МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

КУРСОВИЙ ПРОЄКТ: ВВЕДЕННЯ В МЕРЕЖІ

Методичні рекомендації

для студентів спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня

Харків
ХНЕУ ім. С. Кузнеця
2021

УДК 004.7(07.034)
К93

Укладачі: С. П. Євсеєв
О. Г. Король
А. А. Гаврилова

Затверджено на засіданні кафедри кібербезпеки та інформаційних технологій.
Протокол № 10 від 05.01.2021 р.

Самостійне електронне текстове мережеве видання

Курсовий проєкт: Введення в мережі [Електронний ресурс] : методичні рекомендації для студентів спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня / уклад. С. П. Євсеєв, О. Г. Король, А. А. Гаврилова. – Харків : ХНЕУ ім С. Кузнеця, 2021. – 52 с.

К93

Надано структуру, рекомендації та приклад виконання курсового проєкту "Введення в мережі".

Рекомендовано студентам, які навчаються за освітною програмою "Кібербезпека" першого (бакалаврського) рівня вищої освіти спеціальності 125 "Кібербезпека".

УДК 004.7(07.034)

Вступ

Методичні рекомендації та приклад виконання курсового проєкту "Введення в мережі" розроблено для студентів другого курсу, які навчаються за освітньою програмою "Кібербезпека" першого (бакалаврського) рівня вищої освіти спеціальності 125 "Кібербезпека".

Метою цього видання є забезпечення в межах курсового проєкту виконання практичного ситуаційного завдання зі створення корпоративної мережі, що повинно продемонструвати отримані студентами протягом вивчення даної дисципліни навички та вміння згідно із переліком компетентностей за освітньою програмою "Кібербезпека".

Завданням цих методичних рекомендацій є забезпечення підтримки необхідним матеріалом усіх етапів курсового проєктування, а саме:

постановку завдання курсового проєкту та його дефрагментацію на окремі завдання;

виконання необхідних розрахунків щодо побудови та розгортання корпоративної мережі, розроблення логічної та фізичної структурних схем корпоративної мережі;

розроблення практичних рекомендацій щодо розгортання системи безпеки за відповідним варіантом;

використання отриманих протягом навчання компетентностей для реалізації практичної частини проєкту;

використання довідкового матеріалу;

написання пояснювальної записки за результатом проєктування;

формулювання висновків за проведеною роботою.

Важливою частиною цих методичних рекомендацій також є підтримка самоорганізації, розподілення і контролю робіт протягом виконання усього курсового проєкту. Компетентності та результати навчання наведені в табл. 1.

Таблиця 1

Компетентності та результати навчання за освітньою компонентою "Курсовий проєкт: Введення в мережі"

Компетентності	Результати навчання
КФ-2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки	РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 13 – аналізувати проєкти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та здійснювати оцінювання результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем
	РН 47 – вирішувати завдання захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 53 – вирішувати завдання аналізу програмного коду на наявність можливих загроз

Розділ 1
Завдання на виконання курсового проєкту

Ознайомтеся із вхідними даними

Вас прийняли на роботу в якості системного інженера IT-компанії *"Pronet"* і доручили виконати перше відповідальне завдання: опрацювати ескізний варіант інфраструктури проєктованої мережі корпорації *"CorpXYZ"* (у якості XYZ – повинні фігурувати ініціали виконавця, наприклад, Сидоров Олексій Петрович *CorpSAP*).

Корпорація має головний офіс (будівля А) та дві філії:

- виробництво продукції **Manufacture** (M) – будівля B;
- відділ досліджень та новітніх розробок **Research** (R) – будівля C (рис. 1).

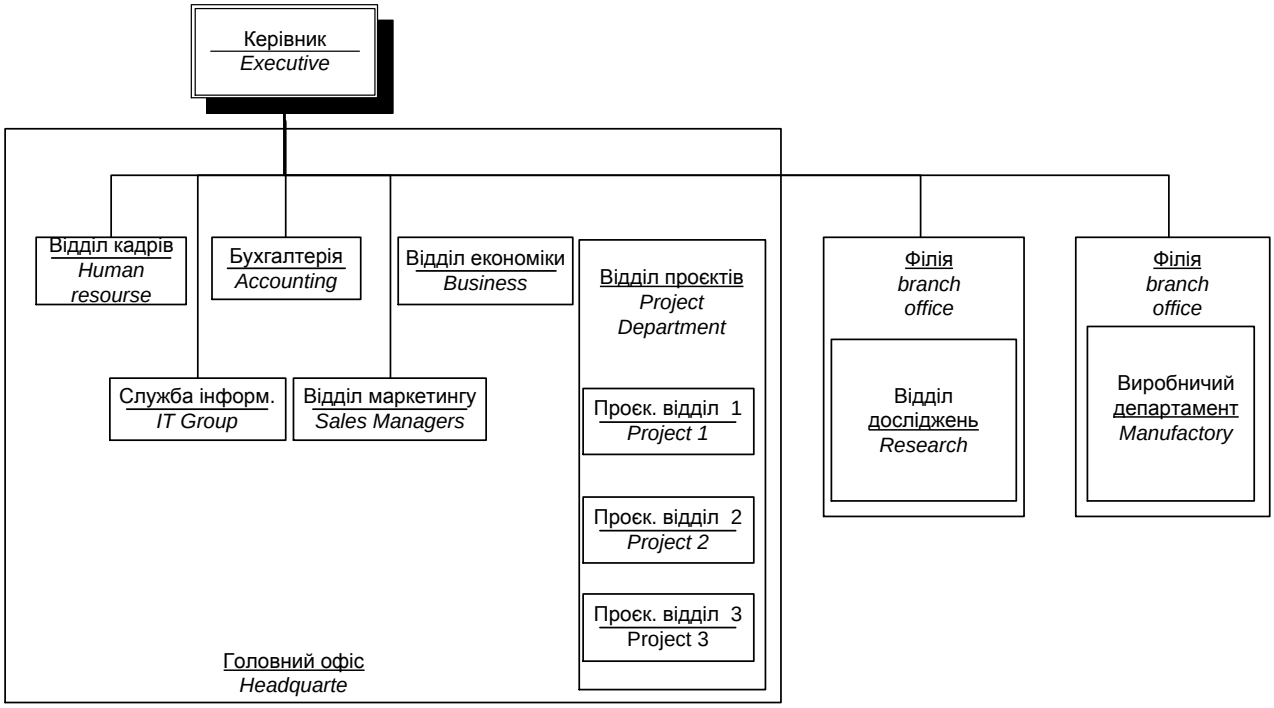

Рис. 1. **Структура підрозділів корпорації CorpXYZ**

Функціональні служби корпорації в головній будівлі А розташовані в такий спосіб:

Перший поверх. Підрозділи корпорації:

- відділ кадрів та підготовки спеціалістів **Human Resource** (HR);
- відділ маркетингу **Marketing** (M);

- служба інформаційних технологій і технічної підтримки **Information Technologies** (IT).

Другий поверх. Підрозділи:

- керівництво компанією **Executive** (E);
- бухгалтерія **Accounting** (Acc);
- відділ економіки та планування **Business** (Bus).

На третьому, четвертому та п'ятому поверхах розташоване проєктне відділення, при цьому:

Третій поверх. Проєктний відділ **Project 1** (P1);

Четвертий поверх. Проєктний відділ **Project 2** (P2);

П'ятий поверх. Проєктний відділ **Project 3** (P3).

Кожен проєктний відділ має свій конфіденційний сервер додатків.

Дві незалежні групи співробітників відділу маркетингу в основному працюють на ноутбуках і подали заявку на створення захищеної бездротової мережі WLAN з виходом в інтернет.

В одноповерховій будівлі B філії виробляються вироби двох типів, один з них на площах M1, інший – на площах M2. Крім того, є автоматизований склад готової продукції *Production* (P). Філія *Manufacture* (M) (будівля B) розташована в іншому місті, віддаленому на значну відстань, і з'єднана з головним офісом каналом T1. Філія *Research* (будівля C) зв'язується з головним офісом через інтернет з використанням *Site-to-Site VPN IPSec*. У двоповерховій будівлі третій відділ *Research* займає два поверхи, при цьому на 1 поверсі розташована робоча група *Research 1* (R1), на 2 поверсі – група *Research 2* (R2).

Ви створюєте ескізний проєкт інфраструктури мережі компанії *CorpXYZ*, що має один головний офіс, виробничу філію і дослідницький центр. У даний час у кожному офісі є невеликі локальні обчислювальні мережі (ЛОМ), які будуть об'єднані в єдину корпоративну мережу. В якості робочих станцій використовуються комп'ютери з встановленими операційними системами (ОС) *WinXP Prof*, частково з ОС різнорідних сімейств *Linux*. У найближчі 6 місяців планується перехід частини співробітників корпорації на ОС сімейства *MS Wi*n7, частково на *ОС Linux XX*. IT-керівництво *CorpSAP* прийняло рішення використовувати в якості базової мережевої *ОС MS Windows Server 2012* і готове використовувати активне мережеве обладнання (ваш варіант, наприклад, HP) там, де ви обґрунтовано його сплануєте.

Кілька груп співробітників працюють в Україні і Європі в своїх домашніх офісах SOHO, що підключаються до головного офісу за допомогою інтернету із використанням VPN-client. Максимальна кількість комп'ютерів у SOHO не більша 5. Крім того, є невеликий штат корпоративних співробітників *Teleworker*, які з'єднуються з головним офісом, використовуючи стільниковий інтернет (рис. 2).

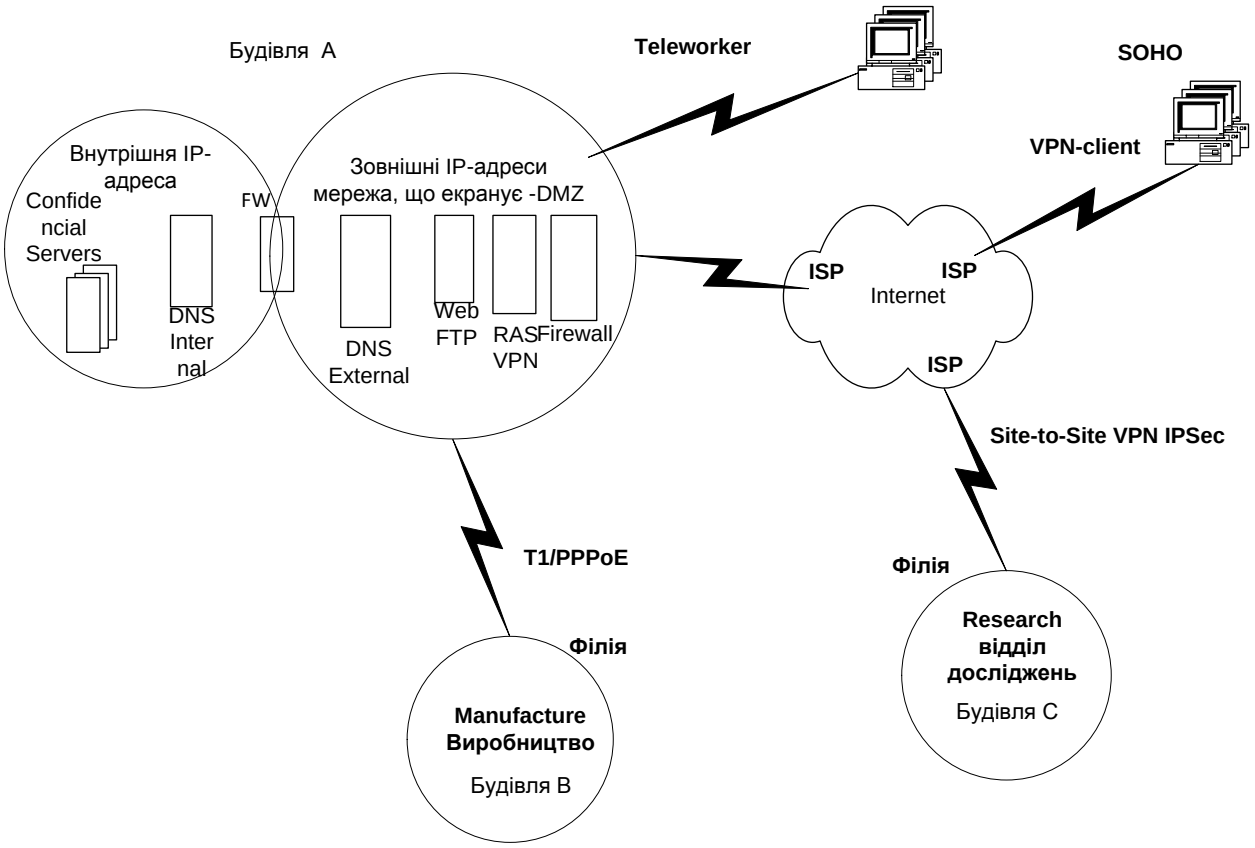

Рис. 2. **Схема розташування корпорації CorpXYZ**

У якості вихідних даних прийміть достатність смуги пропускання каналів передачі даних для забезпечення мережевого трафіка із задовільним клієнтським відгуком. Однак ви повинні так спроєктувати розташування серверів, щоб мінімізувати службовий трафік мережі.

