

АНАЛІЗ МЕХАНІЗМІВ БЕЗПЕКИ В БАНКІВСЬКІЙ ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ЗА РАХУНОК VPN

*Волинський А.В., студент, mandarin1@mail.ua;
ДонНТУ, м.Покровськ, Україна*

Історично склалося, що більшість питань захисту інформації в банках вирішувалося контролем фізичного доступу співробітників до певних інформаційних ресурсів (комп'ютерів, принтерів, документам). Але сьогодні питання з інформаційної безпеки вже не можуть бути вирішені таким підходом, оскільки:

- неможливо забезпечити фізичний контроль над лініями зв'язку, які лежать поза стінами банку;
- атака може здійснюватися з будь-якої точки планети;
- спектр можливих атак на інформацію надзвичайно широкий;
- відмова відправника від факту відправки / авторства інформації;
- атакуючий може отримати контроль над внутрішніми ресурсами банку, блокувати канали, здійснювати комплексні атаки;
- факт здійснення атаки може залишитися невідомим.

Надійний захист інформації, що передається по будь-яким мережам можливий тільки криптографічними методами (шифруванням). Однак, захисту інформації на рівні шифрування файлів, електронної пошти та окремих додатків вже недостатньо. Зростаючі потреби банківського бізнесу вимагають систем захисту, здатних "на льоту" захистити канали між будь-якими клієнт-серверними та інтернет-додатками, ізолювати онлайнові платіжні системи, забезпечити захищений зв'язок із зовнішніми клієнтами банку. Ці та багато інших завдань можуть бути успішно вирішені за допомогою технології віртуальних захищених мереж (VPN - Virtual Private Networks). На ринку існує безліч VPN систем, що відрізняються підходами до організації захисту, розповсюдженими стандартами. При виборі такої системи необхідно звернути увагу на декілька аспектів, що описують основні характеристики VPN систем і на задачі які вони вирішують.

Найбільш широко використовується VPN стандарт IPSec. Він передбачає прозоре шифрування потоку інформації "на виході". При правильній реалізації стандарту IPSec додатки і користувачі банку продовжать звичну роботу в мережі, не помічаючи, що інформація, яка передається/отримується проходить етап шифрування/дешифрування. У цьому випадку створення VPN не зупиняє робочий процес і не вносить змін в використовуванні прикладної системи. VPN можна розглядати як захищену інформаційну "трубу" між двома або більше комп'ютерами, які беруть участь в інформаційному обміні. Ці "труби" потім можуть бути прокладені через потенційно небезпечні мережі. VPN здатна ефективно вирішувати два завдання: захист зовнішніх каналів і захист внутрішніх мереж.

На практиці організація захищеного каналу зв'язку між офісами банку найчастіше вирішується шляхом створення власних виділених каналів. Але навіть таке дороге рішення не витримує жодної критики - адже ці канали проходять по неконтрольованій банком території, через обладнання різних провайдерів. Найчастіше використовуючи основний протокол Internet - TCP/IP. В більшості випадків такі канали є частиною Internet, а отже і мають типові проблеми, зокрема у питанні безпеки. VPN вирішує проблему контролю на всій довжині каналу. Наприклад, можна підключити в кожному місті локальні мережі філій банку до місцевого провайдера Internet. Потім встановити на прикордонному з Internet комп'ютері кожної філії програмне забезпечення, яке виконує шифрування інформації, що проходить. Важливо, щоб VPN дозволяла встановити відповідне програмне забезпечення на окремі комп'ютери співробітників, що мають право доступу до локальних мереж. На малюнку 1 схематично представлена мережа VPN, що дозволяє створити захищені канали через громадські (публічні) комп'ютерні мережі.

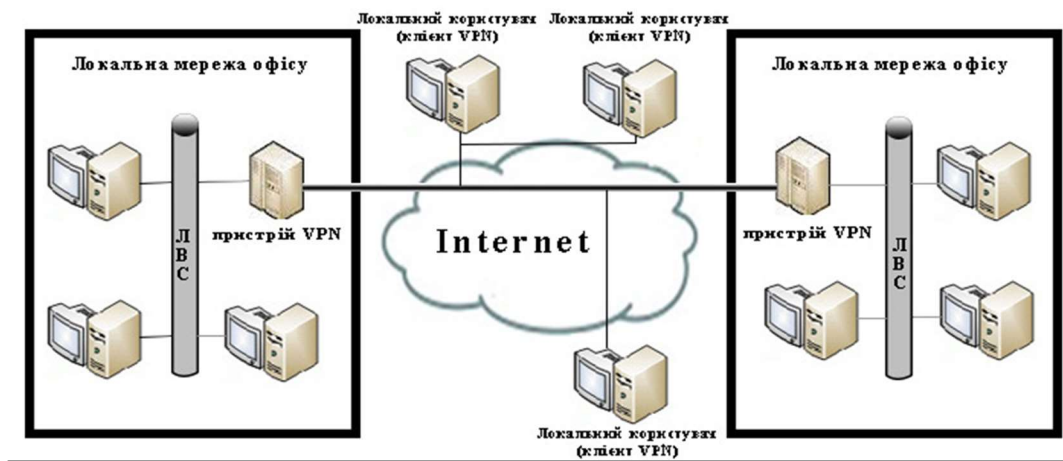


Рисунок 1. VPN через відкриті мережі та Internet

Таким чином, можна отримати свою власну захищену мережу (VPN), накладену на загальнодоступні.

