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

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## кваліфікаційної роботи ступеня бакалавра

**здобувача** Баскін Ростислав Владиславович
(ПІБ)

**академічної групи** 123-21-1
(шифр)

**спеціальності** 123 Комп'ютерна інженерія
(код і назва спеціальності)

**за освітньо-професійною програмою** Комп'ютерна інженерія
(офіційна назва)

**на тему** "Комп'ютерна система технологічної компанії з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"
(назва за наказом ректора)

| Керівники | Прізвище, ініціали | Оцінка за шкалою | | Підпис |
|---|---|---|---|---|
| | | рейтинговою | інституційною | |
| кваліфікаційної роботи | доц. Шедловський І.А | | | |
| спеціальної частини | доц. Шедловський І.А | | | |
| розділів: | | | | |
| розробка корпоративної мережі | ас. Панферова Я.В. | | | |
| **Рецензент** | | | | |
| **Нормоконтролер** | проф. Цвіркун Л.І. | | | |

**Дніпро**
**2025**

**ЗАТВЕРДЖЕНО:**
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

"____" _____ 2025 року

# ЗАВДАННЯ
## на кваліфікаційну роботу
## ступеня бакалавр

**здобувача** Баскін Р.В. **академічної групи** 123-21-1
(прізвище та ініціали) (шифр)

**спеціальності** 123 Комп'ютерна інженерія

**за освітньо-професійною програмою** Комп'ютерна інженерія
(офіційна назва)

**на тему** "Комп'ютерна система технологічної компанії з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 05.05.2025 № 336-с

| Розділ | Зміст | Термін виконання |
|---|---|---|
| Стан питання та постановка завдання | На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання | 05.05.2025 |
| Розробка апаратної частини | На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи | 12.05.2025 |
| Розробка корпоративної мережі | Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі | 26.05.2025 |
| Розробка компонента системи | Виконується детальна розробка компонента системи | 02.06.2025 |

**Завдання видано** _____ доц. Шедловський І.А
(підпис керівника) (прізвище, ініціали)

**Дата видачі** 25.02.2025

**Дата подання до екзаменаційної комісії** 16.06.2025

**Прийнято до виконання** _____ Баскін Р.В..

# РЕФЕРАТ

Пояснювальна записка: 107 с., 36 рис., 10 табл., 2 дод., 12 джерел.

КОМПАНІЯ, БЕЗПЕКА, СИСТЕМА, ЛОКАЛЬНА МЕРЕЖА, КОРПОРАТИВНА МЕРЕЖА, МЕРЕЖЕВІ ЗАСОБИ

Об’єкт розробки – комп'ютерна система технологічної компанії з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета роботи – створення комп'ютерної система для технологічної компанії Playtech.

Здійснено розробку комп’ютерної системи з можливістю гнучкої зміни виду та набору виконуваних функцій шляхом перепрограмування. Система орієнтована на застосування в комп'ютерній системі для технологічної компанії.

Ця комп'ютерна система дозволить оновлювати технології та програмне забезпечення і забезпечить автоматичний контроль планування і виконання робіт, облік та управління обслуговуванням мережевого обладнання, підвищить надійність зберігання інформації, забезпечить збір різноманітної статистичної інформації її класифікацію та здійснення підготовки рекомендацій.

Розроблена комп'ютерна система для технологічної компанії виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Робота комп’ютерної системи перевірена за допомогою моделі схеми корпоративної мережі у програмному застосунку Cisco Packet Tracer.

Результати перевірки працездатності комп’ютерної системи представлені у вигляді таблиць та графіків описані і наводяться у пояснювальній записці та додатках.

# ЗМІСТ

# ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КС – комп’ютерна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

Ethernet – технологія передачі даних по мережі;

Wi–Fi – технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11;

# ВСТУП

Інформаційні технології є невід'ємною частиною сучасного суспільства, що є рушійною силою прогресу та інновацій у різних секторах. Вплив на зв'язок, управління даними, кібербезпеку, розробку програмного забезпечення та хмарні обчислення є глибоким. У міру того, як IT продовжує розвиватися, він формуватиме майбутнє, пропонуючи нові можливості та рішення для вирішення проблем цифрового світу. Прийняття IT має важливе значення для окремих осіб, компаній та урядів для процвітання у 21 столітті [6].

У міру того, як світова економіка оговтується від однієї з найжахливіших економічних криз за минулі роки, інформаційно-комунікаційні технології (ІКТ) неодмінно візьмуть на себе невблаганно безпомилкову роль ключового фактору поширення інформації, що призведе до зростання, враховуючи те, що нові медіа-технології повинні бути доступними, доступними і дуже розвиненими, коли така велика кількість нових повідомлень передається швидко і адекватно.

За даними Datamation International, нові технології ввели період, який дав країнам, що розвиваються, потенційні канали зв'язку та інформації, які можуть мати імперативний вплив на соціальний та економічний розвиток. Інтенсивна потужність ІКТ має вирішальне значення не тільки для розвинених країн для управління і поліпшення використання технологій для обміну даними і аналізу в таких важливих сферах, як навколишнє середовище, добробут, умови праці, але і в країнах, що розвиваються, в розширенні кваліфікації, сприянні структурним перетворенням і розпорошенні технологій в межах своїх сфер і в порівнянні з більш розвиненими економіками.

У разі, якщо технологія бере на себе головну роль у гарантуванні економічної стійкості, вона може і повинна взяти на себе таку ж важливу роль у сприянні гармонії між розвитком і навколишнім середовищем, а також як ключовий

компонент формування громадської думки, необхідної для омолодження навколишнього середовища і створення свідомості. Сталий розвиток у кожній його частині має бути потребою як для політиків, організацій, так і для звичайного суспільства для створення ще більш простого, всеосяжного та стійкого до криз світу. Тепер технології повинні адаптуватися до нинішніх обставин.

Прогрес у цифрових технологіях ще більше підштовхнув до впровадження відповідних заходів для зміни громад та економік, які покращать взаєморозуміння, підтримають грошові вигоди та надає людям на низовому рівні можливість взяти на себе важливу роль у внесенні змін до своїх зборів та груп. Технології є переконливими і нелінійними за своєю природою, надаючи клієнту різні шляхи, за допомогою яких можна ідеально використовувати ці інновації.

Комп1ютерні системи, побудовані на базі інформаційних технологій можуть модернізувати можливості для різних поліпшень в будь-якій слаборозвиненій країні, наприклад, в агробізнесі, освіті, економічних питаннях, соціальній базі та інших питаннях, які можуть полегшити бідне становище людини.

Комп1ютерні системи можуть бути дуже активною використані у сфері комунікації. У країнах, що розвиваються, було відзначено, що Інтернет вважається потужним інструментом для прогресу, який дозволить націям стрибати вперед у грошовому та соціальному плані [7].

.

# 1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

## 1.1 Характеристика підприємства та умов застосування комп'ютерної системи в IT-компаніях

### 1.1.1 Загальні відомості про IT-ринок

Інформаційні технології (IT) стали життєво важливим компонентом сучасного суспільства, трансформуючи спосіб нашого життя, роботи та взаємодії. Від базової комунікації до складного управління даними, IT відіграє вирішальну роль у різних аспектах нашого повсякденного життя.

Інформаційні технології охоплюють використання комп'ютерів, програмного забезпечення, мереж та інших електронних пристроїв для зберігання, обробки та передачі інформації.


Рисунок 1.1 - Інформаційні технології

Це все включає в себе широкий спектр технологій і застосувань, в тому числі:

- апаратне забезпечення: фізичні пристрої, як-от комп'ютери, сервери та мережеве обладнання;

- програмне забезпечення: програми та застосунки, які виконують певні завдання на обладнанні;

- мережі: системи та протоколи, які з'єднують апаратне та програмне забезпечення, забезпечуючи зв'язок та обмін даними;

- управління даними: методи та інструменти для зберігання, отримання та аналізу даних.

Ключові напрямки IT:

1. Зв'язок. IT зробила революцію в комунікації за допомогою електронної пошти, обміну миттєвими повідомленнями, відеоконференцій та платформ соціальних мереж. Ці технології полегшують взаємодію та співпрацю в режимі реального часу, руйнуючи географічні бар'єри.

2. Управління даними. Здатність збирати, зберігати та аналізувати величезні обсяги даних є одним із найважливіших внесків IT. Інструменти та системи управління даними допомагають організаціям приймати обґрунтовані рішення, оптимізувати операції та покращувати взаємодію з клієнтами.

3. Кібербезпека. У зв'язку зі зростаючою залежністю від цифрових технологій захист конфіденційної інформації від кіберзагроз став надзвичайно важливим. Кібербезпека передбачає впровадження заходів щодо захисту даних, мереж і систем від несанкціонованого доступу, порушень і атак.

4. Розробка програмного забезпечення. Розробка програмних додатків, адаптованих до конкретних потреб, стимулює інновації та ефективність. Від мобільних додатків до корпоративного програмного забезпечення – професіонали IT розробляють, кодують і підтримують програми, які підвищують продуктивність і взаємодію з користувачем.

5. Хмарні обчислення. Хмарні обчислення дозволяють організаціям зберігати та отримувати доступ до даних і додатків через Інтернет, пропонуючи масштабованість, гнучкість і економію коштів. Він підтримує віддалену роботу, аварійне відновлення та розподіл ресурсів на вимогу.

6. Вплив IT на різні сектори. Бізнес IT змінив бізнес-середовище, автоматизувавши процеси, уможлививши електронну комерцію та сприяючи

глобальній торгівлі. Компанії використовують ІТ для покращення обслуговування клієнтів, оптимізації ланцюжків поставок та отримання конкурентної переваги.

7. Охорони здоров'я. У сфері охорони здоров'я ІТ відіграє вирішальну роль у веденні пацієнтів, медичних дослідженнях та наданні лікування. Електронні медичні записи (ЕМК), телемедицина та медичні інформаційні системи підвищують якість медичної допомоги та спрощують адміністративні завдання.

8. Освіта. Навчальні заклади використовують ІТ для надання платформ онлайн-навчання, цифрових ресурсів та інтерактивних інструментів. ІТ підтримує дистанційну освіту, персоналізоване навчання та доступ до великої кількості інформації, що робить освіту більш доступною та захоплюючою.

9. Уряд. Уряди використовують ІТ для покращення державних послуг, підвищення прозорості та взаємодії з громадянами. Ініціативи електронного урядування, онлайн-портали та аналітика даних допомагають оптимізувати процеси, зменшити бюрократію та сприяти ефективному врядуванню.

10. Фінанси. Фінансова індустрія значною мірою покладається на ІТ для безпечних транзакцій, управління ризиками та аналізу даних. Фінансові установи використовують ІТ для надання онлайн-банкінгу, мобільних платежів та інвестиційних послуг, забезпечуючи зручність та безпеку для клієнтів.

Майбутні тенденції в ІТ:

1. Штучний інтелект (AI) та машинне навчання. Штучний інтелект і машинне навчання мають революціонізувати різні галузі, забезпечуючи передовий аналіз даних, автоматизацію та персоналізовані послуги. Ці технології можуть покращити процес прийняття рішень, покращити якість обслуговування клієнтів та стимулювати інновації.

2. Інтернет речей (IoT). IoT підключає повсякденні пристрої до Інтернету, дозволяючи їм збирати та обмінюватися даними. Цей зв'язок може призвести до

розумніших домівок, ефективних промислових операцій та покращення моніторингу охорони здоров'я.

3. Технологія 5G. Розгортання мереж 5G обіцяє вищу швидкість Інтернету, меншу затримку та покращене підключення. Ця технологія сприятиме зростанню IoT, забезпечить зв'язок у режимі реального часу та сприятиме прогресу в різних галузях.

4. Блокчейн. Технологія блокчейн пропонує безпечні та прозорі способи запису транзакцій та керування даними. Його застосування виходить за рамки криптовалют і включає управління ланцюгами поставок, охорону здоров'я та перевірку цифрової особи [6].

### 1.1.2 Гравці IT-ринку України

Попри війну з Росією прибутки IT-компаній. Найбільші гравці IT-ринку продовжують заробляти. У 2022 році українські IT-компанії заробили вдвічі більше, ніж у довоєнному 2021 році, їх дохід становить 103 млрд грн. У 2021 році прибуток першої сотні технологічних компаній склав близько 50 млрд грн.

Рейтинг топ-5 компаній за розміром прибутку в Україні мають 56,4% всього прибутку IT-галузі, а рейтинг топ-10 – становить 67,3%.

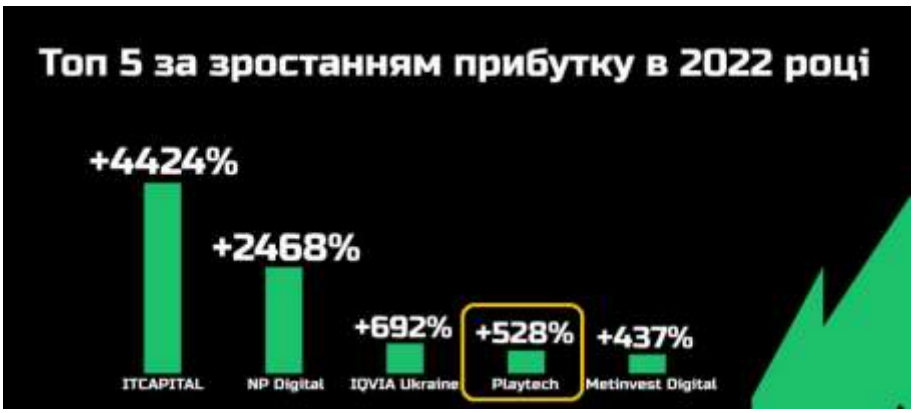


Рисунок 1.2 - Топ 5 IT-компаній України за зростанням прибутку у 2022 році

Найкраще зростають фінтех-компанії, продуктовий e-commerce, medtech та IT-курси.

Найбільше зростають фінтех-компанії CS LTD (провайдер рішень для банків) та Visa Ukraine (350 й 300% відповідно). Це дозволило їм потрапити у першу десятку рейтингу. Також там опинився маркетплейс Prom, який наростив прибуток утричі - від 56 млн грн у 2021 році до 225 млн грн у 2022 році..

Рекордсменами стали маркетингова агенція NP Digital (+2468%) та група компаній IT Capital, яка зросла у 44 рази. Компанія, що займається курсами для IT та розробляє сайти, отримала прибуток у 15 млн грн.

Неймовірне зростання також показали: гемблінгова компанія Playtech (+528%) та IQVIA Ukraine (+692%), які обробляють дані для medtech.

У 2022 році державні IT-компанії мають значно нижчі прибутки. Більшість державних підприємств, які займаються IT, показали у 2022 році нижчий прибуток, ніж у 2021 році. Це головний інформаційно-обчислювальний центр КМДА, такий же центр Мінсоцполітики, ДП «Інформаційні судові системи», ProZorro, СЕТАМ тощо. Зауважимо, що йдеться не про збитковість, а саме про нижчий прибуток.

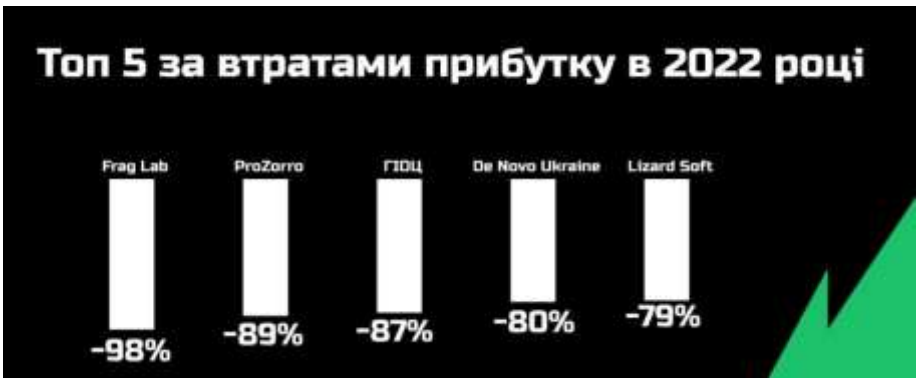


Рисунок 1.3 – Топ-5 IT-компаній в Україні за втратами прибутку у 2022 році

Технологічна компанія ТОВ "ПТС ЮА СЕРВІСЕЗ" зайняла 13 позицію у рейтингу топ 20 IT-компаній України з найбільшим прибутком.

У 2023, та 2024 роках Технологічна компанія ТОВ "ПТС ЮА СЕРВІСЕЗ" зайняла 33 та 29 відповідно позиції у рейтингу топ-50 IT-компаній України [5].

Таблиця 1.1 – Топ 20 IT-компаній України з найбільшим прибутком

| Позиція | Юридична особа | Назва | Чистий прибуток у 2022 році, тис. грн | Чистий прибуток у 2021 році, тис. грн | Динаміка, % |
|---|---|---|---|---|---|
| 1 | ТОВ "ЕПАМ СИСТЕМЗ" | EPAM Systems | 3 443 159 | 1 198 502 | 187 |
| 2 | ТОВ "ГлобалЛоджик Україна" | GlobalLogic Ukraine | 1 138 589 | 470 979 | 142 |
| 3 | ТОВ "Інфопульс Україна" | Infopulse Ukraine | 512 606 | 342 492 | 50 |
| 4 | ТОВ «ВЕЛЬЮТЕК» | Valuetek | 418 704 | - | - |
| 5 | ПрАТ "УКРАЇНСЬКИЙ ПРОЦЕСІНГОВИЙ ЦЕНТР" | UPC | 341 604 | 404 573 | -16 |
| 6 | ТОВ "ЛЮКСОФТ СОЛЮШНС" | Luxoft | 292 111 | 152 819 | 91 |
| 7 | ТОВ "УАПРОМ" | PROM.UA | 225 208 | 56 118 | 301 |
| 8 | ТзОВ "ІІТ" "Інтелліас" | Intellias | 213 626 | 108 828 | 96 |
| 9 | ТОВ "СІЕС ІНТЕГРА" | CS LTD | 204 106 | 45402 | 350 |
| 10 | ТОВ "ВІЗА УКРАЇНА" | Visa Ukraine | 194 857 | 48748 | 300 |
| 11 | ТОВ "ЛОГІКА ЛТД" | Capgemini Engineering | 193 913 | 168551 | 15 |
| 12 | ТОВ "ЕПАМ ДІДЖИТАЛ" | EPAM Digital | 168 463 | - | - |
| 13 | ТОВ "ПТС ЮА СЕРВІСЕЗ" | Playtech | 157 153 | 25 013 | 528 |
| 14 | ТОВ "ПЛЕЙТИКА УКРАЇНА" | Playtika | 156 861 | 137 245 | 14 |
| 15 | ТОВ "ПЛАРІУМ ЮКРЄЙН" | Plarium Ukraine | 144 080 | 49 739 | 190 |
| 16 | ТОВ "ІБМ УКРАЇНА" | IBM Ukraine | 136 298 | 77 333 | 76 |
| 17 | ТОВ "Сігма Софтвеа" | Sigma Software | 133 389 | 117 653 | 13 |
| 18 | ТОВ "ЕСТАУНД КОММЕРС" | Astound Commerce | 132 385 | 61 328 | 116 |
| 19 | ТОВ «СОФТВАРЕ ПРОДАКТ ДЕВЕЛОПМЕНТ» | Software Product Development LLC | 119 442 | 43 577 | 174 |
| 20 | ТОВ "Регіональна Газова Компанія" | RGC | 116 963 | 92 735 | 26 |

Багато керівників та CEO IT-компаній визнають, що 2025 рік буде складним. Це головним чином тому, що український IT-сектор потрапив у «ідеальний шторм»,

спричинений низкою несприятливих умов. До них відносяться війна, високі процентні ставки, стагнація після зростання в епоху Covid-19 та можливості кодування штучного інтелекту (ШІ). Учасники ринку вважають, що розробка власних продуктів imil-tech є виходом із ситуації [1].

### 1.1.2 Технологічна компанія

Глобальна Технологічна компанія заснована в 1999 році, компанія має преміальний лістинг на головному ринку Лондонської фондової біржі та зосереджена на регульованих та регулюючих ринках у своїх бізнесах B2B та B2C. Обидва підрозділи використовують запатентовану технологію для надання інноваційних продуктів і послуг для забезпечення безпечного, захоплюючого та розважального досвіду ставок та ігор.

Рисунок 1.4 - Офіси Технологічна компанія

Playtech є провідною платформою, постачальником контенту та послуг в індустрії онлайн-гемблінгу з чіткою стратегією, спрямованою на користь наших акціонерів, клієнтів, колег та навколишнього середовища.

Технологічна компанія зі штаб-квартирою у Великій Британії має офіси в 20 країнах, де працює понад 7 900 співробітників. Playtech має локації в наступних країнах: Австралія, Австрія, Болгарія, Кіпр, Естонія, Німеччина, Гібралтар, Ізраїль, Латвія, Перу, Румунія, Швеція, Україна, Великобританія, США та Мальта. Технологічна компанія має 7 900 співробітники, більше 180 ліцензіатів, більше 40 регульованих юрисдикцій [2].

Будучи частиною великої родинитехнологічна компанія, Київський R&D центр (ТОВ "ПТС ЮА СЕРВІСЕЗ») був створений в серпні 2011 році і з тих пір перетворився в один з основних центрів розробки всієї групи Playtech, що об'єднує 750 фахівців.

Playtech в Україна зібрав творчих, енергійних та розумних людей. Кращі розробники, тестувальники, дизайнери, проектні та продакт менеджери і всілякі фахівці разом творять цей дивовижний світтехнологічна компанія Kyiv.

Утехнологічна компанія Kyiv представлені підрозділи: Asian Pacific Operations, BetBuddy, Bingo, BIT, Casino Mobile, Casino Turnkey & JV, Billing, Finance, Geneity, GPA&POP, IMS Engagement, Live, Mexos, Mobenga, Mobile & Web Services, Origins, Psiclone, PT Sports, Quickspin, Rarestone, Videobet, Infrastructure. Не кажучи вже про підрозділи підтримки бізнесу, такі як IT, Site Operations, HR та Finance [3].

Технологічна компанія Kyiv представлена в Україні юридичною особою ТОВ "ПТС ЮА СЕРВІСЕЗ", код ЄДРПОУ 38749239, було зареєстровано 10.06.2013.

Основний вид діяльності (КВЕД) ТОВ "ПТС ЮА СЕРВІСЕЗ"– 62.01 Комп'ютерне програмування.

Юридична особа ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "ПТС ЮА СЕРВІСЕЗ" зареєстрована за юридичною адресою: Україна, **1, місто Київ, СПОРТИВНА ПЛОЩА , будинок ** А [4].


Рисунок 1.5 – Київський офістехнологічна компанія Kyiv

Відділеннятехнологічна компанія Services спеціалізується на наданні операційних послуг, включаючи підтримку клієнтів, управління ризиками та інші послуги, ліцензіатамтехнологічна компанія та їх кінцевим користувачам. Команда фахівців з ризиків, фінансів, KYC та комплаєнсу, швидко зростає, використовує передові системи запобігання шахрайству для захисту бізнесу клієнтів. Надійні платформи обробки платежів об'єднують наші послуги для безперебійної роботи [2].

Рисунок 1.6 - Керовані послугитехнологічна компанія

Технологічна компанія надає керовані технічні послуги доставки, щоб допомогти операторам ігор підключитися до платформитехнологічна компанія, спираючись на найкращі практики галузі та багаторічний досвід B2B та B2C. Після того, як оператори запрацюють, ми зможемо надавати оперативні консультаційні послуги, а також навчання та консультації за підтримки нашого центру знаньтехнологічна компанія Academy [2].

Рисунок 1.7- Технічні послуги

Технологічна компанія є новатором безпечних рішень для азартних ігор.технологічна компанія є піонером інноваційних та науково обґрунтованих рішень, які сприяють безпечнішій грі в усіх операціях та в галузі. За

допомогоютехнологічна компанія Protect надається ліцензія там передові технології відповідальної гри, адаптовані до бізнесу.

Playtech робить значний вклад в індустрію азартних ігор і суспільство наданням технологій для просування безпечніших азартних ігор і захисту гравців. Завдяки технологічним рішенням для безпечної гритехнологічна компанія допомагає операторам і індустрії посилити заходи захисту гравців і створити безпечніший досвід азартних ігор.

