МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Одарченко Р.С.
“_____”_____2021 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Організація безпеки мережі підприємства з використанням операційної системи Linux»

Виконавець: _____ Кошелівський В. О.
(підпис)

Керівник: _____ Мачалін І. О.
(підпис)

Нормоконтролер: _____ Бахтіяров Д. І.
(підпис)

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Одарченко Р.С.
“_____”_____2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

Кошелівського Владислава Олександровича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломної роботи (проекту): «Організація безпеки мережі підприємства з використанням операційної системи Linux»
затверджена наказом ректора від «06» квітня 2021 р. №559 / ст
2. Термін виконання роботи: з 17.05.2021 р. по 20.06.2021 р.
3. Вихідні дані до роботи: корпоративна мережа підприємства, операційна система Linux Suse
4. Зміст пояснювальної записки: спроектована корпоративна мережа підприємства; налаштування параметрів безпеки операційної системи Linux на базі ядра 5.0
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: приклад налаштування вбудованого в ядро операційної системи Linux брандмауера; схема розміщення мережевого устаткування; слайди презентації в програмному пакеті MS PowerPoint

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів диплому	17.05.2021-20.05.2021	Виконано
2	Вступ	21.05.2021-22.05.2021	Виконано
3	Назва першого розділу	23.05.2021-27.05.2021	Виконано
4	Назва другого розділу	28.05.2021-03.06.2021	Виконано
5	Назва третього розділу	04.06.2021-09.06.2021	Виконано
6	Усунення недоліків дипломної роботи	10.06.2021-14.06.2021	Виконано

7. Дата видачі завдання: “26" квітня 2021 р.

Керівник дипломної роботи _____ Мачалін І. О.
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Кошелівський В. О.
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Дипломна робота «Організація безпеки мережі підприємства з використанням операційної системи Linux» містить 67 сторінок, 13 рисунків, 6 таблиць, 14 використаних джерел.

БРАНДМАУЕР, ОПЕРАЦІЙНА СИСТЕМА, БЕЗПЕКА ДАННИХ, СЕРВЕР.

Об’єкт дослідження – інформаційна безпека корпоративної мережі малого підприємства.

Предмет дослідження – програмний брандмауер на базі операційної системи Linux.

Мета дипломної роботи – побудова захищеної корпоративної мережі малого підприємства з використанням програмних рішень захисту інформації вбудованих в ядро операційної системи Linux.

Метод дослідження – методи комп’ютерного моделювання.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

АБ - адміністратор безпеки

АД - адміністратор баз даних

АРМ - автоматизоване робоче місце

БД - база даних

ІО - інформаційний об’єкт

ІТС - інформаційно-телекомунікаційна система

КЗЗ - комплекс засобів захисту

СЗІ - система захисту інформації

ЛОМ - локальна обчислювальна мережа

МПД - мережа передачі даних

НСД - несанкціонований доступ

ОС - операційна система

ПЗ - програмне забезпечення

СА - системний адміністратор

СКБД - система керування базами даних

ТЗ - технічне завдання

ЦБД - централізована база даних

ЦВ - центральний вузол

ВСТУП

Актуальність теми. Комп'ютерна мережа – це система спільного використання інформації, яка складається принаймні з двох комп'ютерів, що взаємодіють один з одним. В першу чергу постає питання безпеки вашої інформації або вашого комп'ютера. Безпека є одним з найбільш важливих питань, що розглядаються при установці ПК в мережі. Правильний підхід до безпеки позбавить вас від неприємностей, заощадить вам багато часу і грошей. Важливо, щоб зловмисники не могли увійти в систему, а дані та послуги були доступні будь-кому, хто відповідає критерію права доступу до них. Оскільки великими мережами важко керувати, розбиття мережі на більш дрібні частини може бути кращим способом роботи з усією системою. Для кожної системи, яка піддасться загрозам, необхідно визначити етапи захисту, а також засоби їх реалізації [1-14]. Необхідно вирішити, які частини системи є найбільш важливими, захистити сервіси і дані. Система може бути атакована різними способами, і безпека мережі означає саме те, що може статися і як це запобігти.

Атаки можуть бути згруповані в кілька категорій:

Фізичні атаки – можуть відбутися в будь-який час доби, коли людина отримує фізичний доступ до комп'ютерної системи. Фізична атака може полягати, наприклад, в тому, що хтось, сидячи на файловому сервері, перезапускає машину, копіюючи ваш вихідний код [2, 6].

Атаки на сервіси – реалізується через закидання мережевих портів запитами на підключення (DDoS) , щоб відключити поштовий сервер. В обох випадках кінцевим результатом є те, що законні виклики служб не контролюються через ті, які викликають проблеми в результаті атаки або "заморожують" весь сервер. Організаторів таких атак дуже важко відстежити, так як системи атаки зазвичай використовують підроблені IP-адреси або вкрадені облікові записи [6].

Атака на права доступу – коли хтось намагається отримати права доступу в системі або отримати доступ до спеціальних облікових записів користувачів, які їм заборонено використовувати. Це може бути зловмисник, який намагається отримати

права доступу кореневого користувача (адміністратора), щоб прикинутися, що у нього проблеми, або хтось із зовнішньої мережі, який намагається отримати доступ до файлів [6]. Кількість атак може бути невеликою, але адміністратор, який піклується про безпеку, винен у запобіганні появи очевидних дірок в безпеці.

Мета – побудова захищеної корпоративної мережі малого підприємства з використанням програмних рішень захисту інформації вбудованих в ядро операційної системи Linux.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Аналіз програмно-апаратних рішень для побудови захищених корпоративних мереж.
2. Аналіз технологій та топологій для побудови корпоративних телекомунікаційних мереж.
3. Побудова телекомунікаційної корпоративної мережі малого підприємства.
4. Організація безпеки корпоративної мережі малого підприємства з використанням операційної системи Linux.

Об'єктом дослідження – інформаційна безпека корпоративної мережі малого підприємства.

Предметом дослідження – програмний брандмауер на базі операційної системи Linux.

Методи досліджень. Методи комп'ютерного моделювання.

Практичне значення отриманих результатів.

Результати дипломної роботи можна використовувати при побудові корпоративних мереж для малих підприємств у разі забезпечення інформаційної безпеки відносно дешевими способами.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2021 р.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ДЛЯ ПОБУДОВИ ЗАХИЩЕНИХ МЕРЕЖ

1.1. Загальні положення щодо організації безпеки мереж

Існує безліч спеціальних захисних пристроїв. Це можуть бути спеціальні карти, наприклад, карти брандмауера PCI-E і 3Com Firewall PC, які встановлюються в стандартні шини PCI-E або PCI і використовуються замість звичайних мережевих адаптерів Fast Ethernet. Виконання функцій безпеки передається процесору карти брандмауера, що дозволяє підвищити продуктивність системи. Плати брандмауера можуть функціонувати незалежно від операційної системи, встановленої на клієнтських комп'ютерах, і практично невразливі для атак з Інтернету, дій кінцевих користувачів або шкідливих програм [1].

1.2. Stronghold Firewall, версія 2.0

Брандмауер Stronghold Firewall версії 2.0 – це апаратно-програмний пакет, заснований на платформі Intel Core ™ і керований спеціально розробленою операційною системою. У типовій конфігурації екран Stronghold Firewall має 4 інтерфейси Ethernet basetx 100/1000. В одному пристрої можна підтримувати до 16 інтерфейсів Ethernet або X21), який підтримує P2P, PPP, HDLC і Frame Relay. На передній панелі комплексу розташований рідкокристалічний дисплей і діагностичні індикатори, що використовуються для отримання інформації про діагностику, версії програмного та апаратного забезпечення, IP-адресу, стан, конфігурацію, завантаження інтерфейсу і т.д. [2]. Це безумовно полегшує діагностику можливих проблем, а також дозволяє нетехнічному персоналу надавати інформацію адміністратору в разі виникнення проблем. Комплекс Stronghold Firewall забезпечує захищену, надійну та ефективну взаємодію мережі Інтернет та інтрамережі завдяки по-

тужному і гнучкому механізму IP-маршрутизації з вбудованою функцією фільтрації пакетів, механізмом перетворення адрес (NAT) і шлюзу додатків. Використання модульної архітектури на базі платформи Intel Core ™ і шини PCI-E захищає ваші інвестиції, забезпечуючи перехід на нові технології за рахунок зміни версії інтерфейсного модуля і керованої операційної системи [2].

Рис. 1.1. Програмно-апаратний комплекс Stronghold Firewall

1.3. Комплекс міжмережевого екранування "FPSU-IP"

Даний програмно-апаратний комплекс також є організатором VPN з'єднання для інформаційних систем, що використовують стек власних сертифікованих протоколів FPSU-IP або TCP/IP. Він володіє високими експлуатаційними характеристиками (за рахунок ефективної реалізації наскрізного стиснення даних), що ставить даний комплекс в розряд самих передових рішень по відношенню до вітчизняних та імпортних продуктів для організації VPN з'єднань [2].

Якщо інші засоби організації VPN, виконані на основі типових алгоритмів (наприклад, протокол SKIP), характеризуються досить значним зниженням швидкості IP-взаємодії за рахунок введення надмірності в кожному пакеті передачі, то при використанні комплексу "FPSU-IP" мінімізується надмірність переданої інформації, що також забезпечує збільшення швидкості передачі.

Рис. 1.2. Програмно-апаратний комплекс "FPSU-IP"

1.4. Продукти серії Cisco PIX

Апаратним вирішенням проблеми мережевої безпеки є серія продуктів Cisco PIX (Private Internet Exchange). Програмне забезпечення Cisco PIX є пропрієтарною розробкою для систем Cisco і не засноване на будь-яких клонах Unix, що дозволило мати мінімальні вимоги до дисків (в Cisco PIX замість дисків використовується SSD накопичувачі) і оперативної пам'яті SODIMM DDR4, а використання унікального алгоритму ASA (adaptive security algorithm) забезпечило продуктивність понад 64 000 одночасних сеансів, що на даний момент недосяжно жодним з брандмауерів на базі Unix або Windows NT [12].

Можливості комплексу [12]:

- Безпека, заснована на технології контролю, що захищає мережеві підключення, дозволяє заборонити несанкціонованим користувачам доступ до мережевих ресурсів.
- Технологія перехоплення з'єднань на рівні додатків дозволяє аутентифікувати користувачів з використанням стандартних протоколів tacac + і radius.
- Підтримує більше 16 000 одночасних підключень.
- Зручний і простий менеджер брандмауерів забезпечує просте адміністрування декількох брандмауерів.

- Реалізація підтримки протоколу тунелювання Microsoft Point-to-Point (PPTP) віртуальної корпоративної мережі (VPN).
- Oracle SQL * підтримка протоколу. NET для додаткової безпеки клієнт / сервер.
- Командний інтерфейс, характерний для систем Cisco IOS.
- Висока надійність за рахунок можливості дублювання і гарячого очікування.
- Перетворення мережевих адрес (NAT) відповідно до RFC 1631.
- Перетворення портів (PAT) дозволяє розширити пул адрес компанії - через одну IP-адресу ви можете відображати до 64 000 адрес (16 384) одночасно).
- Псевдоніми мережевих адрес дозволяють зіставляти IP-адреси, які перекриваються в одному і тому ж адресному просторі.
- Для зареєстрованих IP-адрес ви можете скасувати режим трансляції адрес, який дозволяє користувачам використовувати свою реальну адресу.
- Прозора підтримка всіх поширених служб TCP / IP-www, FTP, Telnet.
- Підтримка типів мультимедійних даних з перекладом адрес і без нього, включаючи RealAudio від progressive networks, streamworks від Xing technologies, Qsem від White Pines, інтернет-телефон vocal TEC, videolive від VideoNet, netshow від Microsoft, веб-театр vxtreme 4.
- Підтримка доповнень для роботи з відеоконференціями, сумісних зі специфікацією 323, включаючи Інтернет-відеотелефон (Intel) і netmeeting.
- Можливість фільтрації потенційно небезпечних Java-аплетів.
- Захищена система реального часу.
- Підтримка декількох рівнів входу в систему.
- Підтримка перехоплень (пасток) протоколу SNMP.
- Збір аудиту за допомогою утиліти системного журналу.
- Підтримка інформаційної бази управління для системного журналу (MIB).
- Аудит використання URL-адрес і обмінів по протоколу FTP.
- Підтримка віддаленого виклику процедур (RPC).

- Програма управління поштовим трафіком дозволяє заборонити статус зовнішнього поштового сервера в демілітаризованій зоні (DMZ).
- Захист від атак sin захищає хост від таких атак, як "відмова в обслуговуванні"
- Потоковий протокол забезпечує підтримку NetBIOS для взаємодії між клієнтом і сервером.

Рис. 1.3. Брандмауер серії Cisco PIX

1.5. Криптомаршрутизатор

Криптомаршрутизатор – комплекс програмних і апаратних засобів, що забезпечують безпечну передачу потоків IP-даних по каналах Інтернету / Інтранету та призначених для захисту даних, що містять особисту інформацію.

Криптомаршрутизатор в IP-мережі має вузол для криптографічної обробки даних і забезпечує прийом даних, відправлених користувачами, що працюють на одній з робочих станцій локальної мережі, шифрування цих даних і їх безпечну передачу на аналогічний Криптомаршрутизатор через відкриту IP-мережу, яка розшифровує отримані дані і розподіляє їх одержувачу – користувачеві, що працює на PC локальної мережі [2].

Передача даних здійснюється за допомогою власної сертифікованої технології CryptoLocker по виділених або комутованих телефонних каналах зв'язку відповідно до протоколів PPP, P2P або P2MP, а також по каналах локальної мережі (протоколи TCP/IP) і каналах мереж комутації пакетних даних відповідно до рекомендацій ITU-T X25.

Криптомаршрутизатор шифрує потік даних, що проходить через нього відповідно до протоколу, що дозволяє приховати інформацію про реальних суб'єктів обміну і прикладних протоколах користувача, які вони використовують у відкритій IP-мережі.

1.6. Брандмауер на базі ядра ОС Linux

IP-брандмауер (ядро 5.0). Перше покоління IP-брандмауерів для Linux з'явилося ще в ядрі 1.1 і удосконалювалось з покоління в покоління. Це була версія BSD брандмауера IPFW для Linux (автор Алан Кокс). Підтримка брандмауерів іншого покоління з'явилася в ядрі 2.0 (автори Хосе Вос, Полін Мідлінк та інші), і з цього моменту стало можливим дійсно працювати з брандмауером в Linux [14].

Ланцюжок IP-брандмауерів (ядро 2.2). Більшість аспектів сучасних дистрибутивів Linux еволюціонують, щоб задовольнити потреби користувачів, які ростуть. IP-брандмауер не є винятком. Традиційна версія IP-брандмауера підходить для більшості прикладних програм, але може бути відключена для налаштування складних середовищ. Для вирішення цієї проблеми був розроблений новий метод налаштування IP-брандмауера і пов'язаних з ним властивостей. Цей новий метод був названий "ланцюгом IP-брандмауера" і вперше був випущений для загального використання ще в ядрі Linux 2.2.0.

