1. ОБЪЕКТЫ СКУД

Системой контроля и управления доступом **(СКУД) и** системой контроля доступа (СКД) называется совокупность программно-технических средств и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением отдельных помещений, а также оперативный контроль перемещения персонала и времени его нахождения на территории объекта.

Средства и системы контроля и управления доступом могут быть рассмотрены как технические средства защиты объектов и имущества от несанкционированного проникновения и способны играть существенную роль в защите от террористических и криминальных угроз.

СКУД должна обеспечивать выполнение следующих основных функций:

- открывание устройств преграждающих управляемых (УПУ) при считывании идентификационного признака, доступ по которому разрешен в данную зону доступа (помещение) в заданный временной интервал или по команде оператора СКУД;
- запрет открывания УПУ при считывании идентификационного признака, доступ по которому не разрешен в данную зону доступа (помещение) в заданный временной интервал;
- санкционированное изменение (добавление, удаление) идентификационных признаков в устройств управления (УУ) и связь их с зонами доступа (помещениями) и временными интервалами доступа;
- защиту от несанкционированного доступа к программным средствам УУ для изменения (добавления, удаления) идентификационных признаков;
- сохранение настроек и базы данных идентификационных признаков при отключении электропитания;
- ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;
- автоматическое закрытие УПУ при отсутствии факта прохода через определенное время после считывания разрешенного идентификационного признака;
- выдачу сигнала тревоги (или блокировку УПУ на определенное время) при попытках подбора идентификационных признаков (кода);
- регистрацию и протоколирование текущих и тревожных событий;
- автономную работу считывателя с УПУ в каждой точке доступа при отказе связи с УУ;

Программное обеспечение СКУД должно обеспечивать возможность учёта рабочего времени.

К объектам СКУД в настоящее время могут относиться:

1. Проходы на открытые огороженные территории.
2. Проходы (проезды) на такие территории могут быть оборудованы воротами (автомобильными, железнодорожными) с автоматическими приводами, управляемыми шлагбаумами, турникетами, шлюзовыми кабинами с применением спецоборудования для обнаружения диверсионно-террористических средств и специальных исполнительных устройств разграничения доступа.
3. Совокупность периметрально расположенных объектов такого типа образует систему контрольно-пропускных пунктов (проходных).
4. При необходимости рад контролируемых подсистемой проходов могут логически объединяться, образуя контролируемый маршрут персонала учреждения, например, маршрут службы охраны или инкассации;
5. Входы в отдельные помещения или их группы;
6. Входы на изолированные объекты, расположенные в местах массового скопления людей и требующие ограничения или контроля доступа (например, множительная или иная оргтехника);
7. Доступ к ПЭВМ и в вычислительные сети и системы;
8. Доступ к жизненно-важному оборудованию и приборам.
9. Доступ к художественным ценностям и т.п.

2. НОРМАТИВНО – ПРАВОВАЯ БАЗА СКУД

Первые российские стандарты, рассматривающие системы СКУД с точки зрения обеспечения безопасности от несанкционированного проникновения, были разработаны, соответственно, в 1998 и 2000 годах. (ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний» и ГОСТ Р 51558-2000 «Системы охранные телевизионные. Общие технические требования и методы испытаний».)

В настоящее время разрабатывается технический регламент «О технических средствах обеспечения противокриминальной защиты объектов и имущества».

Введенная в стандарте классификация средств и систем КУД, принятая в нем терминология, перечень параметров и требований к средствам и системам обеспечили

развитие взаимопонимания между разработчиками, изготовителями и заказчиками этого оборудования.

Однако со времени принятия ГОСТа прошло более 10 лет, он в значительной степени устарел и нуждается в доработке, в ходе которой должны быть учтены изменения в области развития СКУД, произошедшие за этот период.

В частности, предъявляемые ГОСТом требования к отечественной продукции и услугам, как минимум, не должны противоречить соответствующим международным требованиям, правилам и нормам, а, по возможности, не уступать им или даже превосходить их.

С принятием Федерального закона от 27 декабря 2002 г. № 184-ФЗ «**О техническом регулировании**» появилась реальная возможность решить ряд важных вопросов в области антитеррористической и противокриминальной защиты имущества посредством разработки и утверждения на федеральном уровне свода соответствующих технических регламентов. В соответствии со статьей 6 данного Федерального закона, «Технические регламенты принимаются в целях: защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества», что в полной мере соответствует области применения технических систем антитеррористической и противокриминальной защиты.

