

При относительно плохих условиях РРВ от АУ к БС (условиях затенения мест скопления абонентов зданиями) суммарная интенсивность ЭМП, создаваемая электромагнитным излучением АУ, может достигать $0,08 \text{ Вт/м}^2$. Предельно допустимый уровень ЭМП сотовой связи, ограничивающий вынужденный риск для здоровья населения, в Республике Беларусь составляет $0,1 \text{ Вт/м}^2$. При $\rho_{MS} = 0,16 \text{ АУ/м}^2$ верхняя граница диапазона суммарной интенсивности ЭМП, создаваемого электромагнитным излучением АУ, составляет $0,06 \text{ Вт/м}^2$. В случае нахождения АУ в прямой видимости с ближайшей БС этот уровень снижается до $0,001 \text{ Вт/м}^2$.

Таким образом, при относительно плохих условиях РРВ от АУ к БС в местах скопления абонентов излучение АУ в активном состоянии может вносить существенный вклад в общий уровень ЭМП, создаваемый многими другими источниками электромагнитного излучения.

ПРОТОКОЛ ЗАЩИТЫ ТРАНСПОРТНОГО УРОВНЯ

М.А. Севостьянюк, А.С. Шелягович

Протокол TLS шифрует интернет-трафик любого вида, тем самым делая безопасными общение и транзакции в сети. Если ваши данные не шифруются, любой может проанализировать их и прочесть конфиденциальную информацию. Кроме веб-трафика, TLS также используется в почте и системах телеконференций. TLS использует самый безопасный метод шифрования – асимметричный. Так как в асимметричном шифровании применяются сложные математические расчеты, нужно много вычислительных ресурсов, поэтому TLS решает эту проблему, используя шифрование только в начале сессии, чтобы зашифровать общение между сервером и клиентом. Сервер и клиент должны договориться об одном ключе сессии, который они будут вдвоем использовать, чтобы зашифровать пакеты данных. Основной целью создания данного протокола являлось получение относительно безопасного канала для осуществления покупок или управления банковским счетом. В современном Интернете на TLS полагаются не только в коммерческой деятельности, но и при решении гораздо более общей задачи сохранения приватности и конфиденциальности важной информации. Одним из самых распространенных применений TLS является HTTPS. HTTPS стремительно вытесняет незащищенную версию (HTTP): доля зашифрованного веб-трафика растет, скорее всего, в скором будущем ожидается, что, практически весь веб-трафик будет зашифрован. Сегодня SSL/TLS – один из самых изученных, исследованных протоколов современного Интернета. Ключевым отличием TLS от SSL является наличие поддержки целого ряда расширений протокола, позволяющих реализовать современные методы защиты информации. На сегодняшний день TLS 1.2 является самой распространенной версией протокола. В новой версии TLS 1.3 будет совместимость с предыдущими версиями: например, соединение откатится до версии TLS 1.2, если одна из сторон не сможет использовать более новую систему шифрования в списке разрешенных алгоритмов протокола версии 1.3. Однако при атаке типа активного вмешательства в соединение, если хакер принудительно попытается откатить версию протокола до 1.2 посреди сессии, это действие будет замечено, и соединение прервется. Версия 1.3 протокола TLS, которая скоро будет выпущена, решает множество проблем с уязвимостями тем, что отказывается от поддержки устаревших систем шифрования [1, 2].

Литература

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на языке С. М.: ЗАО Компьютерное издательство «Диалектика», 2016. 221 с.
2. Бабаш А. Криптографические методы защиты информации. Т. 1. М.: Инфра-М, 2013. 124 с.

ОСОБЕННОСТИ ФОРМИРОВАНИЯ РЕЧЕПОДОБНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ НА КАЗАХСКОМ ЯЗЫКЕ

Е.Н. Сейткулов, А.В. Потапович, Г.В. Давыдов, В.А. Попов

Методы формирования речеподобных сигналов на русском и белорусском языках рассматриваются в работах [1–3]. Для формирования речеподобных последовательностей на казахском языке за основу можно использовать метод синтеза речеподобных сигналов