VPN дозволяє розділити інформаційні потоки різних підрозділів банку. При цьому нова сегментація буде відображати тільки структуру бізнес-процесів і не буде залежати від конкретної топології внутрішніх локальних мереж. На рис. 2 показана можлива схема реалізації такого підходу. За допомогою VPN створені три логічно розділені віртуальні мережі. Перша VPN включає 3 комп'ютери і знаходиться цілком в локальній мережі підприємства. Друга частково виходить в зовнішні мережі, забезпечуючи доступ до інтернет-сервера оператору з локальної мережі і трьом клієнтам банку, підключеним через Internet. Третя VPN забезпечує співробітнику захищений доступ з дому до свого робочого комп'ютера і комп'ютера, наприклад, секретаря через модемний вхід сервера доступу. Всі користувачі VPN можуть бути впевнені, що їх інформація доступна заданому колу учасників взаємодії незалежно від їх місцезнаходження (всередині або зовні) і способу доступу до мережі.

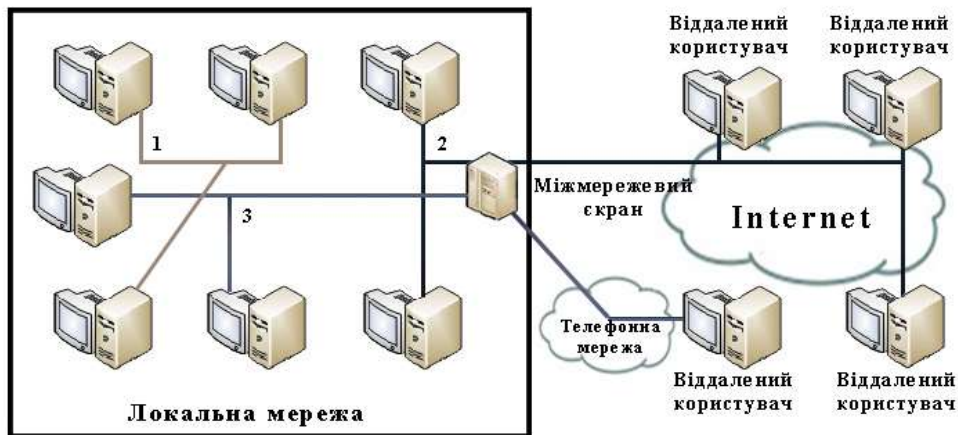


Рисунок 2. Сегментація внутрішніх мереж банку за допомогою VPN

Основним завданням VPN є шифрування трафіку, надійність якого визначається двома функціональними характеристиками. Перша полягає в стійкості використовуваних алгоритмів. Найбільш надійний захист будуватиметься тільки на перевірених часом і фахівцями алгоритмах, затверджених в міжнародних, державних і галузевих стандартах. Виключно небезпечно покладатися на системи, надійність яких базується тільки на тому, що їх автори ніколи не розкривають суті і коду своїх алгоритмів. В сучасній криптографії вся секретна частина захисту захована не в знанні коду алгоритму, а в наявності ключа. Друга характеристика - довжина ключа. Зазначимо, що мінімально розумною довжиною ключа вважається 128 біт.

Література

1. Браун С. Виртуальные частные сети. — М.: Лори, 2001. — 508 с.
2. Аллен Д. Следующая волна VPN на базе IP // LAN. 2001. № 3. — С. 86-95.

Анотація

Розглянуто недоліки існуючих механізмів безпеки в банківських телекомунікаційних мережах. Проведено аналіз внутрішніх і зовнішніх завдань захисту інформації з використанням технології віртуальних приватних мереж.

Ключові слова: VPN, захист інформації, локальні мережі.

Аннотация

Рассмотрены недостатки существующих механизмов обеспечения безопасности в банковских телекоммуникационных сетях. Проведен анализ внутренних и внешних задач защиты передаваемой информации с использованием технологии виртуальных частных сетей.

Ключевые слова: VPN, защита информации, локальные сети.

Abstract

The article examines the shortcomings of existing security mechanisms in banking telecommunication networks. The analysis of internal and external information transmitted protection tasks by using virtual private network technology.

Keywords: VPN, data protection, local area networks.