Рисунок 1.8 - Інноваційні науково обґрунтовані рішення для безпечнішої гри

Новаторські безпечніші рішення для азартних ігор завжди були життєво важливою сферою длятехнологічна компанія і сектору, в якому вона працює, і стануть ще важливішими в найближчі роки, оскільки ми працюємо над тим, щоб:

## 1.2 Принципи, технічні способи та математичні методи інформаційного забезпечення IT-компаній

### 1.2.1 Інформаційна система та комп'ютерна система

З точки зору цифрових технологій, основною проблемою є продуктивність використання та управління інформаційними активами. Накопичена роками

корпоративна інформація являє собою обсяги, які майже в десять разів перевищують річний бюджет на інформаційні системи і в сто разів перевищують річний бюджет на IT

Для інформаційних систем можливостей ще більше. Вони стосуються дематеріалізації тих чи інших видів діяльності, загальної продуктивності процесів, а також інновацій. Загальне керівництво та операційні або функціональні відділи повинні усвідомлювати трансверсальність багатьох видів діяльності. Комп'ютеризація підступно породила горезвісні осередки низької продуктивності за рахунок децентралізації обробки та розподілу багатьох завдань між усіма співробітниками компанії. Оскільки інформаційна система становить не більше і не менше кістяк нематеріальної діяльності сучасної компанії, вона, безсумнівно, є першим важелем ефективності для організацій.

Останніми роками спостерігається низка серйозних змін у сфері інформаційних систем. Нові підходи в цій сфері виходять далеко за рамки традиційних підходів.

Визначення інформаційної системи (ІС) можна визначити як «інформаційну систему для управління», «організаційну інформаційну систему» або «систему обробки інформації». ІС є частиною базового процесу прийняття рішень і надає допомогу особі, яка приймає рішення. Іншими авторами були запропоновані визначення, які враховують всю організовану діяльність, наприклад, як «інтегровану систему «користувач-машина», яка виробляє інформацію для допомоги людським істотам у функціях виконання, управління та прийняття рішень». Як і в попередньому визначенні, роль ІС обмежується наданням інформації.

Сучасне визначення ІС вийшло за межі стадії інструменту і стала структуруючим елементом організації, що суті є організованою сукупністю ресурсів: апаратних, програмних, кадрових, даних, процедур отримання, обробки, зберігання, передачі інформації (у вигляді даних, текстів, зображень, звуків і т.д.) в організаціях.

У проекті власник проекту (МОА: користувач-менеджер) відповідає за визначення та впровадження інформаційної системи, а саме:

- мета управління, керує визначенням ІС, визначає виробничу мету;

- організовує інформацію - ту інформацію, якою компанія вирішує керувати, визначає та структурує;

- користувач, робоче місце - це людина або машина, яка створює, маніпулює, перетворює інформацію або яку спонукає наявність чи цінність певної інформації;

- процес – це загальний план, що вказує на те, як учасники співпрацюють, використовуючи керовану інформацію для досягнення виробничої мети.


Рисунок 1.9 - Інформаційна система та комп'ютерна система

Комп'ютерна система – це «організований набір технічних об'єктів – апаратного забезпечення, програмного забезпечення, додатків – що представляє інфраструктуру інформаційної системи». У проекті керівник проекту (КПК: проектувальник) відповідає за проектування та створення ІТ-системи.

Дві різні концепції комп'ютерних систем:

- централізована комп'ютерна система: Ця концепція відповідає класичній діяльності ІТ-відділу. Традиційно він працює з використанням мейнфреймів та

пов'язаних з ними серверів, мобілізуючи відповідні команди та все необхідне програмне забезпечення. Залежно від компанії та її сектору діяльності, вони становлять від 1 до 2% обороту компанії.

- комп'ютерна система в широкому сенсі: Це функція комп'ютера. Він об'єднує всі центральні IT-системи та ті, що розташовані в різних підрозділах компанії. Ця область відповідає децентралізованим обчисленням. Комп'ютерна система в широкому сенсі цього терміну є сумою централізованих та децентралізованих обчислень. Вони становлять від 1,5% до 5% обороту компаній [8].

### 1.2.2 Практики щодо інформаційних систем організацій

Належні практики, пов'язані з ІС, відомі та застосовуються всіма фахівцями, а точніше, повинні застосовуватися. І навпаки, їх неефективне впровадження ризикує призвести до значного зниження ефективності та продуктивності.

Практики численні та різноманітні, наприклад:

- необхідність чіткого визначення області застосування кожної ІС (функції, групи функцій або процесу);

- необхідність розробки ефективної та результативної ІС;

- важливість процесів серед різних можливих підходів до ІС: одним з найефективніших є процесний підхід (глибинна тенденція, пов'язана з підходом до комплексного управління якістю: TQM);

- кожен процес повинен керуватися менеджером (для вжиття заходів щодо коригування);

- для контролю кожного процесу необхідно мати панель керування процесом для моніторингу його активності (визначення значущих показників, встановлення цілей для досягнення);

- процес повинен мати керівний комітет, щоб усі залучені особи, які приймають рішення, могли консультуватися та впливати на його функціонування.

- моніторинг аномалій, що виникають під час лікування (виявлення несправностей відповідно до їх ступеня тяжкості);

- необхідно запровадити достатні механізми контролю (гарантувати застосування правил внутрішнього контролю);

- ключовим моментом інформаційних технологій є здатність справлятися зі швидким зростанням обсягів обробки (наявність достатньо потужних систем обробки та зберігання);

- необхідно постійно докладати зусиль для зниження собівартості одиниці операцій; цей розвиток є результатом регулярно докладених зусиль щодо підвищення продуктивності (кращий контроль інформаційних систем).

Планування ІТ-розробок має бути впроваджено, оскільки розробки часто займають багато часу, а їх впровадження іноді є делікатним.

Ці різні найкращі практики спрямовані на вирішення проблем, пов'язаних з професіями. Мета полягає в кращому контролі складних комплексів, які мають ІТ-вимір, але також включають важливий бізнес-фактор. Знання та застосування цих різних передових практик може значно підвищити ефективність інформаційних систем [8].

## 1.3 Огляд існуючих інженерних рішень комп’ютерних систем для ІТ-компаній

### 1.3.1 Моделювання інформаційних систем

Моделювання - це представлення реальної системи відповідною мовою шляхом формалізації та використання знань у формі, яка може бути зрозумілою та використаною різними людьми або програмним забезпеченням, таким чином, щоб вона могла відтворювати операцію або передбачати поведінку за інших умов.

ІС – це складні реальності, складні системи, які повинні розуміти як керівник проекту, так і клієнт. Щоб зробити їх зрозумілими та проаналізувати, зрозуміти, передати та діяти, необхідно їх моделювати. «Так само, як будівництво будівлі чи мосту базується на планах та кресленнях», побудова інформаційної системи базується на різних моделях для кращого розуміння проблеми шляхом створення спрощеного представлення, на основі якого ми можемо діяти, щоб змінити її, та повідомляти про проект, щоб люди зрозуміли, якою буде цільова система.

Реальність описується за допомогою моделей, максимально точних до досліджуваної системи.

### 1.3.2 Інструменти та мови моделювання

Мова моделювання - це набір концепцій та правил для побудови моделей. Елементи, що складають мову моделювання, можуть бути представлені моделлю, яка називається метамоделлю.

Мови моделювання походять з різних наукових спільнот, де пропонується класифікувати основні методи, методології, еталонні архітектури та рамки моделювання за чотирма категоріями:

1. Структуровані підходи: базується на принципі низхідної, модульної, ієрархічної та структурованої декомпозиції, що дозволяє осягнути всю складність системи. Серед найвідоміших можна назвати SADT (техніку структурованого аналізу проектування) та сімейство методів IDEFx (IDEF0.

2. Системні підходи: зосереджені на взаємодії систем і, зокрема, на аналізі потоків: MERISE, GRAI (Графік взаємопов'язаних результатів та діяльності), PERA (Архітектура еталонних даних підприємства Purdue), CIMOSA (Архітектура відкритої системи CIM), GERAM (Узагальнена архітектура та методологія еталонних даних підприємства).

3 Процесно-орієнтований підхід. Багато інструментів та мов програмування є процесно-орієнтованими: ARIS (Архітектура інтегрованих інформаційних систем), SCOR (Довідник з операцій ланцюга поставок), MECI (Моделювання підприємства для інтегрованого проектування), BPMN (Нотація управління бізнес-процесами).

4. Об'єктно-орієнтовані підходи OMT (Метод моделювання об'єктів), OOD (Орієнтоване проектування об'єктів), OOSE (Об'єктно-орієнтоване програмне забезпечення), UML (Уніфікована мова моделювання).

Різні підходи враховують численні інструменти та методи для аналізу та моделювання промислових систем (включаючи інформаційні системи), показуючи, що якщо кожен з них пропонує рішення кількох проблем, то жоден з них не є достатнім для аналізу та моделювання складних систем.

### 1.3.3 Синтез

З огляду різних досліджень, проведених на тему моделювання складних систем, ми робимо висновок, що для оптимального представлення системи моделювач повинен вміти маніпулювати різними мовами моделювання, кожна з яких дозволяє зосередитися на заданій точці зору системи. Знання, необхідні для опису кожної точки зору, мають дуже різноманітну природу та типи, різне походження та часто підлягають інтерпретації відповідно до культури моделювання. Дотримуючись системної парадигми, необхідно відповісти на такі питання:

- Для яких цілей має бути створена система?
- Які функції реалізовані для їх досягнення?
- Які механізми генерації часових траєкторій змінних, що описують еволюцію системи? (можливі сценарії)?
- Які є ресурси? (Підтримка досягнення цілей)

Ці знання можуть походити з різних професійних категорій. Тоді необхідно дозволити кожному учаснику висловлюватися та обмінюватися думками з іншими відповідно до його рівня розуміння та компетентності.

### 1.3.4 Оцінка продуктивності системи за допомогою моделювання

Моделювання є одним з найефективніших інструментів прийняття рішень, доступних розробникам та керівникам складних систем. Він полягає в проведенні експериментів на моделі реальної системи з метою розуміння її поведінки та покращення її продуктивності.

#### 1.3.4.1 Підхід до моделювання

Моделювання - це використання або розв'язання моделей, що відповідають заданій системі, для вивчення її поведінки в певному контексті. Йдеться про дотримання певного процесу.

Таким чином, підхід до моделювання, проходить окремі етапи:

- етап моделювання: який полягає у побудові моделі явища, що вивчається;

- етап експериментування: який полягає у піддаванні цієї моделі певному типу варіацій;

- етап валідації, який полягає у порівнянні експериментальних даних, отриманих за допомогою моделі, з реальністю;

- аналіз: відповідає процесу виявлення, опису (тип проблеми, область застосування);

- моделювання: відповідає процесу визначення структурованого представлення.

- комп'ютерна реалізація: відповідає процесу побудови функціонального рішення проблеми (кодування рішення за допомогою певних мов програмування).

- моделювання: відповідає фазі використання реалізованої моделі.

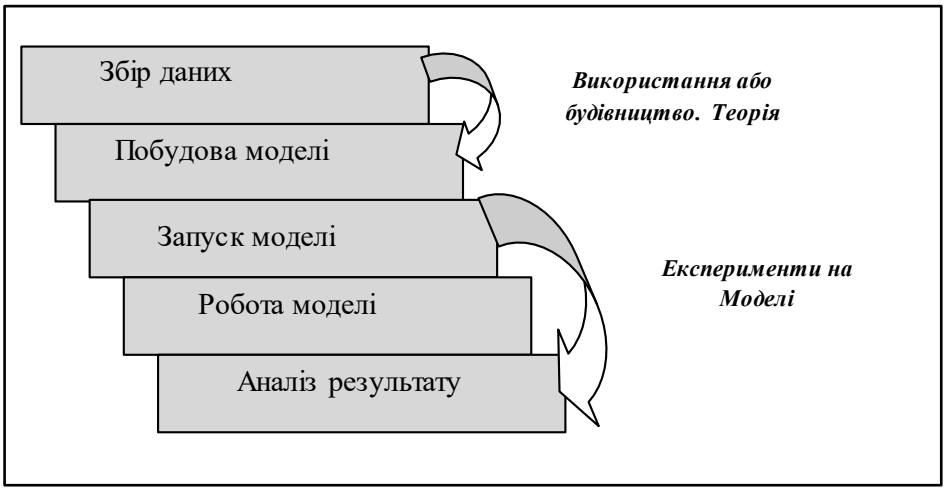


Рисунок 1.10 - Етапи процесу моделювання

#### 1.3.4.2 Синтез

Симуляційні дослідження, після широкого поширення в 1990-х роках, стають дедалі актуальнішими: моделі повинні бути близькими до реальності, зрозумілими та, по можливості, придатними для використання зацікавленими сторонами системи.

Моделювання стає поширеним інструментом для вивчення організації та управління системами з метою покращення їхньої роботи та зниження витрат. Іншими словами, моделювання все ще є потужним інструментом, що пропонує багато можливостей. Однак важливо не нехтувати фазами валідації та інтерпретації моделі, щоб сприяти її використанню [8].

## 1.4 Розробка схеми організаційної структури технологічної компанії Playtech

Майже кожен бізнес зараз покладається на технології, а технології ніколи не працюють абсолютно ідеально. Завжди необхідне технічне обслуговування, яке може включати ремонт, модернізацію та виправлення безпеки. Ці вимоги та завдання підпадають під категорію інформаційних технологій (IT). Отже, будь-яка

організація повинна враховувати IT-ініціативи при плануванні своїх бізнес-стратегій.

Варто починати планувати, як будуть впроваджуватися IT. Планування IT-структури має починатися з моменту зародження бізнесу. Це може бути дуже невеликий набір ресурсів для початку. Але з огляду на те, як вони можуть вплинути на діяльність бізнесу, важливо планувати їх на ранніх стадіях.

Перерахуємо фактори, які впливають на IT-планування.

1. Бізнес і стратегія:

- бізнес-стратегія - узгодження структури IT із загальними бізнес-цілями та стратегіями;

- тип галуз - галузеві нормативи та стандарти впливають на структуру IT, наприклад, у сфері охорони здоров'я, фінансів або юриспруденції;

- глобальна присутність - глобальним організаціям може знадобитися структура, яка підтримує діяльність у різних регіонах.

- інноваційні цілі - організації, орієнтовані на інновації, можуть мати спеціалізовані ролі та підрозділи;

- управління змінами - здатність організації адаптуватися до змін і потреба в структурах управління змінами;

- конкурентне середовище - конкурентне середовище та потреба в гнучкості та реагуванні;

- стратегічне партнерство: наявність стратегічного партнерства та вплив на співпрацю в IT.

2. Організаційні атрибути:

- розмір і масштаб: розмір організації впливає на складність і рівні IT-структури;

- культура організації може впливати на гнучкість та адаптивність IT-структури;

- IT-зрілість та технологічна складність в організації;

- клієнтська база - тип і розмір клієнтської бази може впливати на структуру надання IT-послуг.

- доступність набору навичок - наявність і розподіл конкретних навичок у робочій силі;

- уподобання працівників - уподобання та очікування IT-персоналу.

3. IT-середовище:

- кількість проектів і складність поточних проектів впливають на структуру управління та реалізації проектів.

- вимоги до співпраці - потреба в міжфункціональній співпраці та каналах зв'язку.

4. Технології:

- вимоги до технології: характер і складність технології, що використовується в організації;

- ініціативи цифрової трансформації: організаціям, які проходять цифрову трансформацію, може знадобитися структура, яка підтримує нові технології та практики;

- новітні технології: інтеграція новітніх технологій та потреба в спеціалізованих ролях.

5. Фінанси:

- бюджетні обмеження - фінансові міркування впливають на розподіл ресурсів і персоналу.

6. Корпоративне управління та відповідність:

- управління IT - рамки та політики управління IT впливають на структуру прийняття рішень;

- безпека та відповідність - суворі вимоги до безпеки та відповідності впливають на структуру, особливо в регульованих галузях;

- нормативно-правове середовище - дотримання галузевих норм і вимог відповідності.

7. Експлуатація та доставка:

- стратегія аутсорсингу - організації, які покладаються на аутсорсинг, можуть мати іншу структуру порівняно з тими, що мають внутрішні можливості;

- відносини з постачальниками: залежність від зовнішніх постачальників і потреба в структурах управління постачальниками;

- чутливість даних: чутливість і критичність даних, якими керує IT-організація;

- толерантність до ризику: толерантність організації до ризику та потреба в структурах управління ризиками [9].

Органограма - це візуальне представлення організаційної структури. Існує два типи органограм: органограми управління та органограми компанії.

1. Органограма управління показує взаємозв'язки між різними відділами, підрозділами та ролями в організації. Органограма зазвичай включає посади в організації та зв'язки підпорядкування між цими посадами. Вона може бути корисним інструментом для візуалізації та розуміння ролей і обов'язків в організації.

2. Органограма компанії може використовуватися для відображення акціонерів корпорації або учасників товариства з обмеженою відповідальністю. Органограму можна змінити, щоб включити інформацію про структуру власності компанії, таку як відсоток власності, що належить кожному акціонеру або учаснику. Це може бути корисним для демонстрації розподілу власності та повноважень щодо прийняття рішень у компанії [10].

Органограма управління технологічної компанії Playtech показана на рис. 11.1 за допомогою спрощеної функціональної структури, фахівці одного рівня об'єднуються в спеціалізовані підрозділи.

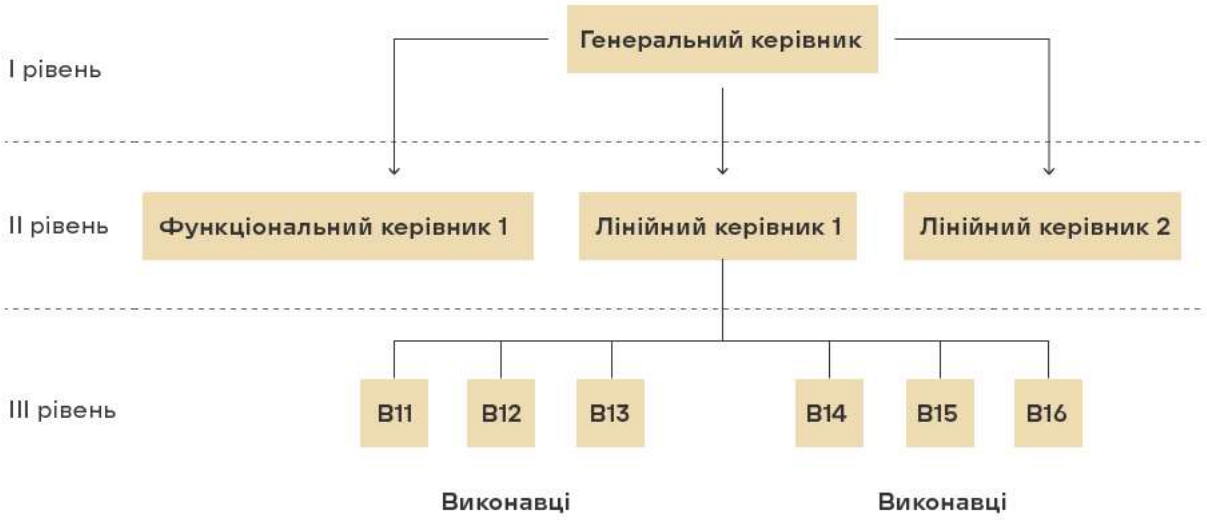


Рисунок 1.10 - Органограма управління технологічної компанії Playtech

Тобто спеціалісти з продажів - у відділ продажів, програмісти – відділ розробки програмного забезпечення, усі фахівці бухгалтерії - у фінансовий відділ тощо. До середньої ланки така структура буде аналогічна лінійній, а от нижче - вже формуватиметься за функціональною ознакою.

### 1.5 Постановка завдання

Бакалаврська кваліфікаційна робота спрямована на розробку комп'ютерної системи (КС) для технологічної компанії Playtech. Робота має окреме деталізоване завдання з побудови, налаштування та безпеки корпоративної мережі.

Метою бакалаврської кваліфікаційної робота є визначення основних завдань у сучасній телекомунікаційній галузі, зокрема організації централізованої корпоративної мережі, її різноманітного спектру, високоякісних та доступних послуг для користувачів цієї мережі. Для досягнення цілей дослідження враховуються такі вимоги:

– аналіз основної наукової, статистичної та довідкової інформації, дані, що пов'язані з інтернет-провайдером;

– розглядаються теоретичні аспекти проблеми на основі статистичної, наукової та практичної літератури, обговорюються причини вибору пристроїв Cisco, структура мережі компанії;

– представлено короткий огляд розширених параметрів для вибраних пристроїв та типу магістрального кабелю, а також процесу призначення IP-адрес, заснований на практичній, науковій та статистичній літературі.

Розроблена КС має відповідати показникам з високої надійності роботи, підвищеної стійкості до кіберзагроз програмного та апаратного забезпечення КС.

Спираючись на архітектуру КС, яка має значну кількість підмереж, їх складну взаємодію між собою, значну апаратного забезпечення мережі та робочих станцій користувачів слід ретельно виконати розрахунок для налаштувань пристроїв мережі, обрати належні інтерфейси та протоколи зв’язку, розрахувати налаштування маршрутизаторів. Особливим ключовим моментом є моделювання роботи мережі для впевненості її адекватного функціонування.

# 2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ТЕХНОЛОГІЧНОЇ КОМПАНІЇ PLAYTECH

Комп'ютерна система − це електронний пристрій, призначений для обробки даних. Вона складається з програмно - апаратних компонентів, таких як − мережеві пристрої, процесори, пам'ять та пристрої введення.

## 2.1 Технічні вимоги до комп'ютерної системи технологічної компанії Playtech

У широкому сенсі, технічні вимоги на розробку КС – це завдання для інженера, спрямоване на проектування та створення КС.

Це документ, у якому перелічено набір правил та обмежень, яких має дотримуватися розробники КС. Цей документ за рівнем деталізації заздалегідь узгоджується між Замовником та Розробником, та може в подальшому корегуватися до моменту повного узгодження між сторонами.

Загальноприйнятими форматами для створення технічних вимог є потреби користувачів та варіанти їх використання. Однак кожна компанія розробляє власні оптимальні шаблони для технічних вимог. Головне завдання технічних вимог − донести вимоги клієнтів до розробників. Оскільки клієнти не хочуть думати про деталі того, як працюватиме їхня майбутня КС, а розробники здебільшого прагнуть до належної деталізації.

### 2.1.1 Вимоги до комп'ютерної системи в цілому

#### 2.1.1.1 Вимоги до структури і функціонування комп'ютерної системи

Комп'ютерна система технологічної компанії Playtech це − інформаційна система (далі Система) побудована за допомогою програмно-апаратного

комплексу, цільовою метою, якої є управління та організація ефективної роботи технологічної компанії Playtech.

Локальна мережа КС використовується для об'єднання декількох комп'ютерів. Локальна мережа з'єднує комп'ютери в певній області (в одному департаменті, в одному приміщенні, на заводі чи станції тощо). Корпоративний мережевий пристрій використовується для з'єднання всіх комп'ютерів у фізичному середовищі та передачі певних даних.

В технологічній компанії Playtech створюють власну мережу, тобто корпоративну мережу, необхідну для захисту інформації, що зберігається в їхніх мережах, від несанкціонованого доступу. Користувачами корпоративної мережі можуть бути лише співробітники цього підприємства. Корпоративна мережа не надає послуг іншим користувачам та організаціям.

Корпоративна мережі поділяється на такі типи – глобальна і місцева.

Локальні корпоративні мережі організовані в кількох департаментах, розташовані поблизу одна від одної. Щоб створити та організувати їх, треба активувати технічний та інтелектуальний потенціал. Для створення багаторівневої локальної мережі потрібне спеціальне мережеве обладнання. Зазвичай використовується: маршрутизатори, комутатори. Існує кілька способів об'єднання комп'ютерів та мережевого обладнання в єдині комп'ютерні мережі: дротові, оптичні та бездротові. Переваги використання локальної мережі – це переваги, які мають будь-які пристрої, підключені до мережі. Ці пристрої можуть використовувати одне інтернет-з’єднання, обмінюватися файлами один з одним і друкувати на спільних принтерах.

