РЕГИСТРАЦИЯ И ОБРАБОТКА БИОМЕДИЦИНСКИХ СИГНАЛОВ

Т.П. Куль

Для регистрации речевых сигналов используется следующее аппаратное обеспечение:

1. Беспроводная Bluetooth гарнитура с чувствительным микрофоном для записи речевых тестов. Беспроводная Bluetooth гарнитура обеспечивает: одинаковое расстояние от речевого аппарата всех испытуемых до записывающего устройства (микрофона), что позволяет в последствии анализировать абсолютные значения амплитуды речевого сигнала, а также его динамику в процессе теста; высокое качество записи речи при проведении диагностики; комфортные условия для испытуемых.

2. Мобильное устройство со специально разработанным мобильным приложением для воспроизведения испытуемому видеоряда с речевыми тестами и одновременной регистрацией данных с микрофона посредством Bluetooth-интерфейса.

Мобильное приложение работает на платформе Android и реализует следующие функции: демонстрация ранее описанного видеоряда с речевыми тестами; одновременная по отношению к воспроизведению видеоряда регистрация речевого сигнала через беспроводную Bluetooth гарнитуру; автоматическое сохранение записанных речевых сигналов в формате .wav; воспроизведение и удаление записи.

Далее записанный в единый файл речевой сигнал разделяется на отдельные речевые тесты и подвергается цифровой обработке посредством специально разработанного программного обеспечения в среде MatLab [1, 2].

Литература

1. Метод диагностики и контроля эффективности лечения бульбарных нарушений на основе цифровой обработки речевых сигналов / А.Н. Осипов [и др.] // Новости медико-биологических наук. 2017. Т.15, № 2. С. 65–75.

2. Цифровая обработка речевых сигналов в диагностике бульбарных нарушений. / А.Н. Осипов [и др.] // Материалы третьей Междунар. конф. «BIG DATA and Advanced Analytics. BIG DATA и анализ высокого уровня». Минск, 2017. С. 312–318.

ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ

С.Г. Кульгавик, П.М. Буй

В Республике Беларусь в последнее время наблюдается процесс стремительной информатизации и компьютеризации практически всех отраслей народного хозяйства. В рамках этого процесса на вооружение принимаются информационные системы – системы, предназначенные для хранения, поиска и обработки информации, которые, помимо прочего, включают человеческие, технические и прочие организационные ресурсы, взаимодействующие с информацией. Особое место занимают информационные системы, выполняющие функции автоматизированных систем управления технологическими процессами (АСУ ТП).

Вместе с тем процессы информатизации и компьютеризации, а также использование современных сетевых технологий таят в себе множество потенциальных опасностей, область реализации которых касается исключительно сферы высоких технологий. При отсутствии адекватной системы защиты опасности такого рода могут привести к нарушению штатной работы информационных систем, что особенно критично для АСУ ТП. В таких условиях обязательным является проведение анализа опасностей характерных как для самих информационных систем, так и для среды их функционирования.

Для защиты информационных систем от атак разрабатываются специальные мероприятия по обеспечению их безопасности, часть из которых обеспечивает их надежное функционирование в условиях воздействия угроз, часть направлено на обеспечение информационной безопасности, т. е. сохранению таких свойств защищаемой информации, как конфиденциальность, доступность и целостность.

В реальной среде функционирования любой информационной системы независимо от нее существует множество угроз его безопасности – возможных воздействий на систему, которые прямо или косвенно могут нанести ущерб ее безопасности. Следует разделять угрозы

функциональной и информационной безопасности исходя из функций информационных систем, на которые они нацелены.

Оптимальным методом анализа угроз является метод экспертных оценок, при котором экспертам предлагается оценить возможность реализации некоторого перечня угроз. В качестве критериев оценки опасности конкретной угрозы можно выбрать возможность возникновения источника угрозы, степень его готовности произвести атаку, а также фатальность для объекта от реализации угрозы.

При наличии множества уязвимостей информационной системы и множества угроз ее безопасности в реальных условиях функционирования велика вероятность реализации одной из угроз, нацеленной на процесс функционирования объекта или безопасность информации, которая в нем используется. Анализируя коэффициенты опасности совокупности уязвимостей, можно произвести их ранжирование и определить те из них, устранением которых необходимо заняться в первую очередь.

Для защиты информационных систем от атак разрабатываются специальные мероприятия по обеспечению их безопасности, часть из которых обеспечивает их надежное функционирование в условиях воздействия угроз, часть направлено на обеспечение информационной безопасности, т. е. сохранению таких свойств защищаемой информации, как конфиденциальность, доступность и целостность.

Учитывая многообразие угроз современного информационного мира, построить абсолютно адекватную систему защиты не представляется возможным, ведь затраты на ее организацию и сопровождение не должны превышать предполагаемый ущерб от ее нарушения в результате реализации угроз. Таким образом, необходимо выбрать методику, которая позволит выбрать наиболее опасные для исследуемой информационной системы угрозы и защищаться только от них. Также важным является определение наиболее опасных уязвимостей, устранение которых позволит существенно повысить уровень безопасности информационной системы.

В реальных условиях функционирования одна и та же уязвимость безопасности информационной системы может стать причиной реализации сразу нескольких угроз.

ЭЛЕКТРИЧЕСКИЕ СВОЙСТВА ГЕТЕРОСТРУКТУРЫ ОКСИД ТИТАНА–КРЕМНИЙ ПРИ ОБЛУЧЕНИИ СОЛНЕЧНЫМ СВЕТОМ

А.А. Курапцова

Диоксид титана (TiO_2) достаточно широко используется в разных устройствах фотовольтаики: в процессах фотокатализа, при фотолизе воды, очистке воздуха и воды от загрязнений, в том числе от тяжелых металлов и органических соединений. Также композитные материалы на основе диоксида титана находит применение для экранирования помещений от электромагнитного излучения и создания физических ультрафиолетовых фильтров.

Было проведено моделирование электрических параметров гетероструктуры оксид титана / кремний (n-TiO2/p-Si) с помощью программы PC1D 5.9. Толщина диоксида титана – 1 мкм, кремния – 5 мкм. Ширине запрещенной зоны оксида титана (анатаз) 3,2 эВ соответствует энергия кванта с длиной волны 388 нм, что попадает в ультрафиолетовую часть спектра. Получены зависимости скорости генерации носителей заряда от расстояния от фронтальной поверхности и вольт-амперные характеристики структуры n-TiO_2/p-Si для различных длин волн солнечного излучения (мощность излучения 0,06 Вт/см^2).

Сравнение зависимости тока короткого замыкания структуры от длины волны излучения со спектром солнечного излучения показало, что его максимум в гетероструктуре приблизительно соответствует максимуму мощности солнечного излучения.

Таким образом, проведенное моделирование электрических характеристик гетероструктуры показало, что ВАХ в условиях освещения солнечным светом характеризуется насыщением тока, величина которого нелинейным образом зависит от длины волны солнечного света. Ток короткого замыкания характеризуется максимумом при длине волны, соответствующей генерации носителей заряда в кремнии.

Полученные результаты необходимы для исследования электронных процессов, протекающих на поверхности оксида титана, которые обусловливают его фотокаталитические свойства.