ориентировалась веб-разработка. Сегодня распределенные веб-приложения заменяют монолитные десктопные во многих сферах бизнеса. Поэтому крайне важно соблюдать нормы защиты веб-приложений. Фреймворк Angular.js поставляется с предварительно настроенными стратегиями по обеспечению безопасности от JSON уязвимостей и XSRF атак.

JSON уязвимости дают возможность веб-сайту третьих лиц подменить ваш URL для ресурса JSON, на запрос JSONP при определенных условиях. Для защиты от данного вида атаки сервер добавляет префикс ")]}',n" для всех ответов на запросы в формате JSON. Angular.js будет автоматически вырезать префикс перед обработкой ответа в формате JSON.

CSRF – вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Смысл атаки заключается в выполнении нежелательных действий на сайте ом имени аутентифицированного там пользователя. Angular.js предоставляет следующий механизм защиты от CSRF. При выполнении запросов XHR сервис $http считывает токен из файла cookie (по умолчанию XSRF-TOKEN) и задает его в качестве заголовка HTTP (по умолчанию X-XSRF-TOKEN). Поскольку только JavaScript, который работает на вашем домене, может читать cookie, ваш сервер может быть уверен, что XHR пришел из JavaScript, работающего на вашем домене. При первом GET запросе сервер возрващает в файле cookie токен с именем XSRF-TOKEN. Последующие XHR запросы сервер способен проверить, сравнивая значение coockie и присланного HTTP заголовка X-XSRF-TOKEN, чтобы удостовериться, что запрос не подделанный. Токен должен быть уникальным для каждого пользователя.

**Литература**

1. The Cross-Site Request Forgery (CSRF/XSRF) [Электронный ресурс]. – URL http://www.cgisecurity.com/csrf-faq.html (дата обращения: 16.05.2018).

2. Официальная документация по AngularJS [Электронный ресурс]. – URL: https://docs.angularjs.org/api/ng/service/$http (дата обращения: 16.05.2018).

## ЭЛЕКТРОМИГРАЦИОННЫЕ ПРОЦЕССЫ В МЕЖСОЕДИНЕНИЯХ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

А.Г. Черных, В.В. Шульгов

Информационная безопасность требует совершенствования элементной базы микроэлектронных устройств защиты информации. По мере уменьшения размеров и совершенствования структуры микроэлектронных устройств возрастает роль многоуровневой системы межсоединений интегральных микросхем (ИМС) и основным ограничительным фактором в системе межсоединений является электромиграционная стойкость.

В работе представлены методы, которые позволяют провести оценку электромиграционной стойкости металлических межсоединений ИМС. Основные методы испытаний на стойкость к электромиграции условно можно разделить на испытания структур в составе корпуса (EM PLR) и испытания структур в составе пластины (EM WLR). При EM PLR испытания на электромиграцию проводятся в составе корпуса при постоянном токе и температуре К методам WLR–испытаний на отказ, вызванный электромиграцией, относят: изотермический тест (ISOT) и стандартный тест для ускорения электромиграции в структурах на пластине (SWET). Проведен анализ указанных методов, показано, что выбор метода зависит от задач, поставленных перед исследованиями.

Проведены исследования параметров электромиграции в межсоединениях ИМС на тестовых структурах с алюминиевой пленкой, а также сплавов Al+2%Cu и Al+1%Ho. После окончания электромиграционного теста структуры исследовали на оптическом и сканирующем электронном микроскопе, а микроструктуру пленок исследовали методом, основанном на дифракции обратно рассеянных электронов в электронном микроскопе. Проведенные исследования показали, что при наличии в алюминиевых пленках 2%Cu и 1%Ho приводит к малому порообразованию и следовательно к меньшему сопротивлению, чем в чистой алюминиевой пленке. Представлена корреляция полученных результатов для различных методов испытаний.