Залежно від розміру відділів та департаментів підприємства, а також різноманітності проблем, які необхідно вирішити.

Відділові мережі – це мережі, що використовуються невеликою групою співробітників, що працюють в одному відділі підприємства. Ці співробітники виконують загальні завдання, такі як маркетинг або бухгалтерський облік.

Головною метою мережі департаментів є розподіл місцевих ресурсів. Локальні ресурси включають лазерні принтери та модеми, дані та програми. Відділи мають один або два файлові сервери у своїх мережах та не більше 30 користувачів. Також відомчі мережі не поділяються на підмережі. Більшість корпоративного трафіку ізольована в цих мережах. Завдання мережевого адміністрування на рівні відділу дуже прості: додавання нових користувачів, усунення простих збоїв, встановлення нових вузлів та оновлення програмного забезпечення.

### 2.1.1.2 Показники призначення

Комп’ютерна мережа будівлі центрального офісу технологічної компанії Playtech складається з 3 поверхів. На першому поверсі є 19 настільних комп'ютерів. На другому поверсі є 21 настільний комп'ютер. На третьому поверсі є 22 настільні комп'ютери. На кожному робочому місці встановлено телефони. Всі кабелі прокладаються в кабель-каналах на стелі кожного поверху.

Кабель прокладено за стандартом UTP категорії 5, що відповідає міжнародному стандарту. Цей стандарт передбачає наявність чотирьох пар мідних кабелів, два з яких здатні передавати дані зі швидкістю 100 МБ за секунду. Решта пар зарезервовані для інших завдань CSP.

### 2.1.1.2 Вимоги до експлуатаційної документації

Експлуатаційна документація на обладнання повинна містити такі розділи:

– інструкція з експлуатації;

– функціональна електрична схема;

– форма (для кожного центру зв'язку);

– схема електричних з'єднань (список елементів і таблиця з'єднань);

– перелік експлуатаційних документів;

– лист SPTA.

У керівництві по експлуатації повинен бути докладно описаний порядок роботи з обладнанням, аж до переліку команд. Метою інструкції з експлуатації є зменшення впливу людської помилки шляхом документування всієї роботи з обладнанням та програмним забезпеченням.

Експлуатаційна документація на програмне забезпечення повинна містити такі документи:

– «Інструкція з експлуатації»;

– «Керівництво адміністратора».

#### 2.1.1.4 Мінімальні вимоги до документації

Вся документація повинна відповідати наступним нормативним документам:

1. Оформлення документів. Ескізний проект.

2. Проектно-кошторисна документація. Технічні завдання на створення. Проект техноворкінгу.

3. Технічний проект. Специфікація обладнання, виробів і матеріалів.

4. Види випробувань автоматизованих систем.

5. Види, комплектність і позначення документів при створенні автоматизованих систем.

6. Технічне завдання на створення автоматизованої системи.

7. Інформаційні технології. Види випробувань автоматизованих систем.

Для Системи не передбачається використання запатентованих винаходів з обов’язковим ліцензуванням.

Система має будується виключно на ліцензованих в Україні стандартних виробах.

ПЗ є оригінальним без комерційного коду та алгоритмів, що може порушувати права інтелектуальної власності третіх осіб.

### 2.1.1.5 Додаткові вимоги

Пропонується розділити весь парк ПК в технологічній компанії Playtech на наступні стандартні конфігурації АРМ:

– Тип АРМ 1. Персональний комп'ютер для роботи зі спеціалізованим прикладним програмним забезпеченням (офісні системи, фінансові системи, СЕД і т.д.);

– Тип 2 AWP. Потужний персональний комп'ютер для роботи з графічними пакетами, програмними пакетами моделювання, CAD, ASUI, I&CS і т.д., використовується для додатків з просунутою графікою, високими вимогами до продуктивності процесора і оперативної пам'яті;

– Тип 3 AWP. Клієнт. Малопотужний персональний комп'ютер для роботи з додатками в термінальному середовищі, або з тонкими клієнтськими програмами в архітектурі клієнт-сервер. При цьому основні ресурсомісткі операції виконуються на сервері.

– Мобільне робоче місце. Ноутбук для мобільних користувачів..

Кожен АРМ складається з системного блоку, монітора (є можливість об'єднати системний блок і монітор в моноблок), клавіатури, маніпулятора миші (при необхідності) з встановленим і налаштованим загальносистемним програмним забезпеченням.

### 2.1.2 Мінімальні вимоги до інфраструктури дата-центру Системи

#### 2.1.2.1 Мінімальні вимоги до систем обробки та зберігання даних в технологічній компанії Playtech

Рекомендовані вимоги до сервера:

– CPU - останнє покоління, кількість обчислювальних ядер, розмір оперативного кешу різних рівнів підбираються під поставлену задачу з урахуванням рекомендацій виробника;

– оперативна пам'ять – не менше 256 ГБ з можливістю розширення принаймні до 1024 ГБ;

– відеопідсистема – підтримується використовуваною операційною системою; Дискова підсистема:

– контролер SAS, мінімум 2 (два) канали,

– використовуються тільки накопичувачі з гарячою заміною;

– двоканальний RAID-контролер, кеш контролера з автономним живленням, апаратна підтримка RAID 0, 1, на системах з декількома приводами – апаратна підтримка RAID 5;

– можливість встановлення двох iSCSI HBA;

– інімум 2 порти USB 2.0;

– інімум два мережевих адаптера – Ethernet 1000/10000 Мбіт/с з автоматичним вибором швидкості передачі даних;

– віддалене керування через Ethernet – виділений або загальний порт;

– можливість установки резервного блоку живлення з можливістю гарячої заміни;

– можливість встановлення в 19-дюймову шафу.

#### 2.1.2.2 Вимоги до телекомунікаційних шаф

Телекомунікаційні шафи мають відповідати наступним пунктам:

1. Тип – стандартна закрита шафа 19", висота – 42U (глибина шафи – 1000 мм, ширина шафи – 600 мм).

2. Знімні бічні і задні стінки − вхідні двері з замком.

3. Монтажний комплект.

### 2.1.2.3 Вимоги до джерел безперебійного живлення

Джерела безперебійного живлення мають відповідати наступним вимогам:

1. Номінальна потужність та час автономної роботи для забезпечення того, щоб підключене обладнання було не менше 10 хвилин; Технологія – подвійне перетворення;

2. ККД (коли підтримувані пристрої живляться від зовнішньої мережі) – 90% і використання коректора активного коефіцієнта потужності;

3. Вихідна напруга:

− форма – синусоїда;

− номінальне значення – 230/400 В;

4. Тестування акумулятора:

− при включенні;

− ручний режим тестування;

− автоматичні періодичні тестування;

5. Апаратний захист акумуляторної батареї від глибокого розряду;

6. Можливість підключення додаткового акумулятора;

7. Діапазон вхідної напруги 220 В ± 20%;

8. Звукова індикація режиму роботи акумуляторної батареї з можливістю вимкнення;

9. Можливість моніторингу та управління через локальний порт (USB/RS232);

10 Оснащений: порт LAN RJ-45 для моніторингу та керування SNMP UPS.

11. Може бути встановлений у стандартну 19-дюймову шафу.

12. Монтажний комплект для встановлення в стандартний 19-дюймовий корпус.

### 2.1.3 Вимоги до видів забезпечення

#### 2.1.3.1 Прикладне програмне забезпечення

Прикладне програмне забезпечення є однією з основних складових сучасної IT-інфраструктури. З точки зору кінцевого користувача, саме прикладне програмне забезпечення допомагає вирішувати ті чи інші бізнес-завдання.

Характеристики прикладного програмного забезпечення:

– функціональність – здатність програмного забезпечення максимально ефективно виконувати заявлені функції з необхідними характеристиками; Функціональна повнота – це повний набір функцій, на які здатне дане програмне забезпечення;

– незалежність платформи – здатність програмного забезпечення функціонувати в різних програмних і апаратних середовищах, під управлінням різних операційних систем; Продуктивність – здатність програмного забезпечення забезпечувати збір, обробку та зберігання

– певний обсяг інформації для заданої конфігурації апаратної платформи певної архітектури.

– масштабованість – здатність Програмного забезпечення коректно працювати на малих і великих системах з продуктивністю, яка в загальному випадку зростає послідовно відповідно до збільшення обчислювальної потужності системи (кількість процесорів і їх ядра, розмір доступної оперативної пам'яті, швидкість дискових масивів, кількість серверів і т.д.), що використовуються для роботи з цим Програмним забезпеченням;

– здатність до інтеграції – здатність програмного забезпечення інтегруватися та взаємодіяти з іншими

– системи, включаючи застаріле програмне забезпечення та сторонні системи, а також працюють на інших платформах.

– maturity – історія розвитку даного програмного забезпечення (наявність даного програмного забезпечення на ринку протягом певного періоду часу, регулярний випуск нових версій, релізів і оновлень виробником) і заявлені виробником плани по його розвитку. Наявність «екосистеми» – кількість організацій, що експлуатують програмне забезпечення, кількість розробників і фахівців, здатних впроваджувати і розгортати програмне забезпечення, наявність навчальних закладів (навчальні центри, навчальна література і т.д.);

– надійність і відмовостійкість – здатність програмного забезпечення і побудованих на його основі систем до безперебійної, безперебійної роботи, а в разі програмних і апаратних збоїв – здатність швидко відновлювати працездатність системи.

Загальна вартість володіння програмного забезпечення складається з витрат на первинну покупку апаратної складової та придбання (розробку) програмного забезпечення, його введення в експлуатацію та витрати на його експлуатацію та обслуговування протягом стандартного терміну експлуатації цього програмно-апаратного комплексу. Загальна вартість володіння включає витрати на: модернізацію програмного та апаратного забезпечення; за навчання, обслуговування, адміністрування та технічну підтримку.

З точки зору процесів розробки, поставки та супроводу весь набір прикладного програмного забезпечення можна розділити на дві групи:

1. Універсальне (відтворюване) програмне забезпечення – програмне забезпечення, доступне на ринку і використовується для вирішення універсальних завдань.

2. Custom software – програмне забезпечення, розроблене на замовлення IT-відділу або третьої сторони.

Якщо на ринку існує програмне забезпечення з відкритим вихідним кодом, функціональність, надійність та зручність використання закритого вихідного коду порівнянна або краща за програмним забезпеченням із закритим вихідним кодом, слід віддавати перевагу програмному забезпеченню з відкритим вихідним кодом.

### 2.1.3.2 Загальні вимоги до користувацького програмного забезпечення

При виборі та впровадженні нового прикладного програмного забезпечення повинні бути дотримані такі вимоги:

– все використовуване прикладне програмне забезпечення повинно бути уніфіковане і каталогізоване в рамках КПЗ у вигляді переліку програм, прийнятних для використання;

– програмне забезпечення клієнтського ПК має бути функціонально повноцінним і забезпечувати як стандартні бізнес-процеси, так і конкретні бізнес-завдання для користувача.

– програмне забезпечення повинно бути зрілим: виробник (постачальник) повинен гарантувати підтримку та обслуговування цього програмного забезпечення протягом усього нормативного терміну дії цього програмного забезпечення;

– рекомендується використовувати платформонезалежне програмне забезпечення, яке забезпечує свободу вибору програмних і апаратних засобів для її роботи і, в кінцевому підсумку, знижує загальну вартість володіння системою;

– рекомендується використовувати продуктивне, масштабоване програмне забезпечення, що забезпечує гарантії безперервності бізнес-процесів при збільшенні обсягу оброблюваної і збереженої інформації. Бажано, щоб виробник програмного забезпечення регулярно проводив широке і навантажувальне тестування свого програмного забезпечення і надавав дані про результати цього тестування;

– рекомендується використовувати тільки програмне забезпечення, яке інтегрується з іншими системами і має відкриту архітектуру. При виборі програмного забезпечення необхідно враховувати можливості його інтеграції в існуючу IT-інфраструктуру підприємства;

– при виборі програмного забезпечення повинні вигравати системи з перевіреним досвідом використання в державних установах.

– рекомендується відмово-стійке програмне забезпечення для забезпечення критичних бізнес-процесів і сервісів;

– сумарна вартість володіння програмним забезпеченням, розрахована на весь стандартний термін служби даного програмного забезпечення, повинна служити найважливішим критерієм при виборі конкретного постачальника і програмного забезпечення;

– програмне забезпечення, призначене для забезпечення інформаційної безпеки, повинно мати сертифікати відповідності вимогам інформаційної безпеки;

– програмне забезпечення має бути належним чином задокументоване. Мінімальними вимогами до документації є наявність Керівництва користувача та документів Посібника адміністратора.

#### 2.1.3.3 Загальні вимоги до універсального прикладного програмного забезпечення

При придбанні нового універсального прикладного програмного забезпечення необхідно дотримуватися таких вимог:

– рекомендується купувати програмне забезпечення за спеціальними моделями ліцензування, які здешевлюють закупівлі;

– при використанні ліцензійного програмного забезпечення воно повинно бути ліцензованим і належним чином зареєстрованим. Рекомендується використовувати програмне забезпечення виробників, які добре зарекомендували

себе на ринку в цій сфері. Бажано, щоб цей виробник був на ринку з таким або подібним програмним забезпеченням не менше трьох років. Не рекомендується використовувати застарілі версії програмного забезпечення, а також занадто нові, «незрілі» версії програмного забезпечення;

– слід заборонити використання програмного забезпечення, яке не має як ліцензій, так і підтримки (обслуговування) від виробника;

– при виборі універсального програмного забезпечення слід керуватися загальними вимогами до прикладного програмного забезпечення, а також рекомендаціями «Сучасні тенденції в ІТ».

#### 2.1.3.4 Адресація в комп'ютерній мережі

Адресація в комп'ютерній мережі має бути розбита на п'ять підмереж, згідно структура технологічної компанії Playtech, складатися з підмереж:

LAN1 – адміністративно-управлінська частина, для обслуговування:

– адміністративного відділу;

– відділу бухгалтерського обліку та звітності;

– планово–економічного відділу;

– загально-програного відділу;

LAN2 – підрозділи розробки спеціалізованого ПЗ;

LAN3 – підрозділи для обслуговування клієнтів;

LAN4 – – підрозділи сервісного обслуговування;

LAN5 – господарсько-обслуговуюча частина.

### 2.2 Розробка апаратної частини системи

#### 2.2.1 Розробка загальної архітектура мережі підприємства

Для проектування модернізованої мережі, роблено наступне. Перш за все, змінена стара схема мережі, оскільки порти використовували хаби, а також керовані

комутатори без захисту портів. Як відомо, всі пакети, що надходять до порту-хаба, розподіляються на решту портів і тому піддаються широкомасштабній розсилці, яка перевантажує мережу, що може призвести до її збою. Якщо мова йде про комутатор, розташований у центральному офісі компанії технологічної компанії Playtech, немає можливості налаштувати порти для запобігання несанкціонованому доступу. У зв'язку з вищесказаним можна відзначити такі недоліки цієї мережі:

– немає можливості дистанційно керувати вимикачами;

– незахищені порти;

– використання концентраторів або хабів.

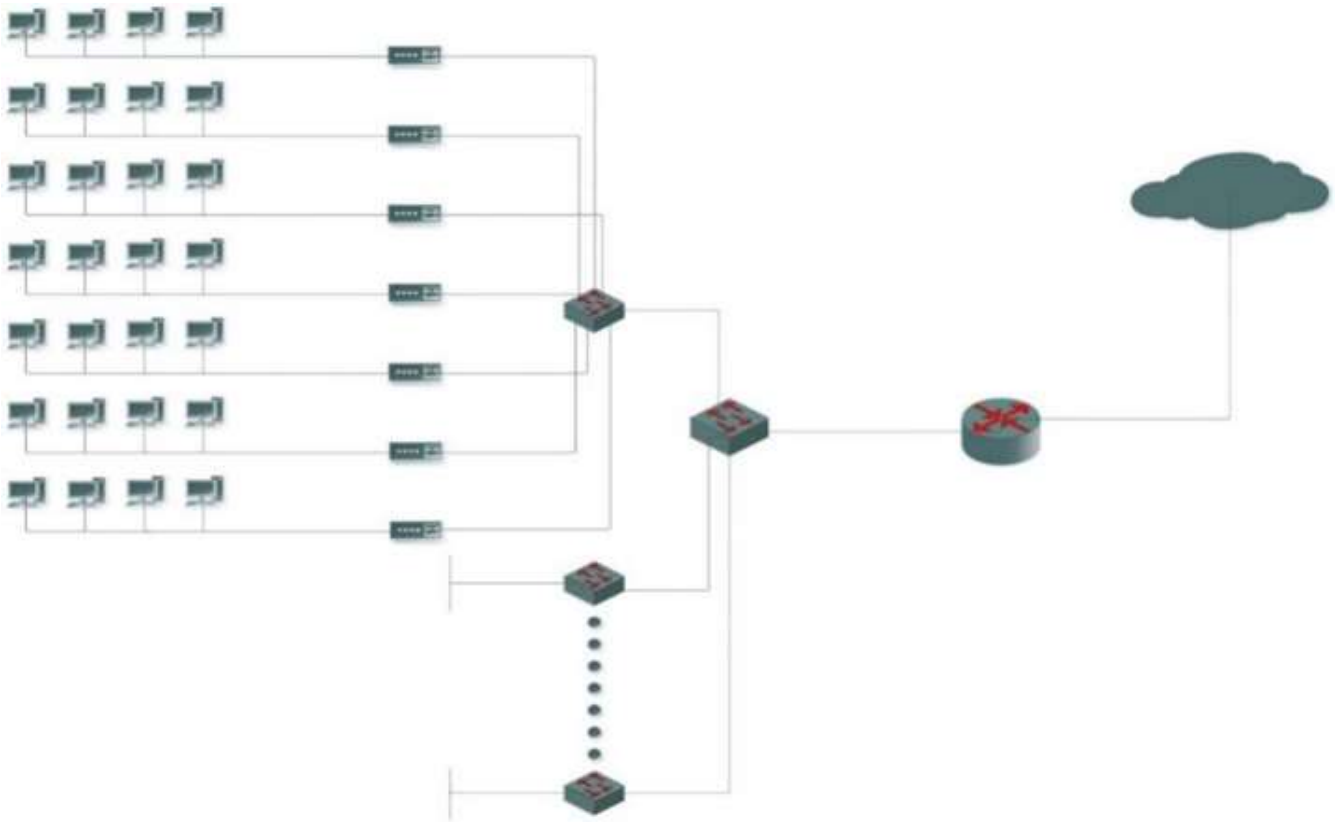

Рисунок 2.7 – Існуюча мережа технологічної компанії Playtech

Щоб усунути ці недоліки, вжито наступних заходів:

– замінено усі хаби на комутатори другого рівня;

– використано можливість запам'ятовувати MAC-адресу останнього пристрою, щоб захистити порт від несанкціонованого доступу;

– використано комутатори третього рівня для резервного копіювання мереж та на випадок відключення або виходу з ладу одного з комутаторів, тим самим підвищуючи стійкість мереж до збоїв.

Відповідно до організаційної структури технологічної компанії Playtech, яка, вимагає поєднання всі команди IT–фахівців компанії у комп'ютерну мережу.

Структура комп'ютерної системи технологічної компанії Playtech відповідає визначенням по завданню до кваліфікаційної роботи бакалавра.

Загальна структура мережі КС технологічної компанії Playtech має вигляд як показано на рис. 2.1.

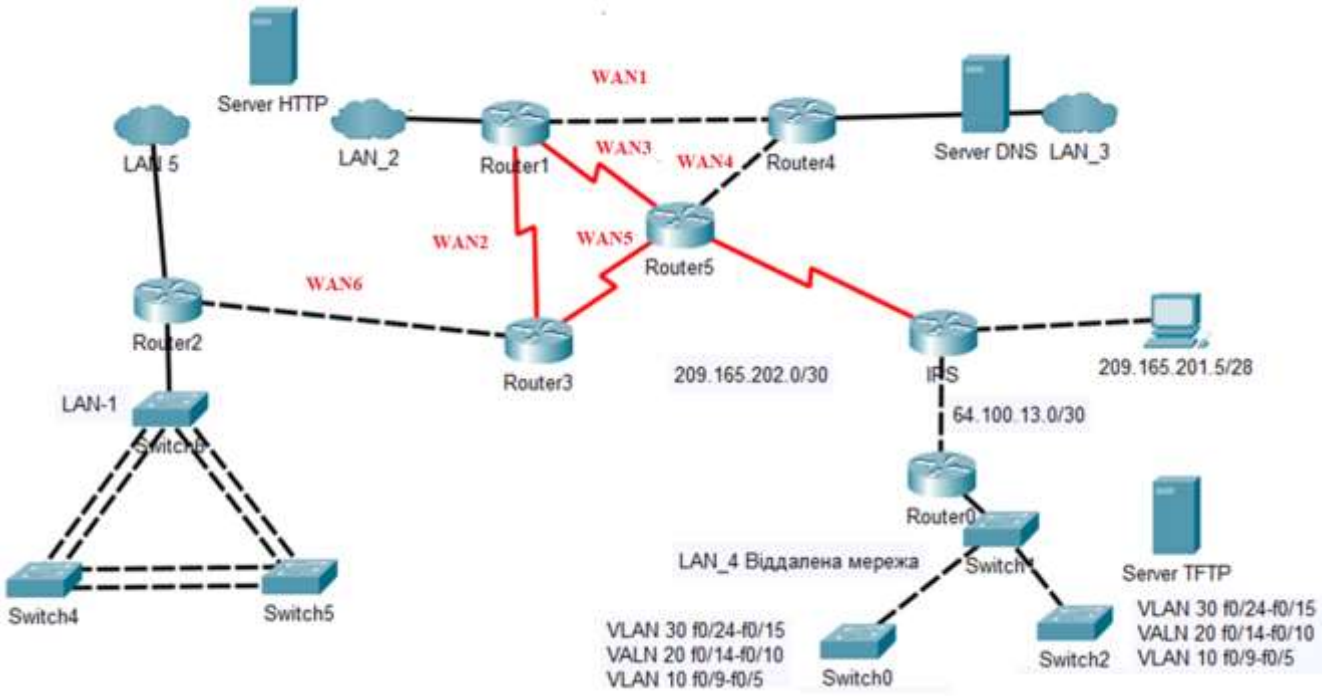


Рисунок 2.8 – Топологія мережі технологічної компанії Playtech

### 2.2.2 Розробка загальної архітектура мережі підприємства

Раніше в мережах використовувалася статична IP-адресація, при розробці мережі КС було змінено на динамічну IP-адресацію за допомогою протоколу маршрутизації OSPF.

Рисунок 2.2 – Мережева безпека від Cisco

OSPF - це масштабований протокол маршрутизації, який можна використовувати як в одній області невеликої мережі, так і в кількох областях великої мережі. OSPF - це найпоширеніший протокол внутрішньої маршрутизації. Коли ми говоримо про внутрішню маршрутизацію, це означає, що з'єднання між маршрутизаторами встановлюється в межах одного домену маршрутизації або в межах однієї автономної системи. Уявіть собі компанію середнього розміру з кількома будівлями та різними відділами, кожен з яких з'єднаний з іншими за допомогою резервного каналу зв'язку для підвищення надійності. Усі будівлі є частиною єдиної автономної системи.

Було заплановано підключення комутаторів рівня 3 за допомогою команди port_chenel, яка дозволяє мені використовувати два канали як один, і якщо один з каналів вийде з ладу, комутатори працюватимуть один з одним, використовуючи другий канал. Знову ж таки, використовуючи вирішувач, можна використовувати протокол HSRP (HSRP – це протокол Cisco, розроблений для підвищення доступності маршрутизаторів, що діють як шлюзи за замовчуванням) власний протокол), що дозволяє мені перевести кілька VLAN у режим очікування, тобто один комутатор відповідає за третій рівень, одну групу VLAN, а інші відповідають за другий. Наприклад, VLAN активна на першому комутаторі, тоді як на другому

комутаторі вона очікує на розгляд. Іншими словами, мережа не втрачає своєї працездатності

### 2.2.3 Вибір і обґрунтування структурної схеми технологічної компанії Playtech

Компанія Cisco має унікальну перевагу в галузі кібербезпеки, оскільки щодня обробляємо в середньому 715 мільярдів DNS-запитів, ми стикаємося з більшою кількістю загроз безпеці даних, шкідливим програмним забезпеченням і кібератак, ніж будь-який інший постачальник рішень безпеки.