IP-брандмауер розроблений Ченом Полом Расселом і Майклом Ньюлінгом. Ланцюжок IP-брандмауерів дозволяє розробляти класи правил брандмауера, в яких можна додавати і видаляти комп'ютери або мережі. Цей підхід може підвищити продуктивність брандмауера в конфігураціях з великою кількістю правил [14].

Ланцюжок IP-брандмауера підтримується ланцюжком ядра 2.2-4.4 і доступний в якості виправлення для ланцюжка ядра 2.0. * Howto пояснює, де отримати патч, і дає велику кількість корисних порад про те, як використовувати утиліту Налаштування ipchain.

Netfilter і таблиця IP (ядро 5.0). При розробці ланцюга IP-брандмауерів Пол Рассел вирішив, що IP-брандмауери легко скомпрометувати. Він почав покращувати код фільтра і створив пакет, який виявився набагато простішим і потужнішим. Це Netfilter.

Отже, що ж було не так з ланцюжком IP-адрес? Вони значно підвищили ефективність і управління правилами брандмауера. Але вони обробляли всі пакети набагато довше, особливо в поєднанні з іншими можливостями брандмауера, такими як імітатори IP та інші форми перетворення адрес. Частково ця проблема виникла через те, що IP-маскування (IP masking) і перетворення мережевих адрес (Network Address Translation) були розроблені незалежно від IP-брандмауера і згодом інтегровані в нього.

Однак були й інші проблеми. Зокрема, набір правил введення, що описував весь вхідний потік IP-рівня в цілому. Цей набір вплинув як на ті пакети, які призначені для цього комп'ютера, так і на ті, які будуть передані їм. Це було неправильно, тому що такий підхід плутав функцію ланцюжка введення з функцією прямого ланцюжка, яка застосовувалася тільки до результуючого пакету. Існували дуже складні конфігурації для різної обробки вхідних і широкомовних пакетів.

Інша проблема полягала в тому, що механізм фільтрації розташовувався безпосередньо в ядрі системи, і неможливо було змінити логіку її роботи без радикального порушення всього ядра. Так з'явився Netfilter з виходом язра 5.0, який дозволяє вбудовувати в ядро додаткові модулі з різною логікою фільтрації і має просту схему конфігурації [14].

Основними відмінностями були видалення коду маскування IP з ядра і зміна логіки наборів правил введення і виведення. Існує новий розширюваний інструмент налаштування iptables.

У ланцюжках IP набір правил введення застосовується до всіх пакетів, отриманих комп'ютером, незалежно від того, призначені вони локальному комп'ютеру або перенаправлені на інший комп'ютер. У Netfilter набір правил введення застосовується тільки до пакетів, призначених для локальних комп'ютерів. Подальша

серія тепер застосовується виключно до пакетів, призначених для передачі на інший комп'ютер. У ланцюжках IP набір правил виводу застосовується до всіх пакетів, згенерованих з комп'ютера, навіть якщо вони згенеровані на локальному комп'ютері. У Netfilter цей набір застосовується тільки до тих пакетів, які генеруються на цьому комп'ютері, а не до тих пакетів, які знаходяться в процесі передачі. Ця зміна значно спростила налаштування.

Ще однією новиною стало впровадження компонентів для роботи з маскуванням IP в окремих модулях ядра. Вони були переписані як модулі Netfilter. Для служб, які повинні проходити через брандмауер, але не потрапляють на локальний комп'ютер, потрібно тільки два правила: для прямого і зворотного проходів тільки в наборі правил.

РОЗДІЛ 2
ОБҐРУНТУВАННЯ ВИБОРУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ФУНКЦІОНУВАННЯ МЕРЕЖІ ПІДПРИЄМСТВА

2.1. Вибір програмного забезпечення

Для зручності комп'ютери розділені на групи (група створюється відповідно до конфігурації комп'ютера) і відповідного призначення:

- Сервер OPC (офісний персональний комп'ютер) / n.
- OPC WS (робоча станція) / n.
- OPC GWS (графічна робоча станція) / n.
- Разом до 3 груп OPC server / n, OPC WS / n, OPC GWS / n
- Для серверів і робочих станцій був обраний Linux: Suse 15.2 «Leap».

SUSE була обрана тому, що Linux-це безкоштовна ОС. Linux: Suse 15.2 «Leap» – відносно новий дистрибутив. Fedora-це продовження знаменитого Linux: RED HAT.

Дистрибутив включає в себе такі програми, як веб-сервер для патча 2, FTP-сервер, open office (аналогічно MS Office), Samba (допомагає Linux взаємодіяти з Windows через локальну мережу), GIMP (аналогічно Photoshop) та інші корисні програми.

При установці Linux знижується відсоток вірусних атак і втрати даних, оскільки сьогодні віруси в основному пишуться для Windows.

Але все одно Лінукс не може задовольнити усі потреби співробітників підприємства. Редакторам потрібні робочі станції для роботи з графікою. Для цих цілей була обрана операційна система MS Windows 10 Pro, що добре зарекомендувала себе в роботі. Windows 10 Pro поєднує в собі такі поняття, як стабільність, надійність та безпека, і може працювати з комерційними продуктами, такими як PhotoShop, 3D Max, Corel Draw та іншими програмами.

Таблиця 2.1

Вибір програмного забезпечення

Програмні продукти використовувані в мережі підприємства	Обрана операційна система
GNOME net filter A patch Server FTP Server DHCP Server Mysql Server Dr web	Linux: Suse 15.2 «Leap»
GNOME NFS,Firefox Open Office (Write, Math Calc, Draw...) Gimp, Dr Web C++ Base Date client XPDF (PDF Viewer) Samba.	Linux: Suse 15.2 «Leap»
3d Max, Adobe Photoshop DC, Corel Draw, AutoCAD, Macromedia Flash.	Windows 10 Pro;

2.2. Теоретичні основи проектування локальних обчислювальних мереж

При проектуванні мережі необхідно збирати дані про структуру організації. Ці дані повинні включати інформацію про організацію, методи управління, плановані розробки, офісні системи, а також думки членів робочого персоналу. Необхідно з'ясувати, хто у організації має право вказувати імена, встановлювати адреси, встановлювати конфігурації і планувати топології [5]. Ви повинні задокументувати існуюче обладнання та програмне забезпечення організації.

Перед розробкою мереж і установкою обладнання слід визначити всі джерела даних і параметри, які необхідно для них задати. Важливо протестувати доповнення, які можуть викликати проблеми в мережі, пов'язані з передачею даних. Дії, які викликають перевантаження мережі, включають в себе:

- Передача графічної та відеоінформації;
- Доступ до центральної бази даних;
- Завантаження програмного забезпечення з віддаленого сервера;
- Доступ в Інтернет та інші.

Ще одне завдання-оцінити попит користувачів. Необхідно зробити відповідні дії для задоволення інформаційних потреб організації та її співробітників.

2.3. Основні етапи проектування ЛОМ

Дані етапи включають в себе:

- Функції та розташування сервера.
- Дизайн мережі розділений на дві частини.
- У першій частині описується фізичний дизайн мережі.
- Друга частина описує проектування програмного забезпечення мережі.
- Документування фізичної та логічної структури мережі.

Вибір топології. Щоб підключити ПК до запропонованої локальної мережі, ми повинні вибрати топологію підключення комп'ютера. Одну з найвищих позицій в сучасній промисловості займає зіркоподібна топологія фізичних зв'язків комутаційного устаткування. Ця топологія забезпечує простоту обслуговування і високу надійність мережі [5].

Термін "топологія", або" топологія мережі", описує фізичне розташування комп'ютерів, кабелів та інших мережевих компонентів.

Топологія мережі відповідає її характеристикам. Зокрема, вибір конкретної топології впливає на:

- Про структуру мережевого обладнання;
- Характеристики мережевого обладнання;
- Варіанти розширення мережі;
- Метод управління мережею [5].

Для спільного використання ресурсів або виконання інших мережевих завдань комп'ютери повинні бути підключені один до одного. Більшість людей використовують для цієї мети кабель.

Однак простого підключення комп'ютера до кабелю, що з'єднує інші комп'ютери, недостатньо. Різні типи кабелів у поєднанні з різними мережевими картами, мережевими операційними системами та іншими компонентами вимагають різного відносного положення комп'ютера. Всі мережі побудовані за базовою топологією: шина, кільце, зірка.

Функції сервера. Для стабільної і якісної роботи мережі необхідно правильно вибрати, встановити і налаштувати апаратне і програмне забезпечення.

Однорангові мережі і серверні мережі об'єднані спільним знаком – поділом ресурсів.

Нам потрібно визначити, чи потрібні нам сервери або ми можемо побудувати нашу мережу без них [4].

Приклад: для секретарів доступ в Інтернет потрібно тільки для електронної пошти, для бухгалтерії – доступ до підключень з віддалених баз даних, директор повинен мати доступ в Інтернет. Для цього необхідно встановити сервер, який буде спільно використовувати права між користувачами локальної мережі. Сервери можна розділити на два класи [4]:

- Сервер робочої групи обслуговує певну групу користувачів і надає їм такі послуги, як обробка текстів або доступ до сумісних файлів. Сервери робочих груп повинні розташовуватися на проміжних розподільних станціях (Ors), як можна ближче до користувачів, які використовують розширення для цих серверів.
- Сервер організації підтримує всіх користувачів в мережі, надаючи різні послуги, такі як електронна пошта або DNS [4].

Сервер організації повинен розташовуватися в головній розподільній станції (GDS). У цьому випадку потік даних буде надходити тільки в GDS, не проходячи через інші сегменти мережі.

Для правильної роботи нашої компанії нам потрібні 3 типи серверів: файловий, Інтернет - і сервер управління обліковими записами. Це не означає, що нам

потрібні 3 комп'ютери, які будуть виконувати ці три завдання. Виходячи з розміру мережі нашого підприємства, ми оцінимо, скільки серверних комп'ютерів нам буде потрібно для правильної роботи локальної мережі. Чим більше мережа, тим більше серверів може знадобитися для правильної роботи. Але тільки грамотне планування функцій сервера між собою може гарантувати якісну продуктивність мережі.

Файловий сервер. Файловий сервер допомагає зберігати інформацію з декількох комп'ютерів в одному місці, що дозволяє збільшити безпечний обмін інформацією. Тому що, якщо інформація буде розкидана по всьому підприємству, захистити її від небажаних очей буде складніше [4]. Набагато простіше захистити 1-10 ПК (серверів), ніж 30 ПК підприємства.

Сервер доступу в інтернет. Сервер доступу в Інтернет дозволяє корпоративним художникам виходити в інтернет. Він взаємодіє з постачальником послуг через мережеве комутаційне устаткування – мережеву карту або інший тип з'єднання [4]. Його основна функція полягає в тому, що пакети з інформацією, шкідливою для нашої мережі, не потрапляють з глобальної мережі "Інтернет".

Сервер управління локальною мережею – цей тип сервера управляє обліковими записами, адресами мережевих ПК і розташуваннями серверів робочих груп.

Кабельна система (СКС). При створенні СКС виділяють наступні елементи:

- Телекомунікаційні Монтажні шафи;
- Магістральна кабельна система;
- Приміщення для обладнання;
- Робочі місця і засоби введення.

Кабельна система включає в себе мережевий носій даних, телекомунікаційну розетку або роз'єм, комутаційний шнур в монтажному відсіку шафи і механічні з'єднання "все в одному" [8].

Для горизонтальних кабельних систем частіше використовується неекранована кручена пара (UTP, Специфікація 100 base t) категорій 5 або 5е, яка широко використовується в локальній мережі, оскільки забезпечує підтримку сучасних те-

хнологій високошвидкісної передачі даних. Максимальна протяжність ділянки становить 100 метрів (328 футів) [8]. Існує кілька специфікацій, які регулюють кількість витків на одиницю довжини в залежності від призначення кабелю.

Кручена пара, визначена в спеціальному стандарті EIA / Tia 568, не екранована - на основі UTP з різними стандартами корпусу, що гарантують однорідність виробництва. UTP 5 - це кабель, здатний передавати дані зі швидкістю до 1000 Мбіт/с. Він складається з чотирьох кручених пар мідного дроту [8].

Для створення з'єднання UTP-5 можна використовувати роз'єм RJ45.

Створити розвинену кабельну систему і одночасно спростити роботу з її допомогою допоможе ряд корисних компонентів:

- Розподільні Стелажі і полиці-призначені для монтажу кабелів. Вони дозволяють централізовано організувати безліч з'єднань і одночасно займати значний простір.
- Патч-панель. Вони підтримують до 96 портів і швидкість передачі даних до 1000 Мбіт / с.
- Рознімання. Одинарні або подвійні RJ - 45 підключаються до панелей розширення або настінних розеток. Вони забезпечують швидкість передачі даних до 1000 Мбіт / с.
- Настінна розетка. До розетки можна підключити два (або більше) роз'єми.

Для можливого збільшення відстані рекомендується залишити невеликий запас кабелю з обох кінців, наприклад, при повторному підключенні.

Після установки кабелю необхідно скласти схему прокладки відрізків кабелю. Стандарт EIA / Tia вимагає, щоб фізичному з'єднанню було присвоєно унікальний ідентифікатор, який може бути вказаний на блоці фізичного краю або прикріпленій до нього етикетці.

Основний кабель з'єднує приміщення з системним комутаційним обладнанням. Це включає в себе сегменти магістральних кабелів, основні та проміжні перехресні з'єднання, а також комутаційні шнури, які використовуються для перетину магістральних кабелів.

Для магістральних кабельних систем можна використовувати коаксіальний кабель, екрановану і неекрановану кручену пару, а також ВОЛЗ. В основному, найбільш використовувана пара 5е, тому що вона не дорога, підтримує технології Ethernet, Fast Ethernet і Gigabit Ethernet, надійна у використанні. У разі обриву кабелю поломку буде легко виявити.

Інфраструктура локальної мережі відповідає стандартам EIA / Tia і заснована на комутації Ethernet, що дозволяє перемикатися на більш високі швидкості без зміни фізичної схеми підключення.

Монтаж комутаційного обладнання. Після прокладки кабелю горизонтальної кабельної системи необхідно провести підключення до приміщення для комутаційного обладнання. Обладнання, розташоване в цій кімнаті, що включає в себе комутатори, маршрутизатори, комутатори та концентратори.

Приміщення для комутаційного обладнання відповідають стандарту EIA / Tia-вони досить великі, так як в майбутньому можливий розвиток локальної мережі.

Місце, вибране для комутаційного обладнання, відповідає всім вимогам до електропостачання, опалення та вентиляції. Крім того, місце надійно захищене від несанкціонованого доступу і відповідає стандартам всіх правил безпеки.

Резервне живлення забезпечується для кожного сервера, присутнього в мережі, а також для всіх мережевих пристроїв, таких як комутатори, маршрутизатори і концентратори. Джерела безперебійного живлення використовуються для захисту від електричних перешкод і перебоїв в подачі електроенергії.

