Русятинська А.О., магістрантка, гр. КІм-22-1,
Воротніков В.В., д.т.н, доц.,
професор кафедри комп'ютерної інженерії та кібербезпеки
Державний університет «Житомирська політехніка»

НЕОБХІДНІСТЬ РОЗРОБКИ ПІДСИСТЕМИ ПРОГРАМНОГО ТА АПАРАТНОГО ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Інформаційні та комп'ютерні технології розвиваються, мережі розширюються, атаки здійснюються все частіше та покращується їх якість, саме тому важливо створювати підсистеми захищені, як програмно так і апаратно. Для кожного підприємства виконується розробка індивідуального проекту, який повинен задовольняти потреби всіх департаментів, саме через створення унікального рішення неможливо застосовувати загальний підхід, як при будові підмережі, так і формуванні її захисту.

Під час розробки мережі необхідно враховувати способи маршрутизації, а саме виконувати вибір статичної або динамічної маршрутизації, враховуючи потреби компанії. Окрім цього, важливо проаналізувати приблизну кількість користувачів, а також обрати тип адресації IPv4 або IPv6. При розподілі адресації слід виконати аналіз CIDR і VLSM – це терміни, які потрібні під час проектування мережі. CIDR необхідний для об'єднання маршрутів з метою зменшення інформації про маршрутизацію, що передається основними маршрутизаторами, а VLSM сприяє оптимізації доступного адресного простору.

Апаратний захист мережі полягає в забезпеченні захисту пристроїв та каналів за допомогою яких побудована мережа, а також використовуються для запобігання навмисних дій, що здійснюються технічними програмними, змішано-апаратними засобами. Для захисту мережі та збільшенню ступеня її відмовостійкості варто будувати резервні канали зв`язку, сервера, для боротьби з вірусами встановлювати плати безпосередньо в пристрої, налаштовувати контроль доступу, а також розмежування повноважень користувачів. Також варто мати резервне обладнання, оскільки бувають збоїв кабельних систем, перебої електроживлення, збоїв роботи серверів та робочих станцій, що зможе причинити втрату даних.

Програмний захист мережі можна реалізувати за допомогою спеціально-призначеного програмного забезпечення, а також відповідно-розроблених протоколів, систем та конфігурацій, що налаштовуються безпосередньо на пристроях. Одним з важливих моментів для захисту мережі є налаштування ідентифікації користувачів, логування їх дій, налаштування контролю доступу. Це можна реалізувати за допомогою архітектури AAA — це стандартна структура, яка використовується для контролю того, кому дозволено використовувати мережеві ресурси (через автентифікацію), що вони мають право робити (через авторизацію) і фіксувати дії, які виконуються під час доступу до мережі (через облік). Окрім налаштування доступу також необхідно блокувати Spoof/Malicious пакети. За допомогою цього методу можна реалізувати заборону зарезервованій IP-адресі досягати зовнішнього доступу, а також відхилення широкомовних адрес. Для забезпечення захисту даних варто також виконувати шифрування всіх паролів, за допомогою складного паролю.

Всі проаналізовані апаратні та програмні засоби надають можливість побудувати унікальну, захищену мережу, що буде відповідати заданим вимогам, а також матиме високий рівень відмовостійкості.

Під час аналізу літератури для реалізації системи було використано підручник автора Бурова Є.В. з назвою "Комп'ютерні мережі" в ньому описані базові поняття про комп`ютерні мережі, їх побудову, параметри маршрутизації та адресації.

Також під час пошуку інформації для формування та аналізу тематики робити було обрано навчальні курси від компанії Cisco, а саме Introduction to Network, CCNP Enterprise: Core Networking в них проаналізовано та продемонстровано можливі елементи захисту мережі, приклади реалізації транкових каналів, розбиття мережі на VLAN, розбір протоколу Spanning tree protocol, ip routing.

Оскільки під час налаштування мережі буде використано динамічний протокол маршрутизації тому для більш детального розуміння було використано електронний ресурс "Налагодження та дослідження роботи протоколу маршрутизації EIGRP" в якому наведені приклади налаштування та загальна інформації про даний протокол.

Оскільки одним з видом налаштування програмного захисту мережі буде використано реалізація механізму AAA, тому для детального аналізу була використана стаття AAA Local Command Authorization на сайті NetworkLessons.com в якому наведені основні команди для налаштування AAA та тестування роботи, а також основні відомості про AAA.

Для віддаленого доступу на комутаторах та маршрутизаторах, а також швидкого та зручного налаштування пристроїв було проаналізовано джерело з назвою Configure SSH on Routers and Switches, в якому описано всі поняття, що стосуються SSH, а також команди за допомогою яких можна провести налаштування на пристроях.