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

НЕОБХІДНІСТЬ РОЗРОБКИ ПРОЕКТУ КОРПОРАТИВНОЇ ЛОКАЛЬНОЇ ПІДМЕРЕЖІ З ВИКОРИСТАННЯМ РІЗНИХ ТЕХНОЛОГІЙ ЗАХИСТУ

У наші дні інтернет став невід'ємною частиною нашого життя, він з'єднує людей по всьому світу та дозволяє залишатися на зв'язку зі своїми друзями, родичами та колегами. Сучасне життя зупиниться без інтернету, оскільки він допомагає здійснювати торгові операції онлайн, керувати банківськими рахунками, оплачувати рахунки за газ або електрику і посилати електронні повідомлення.

Для забезпечення зв'язку у всіх куточках нашої планети локальні мережі різних компаній та підприємств об'єднуються в глобальну, надаючи доступ до своїх ресурсів одне одному. Звісно не уся інформація повинна бути доступної, також з'являється необхідність захисту цієї інформації від несанкціонованого доступу.

Забезпечення мережевого захисту є одним з найскладніших завдань у сфері захисту інформаційних та комунікаційних систем. Більшість сучасних систем має розподілену структуру, в основі архітектури яких лежить використання мережевих технологій. Для забезпечення розмежування та захисту даних використовується підходи та технології.

Наприклад, для забезпечення екранування використовуються програмні та апаратні рішення розмежування доступу між різними підмережами більш глобальнішої мережі, все це забезпечує відстеження вхідного і вихідного мережевого трафіку та вирішення питань дозволу чи блокування певного трафік на основі визначеного набору правил безпеки. Брандмауер може бути апаратним, програмним, програмним як послугою (SaaS), публічною хмарою або приватною хмарою. Не менш важливим є вирішення питань локального захисту пристрої мережі, адже захист від внутрішніх атак стоїть на рівні зовнішніх.

У наші дні значна увага приділяється зовнішнім атакам, а питання внутрішньої безпеки, на жаль, залишаються відкритими. Для забезпечення такого роду безпеки використовується різні види захисту комутаційних пристроїв мережі. Після вирішення питань безпеки пристроїв мережі постає питання віддаленого доступу до них. Доступ до пристроїв може виконуватися на основі розробки серверного рішення AAA, що надасть контроль доступу до комп'ютерних ресурсів, забезпечить виконання політик і перевірку використання на базі процесів аутентифікації, авторизації та аудиту. AAA та його комбіновані процеси відіграють важливу роль в управлінні мережею та кібербезпеці, перевіряючи користувачів і відстежуючи їхню активність, коли вони підключені. Таким чином можна не допустити зловмисників, які зловживають своїми привілеями, відстежуючи їх діяльність. Все це надає адміністраторам цінну інформацію про їхню діяльність та контроль над їхніми діями. Поєднання усіх вище наведених пунктів забезпечать безпеку локальної мережі та її стабільну роботу.

Після визначення усіх необхідних підходів та методів забезпечення захисту мережі необхідно перейти до проектування самої локальної мережі. Даний процес включає в себе такі основні пункти: визначення кінцевих потреб та розрахунок адресного простору, побудова схеми окремих підмереж вирішення питань адресування та маршрутизації, визначення з апаратним забезпеченням на основі вхідних даних, побудова мережі, налаштування мережі включно з забезпеченням захисту та процесів AAA, перевірка роботи та безпеки створеної мережі.

В процесі аналізу літератури було досліджено підручник автора Кулакова Ю.О під назвою "Комп'ютерні мережі". Дане джерело описує основні аспекти розробки комп'ютерних мереж, їх покрокове дослідження, проектування та побудову. Наступним джерелом є електронний ресурс "CCNA Routing and Switching: Connecting Networks" [1]. Цей курс зосереджений на технологіях комутації та роботі маршрутизаторів, які підтримують мережі малого та середнього бізнесу, включаючи бездротові локальні мережі (WLAN) і концепції безпеки. Також даний курс описує базову конфігурацію мережі та усунення несправностей, виявлення та пом'якшення загрози безпеки локальної мережі. Далі було розглянуто електронний ресурс "Cisco Network Security Master Class", який описує основні пункти підтримки цілісності, конфіденційності і доступності даних і пристроїв. В нього входять наступні пункти дослідження: концепції безпеки, безпечний доступ, VPN, безпечна маршрутизація та комутація, технології брандмауера Cisco, IPS. Також одним з розглянутих джерел було "Cisco Switching, Routing, and Wireless Essentials Course". Цей ресурс описує роботу з маршрутизаторами, комутаторами та бездротовими пристроями для налаштування та усунення несправностей VLAN, бездротових локальних мереж і маршрутизації між VLAN. Також описано налаштування та усунення несправностей резервування в комутаційній мережі за допомогою STP і EtherChannel.