Базовою технологією мережі є *Ethernet* за стандартом 100/1000BASE-T, Gigabit Ethernet 1000BASE.

Кожен підрозділ корпорації має свій конфіденційний сервер даних InfSrv_ ##, доступ до якого можуть мати тільки співробітники відповідного підрозділу.

Для зовнішніх IP-інтернет-адрес корпорації (головна будівля і філії) використовуйте такий діапазон адрес (Public_IP) 199.46. (2 × G-1) ×10 + N.0 / 24, де N – номер варіанта завдання.

Для діапазону внутрішніх адрес (Private_IP) використовуйте:

- для головної будівлі А діапазон адрес 10.10 + G × 20 + N.0.0 / 16;
- для будівлі В – адреси 172.16 + N. (G-1) × 64.0 / 18;
- для будівлі З – адреси 192.168.16 × (Nmod15-1) .0 / 22,

де G – номер групи, N – номер варіанта завдання.

Вихідні числові дані до варіантів курсового проєкту наведені в додатку А у поданому прикладі курсового проєкту.

Під час виконання роботи необхідно дотримуватися таких вимог:

- у якості служби каталогів корпоративної мережі використовувати *Active Directory*;
- надати доступ до розміщених у головному офісі Web-, FTP- та MX-серверів корпорації *CorpXYZ* як користувачам інтернету, так і користувачам внутрішньої корпоративної мережі (*Intranet*) у будь-який час та будь-який день тижня;
- ізолювати корпоративну мережу від інтернету, Web-, FTP- і MX-серверів;
- ізолювати внутрішній простір імен;
- захистити всі дані, що пересилаються між головним офісом і філією *Research*;
- кожен підрозділ повинен мати свій конфіденційний сервер додатків;
- забезпечити захист конфіденційних даних під час пересилання в підрозділах корпоративної мережі з використанням IPSec;
- забезпечити захист конфіденційних даних під час пересилання через інтернет з використанням VPN;
- забезпечити безпечний перегляд корпоративної мережі віддалених користувачів;
- забезпечити захист бездротових мереж WLAN;
- забезпечити надійну роботу з'єднань шляхом введення додаткових резервних маршрутних підключень;
- забезпечити проведення аудиту та відеоконференцій (*);
- передбачити заходи щодо зниження мережевого трафіка, що викликається потоковими аудіо- і відеоконференціями (*);

- виконати оцінювання вартості закупівлі мережевого обладнання, включаючи вартість супутніх програмних продуктів (ПП);
- оцінити витратну вартість матеріалів структурованої кабельної мережі (СКМ), включаючи монтажні стійки (*).

Рекомендації

Під час розроблення інфраструктури мережі візьміть до уваги:

- використання VLAN технології;
- можливість використання IPSec у транспортному і/або тунельному режимі, L2TP/IPSec, PPP для захисту конфіденційних даних, що пересилаються як усередині корпоративної мережі, так і під час приєднання віддалених клієнтів WAN-каналами і інтернетом;
- різноманіття методів аутентифікації. Вирішіть питання про необхідність використання зовнішніх сертифікатів і/або установки власної корпоративної служби сертифікатів;
- способи забезпечення безпеки мережі за допомогою брандмауерів і/або фільтрувальних маршрутизаторів, DMZ;
- можливість використання в обраних вами маршрутизаторах способів VLSM, CIDR-розподілу на підмережі;
- можливість використання служб каталогу *Active Directory WS 2012/2008*;
- можливість використання прямого і зворотнього кешувального чи проксі-сервера;
- спосіб ідентифікації маршрутизаторів і захисту даних, що передаються між маршрутизаторами.

У процесі реалізації рішення у разі *можливості використовуйте мережеві служби операційної системи WS* 2012/2008. Ухвалення інших мережевих ОС, служб і активного мережного обладнання повинно бути обґрунтовано. Вважається, що персонал мережевої підтримки та адміністрування знає систему WS 2019/2012 і додаткових коштів на його перенавчання не передбачено.

---

* Необов'язково (але бажано) для виконання.

Приблизна послідовність виконання курсового проєкту

1. Усвідомте завдання. Визначте параметри і чисельні значення вашого індивідуального варіанта завдання. Осмисліть поставлене перед вами завдання, підберіть матеріали і починайте активно працювати з першого тижня занять.

2. Пам'ятайте, що наступні етапи виконання роботи є ітераційними і вам не раз доведеться корегувати результати пройдених етапів у міру виконання наступних етапів.

3. Розробіть чорновий варіант логічної і фізичної структури мережі з урахуванням принципів і правил побудови структурованих кабельних систем (СКС). Виокремте автономні структурні модулі в ієрархічній структурі корпоративної мережі.

4. Визначте кількість сегментів у мережі, визначте VLANи мережі.

5. Обґрунтуйте вибір мережевого обладнання (*Switches, Routers*) і пов'яжіть його з кожним сегментом мережі

6. Розробіть структуру DNS-служби. Оберіть простір імен DNS. Визначте місце розташування DNS-серверів і їх функції (основна, вторинна, кешувальна, пересильна, заглушка).

7. Спроєктуйте логічну структуру AD-мережі. Призначте простір імен AD. Обґрунтовано вирішіть, чи буде ваша мережа одно- або багатодоменною. Оберіть сайти. Визначте розміщення доменних контролерів, глобальних каталогів і майстрів операцій FSMO.

8. Виконайте розміщення базових мережевих серверів DNS, DHCP, компонентів AD з урахуванням забезпечення надійності та оптимізації аутентифікації у мережі.

9. Скорегуйте розміщення робочих місць і мережевого устаткування в головній будівлі і філіях.

10. Розробіть схему розподілу адресного простору.

11. Обґрунтуйте вибір протоколів маршрутизації, побудуйте ієрархічну схему з'єднання комутаторів і маршрутизаторів мережі, а також таблиці настроювання маршрутизаторів.

12. Подайте у табличному вигляді налаштування статичних і динамічних адрес компонентів мережі у кожному сегменті мережі.

13. Оберіть спосіб забезпечення безпеки корпоративної мережі і типи брандмауерів або фільтрувальних маршрутизаторів. Опишіть налаштування обраного сервісу.

14. Оберіть спосіб забезпечення захисту від несанкціонованого доступу до інформації, розташованої на конфіденційних серверах підрозділів.

15. Оберіть метод підключення до корпоративної мережі віддалених співробітників. Оберіть спосіб забезпечення безпеки й опишіть налаштування сервера і клієнта.

16. Оцініть витрати на придбання мережевого обладнання та програмного забезпечення.

17. Проведіть остаточний аналіз інфраструктури мережі, зробіть висновок.

18. Оформіть графічні аркуші і розрахунково-пояснювальну записку і підготуйтеся до захисту.

Змістовні рекомендації щодо створення курсового проєкту

Текстова частина курсового проєкту повинна містити:

- порівняльний аналіз можливих варіантів інфраструктури мережі;
- обґрунтування обраного варіанта і всіх прийнятих вами технічних рішень;
- фізичну структуру мережі і схему (таблиці) розподіл / призначення адресного простору і налаштування DHCP-серверів;
- схему (таблиці) простору доменних імен корпорації і налаштування DNS-серверів;
- інфраструктуру корпоративної мережі з розміщенням серверів мережевих служб і серверів додатків;
- схему розміщення мережевого обладнання СКС у головній будівлі корпорації;
- структуру AD-мережі з обґрунтуванням обраної топології реплікації;
- опис налаштувань обраних сервісів і засобів забезпечення безпеки мережі;
- економічний розрахунок витратної вартості придбання активного обладнання мережі та програмних продуктів.

Курсовий проєкт повинен бути подано у вигляді:

1. Розрахунково-пояснювальної записки обсягом від 25 машинописних сторінок, містить розрахунки, рисунки, таблиці та ілюстрації (основна частина), а так само графічну частину об'ємом не менше 3-х аркушів формату А4.

2. Електронний документ, поданий на носії даних.

Записка оформляється відповідно до вимог кафедри в середовищі *MS Word, MS Visio*.

Під час захисту курсового проєкту повинні бути висвітлені такі питання:

1. Оформлення РПЗ, склад матеріалів на електронному носії.
2. Планування IP-адрес.
3. Обрання, розміщення та налаштування DHCP-серверів /DHCP Relay agent
4. Обрання, розміщення та налаштування DNS-серверів. Простір імен.
5. Розміщення конфіденційних і інформаційних серверів.
6. Вибір, розміщення й налаштування ієрархії комутаторів VLAN.
7. Вибір, розміщення й налаштування роутерів WAN-з'єднань та інтернет.
8. Розміщення й налаштування NAT/PAT.
9. DMZ. Розміщення і налаштування серверів у захищеній зоні.
10. Реалізація *Remote Access SOHO/TeleWorker/NAPolicy*.
11. Реалізація служб сертифікації.
12. AD – логічна і фізична структура /DC/FSMO/Sites/Replica/GP.
13. Віртуалізація пулу серверів (ферма, фабрика, хмара). Вибір серверів (залізо) і ПЗ.
14. Деталізація мережевого рішення відповідно до ТЗ (WLAN, VPN).
15. Кошторис витрат на активне мережеве обладнання (у тому числі сервера) і ПЗ.

Розділ 2
Розрахунок вихідних даних курсового проєкту

У табл. 2 подано величини K та L залежно від номера варіанта N, який відповідає вашому порядковому номеру в списці групи.

Таблиця 2

Обрання K і L залежно від варіанта N

Номер варіанта N	K	L
1 – 5	N+1	2
6 – 10	N–4	3
11 – 15	N–9	4
16 – 18	N–14	5
19 – 24	N+1	2
25 – 29	N–4	3
30 – 35	N–9	4

У табл. 3 подано поповерхове розташування робочих груп та кількість робочих станцій за трьома проєктними відділами в будівлі A.

Таблиця 3

Поповерхове розташування груп та станцій

Відділи	*Project 1*		*Project 2*		*Project 3*	
Поверхи	Кількість роабочих груп (кімнат)	Кількість робочих станцій у групі, не більше	Кількість робочих груп	Кількість робочих станцій у групі, не більше	Кількість робочих груп	Кількість робочих станцій, не більше
Поверх 1	$12 + \left\lfloor \left\lvert \frac{L-K}{G} \right\rvert \right\rfloor$	6 + G				
Поверх 3			4 + L	12 + |L – K|		
Поверх 5					6 + L	14 – G

У табл. 4 наведені дані за кількістю робочих груп і робочих станцій в одноповерховій будівлі філії B *Manufacture*.

Таблиця 4

Кількість груп та станцій за поверхами філії B

Відділи	*Manufacture*	
Підрозділи	Кількість робочих груп (кімнат)	Кількість робочих станцій у групі, не більше
M1	$32 - \frac{3K + L}{2} \times Grigh$	$4 + \left[\frac{22}{K + L} \times G \right]$
M2	$22 + L - 2 \times K$	$20 + G \times (2 \times L - 1)$
P	$6 + K \times G$	$24 + G \times L - K$

У табл. 5 подані поповерхова кількість груп та робочих станцій у будівлі C філії *Research*.

Таблиця 5

Кількість груп та станцій за поверхами філії C

Відділи	Res 1		Res 2	
Поверхи	Кількість робочих груп (кімнат)	Кількість робочих станцій у групі, не більше	Кількість робочих груп	Кількість робочих станцій, не більше
Поверх 1	8 – L	14 + | L – K |		
Поверх 2			9 + |L – K|	5 + K×G

У таблицях зазначені:

N – номер варіанта, G – номер групи (1, 2, 3,…), |…| – модуль, […] – найменше ціле.

У табл. 6 подано дані загальнокорпоративних служб.

