

10–20% в зависимости от длины волны видимого диапазона. Уровень выходного оптического сигнала достаточен для его регистрации фотодетекторами.

Разработанная система способна работать в гигагерцевом диапазоне частот, что достигается за счет миниатюризации рабочей площади светодиодов. Данная разработка открывает новые возможности для развития кремниевой оптоэлектроники и интегральной электроники в целом.

ИССЛЕДОВАНИЕ ЗАРЯДОВЫХ СВОЙСТВ АНОДНЫХ ПЛЕНОК, ИСПОЛЬЗУЕМЫХ В МЕМРИСТОРНЫХ СТРУКТУРАХ

С.К. Лазарук, В.В. Дудич, Г.Г. Рабатуев, А.С. Хиневич, В.В. Фиалковский

Развитие современной электроники создает постоянный спрос на разработку новых технологий и принципов формирования устройств обработки, хранения и защиты информации, так как возможности кремниевой технологии в области дальнейшей миниатюризации и снижения энергопотребления ячеек памяти ограничены фундаментальными физическими свойствами. Для защиты информации предлагается использование мемристорных структур (энергонезависимых ячеек памяти). Мемристоры демонстрируют эффект переключения сопротивления между высокоомным и низкоомным состояниями под действием внешнего электрического поля. Данный тип памяти способен обеспечить надежное хранение и защиту информации.

Проведено исследование зарядовых свойств анодных пленок оксидов титана и алюминия. Было установлено наличие подвижных и фиксированных зарядов в оксидных пленках, которые в зависимости от условий формирования, могут быть как положительными, так и отрицательными. Было проведено обсуждение влияния зарядовых состояний на мемристорный эффект и выявлено, что данные заряды увеличивают коэффициент переключения, что положительно сказывается на увеличении отказоустойчивости ячеек памяти.

Проведенные исследования позволили увеличить коэффициента переключения на порядок в мемристорной структуре, что открывает новые возможности для практического применения.

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ ПО СПОСОБУ МЫШЛЕНИЯ

А.С. Левковский

По статистике, 40 % системных администраторов хранят свои важные данные в незашифрованном виде, что дает возможность злоумышленнику воспользоваться информацией после несанкционированного доступа в систему. В целях защиты информации могут применяться следующие способы аутентификации: по отпечатку пальца, радужной оболочке или сетчатке глаза, геометрии руки или лица, голосу, рукописному или клавиатурному почерку и др.

В 2010 году на взлом пароля при входе в систему с помощью SSD-устройств на ОС Windows XP требовалось 2–11 секунд. На сегодняшний день на аналогичный способ проникновения в систему требуется гораздо меньше времени.

Одним из эффективных способов решения проблемы защиты информации ограниченного распространения может послужить устройство, созданное в Массачусетском университете и способное с вероятностью до 92 % сканировать мысли человека. С научной точки зрения данные, которые генерирует мозг во время мыслительных процессов, уникальны и их нельзя подменить.

Устройство работает следующим образом. На начальном этапе выполняется его калибровка для того, чтобы определить, как мозг реагирует на различного рода информацию. При этом на челюсть человека передаются вибрации. Они являются сигналами, несущими информацию, предназначенную для обработки мозгом человека. Результаты такой обработки анализируются устройством, на основании чего формируется эталон, который заносится в базу данных и в последующем используется для подтверждения идентификации.