Мережева безпека − це захист базової мережевої інфраструктури від несанкціонованого доступу, неправильного використання або крадіжки. Вона передбачає створення безпечної інфраструктури для пристроїв, програм, користувачів і програм, щоб вони могли працювати безпечним чином.

Мережева безпека поєднує кілька рівнів захисту на периферії та в мережі. Кожен рівень мережевої безпеки реалізує політики та засоби контролю. Авторизовані користувачі отримують доступ до мережевих ресурсів, але зловмисники блокуються від здійснення експлойтів та загроз.

Цифровізація змінила наш світ. Те, як ми живемо, працюємо, відпочиваємо та навчаємося, змінилося. Кожна організація, яка хоче надавати послуги, яких потребують клієнти та співробітники, повинна захищати свою мережу. Мережева безпека також допомагає вам захистити конфіденційну інформацію від атак. Зрештою, це захищає вашу репутацію.

Типи мережевої безпеки

1. Брандмауери. Брандмауер – це мережевий пристрій безпеки, який контролює вхідний і вихідний мережевий трафік і вирішує, чи дозволяти, чи блокувати певний трафік на основі визначеного набору правил безпеки. Cisco пропонує як брандмауери, орієнтовані на загрози, так і пристрої уніфікованого керування загрозами (UTM).

2. Безпека робочого навантаження. Безпека робочих навантажень захищає робочі навантаження, що переміщуються між різними хмарними та гібридними середовищами. Ці розподілені робочі навантаження мають більші поверхні для атак, які необхідно захистити, не впливаючи на гнучкість бізнесу.

3. Безпека мережі. Безпека мережі (NetWORK security) – це бачення Cisco щодо спрощення безпеки мережі, робочих навантажень та багато-хмарних систем шляхом надання уніфікованих засобів контролю безпеки для динамічних середовищ.

4. Сегментація мережі. Програмно-визначена сегментація розподіляє мережевий трафік на різні категорії та спрощує дотримання політик безпеки . В ідеалі класифікації базуються на ідентифікації кінцевих точок, а не лише на IP-адресах. Ви можете призначати права доступу на основі ролі, розташування тощо, щоб надавати правильний рівень доступу потрібним людям, а підозрілі пристрої були локалізовані та виправлені.

5. VPN.Віртуальна приватна мережа шифрує з'єднання від кінцевої точки до мережі, часто через Інтернет. Зазвичай VPN з віддаленим доступом використовує IPsec або Secure Sockets Layer для автентифікації зв'язку між пристроєм і мережею.

6. Контроль доступу.

Не кожен користувач повинен мати доступ до вашої мережі. Щоб захистити себе від потенційних зловмисників, вам потрібно розпізнавати кожного користувача та кожен пристрій. Після цього ви зможете застосувати свої політики безпеки. Ви можете заблокувати кінцеві пристрої, які не відповідають вимогам, або надати їм лише обмежений доступ. Цей процес називається контролем доступу до мережі (NAC).

7. Механізм служб ідентифікації Cisco. Антивірусне програмне забезпечення та програмне забезпечення для захисту від шкідливих програм. «Зловмисне програмне забезпечення», скорочення від «зловмисне програмне забезпечення», включає віруси, хробаків, трояни, програми-вимагачі та шпигунські програми.

Іноді шкідливе програмне забезпечення заражає мережу, але перебуває в сплячому стані протягом кількох днів або навіть тижнів. Найкращі програми захисту від зловмисного програмного забезпечення не лише сканують на наявність шкідливого програмного забезпечення під час входу, але й постійно відстежують файли після цього, щоб знайти аномалії, видалити шкідливе програмне забезпечення та усунути пошкодження.

8. Безпека додатків. Будь-яке програмне забезпечення, яке ви використовуєте для ведення бізнесу, має бути захищене, незалежно від того, чи створює його ваш IT-персонал, чи купуєте ви його. На жаль, будь-яка програма може містити дірки або вразливості, які зловмисники можуть використовувати для проникнення у вашу мережу. Безпека програми охоплює обладнання, програмне забезпечення та процеси, які ви використовуєте для закриття цих прогалин. Повна спостережливість AppDynamics APM Cisco App-first Proposal-first продукти Консультативні послуги з безпеки

9. Поведінкова аналітика. Щоб виявити аномальну поведінку мережі, ви повинні знати, як виглядає нормальна поведінка. Інструменти поведінкової аналітики автоматично розпізнають дії, які відхиляються від норми. Після цього ваша команда безпеки зможе краще виявляти ознаки компрометації, які становлять потенційну проблему, і швидко усувати загрози.

10. Аналітика захищеної мережі Cisco. Вбудована аналітика безпеки в Cisco.

а). Хмарна безпека. Хмарна безпека – це широкий набір технологій, політик і додатків, які застосовуються для захисту інтелектуальної власності в Інтернеті, сервісів, додатків та інших необхідних даних. Це допомагає вам краще керувати своєю безпекою, захищаючи користувачів від загроз у будь-якому місці, де вони мають доступ до Інтернету, і захищаючи ваші дані та програми в хмарі.

б). Захист від втрати даних. Організації повинні переконатися, що їхні співробітники не надсилають конфіденційну інформацію за межі мережі. Технології запобігання втраті даних (DLP) можуть зупинити людей від

завантаження, пересилання або навіть друку важливої інформації в небезпечний спосіб.

в). Шлюзи електронної пошти є вектором загроз номер один для порушення безпеки. Зловмисники використовують особисту інформацію та тактику соціальної інженерії для створення складних фішингових кампаній для обману одержувачів і надсилання їх на сайти, які містять шкідливе програмне забезпечення. Програма безпеки електронної пошти блокує вхідні атаки та контролює вихідні повідомлення, щоб запобігти втраті конфіденційних даних.

11. Безпека промислової мережі. У міру цифровізації промислових операцій, глибша інтеграція між IT, хмарними та промисловими мережами наражає ваші промислові системи керування (ІКС) на кіберзагрози. Вам потрібна повна видимість стану безпеки ваших OT, щоб сегментувати промислову мережу та надавати інструментам IT-безпеки детальну інформацію про пристрої та їхню поведінку.

12. Безпека мобільних пристроїв. Кіберзлочинці все частіше атакують мобільні пристрої та додатки. Протягом наступних трьох років 90 відсотків IT-організацій можуть підтримувати корпоративні додатки на персональних мобільних пристроях. Звичайно, вам потрібно контролювати, які пристрої можуть отримувати доступ до вашої мережі. Вам також потрібно буде налаштувати їхні з'єднання, щоб забезпечити конфіденційність мережевого трафіку.

13. Інформація про безпеку та управління подіями. Продукти SIEM об'єднують інформацію, необхідну вашим співробітникам служби безпеки для виявлення загроз та реагування на них. Ці продукти бувають різних форм, включаючи фізичні та віртуальні пристрої, а також серверне програмне забезпечення.

14. Веб-безпека. Рішення для веб-безпеки контролюватиме використання Інтернету вашими співробітниками, блокуватиме веб-загрози та заборонятиме доступ до шкідливих веб-сайтів. Воно захистить ваш веб-шлюз на місці або в хмарі.

«Веб-безпека» також стосується кроків, які ви вживаєте для захисту власного веб-сайту.

15. Безпека бездротового зв'язку. Бездротові мережі не такі безпечні, як дротові. Без суворих заходів безпеки встановлення бездротової локальної мережі може бути схожим на розміщення портів Ethernet всюди, включаючи парковку. Щоб запобігти поширенню експлойту, вам потрібні продукти, спеціально розроблені для захисту бездротової мережі.

### 2.2.4 Специфікація апаратної частини технологічної компанії Playtech

Для створення специфікації апаратної частини технологічної компанії Playtech необхідно визначити – забезпечення мережевої інфраструктури, забезпечення безпеки мережевих інтерфейсів, скільки часу потрібно як пропонується доступ до інформації в мережі, відповідно до корпоративної політики, кожному клієнту, який запитує доступ до мережі.

Існує два типи мережевих екранів: апаратні та програмні пристрої. У програмі передбачено брандмауер, що працює у фоновому режимі, для моніторингу продуктивності системи в режимі реального часу. Як і у випадку з багатьма іншими системами безпеки, рекомендується встановити лише один брандмауер, щоб не доводилося вручну видаляти файли на завантажувальному диску. Апаратний брандмауер – це спеціалізований апаратний пристрій, оптимізований для фільтрації модулів та захисту від логічних схем. Вважається, що вбудований брандмауер Windows є вибором користувача, оскільки він не запитує користувача спливаючими повідомленнями та захищає комп'ютер від вхідних загроз. Крім того, він не вимагає встановлення брандмауера Windows і не заважає роботі інших програм.

Рисунок 2.3 – Комутатор Cisco Catalyst WS-C2960-48TC-L

Cisco Catalyst 2960 – це нове сімейство комутаторів другого рівня з фіксованою конфігурацією, які дозволяють робочим станціям підключатися до мереж Fast Ethernet та Gigabit Ethernet, задовольняючи зростаючі потреби в пропускній здатності на периферії мережі, а також забезпечуючи підключення до мереж Fast Ethernet та Gigabit Ethernet зі швидкістю широкомовного середовища. Технологія Gigabit Ether Channel використовує інтегровані гігабітні порти uplink, які можна об'єднати в один канал. Крім того, цей комутатор призначений для малого та середнього бізнесу та філій великих компаній. Комутатор забезпечує широкий спектр функцій безпеки та гарантії якості обслуговування, а також управління пропускною здатністю.

Пристрій дозволяє підключати кілька пристроїв до мережі. Завдяки функції Smartports ви можете налаштувати комутатор відповідно до його призначення. Підтримуючи технологію безпеки Network Admission Control (NAC), QoS та високий рівень стабільності системи, комутатор забезпечує високий рівень безпеки даних.

Основні функції комутатора Cisco Catalyst WS-C2960-48TC-L включають:

– швидкісне підключення Ethernet з живленням через Ethernet до 15,4 Вт на порт;

– покращена система усунення несправностей для вирішення проблем з підключенням, включаючи кабельні розв'язки та діагностику;

– керування через одну IP-адресу для максимум 16 комутаторів;

– широкий спектр програмних інструментів, простота використання, високий рівень безпеки бізнес-операцій, стабільність та безмежні мережі.

Таблиця 2.1 – Технічні характеристики комутатора Cisco Catalyst WS-C2960-48TC-L

| Номер статті | WS-C2960-48TC-L |
|---|---|
| Тип обладнання | перемикач |
| Стандарти дротового зв'язку | 802.3 (10BASE-T) Ethernet 802.3ab (1000BASE-T) Ethernet 802.3u (100BASE-TX) Ethernet 802.3x (повний дуплекс) |
| Швидкість передачі | 1000 Мбіт/с |
| Розмір оперативної пам'яті | 64 МБ |
| Розмір вбудованої пам'яті | 32 МБ |
| Порти та інтерфейси | 48 × RJ-45 Ethernet 10/100 2 × RJ-45 10/100/1000 2 × SFP Gigabit Ethernet 1 × консольний порт 10/100/1000 Base-TX 2 порти з 2 підключеними SFP |
| Сервіс | DHCP-сервер, SNMP |
| Індикатори | система, RPS, стан з'єднання, дуплекс, швидкість, узгодженість з'єднання на кожному порту, вимкнення, активність, повний дуплекс швидкість |
| Можливість встановлення на підставку | 1U |
| Додаткові функції | Розмір MAC-таблиці 8K адрес Автоматичне визначення швидкості порту MDI/X Автоматичне визначення |
| Мережеві комутатори | Керований |
| Споживана потужність (макс.) | 39 Вт |
| Харчування | 100-240 В, 0,8-1,3 А |
| Робоча температура | 10...45 °C |
| Робоча вологість | 10...90% |
| Колекція | перемикач |
| Розміри (Ш×В) | Кронштейн для кріплення на стовпі |
| Справа | 4,5 × 4,4 × 23,6 см |
| Вага товару | 3,6 кг |

Рисунок 2.4 – Комутатор Cisco Catalyst WS-C3750-24FS-S

Комутатори Cisco Catalyst 3750 розроблені для середніх підприємств та відділів великих корпорацій, і мають багато інноваційних функцій. Вони характеризуються простотою використання та найвищою відмовостійкістю серед перемикачів зі скляним покриттям. Висока ефективність локальної мережі при використанні стекування досягається завдяки застосуванню технології Cisco StackWise.

Технологія Cisco StackWise − це новий стандарт відмовостійкості для пристроїв на базі скла. Використання інноваційної технології Cisco StackWise підвищує відмовостійкість, простоту використання та експлуатаційну ефективність комутаторів на основі скла. Технологія Cisco StackWise дозволяє об'єднати до 9 комутаторів Cisco Catalyst серії 3750 в один комутаційний блок із пропускною здатністю 32 Гбіт/с.

Керування комутаторами здійснюється через WEB-інтерфейс (через мережеве підключення) або інтерфейс командного рядка (через консольний порт або по мережі через Telnet).

Сімейство керованих скляних комутаторів рівня 2 (комутація на основі MAC-адрес) та рівня 3 (динамічна та статична маршрутизація на основі IP-адрес), які підтримують додаткові сервіси рівня 3 та 4 для робочих груп або ядра мережі. Розроблено для середніх та великих мереж (понад 250 користувачів). Комутатори забезпечують дуже високий рівень відмовостійкості, керованості, безпеки та масштабованості. Стекування комутаторів серії 3750 дозволяє керувати стеком комутаторів як єдиним пристроєм, використовуючи одну IP-адресу. Крім того, пропускна здатність скляного каналу становить 32 Гбіт/с, що дорівнює продуктивності внутрішньої шини комутатора. Стекування здійснюється за

допомогою спеціальних кабелів, які підключаються до перемикачів на задній панелі. Канал скління можна замкнути в кільце, щоб збільшити стійкість стека до відторгнення.

Серія 3750 включає як 50-мегабітні, так і гігабітні моделі комутаторів. Він також має 2 або 4 гігабітні порти Ethernet SFP. Є модель з 2-м і 2-м портами. Лінійка гігабітних комутаторів включає моделі з 24 або 48 «мідними» гігабітними портами та 4 SFP-портами. Також є модель з 12 SFP-портами та модель з 16 «мідними» гігабітними портами та 10 гігабітними портами. Усі моделі комутаторів доступні з різними версіями програмного забезпечення.

Комутатори серії 3750 підтримують стандарт живлення через Ethernet (IEEE 802.3 af). Завдяки цій технології різні мережеві пристрої (такі як точки бездротового доступу, IP-телефони та відеокамери) можуть живитися безпосередньо через мережеве з'єднання. До 24 пристроїв зі споживанням енергії 15,4 Вт на комутатор або можна підключити до 48 пристроїв з потужністю 7,3 Вт.

Керування комутаторами здійснюється через веб-інтерфейс або інтерфейс командного рядка. Комутатори серії 3750 забезпечують швидке розгортання та просте управління мережевою інфраструктурою, з високим рівнем доступності, керованості та безпеки. Є можливість підключення резервного джерела постійного струму. Сімейство комутаторів призначене для монтажу в стійку, висотою 1U.

Рисунок 2.5 – Маршрутизатор Cisco 2911 C2911-VSEC-SRE/K9

Маршрутизатори Cisco 2911 оснащені модульною архітектурою, яка дозволяє виконувати завдання з урахуванням зростаючих потреб. Оснащений надійним захистом від кібератак, шкідливого програмного забезпечення та

несанкціонованого доступу. Дозволяє контролювати споживання електроенергії. Забезпечує високу гнучкість мережі.

Таблиця 2.2 - Технічні характеристики Cisco Catalyst WS-C3750-24FS-S

| Загальні характеристики | |
|---|---|
| Тип пристрою | перемикач |
| Можливість встановлення на підставку | є |
| Розмір оперативної пам'яті | 128 МБ |
| Розмір флеш-пам'яті | 16 МБ |
| Локальна мережа | |
| Кількість портів комутатора | 24 порти Ethernet 10/100 Мбіт/с |
| Кількість слотів SFP | 2 |
| Підтримка операцій стеку | є |
| Внутрішня пропускна здатність | 32 Гбіт/с |
| Розмір таблиці MAC-адрес | 12288 |
| Дошка | |
| Консольний порт | є |
| Веб-інтерфейс | є |
| Підтримка Telnet | є |
| Підтримка SNMP | є |
| Тип управління | рівень 3 |
| Маршрутизатор | |
| Статична маршрутизація | є |
| Динамічна маршрутизація протоколи | RIP версії 1, RIP версії 2, OSPF |
| Керування інтернет-групами протоколи | IGMP версії 1, IGMP версії 2, IGMP версії 3 |
| Додаткові | |
| Підтримка IPv6 | є |
| Підтримка стандартів | Автоматичне виявлення MDI/MDIX – живлення через Ethernet, IEEE<br>Стандарт 802.1 P (переважна категорія), стандарт IEEE 802.1 Q (LS), IEEE<br>Стандарт 802.1 d (жестяна деревина), стандарт IEEE 802.1 S (багатошарові жестяні деревини) |
| Розміри (ШхВхГ) | 445 x 44 x 301 мм |
| Вага | 5,1 кг |
| Додаткова інформація | 24 порти 100BASE-FX |

Модель C2911-VSEC-SRE/K9 підтримує інтерфейси xDSL, GR, T1/E1, T3/E3. Використовується на всіх пристроях Cisco IOS, деякі з яких можна активувати за потреби.

Таблиця 2.3 – Маршрутизатор Cisco 2911 C2911-VSEC-SRE/K9

| Тип пристрою | Маршрутизатор |
|---|---|
| Тип корпусу | Настільний модульний 2U |
| Технологія підключення | Дротове |
| Протокол каналу передачі даних | Локальні мережі, швидкі локальні мережі, локальні гігабітні мережі |
| Мережевий/транспортний протокол | ПРОТОКОЛ L2TP, IPSec та ПРОТОКОЛ PPPoE, типи PPPoA |
| Протокол маршрутизації | Згідно з протоколом OSPF, це BGP з igmpv3, EIGRP з, DVMRP, Pim-cm, де GRE, Pim-CSM, статична маршрутизація IPv4, BGP зі статичною маршрутизацією IPv6, eigrp s, DVMRP, Pim-cm |
| Протокол дистанційного керування | SNMP, RMON |
| Алгоритм шифрування | Використання SSL |
| Особливості | Захист брандмауера, комутація 3-го рівня, комутація 2-го рівня, підтримка VPN, підтримка MPLS, а також підтримка системного журналу, фільтрація контенту, підтримка IPv6, зважена справедлива черга (CBWFQ), зважене раннє виявлення випадкових помилок (WRED), список контролю доступу (ACL), підтримка якості обслуговування (QoS), динамічна багатоточкова VPN мережа (DMVPN) |
| Відповідність стандартам | IEEE 802.1Q, IEEE 802.1ah, IEEE 802.1ag, CISPR 22 Клас A, CISPR 24, EN55024, EN55022 Клас A, EN50082-1, CAN/CSA-E60065-00, ICES-003 Клас A, CS-03, AS/NZS 3548, FCC CFR47 Частина 15, EN300-386, UL 60950-1, IEK 60950-1, EN 60950-1 |
| Оперативна пам'ять | 512 МБ (встановлено) / 2 ГБ (макс.) |
| Флеш-пам'ять | 256 МБ (встановлено) / 8 ГБ (максимум) |
| Індикатор стану | Комунікаційна активність, влада |
| Система зв'язку | |
| Тип | 1 x голосовий/факсимільний модуль |
| Кількість цифрових портів | 16 |
| Протоколи та функції | MCE G.168 |

продовження таблиці 2.3

| | |
|---|---|
| IP-телефонія | |
| голосовий кодек | G.711, G.722, G.723.1, G.728, G.729, G.729a, G.729ab, G.726 |
| Розгорнути / Додати | |
| Міжфазні межі | 3 x 10Base-T/100Base-TX/1000Base - T-RJ-45 Керування: 1X консольний RJ-45 Керування: 1X консольний mini-USB типу B Серія: 1x Sub-RJ-45 USB: 2 x 4 З'єднання USB типу A |
| Слоти розширення | 4 (всього) / 4 (безкоштовно) x EHWIC 2 (всього) / 1 (безкоштовно) x PVDM 3 (всього) / 1 (безкоштовно) x CompactFlash 2 (всього) / 1 (безкоштовно) x слот розширення |
| Сила | |
| Пристрій живлення | Внутрішнє джерело живлення |
| Необхідна напруга | Змінний струм 120/230 В (47 - 63 Гц) |
| Барвистий | |
| Для монтажу на стовпі З набором | Вбудований |
| Вимоги до програмного забезпечення/системи | |
| Включене програмне забезпечення забезпечити | Унікальні комунікації Cisco IOS, Безпека Cisco IOS |
| Розміри та вага | |
| Приблизна ширина | 17,2 дюйма |
| Приблизна глибина | 12 дюймів |
| Приблизна висота | 3,5 дюйма |
| Параметри навколишнього середовища | |
| Мінімальна робоча температура | 32 |
| Максимальна робота температура | 104 |
| Робоча вологість | 5 - 85% |

Рисунок 2.6 – Точка доступу Cisco Aironet серії 1700

Cisco Aironet серії 1700 – це економічно ефективна точка доступу, що підтримує найновішу бездротову технологію 802.11ac, призначена для розгортання в мережах малого та середнього бізнесу. Точки доступу Aironet серії 1700 відповідають зростаючим вимогам бездротових мереж, забезпечуючи чудову продуктивність в одній точці доступу 802.11n та базові функції управління для бездротових мереж з хорошими радіочастотними характеристиками. Точки доступу серії 1700 підтримують можливості стандарту 802.11ac Wave 1, включаючи розрахункову швидкість з'єднання до 868 Мбіт/с.

Збільшуючи пропускну здатність, ми можемо запобігти постійним вимогам до пропускної здатності, а саме:

– кілька бездротових клієнтів в одній мережі;

– зростання кількості мультимедійних програм, що збільшують навантаження на пропускну здатність;

– збільшення використання різних бездротових пристроїв мобільними працівниками.

Переваги та функції. Побудовані на базі технології RF Excellence, що використовується в точках доступу Cisco Aironet, точки доступу серії 1700 побудовані на спеціалізованому, інноваційному наборі мікросхем з найкращою в своєму класі радіочастотною архітектурою. Точка доступу 1700 є компонентом флагманської серії точок доступу.

Ці пристрої є частиною лінійки невеликих продуктів Cisco, призначених для забезпечення бездротового зв'язку в корпоративних мережах. Точки доступу серії 1700 підтримують першу хвилю стандарту 802.11ac, використовуючи 3x7 MIMO та два просторові потоки, що забезпечує конструктивну швидкість з'єднання до 867 Мбіт/с.

Ці рішення реалізують кілька розширених функцій: превентивний захист від радіоперешкод CleanAir Express, оптимізований роумінг, корекцію MIMO.

Пристрої мають елегантний зовнішній вигляд, оснащені вбудованими антенами. Точки доступу Cisco Aironet 1700 можна встановити або вбудовани в підвісну стелю, а також працювати незалежно або з бездротовим контролером.

### 2.2.5 Схема мережі технологічної компанії Playtech

Будівля центрального офісу технологічної компанії Playtech складається з 3 поверхів. На першому поверсі є 19 настільних комп'ютерів. На другому поверсі є 21 настільний комп'ютер. На третьому поверсі є 22 настільні комп'ютери. На кожному робочому місці встановлено телефони. Всі кабелі прокладаються в кабель-каналах на стелі кожного поверху.

