

## **ЗАЩИТА ГОЛОСОВЫХ СОЕДИНЕНИЙ ОТ ПРОСЛУШИВАНИЯ**

Прослушать чужие разговоры при передаче голоса по IP намного проще, чем в случае классической телефонии. Это утверждение касается и корпоративных сетей, но в первую очередь относится к соединениям через Internet. Конечно, для обеспечения конфиденциальности можно применять те же методы, что и при защите традиционной передачи данных, а именно — шифрование или VPN. Однако их внедрение должно отвечать специальным требованиям к качеству голосовой связи.

Сигнальные и голосовые пакеты необходимо изолировать. Для этого существует масса возможностей, выбор которых зависит от предполагаемой среды передачи — Internet, Intranet, Extranet, а также совместимость брандмауэров с VoIP и VPN.

Под Intranet понимают частную сеть IP, по размерам и покрытию сравнимую с классической телекоммуникационной системой. Если применяется единая сеть с концентраторами, то данные сигнализации, а также соответствующие голосовые данные доступны на каждом порту. Подслушивающее устройство или самопрограммируемый инструмент можно установить в любом месте сети и прослушивать все данные.

В общедоступной сети Internet пользователь практически не может влиять на маршрут пакета. Теоретически на любом узле необходимые пакеты можно скопировать. По сравнению с мультиплексорами и телефонными коммутаторами для голосовой связи, узлы Internet защищены хуже. Хакеры уже взламывали их, после чего могли манипулировать всеми проходящими через узлы пакетами или копировать их. Кроме того, закон о телекоммуникациях требует, чтобы спецслужбы имели возможность прослушивания в рамках оперативно-розыскной деятельности.

Технология VoIP сама по себе достаточно незащищена и предоставляет множество возможностей для атаки. Однако в Intranet, да еще на базе коммутируемой сети, многие слабые места уже устранены. При помощи специализированного аппаратного шлюза VPN можно установить защищенную связь между офисами. Однако шлюз VPN не должен быть реализован в виде программного обеспечения на брандмауэре, поскольку в таком случае вариация времени задержки будет зависеть не только от нагрузки процессов VPN, но и от общего трафика данных.

*Научный руководитель – д-р., проф., В.В. Козловский*