Таблиця 6

Дані за загальнокорпоративними службами

Manag.	Служба *Human Resource, IT gr., Sales*,		*Accounting*		*Business*	
Параметр K	Кількість робочих груп (кімнат)	Кількість робочих станцій у групі, не більше	Кількість робочих груп	Кількість робочих станцій у робочій групі	Кількість робочих груп	Кількість робочих станцій у робочій групі
1	6	8	4	9	3	6
2	5	12	3	14	2	5
3	4	8	3	8	2	4
4	6	10	5	12	3	8
5	5	8	4	13	2	7

У табл. 7 подані варіанти детального опрацювання відповідних компонентів інфраструктури корпоративної мережі, включаючи вибір і налаштування мережевого обладнання заданої компанії-виробника, а також конфігурація серверів WS2019/2012 та операційнних систем робочих станцій користувачів.

Таблиця 7

Налаштування компонентів інфраструктури корпоративної мережі

Варіанти	Предметна область	Реалізація	Обладнання та ПЗ
1	2	3	4
01	Інформаційна система для школи (коледжу, гімназії)	WLAN/ EAP2	Juniper
02	Інформаційна система для виставкового центру	QoS/VoIP	DLink
03	Інформаційна система для центру служби зайнятості	QoS/VoIP	Cisco
04	Інформаційна система для акціонерного товариства, яке має філії в інших містах	Remote Access/ RADIUS, NAP	HP
05	Інформаційна система для невеликої фінансової компанії	DMZ/ NAT_PAT	DLink
06	Інформаційна система для невеликої інвестиційної фірми		Huawei
07	Інформаційна система для архітектурної організації	PKI/Cert.Service	Juniper
08	Інформаційна система для машинобудівного підприємства		HP
09	Інформаційна система для автоматизації організаційно-розпорядчого документообігу виробничого підприємства	VPN IPSec client-server	Російські додатки
10	Інформаційна система для автоматизації документообігу оперативного управління виробничого підприємства		HP
11	Інформаційна система для автоматизації документообігу підсистеми збуту виробничого підприємства	Virtual Server Farm	Cisco
12	Інформаційна система для організаційно розпорядчого документообігу установи		Huawei
13	Інформаційна система для факультету університету	Web/ SSL-TLS	Juniper
14	Інформаційна система для кафедри університету		HP
15	Інформаційна система для торгового підприємства	DMZ/ NAT_PAT	Cisco
16	Інформаційна система для авіапідприємства		HP

Закінчення табл. 7

1	2	3	4
17	Інформаційна система для лікувального закладу (лікарні)	QoS/VoIP	Російські додатки
18	Інформаційна система для лікувального закладу (поліклініки)		HP
19	Інформаційна система для банку	VPN IPSec Site to Site	Juniper
20	Інформаційна система для культурно-спортивного центру		Huawei
21	Інформаційна система для видавництва з філіями в інших містах	PKI/Cert.Service	DLink
22	Інформаційна система для школи (коледжу, гімназії)	WLAN/ EAP2	Juniper
23	Інформаційна система для виставкового центру	QoS/VoIP	DLink
24	Інформаційна система для центру служби зайнятості	QoS/VoIP	Cisco
25	Інформаційна система для акціонерного товариства, який має філії в інших містах	Remote Access/ RADIUS, NAP	HP
26	Інформаційна система для невеликої фінансової компанії	DMZ/ NAT_PAT	DLink
27	Інформаційна система для невеликої інвестиційної фірми		Huawei
28	Інформаційна система для архітектурної організації	PKI/Cert.Service	Juniper
29	Інформаційна система для машинобудівного підприємства		HP
30	Інформаційна система для автоматизації організаційно-розпорядчого документообігу виробничого підприємства	VPN IPSec client-server	Російські додатки
31	Інформаційна система для автоматизації документообігу оперативного управління виробничого підприємства		HP
32	Інформаційна система для авіапідприємства		HP
33	Інформаційна система для лікувального закладу (лікарні)	QoS/VoIP	Російські додатки
34	Інформаційна система для лікувального закладу (поліклініки)		HP
35	Інформаційна система для банку	VPN IPSec Site to Site	Juniper
36	Інформаційна система для культурно-спортивного центру		Huawei

У табл. 8 подані варіанти обрання способу реалізації мережі та устаткування з програмним забезпеченням.

Таблиця 8

Обрання способу реалізації мережі та устаткування з програмним забезпеченням

Варіанти	Предметна область	Реалізація	Устаткування та ПЗ
1	2	3	4
01	Інформаційна система для автоматизації організаційно-розпорядчого документообігу виробничого підприємства	WLAN/ EAP2	Huawei
02	Інформаційна система для автоматизації документообігу оперативного управління виробничого підприємства	QoS/VoIP	Juniper
03	Інформаційна система для автоматизації документообігу підсистеми збуту виробничого підприємства	QoS/VoIP	HP
04	Інформаційна система для організаційно-розпорядчого документообігу установи	Remote Access/ RADIUS, NAP	HP
05	Інформаційна система для факультету університету	DMZ/ NAT_PAT	HP
06	Інформаційна система для кафедри університету		Cisco
07	Інформаційна система для торгового підприємства	PKI/Cert.Service	HP
08	Інформаційна система для авіапідприємства		Juniper
09	Інформаційна система для лікувального закладу (лікарні)	VPN IPSec client-server	Huawei
10	Інформаційна система для лікувального закладу (поліклініки)		DLink
11	Інформаційна система для банку	Virtual Server Farm	HP
12	Інформаційна система для культурно-спортивного центру		Cisco
13	Інформаційна система для видавництва з філіями в інших містах	Web/ SSL-TLS	DLink
14	Інформаційна система для автотранспортного підприємства		Juniper
15	Інформаційна система для підприємства зв'язку	DMZ/ NAT_PAT	DLink
16	Інформаційна система для залізничного вокзалу		HP
17	Інформаційна система для школи (коледжу, гімназії)	QoS/VoIP	HP
18	Інформаційна система для виставкового центру		DLink

Закінчення табл. 8

1	2	3	4
19	Інформаційна система для центру служби зайнятості	VPN IPSec Site to Site	Huawei
20	Інформаційна система для акціонерного товариства, що має філії в інших містах		Juniper
21	Інформаційна система для невеликої фінансової компанії	PKI/Cert.Service	HP
22	Інформаційна система для невеликої інвестиційного фірми	WLAN/ EAP2	Cisco
23	Інформаційна система для архітектурної організації	QoS/VoIP	HP
24	Інформаційна система для машинобудівного підприємства	QoS/VoIP	HP
25	Інформаційна система для автоматизації організаційно розпорядчого документообігу виробничого підприємства	WLAN/ EAP2	Huawei
26	Інформаційна система для автоматизації документообігу оперативного управління виробничого підприємства	QoS/VoIP	Juniper
27	Інформаційна система для автоматизації документообігу підсистеми збуту виробничого підприємства	QoS/VoIP	HP
28	Інформаційна система для організаційно розпорядчого документообігу установи	Remote Access/ RADIUS, NAP	HP
29	Інформаційна система для факультету університету	DMZ/ NAT_PAT	HP
30	Інформаційна система для кафедри університету		Cisco
31	Інформаційна система для торгового підприємства	PKI/Cert.Service	HP
32	Інформаційна система для авіапідприємства		Juniper
33	Інформаційна система для лікувального закладу (лікарні)	VPN IPSec client-server	Huawei
34	Інформаційна система для лікувального закладу (поліклініки)		DLink
35	Інформаційна система для банку	Virtual Server Farm	HP

Приклад створення пояснювальної записки за курсовим проєктом з дотриманням встановлених вимог наведено в додатку А, у прикладі виконання курсового проєкту.

Рекомендована література

1. Вимоги до оформлення курсових і дипломних проєктів: методичні рекомендації для студентів галузі знань 12 "Інформаційні технології" / уклад. А. А. Гаврилова, С. П. Євсеєв, Г. П. Коц та ін. – Харків : ХНЕУ ім. С. Кузнеця, 2018. – 49 с.

2. The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes / S. Yevseiev at al. //Восточно-европейский журнал передовых технологий. – 2017. – № 5/9(89). – С. 19–36.

3. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа : http://bdu.fstec.ru/vul.

4. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [Електронний ресурс] : Постанова НБУ від 28.09.2017р. № 95. – Режим доступу : http://zakon2. rada.gov.ua/laws/show/en/v0095500-17/page.

Додатки

Додаток А

Приклад створення пояснювальної записки до курсового проєкту

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КУРСОВИЙ ПРОЄКТ: ВВЕДЕННЯ В МЕРЕЖІ
Тема: "Створення територіально розподіленої корпоративної мережі інформаційної системи для архітектурної організації"

Виконав: ____студент 2 курсу_____
групи 6.04.125.013.19.1_____
спеціальності 125 "Кібербезпека"_____
факультету інформаційних технологій__
Панков Данило Сергійович_____

Перевірив: докт. техн. наук, професор
Євсеєв С. П.

Харків – 202_ рік

РЕФЕРАТ

Курсовий проєкт містить: 34 стр., 5 табл., 10 рис., 20 літ. джерел.

Метою курсового проєкту є створення територіально розподіленої корпоративної мережі корпорації CorpPDS.

Об'єктом проєктування є процес побудови інфраструктури корпоративної мережі акціонерного товариства з філіями в інших містах та деяким штатом працівників SOHO та Teleworker.

Предметом дослідження є розроблення інфраструктури корпоративної мережі корпорації CorpPDS.

Мережа, що розроблена, охоплює головний офіс та дві філії компанії, а також SOHO і співробітників, які віддалено працюють. Дана мережа містить підключення через VPN для забезпечення безпечного з'єднання. Робочі групи обмежені за допомогою технології VLAN.

ACTIVE DIRECTORY, JUNIPER, VPN, БЕЗПЕКА, КОМУТАТОР, МАРШРУТИЗАТОР, СЕРВЕР, КОМП'ЮТЕРНА МЕРЕЖА, ТОПОЛОГІЯ, IPSEC, DNS, SOHO, ПРОТОКОЛ.

ЗМІСТ

ВСТУП 24

ЗАВДАННЯ 6

1 ОПИС СТРУКТУРИ ПІДПРИЄМСТВА 7

2 РОЗПОДІЛ IP-АДРЕС 30

3 ВИКОРИСТАННЯ VLAN 33

4 РОЗРОБЛЕННЯ СХЕМИ МЕРЕЖІ 35

5 ВИБІР ВИКОРИСТОВУВАНОГО ОБЛАДНАННЯ 41

5.1 Вибір комутаторів та точок доступу 41

5.2 Вибір маршрутизаторів та міжмережевих екранів 41

5.3 Розміщення обладнання у стійках 42

6 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖІ 43

6.1 IBM Security Guardian Key Lifecycle Manager 43

6.2 Key Manager Plus 44

7 РОЗРАХУНОК ВАРТОСТІ СТВОРЕННЯ МЕРЕЖІ 47

ВИСНОВОК 48

СПИСОК ДЖЕРЕЛ ІНФОРМАЦІЇ 49

ПЕРЕЛІК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AD – служба каталогів Active Directory

DMZ – Demilitarized zone (демілітаризована зона)

DNS – Domain name system (система доменних імен)

FW – Fire Wall (Файервол / Міжмережевий екран)

GE – Gigabit Ethernet

LAN – Local area network (локальна обчислювана мережа)

SOHO – Small office/Home office (малий / домашній офіс)

TW – Teleworker (телефонний робочий)

VLAN – Virtual LAN (віртуальна локальна мережа)

VPN – Virtual private network (віртуальна приватна мережа)

WAN – Wide area network (глобальна обчислювана мережа)

WLAN – Wireless local area network (бездротова локальна обчислювана мережа)

ОС – операційна система

ВСТУП

На сьогоднішній день успіх більшості компаній будується на використанні комп'ютерних технологій. Для того, щоб пов'язати всі комп'ютери, використовують комп'ютерні мережі. Мережа потрібна для того, щоб усі комп'ютери у мережі мали між собою зв'язок. Але просто побудувати мережу все ж таки недостатньо, потрібно забезпечити її захист, швидкість, безпеку, розподіл. Для побудови комп'ютерної мережі варто враховувати багато факторів, від яких залежить бездоганна робота вашої мережі. Найголовнішим пунктом у проєктуванні мережі є забезпечення її захисту, тому що мережа містить також сервери, а якщо зловмисник отримає доступ до них, то він зможе не тільки викрасти важливу для вашої компанії інформацію, а й взагалі зруйнувати мережу.