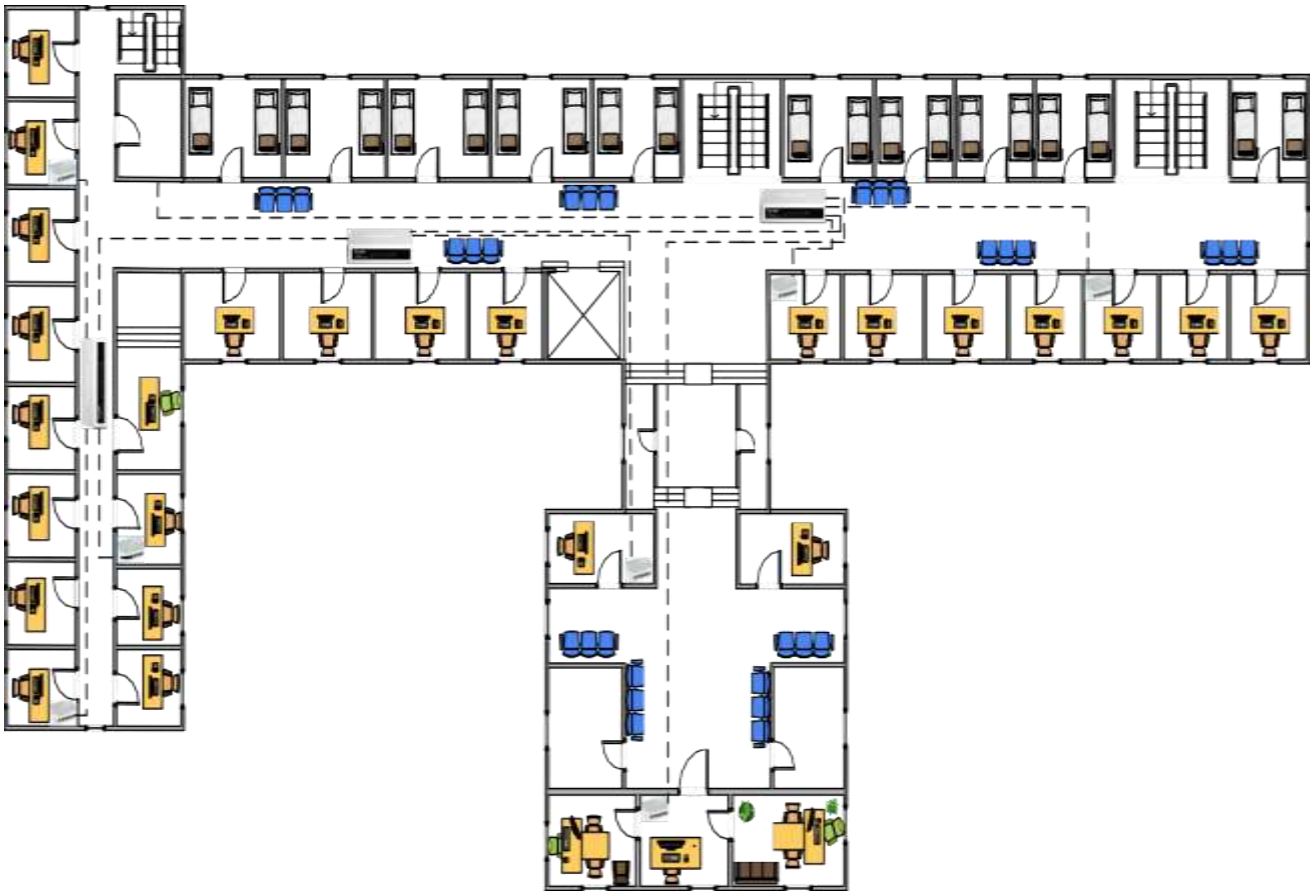

Рисунок 2.7 – Схема мережі технологічної компанії Playtech

Кабель прокладено за стандартом UTP категорії 5, що відповідає міжнародному стандарту. Цей стандарт передбачає наявність чотирьох пар мідних

кабелів, два з яких здатні передавати дані зі швидкістю 100 мегабіт за секунду. Решта пар зарезервовані для інших завдань CSP.

У цій схемі CCS побудована за топологією "шина". У ній усі елементи мережі з'єднані один з одним послідовно у вигляді ланцюга. Ця структура наразі неактуальна, оскільки мережа не є відмово-стійкою. Отже, якщо один мережевий елемент у ланцюжку вийде з ладу, користувачі, що знаходяться за цим елементом, не зможуть отримати доступ до мережі.

Організація робочого місця. Кінці кабелю складаються зі стандартних розеток RJ 45 (восьми-контактний роз'єм для підключення комп'ютерів та телефонів до мережі). Блок розетки є останнім

Кабельний канал, де встановлюються силові дроти та елементи електрообладнання для підключення користувача, розташований у кабель-каналі, встановленому вздовж стіни. Підключення користувацьких терміналів здійснюється за допомогою стандартних патч-кордів RJ 45.

### 2.2.6 Оператор послуг для корпоративних мереж

Будівля центрального офісу технологічної компанії Playtech – це заклад, який потребує мобільності та має корпоративні мережі. Мережу мають обслуговувати троє мережевих інженерів. Оператор мережі технічного обслуговування повинен надавати якісне обслуговування корпоративній мережі. Оператор повинен контролювати безперебійну роботу мережі, запобігаючи затримкам у мережі, регулярно оновлювати програмне забезпечення активного пристрою, негайно усувати проблему у разі виходу пристрою з ладу та замінювати пристрій за необхідності. Постачальником обладнання для проектування та обслуговування планованої мережі обрно компанію Vodafone.

Vodafon» – торгова марка, яка надає високошвидкісний мобільний та фіксований інтернет, дротовий та бездротовий зв'язок, а також послуги IP-телефонії.

«Vodafone» створює корпоративну мережу, яка відповідає потребам та важливим завданням організації. Завдяки власній мережі магістральних каналів, компанія отримує надійний та високошвидкісний сервіс.

Обрана компанія пропонує повний спектр послуг зі створення та обслуговування корпоративних інформаційних мережевих інфраструктур. Для найефективнішого виконання поставлених нами завдань впроваджуються високоінтелектуальні сучасні рішення.

Спеціалізовані напрямки компанії включають: телекомунікаційне обладнання, монтаж та налаштування, постачання обладнання для відеоконференцій, обладнання для інформаційної безпеки, надання мережевих рішень та технічних послуг корпоративним та державним клієнтам, а також приватним підприємствам.

Vodafone обрано в якості інтернет-провайдера для технологічної компанії Playtech. Я проаналізую інформацію про провайдерів і визначу, чи відповідає Vodafone вимогам наших мереж. Вибір провайдера доступу до Інтернету для корпоративної системи.

Інтернет-провайдер − це компанія або організація, яка надає послуги доступу до Інтернету, а також усі додаткові операції. Це включає сам інтернет, дисковий простір на сервері тощо. Зараз цей список включає майже весь доступ до інтернет-телебачення та телефонії.

Інтернет-провайдерів можна розділити на дві групи – первинні провайдери та вторинні провайдери. Перша − це магістраль, тобто вона має власну інтернет-мережу або магістраль. Друга група орендує канали у провайдерів та роздає їх

клієнтам. Звичайно, набагато вигідніше включати послуги постачальників першого рівня.

Щоб скористатися можливостями інтернет-провайдера, необхідно отримати доступ до одного з його серверів, який організовує використання мережевого каналу зв'язку.

Користувачів Інтернету дуже багато. Значно менше компаній пропонують доступ до Інтернету. Таким чином, надається лише частина пропускної здатності каналу зв'язку інтернет-провайдера. Яка саме частина залежить від типу мережевого підключення, а також від тарифного плану.

Вибір інтернет-провайдера – це відповідальний та важливий процес. Адже від типу інтернет-провайдера залежить ефективність та якість обраних послуг. Вибір правильного постачальника дуже важливий, оскільки це дозволяє користувачеві досягти оптимальних умов експлуатації, заощадити гроші та час. Щодня з'являються нові й нові сервіси, і всі вони хочуть отримати доступ до Інтернету.

Розглянемо взаємодію комп'ютера і сервера інтернет-провайдера. Для цього потрібно організувати постійне з'єднання між вашим комп'ютером та сервером інтернет-провайдера. Іншими словами, скористатися послугами провайдера. За допомогою спеціального програмного забезпечення надсилається запит зі свого комп'ютера на сервер віддаленого провайдера для отримання інформації.


Рисунок 2.8 – Структурна схема інтернет-провайдера

Сервер, встановлений у Всесвітній павутині, як показано вище, надає можливість отримувати та передавати інформацію, отриману від сервера постачальника інтернет-послуг, та надсилати її на сервер нашого постачальника інтернет-послуг. Інтернет-провайдер надсилає результат на наш комп'ютер.

Після виконання вищезазначених дій отримується відповідь на запит, надісланий на комп'ютер користувача, тобто з'являється попередження про те, що з різних причин потрібна веб-сторінка або потрібний сервер чи інформація не можуть бути знайдені в Інтернеті. Інтернет складний, але простий у використанні.

Vodafone пропонує послугу, яка дозволяє об'єднати всі офіси організацій в єдину корпоративну мережу, що відповідає всім вимогам установи. При організації корпоративної мережі територіальна віддаленість офісів перестає бути проблемою, тому сьогодні корпоративна мережа є важливою складовою успішного бізнесу. Створення єдиної інфраструктури передачі даних значно спростить взаємодію співробітників всередині компанії, а також відкриє доступ до більш інноваційних бізнес-технологій, включаючи хмарні рішення.

Переваги корпоративних мереж Vodafone:

- інтеграція територіально розрізнених офісів в єдину корпоративну мережу;

- високий рівень пропускної здатності мережі забезпечує якісну роботу бізнес-додатків, надійну передачу даних, голосу та відео;

- безперервна робота та відмовостійкість мережі завдяки резервуванню власних магістральних каналів та резервного обладнання;

- безпечний доступ до корпоративної мережі для віддалених співробітників;

- протяжність основної мережі через Україну становить понад 8 000 км.

Як показано на рис. 2.2, супутниковий зв'язок та послуги віртуальної локальної мережі (VP LAN) призначені для окремих осіб та невеликих організацій. Вони не можуть виконати мої проектні запити.

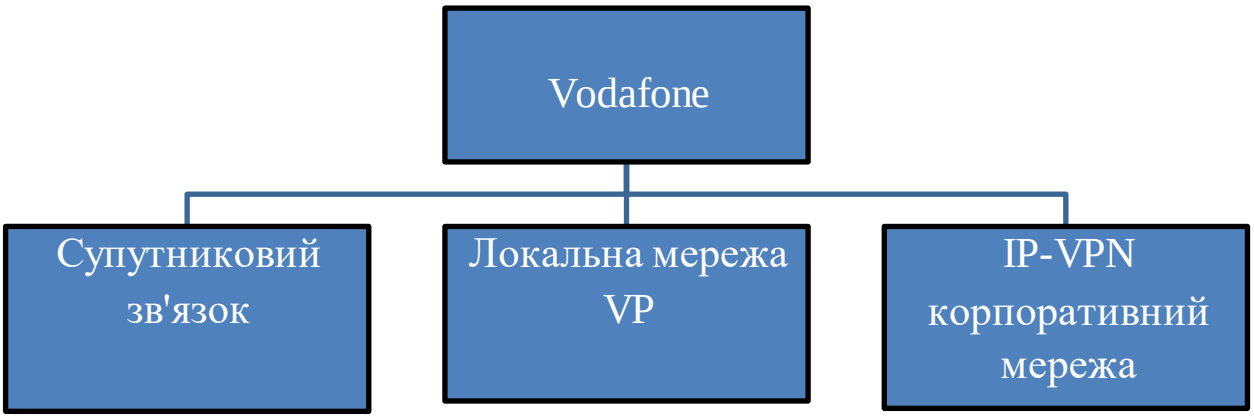


Рисунок 2.9 – Послуги доступу до Інтернету від Vodafone

За допомогою Vodafone можна організувати надійну віртуальну корпоративну мережу для об'єднання всіх офісів в єдину мережу та забезпечення безперебійної роботи, надаючи високоякісну технічну підтримку 24/7.

Vodafone має магістральну волоконна-оптичну мережу протяжністю понад 8 000 км, яка охоплює всі обласні центри та міста республіканського значення по всій Україні.

Безпека даних гарантована, оскільки трафік ізольований від трафіку інших клієнтів. Vodafone забезпечує високу надійність завдяки подвійному резервуванню магістральних каналів.

Компанія постійно вдосконалює свою мережу, щоб відповідати всім вимогам. Їхні магістральні мережі мають високу пропускну здатність та масштабованість. Сервіс забезпечує гнучкість у підключенні до корпоративної мережі, використовуючи будь-які з доступних на даний момент клієнтських портів та протоколів.

# 3 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ТЕХНОЛОГІЧНОЇ КОМПАНІЇ PLAYTECH

## 3.1 Розрахунок схеми адресації корпоративної мережі комп'ютерної системи технологічної компанії Playtech

Комп'ютерна система технологічної компанії Playtech розвивалися органічно, шляхом збільшення потужності, придбання або зміни в управлінні бізнес-операціями. Щоб забезпечити безперебійну трансформацію від початку до кінця та використати можливості сучасних мережевих технологій, Технологічна компанія прагне модернізувати свою існуючу мережеву враховуючи більше суворіші вимоги з мережевої безпеки, що спонукало компанію Playtech встановити нові платформи для усунення прогалин у безпеці та можливих вразливостей.

Згідно розробленій загальній архітектурі мережі підприємства (рис. 2.8) кількість вузлів в підмережах для корпоративної мережі комп'ютерної системи технологічної компанії Playtech, визначено табл. 3.1.

Таблиця 3.1 – Кількість вузлів в підмережах

| LAN1 | LAN2 | LAN3 | LAN4 | LAN5 |
|---|---|---|---|---|
| 72 | 9; | 76 | 103 | 91 |

Підмережі - це поділ великої мережі на інші, менші за розміром, але логічні за своєю природою, або, можна сказати, на менші підмережі. Це робиться за допомогою більш специфічної маски підмережі, таким чином фактично «запозичуючи» деякі біти з хост-частини, щоб створити більше ідентифікаторів мережі. VLSM у мережах або маска підмережі змінної довжини – це метод, що використовується в проектуванні IP-мереж для створення підмереж з різними масками підмережі. Маска підмережі – це 32-бітна послідовність одиниць та нулів, яка визначає, яка кількість бітів IP-адреси використовується для ідентифікації префіксу мережі та ідентифікатора хоста. Маска підмережі 255.255.255.0 означає,

що основні 24 біти IP-адреси відповідають за ідентифікацію префіксу мережі, а останні вісім бітів використовуються для ідентифікації ідентифікатора хоста.

У традиційній схемі розподілу на підмережі до всіх підмереж застосовується фіксована маска підмережі, що може призвести до неефективного використання IP-адрес. Наприклад, якщо мережа має дві підмережі, одну з 10 хостами, а іншу з 50 хостами, для обох підмереж, які ми обговорювали вище, використовуватиметься традиційна маска підмережі 255.255.255.0; це означає, що кожна підмережа матиме 254 доступні IP-адреси. Це може призвести до марнування IP-адрес для меншої підмережі.

Маска підмережі змінної довжини дозволяє мережевим адміністраторам створювати підмережі з різними масками підмережі для ефективного використання IP-адрес. Використовуючи наведений вище приклад, VLSM можна використовувати для призначення маски підмережі 255.255.255.128 меншій підмережі з 10 хостами, яка може пропонувати доступні IP-адреси, та маски підмережі 255.255.255.192 більшій підмережі з 50 хостами, яка може пропонувати 62 доступні IP-адреси. Щоб впровадити маскування підмережі змінної довжини (VLSM), мережеві адміністратори повинні виконати такі дії:

- визначити кількість хостів, необхідних для кожної підмережі в мережі;
- обрати маску підмережі для кожної підмережі на основі кількості хостів;
- призначити IP-адреси кожній підмережі та хосту на основі вибраної маски підмережі;
- налаштувати протоколи маршрутизації, що підтримують VLSM, такі як RIP версії 2, OSPF, EIGRP або BGP.

Протокол OSPF (Open Shortest Path First): це один з найпоширеніших протоколів, який може працювати адаптивна. OSPF повністю підтримує VLSM, завдяки чому він є одним з найпопулярніших у складних динамічних мережах.

Протокол граничного шлюзу (BGP): це протокол маршрутизації за замовчуванням, який використовується для з'єднання різноманітних мереж, наприклад, мережі організації з інтернет-провайдером (ISP). Він також має можливість працювати з VLSM.

Протокол маршрутизації (RIP) : це старіший протокол, але загалом він підтримує VLSM. RIP відносно легко налаштувати порівняно з іншими варіантами, що означає, що він корисний для менших мереж.

Протокол розширеної маршрутизації внутрішнього шлюзу (EIGRP): це власний протокол Cisco, відомий здебільшого простим процесом налаштування.

Після проведеного розрахунку, з’ясовна, що отримана мережа 10.23.0.0/22 може мати максимальну кількість хостів 1022, згідно табл. 3.1 для підмереж LAN1…LAN5 потрібно 72 + 9 + 76 + 103 + 91 = 351хостів. Розподіл підмереж LAN1…LAN5 з маски змінної довжини наведено в табл. 3.2.

Проведемо розрахунок адресації для каналів маршрутизаторами, застосовуючи блок адрес 10.0.1.0/24.

Спираючись на аналіз максимальної кількості для вузлів в підмережі WAN, яка дорівнює. 2, можна застосувати блок адрес 10.0.1.0/30.

Розрахунок підмереж між маршрутизаторами наведено на рис. 3.2.

Розподілу підмереж WAN1…WAN5 представлено в табл. 3.4.

Мережа 10.0.1.0/30 має 2 хоста, для WAN підмережам потрібно 10 хостів.

Адресація в підмережі VLAN з застосуванням заданого блоку адрес 10.23.0.0/25, для 4 підмереж WLAN20, WLAN30, WLAN40 та WLAN50 представлена представлено в табл. 3.4.

Для мережа 10.23.0.0/25 є обмеження у 126 хостів, для WLAN підмереж але потрібно всього 103 хости.

Схема адресації пристроїв мережі наведена в табл. 3.5.

Таблиця 3.2 – Розподіл адресів для підмереж LAN1…LAN5 комп'ютерної системи Playtech

| Name | Hosts Needed | Hosts Available | Unused Hosts | Network Address | Slash | Mask | Usable Range | Broadcast | Wildcard |
|---|---|---|---|---|---|---|---|---|---|
| LAN1 | 68 | 126 | 58 | 10.23.1.0 | /25 | 255.255.255.128 | 10.23.1.1 - 10.23.1.126 | 10.23.1.127 | 0.0.0.127 |
| LAN2 | 15 | 30 | 15 | 10.23.2.0 | /27 | 255.255.255.224 | 10.23.2.1 - 10.23.2.30 | 10.23.2.31 | 0.0.0.31 |
| LAN3 | 65 | 126 | 61 | 10.23.1.128 | /25 | 255.255.255.128 | 10.23.1.129 - 10.23.1.254 | 10.23.1.255 | 0.0.0.127 |
| LAN4 | 99 | 126 | 27 | 10.23.0.0 | /25 | 255.255.255.128 | 10.23.0.1 - 10.23.0.126 | 10.23.0.127 | 0.0.0.127 |
| LAN5 | 88 | 126 | 38 | 10.23.0.128 | /25 | 255.255.255.128 | 10.23.0.129 - 10.23.0.254 | 10.23.0.255 | 0.0.0.127 |

Таблиця 3.3 – Розподіл адресів для підмереж WAN1…WAN5 комп'ютерної системи Playtech

| Name | Hosts Needed | Hosts Available | Unused Hosts | Network Address | Slash | Mask | Usable Range | Broadcast | Wildcard |
|---|---|---|---|---|---|---|---|---|---|
| WAN1 | 2 | 2 | 0 | 10.0.1.0 | /30 | 255.255.255.252 | 10.0.1.1 - 10.0.1.2 | 10.0.1.3 | 0.0.0.3 |
| WAN2 | 2 | 2 | 0 | 10.0.1.4 | /30 | 255.255.255.252 | 10.0.1.5 - 10.0.1.6 | 10.0.1.7 | 0.0.0.3 |
| WAN3 | 2 | 2 | 0 | 10.0.1.8 | /30 | 255.255.255.252 | 10.0.1.9 - 10.0.1.10 | 10.0.1.11 | 0.0.0.3 |
| WAN4 | 2 | 2 | 0 | 10.0.1.12 | /30 | 255.255.255.252 | 10.0.1.13 - 10.0.1.14 | 10.0.1.15 | 0.0.0.3 |
| WAN5 | 2 | 2 | 0 | 10.0.1.16 | /30 | 255.255.255.252 | 10.0.1.17 - 10.0.1.18 | 10.0.1.19 | 0.0.0.3 |
| WAN6 | 2 | 2 | 0 | 10.0.1.20 | /30 | 255.255.255.252 | 10.0.1.21 - 10.0.1.22 | 10.0.1.23 | 0.0.0.3 |

Таблиця 3.4 – Схема адресації підмережі мережі VLAN комп'ютерної системи Playtech

| Name | Hosts Needed | Hosts Available | Unused Hosts | Network Address | Slash | Mask | Usable Range | Broadcast |
|---|---|---|---|---|---|---|---|---|
| VLAN50 | 29 | 30 | 1 | 10.23.0.0 | /27 | 255.255.255.224 | 10.23.0.1 - 10.23.0.30 | 10.23.0.31 |
| VLAN60 | 28 | 30 | 2 | 10.23.0.32 | /27 | 255.255.255.224 | 10.23.0.33 - 10.23.0.62 | 10.23.0.63 |
| VLAN40 | 27 | 30 | 3 | 10.23.0.64 | /27 | 255.255.255.224 | 10.23.0.65 - 10.23.0.94 | 10.23.0.95 |
| VLAN50 | 25 | 30 | 5 | 10.23.0.96 | /27 | 255.255.255.224 | 10.23.0.97 - 10.23.0.126 | 10.23.0.127 |

Таблиця 3.5 – Схема адресації підмережі мережі VLAN комп'ютерної системи Playtech

| Name | Hosts Needed | Hosts Available | Unused Hosts | Network Address | Slash | Mask | Usable Range | Broadcast |
|---|---|---|---|---|---|---|---|---|
| IPS | 2 | 2 | 0 | 209.165.202.0 | /30 | 255.255.255.252 | 209.165.202.1 - 209.165.202.2 | 209.165.202.3 |
| Remout1 | 10 | 14 | 4 | 209.165.201.0 | /28 | 255.255.255.240 | 209.165.201.1 - 209.165.201.14 | Remout1 |
| Remout2 | 6 | 6 | 0 | 209.165.201.16 | /29 | 255.255.255.248 | 209.165.201.17 - 209.165.201.22 | 209.165.201.23 |

Таблиця 3.6 – Схема адресації пристроїв мережі комп'ютерної системи Playtech

| Ім'я пристрою | Інтерфейс | IP-адреса | Маска | Шлюз |
|---|---|---|---|---|
| Маршрутизатори | | | | |
| R1_Baskin | Fa0/0 | 10.23.0.128 | /25 | – |
| R1_Baskin | Fa0/1 | 10.23.1.0 | /25 | – |
| R1_Baskin | Se0/1/1 | 10.0.1.21 | /30 | – |
| R2_Baskin | Se0/3/0 | 10.0.1.22 | /30 | – |
| R2_Baskin | Se0/1/1 | 10.0.1.6 | /30 | – |
| R2_Baskin | Se0/1/0 | 10.0.1.18 | /30 | – |
| R3_Baskin | Se0/3/0 | 10.0.1.10 | /30 | – |
| R3_Baskin | Se0/1/1 | 10.0.1.1 | /30 | – |
| R3_Baskin | Se0/1/0 | 10.0.1.6 | /30 | – |
| R3_Baskin | Fa0/0 | 10.23.2.1 | /25 | – |
| Router_IPS | Se0/3/1 | 10.0.1.10 | /30 | – |
| Router_IPS | Se0/1/1 | 10.0.1.17 | /30 | – |
| Router_IPS | Se0/3/0 | 10.0.1.13 | /30 | – |
| Router_IPS | Se0/1/1 | 209.165.202.1 | /30 | – |
| R5_Baskin | Se0/3/1 | 10.0.1.14 | /30 | – |
| R5_Baskin | Se0/1/0 | 10.0.1.12 | /30 | – |
| R5_Baskin | Fa0/0 | 10.23.1.29 | /25 | – |
| R6_Baskin | Se0/1/0 | 64.100.13.1 | /30 | – |
| R6_Baskin | Fa0/0 | 10.23.0.1 | /25 | – |
| RIPS_Baskin | Se0/3/1 | 10.0.1.14 | /30 | – |
| RIPS_Baskin | Se0/1/0 | 209.165.202.1 | /30 | – |
| RIPS_Baskin | Fa0/0 | 255.255.255.1 | /28 | – |
| LAN1 | | | | |
| LAN_1_PC_1 | NIC | 10.23.1.1 | /25 | 10.23.1.0 |
| LAN_1_PC_2 | NIC | 10.23.1.2 | /25 | 10.23.1.0 |
| LAN_1_PC_3 | NIC | 10.23.1.3 | /25 | 10.23.1.0 |
| LAN_1_PC_4 | NIC | 10.23.1.3 | /25 | 10.23.1.0 |
| LAN2 | | | | |
| LAN_2_PC_1 | NIC | 10.23.2.1 | /27 | 10.23.2.0 |
| LAN_2_PC_2 | NIC | 10.23.2.2 | /27 | 10.23.2.0 |
| LAN_2_PC_3 | NIC | 10.23.2.3 | /27 | 10.23.2.0 |
| LAN3 | | | | |
| LAN_3_PC_1 | NIC | 10.23.1.129 | /25 | 10.23.1.128 |
| LAN_3_PC_2 | NIC | 10.23.1.130 | /25 | 10.23.2.0 |
| Server DNS LAN_3 | NIC | 10.23.1.131 | /25 | 10.23.2.0 |
| LAN4 | | | | |
| PC_VLAN_1 | NIC | 10.23.0.1 | /25 | 10.23.0.0 |
| PC_VLAN_2 | NIC | 10.23.0.2 | /25 | 10.23.0.0 |
| PC_VLAN_3 | NIC | 10.23.0.3 | /25 | 10.23.0.0 |
| PC_VLAN_4 | NIC | 10.23.0.4 | /25 | 10.23.0.0 |
| PC_VLAN_5 | NIC | 10.23.0.5 | /25 | 10.23.0.0 |
| PC_VLAN_6 | NIC | 10.23.0.6 | /25 | 10.23.0.0 |

Кінець таблиці 3.6

| | | | | |
|---|---|---|---|---|
| LAN5 | | | | |
| LAN_5_PC_1 | NIC | 10.23.0.129 | /25 | 10.23.0.128 |
| LAN_5_PC_2 | NIC | 10.23.0.130 | /25 | 10.23.0.128 |
| LAN_5_Server_HTTP | NIC | 10.23.0.131 | /25 | 10.23.0.128 |
| Provider | | | | |
| PC-PT | NIC | 209.165.201.5 | /28 | 209.165.201.0 |

Слід зазначити, що призначення IP-адрес є фундаментальною частиною конфігурації мережі. Правильне керування IP-адресами забезпечує ефективну маршрутизацію та підключення в мережі.