Комутаційна панель. Комутаційна панель являє собою пристрій для підключення з'єднань, за допомогою якої кабельні сегменти горизонтальної підсистеми підключаються до мережевих пристроїв, таких як концентратори, маршрутизатори і комутатори [8].

Комутаційні панелі можуть встановлюватися або на стіні, або в розподілених стелажах, або в шафах, обладнаних внутрішніми стелажами. Найчастіше розподі-

лені стійки використовуються для установки комутаційних панелей, які забезпечують легкий доступ до обладнання як з передньої, так і з задньої панелей. Стандартна ширина стійки становить 19 дюймів, а висота може становити 39" - 74".

Кабелі в комутаційній панелі слід кріпити в порядку їх збільшення кількості, яке їм було присвоєно при прокладці з робочої зони в приміщення для комутаційного обладнання. Такі кабелі дозволяють легко діагностувати і виявляти проблеми.

Технології локальної мережі. Найбільш популярною технологією локальної мережі є Ethernet. Ця технологія використовує метод доступу CSMA / CD для обміну даними між мережевими пристроями і забезпечує передачу даних зі швидкістю до 1000 Мбіт/с [8].

Технологія Ethernet має безліч фізичних стандартів, найбільш популярними з яких є 100 base-T 1000 base-T, які мають топологію у формі зірки і використовують кабельні діапазони UTP-3-5 в якості фізичного середовища передачі даних.

Найбільш популярним фізичним рівнем для мереж Fast Ethernet є стандартний 100 base-TX, який використовує кабель категорії UTP-5 в якості фізичного носія даних, і 100 Base-FX, який використовує багатомодові волокна [11].

У мережах, заснованих на скрученому стані кабелю, можна використовувати різні нестандартні провідники, які дозволяють додавати нові характеристики і властивості мережі. Швидкість передачі даних становить близько 80-100 мегабайт в секунду.

Наступні фактори негативно впливають на продуктивність локальної мережі Ethernet:

- Характер передачі кадрів даних;
- Збільшена Затримка поширення кадрів при використанні мережевих пристроїв;
- Збільшення кількості зіткнень, а, отже, зменшення пропускної здатності мережі та збільшення кількості станцій у мережі;
- Метод доступу CSMA / CD, який дозволяє передавати дані тільки на одну станцію одночасно [11].

Принцип сегментації мережі. Інструменти рівня 2 призначені для забезпечення управління потоком даних, виявлення та виправлення помилок, а також зменшення перевантаження мережі. На цьому етапі працюють такі пристрої, як мережеві адаптери, мости і комутатори. Пристрої на цьому етапі визначають розмір області зіткнення. Великий розмір домену колізії негативно впливає на ефективність роботи мережі. Використовуючи мости і перемикачі, ви можете розділити шаблон, зменшивши розмір домену перкусії [11].

Щоб визначити розмір домену зіткнення, необхідно знати, скільки хостів фізично підключено до одного порту комутатора. При мікросегментації розмір області зіткнення дорівнює двом (порти комутатора і, наприклад, порти робочої станції). У разі концентраторів кілька комп'ютерів підключаються до одного і того ж порту комутатора, створюючи домен зіткнення і розділяючи пропускну здатність між собою.

РОЗДІЛ 3
ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX

3.1. Технологія запропонованої комп'ютерної мережі

Для нашої мережі були обрані дві технології: Fast Ethernet і Gigabit Ethernet (base-t). Вони будуть застосовуватися до крученої пари категорії 5E.

Технологія Ethernet вже давно використовується в локальних мережах і зарекомендувала себе дуже добре. Технологія Fast Ethernet буде використовуватися для підключення робочих станцій в більшості офісів. Причому Gigabit Ethernet буде використовуватися як для підключення сервера, так і в офісі графічних редакторів, де потрібна значна пропускна спроможність каналу зв'язку для рендерингу контенту на сервері в режимі реального часу.

Розміщення робочих станцій

Перший поверх:

- У вітальні є 7 робочих місць.
- Безпека в офісі-3 робочих місця
- Секретар-6 робочих місць.
- Кімната з комутаційним обладнанням.

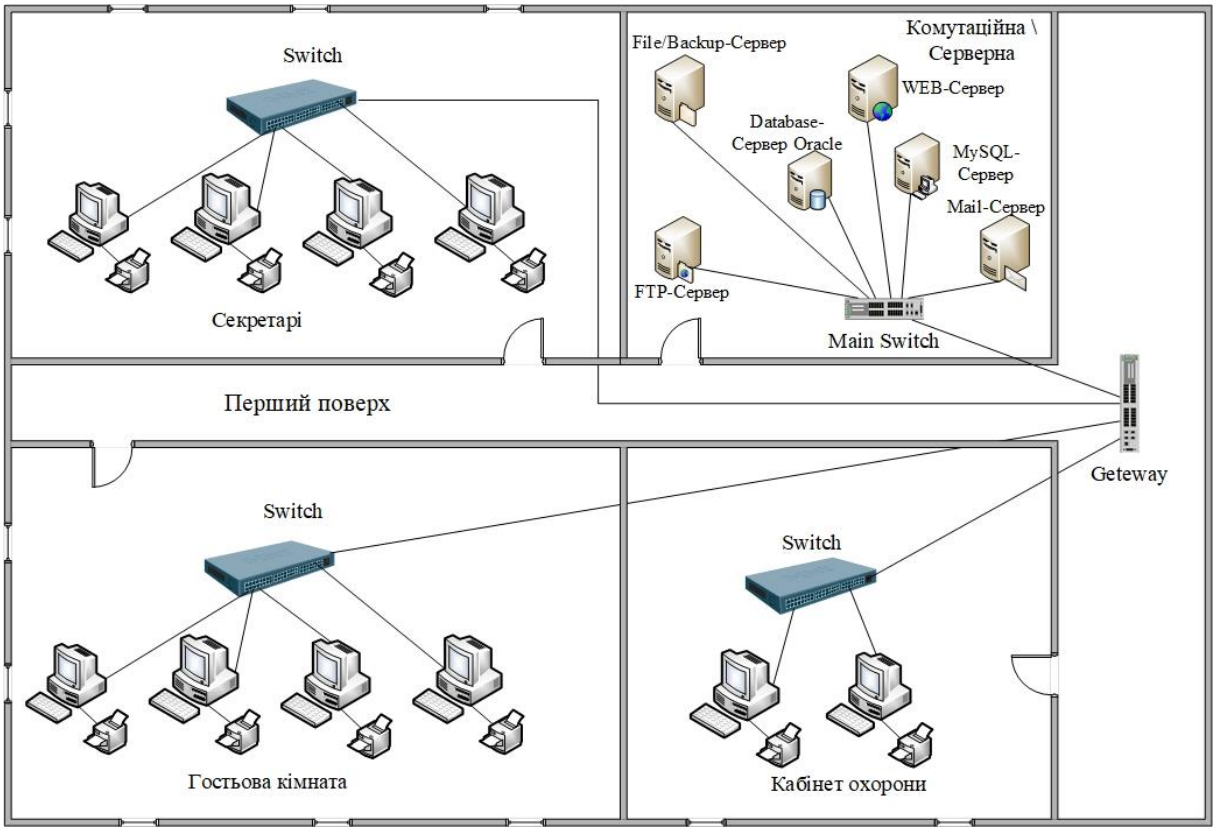


Рис. 3.1. План розрашування телекомунікаційного обладнання на 1 поверсі підприємства

Гостьова кімната – комп'ютери підключені по топології "зірка". Кабель крученої пари, що йде від кожної робочої станції до комутатора, що з'єднує цю шафу з іншим комутатором та з сервером.

Робочі місця секретарів підключені до комутаторів 12 робочих станцій.

У приміщенні з комутаційним обладнанням встановлений шлюз, який з'єднує перший поверх з другим і третім.

Другий поверх:

- Офіс графічного редактора - 10 робочих місць.
- Кабінет редагування тексту - 10 робочих станцій.
- В інформаційному відділі є 5 робочих місць.
- Бухгалтерія-5 робочих місць.

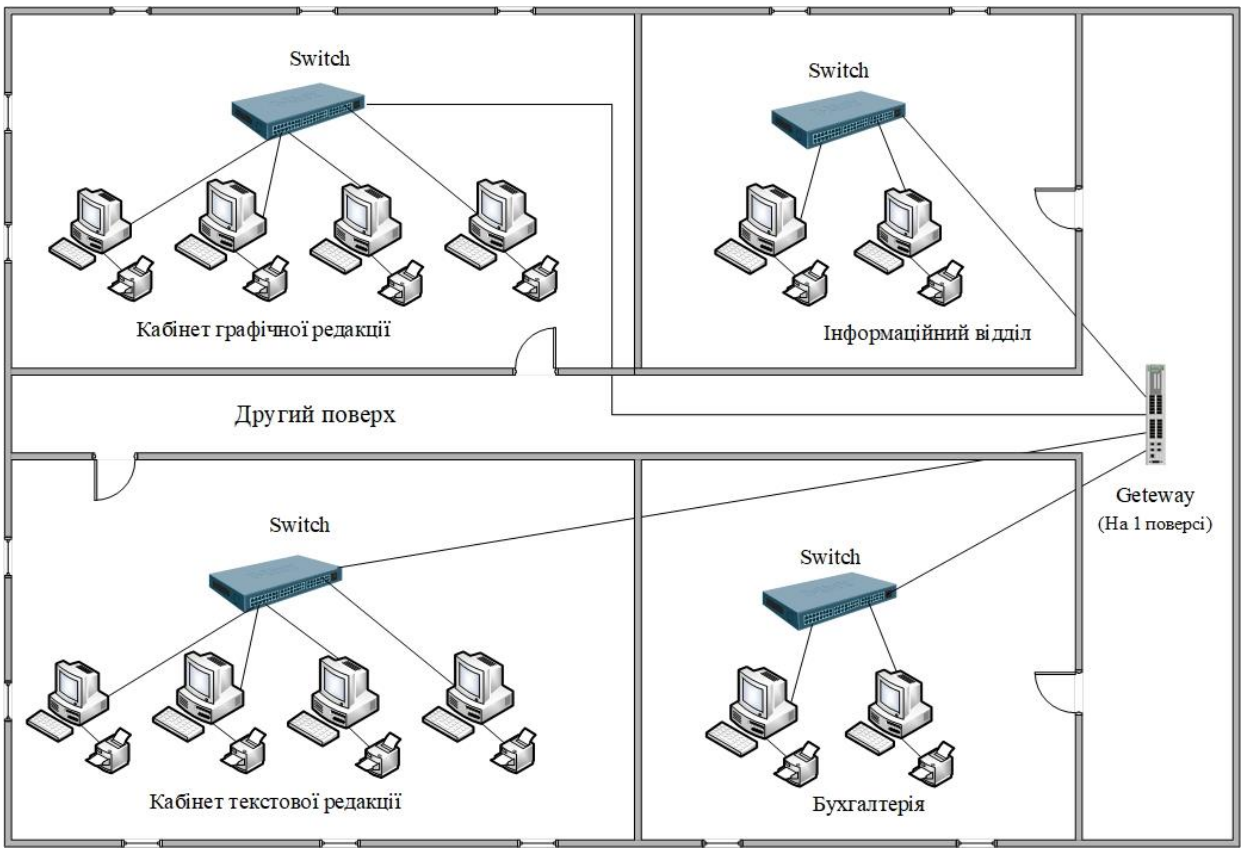


Рис. 3.2. План розрашування телекомунікаційного обладнання на 2 поверсі підприємства

Офіс – робочі станції графічного редактора підключені до комутаторів, що не підключені один до одного. Це дозволить нам збільшити швидкість між графічним сервером і робочою станцією мережі.

В офісі текстового редактора є концентратор з 8 портами, які допомагають підключити всі комп'ютери в мережі і підключити їх до сервера.

В інформаційному відділі 5 робочих станцій підключені до комутатора.

Бухгалтерія – 5 робочих станцій підключені до комутатора.

У комутаційній кімнаті встановлений комутатор, сервер необхідний для роботи офісу текстового редактора, інформаційного відділу та бухгалтерії. Комутатор S2 необхідний для підключення офісу і сервера графічного редактора.

Третій поверх:

- Кабінет директора - 2 робочих місця.
- Бібліотека - 15 робочих станцій.
- Кабінет головного редактора - 1 роботизована станція.

- Кабінет головного бухгалтера-1 робоче місце.

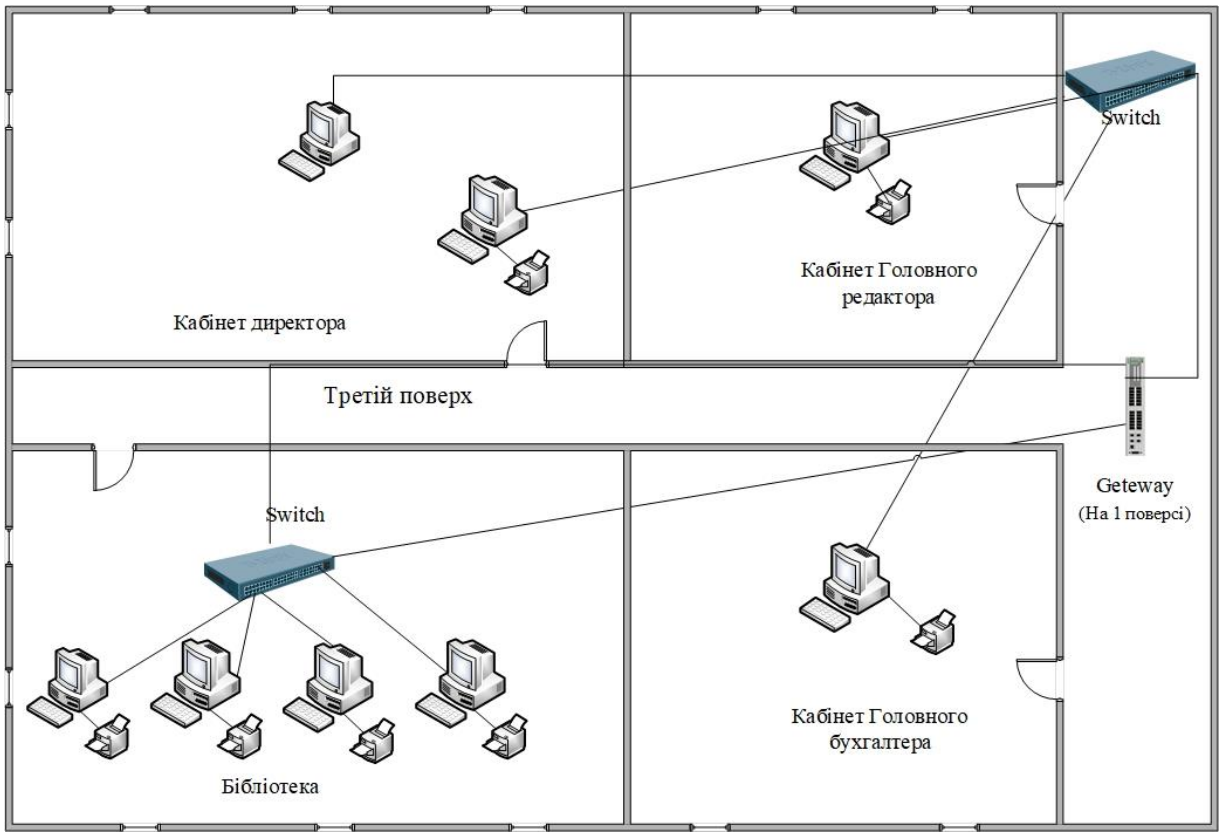


Рис. 3.3. План розрашування телекомунікаційного обладнання на 2 поверсі підприємства

У будівлі кабелі між офісами і серверами будуть проходити по даху. Всередині шаф кабель буде проходити між поверхами. Комутаційні пристрої шаф будуть встановлені безпосередньо в спеціальних стійках, щоб до них не було несанкціонованого доступу.

