полиномиальные алгоритмы; 2) подкласс, содержащий только экспоненциальные алгоритмы.

Функции типа 2^n, n^n, $n!$.. могут рассматриваться, как имеющие одинаковые свойства экспоненциального роста. Функции типа kn, kn^2, kn^3, ..., где k – коэффициент, могут рассматриваться как полиномиальные. Основное отличие полиномиальной функции от экспонециальной состоит в том, что n никогда не появляется в экспоненте.

Сложность алгоритма характеризуется числом операций N и общим объемом памяти V, необходимой для его реализации. С числом операций связано время реализации алгоритма, то есть функция $T= f(N)$. Выполнение каждой операции требует свое время. В связи с этим для определения сложности алгоритма необходимо знать и число используемых в алгоритме типов операций. На основе анализа алгоритма можно построить множество встречаемости операций в алгоритме $N=\{o_1, o_2, \dots, o_n\}$, где oi – число операций i-го типа; n – число типов операций. Умножая время выполнения каждой операции на число этих операций и суммируя результаты по всем операциям, получаем время работы алгоритма $T = \sum_{i=1}^{n} Oi\, ti$, где ti – время выполнения i-й операции. Тогда общее число условных элементарных операций составит $N\text{э} = \sum_{i=1}^{n} Oi\, Ci$, где $Ci = ti/t\text{э}$, $t\text{э}$ – время реализации эталонной операции, а общее время их реализации $T\text{э} = N\text{э}t\text{э}$. Общий объем памяти, который необходимо зарезервировать: $V=V_п+V_и+V_{пр}+V_в$, где $V_п$, $V_и$, $V_{пр}$, $V_в$ – объемы памяти для размещения: программы, исходной, промежуточной и выходной информации соответственно; V – общий объем памяти. Тогда обобщенный коэффициент сложности алгоритма вычисляется: $Ксл = N\text{э}/V$.

В качестве примера осуществим оценку сложности алгоритма решения системы n линейных уравнений, которые широко используются в выполнении различных прикладных задач. Рассмотрим задачу решения 10^4 уравнений на компьютере со средним быстродействием 10^6 операций в секунду.При этом необходимое количество арифметических операций составит $N\approx 1/3\cdot 10^{12}$ (в общем случае для решения системы n уравнений требуется $\approx n^3/3$). Следовательно,время решения задачи на компьютере составит: $T\approx 1/3\cdot 10^{12}/10^6 = 1/3\cdot 10^6$сек.≈93часа≈3,8суток.Если решать систему при $n=10^3$, то получаем T≈0,1часа=6минут и требуемый объем памяти компьютера 4гигабайта.Отсюда следует, что при увеличении n растет сложность алгоритма по временным и запоминающим показателям. Рассмотрим еще один пример: необходимо использовать два алгоритма A_1 и A_2 для решения одной и той же задачи размерности $n=10^6$. A_1 имеет сложность $O_1(n^2)$ и выполняется на компьютере с быстродействием 10^8 оп/с, а A_2 со сложностью $O_2(n\log_2 n)$ – на компьютере с быстродействием 10^6 оп/с. Найти время решения задачи T_1 и T_2. Решение: $T_1=10^{12}/10^8=10^4$с ≈ 2,8ч.; $T_1=10^6\log_2 10^6/10^6=6\log_2 10\approx 20$с.

В результате проведенной оценки сложности алгоритмов можно сделать вывод о том, что при решении различных прикладных задач предпочтительнее использовать полиномиальные алгоритмы, позволяющие существенно сэкономить информационно-вычислительные ресурсы по сравнению с экспоненциальными.

Список использованных источников:

1.Кузюрин,Н.Н. Эффективные алгоритмы и сложность вычислений. http://discopal.ispras.ru/ru.book-advanced-algorithms.htm). Дата доступа 27.04.2017.

2.Морозов, К.К. Автоматизированное проектирование конструкций радиоэлектронной аппаратуры./ К.К.Морозов, В.Г.Одиноков, В.М.Курейчик. – М. : Радио и связь, 1983. – 280 с.

УСТРОЙСТВО КОНТРОЛЯ ОБМЕНА БИПОЛЯРНЫМ КОДОМ

Институт информационных технологий БГУИР, г.Минск, Республика Беларусь

Юницкий А.А.

Стешенко П.П. – канд. техн. наук, доцент

Целью разработки устройства контроля обмена биполярным кодом, возможность его применения для проверки электронных плат, интегральных микросхем на наличие неисправностей, а также для более точного нахождения неисправностей в изделиях, радиоэлектронных блоках, оборудовании, обмен информацией в которых осуществляется биполярным кодом (ГОСТ 18977-79 или ARINC-429).

В настоящее время одновременно используется несколько разных интерфейсов. Одни из них нужны для передачи непрерывных потоков цифровизированных видео- и аудиосигналов (радар, оптико-локационная станция, видеокамеры, внебортовые источники информации), другие используются при передаче сигналов от датчиков,

Идеальным решением был бы единый интерфейс, объединяющий все функциональные задачи, соединяющий в единую сеть все модули и блоки. Для того, чтобы удовлетворить требованиям различных приложений, единый интерфейс должен быть очень гибким. Он должен быть масштабируемым, так как может применяться как для связи дешевых простых датчиков, нетребовательных к пропускной способности и задержке информации, так и в сложных системах с большим потоком информации и жесткими ограничениями на допустимую задержку.

