ТЕПЛОВАЯ СТАБИЛЬНОСТЬ АКУСТООПТИЧЕСКИХ ФИЛЬТРОВ

Е.Н. Наумович, В.И. Журавлёв, В.С. Колбун

Одним из методов защиты информации от несанкционированного доступа к физическому каналу беспроводных интерфейсов является преобразование сигналов, обеспечивающих высокую скрытность передачи, посредством многополосных акустооптических фильтров (АОТФ). В основе таких систем лежит принцип кодирования сигналов в спектральной области, когда последовательность Уолша представляется набором спектральных линий в сигнале с определенной последовательностью спектральных интервалов между ними. При работе АОТФ необходимо обеспечить тепловую стабильность кристаллов, что достижимо с использованием адекватных тепловых моделей.

В работе предлагается использовать тепловые модели АОТФ с распределенными параметрами и различной рассеиваемой мощностью вдоль акустического канала. Кристалл представляется как анизотропное тело с несколькими тепловыми источниками. Для расчета целесообразно использовать частное решение уравнения теплопроводности численными методами. Распределение акустической мощности по траектории ее распространения в кристалле является неравномерным и сильно зависит от геометрии кристалла и частоты волны. Результаты моделирования кристаллов указывают на наличие перегрева в области преобразователя АОТФ и увеличение неравномерности распределения температуры в объеме кристалла с течением времени. Это ведет ухудшение дифракционной эффективности к расфокусировке луча. При еще больших мощностях возрастает температура нагрева, и градиент в объеме кристалла усиливается. Это связано как низкой теплопроводностью материала кристалла, так и неравномерно распределенной выделяемой мощностью вследствие работы АОТФ.

РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА С ИСПОЛЬЗОВАНИЕМ FIREBASE AUTHENTICATION В ANDROID-ПРИЛОЖЕНИИ

Е.В. Пендо

Основой безопасной работы приложения является система аутентификации пользователей, позволяющая осуществлять разграничение прав доступа. Помимо разграничения по правам данная система также предоставляет возможность приложению безопасно сохранять пользовательские данные в облаке и обеспечивать одинаковую персонализированную работу на всех устройствах пользователя.

Аутентификация Firebase предоставляет backend-сервисы, простые в использовании SDK и готовые библиотеки пользовательского интерфейса для аутентификации пользователей в приложении. Firebase поддерживает аутентификацию с использованием паролей, телефонных номеров, учетных записей Facebook, Twitter, и многого другого [1].

Аутентификация Firebase тесно интегрируется с другими сервисами и использует отраслевые стандарты, такие как OAuth 2.0 и OpenID Connect [2].

Для использования Firebase Authentication с целью разграничения прав доступа необходимо создать Google Account, который будет использоваться для создания проектов в Firebase Console. После чего необходимо зарегистрировать Android-приложение в проекте, используя package name в качестве идентификатора. После успешного прохождения процедуры регистрации Firebase предоставляет файл конфигурации в формате json, который помещается в приложение. Последним шагом для использования Firebase Authentication в Android-приложении является добавление зависимостей для библиотеки в модули (уровень приложения и уровень модуля) [3].

Таким образом Firebase Authentication является оптимальным сервисом для разграничения прав доступа в Android-приложении, так как в нем используются отраслевые стандарты (OAuth 2.0 и OpenID Connect), а его интеграция занимает не более 10 минут ввиду наличия простых в использовании SDK и готовых библиотек.

Список литературы

1. Firebase Authentication // Firebase [Электронный ресурс]. URL: https://firebase.google.com/docs/auth/ (дата обращения: 06.04.2019).

2. Get Started with Firebase Authentication on Android // Firebase [Электронный ресурс]. – URL: https://firebase.google.com/docs/auth/android/start (дата обращения: 06.04.2019).

3. Add Firebase to your Android project // Firebase [Электронный ресурс]. URL: https://firebase.google.com/docs/android/setup (дата обращения: 06.04.2019).

МЕТОДИКА ИЗГОТОВЛЕНИЯ ГИБКИХ ЭЛЕКТРОМАГНИТНЫХ ЭКРАНОВ НА ОСНОВЕ ПОРИСТЫХ ПОРОШКООБРАЗНЫХ МАТЕРИАЛОВ

Д.И. Пеньялоса, М.В. Тумилович

Авторами предложена методика изготовления гибких электромагнитных экранов на основе пористых порошкообразных материалов. Она включает в себя следующие этапы.

Этап 1. Раскрой пенополиуретановых пластин и полиэтиленовой сетки на фрагменты.

Этап 2. Нарезка алюминиевой пленки на фрагменты, длина и ширина которых не превышают 1 см.

Этап 3. Изготовление водного раствора $CaCl_2$ с максимальной концентрацией.

Этап 4. Пропитывание изготовленным водным раствором порошкообразного пористого материала (активированного угля, электрокорунда, перлита т. п.).

Этап 5. Размещение фрагмента полиэтиленовой сетки на фрагменте пенополиуретановой пластины.

Этап 6. Нанесение влагосодержащего пористого порошкообразного материала на фрагмент полиэтиленовой сетки, размещенный на фрагменте пенополиуретановой пластины.

Этап 7. Размещение фрагмента полиэтиленовой сетки на слое из влагосодержащего порошкообразного древесного угля.

Этап 8. Равномерное распределение фрагментов алюминиевой пленки, полученных в результате реализации этапа 2, на фрагменте полиэтиленовой сетки, размещенном поверх слоя влагосодержащего порошкообразного древесного угля.

Этап 9. Размещение фрагмента пенополиуретановой пластины поверх фрагментов алюминиевой пленки.

Этап 10. Герметизация полученной конструкции посредством полиэтилентерефталатной пленки.

Преимущества предложенной методики заключаются в быстроте ее реализации, а также в том, что изготовленные в соответствии с ней электромагнитные экраны характеризуются пониженной массой, ввиду того, что не содержат связующих веществ, используемых для фиксирования частиц порошкообразных материалов.

Электромагнитные экраны, изготовленные в соответствии с предложенной методикой, могут быть использованы для электромагнитного экранирования помещений, в которых располагаются средства обработки информации.

МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ ТРЕБОВАНИЯМ СТБ 34.101.73-2017

И.И. Печень

Деятельность по оценке соответствия средств защиты информации является одним из основных механизмов управления информационной безопасностью государства. В рамках представляемой работы выполнены испытания маршрутизатора Cisco ASR 1001, в котором предусмотрена функция межсетевого экранирования, на предмет соответствия требованиям СТБ 34.101.73-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Межсетевые экраны. Общие требования». Испытания выполнены в соответствии с предложенной методикой, включающей в себя следующие шаги.