**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Одеський коледж комп’ютерних технологій «Сервер»**

циклова комісія «Професійної та практичної підготовки з комп’ютерних технологій»

**РОЗРАХУНКОВО-ГРАФІЧНА РОБОТА З ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ**

Тема роботи **– «**Впровадження алгоритмів шифрування, та інші засоби інформаційної безпеки в сучасні підприемства**»**

Спеціальність 121 - Інженерія програмного забезпечення

Дипломна робота молодшого спеціаліста

ВИКОНАВ:

Студент групи  К17      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_     В.В. Шишелов

КЕРІВНИК:      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    Д.С. Шибаєв

Одеса – 2020

СОДЕРЖАНИЕ

ВСТУП

У великому бізнесі безпека інформації завжди була найважливішим аспектом проектування інтелектуальних систем. Окрім банальної крадіжки інформації компанії піддаються хакерським атакам з боку конкурентів або так званих «Фрілансерів».Тому потрібно виділяти більше часу і грошей на системи безпеки мереж, обладнання, програмного забезпечення та підготовку персоналу. В цій роботі буде проведений аналіз можливостей покращення стану безпеки інформації на підприємстві.

ПРОФІЛАКТИКА І ВИЯВЛЕННЯ ПРОБЛЕМ З БЕЗПЕКОЮ

У великому бізнесі безпека інформації завжди була найважливішим аспектом проектування інтелектуальних систем. Окрім банальної крадіжки інформації компанії піддаються хакерським атакам з боку конкурентів або так званих «Фрілансерів».

В арсеналі сучасних спеціалістів величезний вибір інструментів для захисту серверу і мережі в цілому. Окрім звичайного апаратного захисного обладнання контролюючого вхідні та вихідні потоки інформації, величезну роль грають саме програмні засоби безпеки.

Програмні засоби - спеціальні програми, програмні комплекси і системи захисту інформації в інформаційних системах різного призначення і засобах обробки (збір, накопичення, зберігання, обробка і передача) даних.

В рамках роботи, варто виділити основні, найслабкіші уразливості в підприємстві, які необхідно вирішити.

1. Використання Брандмауеру на сервері підприємства. Застосування брандмауеру суттєво знизить вірогідність втрати важливої інформації.
2. Проблеми пов'язані з втратою або крадіжкою паролю. Проблема пов'язана с низькою кваліфікацією або інформованістю працівника.
3. Вимоги до безпеки носіїв на підприємстві. Найпростішим варіант покращити зовнішню безпеку та викреслити соціальну інженерію з методів проникнення – це використовувати шифрування носіїв
4. Тільки авторизовані працівники. Можливість до інформації підприємства надається лиш користувачам, які є в базі даних підприємства.
5. Використання лише безпечних, перевірених протоколів обміну інформації в мережі.
6. Захист веб-додатків пов'язаних з підприємством. Організація захисту сайтів та сервісів підприємства.

РОЗРОБКА ІНЖЕНЕРНОГО ПРОЕКТУ

В роботі розглядається принцип роботи, можливості та особливості ролі мережевого екрану на підприємстві під управлінням операційної системи Windows Server 2019 .

«DATA.Net» - підприємство інтернет-провайдер, яке забезпечує якісним інтернет покриттям місто з населенням 2500 чоловік. Підприємство займається постачанням якісного та захищеного інтернет трафіку користувачам за допомогою технологій GPON та FireWall.

**Мета роботи**

Метою роботи є впровадження технології FireWall у підприємство постачання інтернет трафіку під управлінням ОС Windows Server 2019.

**Вхідні дані**

Підприємство «DATA.Net» базується у двох будівлях. Перша двоповерхова будівля призначена для керуючого та обслуговуючого персоналу підприємства. Друга будівля призначена для технічного персоналу та зберігання матеріалів монтажу та ремонту ліній передачі трафіку. В цих будівлях знаходяться наступні кабінети:

* Генеральний директор - 1 працівник (через своїх заступників і відповідні відділи здійснює керівництво всією виробничої, господарської та фінансової діяльністю).
* Заступник директора - 1 працівник, як правило, є першим заступником директора. Він безпосередньо керує основною виробничою діяльністю.
* Головний інженер - 1 працівник, здійснює технічне керівництво. Він очолює роботи з розвитку та реконструкції мереж.
* Заступник з економічних питань - 1 працівник, керує роботами по перспективному і поточному планування та обліку господарської діяльності, займається питаннями оптимізації та ефективності діяльності підприємства, організацією праці та заробітної плати, автоматизацією управління персоналом.
* Комерційний відділ - 3 працівника, розробляє проекти договірних умов з клієнтурою, проекти місцевих тарифів на надання послуг провайдера, розглядає претензії і позови.
* Відділ матеріально-технічного постачання - 2 працівника, забезпечує підприємство обладнанням, матеріалами, інструментом. Складає зведені заявки на всі види постачання і організовує задоволення цих заявок. Організовує прийом, зберігання і видачу обладнання і матеріалів за заявками, контролюючи при цьому норми витрат.
* Відділ організації праці та заробітної плати - 2 працівника, займається питаннями нормування праці та його вдосконаленням, розробкою місцевих норм праці; складає штатний розклад і здійснює контроль за витрачанням фонду заробітної плати, контролює дотримання штатної дисципліни і трудового законодавства; готує матеріали по підведенню його підсумків.
* Бухгалтерія - 3 працівника, веде облік, контроль і аналіз виробничо-фінансової діяльності підприємства в грошовому вираженні; контролює прийом і витрачання матеріалів та платіжок за послуги підприемства, нараховує і видає заробітну плату, складає звіти і баланси.
* Відділ серверної - 1 працівник, забезпечується збір інформації, її обробка відповідно до характеру вирішуваних завдань, проводиться аналіз отриманої інформації, здійснюється розробка оптимальних рішень і передає їх для виконання відповідним підрозділам підприємства.
* Відділ кадрів - 2 працівника займається підбором, вивченням і розстановкою кадрів за діловими якостями; розробляє заявки на підготовку інженерно-технічних працівників і робітників; закріплення кадрів; аналізує та узагальнює причини плинності кадрів і вживає заходів до усунення цього явища; веде облік кадрів.
* Відділ маркетингу – 2 працівника займаються розповсюдженням інформації про підприємство, розробляють нові маркетингові ідеї для притянення нових клієнтів.
* Відділ абонентів – 3 працівника займаються прийняттям і обробкою запитів від абонентів.
* Технічний відділ – 20 працівників що займаються монтажем, демонтажем, модернізацією, ремонтом мереж та підключенням нових абонентів.
* Відділ безпеки – 2 працівника агенства охорони, відповідають за безпеку будівлі і майна підприємства.
* Кол-центр – 3 працівника, відповідають на питання та переадресовують на інші відділи.
* Юридичний відділ – 2 працівника займаються юридичними питаннями та проблемами.

**Завдання дипломної роботи**

До виконання дипломної роботи входять наступні пункти:

* Виконати порівняльний аналіз технологій мережевих екранів.
* Зробити проектування локальної мережі: вибір технології, топології, та мережної адресації, обладнання, підключення до глобальної мережі, кабельні системи.
* Зробити розрахунок вартості мережевого обладнання: комп'ютерів, периферійних пристроїв, серверного та мережевого обладнання для підприємства.
* Виконати опис конфігурування мережевого екрану та інших служб серверів підприємства за допомогою Windows Server 2019.
* Виконати впровадження FireWall у підприєство.
* Розрахувати економічні витрати на реалізацію дипломного проекту.

**Вимоги дипломної роботи**

* Налаштувати мережеві пристої на підприємстві.
* Забезпечити доступ до мережі Інтернет зі швидкістю 1000 Мбіт/сек.
* Реалізувати резервний iнтернет-канал.
* Забезпечити резервне щоденне копіювання даних.
* Втілити впровадження технології FireWall на підприємстві.
* Забезпечити облік бухгалтерії на підприємстві.
* Забезпечити доступ користувачів різних підрозділів підприємства до файлового серверу.
* Реалізувати відмовостійкість серверноі інфраструктури.