ARINC 429 **(**ГОСТ 18977-79) — стандарт на компьютерную шину (рисунок 1) разработан фирмой ARINC [1]. Стандарт описывает основные функции и необходимые физические и электрические интерфейсы для цифровых систем. Сегодня ARINC 429 является доминирующей авиационной шиной для большинства самолётов. Передача, как правило, асинхронная. Уведомление источника о том, что данные приняты верно, не предусматривается. Основная информация передается циклически, поэтому неверно принятые данные могут быть приняты в следующем цикле.

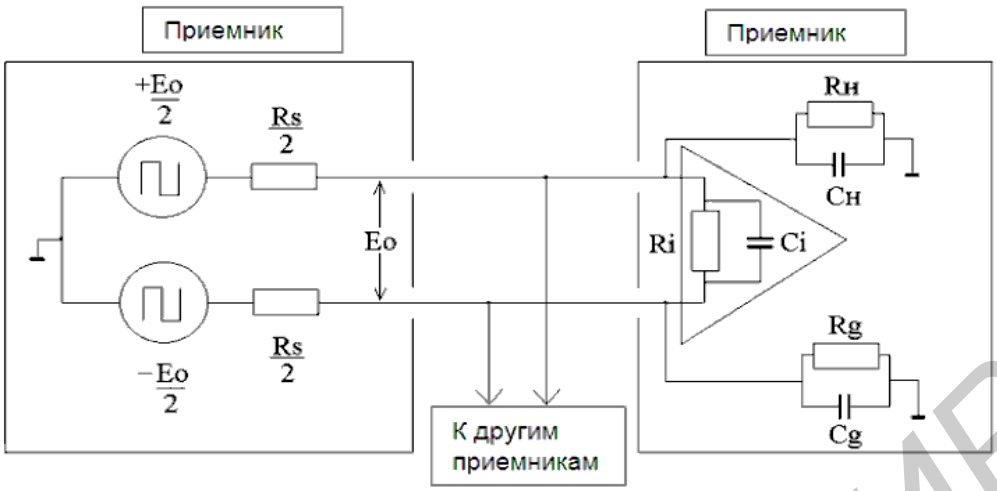

Рисунок 1.Структурная схема системы ARINC 429.

Используется трехуровневая модуляция сигнала: высокий уровень, ноль, низкий уровень , высокий уровень соответствует логической «1», низкий – логическому «0», а нулевой уровень означает паузу между передаваемыми битами (рисунок 2).

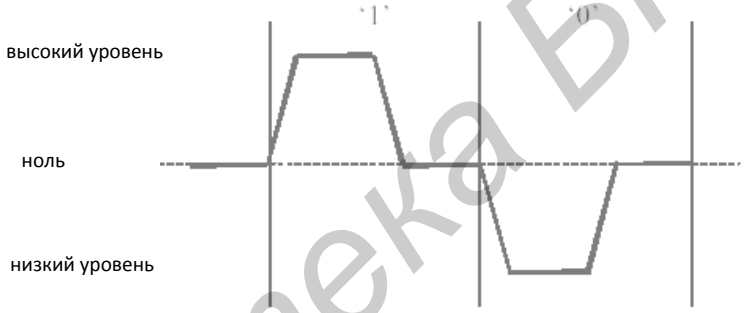

Рисунок 2 - Трехуровневая модуляция сигнала.

Передачу информации последовательным кодом регламентирует документ РТМ 1495-75 с изменением 3. Он почти полностью соответствует ARINC 429, но имеет следующие особенности: если система в состоянии выдавать данные с пониженной точностью, то в матрице состояния указывается «Нормальная работа», а о пониженной точности сигнализирует «1» в 11 разряде.

Мультиплексный канал информационного обмена (МКИО) впервые появился в 1973г. Позднее он был принят в качестве стандартного интерфейса в США (военный стандарт MIL-STD-1553B), а затем и в других странах (отечественный ГОСТ 26765.52-87).В настоящее время МКИО используется на большинстве военных аппаратах. Его широкое распространение связано со следующими достоинствами:

1.Линейная топология идеально подходит для распределенных комплексов оборудования подвижных объектов. Надёжность МКИО обеспечивается автоматическим переключением на резервную шину при отказе основной.

2.Протокол «команда-ответ» обеспечивает работу в реальном масштабе времени, что крайне важно для критических функций.

3.Предусмотрена возможность подключения простых терминалов – датчиков, исполнительных устройств.

4.Высокая устойчивость к отказам и широкая доступность компонентов.

При выборе способов контроля передаваемой информации основная проблема заключается в обеспечении заданных, достаточно высоких показателей достоверности передачи информации при минимальных затратах на нужды контроля [2]. Исходя из этого критерия, нами использован пословный контроль, который предусматривает проверку каждого принятого слова на соответствие следующим условиям:

1.Началом слова является синхросигнал с соответствующими параметрами.

2.Следующие за синхросигналом 17 информационных сигналов слова удовлетворяют проверке на четность, для чего и используется последний 17-йразряд.В случае, если эти условия не выполняются, слово считается недостоверным, т. е. переданным с ошибкой. Контроль сообщений (группы слов) обеспечивается за счет:

- подсчета фактического количества переданных информационных слов и определения соответствия

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.