Мета курсового проєкту – створення територіальної розподіленої корпоративної мережі корпорації CorpPDS.

Під час проєктування мережі необхідно враховувати як адміністративну структуру, так і територіальне розташування об'єктів. Корпоративна мережа повинна забезпечувати достатню облікову швидкість для обміну даними, а частка службового трафіка повинна бути мінімальною.

Завдання, що вирішуються у процесі виконання курсової роботи:

аналіз поставленого завдання;

створення фізичної схеми мережі;

створення логічної схеми мережі;

проєктування підключення VPN;

проєктування структури Active Directory;

забезпечення підключення VLAN;

забезпечення підключення філій за допомогою WWAN.

Отриманий у результаті виконання роботи проєкт корпоративної мережі повинен відповідати технічним завданням та мати найменшу можливу вартість.

ЗАВДАННЯ

Варіант № 7.

Створити територіально розподілену корпоративну мережу інформаційної системи для архітектурної організації.

Корпорація має головний офіс та дві філії.

Для формування безпеки даних використовувати PKI/Cert.Service.

Обладнання та програмне забезпечення компанії Juniper.

Для зовнішніх IP-адрес корпорації (головний будинок та філії) використовується такий діапазон адрес 199.46.50.0/24.

Для діапазону внутрішніх адрес використовується:

для головного будинку А діапазон адрес 10.60.0.0/16;

для будинку В діапазон адрес 172.36.64.0/18;

для будинку С діапазон адрес 192.168.64.0/22.

1 ОПИС СТРУКТУРИ ПІДПРИЄМСТВА

Об'єктом проєктування є корпоративна мережа корпорації CorpPDS з філіями в інших містах (рис. 1.1).

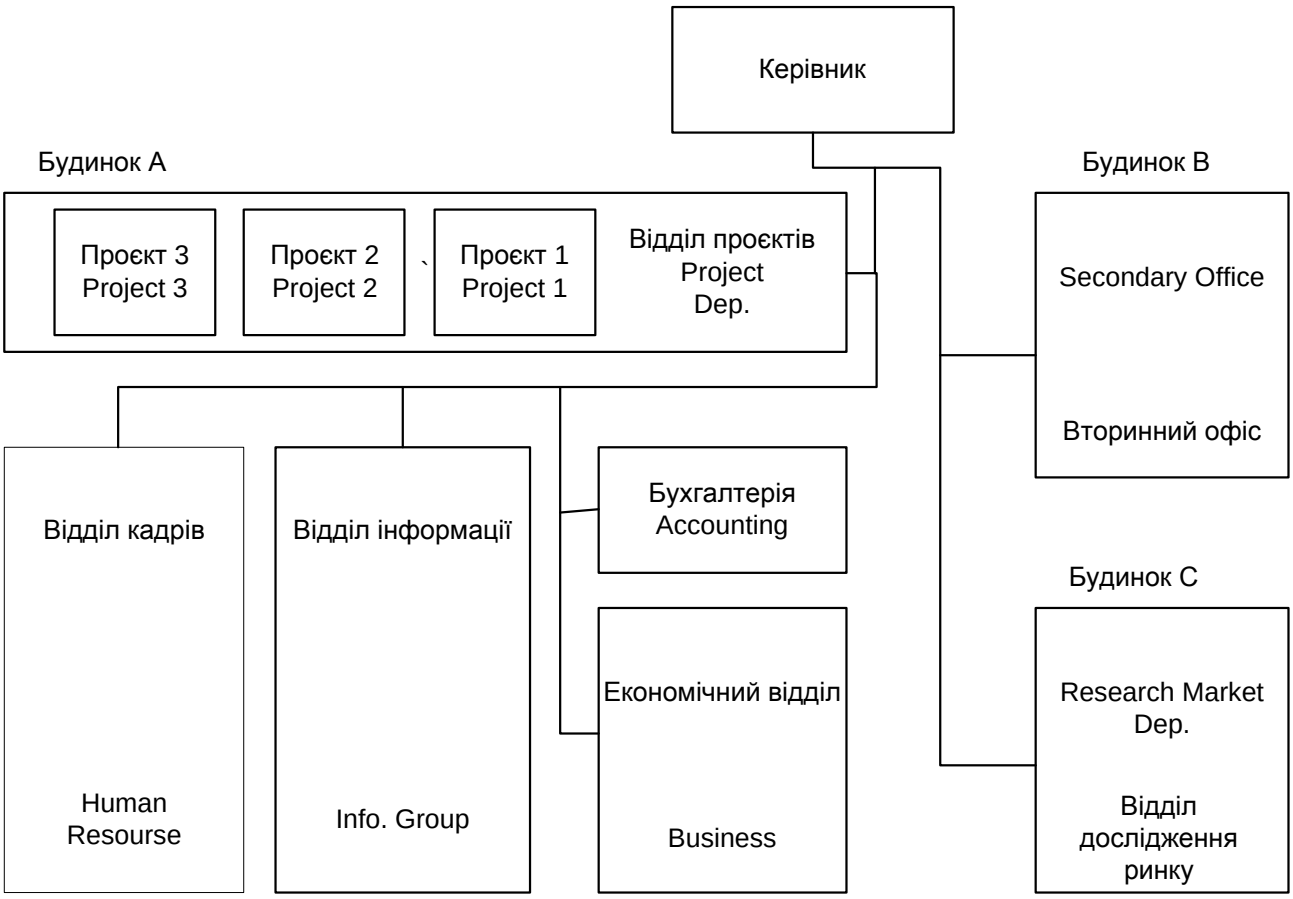

Рисунок 1.1 – Структура підрозділів та філій корпорації CorpPDS

Корпорація має головний офіс та дві філії:

вторинний офіс компанії Secondary (Se) – будинок В;

відділ досліджень ринку Research (R) – будинок С.

Функціональні служби корпорації у головному будинку А розташовані таким чином:

Перший поверх. Підрозділи корпорації:

відділ кадрів та підготовки спеціалістів Human Research (HR);

відділ інформації ринкової ситуації Info**.** Group (IG).

Другий поверх. Підрозділи корпорації:

бухгалтерія Accounting (Ac);

відділ спостереження за економічною ситуацією Business (Bs).

Третій, четвертий та п'ятий поверхи. Підрозділи проєктних відділень, при цьому:

третій поверх – проєктне відділення 1 Project 1 (P1);

четвертий поверх – проєктне відділення 2 Project 2 (P2);

п'ятий поверх – проєктне відділення 3 Project 3 (P3).

Кожен проєктний відділ має свій особистий сервер додатків.

Дві незалежні групи співробітників відділення інформації в основному працюють на ноутбуках, подали заяву на створення захищеної бездротової мережі WLAN з можливістю виходу до інтернету.

В одноповерховому будинку B філії відбуваються економічні дослідження двох типів, одне з них на розділі SR1, а друге – на розділі SR2. Також філія має розділ підсумкового дослідження Final Research (FR). Будинок філії B розташований у другому місті та з'єднаний з головним офісом за допомогою каналу T1. Будинок C має два поверхи з відділами Market Research (MR1, та MR2), кожен з яких знаходиться на першому та другому поверсі відповідно. Філія будинку C пов'язана з головним офісом через інтернет за допомогою Site-to-Site VPN.

Керівництво корпорації CorpPDS прийняло рішення використовувати у якості базової мережевої ОС MS Windows Server 2019/2012 та готове використовувати мережеве обладнання компанії Juniper там, де його застосування буде необхідне.

Декілька груп співробітників працюють у близькому та далекому зарубіжжі у своїх домашніх офісах SOHO, які підключаються до головного офісу через інтернет за допомогою VPN-client. Максимальна кількість комп'ютерів у SOHO не більше ніж 5. Більш того, наявний невеликий штат співробітників Teleworker (TW), який з'єднується з головним офісом за допомогою стільникового інтернету (рис. 1.2).

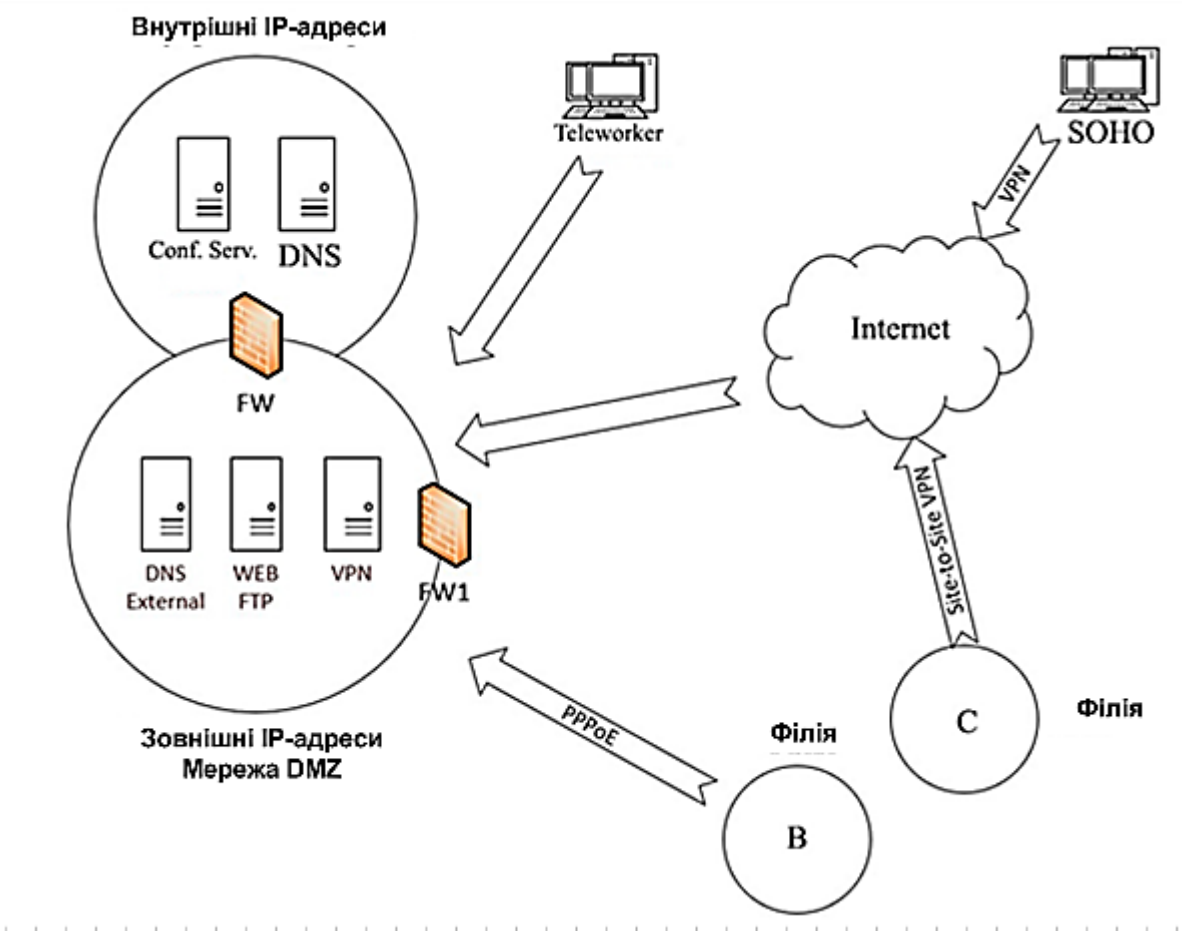

Рисунок 1.2 – Схема розташування корпорації CorpPDS

Смуга пропускання каналів передачі даних повинна бути достатньою для забезпечення мережевого трафіка з задовільним клієнтським відгуком.

Службовий трафік повинен бути мінімізований.

Базовою технологією мережі є Ethernet за стандартом 100/1000BASE-T, Gigabit Ethernet 1000BASE.

Кожен із підрозділів повинен мати свій особистий сервер даних, доступ до яких можуть мати лише співробітники відповідного відділення.

Для зовнішніх IP-адрес корпорація (головний будинок та філії) використовується такий діапазон адресів 199.46.50.0/24.

Для діапазону внутрішніх адресів використовується:

для головного будинку А діапазон адресів 10.60.0.0/16;

для будинку В діапазон адресів 172.36.64.0/18;

для будинку С діапазон адресів 192.168.64.0/22.

У табл. 1.1 наведено розташування робочих груп та станцій різних підрозділів.