**План будівлі та топологія мережі**

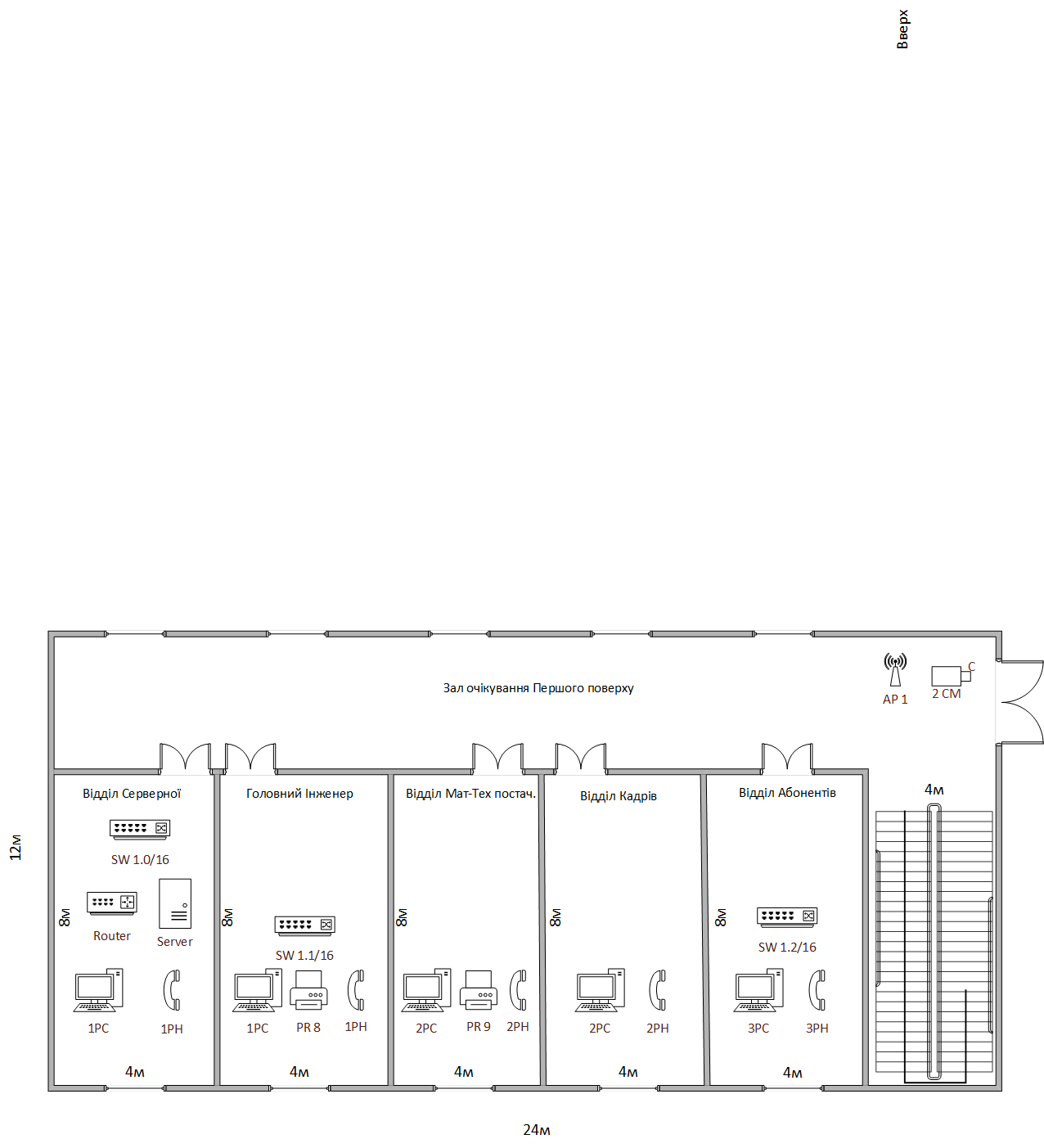


Рисунок 1. План першого поверху будівлі

 Рисунок 2. План другого поверху будівлі

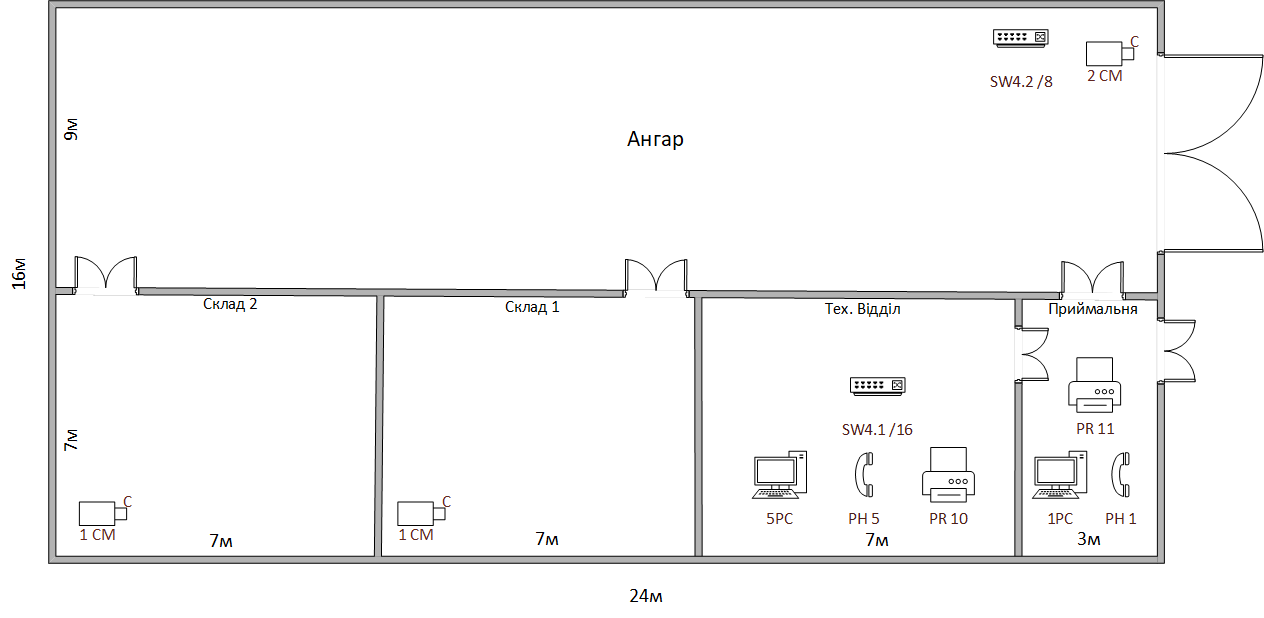


Рисунок 3. План технічної будівлі

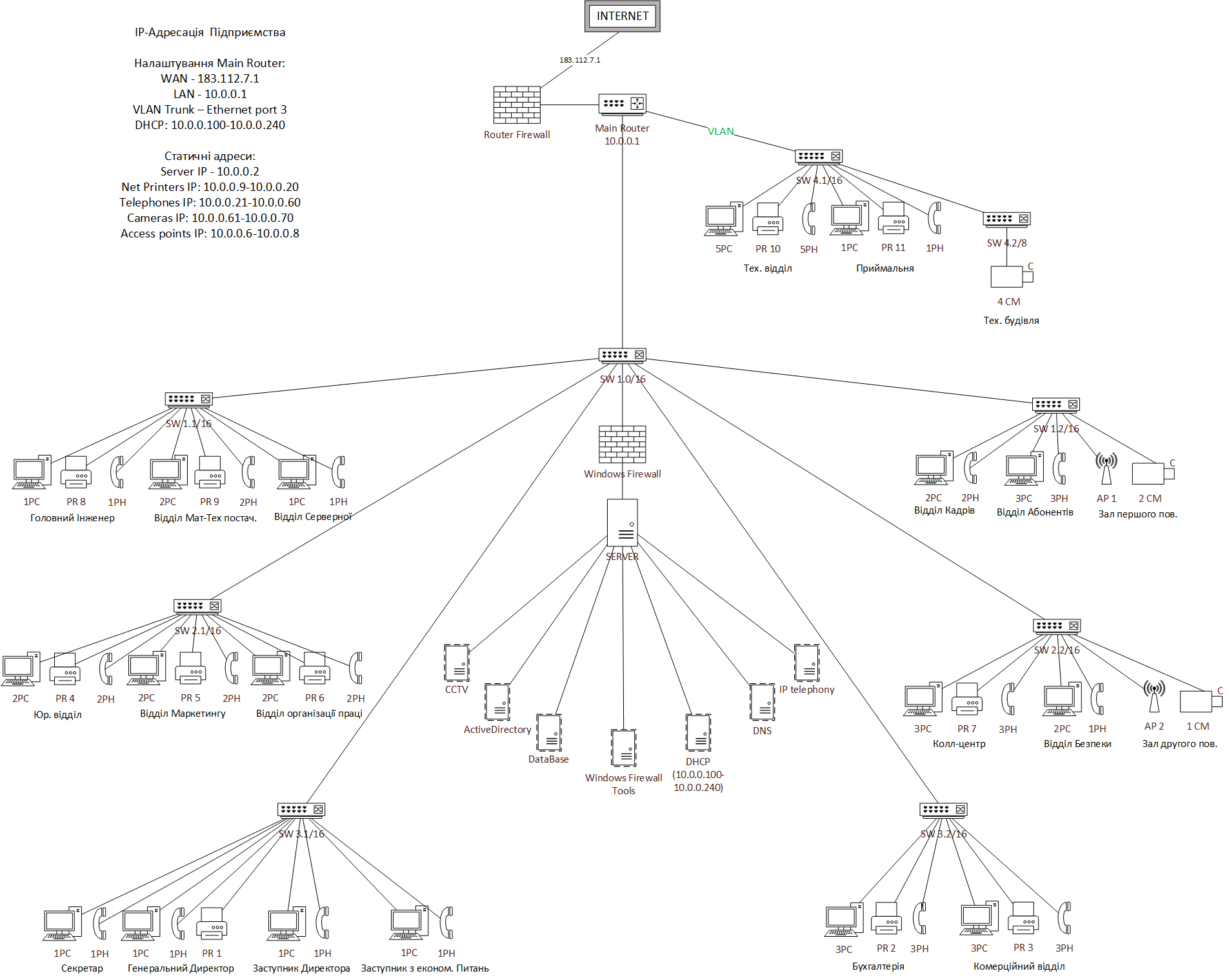


Рисунок 4. Топологія локальної мережі підприємства

КОШТОРИС ІНЖЕНЕРНОГО ПРОЕКТУ

1. Сервер AD - Lenovo ThinkSystem SR530 SILVER4108 16GB/7X08A01W(рис 1.)



Рис 1

Тех. характеристики:

* Форм-фактор - 1U
* ОЗУ - 8GB DDR4 2933MHz
* Роз’єми - 3 PCIe 3.0
* Мережеві інтерфейси - 2 порта 1GbE + 1GbE для кирування.
* Процесор - 2 х Intel Xeon scalable

1. Сервер FTP - Synology RS1219+ (рис 2.)



