен здійснюватись на трьох рівнях мережі: апаратній частині серверів та робочих станціях; комунікаційному обладнання та каналах зв'язку; шлюзах, мостах і тунелях усього діаметра мережі включаючи сегменти і домени.

Напрямками підвищення ЗІ на рівні апаратного забезпечення слід обирати:

- апаратні ключі, наприклад, електронний замок із ключем на базі smart-карти, що реалізується на мікропроцесорі;
- системи сигналізації із застосуванням та криптографічних протоколів аутентифікації;
- засоби блокування пристроїв та інтерфейсів вводу-виводу інформації.

На мережевому рівні доцільно використовувати:

- між мережеві екрани для блокування атак з зовнішнього середовища, що керують проходженням мережевого трафіку відповідно до встановлених правил захисту.
- системи виявлення втручань — для виявлення спроб НСД як ззовні, так і всередині мережі. Це спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою внаслідок атаки й витрат на підтримку працездатності мережі.
- засоби створення віртуальних приватних мереж — для організації захищених каналів передачі даних через незахищене середовище.
- засоби аналізу захищеності — для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації. Це дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

Іншим напрямком підвищення ЗІ, які підлягають подальшому дослідженню можна рахувати апаратно-програмні і організаційно правові [1-3, 8]. Це комплекси спеціальних методів ЗІ, що включають автономні програми захисту та контролю захищеності, програми обробки і захисту, що працюють у комплексі з апаратними пристроями захисту, наприклад, переривають роботу ПК при порушенні системи доступу, стирають дані при несанкціонованому вході в базу даних. Вибір і обґрунтування організаційно-правових засобів залежить від специфіки компанії, можливостей та архітектури телекомунікаційної мережі, необхідного рівня захисту та впливу ролі людського фактора у роботі системи. Серед головних зазначаються - керування доступом персоналу до системи. контроль стану технічних та апаратно-програмних засобів ЗІ, розробка та контроль дотримання правил обробки інформації, підбір лояльних кадрів, організація контролю над спробами НСД до інформації, збоями та відмовами.

В даний час на ринку представлено велику різноманітність апаратно-програмних засобів захисту, які умовно можна розділити на декілька груп:

- засоби, що забезпечують захист від впливу програм-вірусів:
- засоби, що забезпечують розмежування доступу до інформації;
- матеріали, що забезпечують безпеку зберігання, транспортування носіїв інформації та захист їх від копіювання;
- засоби, що забезпечують захист інформації під час передачі її каналами зв'язку;

• засоби, що забезпечують захист від витоку інформації щодо акустичних та електромагнітним полям, які виникають при роботі технічних засобів.

Крім того доцільно зазначити про застосування сучасних методів криптографічного перетворення даних як найбільш ефективних засобів забезпечення конфіденційності, цілісності та достовірності інформації в процесі її зберігання, обробки та передачі по каналах зв'язку. Використання криптографічних засобів захисту в сукупності з необхідними технічними та організаційно-правовими заходами дозволяє забезпечити надійний захист інформації в мережі від широкого спектра загроз.

Вибір складу комплексних засобів захисту може бути здійснений рішенням оптимізаційної задачі, сформульованої на основі побудованої моделі дій зловмисника.

Висновки

При побудові корпоративних мультисервісних мереж визначну роль відіграє правильний вибір архітектури і топології мережі, який повинен передбачати багаторівневий підхід. Він полягає в поданні архітектури створюваної мережі у вигляді ієрархічних рівнів, кожен з яких вирішує певні для цього рівня завдання.

Це дозволяє масштабувати мережу, удосконалювати її розширюючи функціональні можливості, мінімізувати ресурсні витрати для пошуку і усунення відмов та наслідків негативного впливу зловмисників.

Найважливішим напрямком захисту інформації в корпоративній мультисервісній мережі вважається технічний захист інформації на апаратному і канальному рівнях, перед яким ставляться дві головних задачі - захист інформації від несанкціонованого доступу та від її витоку технічними каналами.

Комплексним рішенням підвищення ЗІ крім технічного слід реалізовувати напрямки апаратно-програмні і організаційно правові, які вимагають подальшого дослідження.

