УДК 621.382

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В МЕРЕЖІ ПІДПРИЄМСТВА НА ОСНОВІ МЕТОДІВ ЯКОСТІ ОБСЛУГОВУВАННЯ

Бондар О.Р., Верес Л.А.
Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: sashashel@gmail.com

Developing security recommendations for the enterprise network based on quality of service methods

The article discusses the requirements for a modern enterprise network and characteristics of this network. Proved the importance of ensuring an adequate level of security in enterprise network. Described the concept of security and quality of service. Provided a method for protecting enterprise network using the Fail2ban software package.

У статті розглядаються вимоги до мережі сучасного підприємства, надається характеристика такої мережі. Обґрунтовується важливість забезпечення належного рівня безпеки в такій мережі. Надано опис поняття безпеки і якості обслуговування. Наведено метод захисту такої мережі з допомогою програмного пакету Fail2ban.

Сучасні мережі, незалежно від їх розміру, вимагають чіткого дотримання норм їх побудови. Вони повинні підтримувати велику кількість додатків і послуг, а також пристроїв з яких складається фізична інфраструктура. Основною функцією мережі є забезпечення доступу до ресурсів всіх пристроїв об’єднаних в мережу. Вимоги до мережі можуть бути різними в залежності від того де саме вона проектується і для кого. Великі підприємства потребують надзвичайно громіздких мереж з максимальним рівнем захисту і безліччю послуг які зменшують вартість обслуговування, полегшують адміністрування, або ж просто необхідні для успішного ведення бізнесу. В той же час для малих підприємств немає дуже суворих вимог до якості виконання мережі. Повільна робота такої мережі не буде мати таких катастрофічних наслідків у порівнянні з мережею великого бізнесу. Незважаючи на це, належне забезпечення безпеки є необхідним завданням в будь-якій мережі.

Ціль дослідження, запропонувати нетипові рішення для покращення рівня захисту мережі базованої на Linux-системі. Такі рішення зазвичай роблять злам мережі більш складним для потенційного зловмисника, так як є незвичайними і неочікуваними.

Безпека - найважливіша з вимог до мережі саме для підприємств,

особливо для великих. Мережа великої компанії обов'язково повинна бути захищена, так як, вона містить в собі важливу, часто навіть секретну, корпоративну інформацію. Зловмисники легко можуть вдертися в незахищену мережу, викрасти дані, привести мережу в неробочий стан і тим самим зірвати нормальну роботу підприємства, що призведе до значних збитків. Можна виділити два типи проблем з безпекою мережі: безпека мережевої інфраструктури і безпека інформації. Забезпечення безпеки інфраструктури означає захист всіх пристроїв, що забезпечують підключення до мережі, і попередження несанкціонованого доступу до програмного забезпечення керування, встановленого на них. Безпека інформації означає захист пакетів з даними, що передаються по мережі, а також захист інформації, що зберігається на пристроях користувачів. Для захисту інформації існує три основні вимоги: конфіденційність, цілісність і доступність. Інформація повинна бути доступна тільки авторизованим користувачам, інформація не повинна бути змінена або спотворена, до інформації повинен бути своєчасний і надійний доступ[1].

Якість обслуговування, поруч з безпекою, є основною темою даної роботи. По суті своїй, цей термін означає пріоритизацію трафіку. Тобто певні типи даних мають вищий пріоритет і передаються швидше. Для чого це необхідно. Якщо попит на канали зв'язку перевищує можливості мережі виникає перевантаження каналу. Коли таке трапляється, пакети не можуть одразу потрапити в канал передачі. Пристрої маршрутизації ставлять такі пакети в чергу в буфері пам'яті, до тих пір, доки канал не звільниться. Користувач в цей момент спостерігає велику затримку між запитом, наприклад до серверу, і відповіддю. На практиці це означає, що користувач змушений гаяти час не непотрібне очікування. Для деяких випадків такі затримки допустимі, а от для інших зовсім навпаки. Це не критично, якщо доведеться декілька секунд почекати доки завантажиться поштовий клієнт. Проте такі затримки фатальні при передачі голосового або відео трафіку. Щоб такого не траплялося, якість обслуговування визначає певні типи трафіку які мають вищий пріоритет над іншими. Пакети з голосовим або відео трафіком завжди будуть першими в черзі на передачу, навіть якщо прийшли ну вузол останніми і опинились в кінці довгої черги[2].

Тепер слід більш детально розглянути поняття мережі підприємства. Мережа підприємства – це сукупність мереж і служб, призначених для надання захищеного мережного простору користувачам в межах підприємства[3]. Основними особливостями мережі підприємства є:

1) Ті ж самі засоби управління, що використовуються в мережах загального користування.

2) Доступ до інформації надається тільки обмеженій групі користувачів всередині локальної мережі підприємства. Ця локальна мережа відділена від глобальної мережі міжмережевими екранами.

3) Всередині мережі інформація поділяється на три типи. Офіційна (розповсюджується на рівні організації), групова(призначена для використання групою осіб), неофіційна(особиста інформація працівників).

4) Наявність централізованої системи керування мережею.

Узагальнена структура мережі підприємства представлена на рис.1.

