ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ И ТЕХНОЛОГИЯ eSIM

А.С. Шелков

Интернет вещей (IoT) – одно из самых развивающихся направлений в области информационных технологий и беспроводной связи. Одной из важных проблем в развитии данного направления является информационная безопасность (ИБ) инфраструктуры IoT. Инфраструктура IoT представляет собой совокупность устройств: датчиков, измерительных устройств, видеокамер, управляемых переключателей и т.д. Указанные компоненты, взаимодействуя между собой, или с внешней средой по определенным протоколам, образуют IoT. С момента создания концепции IoT отсутствовали жесткие ограничения и стандарты информационной безопасности устройств IoT, что делает небезопасным применение IoT для реальных задач. К основным слабым сторонам использования IoT относятся следующие пункты: питание датчиков, отсутствие единой стандартизации архитектуры и протоколов, отсутствие системы управления правами доступа, трудности обновления ПО, использование небезопасного ПО и др. Существенная часть этих недостатков может быть устранена применением технологии embedded SIM (eSIM) для устройств IoT. eSIM – технология, позволяющая виртуализировать модуль идентификации абонента (SIM): виртуальная SIM загружается через OTA-интерфейс на встроенный в мобильное устройство чип (eUICC). Идентификационные данные для виртуальной SIM предоставляются провайдером связи на узел SM-DP (Subscription Manager Data Preparation), который формирует профиль SIM-карты, впоследствии загружаемый и устанавливаемый в eUICC мобильного устройства. Применение этой технологии позволит реализовать следующие меры безопасности:

1) устройство становится частью сети сотового оператора, чем решается вопрос с аутентификацией;

2) провайдер услуг IoT может внедрить в профиль eSIM сканирующее ПО, которое может быть в дальнейшем использовано как часть IDS;

3) устройства с поддержкой eSIM должны проходить сертификацию GSMA;

4) появляется возможность обновления ПО устройства при помощи технологий OTA;

5) провайдер IoT может предоставлять специальных платформу для централизованного контроля и управления устройствами IoT для конкретных объектов.

Использование eSIM не решает всех вопросов ИБ, но позволит нивелировать самые критические уязвимости.

ПОДХОДЫ К БЕЗОПАСНОМУ КОНФИГУРИРОВАНИЮ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА WINDOWS

А.С. Шилов, О.В. Бойправ

Операционные системы семейства Windows имеют ряд схожих характерных черт, в частности, защитные технологии, что облегчает обеспечение их безопасности и отчасти сводит его к правильной конфигурации параметров безопасности системы администратором. Данные параметры могут быть классифицированы в зависимости от механизмов операционной системы, с которыми они связаны: параметры контроля учетных записей, параметры устройств, параметры сетевого доступа, параметры завершения работы, параметры аудита, параметры входа в систему и т.д.

К критически важным параметрам безопасности относятся, в первую очередь те, которые связаны с учетными записями. В связи с неограниченным числом попыток неверного входа для данной записи, следует отключать параметр «состояние учетной записи «Администратор»» на рабочих машинах рядовых пользователей сети, что не позволит использовать данную запись при обычном входе, а также отключить автоматический вход администратора в консоль восстановления. Также необходимо ограничивать возможности пользователей по добавлению новых учетных записей настройкой параметра «блокировать учетные записи Майкрософт» и использование встроенной учетной записи «Гость», отключив параметр «состояние учетной записи «Гость»». Также следует контролировать установку

приложений и повышение прав, запрашивая пароль от администратора, активировав соответствующий параметр. Среди дополнительных настроек можно выделить следующие:

– отключение необязательных подсистем, т.к. используемая по умолчанию подсистема допускает запуск процесса одним пользователем, а последующее – работу с процессом другого пользователя, что способствует сокрытию фактов несанкционированного доступа;

– включение аудита использования привилегии на архивацию и восстановление, т. к. при резервном копировании создается копия файловой системы, чем может воспользоваться злоумышленником.