Приміщення, що виділені під серверні кімнати будуть оснащені стабілізаторами енергії від генератора резервної потужності, так що в разі перебоїв в подачі електроенергії сервери будуть працювати в штатному режимі. На дверях буде встановлений унікальний замок, щоб не було фізичного доступу до сервера для тих, хто не має на це права.

Магістральна кабельна система. Всі кабелі будуть проходити між підлогою і стелею щоб приховати кабель від сторонніх очей, фізичних пошкоджень і т. д.

Між поверхами кабель пройде по спеціальному тунелю, що являє собою трубу шириною 10 см та дозволить легко підключати або замінювати магістральні кабелі.

У будівлі встановлені всі 65 робочих станцій.

Інтернет-сервер буде встановлений в GDS. У ньому буде встановлена операційна система Linux і налаштовано FireWall (брандмауер), що відокремить корпоративну мережу від Інтернету.

У таблиці IP-адрес показаний діапазон адрес підприємства.

Таблиця 3.1

IP – адресація в корпоративній мережі підприємства

Мережа	Опис
20.34.34.0	Для з'єднання з провайдером
192. 168.1. 0	Для серверів підприємства (2)
192. 168.2. 0	Для робочих станцій підприємства
IP адресация	
IP-Address	Опис
10.42.32.12	Proxy Cash Server (Провайдер)
192.168.1.1 192.168.2.1 10.42.0.10	Сервер безпеки, Web server, файловий сервер OPC Serv/2
192. 168.1.2	Контролер домену, файловий Сервер, Mysql Server
192.168.2.12-192.168.2.32	Секретарі
192.168.2.33-192.168.2.53	Бібліотека
192.168.2.54-192.168.2.64	Інформаційний відділ
192.168.2.65-192.168.2.75	Охорона
192.168.2.100- 192.168.2.115	Адміністрація підприємства
192.168.2.116- 192.168.2.136	Бухгалтерія
192.168.2.137- 192.168.2.200	Редакція

Для серверів перші 10 адрес були зарезервовані в кожній мережі. По-перше, сервер повинен мати статичні IP-адреси, щоб кожна робоча станція використовувала сервер для виконання відповідних функцій в локальній мережі. Наприклад, такі, як доступ в інтернет або доступ до баз даних. По-друге, це було зроблено для того,

щоб ці адреси можна було безпечно призначати у випадках з розширення функцій сервера.

Враховуючи розширення мережі, для кожної групи співробітників були виділені ліміти адрес. Наприклад, для забезпечення безпеки виділено 10 адрес, хоча насправді використовуються три адреси.

Створення мережі – це не тільки IP-адреси, також знадобляться інструменти, завдяки яким ми зможемо реалізувати нашу мережу.

Документація для кабельних трас. У цій таблиці показано підключення магістралі і з'єднання між робочою кімнатою і магістраллю.

Таблиця 3.2

Маркування кабелю

З'єднання	Ідентифікатор кабелю	Крос з'єднання	Тип кабелю	Використання
Перший Поверх				
Switch 11-S1	1-1-0	Горизонтальний крос з'єднання 1.1 / порт 1	UTP5e	Використ.
Switch 12-S1	1-2-0	Горизонтальний крос з'єднання 1.2 / порт 2	UTP5e	Використ.
Switch 13-S1	1-3-0	Горизонтальний крос з'єднання 1.3. 3 / порт 3	UTP5e	Використ.
Другий та третій Поверхи				
Switch 21 – Switch 22	2-1-0	Горизонтальний крос з'єднання 2.1 / порт 1	UTP5e	Використ.
Switch 22 –S2	2-1-1	Горизонтальний крос з'єднання 2.1 / порт 1	UTP5e	Використ.
Switch 23 - Switch 24	2-2-3	Горизонтальний крос з'єднання 6 / порт 6	UTP5e	Використ.

3.2. Організація захисту мережі під управлінням ОС Linux

Питання безпеки завжди актуальне в наш час.

Оновлення системи. Це хороша звичка - вчасно встановлювати оновлення ОС. Звичайно, бувають випадки, коли оновлення тягне за собою негативні наслідки, але це вкрай рідко. Цей процес можна спростити за допомогою автоматичного оновлення системи.

Якщо сервер знаходиться під значним навантаженням, слід використовувати стандартні інструменти.

```
sudo apt-get update
sudo apt-get upgrade
```

Користувачі системи з обмеженими правами. Підключення до сервера під обліковим записом суперкористувача root небезпечно. Крім того, рекомендовано змінити будь-якого користувача, який не є користувачем root, присутнього в системі за замовчуванням. Так, принаймні, паролі теж. Команда змінить пароль для користувача, з якого вона запущена. Якщо вам потрібно змінити пароль для іншого користувача, виконайте команду наступним чином.

```
passwd <username></username>
```

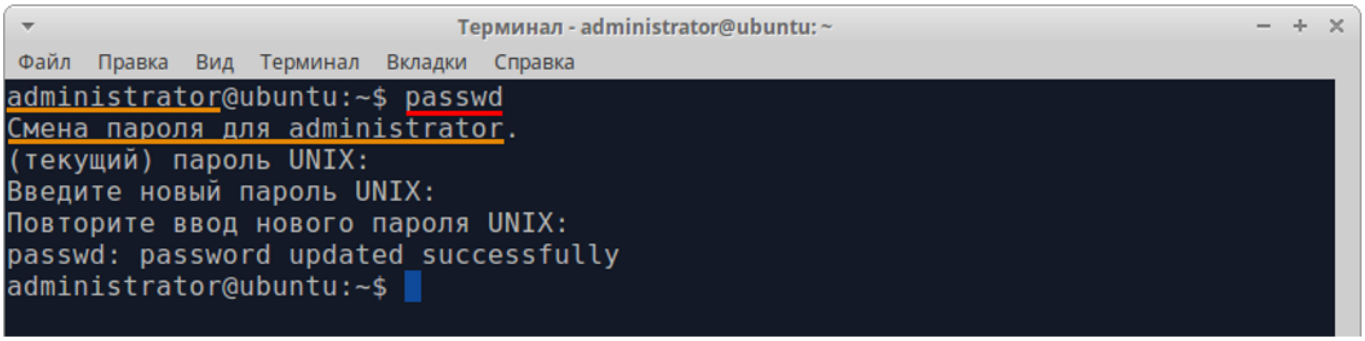


Рис. 3.4. Зміна паролю Адміністратору в ОС Linux

Якщо у вас тільки користувач root, то обґрунтовано буде створити користувача з обмеженими правами командою:

```
adduser <user_name></user_name>
```

В ході своєї роботи програма запросить пароль для облікового запису та після закінчення заповнення даних програма запросить підтвердження коректності інформації.

Наділяємо користувача правами адміністратора додаванням його в групу sudo:

```
adduser <user_name> sudo</user_name>
```

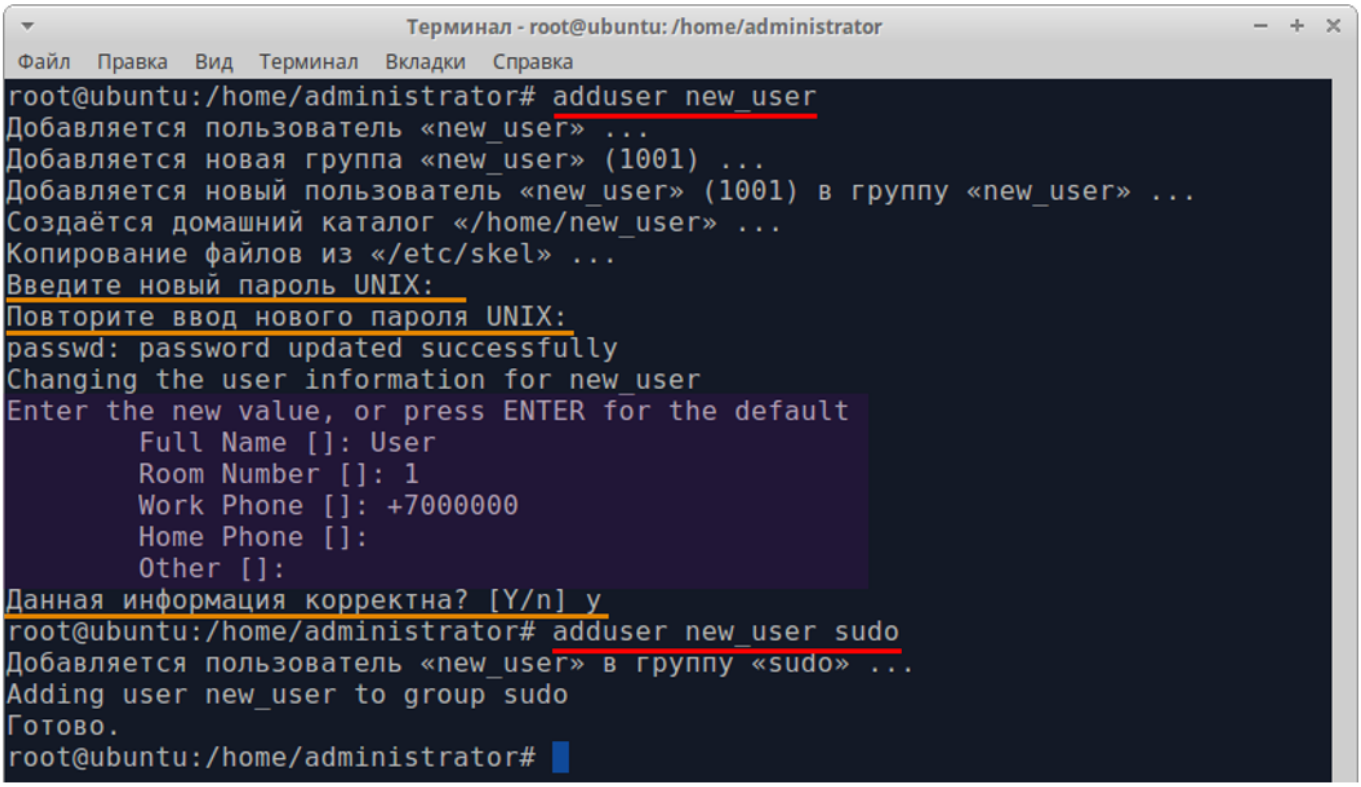


Рис. 3.5. Надання прав адміністратора для користувача мережі

Безпечне з'єднання по SSH. За замовчуванням, доступ до сервера Linux здійснюється по парі логін-пароль на 22 TCP-порту, що звісно рекомендується поміняти (принаймні адресу порту сервера), а підключення проводити по парі логін-ключ [4]. На початку налаштування перевіряємо генерувалися раніше ключі для даного облікового запису:

```
ls ~/.ssh/id_rsa*
```

Якщо результат буде не порожнім, то слід пропустити крок створення ключа, в іншому випадку використовуємо команду:

```
ssh-keygen -t rsa
```

В ході виконання програми, може бути запитана парольна фраза і її підтвердження для додаткового захисту ключа окремим паролем.

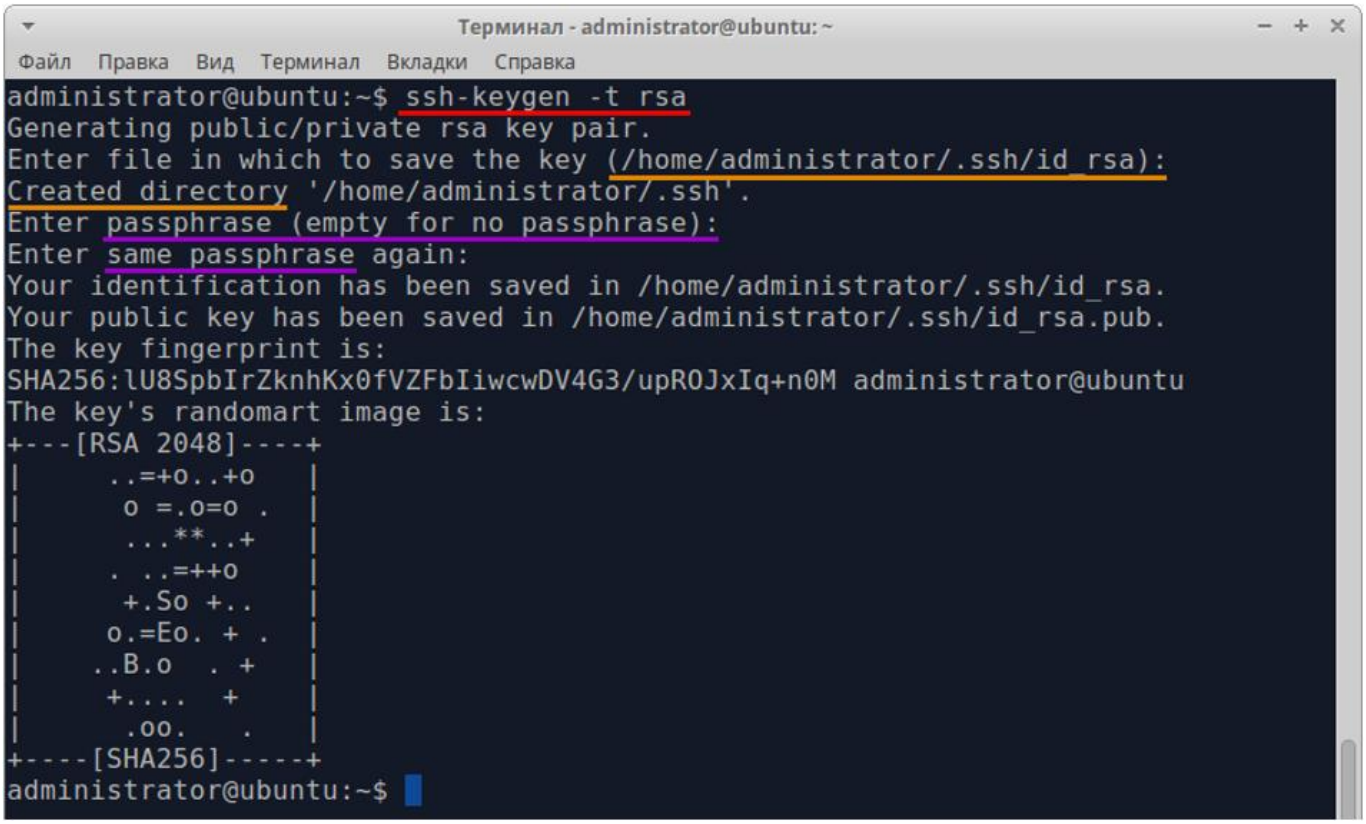
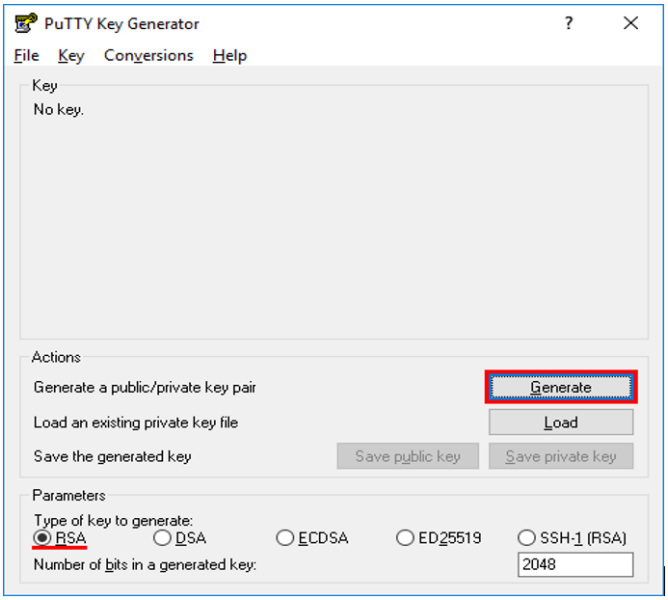


