УДК 681.324

Обеспечение безопасности беспроводных локальных сетей

Белова С.В.
Белорусский национальный технический университет

В беспроводной локальной сети несанкционированный доступ можно осуществить гораздо проще, чем в проводной, достаточно оказаться в зоне распространения радиоволн этой сети. Для этого существует множество готовых программных средств, например, AirMagnet или AiroPeek. Используя их можно полностью раскрыть содержимое пакетов данных. Для серьезной атаки на беспроводную сеть используются узконаправленные антенны типа randome или parabolic.

В наиболее распространенном на сегодня стандарте беспроводных локальных сетей 802.11 предусмотрены средства безопасности, которые повышают защищенность беспроводной сети до уровня обычной проводной. Поэтому основной протокол защиты данных в сетях 802.11 так и называется — **WEP** (Wired Equivalent Privacy — секретность, эквивалентная проводной).

Однако алгоритмы аутентификации и шифрования, определенные в стандарте 802.11 имеют множество недостатков. Система аутентификации, так же как алгоритм WEP-шифрования, могут быть взломаны за короткое время.

Чтобы обеспечить защищенность, масштабируемость и управляемость беспроводных сетей, IEEE разработал улучшенный механизм аутентификации и шифрования. Эти изменения были введены в проект стандарта 802.11i. На сегодняшний день проект 802.11i не утвержден как стандарт, поэтому Альянс Wi-Fi (Wi-Fi Alliance) собрал поднабор компонентов, соответствующих стандарту 802.11i, который получил название "защищенный доступ к Wi-Fi" (Wi-Fi Protected Access, WPA).

Был предложен временный протокол целостности ключа (temporal key integrity protocol, TKIP), который обещает ликвидировать недостатки WEP-шифрования и системы аутентификации в краткосрочной перспективе, а стандарт 802.1X и AES предоставят долговременное решение проблемы безопасности беспроводных локальных сетей.