Список використаної літератури

1. Ложковський, А.Г. Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання. – Видання друге (доповнене) / А.Г. Ложковський, П.П. Воробієнко, С.О. Довгий, К.Д. Гуляєв; К.: «Азимут-Україна». – 2013.

2. Ворбієнко П.П. Телекомунікаційні та інформаційні мережі. Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.

3. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

4. Косенко В. В., Персіянова О. Ю. Адаптивне управління ризиками інформаційної мережі для інформаційної безпеки систем критичної інфраструктури. Математичні моделі та новітні технології управління економічними та технічними системами: Монографія / за заг. ред. В. О. Тімофєєва, І. В. Чумаченко. Харків. 2017. С. 284-301.

5. Букет Д.А. Управління інформаційною безпекою за допомогою комплексної системи захисту / Д.А. Букет // ДУТ, Сучасний захист інформації. – 2022. -№1(49). - С 56-60.

6. Ложковський А.Г. Методи проектування телекомунікаційних систем та мереж в умовах реального трафіка / А.Г. Ложковський, В.М. Колчар, В.Ю. Гордієнко, О.В. Вербанов // Наукові праці ОНАЗ ім. О.С. Попова. – 2014. – №2. – С.54-63.

7. Соловська І.М. Оценка характеристик качества обслуживания разнородного трафика в мультисервисной сети / І.М. Соловська, І.В. Стрелковська // Цифрові технології. Збірник наукових праць. – 2013. – №13. – С.34-41.

8. Mukhin V., Romanenkov Yu., Bilokin Ju., Rohovyi A., Kharazii A., Kosenko V., Kosenko N., Jun Su. The Method of Variant Synthesis of Information and Communication Network Structures

on the Basis of the Graph and Set-Theoretical 12 Models. International Journal of Intelligent Systems and Applications (IJISA). 2017. Vol. 9. No. 11. P. 42-51.

References

1. Lozhkovskyi, A.H. Modern telecommunications: Networks, technologies, security, economy, regulation. – Second edition (amended) / A.H. Lozhkovskyi, P.P. Vorobienko, S.O. Dovgyi, K.D. Gulyaev; K.: "Azimuth-Ukraine". - 2013.

2. Vorbienko P.P. Telecommunication and information networks. Textbook [for higher educational institutions] / P.P. Vorobienko, L.A. Nikityuk, P.I. Reznichenko. - K.: SAMMIT-Knyga, 2010. - 708 p.

3. Information and cyber security: socio-technical aspect: textbook / [V. L. Buryachok, V. B. Tolubko, V. O. Khoroshko, S. V. Tolyupa]; in general ed. Dr. Tech. of Sciences, by Professor V. B. Tolubka.— K.: DUT, 2015.— 288 p.

4. Kosenko V.V., Persiyanova O.Yu. Adaptive risk management of the information network for information security of critical infrastructure systems. Mathematical models and the latest technologies of management of economic and technical systems: Monograph / by general. ed. V. O. Timofeeva, I. V. Chumachenko. Kharkiv. 2017. P. 284-301.

5. Bouquet D.A. Managing information security using a comprehensive protection system / D.A. Bouquet // DUT, Modern information protection. – 2022. - No. 1(49). - C 56-60.

6. A.H. Lozhkovskyi Design methods of telecommunication systems and networks under real traffic conditions / A.H. Lozhkovskyi, V.M. Kolchar, V.Yu. Gordienko, O.V. Verbanov // Scientific works of ONAZ named after O.S. Popova – 2014. – No. 2. - C.54-63.

7. I.M. Solovska Evaluation of the characteristics of the quality of service of heterogeneous traffic in a multiservice network / I.M. Solovska, I.V. Strelkovska // Digital technologies. Collection of scientific works. – 2013. – No. 13. - C.34-41.

8. Mukhin V., Romanenkov Yu., Bilokin Ju., Rohovyi A., Kharazii A., Kosenko V., Kosenko N., Jun Su. The Method of Variant Synthesis of Information and Communication Network Structures on the Basis of the Graph and Set-Theoretical 12 Models. International Journal of Intelligent Systems and Applications (IJISA). 2017. Vol. 9. No. 11. P. 42-51.