Рис. 3.6. Використання додаткової парольної фрази

Для генерації ключа у разі управління системою з робочої станції зі встановленою ОС Windows підходить безкоштовне ПЗ PuTTY-Gen, де після запуску потрібно обрати тип ключа RSA і натиснути на кнопку Generate.



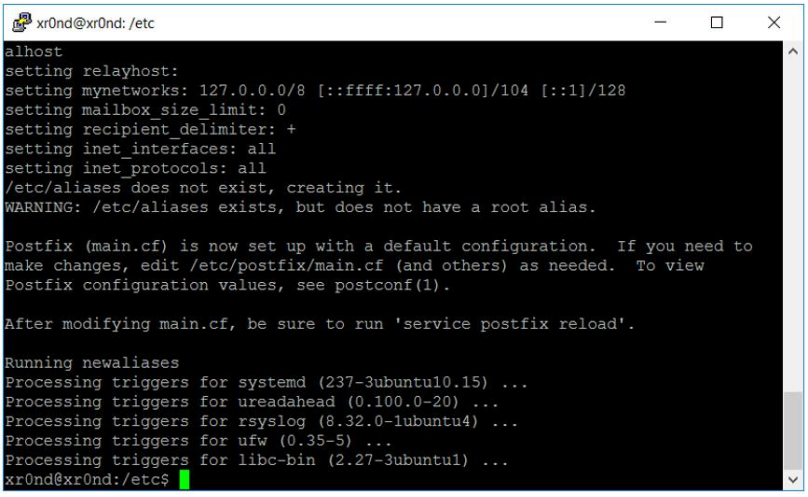


Рис. 3.7. Генерація ключа за допомогою ПЗ PuTTY-Gen

Копіюємо публічний ключ і зберігаємо в файл та додаємо його на віддалений сервер командою:

```
ssh-copy-id remoteuser@10.10.0.1
```

Налаштування служби SSH. Забороняємо авторизацію від користувача root, проте обліковий запис повинен бути в групі sudo для того щоб виконувати команди від суперкористувача, що потребує перед командою використання Службової команди sudo:

```
sudo reboot
```

Також для переходу в режим суперкористувача можна використовувати одну з двох команд:

```
Su \ sudo su
```

Тепер відключимо авторизацію під користувачем root. Для цього відкриваємо на редагування файл sshd_config:

```
sudo nano /etc/ssh/sshd_config
```

Знаходимо рядок PermitRootLogin і замінюємо його значення на no.

Захист SSH-з'єднань за допомогою Fail2Ban — додаток, що дозволяє блокувати SSH-підключення з певної IP-адреси після досягнення ліміту. Розумно вважати, що якщо користувач знає пароль до сервера, але помиляється при введенні, то досить буде 3-5 спроб, в іншому випадку це брутфорс [4].

Fail2Ban здатна здійснювати моніторинг і інших протоколів, таких як HTTP, HTTPS, FTP та ін.

Налаштування Firewall. Фільтрація трафіку дозволяє уникнути різного роду вторгнення в корпоративну мережу підприємства. Рекомендується надавати доступ тільки до тих TCP / UDP-портів, які насправді необхідні та обмежувати доступ до них — тільки з певних IP-адрес.

IPTables – утиліта командного рядка, стандартний інтерфейс управління роботою міжмережевого екрану netfilter в Linux. Для використання IPTables потрібні права суперкористувача. Існують також і альтернативні рішення UFW і ShoreWall [4].

Для перегляду діючих правил фільтрації використовують наступні команди.

IPv4:

```
sudo iptables -L
```

IPv6:

```
sudo ip6tables -L
```

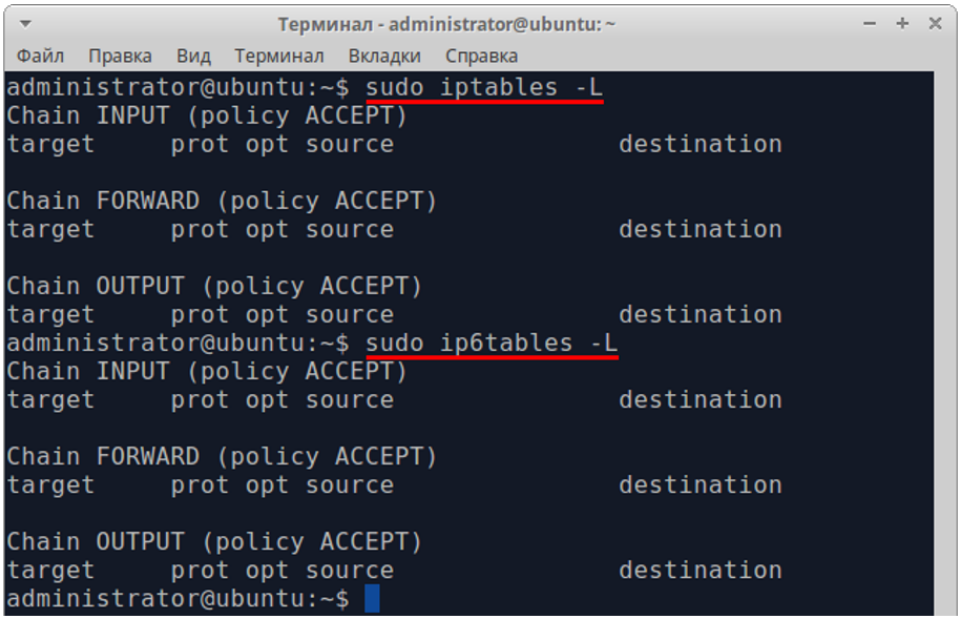


Рис. 3.8. Налаштування IPTables для IPv4 та IPv6 в ОС Linux

Це означає, що в режимі роботи за замовчуванням дозволений весь вхідний, вихідний і транзитний трафік. Налаштування міжмережевого екрану і політика його роботи залежить від роботи сервісів корпоративної мережі підприємства (окремий випадок налаштування порту для RDP).

Для IPv4 (файл /tmp/v4):

```
    *filter
    # Allow all loopback (lo0) traffic and reject traffic
    # to localhost that does not originate from lo0.
    -A INPUT -i lo -j ACCEPT
    -A INPUT ! -i lo -s 127.0.0.0/8 -j REJECT
    # Allow ping.
    -A INPUT -p icmp -m state --state NEW --icmp-type 8 -j ACCEPT
    # Allow SSH connections.
    -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
    # Allow HTTP and HTTPS connections from anywhere
    # (the normal ports for web servers).
    -A INPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
    -A INPUT -p tcp --dport 443 -m state --state NEW -j ACCEPT
    # Allow inbound traffic from established connections.
    # This includes ICMP error returns.
    -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
    # Log what was incoming but denied (optional but useful).
    A INPUT -m limit --limit 5/min -j LOG --log-prefix
"iptables_INPUT_denied: " --log-level 7
```

```
    # Reject all other inbound.
    -A INPUT -j REJECT
    # Log any traffic that was sent to you
    # for forwarding (optional but useful).
    -A FORWARD -m limit --limit 5/min -j LOG --log-prefix
"iptables_FORWARD_denied: " --log-level 7
    # Reject all traffic forwarding.
    -A FORWARD -j REJECT
    COMMIT
```

Для IPv6 (/tmp/v6):

```
    *filter
    # Allow all loopback (lo0) traffic and reject traffic
    # to localhost that does not originate from lo0.
    -A INPUT -i lo -j ACCEPT
    -A INPUT ! -i lo -s ::1/128 -j REJECT
    # Allow ICMP
    -A INPUT -p icmpv6 -j ACCEPT
    # Allow HTTP and HTTPS connections from anywhere
    # (the normal ports for web servers).
    -A INPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
    -A INPUT -p tcp --dport 443 -m state --state NEW -j ACCEPT
    # Allow inbound traffic from established connections.
    -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
    # Log what was incoming but denied (optional but useful).
    -A INPUT -m limit --limit 5/min -j LOG --log-prefix
"ip6tables_INPUT_denied: " --log-level 7
    # Reject all other inbound.
    -A INPUT -j REJECT
    # Log any traffic that was sent to you
    # for forwarding (optional but useful).
    -A FORWARD -m limit --limit 5/min -j LOG --log-prefix
"ip6tables_FORWARD_denied: " --log-level 7
    # Reject all traffic forwarding.
    -A FORWARD -j REJECT
    COMMIT
```

Застосування наведених вище правил.

1. Створюємо файли `/etc/iptables/iptables.rules` та `/etc/iptables/ip6tables.rules`, де вставляємо правила (/tmp/v4 і/tmp/v6).

2. Імпортуємо ці правила для застосування iptables:

```
sudo iptables-restore < /etc/iptables/iptables.rules
sudo ip6tables-restore < /etc/iptables/ip6tables.rules
```

3. У Linux, за замовчуванням, iptables не запущений:

```
sudo systemctl start iptables && sudo systemctl start ip6tables
sudo systemctl enable iptables && sudo systemctl enable ip6tables
```

Міжмережевий екран буде запускатися до підключення сервера до мережі.

Результат буде приблизно таким:

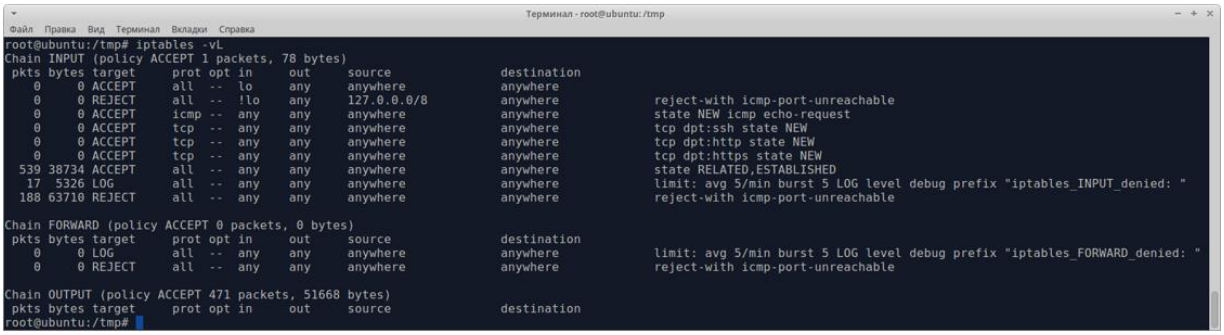


Рис. 3.9. Запуск міжмережевого екрану через командну строку

Перезапускаємо сервер:

```
sudo reboot
```

Після перезапуску, перевіряємо правила. Правила повинні бути присутніми в тій же кількості.

Додавання, зміна та видалення правил iptables

Логіка роботи iptables така, що правила працюють послідовно від першого до останнього. З цієї причини неможливо додати правила звичними командами:

```
iptables -A
ip6tables -A
```

Для додавання правил в цьому випадку використовується:

```
iptables -I
ip6tables -I
```

Для відображення нумерованого списку існує команда:

```
sudo iptables -L -line-numbers
```

Наприклад, необхідно додати нове дозвіл для з'єднань на порт 8080, до існуючих раніше з нашого прикладу вище. Виконуємо команду:

```
sudo iptables -I INPUT 9 -p tcp --dport 8080 -j ACCEPT
```

Заміна правил.

Заміна правил виконується ключем " - R":

```
iptables -R
```

Наприклад:

```
sudo iptables -R INPUT 11 -m limit --limit 3/min -j LOG --log-
prefix "iptables_INPUT_denied: " --log-level 7
```

Видалення правил

Як приклад, видалимо правило, яке ми додали раніше:

```
sudo iptables -D INPUT 9
```

Тобто буде видалено правило, в якому ми дозволяли підключення до 8080 порту.

Важливо! Застосовувані правила не застосовуються автоматично. Для цього необхідно виконати дії застосовні тільки для вашого дистрибутива, які ми розглядали вище.

<u>База даних.</u>

Не менш важливим є захист даних знаходяться в якійсь СУБД. Розглянемо на прикладі MariaDB.

Після успішної установки необхідно виконати одну команду:

```
sudo mysql_secure_installation
```

Після чого, програма задасть кілька питань стосуються безпеки.

Таблиця 3.3

Change the root password? [Y/n]	Змінити пароль користувача root?
Remove anonymous users? [Y/n]	Видалити анонімних користувачів?
Disallow root login remotely? [Y/n]	Заборонити віддалене підключення від імені root?
Remove test database and access to it? [Y/n]	Видалити базу даних test і доступ до неї?
Reload privilege tables now? [Y/n]	Перезавантажити таблицю привілеїв зараз?