АЛЮМООКСИДНЫЕ ОСНОВАНИЯ С ПОКРЫТИЯМИ, МОДИФИЦИРОВАННЫМИ НЕОРГАНИЧЕСКИМИ ДИЭЛЕКТРИЧЕСКИМИ ПЛЕНКАМИ

Д.Л. Шиманович, Е.Д. Беспрозванный, Е.Е. Алясова

В результате проведенных исследований отработаны технологические методы формирования дополнительных диэлектрических пленок на пористых алюмооксидных основаниях с целью получения модифицированных многослойных структур, обладающих закрытой пористостью и приводящих к улучшению теплофизических и электрофизических свойств конечных диэлектрических покрытий на алюминиевых основаниях [1].

Отработаны режимы вакуумного осаждения на пористые алюмооксидные поверхности неорганических диэлектрических пленок трех видов: 1) Al_2O_3 из мишени поликора (ВК100-1); 2) SiO_2 из мишени кварца (С5-1); 3) композита на основе Al_2O_3, SiO_2 и MnO из мишени корундовой керамики (22ХС). Осуществлено теоретическое моделирование послойного осаждения и установлено, что для модификации пористой структуры осажденными диэлектриками (с перекрытием и захлопыванием пор) необходимо проводить напыление пленок толщиной ~300-2000 нм в зависимости от толщины анодного Al_2O_3 и диаметра пор. Установлена зависимость коэффициента теплопроводности многослойной структурной системы «несущий Al + анодный Al_2O_3 + осажденный диэлектрик» от толщины Al-оснований из сплава АМг-2 (в диапазоне ~ 1–3 мм), толщины анодного Al_2O_3 (в диапазоне ~ 50–100 мкм) и толщины осажденных диэлектрических пленок (~1000 нм и ~2000 нм). Выяснено, что значения параметра теплопередачи многослойных модифицированных покрытий возрастают при уменьшении толщины такой составляющей, как анодный Al_2O_3, а уплотнение осажденными диэлектриками позволяет увеличить значения коэффициента теплопроводности. Так для толщины пористого Al_2O_3 ~50 мкм значения коэффициента теплопроводности возрастают с ~82 Вт/м·К до ~91 Вт/м·К соответственно при увеличении значений толщины осажденного (из мишени поликора (ВК100-1)) Al_2O_3 от ~1000 нм до ~ 2000 нм, в то время как параметр теплопередачи для немодифицированного пористого Al_2O_3 такой же толщины (~ 50 мкм) в общей системе с Al (~ 2 мм) составляет ~ 52 Вт/м·К. Объяснение этого факта заключается в том, что исходная пористая Al_2O_3-структура содержит газовую фазу с воздушным наполнением и составляющей адсорбированных на стенках пор водяных паров, коэффициенты теплопроводности которых низкие, составляют ~ 0,022 Вт/м·К (для воздуха) и ~ 0,6 Вт/м·К (для воды) и отрицательно влияют на теплопроводность твердофазной алюмооксидной структуры.

Литература

1. Шиманович Д.Л. Технологические режимы формирования дополнительных диэлектрических пленок на пористой поверхности алюмооксидных оснований и исследование электрофизических и теплофизических характеристик модифицированных покрытий // Фундаментальные проблемы радиоэлектронного приборостроения. 2017. Т. 17, № 2. С. 573–576.

МЕТОДЫ ФОРМИРОВАНИЯ ТОПОЛОГИЧЕСКИХ ЗОН ОТКРЫТОГО ВЫХОДА НА АЛЮМИНИЕВЫХ ОСНОВАНИЯХ В ТОЛСТОСЛОЙНЫХ Al_2O_3-ПОКРЫТИЯХ

Д.Л. Шиманович, Е.Д. Беспрозванный, Е.Е. Алясова

Исследованы технологические методы толстослойного анодирования алюминия в локальных топологических областях при различных методах маскирования для