Таблиця 1.1 – Розташування робочих груп та станцій

Відділи	Будинки	Поверхи	Кількість робочих груп (кімнат)	Кількість робочих станцій
Project 1	A	3	12	8
Project 2	A	4	9	13
Project 3	A	5	11	12
SR1	B	1	9	8
SR2	B	1	15	38
FR	B	1	18	28
MR1	C	1	10	17
MR2	C	2	3	15
Hum. Res.	A	1	5	8
Accounting	A	2	4	13
Business	A	2	2	7
Info. Group	A	1	5	8

Використовуване обладнання: Juniper.

2 РОЗПОДІЛ IP-АДРЕС

Згідно з технічним завданням, у кожному з трьох будинків слід використовувати IP-адреси з таких діапазонів:

будинок А: 10.60.0.0/16;

будинок В: 172.36.64.0/18;

будинок С: 192.168.64.0/22.

Розрахунок необхідної кількості IP-адрес відбуваються з міркувань, викладених далі.

Кожен кінцевий пристрій повинен мати IP-адресу. До кінцевих пристроїв належать:

сервери;

робочі станції;

IP-телефони;

мережеві принтери.

Крім того, IP-адреси на різних інтерфейсах повинні мати роутери та міжмережеві екрани.

Комутатори, зв'язок між якими регламентується технологією VLAN, можуть не мати IP-адрес.

Для кожного виокремленого піддіапазону адрес закладається двадцятивідсотковий запас, а також ураховуються дві адреси, які не можуть бути виокремлені пристроями широкомовної та адресної мережі.

У табл. 2.1 показаний розрахунок кількості адрес для кожного сегмента мережі.

Таблиця 2.1 – Розрахунок кількості IP-адрес

Відділи	Комп'ю-тери	Телефони	Прин-тери	Кімнатні	Поверхові	Кількість кімнат	Усього	Запас	Розмір мережі
Hum. Res.	8	5	1	1	1	5	16	16	32
Acc.	13	4	1	1	1	4	20	12	32
Busi.	7	2	1	1	1	2	14	113	127
MR1	17	10	1	1	1	10	30	34	64
MR2	15	3	1	1	1	3	21	42	64
SR1	8	9	1	1	1	9	20	43	64
SR2	38	15	1	1	1	15	56	71	127
FR	28	18	1	1	1	18	49	78	127
Info. Group	8	5	1	1	1	5	16	239	256
Prj1	8	12	1	1	1	12	23	489	512
Prj2	13	9	1	1	1	9	25	103	128
Prj3	12	11	1	1	1	11	26	230	256

У табл. 2.2 показано розподіл IP-адрес у підрозділах підприємства. Під час розрахунків використовувався ресурс табл. 2.1.

Таблиця 2.2 – Розподіл IP-адрес у підрозділах підприємства

Підрозділи	VLAN	Підмережі	Діапазони IP-адрес
Accounting	220	10.60.2.0/27	10.60.2.0 – 10.60.2.31
Business	325	10.60.3.0/25	10.60.3.0 – 10.60.3.127
Info. Group	120	10.60.1.0/24	10.60.1.0 – 10.60.1.127
Human Res.	20	10.60.0.0/27	10.60.0.0 – 10.60.0.31
MR1	189	192.168.64.0/26	192.168.64.0 – 192.168.64.63
MR2	192	192.168.66.0/26	192.168.66.0 – 192.168.66.63
Project1	455	10.60.4.0/23	10.60.4.0 – 10.60.5.255
Project2	560	10.60.5.0/25	10.60.5.0 – 10.60.5.127
Project3	670	10.60.6.0/24	10.60.6.0 – 10.60.6.255
FR	564	172.36.66.0/25	172.36.66.0 – 172.36.66.127
SR1	1502	172.36.65.0/26	172.36.65.0 – 172.36.65.63
SR2	763	172.36.64.0/25	172.36.64.0 – 172.36.64.127

Також необхідно виокремити IP-адресу включно з зовнішніми адресами у діапазоні 199.46.50.0/24 ряду пристроїв. Ці адреси показані у табл. 2.3.

Таблиця 2.3 – IP-адреси пристроїв

Пристрої	Інтерфейси	IP-адреси
RA01	G1 0/0	10.60.0.1
	G2 0/0	10.60.1.1
	G3 0/0	10.60.2.1
	G4 0/0	10.60.3.1
	G5 0/0	10.60.4.1
	G6 0/0	10.60.5.1
	G7 0/0	10.60.6.1
FWA01	G1 3,4	10.60.7.3
	G2 1,2	10.60.7.2
FWA02	G1 1,2	10.60.7.1
	G2 3	199.46.50.1
Web	–	10.60.7.4
DNS Ext	–	10.60.7.5
DNS Int	–	10.60.7.6
Database	–	10.60.7.7
ADA01	–	10.60.7.8
RB01	G1 0/0	172.36.64.1
	G2 0/0	172.36.65.1
	G3 0/0	172.36.66.1
FWB01	G1 1,2	172.36.64.1
	G2 1,2	172.36.65.2
	G3 1,2	172.36.66.3
	G4 3	199.46.50.2
ADB01	–	172.36.67.1
RC01	G1 0/0	192.168.64.1
	G2 0/0	192.168.66.1
FWC01	G1 3	199.46.50.3
	G2 1,2	192.168.66.1
	G3 1,2	192.168.67.1
ADC01	–	192.168.67.2

3 ВИКОРИСТАННЯ VLAN

Для розмежування робочих груп, зниження об'єму службового трафіка у мережі та підвищення безпеки застосовується технологія VLAN.

VLAN (Virtual Local Area Network) – це топологічна або "віртуальна" локальна комп'ютерна мережа, яка становить групу хостів із загальним набором вимог, які взаємодіють так, як якщо б вони були підключені до широкомовного домена, незалежно від їх фізичного місця знаходження. VLAN має ті ж самі властивості, що й фізична локальна мережа, але дозволяє кінцевим членам групуватися разом, навіть якщо вони не знаходяться в одній фізичній мережі. Така реорганізація може бути зроблена на основі програмного забезпечення замість фізичного переміщення пристроїв. Технологія VLAN використовує нумерацію від 1 до 4 095, але важливо, що використовувати перший та останній номер не варто через те, що вони зарезервовані.

VLAN надає такі можливості:

- логічний розподіл комутатора на декілька мереж, які між собою не пов'язані;
- пристрій такого розподілу на мережі з двома або більше комутаторами без потреби проведення додаткових кабелів;
- дворівневе вкладення VLAN міток у кадр, а також трансляція позначень міток "у польоті";
- реалізація Promiscous/Community/Isolated портів (у цьому випадку використовується логічне вкладення декількох вторинних VLAN в одну первинну).

Переваги використовування VLAN:

- полегшується переміщення, додавання пристроїв та зміна їх з'єднань один з одним;

- досягається більший ступінь адміністративного контролю внаслідок наявності пристрою, який здійснює між мережами VLAN маршрутизацію на третьому рівні;
- зменшується потреба полоси пропускання відносно з ситуацією одного широкомовного домена;
- зменшується невиробниче використання CPU за рахунок скорочення пересилання широкомовних повідомлень;
- запобігання широкомовних штормів та запобігання втрат.

У табл. 2.2 було показано відповідність між відділами та VLAN.

4 РОЗРОБЛЕННЯ СХЕМИ МЕРЕЖІ

У якості основної фізичної структури мережі взято вимоги технічного завдання.

На рівні доступу всі комп'ютери підключені до 24-портових керованих L2 комутаторів. Комп'ютери підключені до керованого комутатора напряму. Розподіл між підрозділами підприємства здійснюється шляхом створення VLAN-ів.

Загально корпоративні служби мають два типи кімнат: зі стаціонарними робочими станціями та з ноутбуками, які підключаються до мережі через безпечне бездротове з'єднання. Для забезпечення безпеки кожна з точок доступу має пароль та використовує технологію WPA2.

Кімнатні керовані комутатори отримують назви за типом BBF2R12, де X – індекс будинку (A/B/C), Y – номер поверху, Z – номер кімнати на поверсі.

Рівень розподілу створюють поверхові комутатори – керовані 24-портові L2. Вони з'єднують послідовно до ядра. Даний вид підключення дозволяє зменшити витрати з монтажу СКС, однак декілька зменшують надійність такого з'єднання. Дана проблема усувається надмірним з'єднанням з метою резервування лінії зв'язку та портів пристроїв.

Імена поверхових комутаторів складаються у вигляді BBF2.

Внутрішня мережа підприємства відділена від зовнішньої мережі за допомогою між мережевого екрана. Для офісів B та C між мережевий екран є також роутером. У офісі A наявні два міжмережеві екрани, між якими розташована демілітаризована мережа. Для підвищення надійності зв'язку у DMZ дубльовані.

Імена роутерів мають вигляд RA12 (RXYY), де R – загальний префікс роутерів, X – індекс будинку (A/B/C), YY – порядковий номер пристрою.

Імена міжмережевих екранів мають вигляд FWA12 (FWXYY), де FW – загальний префікс міжмережевих екранів, X – індекс будинку (A/B/C), YY – порядковий номер пристрою.

Підключення до віддалених офісів SOHO здійснюється за допомогою мережі "Інтернет" з використанням систем контролю ключів та сертифікатів.

Загальну схему з'єднання трьох будинків подано на рис. 4.1.

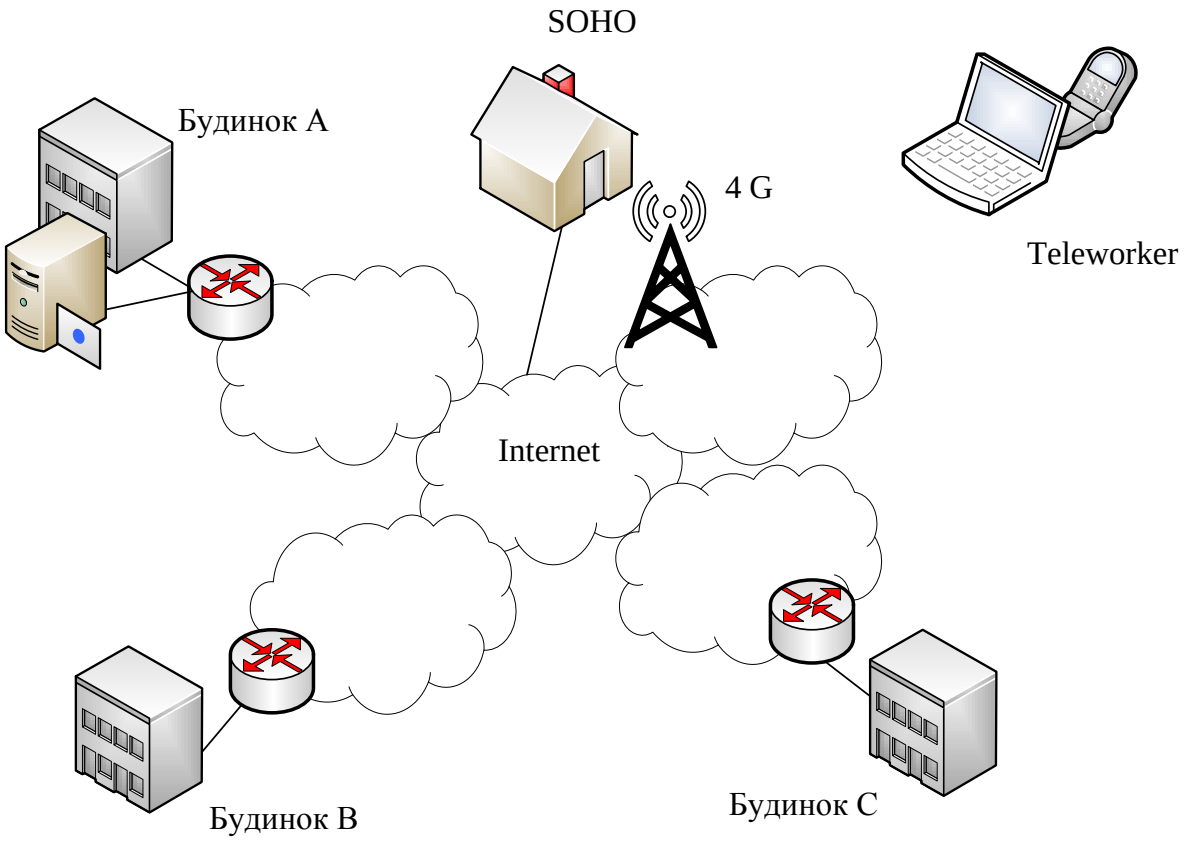

Рисунок 4.1 – Схема з'єднання трьох будинків

Фізичну схему мережі подано для кожного будинка окремо на рис. 4.2 – 4.4.