Результат буде приблизно таким:

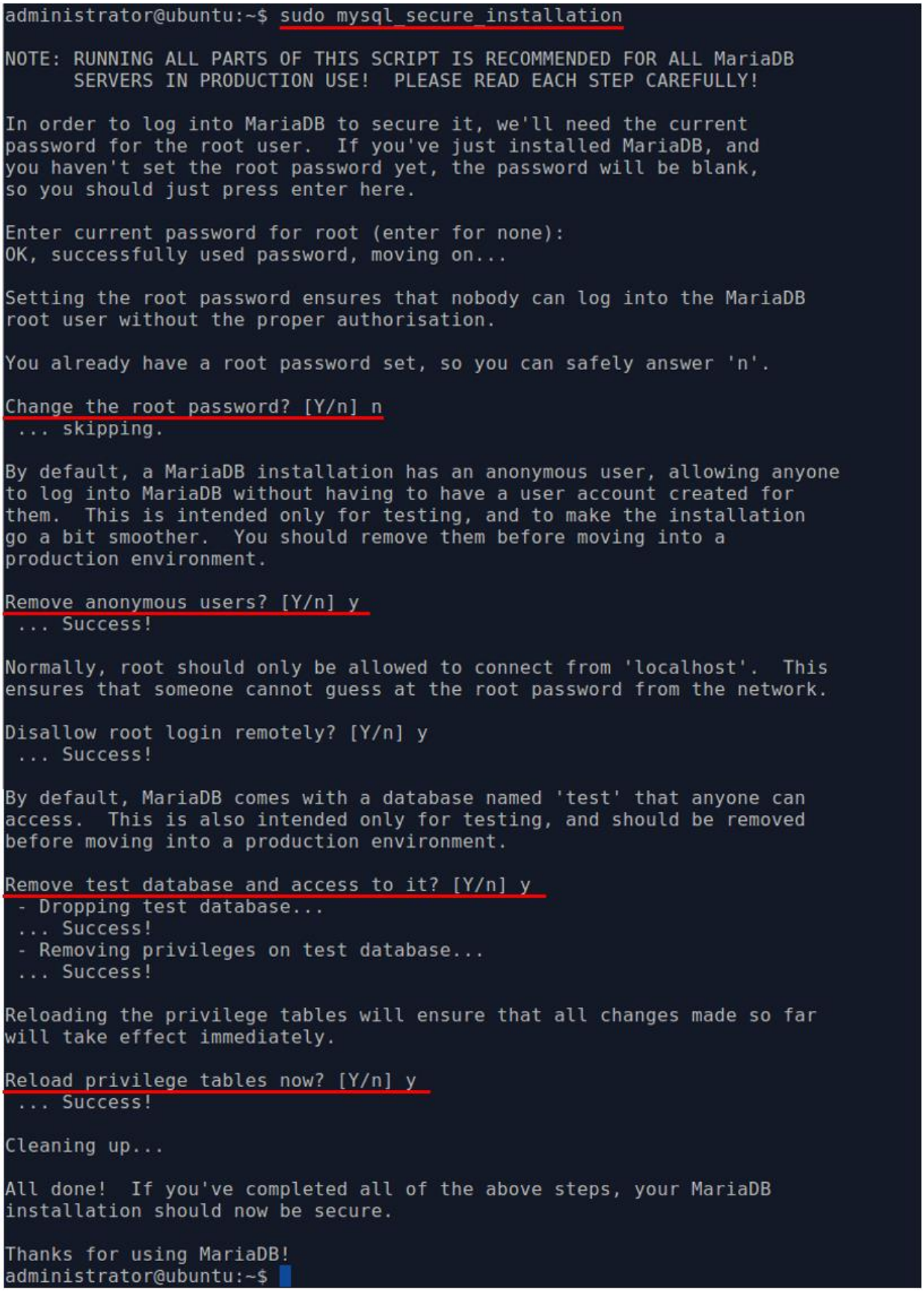


Рис. 3.10. Безпека даних

Також не рекомендується виконувати з'єднання від імені користувача root. Краще створити одного користувача і з обмеженими правами. Для сайту буде достатньо наступних прав для виконання запитів виду [6]:

SELECT-вибірка з бази

UPDATE-Оновлення записів

INSERT-додавання нових записів.

DELETE-видалення записів (іноді, але краще не використовувати).

Не рекомендується наділяти правами:

ALTER-зміна структури таблиць

DROP-видалення баз даних і таблиць бази

Цілком розумним є і те, щоб один користувач був для однієї бази даних.

Загальні вимоги до облікових даних

Для захисту сервера і баз даних слід, навіть якщо ви не використовуєте авторизацію по ключу, логічним буде використовувати грамотно створені ім'я користувача і пароль.

Так як підбір Імен і паролів (брутфорс) відбувається за словником, логічно було б використовувати таке ім'я користувача, яке з найменшою ймовірністю виявиться в словнику. Наприклад, xd11rn і подібні. Не варто використовувати занадто короткі імена користувачів. Головне, потім не забути ім'я користувача.

До паролів є ряд загальних вимог:

- не використовувати паролі коротше 10 символів;
- * використовувати букви верхнього і нижнього регістра, а також цифри;
- * використовувати спеціальні символи, але тільки там, де це можливо [14].

3.3. Встановлення та налаштування Netfilter

Чудова гнучкість Linux Netfilter ілюструється можливістю успадковувати інтерфейси ipfwadm і ipchain. Емуляція брандмауера трохи полегшує перехід на нове покоління програмного забезпечення у версії ядра 5.0.

Два модулі ядра з Netfilter під назвою ipfwadm_o і ipchains_o можуть забезпечити зворотну сумісність з ipfwadm і ipchain. Ви можете завантажити тільки

один з цих модулів за один раз і використовувати його тільки в тому випадку, якщо ip_tables_o модуль не завантажений [4]. При завантаженні відповідного модуля Netfilter працює аналогічно зазначеної реалізації брандмауера.

Інтерфейс ipchain в Netfilter:

```
# rmmod ip_tables
# modprobe ipchains
# ipchains
```

Утиліта iptables використовується для налаштування правил Netfilter. Синтаксис запозичений з ipchain, але у нього є одна важлива відмінність: він був розширений. Це означає, що функціональність може бути збільшена без перекомпіляції пакета. Для цієї мети використовуються вкладені бібліотеки [14].

Перед використанням команди iptables необхідно завантажити модуль ядра Netfilter, який дозволяє йому працювати. Найпростіший спосіб зробити це-за допомогою команди modprobe: # modprobe ip_tables

Команда iptables використовується для налаштування фільтрів IP і перетворення мережевих адрес. Для цього використовуються дві таблиці: filter і Nat. Якщо параметр -t опущений, використовується таблиця фільтрів. Існує п'ять універсальних ланцюжків (наборів правил): введення і пересилання для таблиць фільтрів, попередня і подальша маршрутизація для таблиць Nat і вихід для всіх таблиць [14].

В нашій організації корпоративна мережа буде захищена за допомогою брандмауера, що працює на машині Linux. Всі внутрішні користувачі мають доступ до серверів www в Інтернеті.

Мережа використовує 24 - бітну мережеву маску (клас С) і має мережеву адресу 172.16.1.0, необхідно використовувати правила iptables:

```
    # modprobe ip_tables
    # iptables -F FORWARD
    # iptables -P FORWARD DROP
    #  iptables  -A  FORWARD  -m  tcp  -p  tcp  -s  0/0  -isport  80  -d
172.16.1.0/24 / -isyn -j DROP
    # iptables -A FORWARD -m tcp -p tcp -s 172.16.1.0/24 -isport / 80
-d 0/0 -j ACCEPT
    # iptables -A FORWARD -m tcp -p tcp -d 172.16.1.0/24 -idport 80 -s
0/0 -j / ACCEPT
```

Iptables не підтримує опцію -b, так що ми повинні окремо задати правило для шкірного напрямку.

3.4. Типи пакетів ICMP

Кожна команда налаштування брандмауера дозволяє визначити типи пакетів ICMP. На відміну від портів TCP і UDP, немає зручного файлу конфігурації, в якому перераховані типи пакетів і їх значення. Типи пакетів ICMP визначені в RFC - 1700 (присвоєні номери RFC). Вони також перераховані в одному зі стандартних файлів бібліотеки /usr/include/netinet/ip_icmp, що належить до звичайної бібліотеки GNU і використовується програмістами на мові C# при написанні мережевого програмного забезпечення, що працює з протоколом ICMP і визначає типи пакетів ICMP. Для зручності вони наведені в таблиці 3.4. Командний інтерфейс iptables дозволяє визначати типи ICMP за їхніми іменами [7].

Управління бітами TOS. Тип службових бітів(tos)-це набір чотирьохбітових прапорів у заголовку IP-пакета. Коли встановлено кожен з цих прапорців WZ, маршрутизатори можуть обробляти пакети інакше, ніж пакети без набору бітів TOS. Кожен з чотирьох бітів має різне призначення, і тільки один з бітів TOS може бути встановлений протягом однієї години, тому комбінації не допускаються. Прапори називаються типами служб, оскільки вони дозволяють прикладній програмі, що передає дані, повідомляти мережі тип необхідної служби.

Таблиця 3.4

Типи пакетів ICMP

Номер типу	Позначення iptables	Опис
0	echo-reply	Echo Reply
3	destination-unreachable	Destination Unreachable
4	source-quench	Source Quench
5	redirect	Redirect
8	echo-request	Echo Request
11	time-exceeded	Time Exceeded
12	parameter-problem	Parameter Problem
13	timestamp-request	Timestamp Request
14	timestamp-reply	Timestamp Reply
15	none	Information Request
16	none	Information Reply
17	address-mask-request	Address Mask Request
18	address-mask-reply	Address Mask Reply

Налаштування бітів tos за допомогою ipfwadm або ipchain

Команди Ipfwadm і ipchain мають повноваження з бітами TOS . В обох випадках ви визначаєте правило, яке відповідає на пакети з певним бітом tos, і використовуєте параметр-T для визначення змін, які ви хочете внести.

Зміна виявляється за допомогою двобітної маски. Перша WZ з цих бітових масок використовується в логічних операціях і з полями параметрів IP-пакета, друга-в операції або. Якщо це здасться складним, Я дам рецепти для негайного надання кожного виду послуг.

Бітові маски визначаються з використанням восьмибітних шістнадцяткових значень. Ipfwadm і ipchain використовують один і той же синтаксис:

Найбільш корисні додатки для масок перераховані в таблиці 3.5 з їх значеннями.

Таблиця 3.5

Використання ToS-бітів

TOS	ANDmask	XORmask	Використання, яке рекомендує
Minimum	Delay	0x01 0x10	ftp, telnet, ssh
Maximum	Throughput	0x01 0x08	ftp-данные, www
Maximum	Reliability	0x01 0x04	snmp, dns
Minimum	Cost	0x01 0x02	nntp, smtp

Налаштування iptables з використанням біт tos

Команда iptables дозволяє визначити правила збору даних із зазначеними бітами tos за допомогою параметра-M tos і задати біти за допомогою параметра-J tos. Ви можете встановити тільки ToS-біти в правилах прямого і вихідного рядів. Відповідність вимогам і установка повністю безкоштовні. Ми можемо налаштувати кілька цікавих правил . Наприклад, налаштуйте правило для відхилення пакетів із зазначеними бітами tos або для установки бітів tos в пакетах з певного комп'ютера. На відміну від ipfwadm і ipchains, iptables використовує більш простий підхід, чітко визначаючи, чому ToS-біти повинні відповідати або які ToS-біти повинні бути встановлені. Бітам присвоюються імена, що дозволяє краще запам'ятовувати їх числові маски.

Синтаксис для вказівки відповідних бітів tos в правилах:

```
-m tos -itos mnemonic [other-args] -j target
```

Синтаксис для установки ToS-бітів в правилах:

```
[other-args] -j TOS -iset mnemonic
```

Перевірка конфігурації Firewall

Загальна процедура тесту наступна:

Виберіть тип firewall для використання: ipfwadm, ipchains або iptables.

Для iptables використання прямого набору правил було включено через невідповідність в реалізації набору правил введення в Netfilter. Це має значення: відмінність означає, що брандмауер правил WZ не захищає головний комп'ютер безпосередньо. Щоб скопіювати приклад ipchain, ми скопіювали кожне з наших правил у вхідні дані. Для ясності ми опустили всі вхідні пакети (дейтаграми), які ми отримали від нашого інтерфейсу.

```
#!/bin/bash
############################################################
# IPTABLES VERSION
# This sample configuration is for a single host firewall
configuration
# with no services supported by the firewall machine itself.
############################################################
# USER CONFIGURABLE SECTION
# The name and location of the ipchains utility.
IPTABLES=iptables
# The path to the ipchains executable.
PATH="/sbin"
# Our internal network address space and its supporting network
device.
OURNET="172.29.16.0/24"
OURBCAST="172.29.16.255"
OURDEV="eth0"
# The outside address and the network device that supports it.
ANYADDR="0/0"
ANYDEV="eth1"
# The TCP services we wish to allow to pass - "" empty means all
ports
# note: comma separated
TCPIN="smtp,www"
TCPOUT="smtp,www,ftp,ftp-data,irc"
# The UDP services we wish to allow to pass - "" empty means all
ports
# note: comma separated
UDPIN="domain"
UDPOUT="domain"
# The ICMP services we wish to allow to pass - "" empty means all
types
```

```
    # ref: /usr/include/netinet/ip_icmp.h for type numbers
    # note: comma separated
    ICMPIN="0,3,11"
    ICMPOUT="8,3,11"
    # Logging; uncomment the following line to enable logging of
datagrams
    # that are blocked by the firewall.
    # LOGGING=1
    # END USER CONFIGURABLE SECTION
    ############################################################
    # Flush the Input table rules
    $IPTABLES -F FORWARD
    # We want to deny incoming access by default.
    $IPTABLES -P FORWARD deny
    # Drop all datagrams destined for this host received from outside.
    $IPTABLES -A INPUT -e $ANYDEV -j DROP
    # SPOOFING
    # We should not accept any datagrams with a source address matching
ours
    # from the outside, so we deny them.
    $IPTABLES -A FORWARD -s $OURNET -e $ANYDEV -j DROP
    # SMURF
    # Disallow ICMP to our broadcast address to prevent "Smurf" style
attack.
    $IPTABLES -A FORWARD -m multiport -p icmp -e $ANYDEV -d $OURNET -j
DENY
    # We should accept fragments, in iptables we must do this
explicitly.
    $IPTABLES -A FORWARD -f -j ACCEPT
    # TCP
    # We will accept all TCP datagrams belonging to an existing
connection
    # (i.e. having the ACK bit set) for the TCP ports we're allowing
through.
    # This should catch more than 95 % of all valid TCP packets.
    $IPTABLES -A FORWARD -m multiport -p tcp -d $OURNET -idports $TCPIN
/
    ! -itcp-flags SYN,ACK ACK -j ACCEPT
    $IPTABLES -A FORWARD -m multiport -p tcp -s $OURNET -isports $TCPIN
/
    ! -itcp-flags SYN,ACK ACK -j ACCEPT
    # TCP - INCOMING CONNECTIONS
    # We will accept connection requests from the outside only on the
    # allowed TCP ports.
    $IPTABLES -A FORWARD -m multiport -p tcp -e $ANYDEV -d $OURNET
$TCPIN /
```

```
    -isyn -j ACCEPT
    # TCP - OUTGOING CONNECTIONS
    # We will accept all outgoing tcp connection requests on the allowed
/
    TCP ports.
    $IPTABLES -A FORWARD -m multiport -p tcp -e $OURDEV -d $ANYADDR /
    -idports $TCPOUT -isyn -j ACCEPT
    # UDP - INCOMING
    # We will allow UDP datagrams in on the allowed ports and back.
    $IPTABLES -A FORWARD -m multiport -p udp -e $ANYDEV -d $OURNET /
    -idports $UDPIN -j ACCEPT
    $IPTABLES -A FORWARD -m multiport -p udp -e $ANYDEV -s $OURNET /
    -isports $UDPIN -j ACCEPT
    # UDP - OUTGOING
    # We will allow UDP datagrams out to the allowed ports and back.
    $IPTABLES -A FORWARD -m multiport -p udp -e $OURDEV -d $ANYADDR /
    -idports $UDPOUT -j ACCEPT
    $IPTABLES -A FORWARD -m multiport -p udp -e $OURDEV -s $ANYADDR /
    -isports $UDPOUT -j ACCEPT
    # ICMP - INCOMING
    # We will allow ICMP datagrams in of the allowed types.
    $IPTABLES -A FORWARD -m multiport -p icmp -e $ANYDEV -d $OURNET /
    -idports $ICMPIN -j ACCEPT
    # ICMP - OUTGOING
    # We will allow ICMP datagrams out of the allowed types.
    $IPTABLES -A FORWARD -m multiport -p icmp -e $OURDEV -d $ANYADDR /
    -idports $ICMPOUT -j ACCEPT
    # DEFAULT and LOGGING
    # All remaining datagrams fall through to the default
    # rule and are dropped. They will be logged if you've
    # configured the LOGGING variable above.
    #
    if [ "$LOGGING" ] then
    # Log barred TCP
    $IPTABLES -A FORWARD -m tcp -p tcp -j LOG
    # Log barred UDP
    $IPTABLES -A FORWARD -m udp -p udp -j LOG
    # Log barred ICMP
    $IPTABLES -A FORWARD -m udp -p icmp -j LOG
    #
    # end.
```

