

уменьшению затрат на организацию каналов передачи данных за счет уменьшения объема передаваемой информации, уменьшению количества компьютерного оборудования и объема архивного пространства за счет уменьшения количества обрабатываемой информации. Также снизится стоимость эксплуатации и обслуживания системы за счет существенного упрощения инфраструктуры.

Принцип работы тепловизора основан на его способности воспринимать тепловое излучение от всех объектов, находящихся на этой сцене. При преобразовании энергии теплового излучения в видимое изображение наиболее холодному объекту на сцене ставится в соответствие черный цвет, наиболее горячему объекту — белый цвет. Весь динамический диапазон получаемой энергии от самого холодного до самого горячего объекта делится на 256 градаций, и каждому значению равномерно присваивается свой оттенок серого. Палитра в градациях серого — это классический пример линейного отображения информации.

Ещё одним преимуществом использования тепловизоров является возможность выбора палитры. Предложено использовать палитру в градациях красного, которая привлекает внимание оператора, поскольку красный воспринимается как цвет опасности.

Таким образом, можно сделать вывод, что тепловизоры являются незаменимыми приборами для обнаружения объекта и для круглосуточного сканирования периметра в любое время года.

АЛГОРИТМ КОДИРОВАНИЯ ИНФОРМАЦИИ И ВЗАИМНОЙ АУТЕНТИФИКАЦИИ В СЕНСОРНОЙ СЕТИ НА ОСНОВЕ ХЕШ-ФУНКЦИИ КЕССАК

Т.М. КАЗУБОВИЧ, С.Б. САЛОМАТИН

Сенсорные сети на основе RFID технологии используются в различных областях управления и защиты информации. Надежная работа сенсорной сети предполагает надежное кодирование данных и использование протоколов взаимной аутентификации узлов сети.

Одним из эффективных механизмов кодирования и аутентификации являются хеш-функции, среди которых можно выделить хеш-функцию Кессак, лежащую в основе стандарта SHA-3.

Алгоритм Кессак устойчив к коллизиям первого и второго рода. Благодаря использованию в алгоритме функции перемешивания, алгоритм так же обладает лавинным эффектом: незначительное изменение в открытом тексте полностью меняет хеш-функцию.

Рассматривается алгоритм кодирования информации кодом фиксированной длины и переменной скоростью передачи данных на основе алгоритма Кессак.

Приводится протокол взаимной аутентификации RFID-меток и алгоритм локализации объекта по корреляционной функции сигнала Кессак в системе дистанционного мониторинга и управления доступом объекта.

Оценивается возможность применения алгоритмов для имитозащиты в автоматизированной системе контроля и управления доступом (АСКУД) транспортного средства на основе RFID-технологии, в состав которой входят: сенсорная сеть датчиков, считыватель (портал), модуль метка-ключ, модуль метка-замок, система оповещения, система хранения и управления данными и инфраструктурой ключевого пространства.