Рис 2

Тех. характеристики:

* Форм-фактор - 2U
* Кількість ЖД – 8
* Швидкість мережевої карти – 1Гбит/с
* ОЗУ – DDR3 8GB
* Продуктивність – 1310Мб/с
* Процесор – 4 ядра, 2.4 ГГц
* Максимальная емкость – 128 ТБ

1. Маршрутизатор - MIKROTIK CCR1009-7G-1C-1S+ (рис 3.)



Рис 3

Тех. характеристики:

* Форм-фактор - 1U
* SFP порти - 2
* Ethernet порти – 8
* COM
* USB 4G
* Швидкість – 1Гбит/с
* VPN

1. Комутатор 8п. - CISCO SG110D-08HP-EU(рис 4.)



Рис 4

Тех. характеристики:

* Тип -некерований
* Форм-фактор - настільних
* Кількість портів - 8
* Порти - Gigabit Ethernet

1. Комутатор 16п. - TP-LINK TL-SF1016DS(рис 5.)



Рис 5

Тех. характеристики:

* Тип - некерований
* Форм-фактор – у стійку U1
* Кількість портів - 16
* Порти - Fast Ethernet

1. Точка доступу - MIKROTIK RBCAPGI-5ACD2ND(рис 6.)



Рис 6

Тех. характеристики:

* Режими работи - Wi-Fi точка
* Стандарти мережі -b (до 11 Мбіт/с), g (до 54 Мбіт/с), n (до 300 Мбіт/с), ac (до 867 Мбіт/с)
* Робоча частота - 2.4 / 5 ГГц
* Тип антени – вмонтована

1. Кабель мережевий - OK-NET UTP-CAT.5E LSFROH 305М (рис. 7)

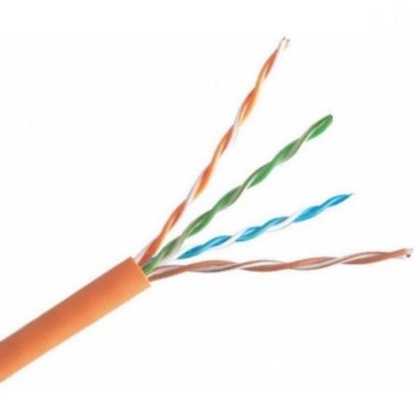


Рисунок 7

Тех. характеристики:

* Артикул – КП Внг-HF-ВП(350) 4\*2\*0,51
* Тип кабелю - UTP
* Матеріал - мідь
* Січення - 0.51 мм
* Категорія - cat 5e

1. Телекомунікаційна шафа (рис 8.)