У багатьох простих випадках все, що вам потрібно зробити для конкретного застосування цього додатка - це налаштувати блок з написом "настроюється користувачем" на початку файлу, щоб вказати, які протоколи і пакети слід пропускати. Для більш складної конфігурації необхідно повністю виправити цей розділ.

Налаштування обліку IP-адрес оскільки облік IP-адрес дуже тісно пов'язаний з брандмауерами IP, для їх налаштування використовується одна програма. Залежно від реалізації це ipfwadm, ipchains або iptables. Синтаксис команди аналогічний синтаксису, який використовується при налаштуванні правил брандмауера.

Загальний синтаксис для обліку IP з ipfwadm:

```
# ipfwadm -A [direction] [command] [parameters]
```

З'явився новий параметр напрямку. Він приймає значення, або те й інше разом. Всі значення розглядаються з точки зору машини Linux, тому вона і задає вхідний трафік, обидва типи одночасно.

Загальний синтаксис для ipchains і iptables:

```
# ipchains -A chain rule-specification
# iptables -A chain rule-specification
```

Команди ipchains і iptables дозволяють вам визначати напрямок в стилі, більше схожому на визначення правил. IP Firewall Chains не дозволяє налаштувати правила для обох напрямків відразу, але дозволяє налаштувати правила в наборі forward, чого Стара реалізація не вміла.

Команди аналогічні своїм аналогам для правил брандмауера, за винятком того, що стратегії тут не реалізовані. Ми можемо додавати, вставляти, видаляти і змінювати список правил аудиту. У випадку ipchains і iptables всі дійсні правила вважаються Правилами обліку, і жодна команда, що визначає параметр -J, не виконує тільки облік.

Параметри специфікації правил обліку IP-адрес такі ж, як і для брандмауера IP.

Облік за адресою. Давайте на прикладі покажемо, як ми будемо використовувати облік IP-адрес.

Припустимо, у нас є маршрутизатор Linux, який функціонує в двох відділах підприємства. Він має два пристрої Ethernet, AT0 і AT1, по одному на кожен відділ, і пристрій PPP, PPP0, для зв'язку.

Для цілей виставлення рахунків ми хочемо знати загальний обсяг трафіку, що генерується кожним відділом по послідовному зв'язку, а для цілей управління ми хочемо знати загальний обсяг трафіку між двома відділами.

Щоб відповісти на питання про те, скільки даних кожен відділ передає по мережі, ми можемо використовувати правило, яке виглядає наступним чином:

```
# ipfwadm -A both -W ppp0 -S 172.16.3.0/24 -b
# ipfwadm -A both -W ppp0 -S 172.16.4.0/24 -b
```

або:

```
# ipchains -A input -e ppp0 -d 172.16.3.0/24
# ipchains -A output -e ppp0 -s 172.16.3.0/24
# ipchains -A input -e ppp0 -d 172.16.4.0/24
# ipchains -A output -e ppp0 -s 172.16.4.0/24
```

або з iptables:

```
# iptables -A FORWARD -e ppp0 -d 172.16.3.0/24
# iptables -A FORWARD -o ppp0 -s 172.16.3.0/24
# iptables -A FORWARD -e ppp0 -d 172.16.4.0/24
# iptables -A FORWARD -o ppp0 -s 172.16.4.0/24
```

Перша половина набору правил skin визначає кількість всіх даних, що передаються по інтерфейсу PPP0 з адресою джерела або призначення 172.16.3.0/24. Тут корисна опція - b в ipfwadm і iptables. Друга частина набору правил встановлює те ж саме, але для другої мережі Ethernet.

Щоб відповісти на питання про те, скільки трафіку має проходити між відділами, вам потрібно правило, яке виглядає наступним чином:

```
# ipfwadm -A both -S 172.16.3.0/24 -D 172.16.4.0/24 -b
```

або:

```
# ipchains -A forward -s 172.16.3.0/24 -d 172.16.4.0/24 -b
```

або:

```
# iptables -A FORWARD -s 172.16.3.0/24 -d 172.16.4.0/24
```

Ці правила будуть поважати всі пакети з вихідною мережевою адресою одного відділу та мережевою адресою призначення іншого.

Облік по портах обслуговування. Можливо, ми також хочемо знати, який трафік живе на PPP-з'єднанні. Наприклад, вам потрібно з'ясувати, скільки даних проходить через протоколи FTP, SMTP і World Wide Web.

Для збору цієї інформації підходить скрипт з правилами:

```
#!/bin/sh
# Collect FTP, smtp and www volume statistics for data carried on
our
# PPP link using ipfwadm
#
ipfwadm -A both -W ppp0 -P tcp -S 0/0 ftp ftp-data
ipfwadm -A both -W ppp0 -P tcp -S 0/0 smtp
ipfwadm -A both -W ppp0 -P tcp -S 0/0 www
```

або:

```
#!/bin/sh
# Collect ftp, smtp and www volume statistics for data carried on
our
# PPP link using ipchains
#
ipchains -A input -e ppp0 -p tcp -s 0/0 ftp-data:ftp
ipchains -A output -e ppp0 -p tcp -d 0/0 ftp-data:ftp
ipchains -A input -e ppp0 -p tcp -s 0/0 smtp
ipchains -A output -e ppp0 -p tcp -d 0/0 smtp
ipchains -A input -e ppp0 -p tcp -s 0/0 www
ipchains -A output -e ppp0 -p tcp -d 0/0 www
```

або:

```
    #!/bin/sh
    # Collect ftp, smtp and www volume statistics for data carried on
our
    # PPP link using iptables.
    #
    iptables -A FORWARD -e ppp0 -m tcp -p tcp -isport ftp-data:ftp
    iptables -A FORWARD -o ppp0 -m tcp -p tcp -idport ftp-data:ftp
    iptables -A FORWARD -e ppp0 -m tcp -p tcp -isport smtp
    iptables -A FORWARD -o ppp0 -m tcp -p tcp -idport smtp
    iptables -A FORWARD -e ppp0 -m tcp -p tcp -isport www
    iptables -A FORWARD -o ppp0 -m tcp -p tcp -idport www
```

Ось деякі цікаві властивості. По-перше, ми визначили протокол . Коли ми визначаємо порти в наших правилах, ми також повинні визначити протоколи, тому що TCP і UDP мають різні набори портів. Оскільки всі ці служби засновані на TCP, ми визначаємо цей протокол. Очевидно, що ми визначили дві служби, FTP і FTP-дані в одній команді ipfwadm дозволяє визначати окремі порти, діапазони портів або довільні списки портів. Команда ipchain дозволяє визначити один порт або діапазон портів. Запис" FTP-дані": FTP" означає " порт від FTP-даних (20) до FTP (21)", тому Ви можете кодувати порти в ipchains і iptables. Якщо у вас є список портів у правилі обліку, це означає, що будь-які дані для будь-якого порту в списку будуть додані до загальної суми для цього запису. Оскільки FTP використовує два порти, команду та дані, ми об'єднали їх разом у загальний FTP-трафік. Нарешті, ми визначили вихідну адресу як 0/0, що відповідає всім адресам і вимагає ipfwadm і ipchain для визначення портів [7].

Тепер нас цікавить співвідношення корисного трафіку до трафіку по FTP, SMTP і іншим протоколам у всесвітній павутині. Для цього ми встановимо наступні правила:

```
    # ipfwadm -A both -W ppp0 -P tcp -S 0/0 ftp ftp-data smtp www
    # ipfwadm -A both -W ppp0 -P tcp -S 0/0 1:19 22:24 26:79 81:32767
```

Якщо ви вже перевірили свій файл / etc / services, ви побачите, що він охоплює всі порти, крім правил (FTP, FTP-data, SMTP і www).

Як це зробити за допомогою команд ipchains або iptables, оскільки вони дозволяють лише параметр у специфікації порту? Ми можемо використовувати власні ланцюжки в бухгалтерському обліку так само легко, як правила брандмауера. Розглянемо наступний підхід:

```
    # ipchains -N a-essent
    # ipchains -N a-noness
    # ipchains -A a-essent -j ACCEPT
    # ipchains -A a-noness -j ACCEPT
    # ipchains -A forward -e ppp0 -p tcp -s 0/0 ftp-data:ftp -j a-
essent
    # ipchains -A forward -e ppp0 -p tcp -s 0/0 smtp -j a-essent
    # ipchains -A forward -e ppp0 -p tcp -s 0/0 www -j a-essent
    # ipchains -A forward -j a-noness
```

Тут ми створюємо дві умовні ланцюжки користувачів: a-необхідні, де ми збираємо дані для корисного трафіку, і a-неус, де ми збираємо дані для всього іншого. Потім ми додаємо правила в пряму ланцюжок, які реагують на корисні сервіси, і встановлюємо перехід до ланцюжку A-essential, яка враховує тільки трафік. Останнє правило в нашій прямій ланцюжку встановлює перехід до ланцюжка a-nonus, де також існує тільки одне правило, що враховує трафік. Правило, яке відноситься до серії A-nonus, не буде отримано жодним пакетом корисних послуг, так як вони будуть прийняті в своїй серії. Наші лічильники корисних та інших послуг будуть доступні тільки в правилах в рамках тихих ланцюжків. Це просто підхід, який ви можете змінити. Застосування того ж підходу до iptables:

```
    # iptables -N a-essent
    # iptables -N a-noness
    # iptables -A a-essent -j ACCEPT
    # iptables -A a-noness -j ACCEPT
    # iptables -A FORWARD -ые ppp0 -m tcp -p tcp -isport ftp-data:ftp
-j a-essent
    # iptables -A FORWARD -e ppp0 -m tcp -p tcp -isport smtp -j a-
essent
    # iptables -A FORWARD -e ppp0 -m tcp -p tcp -isport www -j a-essent
    # iptables -A FORWARD -j a-noness
```

Це виглядає досить претензійно. На жаль, невелика, але неминуча проблема при спробі створити облік типу послуги. MTU визначає найбільший пакет, який буде відправлений на мережевий пристрій. Коли маршрутизатор приймає пакет, і цей пакет більше, ніж MTU інтерфейсу, який відповідає за його передачу, маршрутизатор виконує фрагментацію. Маршрутизатор ділить великий пакет на більш дрібні частини, що не перевищують MTU інтерфейсу, а потім передає ці частини. Маршрутизатор генерує нові заголовки для пакетів, які закінчилися, за допомогою яких одержувач зможе відновити вихідні пакети. На жаль, під час фрагментації значення порту буде втрачено для всіх, крім першого фрагмента. Це означає, що облік IP-адрес не може правильно підраховувати фрагментовані пакети, а тільки перші фрагменти або нефрагментовані пакети. У Ipfwadm є невеликий трюк, який дозволяє зчитувати пакети, навіть не знаючи порту другого і наступного фрагментів. Перша версія програмного забезпечення призвела до підробленого номера порту 08 fff, який ми могли запобігти. Ми виправляємо другий і наступний фрагменти, використовуючи правило:

```
# ipfwadm -A both -я -W ppp0 -P tcp -S 0/0 0xFFFF
```

Реалізація IP chains має трохи більше складні рішення, але результат тієї ж. При використанні команди ipchains потрібно використовувати правило: # ipchains-a forward-e ppp0-p tcp-f

Для iptables підійде правило:

```
# iptables -A FORWARD -e ppp0 -m tcp -p tcp -f
```

Це правило не скаже нам, який основний порт призначений для цих даних, але, принаймні, mi може бачити, скільки наших даних.

У ядрі 5.0 при налаштуванні можна вибрати параметр, який вирішує цю проблему, якщо ваша машина Linux діє як єдина точка доступу до мережі. Якщо ви включили опцію IP: завжди дефрагментувати при складанні ядра, всі пакети будуть повторно зібрані маршрутизатором Linux перед маршрутизацією і передачею. Ця

операція виконується перед брандмауером, і блок обліку стежить за пакетами . Таким чином, фрагментів просто не буде

Облік пакетів ICMP

Протокол ICMP не використовує номери службових портів, тому збирати статистику з цього питання складніше. ICMP використовує кілька різних типів пакетів . Багато з них нешкідливі і нормальні, в той час як інші з'являються тільки при особливих умовах. Іноді вони намагаються вивести систему з ладу, відправляючи велику кількість пакетів ICMP. Ця атака називається ping flood. Проти такої атаки IP-брандмауер прекрасний, а облік IP-адрес дозволяє з'ясувати, хто це зробив.

ICMP не використовує порти, на відміну від TCP і UDP для введення. Замість цього використовуються типи повідомлень ICMP. Ми можемо створити правила для кожного типу повідомлень ICMP. Для цього визначте тип повідомлення ICMP замість номера порту в команді ipfwadm.