### 3.2 Розробка топологічної схеми корпоративної мережі

Топологічної схеми корпоративної мережі - це візуальне представлення пристроїв, з'єднань та шляхів мережі, що дозволяє уявити, як пристрої з'єднані між собою та як вони взаємодіють один з одним. Діаграми мережі зазвичай створюються для представлення одного або всіх перших трьох мережевих рівнів (фізичного, каналу передачі даних та мережевого) відповідно до моделі взаємодії відкритих систем (OSI), які разом відомі як медіа-рівні.

Топологічної схеми корпоративної мережі допомагають покращити:

Час безвідмовної роботи точна мережева документація дозволяє швидко діагностувати проблеми з мережею або проводити технічне обслуговування.

Ефективність - огляд мережі в режимі реального часу допомагає максимально використати наявні потужності та прогнозувати, коли вони закінчяться.

Продуктивність - надійні мережеві схеми дозволяють заощадити час на усунення несправностей та розгортання нового обладнання, щоб ви могли зосередитися на більш стратегічних проектах.

Розроблена топологічна схема комп'ютерної системи Playtech, представлена на рис. 3.1.

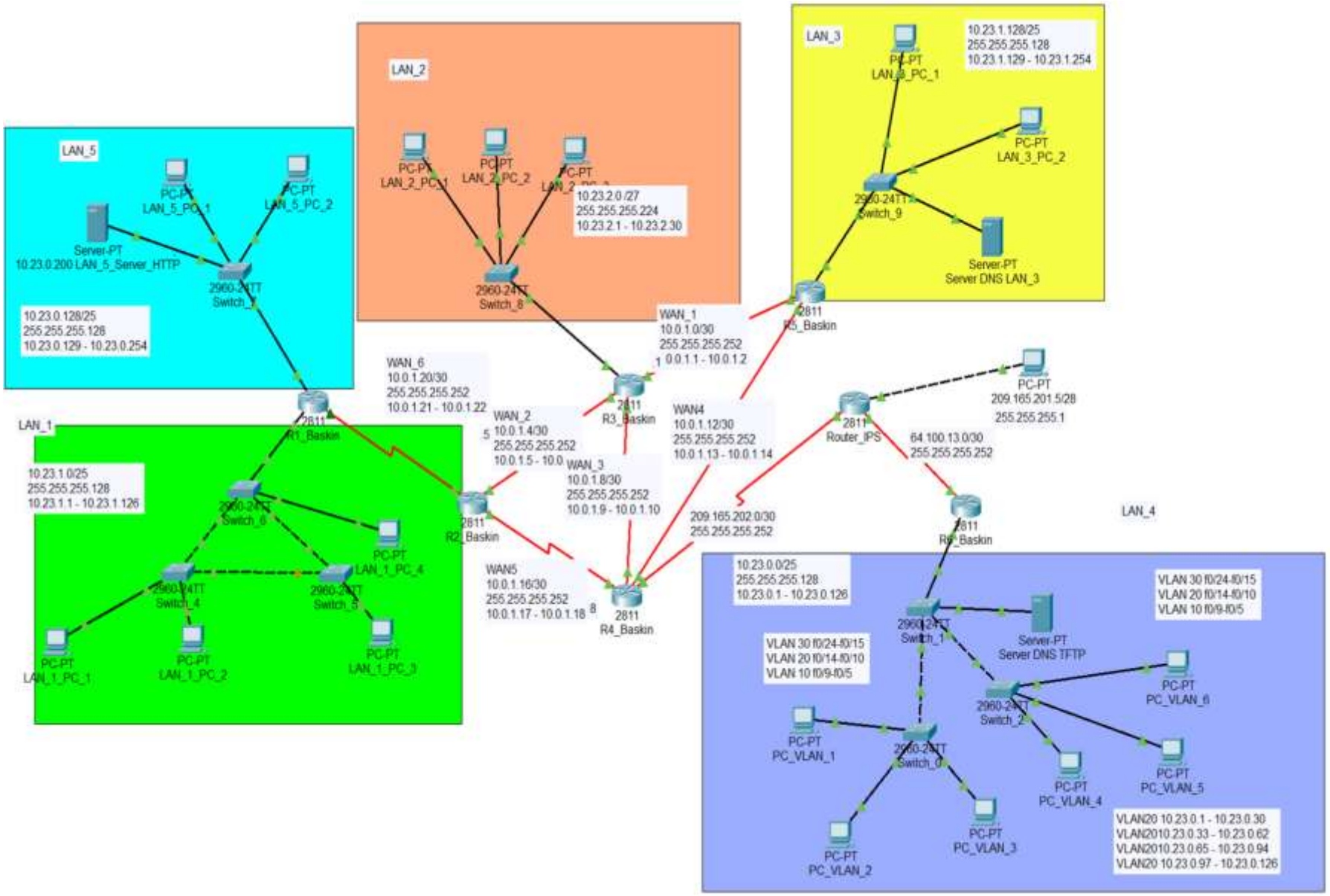


Рисунок 3.2 – Синтезована мережа комп'ютерної системи Playtech

### 3.3 Розрахунок налаштувань маршрутизації корпоративної мережі комп'ютерної системи Playtech

Корпоративна мережа комп'ютерної системи Playtech застосовує протокол динамічної маршрутизації OSPF, який є дистанційно-векторним протоколом, з номером автономної системи 23.

OSPF – це протокол маршрутизації. Два маршрутизатори, що взаємодіють один з одним за допомогою OSPF, обмінюються інформацією про відомі їм маршрути та вартість їх досягнення.

Коли багато маршрутизаторів OSPF є частиною однієї мережі, інформація про всі маршрути в мережі отримується всіма маршрутизаторами OSPF у цій мережі - технічно це називається областю.

Кожен маршрутизатор OSPF передає інформацію про маршрути та витрати, про які він чув, усім сусіднім маршрутизаторам OSPF, які називаються сусідами .

Маршрутизатори OSPF покладаються на обчислення найкоротшого шляху через мережу між собою та віддаленим маршрутизатором або мережевим пунктом призначення. Обчислення найкоротшого шляху виконується за допомогою алгоритму Дейкстри. Цей алгоритм не є унікальним для OSPF. Швидше, це математичний алгоритм, який має очевидне застосування в мережах.

Налаштування маршрутизації на роутерах корпоративної мережі комп'ютерної системи Playtech виконано на serial-інтерфейсі, згідно до технічних параметрів роутерів пропускну спроможність дорівнює значенню 128 кб/с, з метрикою 7'500 та швидкістю каналу 128'000.

```
Router_IPS(config)#interface s0/1/0
Router_IPS(config-if)#bandwidth 128
Router_IPS(config-if)# clock rate 128000
```

## 3.4 Налаштування та перевірка роботи корпоративної мережі комп’ютерної системи Playtech

### 3.4.1 Загальнбі відомості

Конфігурація мережі – це процес налаштування та керування апаратним забезпеченням, програмним забезпеченням, з’єднаннями та каналами зв’язку, що складають корпоративну мережу.

Це включає такі завдання, як налаштування маршрутизаторів і комутаторів, встановлення мережевих з'єднань на хост-машинах, встановлення та налаштування пристроїв мережевої безпеки, таких як брандмауери або системи виявлення вторгнень, а також встановлення правил маршрутизації та контролю даних в інфраструктурі корпоративної мережі. Ефективна конфігурація мережі забезпечує безперебійну, безпечну та ефективну роботу мереж з мінімальним часом простою.

Конфігурація мережі є основоположним елементом у створенні надійного IT-середовища. Правильно налаштовані мережі сприяють безперебійному зв'язку, покращують заходи безпеки та підвищують показники продуктивності. Неправильна або неоптимальна конфігурація мережі може призвести до кількох проблем, таких як:

Неправильна конфігурація мережі може призвести до вузьких місць, які спричиняють затримки та знижують загальну продуктивність мережі. Правильне планування та конфігурація можуть зменшити ці проблеми, забезпечуючи плавніший потік даних та краще використання мережевих ресурсів.

Неправильно налаштована мережа може наражати вашу організацію на різні ризики безпеки, включаючи несанкціонований доступ та витік даних. Дотримання принципів нульової довіри під час процесу налаштування може значно зменшити ці вразливості.

Неоптимальні конфігурації можуть призвести до неефективного використання мережевих ресурсів, що призводить до збільшення експлуатаційних витрат. Ефективна конфігурація мережі оптимізує розподіл ресурсів, тим самим заощаджуючи час і гроші організації.

Неадекватна конфігурація мережі може призвести до неочікуваних простоїв, що впливає як на безперервність бізнесу, так і на задоволеність клієнтів. Правильне управління конфігурацією може мінімізувати ці ризики, забезпечуючи високу доступність послуг.

Конфігурація мережі - це не просто налаштування пристроїв, а й включає низку дій, спрямованих на призначення мережевих параметрів, створення політик, спрямування потоків та встановлення елементів керування. Ось ключові типи конфігурації мережі, з якими зазвичай працюють організації:

Політики визначають, як має оброблятися, визначатися пріоритетність або блокуватися трафік у мережі. Впровадження точних мережевих політик є важливим для безпеки та ефективного використання ресурсів.

Це передбачає встановлення правил щодо того, як пакети даних повинні проходити через мережу. Конфігурація потоку трафіку впливає на ефективність, швидкість та надійність мережі.

Налаштування брандмауерів, систем виявлення вторгнень та інших засобів безпеки має вирішальне значення для захисту мережі від зовнішніх та внутрішніх загроз.

У віртуальній мережі потреба в ручному налаштуванні фізичних пристроїв мінімізується, оскільки вони замінюються програмним забезпеченням. Це спрощує процес внесення змін до конфігурації мережі та підвищує гнучкість.

Кожен із цих кроків та опцій налаштування служить різним цілям та використанню, а вибір конфігурації залежить від конкретних потреб користувача.

### 3.4.2 Базове налаштування конфігурації пристроїв

Процес базового налаштування конфігурації активних мережних пристроїв корпоративної мережі комп'ютерної системи Playtech включає наступні дії:

- застосування сервісу шифрування паролів;

- захист привілейованого режиму ОС, консольного порту та ліній vty;

- призначення банера MOTD;

- для віддаленого доступу до пристрою на лініях vty застосований протокол SSH;

- створено локальні облікові записи (username 123231_Baskin) з паролем admincisco123231;

- створено доменне ім'я пристрою (ip domain-name R1_Baskin);

- створено ключ RSA завдовжки 1024 біт для шифрування даних.

Нижче показано приклад для параметрів базового налаштування на роутері R1_Baskin, який містить наступні пункти:

- заборона пошуку DNS на маршрутизаторі: Router(config)#no ip domain-lookup

- задання пристрою унікального імені: Router(config)#hostname R1_Baskin;

- шифрування всіх паролей, що зберігаються у відкритому вигляді: R1_Baskin(config)#service password-encryption

- встановлення паролю на вхід до привілейованого режиму: R1_Baskin(config)#enable secret class123231;

- встановлення парою на вхід до консольної лінії: R1_Baskin(config)#line console 0, R1_Baskin(config-line)#password cisco123231

- налаштування запиту пароля при вході: R1_Baskin(config-line)#login, R1_Baskin(config-line)#exit;

- налаштуванню банера MOTD: R1_Baskin(config)#banner motd # 123231 Baskin. Enter only have key#;

- налаштування протоколу SSH, створення користувача: R1_Baskin(config)#username 123231_Baskin password admincisco;

-с творення домену: R1_Baskin(config)#ip domain-name R1_Baskin;

- створення ключа RSA для шифрування даних довжиною 1024 біт: R1_Baskin(config)#crypto key generate rsa, How many bits in the modulus [512]: 1024, % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

- налаштування лінії VTY: R1_Baskin(config)#line vty 0 4;

- встановлення необхідності введення логіну та пароля для входу лінії: R1_Baskin(config-line)#login local;

- встановлення входу на лінію тільки по протоколу SSH: R1_Baskin(config-line)#transport input ssh;

- встановлення IPv4-адрес відповідно до табл. 3.4: R1_Baskin(config)#interface g0/1, R1_Baskin (config-if)# ip address 10.22.208.1 255.255.255.0

- запуск інтерфейсу до роботи - обов'язкове увімкнення: R1_Baskin(config-if)#no shutdown.

### 3.4.3 Налаштування маршрутизаторів корпоративної мережі

Згідно технічних вимог для створення корпоративної мережі комп'ютерної системи Playtech використовується протокол динамічної маршрутизації OSPF 23. 23 - номер автономної системи, це сукупність мереж під єдиним адміністративним управлінням, що забезпечує загальну для всіх вхідних в автономну систему маршрутизаторів політику маршрутизації.

Особливості протоколу динамічної маршрутизації OSPF:

- протокол маршрутизації з відкритим стандартом;

- протокол внутрішнього шлюзу (IGP).

- працює в межах одного домену маршрутизації, такого як автономна система (AS);

- використовує концепцію під назвою «області» для оптимізації мережевого трафіку та спрощення адміністрування;

- використовує алгоритм Дейкстри для обчислення найкоротшого маршруту до кожного пункту призначення;

- працює через IP-протокол, але не використовує транспортний протокол (наприклад, TCP або UDP) для інкапсуляції своїх даних;

- інкапсулює свої дані безпосередньо в IP-пакети з номером протоколу 89;

- використовує власний механізм виявлення та виправлення помилок;

- дуже гнучкий, універсальний та масштабований;

- пропонує необмежену кількість стрибків;

- підтримує VLSM/CIDR;

- підтримує розгортання від кількох постачальників;

- мінімізує трафік оновлення маршрутизації;

Переваги протоколу динамічної маршрутизації OSPF:

- протокол відкритого стандарту. Він може працювати на більшості маршрутизаторів;

- використовує алгоритм SPF для забезпечення топології без петель;

- використовує як тригерні оновлення, так і інкрементальні оновлення для забезпечення швидкої конвергенції;

- підтримує VLSM та підсумовування маршрутів для ієрархічної структури;

- підтримує обидві версії IP-протоколу. OSPFv2 підтримує IPv4, а OSPFv3 підтримує IPv6;

- підтримує балансування навантаження з маршрутами з однаковою вартістю для одного й того ж пункту призначення;

- підтримує мережі будь-якого розміру.

Недоліки протоколу динамічної маршрутизації OSPF:

- для розрахунку найкращого маршруту для кожного пункту призначення потрібна велика кількість інформації, для зберігання цієї інформації OSPF споживає більше пам'яті, ніж інші протоколи маршрутизації;

- запускає алгоритм SPF для розрахунку найкращого маршруту, що вимагає додаткової обробки процесора;

- складно налаштувати та важко усунути неполадки, налаштувати можуть лише досвідчені мережеві адміністратори.

Для кожного маршрутизатора корпоративної мережі комп'ютерної системи Playtech виконані наступні кроки:

- оголошені безпосередньо підключені підмережі;

- відключено поширення оновлень маршрутизації на інтерфейси в локальні мережі;

- включено протокол OSPF на маршрутизаторі командою: Router_IPS(config)#router ospf 23;

- задано ідентифікатор маршрутизатора (router ID) – унікальне 32-бітове число, що однозначно ідентифікує маршрутизатор в межах корпоративної мережі: Router_IPS(config)#router-id 17.17.17.17;

- для протоколу OSPF об'явлені мережі, які підключені до маршрутизатора: Router_IPS(config-router)#network 10.68.0.0 0.0.0.127 area 0, Router_IPS(config-router)#network 10.0.10.8 0.0.0.3 area 0, area 0 – зона (area) – сукупність мереж і маршрутизаторів, що мають один і той же ідентифікатор зони.

На Router_IPS додатково налаштовано маршрут за замовчуванням в інтернет (ISP) і поширене його через оновлення маршрутизації OSPF.

Далі виконана перевірка таблиць маршрутизацій на маршрутизаторах, а саме, що кожний маршрутизатор окрім безпосередньо підключених мереж з символом «С» має ще відомості про всі віддалені мережі, отримана по протоколу OSPF з символом «О», також проконтрольовано що є записи маршруту за замовчуванням, який складається з восьми нулів, для підключення до маршрутизатора IPS.

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 15 subnets, 5 masks
O       10.0.10.0/30 [110/15064] via 10.0.10.10, 00:03:06, Serial0/0/1
O       10.0.10.4/30 [110/7564] via 10.0.10.10, 00:03:16, Serial0/0/1
C       10.0.10.8/30 is directly connected, Serial0/0/1
L       10.0.10.9/32 is directly connected, Serial0/0/1
C       10.68.0.0/27 is directly connected, GigabitEthernet0/1.99
L       10.68.0.1/32 is directly connected, GigabitEthernet0/1.99
C       10.68.0.32/27 is directly connected, GigabitEthernet0/1.20
L       10.68.0.33/32 is directly connected, GigabitEthernet0/1.20
C       10.68.0.64/27 is directly connected, GigabitEthernet0/1.30
L       10.68.0.65/32 is directly connected, GigabitEthernet0/1.30
C       10.68.0.96/27 is directly connected, GigabitEthernet0/1.40
L       10.68.0.97/32 is directly connected, GigabitEthernet0/1.40
O       10.68.0.128/25 [110/15065] via 10.0.10.10, 00:03:06, Serial0/0/1
O       10.68.1.0/26 [110/65] via 10.0.10.10, 00:03:16, Serial0/0/1
O       10.68.1.64/27 [110/7565] via 10.0.10.10, 00:03:06, Serial0/0/1
     209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/7564] via 10.0.10.10, 00:03:16, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 3.2– Таблиця маршрутизації на Router_IPS

Виходячи з адресації маршрутизаторів корпоративної мережі комп’ютерної системи Playtech видно, що всі наявні мережі визначені у відповідних таблицях, тому топологія корпоративної мережі комп’ютерної системи Playtech повністю сходиться з завдання до проектування. Таким чином з будь-якої підмережі можна відправляти повідомлення до іншої, та це повідомлення буде обов'язково прийняте.

### 3.4.4 Налаштування роботи Інтернет

Щоб отримати доступ до параметрів Інтернету в корпоративній мережі комп'ютерної системи Playtech через маршрутизатор Cisco його слід налаштувати - для знадобиться доступ до його веб-інтерфейсу конфігурації (GUI).

Обов'язковими параметрами налаштування Інтернету є наступне: DNS-сервери, IP-адреси, маски підмереж, а також потенційно навіть увімкнути або вимкнути такі функції, як DHCP.

Нижче наведені параметри налаштування роботи Інтернет маршрутизатора Router_IPS:

- access-list 5 permit 10.0.0.0 0.255.255.25;
- ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224;
- ip nat inside source list 5 pool Internet overload;
- ip nat inside source static 10.23.0.200 209.165.200.5;
- interface s0/1/0;
- ip nat inside;
- inter s0/1/1;
- ip nat in;
- int s0/3/0;
- ip nat inside;
- inter s0/3/1;
- ip nat outside.

NAT на прикордонному маршрутизаторі налаштовано наступним чином:

- пул адрес: з 209.165.202.1 по 209.165.202.30;
- 10.22.210.10 255.255.255.0 – адреса Server HTTP;
- номер списку доступу: 5;
- ім'я пулу: Internet.

Нижче наведено параметри налаштування NAT на маршрутизаторі Baskin_R3:

- перелік пунктів контролю доступу, що дозволяє всі адреси внутрішньої мережі: Baskin_R3(config)# access-list 5 permit 10.68.0.0 0.0.3.255

- пул для динамічного виділення інтернет адрес: Baskin_R3(config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224;

- підміна адреси внутрішньої мережі на інтернет адреси згідно з списком контролю доступу: Baskin_R3(config)#ip nat inside source list 6 pool Internet

- адреса статичного NAT для серверу HTTP: Baskin_R3(config)#i ip nat inside source static 10.68.0.149 209.165.200.5;

- призначення інтерфейсу в якості вихідного для трафіку з мережі приватних адрес: Baskin_R3(config)#interface F4/0, Baskin_R3(config-if)#ip nat outside;

- призначення інтерфейсу в якості вхідного для трафіку з мережі приватних адрес: Baskin_R3(config-if)#interface Serial2/0, Baskin_R3(config-if)#ip nat inside

Для перевірки роботи NAT отримаємо таблицю перетворювань.

| Protocol | Inside Global | Inside Local | Outside Local | Outside Global |
|---|---|---|---|---|
| icmp | 209.165.202.12:1 | 10.68.0.140:1 | 209.165.202.1:1 | 209.165.202.1:1 |
| icmp | 209.165.202.11:1 | 10.68.0.141:1 | 209.165.202.1:1 | 209.165.202.1:1 |
| icmp | 209.165.202.8:1 | 10.68.1.15:1 | 209.165.200.5:1 | 209.165.200.5:1 |
| icmp | 209.165.202.8:2 | 10.68.1.15:2 | 209.165.200.5:2 | 209.165.200.5:2 |
| icmp | 209.165.202.9:1 | 10.68.1.79:1 | 209.165.200.5:1 | 209.165.200.5:1 |
| icmp | 209.165.202.10:1 | 10.68.1.82:1 | 209.165.202.1:1 | 209.165.202.1:1 |
| --- | 209.165.200.5 | 10.68.0.149 | --- | --- |

Рисунок 3.3 – Таблиця перетворювань NAT на Baskin_R3

### 3.4.4 Перевірка роботи комп'ютерної системи

Для перевірки працездатності корпоративної мережі комп'ютерної системи Playtech проведемо процес пінгування хостів між підмережами LAN2 та LAN1.

