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 Вт/м^2. Предельно допустимый уровень ЭМП сотовой связи, ограничивающий вынужденный риск для здоровья населения, в Республике Беларусь составляет 0,1 Вт/м^2. При ρ_{MS} = 0,16 АУ/м^2 верхняя граница диапазона суммарной интенсивности ЭМП, создаваемого электромагнитным излучением АУ, составляет 0,06 Вт/м^2. В случае нахождения АУ в прямой видимости с ближайшей БС этот уровень снижается до 0,001 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 прочитать 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

на русском и белорусском языках. Особенности формирования речеподобных последовательностей на казахском языке связано с законом сингармонизма (гармонии гласных звуков и гармонии согласных звуков).

Для казахского языка в слове могут сочетаться только твердые, либо только мягкие гласные. Слова иностранного происхождения арабские, персидские и русские могут содержать как мягкие, так и твердые гласные. При формировании речеподобных последовательностей казахского языка использовалось ограничение на применение в одном слове (в корне слова и производных основах) либо мягких либо твердых гласных.

Для согласных звуков используется ассимиляция согласных по звонкости и глухости. Если последний звук корня слова глухой или оканчивается на звонкие *б, в, г, д,* то начальный согласный звук аффикса глухой. Если последний звук корня слова глухой согласный *қ, к, п*, а начальный звук аффикса гласный, то глухие *қ, к, п* переходят в *ғ, г, б*.

Звук *а* не употребляется в словах с гласными *ә, е, і, Ө, ү*, а также с мягкими согласными *г, к*. Звук *г* в начале и конце казахских слов, а также с гласными *а, о, у, ы* не употребляется. Его не употребляют в словах и в сочетании с твердыми согласными *ғ, қ*. *Л* в начале слова в казахском языке пишется, но не произносится, поэтому в речеподобных последовательностях она в начале слова не используется. Звук *о* в конце казахских слов не употребляется.

Указанные особенности казахского языка использовались при формировании речеподобных последовательностей, которые преобразовывались в акустические речеподобные сигналы для маскирования речи. Для защиты речевой информации путем ее маскирования рекомендуется использовать комбинированные помехи, включающие «белый» шум и речеподобные сигналы.

В работе рассматривается механизм формирования речеподобных последовательностей с использованием базы аллофонов казахского языка, а также базы суффиксов и окончаний.

При формировании базы структурных элементов казахского языка для синтеза речеподобных сигналов необходимо использовать статистические данные о частотности длины слов в казахском языке, частотности появления букв в начале слова и частотности появления букв в текстах на казахском языке. По формальным признакам речеподобные сигналы должны соответствовать статистическим характеристикам языка.

Работа выполнена при поддержке грантового финансирования КН МОН РК, № AP05130293.

Литература

1. Воробьев В.И., Давыдов А.Г., Давыдов Г.В. Речеподобные сигналы: разновидности, основные параметры, способы формирования, области применения // Доклады БГУИР. 2009. № 3 (41). С. 9–16.

2. Сейткулов Е.Н., Давыдов Г.В., Потапович А.В. База аллофонов для компиляционного синтеза речеподобных сигналов на русском языке // Современные средства связи: материалы XIX Междунар. науч.-техн. конф. Минск, 14–15 октября 2014 г. С. 193–195.

3. Синтез речеподобных сигналов на белорусском языке / Г.В Давыдов [и др.] // Доклады БГУИР. 2015. № 4. С. 27–32.

СОХРАНЕНИЕ ИНФОРМАЦИИ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ

А.С. Сиденко, В.П. Бурцева

Система охлаждения (СО) оборудования в центрах обработки данных (ЦОД) имеет сложную конструкцию. Первым, можно сказать, основным недостатком этой СО является ее ненадежность в вопросе защиты информации. Так как в случае отключения электроэнергии СО дает сбой, что может привести к перегреванию серверов, а, следовательно, ставит под удар сохранение на них информации. Вторым недостатком СО в ЦОД является низкая теплопроводность охлаждающего вещества (воздуха), которая влечет за собой низкую эффективность охлаждения. Предложенный способ охлаждения серверов с помощью тепловых трубок (ТТ) одновременно устраняет эти два недостатка. ТТ представляет собой устройство, в основе которого лежит фазовый переход (жидкость–пар) и в настоящее время используется