Рисунок 8

* Місткість - 15U
* Органайзери
* Замок



# Перечень конфигураций ПК и перифирии.



# Перечень выполняемых монтажных работ.



СПЕЦИФІКА ОРГАНІЗАЦІЇ ПІДПРИЄМСТВА З ЗАБЕЗПЕЧЕННЯМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Ознайомившись з підприємством можна виявити його слабкі місця. Отже опираючись на розділ профілактики можна зробити висновки, ща для компанії потрібно провести низку заходів для забезпечення безпеки інформації підприємства.

1. Використання Брандмауеру на сервері підприємства

Брандмауер - це система безпеки, що діє як захисний бар'єр між мережею і зовнішнім світом. Брандмауер підключення до Інтернету (Internet Connection Firewall, ICF) - це програмний засіб, що використовується для налаштування обмежень, що регулюють обмін даними між Інтернетом і домашньої або невеликої офісної мережею.

Отже Брандмауер може стати головною ланкою захисту від ураження та проникнення до системи пвдприємства.

1. Проблеми пов'язані з втратою або крадіжкою паролю.

Користувач в силу небажання запам'ятовувати паролі, використовують слабкі паролі або повторюють один і той самий пароль на сайтах, в системі, що забезпечує людині з боку більш просту задачу в плані злому пароля користувача і несанкціонованого входу в систему.

В якості вирішення цієї проблеми великі компанії замовляють програмне забезпечення для збереження паролів. Такі програми представляють із себе зашифровану базу даних, що зберігає всі паролі і доступ до неї надається лише з наявності складного паролю або навіть шифрованого USB-ключа.

1. Вимоги до безпеки носіїв на підприємстві.

На підприємствах працівники часто втрачаюсь носії з важливою інформацією через що, можуть не навмисно передати інформацію конкурентам. Саме через ці ситуації компанії вказують у контракті з працівниками пункт про нерозголошення та відповідальність за втрату даних.

Тому компанії прибігають до шифрування усіх носіїв на підприємствах. Для систем базованих на Windows використовують програми шифрування починаючи з Bitlocker та EncryptStick, закінчуючи VeraCrypt та навіть KasperskyStick. Для систем на Linux використовують GNUpg та GNOME ENCFS.

1. Тільки авторизовані працівники.

Кожен, хто потрапляє в локальну мережу і хоче отримати доступ до сервера повинен бути авторизовані і мати належні права. кращим рішенням для організації буде

Для організації якісної системи безпеки та авторизації краще використовувати Windows Server та Active directory, адже AD вміщує в себе одну з найрізноманітніших і найгнучкіших систем доступу до інформації на підприємствах.

1. Використання лише перевірених та надійних протоколів

Для забезпечення стійкої роботи мережі підприємство має користуватися відповідними, захищеними протоколами передачі інформації. Найчастіше підприємства можуть знехтувати настільки важливою темою, через що можуть статися непередбачені ситуації.

Перевірені протоколи:

* HTTPS;
* SFTP;
* RDP;

1. Захист веб-додатків пов'язаних з підприємством.

Організація захисту сайтів та сервісів підприємства

Для підприємства, яке займається наданням інтернет-трафіку необхідно мати веб-сайт, який працює на локальному сервері підприємства. Навіть якщо сервер знаходиться в захищеному просторі все одно сервер можливо зламати.

Для уникнення можливості проникнення через веб-додатки використовуються всі можливості, що були приведені вище та декілька нових, таких як :

* Захист від скритих мереж (TOR,AGENT-AM).
* Захист від-блок атак.
* Захист від бот-атак.
* Ліміт на вхід користувачів.
* Ліміт на запити.

ВИСНОВКИ

Після розробки інженерного проекту, був проведений аналіз та виявлені най вірогідні та найуразливіші до проникнення вузли системі підприємства. Було запропоновано можливі покращення стану безпеки підприємства.