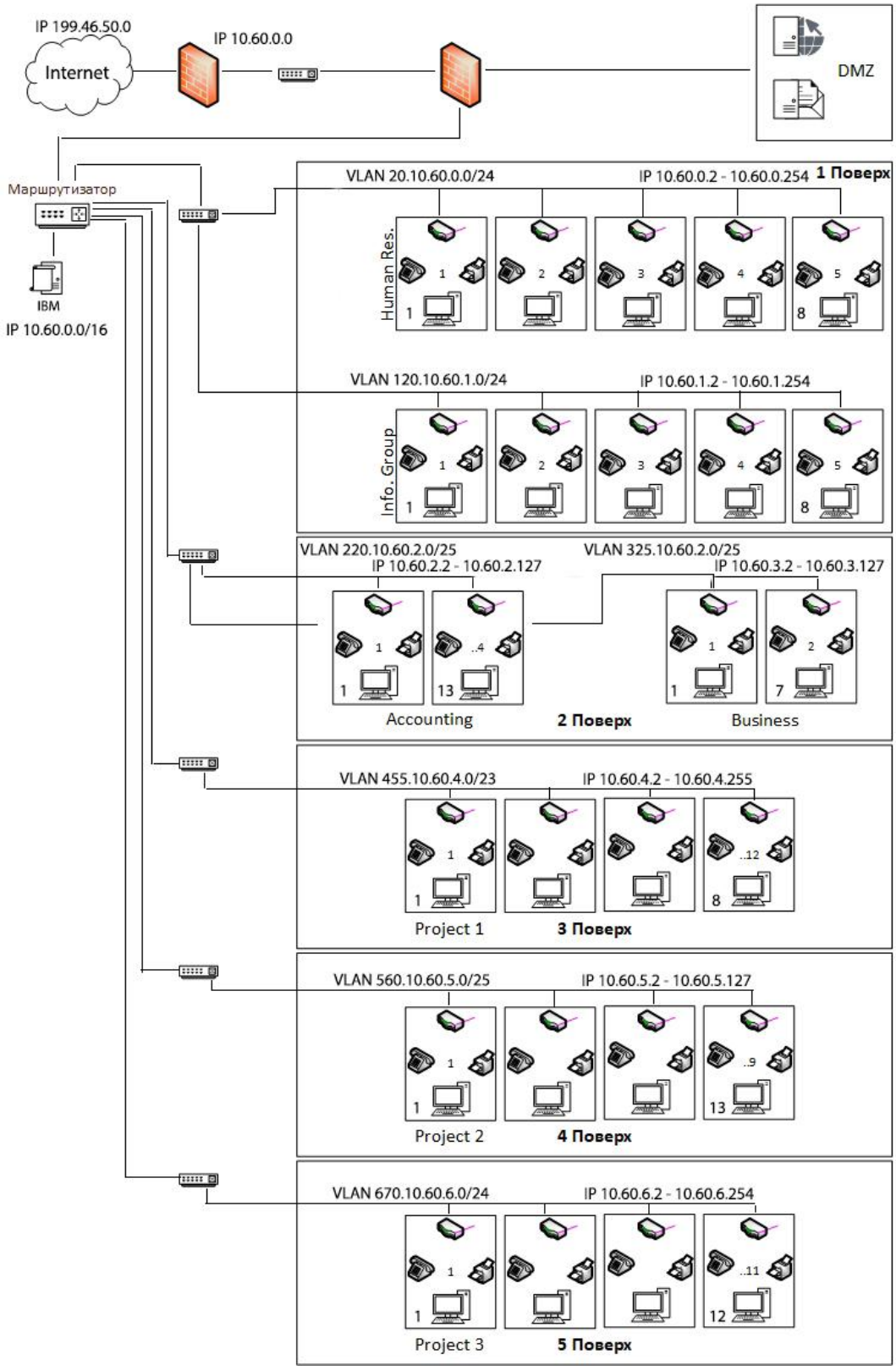

Рисунок 4.2 – Фізична схема мережі будинку А

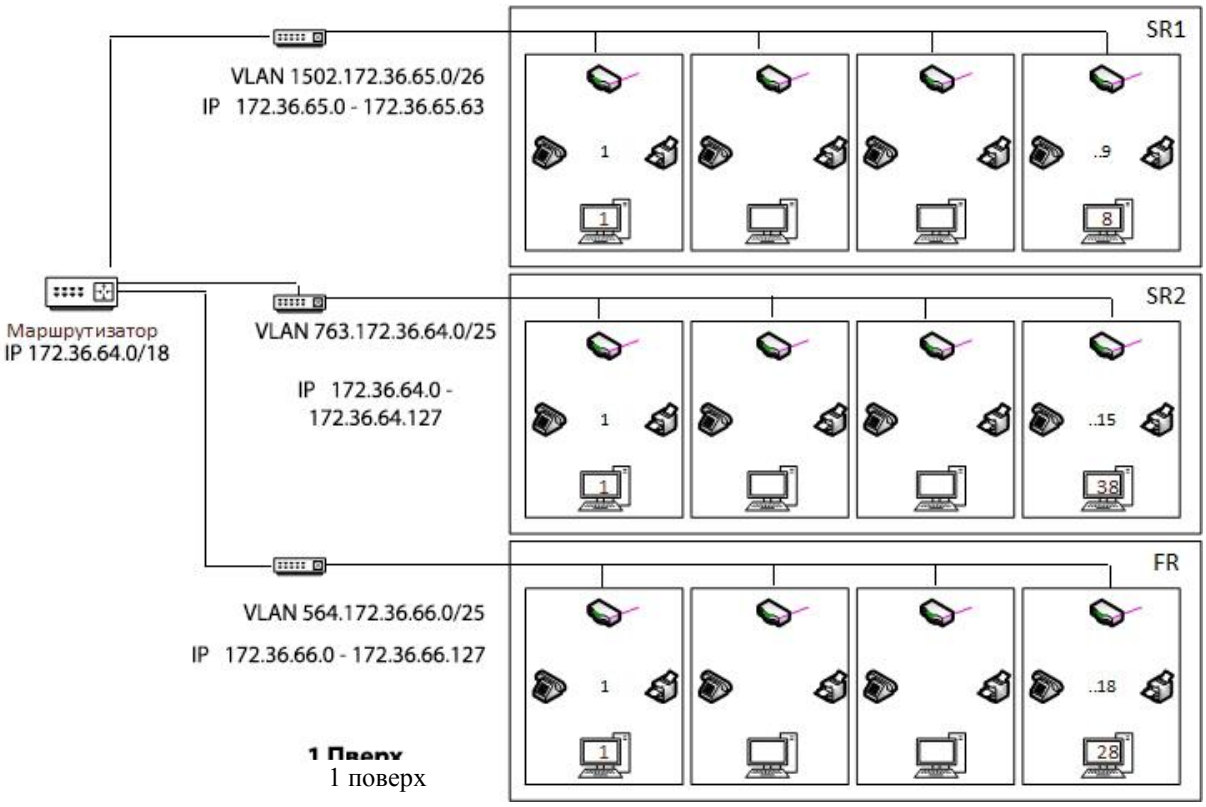

Рисунок 4.3 – Фізична схема мережі будинку B

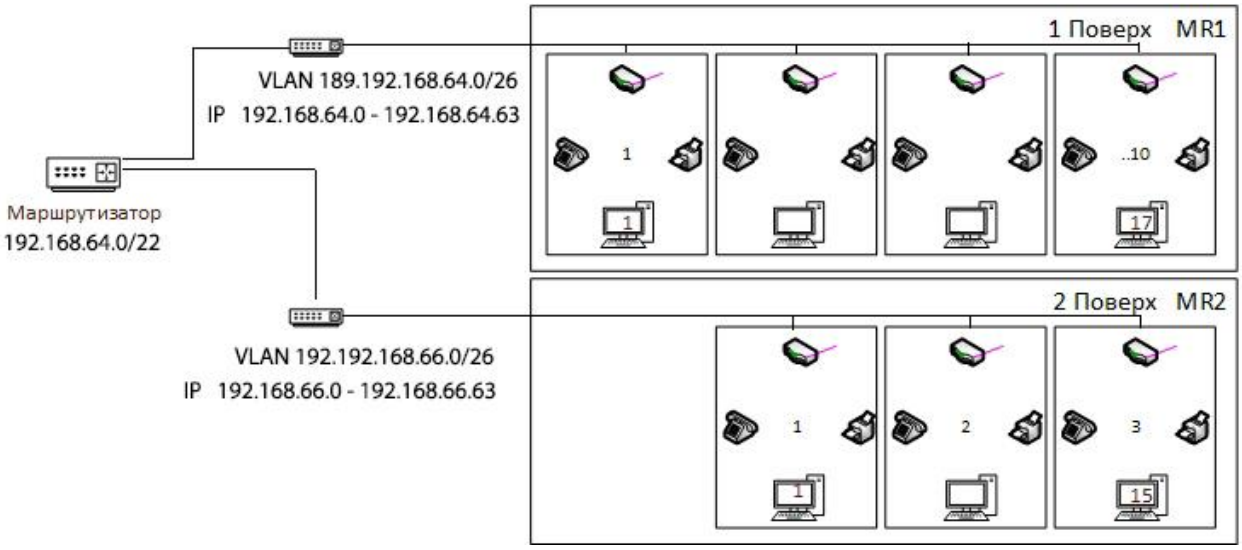

Рисунок 4.4 – Фізична схема мережі будинку C

Логічну схему мережі подано для кожного будинку окремо на рис. 4.5 – 4.7.

