реакции окисления пористого кремния производилось инфракрасным и ультрафиолетовым лазерами. Так оптическое инициирование осуществляли излучением Nd^{3+}:$YAlO_3$ лазера с модулированной добротностью ($\lambda = 1080$ нм, $\tau = 15$ нс) или излучением его третьей гармоники ($\lambda = 360$ нм). Плотность мощности светового потока варьировалась от 20 до 150 МВт/см^2. Проведенные исследования показали, что процессы быстрого окисления в пористом кремнии могут быть инициированы одиночным световым импульсом лазера. Пороговая плотность мощности лазера необходимая для этого составляла 38 МВт/см^2.

Оптическое инициирование предоставляет возможность дистанционного инициирования реакции окисления пористого кремния находящегося, например, на кремниевой подложке микросистемы. Возникающая реакция окисления может приводить к разрушению микросистемы и, следовательно, невозможности несанкционированного копирования информации, хранимой в микросистеме.

ПРОГРАММНЫЙ МОДУЛЬ ЗАЩИТЫ ГОЛОСОВОЙ ИНФОРМАЦИИ В СЕТЯХ ПОДВИЖНОЙ РАДИОСВЯЗИ

А.О. Дударенков, О.Б. Зельманский

Речевые сигналы представляют собой наиболее уязвимый тип данных и очень часто остаются открытыми и легкодоступными. Несанкционированный доступ к каналу передачи речевой информации может привести к утечке конфиденциальных данных. Проведенный анализ действующих стандартов мобильной связи показал, что в них содержится большое количество уязвимостей [1, 2].

Предлагается программный модуль обеспечения безопасности речевой информации в сетях мобильной передачи данных [3]. Данный модуль может быть использован для дополнительного и независимого шифрования информации в мобильных сетях различных стандартов. В основу предлагаемого модуля положен алгоритм шифрования AES. Модуль написан на языке программирования Java. Для его работы потребовался дополнительный кодек: Apache Commons Codec 1.11. Пакет кодека содержит простой кодер и декодер для различных форматов данных, а также большую коллекцию утилит для фонетического кодирования. Модуль состоит из блоков записи речи в аудиофайл, подачи ключа и шифрования, ввода ключа для расшифрования.

В процессе тестирования модуля был создан аудиофайл, содержащий речь. Файл подавался на вход приложения, далее происходило его преобразование в массив значений амплитуд для последующего шифрования и вывод зашифрованного файла для анализа. Далее осуществлялось дешифрование. На каждом этапе выполнялся анализ получаемых файлов посредством вывода их спектрограмм.

Список литературы

1. Securing Speech in GSM Networks using DES with Random Permutation and Inversion Algorithm / K. Merit [et al.] // IJDPS. 2012. № 3.

2. Real-Time End-To-End Secure Voice Communications Over GSM Voice Channel / N.N. Katugampala [et al.] // Signal Processing Conference. 2005. № 13.

3. Khomo K.B., Ogorodnikov E.A., Zelmanski O.B. Protecttion of speech information during transmission via mobile networks // Тез. докл. XVI Белоруско-российской науч.-техн. конф. «Технические средства защиты информации». Минск, 5 июня 2018 г. С. 10.

МОДЕЛЬ РАСЧЕТА ЭКСПЛУАТАЦИОННОЙ НАДЕЖНОСТИ ТРАНСФОРМАТОРОВ ЭЛЕКТРОПИТАНИЯ ЭЛЕКТРОННОЙ АППАРАТУРЫ

А.В. Евилин, С.М. Боровиков, А.В. Будник

В настоящее время ведущие страны мира используют свои методики расчета эксплуатационной надежности трансформаторов электропитания электронной аппаратуры. Методики основаны на моделях надежности, которые отличаются номенклатурой и числом