этой величины их заданному количеству в контрольном слове.

- анализа длительности пауз между отдельными словами, которые должны находиться в пределах 4-12 мкс.

При обнаружении любой из ошибок сообщение считается недостоверным и контроллер производит в этом случае повторную передачу сообщений, максимальное количество которых, до того, как будет сформирован сигнал отказа оборудования, определяется в зависимости от функционального назначения комплекса бортового оборудования.[3]

Список использованных источников:

1. Каналы последовательного кода систем управления авиационным оборудованием по ГОСТ18977-79 (ARINC-429). Электронная Компания «ЭЛКУС». 2000.

2. Шукалов, А.В. Принципы построения вычислительных компонентов систем интегрированной модульной авионики./ А.В. Шукалов, П.П. Парамонов, И.О. Жаринов. - М. 2016.

3. Бортовые информационные системы: курс лекций. Ульяновский государственный технический университет. 2004.

СИСТЕМА КОНТРОЛЯ ДОСТУПА КАК ОСНОВОПОЛАГАЮЩАЯ СИСТЕМА В ОХРАННОЙ ДЕЯТЕЛЬНОСТИ

Институт информационных технологий БГУИР, г.Минск, Республика Беларусь

Яненко Н.В., Житко А.П.

Пачинин В.И. - канд. техн. наук, доцент

В работе представлены результаты разработки системы контроля доступа. Рассмотрены особенности применения оборудования, использования систем идентификации, совместного использования с другими системами.

На текущий момент охранная деятельность становится неотъемлемой частью жизнедеятельности человека. Охране подвергаются практически все территории и объекты любых предприятий, поэтому процесс определения полномочий доступа тех или иных лиц, а также автотранспорта на охраняемую территорию является важным и актуальным.

В системах контроля доступа (СКД) используется специализированное оборудование, которое позволяет идентифицировать человека; определить возможность проноса или провозапрещенных предметов, в том числе оружия, взрывчатых веществ, делящихся материалов и т.п. Они также обеспечивают функции контроля перемещения людей и автотранспорта по территориям организации.

Подобные системы применяются в различных типах офисных зданий, бизнес-центрах, супермаркетах, предприятиях оптовой торговли и т.п.

СКД могут быть тесно интегрированы с системой охранно-пожарной сигнализации, видеонаблюдением, платежной системой, с инженерными системами здания, с информационными системами организации.

Для того чтобы идентифицировать человека в СКД сейчас используются биометрические технологии, к таким устройствам относятся идентификаторы по форме кисти руки, по отпечатку пальца, по радужной оболочке глаза.

Оборудование контроля доступа может устанавливаться на двери всех помещений служебной зоны. Для повышения уровня безопасности на двери, отделяющие клиентскую зону от служебной, могут устанавливаться считыватели двойной технологии – Proх или Smart-карта плюс отпечаток пальца [1,2].

Системы контроля доступа обычно тесно интегрируются с системой охранной сигнализации. Нередко системы контроля доступа и охранной сигнализации разных производителей интегрируются на уровне программного обеспечения, что дает возможность подключения уже установленного на объекте оборудования к единому управляющему центру.

Системы контроля доступа широко используются для управления движением транспортных средств по территориям подземных автостоянок. Идентификация производится постановкой автомобиля на индукционную петлю и предъявлением водителем Proх-карты на считывателе. С учетом приоритета данного пользователя с помощью светофоров, шлагбаумов и ворот организуется трасса для проезда автомобиля. Для предотвращения прорывов в здание могут использоваться гидравлические блокираторы подъемного типа.

На базе систем контроля доступа могут быть построены интегрированные охранные системы, объединяющие в единый комплекс подсистемы безопасности различного назначения. При этом осуществляется управление всеми подсистемами как единой многофункциональной охранной системой, в том числе обеспечивается ведение единого протокола событий всех подсистем, обработка событий всех подсистем, программирование реакций на события, определение сложных алгоритмов взаимодействия подсистем. Такая система должна функционировать в чрезвычайных ситуациях, в том числе в условиях выхода из строя и поражения ее отдельных компонентов.

Список использованных источников:

1. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. - М., 2009.

2. Компьютерная преступность и информационная безопасность / А.П. Леонов [и др.]; под общ. ред. А.П. Леонова. - Минск: АРИЛ, 2010.