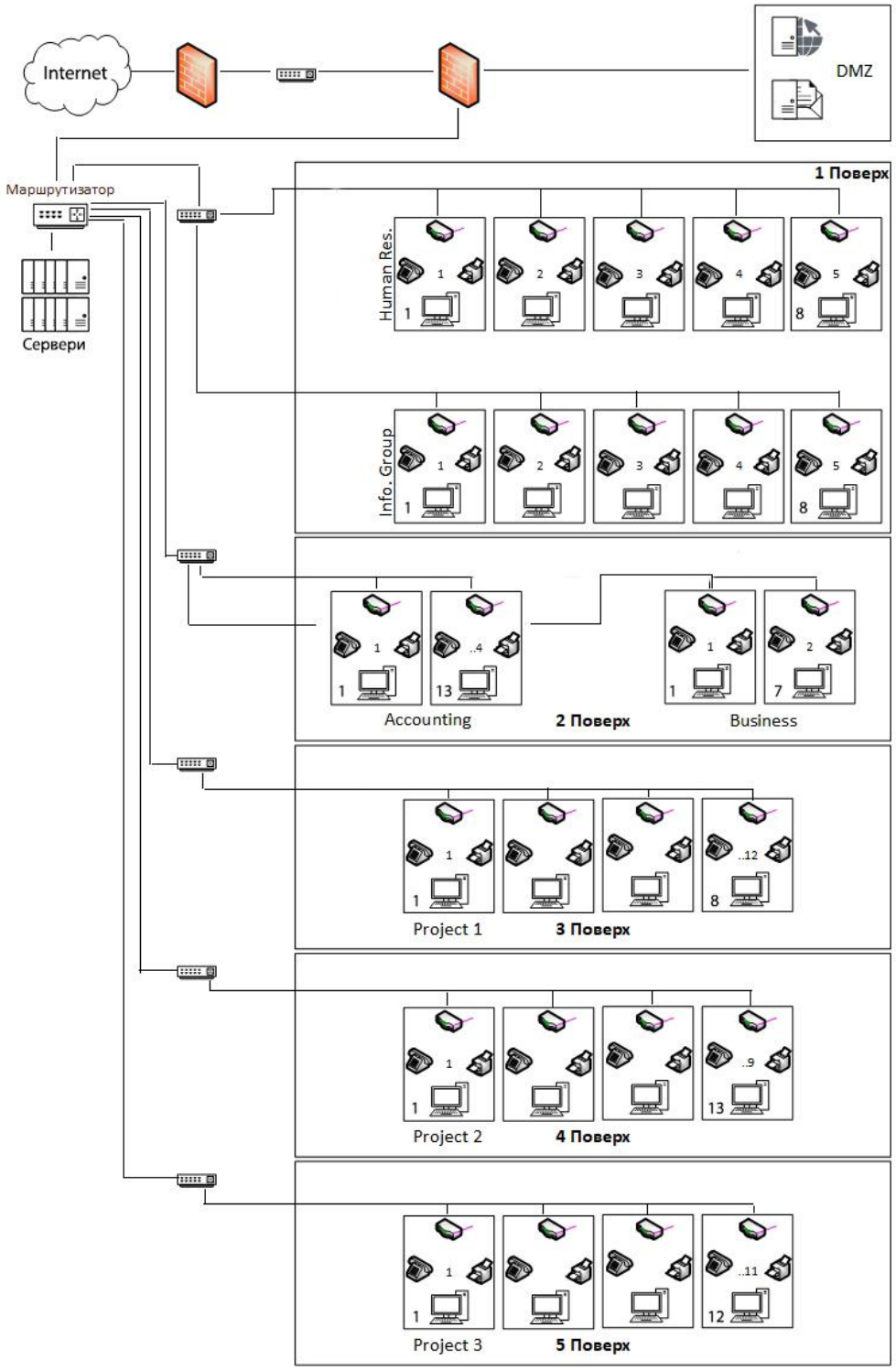

Рисунок 4.5 – Логічна схема мережі будинку А

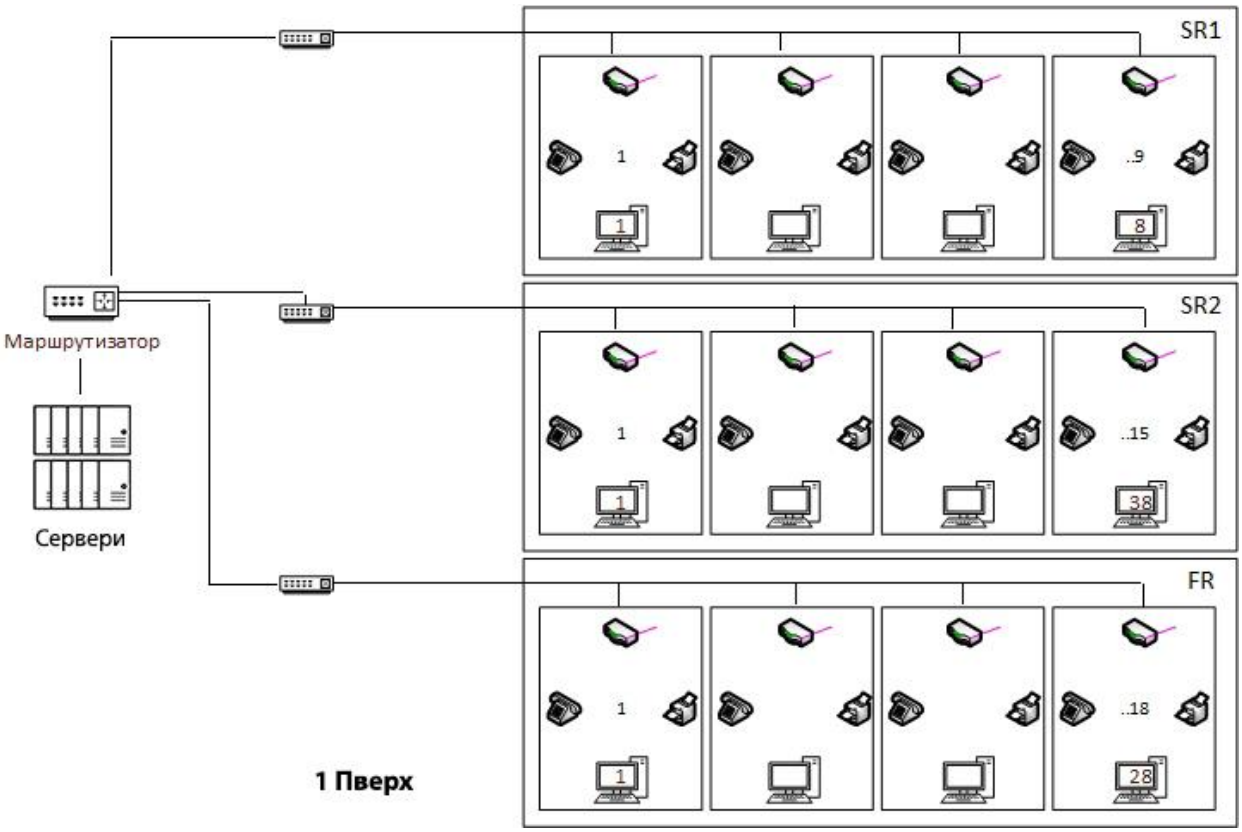

Рисунок 4.6 – Логічна схема мережі будинку B

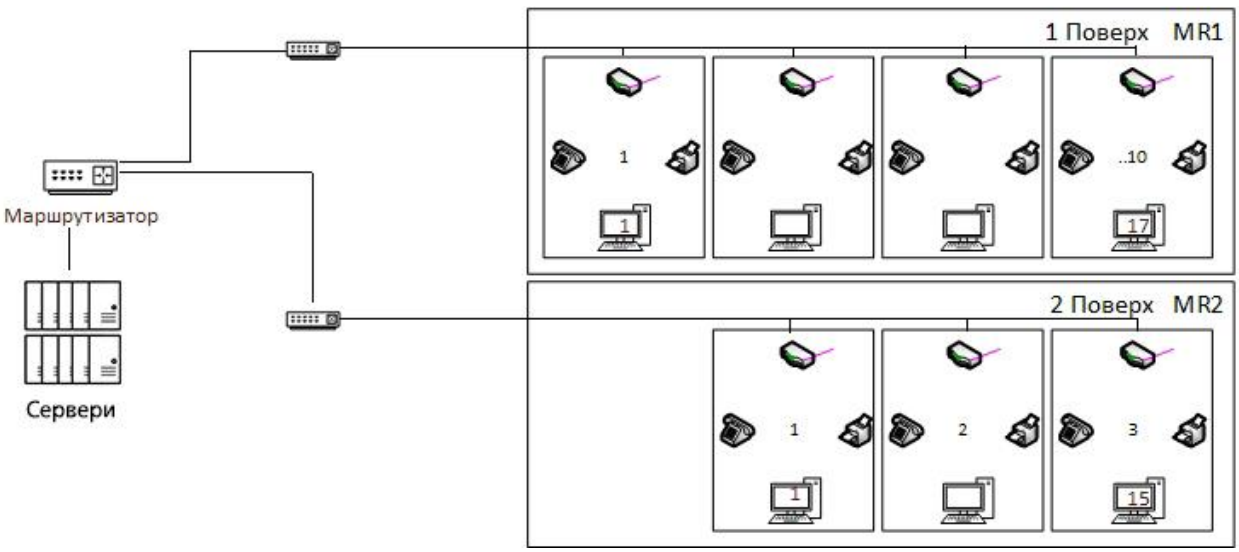

Рисунок 4.7 – Логічна схема мережі будинку C

5 ВИБІР ВИКОРИСТОВУВАНОГО ОБЛАДНАННЯ

5.1 Вибір комутаторів та точок доступу

Згідно з вимогами завдання, необхідно використовувати обладнання компанії Juniper.

Для реалізації рівня доступу був вибраний комутатор моделі EX2200-24P-4G. Цей комутатор становить Ethernet-пристрій с низьким енергоспоживанням, компактним дизайном та низьким шумом, дозволяє розташовувати його у близькості від робочих груп. Даний комутатор має 24 порти 10/100/1000Base-T Ethernet з підтримкою протоколів PoE, PoE+, VLAN, HTTP, HTTPs, Telnet, QoS.

Для реалізації рівня розподілу був обраний комутатор моделі EX3400-24P. Даний комутатор є масштабованим L3 пристроєм с фіксованою конфігурацією. Комутатор має 24 порти 100Base-FX/1000Base-X, підтримує технологію Fast Ethernet, VLAN, QoS, CLI, DHCP, Telnet та має Web Interface.

У якості точки доступу була обрана модель WLA322-WW. Дана точка доступу має підтримку бездротових протоколів 802.11a, 802.11b, 802.11g, 802.11n, підтримує 64 SSID, локальну комутацію, має такі інтерфейси, як 10/100/1000 PoE (RJ-45), енергоспоживання даної точки доступу дорівнює 8Вт, а також протоколи безпеки, а саме 802.1X, WPA, WPA2, PMK, AES.

5.2 Вибір маршрутизаторів та міжмережевих екранів

Для маршрутизації між VLAN-ми був обраний маршрутизатор моделі J2320-JH. Даний маршрутизатор має 4 порти 10/100/1000Base-T та підтримує такі протоколи безпеки, як IPsec, SSH, LDSP, RADIUS, SecureID.

У якості міжмережевого екрана була обрана модель SRX1400Base-XGE-DC. Даний міжмережевий екран становить високопродуктивне рішення, яке містить безпеку, маршрутизацію, комутацію і підключення до глобальної мережі в одному пристрої форм-фактора 3RU. Це надійна, гнучка, модульна платформа забезпечує захист корпоративних мереж середніх і великих розмірів, а також центрів оброблення даних. Серія представлена моделлю SRX1400. Ця модель випускається у варіантах GE (на борту вбудовані гігабітні 6 портів 1000BASE-T і 6 портів SFP) і XGE (на борту вбудовані гігабітні 6 портів 1000BASE-T, 3 порти SFP і 3 порти SFP +). У кожній моделі SRX1400 є модуль управління (routing engine) і блок живлення AC або DC, а також модуль охолодження. Платформа SRX1400 має продуктивність брандмауера до 10 Гбіт / с, IPSec VPN зі швидкістю 4 Гбіт/с і IPS зі швидкістю 3 Гбіт/с.

5.3 Розміщення обладнання у стійках

Розміщення обладнання у стійках для будинків А, В та С показано на рис. 5.1. Усього для розміщення обладнання необхідно 6 стійок по 24U – 750мм кожна.

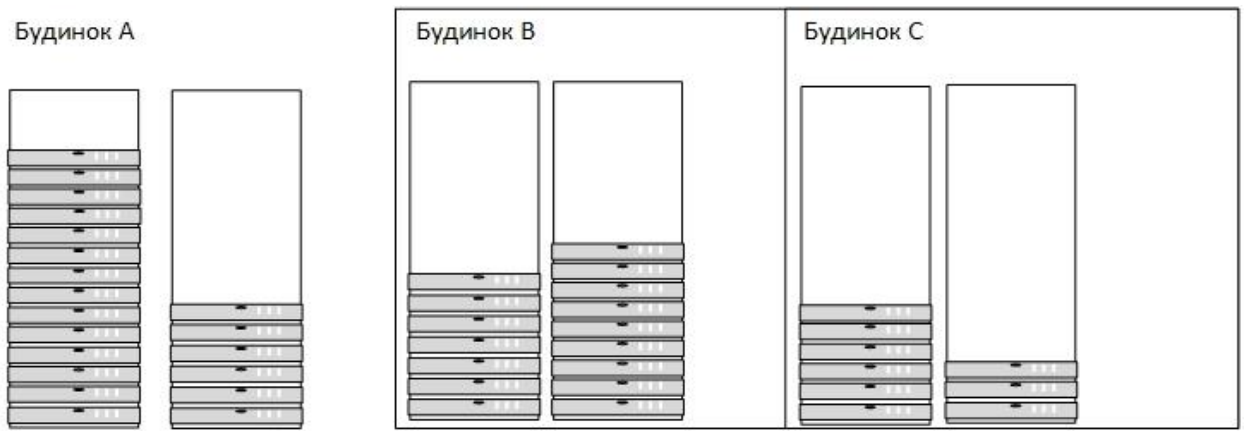

Рисунок 5.1 – Розміщення обладнання у стійках для будинків А, В та С

6 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖІ

6.1 IBM Security Guardian Key Lifecycle Manager

IBM Security Guardian Key Lifecycle Manager – це програмне доповнення для роботи з ключами шифрування. Система централізує, спрощує та автоматизує процес шифрування, що надає можливість звести ризики до мінімуму. Продукт використовує надійний репозиторій для зберігання ключів, а також дозволяє управляти обслуговуванням та всім життєвим циклом кожного ключа шифрування.