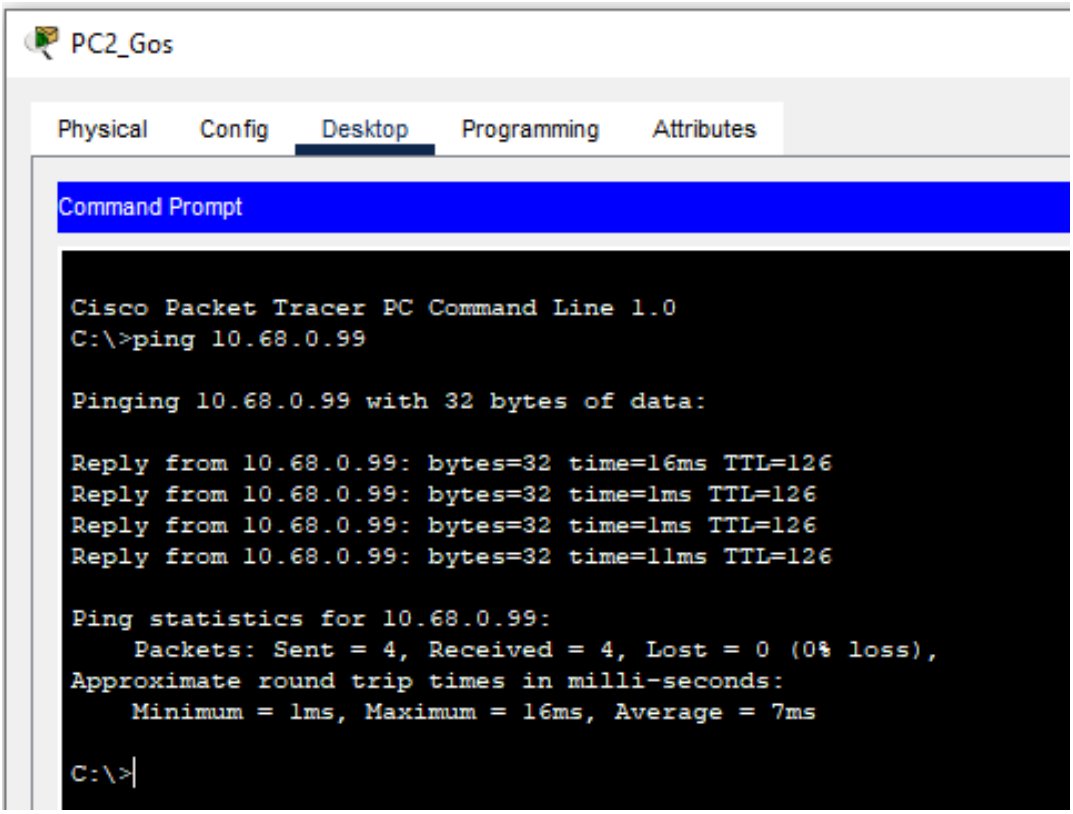


Рисунок 3.5 – Результат команди «ping» між підмережами комп'ютерної системи Playtech

Для здійснення перевірки SSH зробимо підключення з командного рядка Gl_Engineer з підмережі «LAN4» до маршрутизатора R1_Baskin від користувача 123231_Baskin з паролем admincisco123231 командою ssh –l username ip-address.

В підмережах LAN2 та LAN1 хости отримують мережні налаштування за протоколом DHCP, приклад налаштування DHCP на R2_Baskin має основні етапи (R2_Baskin(config)#interface g0/1):

- активовано протокол DHCP: R2_Baskin(config-if)#service DHCP;

- створено пул DHCP з ім'ям Organization_department: R2_Baskin(config-if)#ip dhc pool LAN1;

- вилучено з пулу перші 10 адрес: R2_Baskin(config-if)#ip dhc ex 10. 68.0.32 10. 68.0.42;

- зазначена мережа і шлюз за замовчуванням: R2_Baskin(config-if)#net 10.68.0.32 255.255.255.224, R2_Baskin(config-if)#def 10.68.0.33, R2_Baskin(config-if)#dns 10.68.10.10

| IP address | Client-ID/ Hardware address | Lease expiration | Type |
|---|---|---|---|
| 10.68.0.34 | 0002.1722.B3AD | -- | Automatic |
| 10.68.0.35 | 0007.EC39.1261 | -- | Automatic |
| 10.68.0.36 | 0001.9720.2C99 | -- | Automatic |
| 10.68.0.66 | 00E0.B016.BC25 | -- | Automatic |
| 10.68.0.67 | 0000.0C78.964D | -- | Automatic |
| 10.68.0.68 | 0060.5C72.13EA | -- | Automatic |
| 10.68.0.99 | 000C.CF94.17A9 | -- | Automatic |
| 10.68.0.98 | 00D0.BAA1.008D | -- | Automatic |
| 10.68.0.100 | 0060.7041.7427 | -- | Automatic |

Рисунок 3.4 – Таблиця призначення IP-адрес вузлам за протоколом DHCP в корпоративній мережі комп’ютерної системи Playtech

## 3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу в корпоративній мережі комп’ютерної системи Playtech

### 3.5.1 Загальні відомості

Дослідимо механіку захисту комп'ютерної інформації корпоративній мережі комп’ютерної системи Playtech від несанкціонованого використання або модифікації.

Компанія Cisco має унікальну перевагу в галузі кібербезпеки. Оскільки обладнання Cisco обробляє в середньому 715 мільярдів DNS-запитів, та стикається з більшою кількістю загроз безпеці даних, шкідливим програмним забезпеченням і кібератак, ніж будь-який інший постачальник рішень безпеки.

Захист комп'ютерної інформації в корпоративній мережі вимагає багаторівневого підходу, що охоплює фізичні, технічні та адміністративні заходи. Ключові стратегії включають впровадження надійних політик контролю

доступу, VPN, брандмауерів, антивірусного та антивірусного програмного забезпечення, регулярних оновлень програмного забезпечення та заходів запобігання втраті даних (DLP).

Можна рекомендувати основні складові інформаційної безпеки для корпоративній мережі комп'ютерної системи Playtech:

1. Навчання співробітників з кібербезпеки також має вирішальне значення. Забезпечення фізичного доступу до мережевої інфраструктури та пристроїв є фундаментальним першим кроком.

2. Технічна безпека: VPN: віртуальні приватні мережі забезпечують безпечний віддалений доступ до корпоративної мережі.

3. Брандмауери: мережеві брандмауери діють як бар'єр, фільтруючи вхідний і вихідний мережевий трафік.

4. Антивірус і захист від зловмисного програмного забезпечення: ці програмні рішення захищають від різних загроз, включаючи шкідливе програмне забезпечення та віруси.

5. Оновлення програмного забезпечення: Підтримка програмного забезпечення та операційних систем в актуальному стані має вирішальне значення для виправлення вразливостей безпеки.

6. Захист від втрати даних (DLP): системи DLP допомагають запобігти витоку конфіденційної інформації з мережі.

7. Системи виявлення та запобігання вторгнень: ці системи виявляють і потенційно блокують шкідливу мережеву активність.

8. Шифрування: шифрування даних під час зберігання та передачі захищає від несанкціонованого доступу.

9. Адміністративна безпека:

- політики контролю доступу - чітко визначені політики регулюють, хто може отримати доступ до певних ресурсів і систем;

- аудит безпеки - регулярні аудити безпеки допомагають виявити вразливості та забезпечити ефективність заходів безпеки;

- контроль доступу до мережі: ці системи контролюють доступ до мережі на основі ідентичності користувача та атрибутів пристрою;

- керування ідентифікацією та доступом: керування ідентифікаційними даними користувачів і правами доступу гарантує, що лише авторизовані особи матимуть доступ до конфіденційних систем.

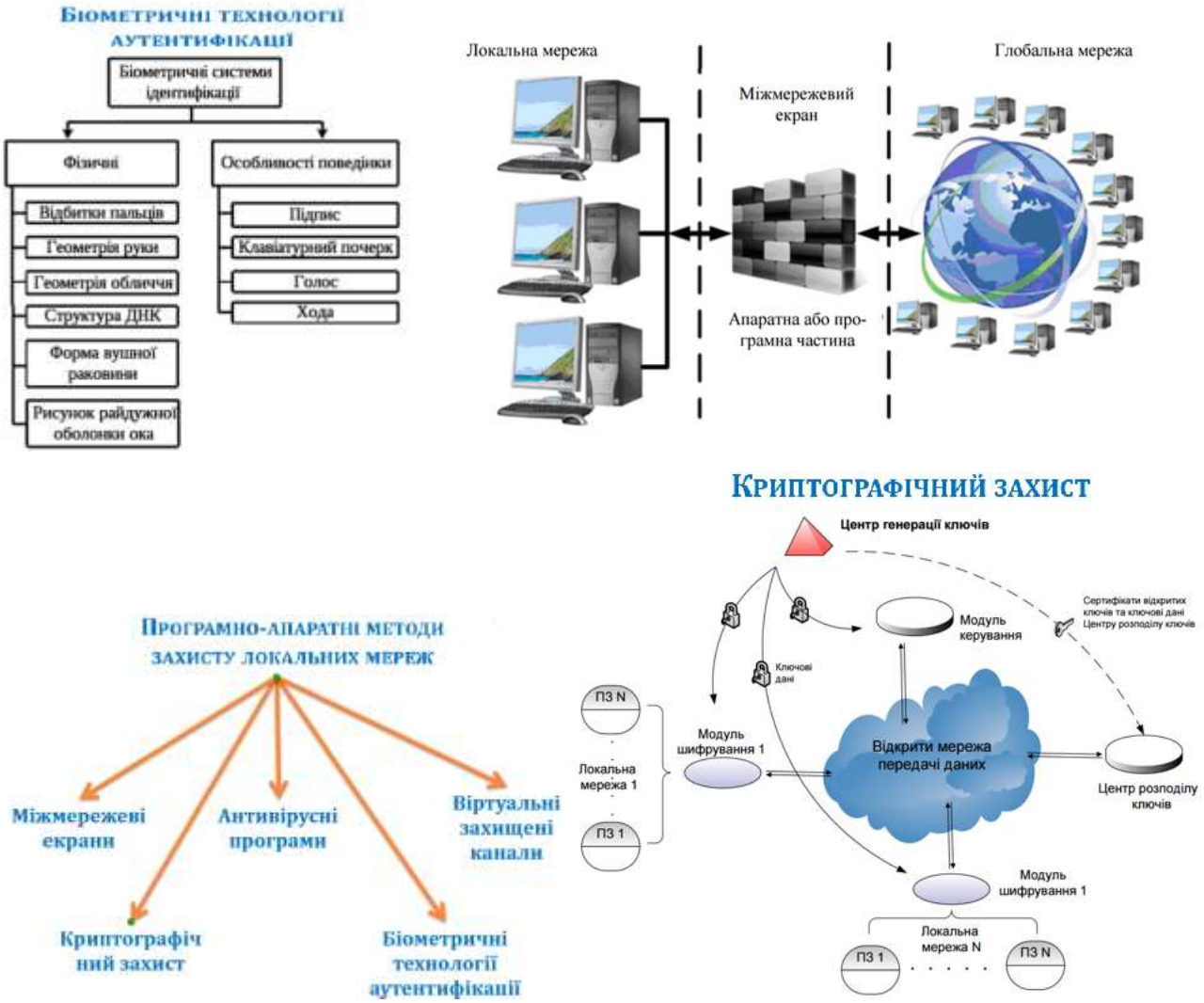


Рисунок 3.6 – Види захисту

### 3.5.2 Налаштування маршрутизаторів на підтримку служби AAA

Надання доступу невірній особі може бути фатальним для бізнесу: кіберзлочинність у всьому світі коштувала бізнесу 5,2 трильйона доларів протягом останніх п'яти років.

Тож стандартною рекомендацією безпеки для організацій є автентифікація співробітників та отримання відповідної авторизації на основі привілеїв їхніх облікових записів.

Зрештою, згенеровані журнали зберігаються для підтвердження кожної виконаної дії, що також може стати в нагоді у сценаріях усунення несправностей.

Найкращим методом для досягнення таких цілей є використання AAA. Оскільки локальний AAA погано масштабується у великих і складних корпоративних мережах, централізований AAA є кращим варіантом. Протоколи AAA, які ви можете використовувати, це RADIUS і TACACS+. Залежно від ваших вимог, ви можете використовувати один або обидва одночасно.

Автентифікація користувачів перед наданням їм доступу до мережевих ресурсів корпоративної мережі комп'ютерної системи Playtech є обов'язковою.


Рисунок 3.6 – Сервісу AAA, сервер RADIUS

Приклад налаштування сервісу AAA та серверу RADIUS для корпоративної мережі комп'ютерної системи Playtech:

- запуск служби AAA: Router_IPS(config)#aaa new-model

- налаштування методу аутентифікації з використання локальної бази користувачів: Router_IPS(config)#aaa authentication login default local

- налаштування методу аутентифікації Login на серевері RADIUS, а якщо він недоступний, то з використанням локальної бази користувачів: Router_IPS(config)#aaa authentication login Login group radius local

- застосування методу аутентифікайфії Login на консольній лінії та vty: Router_IPS(config)#line console 0, Router_IPS(config-line)#login authentication Login, Router_IPS(config)#line vty 0 4, Router_IPS(config-line)#login authentication default;

- налаштування RADIUS-серверу: Router_IPS(config)#radius-server host 10.68.10.10 auth-port 1645, Router_IPS(config)#radius-server key Radius+Baskin123.

Для доступу використовується доменне ім'я пристрою Baskin_R3 з паролем Radius+Baskin123, що був налаштований на сервері RADIUS.

На портах комутатора, де підключені сервери комп'ютерної системи Playtech, налаштовані наступні засоби безпеки:

- дозволений доступ до порту тільки одному вузлу;

- додання пристрою статично в поточну конфігурацію MAC-адреса;

- порт вимикається при порушенні системи безпеки.

### 3.5.3 Налаштування віртуальної приватної мережі VPN

В комп'ютерній системи Playtech VPN-трафік між підмережою «LAN2» (шлюз - інтерфейс роутера Baskin_R1) та підмережою «LAN3» передається (шлюзом - інтерфейс роутера Router_IPS) за допомогою VPN тунелю.

За допомогою команди show crypto ipsec sa здійснена перевірка створеного VPN тунелю передачі трафіку між підмережами.

```
interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.0.10.6

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.68.1.0/255.255.255.192/0/0)
   remote  ident (addr/mask/prot/port): (10.68.1.64/255.255.255.224/0/0)
   current_peer 10.0.10.5 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 8, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.10.6, remote crypto endpt.:10.0.10.5
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
```

Рисунок 3.7 – Перевірка стану IPSec SA на роутері Baskin_R3

# 4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ КОМП'ЮТЕРНОЇ СИСТЕМИ ТЕХНОЛОГІЧНОЇ КОМПАНІЇ PLAYTECH

## 4.1 Загальна інформація

Технологічна компанія застосовує сучасні напрямки підвищення рівня продуктивності та якості роботи. Останнім рішенням є пропозиція активного застосування Інтернет речей (IoT).

«Розумний офіс» використовує технології для підвищення продуктивності, ефективності та загального досвіду співробітників, що призводить до більш оптимізованого та ефективного робочого місця. Він інтегрує різні системи, такі як автоматизація, пристрої IoT та інструменти управління робочим місцем, щоб створити простір, який оптимізує продуктивність і використання ресурсів.

Тенденція до «розумного офісу», також відомого як адаптивне або цифрове робоче місце, базується на використанні технологій, щоб зробити фізичне робоче середовище інтелектуальним та адаптивним до потреб співробітників.

Розумні офіси поєднують у собі пристрої, підключені до Інтернету, інтелектуальні датчики, машинне навчання та покращену комунікацію для підвищення комфорту та продуктивності співробітників, одночасно зменшуючи споживання енергії будівлею.

Розумні офіси можуть бути корисними для віддалених та гібридних працівників завдяки використанню інноваційних конференц-залів, цифрових дошок та вдосконалених систем управління документами.

Ця стаття призначена для власників бізнесу, які цікавляться технологіями розумного офісу.

Поширення більш просунутих технологій змінює спосіб ведення бізнесу. Такі розробки, як Інтернет речей (IoT), надають різноманітні можливості в багатьох галузях промисловості та переосмислюють сучасне робоче місце й оптимізують операції. Цей зсув очевидний у тенденції до створення так званого

розумного офісу, також відомого як адаптивне або цифрове робоче місце, в якому технології використовуються для того, щоб зробити фізичне робоче середовище інтелектуальним та адаптованим до робочих процесів компанії.

Освітлення, вимикачі, димери, реле термостати, камери віртуальної реальності, динаміки віртуальної реальності тощо — все це відіграє важливу роль у розумному офісі.

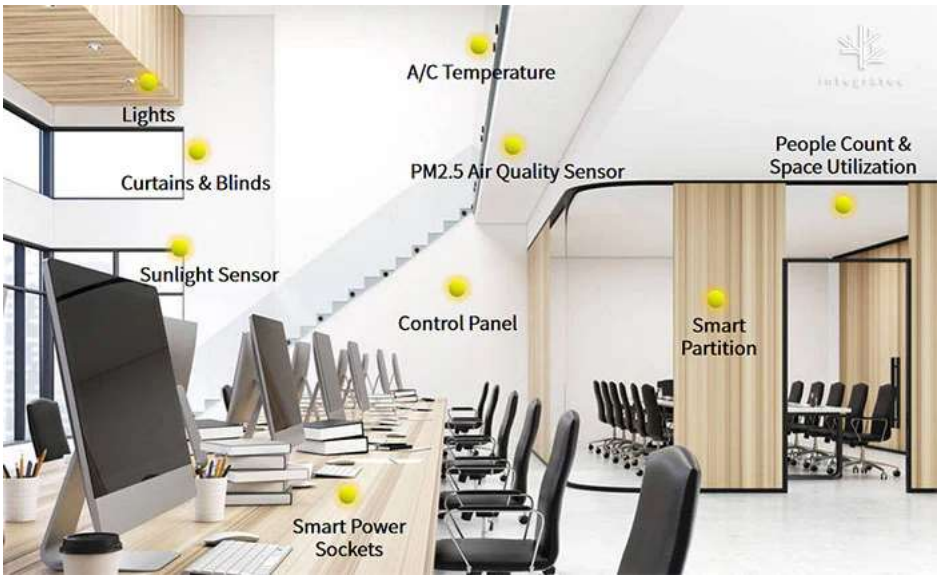


Рисунок 4.1 - Розумний офіс

Розумні офіси також оснащені технологіями, що покращують комунікацію між людьми як для особистої, так і для віддалених співробітників. Ці інструменти можуть включати цифрові дошки для легкої синхронізації нотаток та проведення мозкових штурмів, покращені конференц-зали з камерами високої чіткості та мікрофонами для продуктивних відеоконференцій , а також високоякісні системи управління документами, розміщені в хмарі.

Завдяки використанню вищезазначених інструментів та інших інтелектуальних технологій компанії можуть підвищити моральний дух співробітників , збільшити продуктивність та зменшити споживання енергії. Наприклад, дослідження, проведене Timbergrove, яка спеціалізується на рішеннях для Інтернету речей та автоматизації, показує, що розумні будівлі, що

використовують такі технології, як датчики температури, інтелектуальні термостати та датчики обліку людської присутності, можуть скоротити витрати на енергію на 15…25%.

Потенціал адаптивного робочого місця для розмиття традиційних меж офісу може мати величезний вплив на ставлення працівників та якість їхньої роботи. Поєднання технологій та гнучкості надає працівникам простір, необхідний для роботи на найкращому рівні, не підриваючи при цьому нагляд роботодавця.

Оскільки технології, що лежать в основі розумних офісів, стають все більш поширеними, компанії все частіше впроваджуватимуть різні інструменти для покращення робочого місця.

Компанія Cisco активно впроваджує технології розумного офісу. Вже зараз деякі аспекти, які ще не так давно здавалися неможливими, як-от цифрові простори для спільної роботи та редагування документів у режимі реального часу, є надзвичайно поширеними сьогодні.

## 4.2 Програми безпеки Cisco з Systems Manager для гібридного розгортання в офісі

Cisco Meraki Systems Manager MDM можна використовувати для віддаленого розгортання та налаштування програм Cisco на керованих пристроях. Керовані пристрої можуть належати як організації, так і/або належати кінцевому користувачу. Це означає, що пристрої можуть переміщатися між фізичним особистим домом і фізичним офісом. Для цього гібридного середовища керування пристроями Meraki Systems Manager у поєднанні з безпекою програми Cisco забезпечує одні з найпотужніших варіантів керування в галузі.

Meraki Systems Manager можна використовувати для надсилання програм Cisco та їхніх конфігурацій на керовані пристрої. Під керуванням пристрої реєструються в мережі Meraki Systems Manager. За бажанням можна додати

автентифікацію реєстрації та підвищити безпеку реєстрації та відстежувати особистість кінцевого користувача на зареєстрованих пристроях, а також навіть за потреби додати Duo як запит 2FA під час початкової реєстрації пристрою!

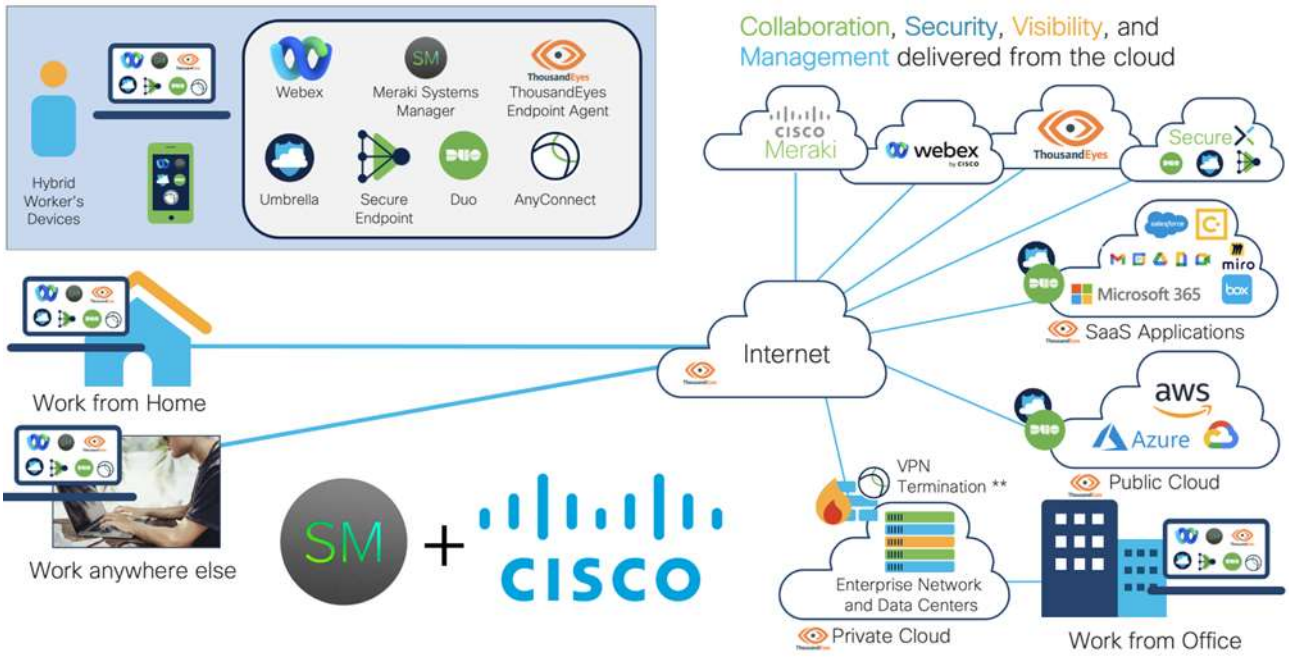


Рисунок 4.2 – Офісна безпека Cisco з Systems Manager

Керовані пристрої можуть бути як пристроями, що належать організації, так і пристроями, що належать кінцевим користувачам.