Для збору даних про передачу пакетів ICMP для всіх типів повідомлень використовуйте правило:

```
# ipfwadm -A both -я -P icmp -S 0/0 8
# ipfwadm -A both -я -P icmp -S 0/0 0
# ipfwadm -A both -я -P icmp -S 0/0 0xff
# ipchains -A forward -p icmp -s 0/0 8
# ipchains -A forward -p icmp -s 0/0 0
# ipchains -A forward -p icmp -s 0/0 -f
```

або в iptables:

```
# iptables -A FORWARD -m icmp -p icmp -isports echo-request
# iptables -A FORWARD -m icmp -p icmp -isports echo-reply
# iptables -A FORWARD -m icmp -p icmp -f
```

Перше правило збирає інформацію щодо пакетів ICMP Echo Request (ping requests), друге правило збирає інформацію щодо пакетів ICMP Echo Reply (ping replies). Третє правило збирає інформацію від-носительно фрагментованих пакетів ICMP. Цей прийом подібний до описаного для фрагментованих пакетів TCP і UDP.

Якщо визначаємо джерела й / або адресата в ваших правилах, можливо стежити, звідки приходять пакети, зсередини мережі або зовні.

Облік по протоколах

Припустимо, нам цікаво, які протоколи використовуються нашим трафіком: TCP, UDP або ICMP. Тут нам допоможе правило:

```
# ipfwadm -A both -W ppp0 -P tcp -D 0/0
# ipfwadm -A both -W ppp0 -P udp -D 0/0
# ipfwadm -A both -W ppp0 -P icmp -D 0/0
```

або:

```
# ipchains -A forward -e ppp0 -p tcp -d 0/0
# ipchains -A forward -e ppp0 -p udp -d 0/0
# ipchains -A forward -e ppp0 -p icmp -d 0/0
```

або:

```
# iptables -A FORWARD -e ppp0 -m tcp -p tcp
# iptables -A FORWARD -o ppp0 -m tcp -p tcp
# iptables -A FORWARD -e ppp0 -m udp -p udp
# iptables -A FORWARD -o ppp0 -m udp -p udp
# iptables -A FORWARD -o ppp0 -m icmp -p icmp
```

За допомогою цих правил трафік буде аналізуватися через інтерфейс ppp0 для визначення типу протоколу: TCP, UDP або imcp, і відповідні лічильники будуть змінені для пакетів skin.

Використання результатів обліку IB

Щоб переглянути зібрані дані про трафік і налаштовані правила, ми використовуємо команду настройки брандмауера. Лічильники пакетів і байтів для кожного з наших правил будуть перераховані в вихідних даних.

Команди Ipfwadm, ipchains і iptables відрізняються тим, як збираються дані, тому ми розглянемо їх незалежно.

Зміна даних за допомогою ipfwadm

Команда ipfwadm дозволяє переглядати зібрані дані про трафік таким чином:

```
# ipfwadm -A -l
IP accounting rules
pkts bytes dir prot sourcedestination ports
9833 2345K i/o all 172.16.3.0/24 anywheren/a
56527 33M i/o all 172.16.4.0/24 anywheren/a
```

Він повідомляє нам кількість пакетів напрямки, які кожен представляє. Якщо ми використовуємо розширений вихідний формат з параметром-OE (не показаний тут, тому що вихідні дані занадто великі для сторінки), у нас також є нав'язливий список опцій і Імен інтерфейсів. Більшість полів у вихідних даних зрозумілі, тому я поясню лише деякі з них:

Напрямок, в якому застосовується правило . Очікувані значення тут-вхід, вихід або введення-виведення (в обох напрямках).

Виступайте проти протоколу, до якого застосовуються правила. Вибирати. Форма параметрів, що використовуються при виклику ipfwadm, кодується.

If name - ім'я інтерфейсу, до якого застосовується правило.

ifaddress

Адреси інтерфейсу, до якого застосовується правило.

За замовчуванням ipfwadm відображає лічильники пакетів і байтів у скороченій формі, округленій до найближчої тисячі (K) або мільйона (m). Ви можете вказати висновок точних чисел без округлення:

ipchains з використанням модифікації даних ipfwadm-a-l-oe-x

До тих пір, поки параметр-V не буде встановлено, команда ipchain не відображатиме облікові дані (лічильники пакетів і байтів:

ipchains-L-V як і у випадку з ipfwadm, ми можемо точно відображати пакети і лічильники байтів, використовуючи опцію-X:

ipchains-модифікація даних L-v-x з використанням iptables

Команда iptables поводиться дуже схоже на ipchain. Потім ми повинні використовувати-V для перегляду результатів відстеження трафіку. :

За допомогою команди # iptables-l-v ipchains ви можете використовувати-X для відображення точних даних.

Перезапуск лічильників

Лічильники для обліку IP-адрес можуть переповнюватися . Якщо вони переповняться, вам буде важко визначити їх реальні значення. Щоб уникнути цієї проблеми, ви повинні періодично реєструвати їх показання, а потім скидати лічильники на нуль, щоб почати збір інформації для наступного інтервалу обліку.

Команди ipfwadm і ipchain дозволяють вам зробити саме це:

```
# ipfwadm -A -z: # ipchains -Z: # iptables -Z
```

Ви можете навіть поєднувати висновок списку і обнулення, щоб гарантувати що ніякі дані обліку не Загублені між цими діями:

```
# ipfwadm -A -l -z: # ipchains -L -Z: # iptables -L -Z -v
```

Ці команди спочатку відобразять всі дані з лічильників, потім негайно скинуть лічильники і знову почнуть підрахунок. Якщо ви регулярно збираєте статистику, має сенс написати скрипт з відповідною командою і викликати його через Cron.

3.5. Інструкції адміністратору корпоративної мережі

Для груп комп'ютерів створіть 3 типи образів дисків:

- Serv / N для групи серверних комп'ютерів (n-номер комп'ютера)
- WS / N для групи робочих станцій
- Для групи комп'ютерів, що працюють з графікою GWS / n, що дозволяє швидко перезапустити систему в разі збою.
- Дані кожного співробітника зберігаються на сервері OPC serve / 1 і періодично синхронізуються на сервері OPC serve/2

- Створіть RAID 5 на кожному сервері.
- На сервері OPC serve / 2 Встановіть DHCP-сервер, який автоматично розподіляє IP-адреси користувачам мережі.
- Зробіть сервер OPC serve / 2 для домену.
- Зробіть сервер OPC serve / 2 маршрутизатором, веб-сервером і FTP-сервером.

Рекомендації щодо відновлення роботи робочих станцій у майбутньому у разі їх збою:

- Установка ОС Linux Suse.
- Файловий сервер (192.168.1.2) має*. файл на диску IMG.
- Запустіть програму True Image і перезапустіть розділ на диску
- Завантажити Linux.
- Перейдіть в меню " Налаштування "(за допомогою команди" Налаштування"), виберіть розділ" Мережа " і виберіть Налаштування інтерфейсу AT0.
- Щоб перезапустити ОС Linux, вам необхідно перезапустити 2 розділи HDA 1 і HDA 3
- HDA 4 краще не чіпати призначені для Користувача дані на ньому.
- Автоматично вказати IP-адресу (опція dhcp), DNS: 192.168.1.1.
- Налаштуйте авторизацію через домен (доменне ім'я-starditor)
- Жорсткий диск на кожній робочій станції з Linux розділений таким чином.

HDA1 = 1Gb filesystem=EXT3 “/boot”HDA3 = 260 Gb EXT3 “/”
HDA2 = 1400 mb “SWAP” HDA4 = 600 Gb EXT3 “/usr”
II) OS Windows 10 Pro

- Завантажити True image.

Зайти на файловий сервер (192.168.1. 2), запустити IMG файл диска. До сервера можна підключиться трьома способами перший через FTP, другий через мережу ms windows і третій через nfs. Зайти в каталог / / secure/recovery/img/windows / win.img

Далі зайти в Windows і налаштувати підключення до домену

На кожній робочій станцій з Windows HDD розбитий таким чином

HDA1 = 1Gb filesystem=NTFS “Loader” HDA3 = 250 Gb NTFS “TEMP”
HDA2 = 250gb filesystem=NTFS“Win&APPS” HDA4 = 600 Gb EXT3 “/usr”

Рекомендації щодо перезапуску сервера:

- Він може бути перезапущений через зображення в звичайному режимі.
- У тих випадках, коли конфігурація сервера не буде працювати, ви можете переналаштувати її вручну.

Встановлення параметрів на сервері:

Для установки сервера нам знадобиться дистрибутив Linux FC4.

OPC serve / 2 або OPC serve Computer / 1.

Перед установкою Linux необхідно переконатися, що ви встановили його на перший диск.

При установці Linux необхідно створити наступні розділи:

- Завантажувальний сокет 1 РОЗДІЛ 1 ГБ з файловою системою XT3 в якості "/ boot".
- Другий розділ-файлова система об'ємом 50 ГБ= XT3 в якості кореневого"/".
- Третій розділ-файлова система об'ємом 170 ГБ= xt3jounal FS tku як "/ usr".
- Після установки в BIOS увімкніть RAID-масив.
- Під час налаштування FTP-сервера він встановить порт 921.

Встановить наступні політики безпеки для папок:

- Вхід в систему дозволений тільки авторизованим користувачам. Коли користувачі входять в систему, вони переходять в свій каталог або папку груп.
- Для мережі 192.168.2.0 дозволений тільки вхід в систему.
- Під час налаштування веб-сервера:
- При вході в систему через порт 4510 виконайте авторизацію. А в разі успішної авторизації надайте доступ до програми, що працює з базою даних, по протоколу HTTP. Щоб увійти в порт 80, відкрийте сторінку підприємства. Доступ тільки для читання відкритий для всіх.

Установка

Демон RC.iptables R. C. Iptables-це наш скрипт, який є сервісом, і ми хочемо, щоб він автоматично завантажувався при завантаженні Linux.

Для цього виконайте наступні дії:

Копія RC.файлів для каталогу iptables / etc / init.d

Це робиться наступним чином: copy/temp / RC. iptables/etc / init.Команда D/

Або виберіть цей файл у Midnight Comander (команда MC) і натисніть клавішу F5.

3.6. Тестування конфігурації

Після того, як ви розробили відповідну конфігурацію брандмауера, важливо переконатися, що він робить те, що вам потрібно. Існує два способи перевірки конфігурації сервера:

Одним з рішень є використання тестового комп'ютера за межами вашої мережі, щоб спробувати прорватися через брандмауер. Але це може бути повільним і обмежується лише адресами, які ви можете використовувати.

Більш швидкий і простий метод, доступний в реалізації брандмауера Linux: дозволяє вручну генерувати тести і запускати їх через брандмауер, як якщо б ви тестували їх за допомогою реальних пакетів. Всі види підтримки брандмауера ядра Linux (ipfwadm, ipchains і iptables) забезпечують підтримку цього стилю тестування. Реалізація включає в себе використання відповідної команди перевірки .

Щоб перевірити вашу конфігурацію першим способом, було налаштовано кілька серверів, які будуть використовувати наступні порти 21 (FTP-файловий транспортний протокол), 80 (HTTP-веб-сервер виправлень), 111 (shtp - веб-служба виправлень), 20(SSH-з'єднання видалено).

До мережевого інтерфейсу at0 підключені наступні IP-адреси:

```
eth0 - 192.168.1.1/24
eth0:1 - 192.168.2.1/24
eth0:2 - 192.168.3.1/24
```

Щоб протестувати перший інструмент, вам знадобиться робоча станція, з якої Ви повинні будете спробувати увійти на сервер. Для тестування він буде встановлений:

Операційна система Linux і Windows 10 pro

Інтернет-браузер (Chrome, fire fox або будь-який інший).

Мережева карта, що підтримує технологію Ethernet .

Після налаштування сервера і робочої станції почніть тестування параметрів.

1. Встановіть IP-адресу на робочій станції на 192.168.1.2 / 24 і спробуйте пройти через будь-який порт, крім порту 20,21,22, SMB для цієї мережі

Повинні працювати тільки порти файлового сервера, і доступ до них повинен бути тільки з корпоративної мережі.

Перевірка: завантажте програму для сканування портів і почніть сканування за адресою 192.168.1.1, після чого нам буде надано список відкритих портів. Щоб переконатися, що програма сканування портів працює, ми намагаємося перейти на порт 80, який винен у відключенні мережі.

2. Ми встановлюємо адресу 192.168.2.2 на робочій станції, щоб відкрити порт FTP, HTTP SSH. Ми повторюємо процедуру зі сканером портів і намагаємося підключитися до сервера Samba через мережеве середовище. Для цієї підмережі Samba повинна бути відключена.

ВИСНОВКИ

В рамках дипломної роботи була спроектована локальна мережа, в якій використовувалися різні технології побудови. Ми проаналізували різні способи захисту мережі від атак. Аналізуються програмні та апаратні засоби забезпечення безпеки .

Проект комп'ютерної мережі підприємства, в якому були продумані і обрані топологія підключення, розміщення серверів і робочих станцій, програмне забезпечення, яке зможе виконувати всі функції, необхідні для функціонування підприємства. Для підключення комп'ютерів була обрана Розширена топологія star, вона є найбільш надійною і перевіреною на сьогоднішній день. Були обрані технології Ethernet. Ці технології дозволяють передавати дані зі швидкістю від 100 до 1000 мегабіт в секунду.

Для створення мережевої безпеки була продумана конфігурація сервера, на якому буде використовуватися брандмауер "Netfilter", який дозволить заборонити доступ. Система брандмауера також буде створювати звіти, в яких будуть записуватися всі невдалі спроби підключення до сервера. У корпоративних мережах буде використовуватися поділ на різні IP-підмережі, що допоможе розділити сервери і робочі станції і ускладнить проникнення хакерів в корпоративну мережу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Куроуз Дж., Росс К. Компьютерные сети. Нисходящий подход. Эксмо, 2016.
2. И. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Курс лекций. Бином. Лаборатория знаний, 2019.
3. Одом Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-105. Маршрутизация и коммутация. Вильямс, 2018
4. Олифер В. Г., Олифер Н. А. Сетевые операционные системы, 2-е изд. СПб.: Питер, 2018.
5. Олифер В. Г., Олифер Н. А. Основы компьютерных сетей. СПб.: Питер, 2019.
6. Олифер В. Г., Олифер Н. А. Безопасность компьютерных сетей. М.: Горячая Линия – Телеком, 2015.
7. Стивенс Ричард. Протоколы TCP/IP. Практическое руководство. СПб.: БХВ, 2013.
8. Таненбаум Э., УэзероллД. Компьютерные сети, 5-е изд. СПб.: Питер, 2019.
9. Sauter Martin. From GSM to LTE-Advanced, John Wiley & Sons, Ltd, 2014.
10. Davies Josef. Understanding IPv6, 3E, Pearson, 2012.
11. Kabiri Peyman. Privacy Intrusion Detection and Response, IGI Global, 2011.
12. Noonan Wes, Dubrawsky Ido. Firewall Fundamentals – Cisco Press, 2016.
13. PieprzykJosef, Hardjono Thomas, SeberryJennifer. Fundamentals of Computer Security – Springer, 2010.
14. Cole Eric. Network Security Bible, 2nd Edition – John Wiley & Sons, 2019.