IBM Security Guardian Key надає:

- гнучкість та легкість використовування на основі кластерів, підтримує мультимастерні кластери. Це дає можливість синхронізації і доставки ключів безпеки в реальному часі, підвищуючи гнучкість і зручність використання. Можливість одночасної синхронізації більше 20 головних вузлів забезпечує підвищену надмірність і готовність локальної системи, гарантуючи доступність ключів у будь-який момент часу;
- ефективне та спрощене управління ключами. Дане рішення автоматизує операції створення, імпорту, поширення резервної копії ключів у рамках управління їх життєвим циклом. Доступно централізоване створення і поширення ключів, а також об'єднання пристроїв в окремі домени для більш зручного управління ключами. Крім цього, підтримується управління доступом на основі ролей для адміністративних облікових записів;
- сертифікований обмін даними. Ваша система обміну інформацією пройде сертифікацію Storage Networking Industry Association Secure Storage Industry Forum (SNIA-SSIF) на відповідність стандарту OASIS KMIP версії 1.2;
- скорочення витрат на управління ключами. Key Lifecycle Manager допомагає оптимізувати вже зроблені інвестиції в безпеку, високу готовність, аварійне відновлення і сервери, а також спростити складні процедури поширення

ключів. Консолідуйте управління ключами на рівні доменів і забезпечте підтримку стандартів для управління сторонніми продуктами, включаючи сховища даних, хмарні пристрої зберігання, мережеві пристрої, що запам'ятовують й інтелектуальні лічильники. Забезпечте підвищену готовність і підтримку аварійного відновлення.

IBM Security Guardium Key Lifecycle Manager централізує, спрощує та автоматизує процес управління ключами шифрування, зводячи до мінімуму ризик і скорочуючи витрати на управління ключами. Дане рішення пропонує безпечне і надійне зберігання ключів, обслуговування та управління життєвим циклом ключів для рішень IBM та інших фірм на основі протоколу OASIS для спільного управління ключами (KMIP). Централізоване управління ключами шифрування в IBM Security Guardium Key Lifecycle Manager допомагає клієнтам в дотриманні вимог законодавства, наприклад "Стандарту захисту інформації" в індустрії платіжних карт (PCI DSS), закону "Сарбейнса – Окслі" і "Закону про мобільність і підзвітності медичного страхування" (HIPAA).

6.2 Key Manager Plus

ManageEngine Key Manager Plus – це вебрішення для управління ключами, яке дозволяє консолідувати, контролювати, відстежувати ключі SSH (Secure Shell) і сертифікати SSL (Secure Sockets Layer) протягом усього їх життєвого циклу, а також керувати ними і проводити їх аудит. З його допомогою адміністратори можуть організувати спостереження за середовищами SSH і SSL, а також взяти під контроль ключі для попередження виникнення проломів і проблем з відповідністю вимогам.

Захист переміщуваних даних завжди було одним із найскладніших завдань для адміністраторів безпеки. Незважаючи на те, що ключі SSH допомагають організаціям забезпечити безпеку у разі віддаленого адміністрування та передання даних, управління цифровими ключами, як і раніше пов'язане з низкою характерних складнощів.

Зазвичай під час організації моніторингу середовища та управління ним ключі SSH залишаються без уваги, що робить організації уразливими для кібератак. Відсутність автоматизованої системи, складання списку всіх використовуваних ключів вручну, пошук і обмеження дозволів на доступ, а також забезпечення періодичної зміни ключів вимагають титанічних зусиль.

Така ж ситуація спостерігається і з управлінням середовищем Secure Socket Layer (SSL), коли в організації використовується велика кількість сертифікатів SSL, виданих різними постачальниками і на різні терміни. З іншого боку, термін дії сертифікатів SSL, які залишилися без уваги, може закінчитися, або замість них можуть використовуватися незаконні або недійсні сертифікати. В обох сценаріях можуть виникати збої у роботі служб і з'являтися повідомлення про помилки, що неминуче призведе до підриву довіри клієнтів до безпеки даних, а в крайньому випадку навіть до виникнення проломів у системі безпеки.

ManageEngine Key Manager Plus виконує управління сертифікатами таким чином:

- виявлення всіх сертифікатів SSL, розгорнутих у мережі;
- об'єднання всіх виявлених сертифікатів у захищеному центральному репозиторії;
- виявлення, відстеження сертифікатів, зіставлених з обліковими записами користувачів у Active Directory, а також управління ними;
- виявлення, відстеження сертифікатів у сховищі Microsoft і управління ними;
- комплексне управління життєвим циклом сертифікатів за допомогою Let's Encrypt;
- розгортання нових отриманих сертифікатів на відповідних серверах домена.

ManageEngine Key Manager Plus надає такі можливості:

- заплановане резервне копіювання бази даних. Підготовка до запланованого резервного копіювання всієї бази даних на випадок аварійного відновлення;
- інтеграція з Active Directory. Імпорт користувачів або груп користувачів з Windows Active Directory і використання механізму перевірки достовірності;
- контроль і обмеження доступу. Зв'язування певних ресурсів з користувачами й організація управління доступом до них;
- забезпечення відповідності вимогам. Ефективне управління ключами SSH, забезпечення відповідності вимогам стандартів, а саме SOX, FISMA, PCI і HIPAA.

7 РОЗРАХУНОК ВАРТОСТІ СТВОРЕННЯ МЕРЕЖІ

Підбір обладнання відбувався залежно від критерія мінімальної вартості за умови достатнього рівня продуктивності без урахування вартості "ManageEngine Key Manager Plus" та "IBM Security Guardian Key Lifecycle Manager". Перелік обладнання та підрахунок загальної вартості показаний у табл. 7.1.

Таблиця 7.1 – Перелік обладнання

Устаткування	Ціна, грн	Кількість, шт.	Вартість, грн
Будинок А			
Бездротова точка доступу WLA322-WW	11 662	5	58 310
Комутатор EX2200-24P-4G	45 629	48	2 190 192
Комутатор EX3400-24P	63 140	6	708 840
Маршрутизатор J2320-JH	67 200	1	67 200
Міжмережевий екран SRX1000	350 000	2	700 000
Сервер HP DL360p Gen8	26 128	21	548 688
Будинок В			
Комутатор EX2200-24P-4G	45 629	42	1 916 418
Комутатор EX3400-24P	63 140	3	189 420
Маршрутизатор J2320-JH	67 200	1	67 200
Сервер HP DL360p Gen8	26 128	16	418 048
Будинок С			
Комутатор EX2200-24P-4G	45 629	13	593 177
Комутатор EX3400-24P	63 140	2	126 280
Маршрутизатор J2320-JH	67 200	1	67 200
Сервер HP DL20 Gen10	26 128	9	235 152
Стійка 24U	2 110	6	12 660
Разом			7 898 725

Проведений розрахунок вартості необхідного обладнання складає 7 898 725 грн та дозволяє розгорнути запропоновану структуру корпоративної мережі, забезпечити необхідний рівень безпеки інформації за рахунок використання IBM Security Guardian Key Lifecycle Manager.

ВИСНОВОК

У результаті виконання курсового проєкту була розроблена корпоративна мережа для корпорації CorpPDS. У ході виконання роботи були розроблені фізична та логічна схема мережі для будинків A, B та C; розподілені IP-адреси для підмереж, виходячи з даних діапазонів IP-адрес для кожного будинку; розглянуто способи забезпечення безпеки для мережі за допомогою систем контролю ключів та сертифікатів.

У ході розгляду варіантів захисту мережі було виокремлено дві системи захисту та управління ключами та сертифікатами. Дані системи надають безпечне та надійне зберігання ключів, допомагають забезпечити клієнта вимогам законодавства. Крім цього системи управління ключами надають змогу знизити затрати завдяки автоматизації таких операцій призначення та зміни ключів; була розрахована вартість створення усієї корпоративної мережі, виходячи з даних про поточні ціни на обладнання.

Розроблений проєкт відповідає вимогам технічного завдання та має найменшу фактичну вартість.

СПИСОК ДЖЕРЕЛ ІНФОРМАЦІЇ

1. Євсеєв С.П., Білова М.О., Жученко О.С., Іванченко С.І., Шматко О.В. Технологія Ethernet: лабораторний практикум з курсу "Комп'ютерні мережі" студентів спеціальностей 121, 122, 126. Львів : "Новий Світ- 2000", 2020. 196с.

2. Євсеєв С.П., Король О.Г., Гаврилова А.А. Курсовий проєкт: Введення в мережі: методичні рекомендації для студентів спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня. Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. 45с.

3. Євсеєв С.П., Король О.Г., Жукарев В.Ю. Технології комп'ютерних мереж: мультимед. інтеракт. електор. вид. комб. викор. Х. : ХНЕУ ім. С. Кузнеця, 2015. 207Мб.

4. Євсеєв С.П., Остапов С.Е., Король О.Г. Кібербезпека: сучасні технології захисту: навч. посіб. для студ. вищ. навч. закл. Львів : "Новий Світ-2000", 2019. 678с.

5. Комутатор EX2200. URL: https://stacl-system.com.ua/ kommutator-juniper-ex2200-24p-4g (дата звернення 01.12.2020).

6. Комутатор EX3400. URL: https://stacl-system.com.ua/ kommutator-juniper-ex3400-24p (дата звернення 01.12.2020).

7. Кулаков В.Г., Леохин Ю.Л. Моделирование компьютерных сетей в симуляторе Cisco Packet Tracer 6: уч. пособ. М. : Изд-во МТИ. 2016. 175с.

8. Маршрутизатор J2330. URL: https://stacl-system.com.ua/marshrutezator-juniper-f2320-jh (дата звернення: 01.12.2020).

9. Мережі на основі намірів. URL: https://www.cisco.com /c/ru_ru/solutions/intent-based-networking.html (дата звернення 02.12.2020).

10. Мережеві рішення CISCO. URL: https://www.cisco-parts.ru/catalog-cisco/setevye-resheniya-cisco (дата звернення 02.12.2020).

11. Міжмережевий екран SRX1000. URL: https://stacl-system.com.ua/ mezhsetevoj-jekran-juniper-srx1400base-xge-dc (дата звернення 01.12.2020).

12. Одома Уэнделла. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822. Изд. 3-е. Изд. "Вильямс", серия Cisco Press. 2013.

13. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Изд. 5-е. СПб. : Питер, 2016. 992с.

14. Основи мережевих технологій. URL: https://www.cisco.com/ c/ru_ru/solutions/small-business/resource-center/networking/ networking-basics.html (дата звернення 02.12.2020).

15. Сервер DL20 Gen10. URL: https://elmir.ua/servers/server_hp_proliant _dl20_gen10_p06477b21.html?gclid=Cj0KCQiAtqLBRC0ARIsAF4K3WGMLNrG VCMPPjg0oUW_source=gmerchant&utm_term=server_hp_proliant_dl20_gen10_p 06477-b21 (дата звернення 02.12.2020).

16. Система управління ключами IBN Security GKLM. URL: https://www.ibm.com/ru-ru/products/ibm-security-key-lifecycle-manager/details (дата звернення 02.12.2020).

17. Система управління ключами Key Manager Plus. URL: https://www.manageengine.com/ru/key-manager (дата звернення 02.12.2020).

18. Стійка для серверів. URL: https://e-server.com.ua/servernye-stojki?pa_vysota.u=24&gclid=Cj0KCQiAtqL.BRC0ARIsAF4K3WEG6xTR7Z9gwv 2T8aoT6bKyBq_zo_lXum_-OpD0TgF76KFn9rhLTMaAnAGEALw_wcB (дата звернення 01.12.2020).

19. Таненбаум Э., Уэзеролл Д. Компьютерные сети. Изд.5-е. СПб.: Питер, 2016. 960с.

20. Точка доступу WLA. URL: https://stacl-system.com.ua/ tochka-dostupa-juniper-wla322-ww (дата звернення 01.12.2020).

Зміст

Вступ 3
Розділ 1 Завдання на виконання курсового проєкту 5
Рекомендації 9
Приблизна послідовність виконання курсового проєкту 10
Змістовні рекомендації щодо створення курсового проєкту 11
Розділ 2 Розрахунок вихідних даних курсового проєкту 13
Рекомендована література 19
Додатки 20

НАВЧАЛЬНЕ ВИДАННЯ

КУРСОВИЙ ПРОЄКТ: ВВЕДЕННЯ В МЕРЕЖІ

Методичні рекомендації
для студентів спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня

Самостійне електронне текстове мережеве видання

Укладачі: **Євсеєв** Сергій Петрович
Король Ольга Григорівна
Гаврилова Алла Андріївна

Відповідальний за видання *С. П. Євсеєв*

Редактор *В. О. Дмитрієва*

Коректор *В. Ю. Труш*

План 2021 р. Поз. № 232 ЕВ. Обсяг 52 с.

Видавець і виготовлювач – ХНЕУ ім. С. Кузнеця, 61166, м. Харків, просп. Науки, 9-А

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру
ДК № 4853 від 20.02.2015 р.