Пристрої, що належать у бізнесу /організації, отримують додаткові переваги та безпеку. Величезною перевагою пристроїв, що належать організації, є те, що вони автоматично реєструються під час початкового налаштування та зберігаються після скидання заводських налаштувань. Це зберігає право власності на пристрої, що належать вашій компанії, і робить майже неможливим втрату пристрою. Вони також дають змогу отримувати потужніші параметри керування додатковими параметрами автоматичної ініціалізації пристроїв, як-от «Нагляд» для пристроїв Apple і «Реєстрація власника пристрою» для пристроїв Android. Зберігайте право власності на пристрої, що належать компанії, інтегруючи Systems Manager із такими автоматичними реєстраціями постачальників:

- автоматична реєстрація пристроїв Apple (iOS/iPadOS, tvOS і macOS);

- автопілот Windows (незабаром);

- реєстрація пристрою з ОС Chrome.

Cisco SecureX забезпечує однакову роботу з усіма вашими продуктами. Об'єднайте всі продукти з цього документа в єдиний інтерфейс за допомогою SecureX.

Systems Manager має інтуїтивно зрозумілу автоматизацію та надійний захист для всього вашого портфоліо систем безпеки в одному місці.

Systems Manager має унікальну інтеграцію з порталом Cisco SecureX для надсилання інформації про пристрій Systems Manager MDM до SecureX через модуль Device Insights. Завдяки цьому інформацію MDM Systems Manager можна легко переглядати разом із усіма іншими платформами безпеки Cisco. [12]

### 4.3 Встановлення пристроїв та послуг Інтернету речей

Технологічна компанія Playtech впроваджує систему «розумний офіс» та вирішує задачу управління, моніторингу станом «розумних» об’єктів в офісі за допомогою технології Інтернету речей «SmartOffice». «Розумні» об’єкти керуються дистанційно через веб-інтерфейс системи.

SmartOffice реалізує хмарні мережі та хмарні обчислення. IP-адреси, маски підмережі та шлюзи за замовчуванням призначаються кожному мережевому пристрою через DHCP. Пристрої Інтернету речей налаштовуються через Wi-Fi для підключення до хмарних сервісів. За допомогою інструментів хмарних сервісів сценарії керування пристроями Інтернету речей реалізуються на віддаленому сервері. Архітектура мережі NetworkStreet реалізує мобільний зв'язок. Кожному мережевому пристрою призначається IP-адреса, маска підмережі та шлюз за замовчуванням через DHCP. Клієнти 3G/4G підключаються до мережі. Мережа складається зі смартфонів та мобільної базової станції. Сервер CentralOffice підключає мережу до маршрутизатора провайдера.


Рисунок 4.3 - технології Інтернету речей «Smart Office»

Усі датчики та контролери в системі Wi-Fi технологічної компанії Playtech налаштовані як пристрої Інтернету речей для підключення до хмарних сервісів.

Завдяки цим сервісам сценарії керування «Sharp Challenge» працюють на віддаленому сервері. Підключення пристроїв базується на технології Wi-Fi та підтримується маршрутизатором Getway DLC100 електронних замків дверей.

Контролер DLC100 призначає адреси підключеним пристроям з блоку приватних адрес 192.168.25.100 - 192.168.25.254 за допомогою DHCP.

Таблиця 4.1 – Конфігурація мережі офісу технологічної компанії Playtech

| Налаштування | значення |
|---|---|
| IP-адреса шлюзу | 192.168.25.1 |
| Маска домашньої підмережі | 255.255.255.0 |
| SSID бездротової мережі | Офіс |
| Процес перевірки | WPA2-PSK-AES |
| Ключ автентифікації (пароль) | 123211 |

Office – це мережа для пристроїв Інтернету речей для технологічної Технологічна компанія, де впроваджена технологія пристроїв Інтернету речей.

Ця мережа включає такі компоненти, як маршрутизатори Cisco WiFi, контролери процесорів, датчики Інтернету речей та інші пристрої, такі як кнопки, двигуни, перемикачі, датчики світла, камери, лампи, сигналізація, датчики руху, кавоварки, розумні двері, розумні розетки, планшети дистанційного керування

тощо. Загалом, усі пристрої Інтернету речей підключаються до WiFi_SH_Router через налаштування Інтернету речей, а потім підключаються до DHCP-сервера для подальшого налаштування.

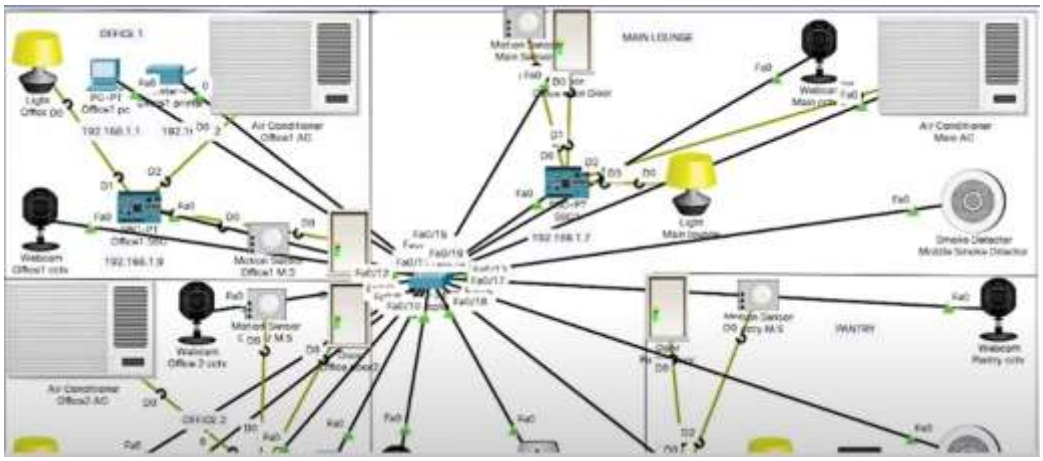

Рисунок 4.4 - Топологічна схема Інтернету речей офісу технологічної компанії Playtech

Усі пристрої в системі інтелектуального доступу технологічної компанії Playtech підключені до бездротової мережі, що підтримується домашнім шлюзом.

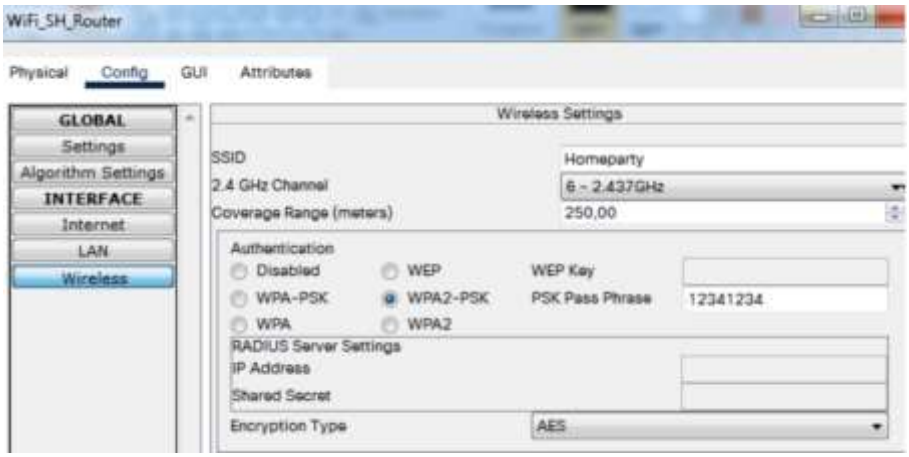


Рисунок 4.5 – Налаштування інтерфейсу бездротового маршрутизатора технологічної компанії Playtech

Щоб смарт-пристрій підключився до мережі, необхідно налаштувати такі параметри, як SSID, метод автентифікації, код автентифікації, отримання IP-адреси через DHCP та призначений сервер Інтернету речей.

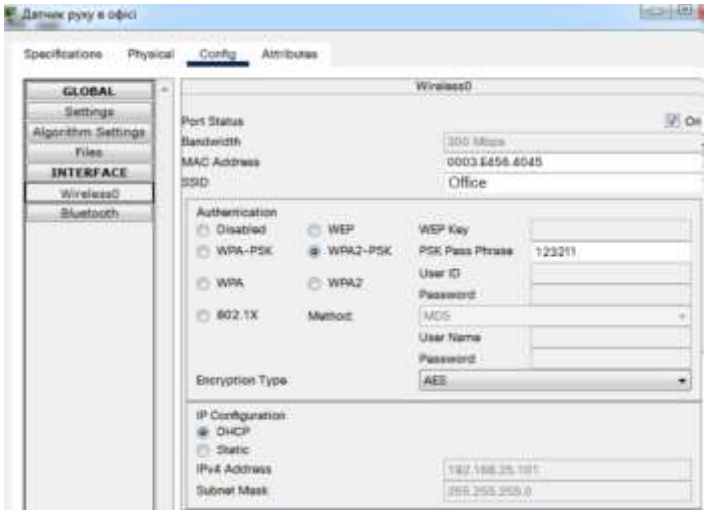


Рисунок 4.6 – Налаштування DHCP та бездротового зв'язку датчика руху в технологічній компанії Playtech

Як IoT-сервер, сервер провайдера налаштовано з IP-адресою 209.165.200.9/24. На головній сторінці сервера відображається список IoT-пристроїв, кожним з яких можна керувати (вмикати/вимикати) або моніторити дистанційно.


Рисунок 4.7 – Налаштування віддаленого доступу до сервера Інтернету речей технологічної компанії Playtech

Хмарні обчислення реалізуються в певній ситуації, за певною логікою. Вони працюють наступним чином: коли спрацьовує датчик світла, кавоварка та освітлення вмикаються. Сигнал від підключеної розетки вимикає освітлення. Потім кавоварка вимикається у запрограмований час. Принцип такий: за

допомогою планшета ви підключаєтеся до IoT-сервера через мережу, використовуючи адресу електронної пошти 209.165.200.10/24.

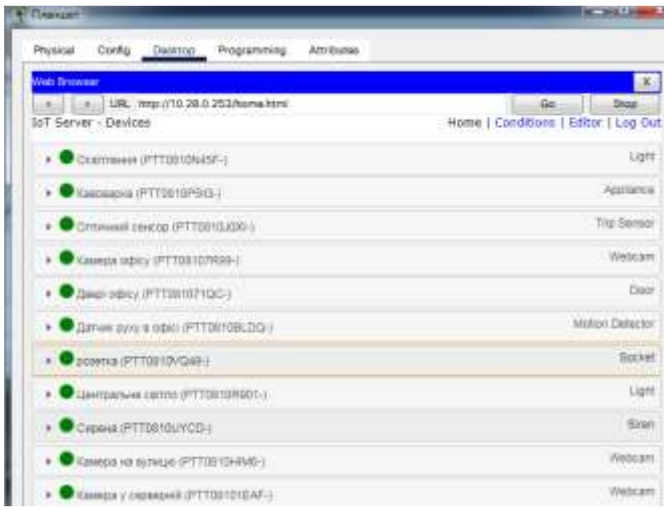


Рисунок 4.8 – Веб-інтерфейс для керування пристроями Інтернету речей технологічної компанії Playtech

За допомогою інтерфейсу веб-сервера IoT було налаштовано систему управління безпекою доступу технологічної компанії Playtech.


Рисунок 4.9 – Сценарії функціонування системи IoT технологічної компанії Playtech

На відміну від хмарних обчислень, туманні обчислення реалізовані в панелі керування за допомогою мови програмування JavaScript. Їхнє основне завдання - керування ролетами для контролю доступу. Перший двигун запускається сигналом від кнопки ввімкнення/вимкнення. Коли надходить сигнал від

кінцевого вимикача 1 на ролику_1, двигун зупиняється, і привід ролика_2 відкривається. Коли надходить сигнал від кінцевого вимикача 2 на ролику_2, двигун зупиняється, і двигун ролика_3 відкривається. Коли надходить сигнал від кінцевого вимикача 3, двигун ролика_3 зупиняється. Важливо зазначити, що всі компоненти підключені до окремих кабелів Інтернету речей: приводи підключені до аналогових виходів, а кнопки - до цифрових виходів. Іншими словами, сигнал двигуна приймає значення від 0 до 255, на відміну від кнопки, яка може отримувати лише сигнал 1 або 0.

```
function setup() {
    pinMode(3, INPUT);
    pinMode(0, INPUT);
    pinMode(A0, OUTPUT);
}

var motorOne = A0;
var motorTwo = A1;
var motorThree = A2;

function loop() {
    if(digitalRead(3, HIGH)){
        digitalWrite(motorOne, HIGH);
    }
    else if (digitalRead(0, HIGH)){
        digitalWrite(motorOne, LOW);
        digitalWrite(motorTwo, HIGH);
    }
    else if (digitalRead(1, HIGH)){
        digitalWrite(motorTwo, LOW);
        digitalWrite(motorThree, HIGH);
    }
    else if (digitalRead(2, HIGH)) {
        digitalWrite(motorThree, LOW);
    }
}
```

Рисунок 4.10 – Налаштування контролера технологічної компанії Playtech

# ВИСНОВКИ

Кваліфікаційна робота спрямована на розробку комп'ютерної системи для технологічної компанії. Робота має окреме деталізоване завдання з побудови, налаштування та безпеки корпоративної мережі.

Метою кваліфікаційної роботи є визначення основних завдань у сучасній телекомунікаційній галузі, зокрема організації централізованої корпоративної мережі, її різноманітного спектру, високоякісних та доступних послуг.

В роботі розглянуті наступні моменти:

- аналіз основної наукової, статистичної та довідкової інформації, дані, що пов'язані з інтернет-провайдером;

- теоретичні аспекти проблем на основі статистичної, наукової та практичної літератури, причини вибору пристроїв Cisco, структура мережі компанії;

- представлено короткий огляд розширених параметрів для вибраних пристроїв та типу магістрального кабелю, а також процесу призначення IP-адрес, заснований на практичній, науковій та статистичній літературі.

Розроблена КС відповідає показникам високої надійності роботи, підвищеної стійкості до кіберзагроз програмного та апаратного забезпечення КС.

Спираючись на архітектуру КС з кількістю підмереж 5, їх взаємодію між собою апаратне забезпечення мережі та робочих станцій користувачів виконано розрахунок для налаштувань пристроїв мережі, обрані належні та протоколи зв’язку, розраховано налаштування маршрутизаторів, проведено моделювання роботи мережі для впевненості її адекватного функціонування.

Система «Розумний офіс» побудована за допомогою IoT та складається з різних рівнів: пристроїв, комунікацій, хмарних сервісів та додатків. Компоненти проектованої системи розташовані в офісі технологічної компанії.

# ПЕРЕЛІК ПОСИЛАНЬ

1. 100 найприбутковіших IT-компаній України. Режим доступу: https://speka.media/100-naipributkovisix-it-kompanii-ukrayini-98grkp

2. Our Locations. Режим доступу: https://www.playtech.com/locations/

3. Kyiv Office. Режим доступу: https://www.playtech.com/locations/ukraine/

4. ТОВ "ПТС ЮА СЕРВІСЕЗ"38749239. Режим доступу: https://youcontrol.com.ua/ru/catalog/company_details/38749239/

5. ТОП-50 IT-компаній: хто сплатив найбільше податків. Режим доступу: https://ain.ua/2024/08/20/50-naibilsix-it-kompanii-xto-splativ-naibilse-podatkiv-za-ii-kvartal/

6. The Role and Importance of Information Technology (I.T.) in Today's World. Режим доступу: https://www.aiu.edu/blog/the-role-and-importance-of-information-technology-i-t-in-todays-world/

7. The Importance of Technology in Economic and Social Development. Режим доступу: https://medium.com/@datamationinter/the-importance-of-technology-in-economic-and-social-development-2a063763d06

8. Méta-analyse sur les Systèmes d'Information de gestion : Etat de l'art et Synthèse. Режим доступу: https://www.researchgate.net/publication/271557745_Meta-analyse_sur_les_Systemes_d'Information_de_gestion_Etat_de_l'art_et_Synthese

9. IT Organizational Charts: 11 Examples for Any Business. Режим доступу: https://www.givainc.com/blog/it-organizational-charts/

10. What is an organogram?. Режим доступу: https://lexchart.com/what-is-an-organogram/

11. Що таке мережева безпека?. Режим доступу: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

12. Cisco Security Applications with Systems Manager for Hybrid Home Office Work Deployments. Режим доступу: https://documentation.meraki.com/SM/Deployment_Guides/Cisco_Security_Applications_with_Systems_Manager_for_Hybrid_Home_Office_Work_Deployments

# ДОДАТОК А
# ТЕКСТ ПРОГРАМИ

**Міністерство освіти і науки України**
**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**
**“ДНІПРОВСЬКА ПОЛІТЕХНІКА”**

# ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми
804.02070743.20015–01 12 01

Листів 6

**2025**

# АНОТАЦІЯ

Документ містить ПЗ програмування налаштування компонентів корпоративної мережі комп'ютерної системи технологічної компанії Playtech. Програма призначена для забезпечення налаштування динамічної маршрутизації, DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену и SSH комп'ютерної системи.

# ЗМІСТ

1 Налаштування роутера R2_Baskin

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2_Baskin
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 10.68.0.129 10.68.0.139
!
ip dhcp pool POOL_LAN2
 network 10.68.0.128 255.255.255.128
 default-router 10.68.0.129
 dns-server 10.68.1.85
!
aaa new-model
!
aaa authentication login Login group radius local
aaa authentication login SSH-LOGIN local
aaa authentication login default group radius local

!
license udi pid CISCO2911/K9 sn FTX1524602K-
!
no ip domain-lookup
ip domain-name Shchetinin_R1
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 description LAN Admin
 ip address 10.68.0.129 255.255.255.128
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
!
interface Serial0/0/1
 description WAN R1
 bandwidth 128
 ip address 10.0.10.2 255.255.255.252
 ip ospf cost 7500
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 23
 router-id 15.15.15.15
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 network 10.0.10.0 0.0.0.3 area 0
 network 10.68.0.128 0.0.0.127 area 0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow-export version 9
!
banner motd #123-18 Baskin. Enter only have key#
!
```

```
radius-server host 10.68.0.150 auth-port 1645
radius-server key Baskin
!
radius server 10.68.0.150
 address ipv4 10.68.0.150 auth-port 1645
!
!
!
line con 0
 password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login authentication SSH-LOGIN
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 transport input ssh
!
!
!
end
```

1 Налаштування комутатора Baskin_Sw4.1

```
!
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Baskin_Sw4.1
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip domain-name Shchetynin_SW_Gosp
!
username 12316z_Shchetynin privilege 1 password 7 082048430017061E010803
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 30
```

```
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 40
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 switchport trunk native vlan 100
 switchport trunk allowed vlan 20,30,40,99
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 20,30,40,99
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 description LAN Menag
 ip address 10.68.0.2 255.255.255.224
!
ip default-gateway 10.68.0.1
!
banner motd
————————————123-18 Baskin.
Enter only have
key————————————
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
!
end
```

# ДОДАТОК Б
# ТАБЛИЦІ МАРШРУТИЗАЦІЇ

## Таблиця маршрутизації на R1_Baskin

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 13 subnets, 5 masks
C       10.0.10.0/30 is directly connected, Serial0/0/1
L       10.0.10.1/32 is directly connected, Serial0/0/1
C       10.0.10.4/30 is directly connected, Serial0/0/0
L       10.0.10.5/32 is directly connected, Serial0/0/0
O       10.0.10.8/30 [110/15000] via 10.0.10.6, 02:51:55, Serial0/0/0
O       10.68.0.0/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.32/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.64/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.96/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.128/25 [110/7501] via 10.0.10.2, 03:57:06, Serial0/0/1
O       10.68.1.0/26 [110/7501] via 10.0.10.6, 03:57:06, Serial0/0/0
C       10.68.1.64/27 is directly connected, GigabitEthernet0/1
L       10.68.1.65/32 is directly connected, GigabitEthernet0/1
     209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/15000] via 10.0.10.6, 03:53:53, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

## Таблиця маршрутизації на R2_Baskin

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 12 subnets, 5 masks
C       10.0.10.0/30 is directly connected, Serial0/0/1
L       10.0.10.2/32 is directly connected, Serial0/0/1
O       10.0.10.4/30 [110/15000] via 10.0.10.1, 03:57:56, Serial0/0/1
O       10.0.10.8/30 [110/22500] via 10.0.10.1, 02:52:45, Serial0/0/1
O       10.68.0.0/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
O       10.68.0.32/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
O       10.68.0.64/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
O       10.68.0.96/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
C       10.68.0.128/25 is directly connected, GigabitEthernet0/0
L       10.68.0.129/32 is directly connected, GigabitEthernet0/0
O       10.68.1.0/26 [110/15001] via 10.0.10.1, 03:57:56, Serial0/0/1
O       10.68.1.64/27 [110/7501] via 10.0.10.1, 03:57:56, Serial0/0/1
     209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/22500] via 10.0.10.1, 03:54:48, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

## Таблиця маршрутизації на Baskin_R3

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 13 subnets, 5 masks
O       10.0.10.0/30 [110/15000] via 10.0.10.5, 03:58:34, Serial0/0/0
C       10.0.10.4/30 is directly connected, Serial0/0/0
L       10.0.10.6/32 is directly connected, Serial0/0/0
C       10.0.10.8/30 is directly connected, Serial0/0/1
L       10.0.10.10/32 is directly connected, Serial0/0/1
O       10.68.0.0/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O       10.68.0.32/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O       10.68.0.64/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O       10.68.0.96/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O       10.68.0.128/25 [110/15001] via 10.0.10.5, 03:58:24, Serial0/0/0
C       10.68.1.0/26 is directly connected, GigabitEthernet0/1
L       10.68.1.1/32 is directly connected, GigabitEthernet0/1
O       10.68.1.64/27 [110/7501] via 10.0.10.5, 03:58:34, Serial0/0/0
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/27 is directly connected, Serial0/1/0
L       209.165.202.2/32 is directly connected, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

## Таблиця маршрутизації на Router_IPS

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 15 subnets, 5 masks
O       10.0.10.0/30 [110/15064] via 10.0.10.10, 02:54:02, Serial0/0/1
O       10.0.10.4/30 [110/7564] via 10.0.10.10, 02:54:02, Serial0/0/1
C       10.0.10.8/30 is directly connected, Serial0/0/1
L       10.0.10.9/32 is directly connected, Serial0/0/1
C       10.68.0.0/27 is directly connected, GigabitEthernet0/1.99
L       10.68.0.1/32 is directly connected, GigabitEthernet0/1.99
C       10.68.0.32/27 is directly connected, GigabitEthernet0/1.20
L       10.68.0.33/32 is directly connected, GigabitEthernet0/1.20
C       10.68.0.64/27 is directly connected, GigabitEthernet0/1.30
L       10.68.0.65/32 is directly connected, GigabitEthernet0/1.30
C       10.68.0.96/27 is directly connected, GigabitEthernet0/1.40
L       10.68.0.97/32 is directly connected, GigabitEthernet0/1.40
O       10.68.0.128/25 [110/15065] via 10.0.10.10, 02:54:02, Serial0/0/1
O       10.68.1.0/26 [110/65] via 10.0.10.10, 02:54:02, Serial0/0/1
O       10.68.1.64/27 [110/7565] via 10.0.10.10, 02:54:02, Serial0/0/1
     209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/7564] via 10.0.10.10, 02:54:02, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

# Таблиця маршрутизації на Baskin_R0

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 10 subnets, 4 masks
O       10.0.10.0/30 [110/15064] via 209.165.202.2, 03:54:58, Serial0/1/0
O       10.0.10.4/30 [110/7564] via 209.165.202.2, 03:54:58, Serial0/1/0
O       10.0.10.8/30 [110/7564] via 209.165.202.2, 02:54:50, Serial0/1/0
O       10.68.0.0/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O       10.68.0.32/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O       10.68.0.64/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O       10.68.0.96/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O       10.68.0.128/25 [110/15065] via 209.165.202.2, 03:54:58, Serial0/1/0
O       10.68.1.0/26 [110/65] via 209.165.202.2, 03:54:58, Serial0/1/0
O       10.68.1.64/27 [110/7565] via 209.165.202.2, 03:54:58, Serial0/1/0
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.0/27 is directly connected, GigabitEthernet0/0
L       209.165.200.1/32 is directly connected, GigabitEthernet0/0
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/27 is directly connected, Serial0/1/0
L       209.165.202.1/32 is directly connected, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 209.165.202.2, 03:54:58, Serial0/1/0
```