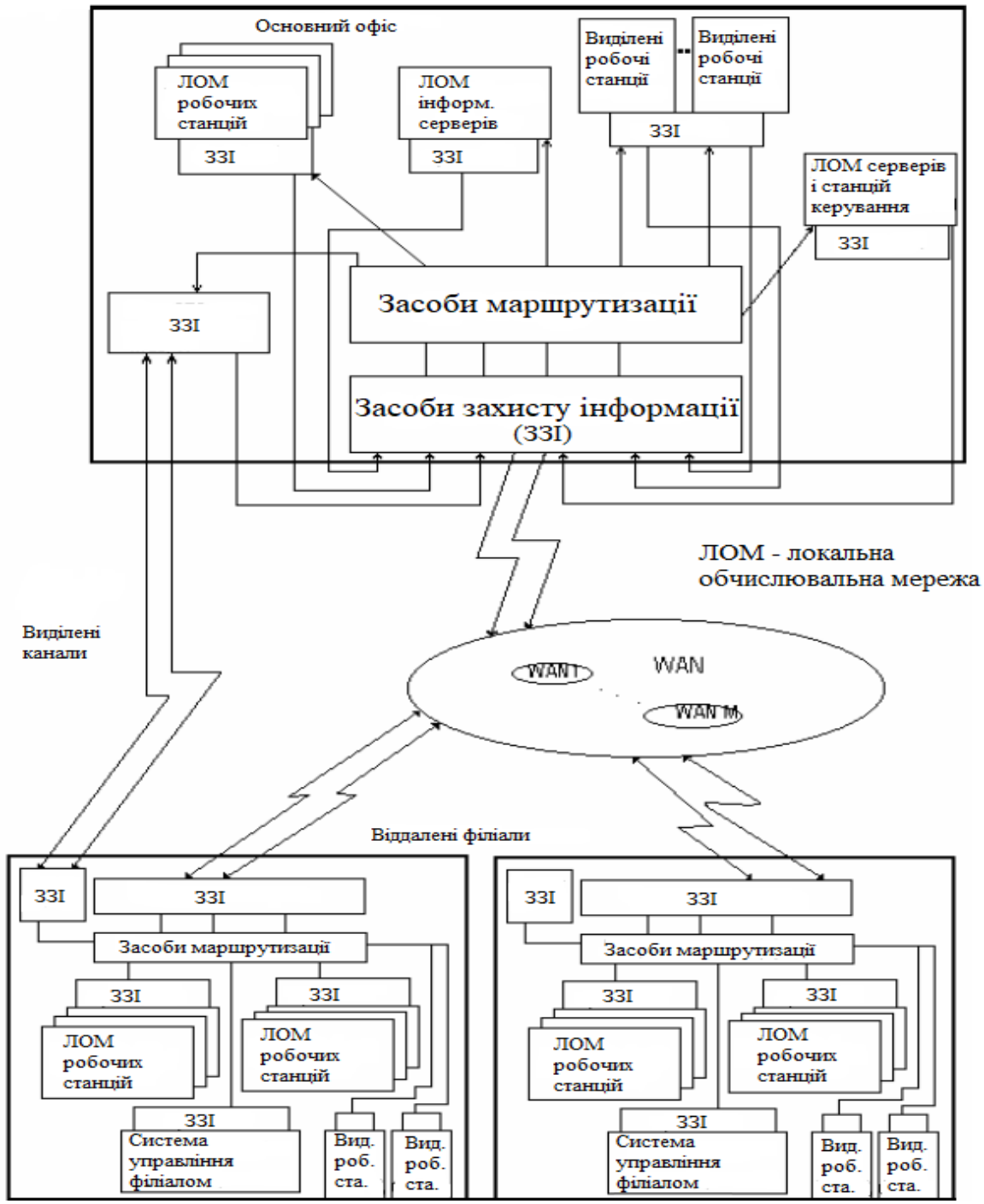

Рис.1. Узагальнена структура мережі підприємства.

Захист одного вузла мережі, як і всієї мережі, підключених до мережі Інтернет, від зовнішніх загроз, зазвичай не обмежується якимось одним апаратним або програмним засобом. Для забезпечення надійного захисту застосовуються комплекси які складаються з окремих програмних засобів. Такий спосіб є більш гнучким і дозволяє варіювати ступінь і рівень захищеності. В даній роботі буде застосовуватись захисний комплекс Fail2ban – програмний пакет, призначений для виявлення і запобігання спроб вторгнення в систему підключену до мережі. Fail2ban для своєї роботи використовує мережевий екран – firewall. В Linux-системі це iptables. Як варіант можна скористатися іншою підсистемою керування і відслідковування мережевих пакетів. Fail2ban виявляє і блокує окремі IP адреси з яких проводяться спроби несанкціонованого доступу до мережі. Ці адреси виявляються шляхом моніторингу файлів журналу – log-файлів. Це дозволяє захистити мережу або вузол мережі від «brute force» атак[4].

Описаний метод дозволяє підвищити рівень захищеності мережі підприємства. Він чудово доповнює існуючі методи захисту, ставлячи перед зловмисниками, додаткові складнощі при спробі злому мережі. Цей метод рекомендується застосовувати на приграничному маршрутизаторі мережі або безпосередньо на вузлі, що потребує захисту(наприклад сервер). Є сенс користуватись цім методом у всіх мережах, що мають доступ до мережі Інтернет.

Література

1. https://www.csoonline.com/article/3285651/what-is-network-security-definition-methods-jobs-and-salaries.html.
2. https://searchunifiedcommunications.techtarget.com/definition/QoS-Quality-of-Service.
3. Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2004. - 161 с.
4. https://www.ibm.com/developerworks/ru/library/l-fail2ban_01/index.html.