Если акцентировать внимание на защите объектов и имущества, то следует четко осознавать, что в настоящее время угрозы криминально-террористического характера часто инициируют чрезвычайные ситуации и могут нанести значительно больший ущерб, чем некоторые угрозы техногенного или природного характера. Техническое регулирование в данной сфере имеет целью установление дифференцированных минимально необходимых требований (показателей, свойств) к системам обеспечения антитеррористической и противокриминальной защиты объектов и имущества в зависимости от категории защищаемого объекта и с учетом допустимых рисков, что помимо прочего позволит минимизировать расходы федерального бюджета, бюджетов субъектов Российской Федерации и муниципальных образований на антитеррористическую и противокриминальную защиту объектов и имущества. Для решения данных вопросов МВД России в 2005 году в Правительство Российской Федерации были внесены предложения по созданию «Системы технического регулирования в сфере антитеррористической и противокриминальной защиты», включающей в себя разработку двух первоочередных технических регламентов. Правительством данные предложения были поддержаны и распоряжением от 29 мая 2006 года № 781-р в Программу разработки технических регламентов были включены:

1. Специальный технический регламент «О требованиях к системе антитеррористической и противокриминальной защиты объектов»;
2. Специальный технический регламент «О требованиях к системам противокриминальной защиты имущества».

При разработке нового стандарта на СКУД предполагалось сотрудничество с МЭК (Международная электротехническая комиссия – International Electrotechnical Commission), IEC – международная организация по стандартизации в области электрических, электронных и смежных технологий. Перечень действующих стандартов МЭК/ТК 79 Alarm systems приведены ниже.

ОБОЗНАЧЕНИЕ ЗАГЛАВИЕ НА РУССКОМ ЯЗЫКЕ

1. IEC 60839-1-1(1988) Системы тревожной сигнализации. Часть 1: Общие требования. Раздел 1: Общие положения.
2. IEC 60839-1-2(1987) Системы тревожной сигнализации. Часть 1: Общие требования. Раздел 2: Источники электропитания, методы испытаний и критерии качества работы.
3. IEC 60839-1-3(1988) Системы тревожной сигнализации. Часть 1: Общие требования. Раздел 3: Испытания на воздействие внешних факторов.
4. IEC 60839-1-4(1989) Системы тревожной сигнализации. Часть 1: Общие требования. Раздел 4: Правила по практическому применению.
5. IEC 60839-2-2(1987) Системы тревожной сигнализации. Часть 2: Требования к системам охранной сигнализации. Раздел 2: Общие требования к охранным извещателям
6. IEC 60839-2-3(1987) Системы тревожной сигнализации. Раздел 3: Требования к извещателям инфракрасным лучевым, устанавливаемым в зданиях.
7. IEC 60839-2-4(1990) Системы тревожной сигнализации. Часть 2: Требования к системам охранной сигнализации. Раздел 4: Доплеровские ультразвуковые извещатели, устанавливаемые в зданиях.
8. IEC 60839-2-5(1990) Системы тревожной сигнализации. Часть 2: Требования к системам охранной сигнализации. Раздел 5: Доплеровские СВЧ-извещатели, устанавливаемые в зданиях.
9. IEC 60839-2-6(1990) Системы тревожной сигнализации. Часть 2: Требования к системам охранной сигнализации. Раздел 6: Пассивные инфракрасные извещатели, используемые в зданиях.
10. IEC 60839-2-7(1994) Системы тревожной сигнализации. Часть 2: Требования к системам охранной сигнализации. Раздел 7: Пассивные извещатели, срабатывающие при разбивании стекла, устанавливаемые в зданиях.

11. IEC 60839-5-1(1991) Системы тревожной сигнализации. Часть 5: Требования к системам передачи сигналов тревоги. Раздел 1: Общие требования к системам

12. IEC 60839-5-2(1991) Системы тревожной сигнализации. Раздел 2: Общие требования к оборудованию.

13. IEC 60839-5-4(1991) Системы тревожной сигнализации. Раздел 4: Системы передачи сигналов тревоги, использующие выделенные каналы передачи.

14. IEC 60839-5-5(1991) Системы тревожной сигнализации. Раздел 5: Требования к системам цифровой связи, использующим телефонную сеть общего пользования.

15. IEC 60839-5-6(1991) Системы тревожной сигнализации. Раздел 6: Требования к системам речевой связи, использующим коммутируемую телефонную сеть общего пользования.

16. IEC 60839-7-1(2001) Системы тревожной сигнализации. Часть 7-1. Форматы сообщений и протоколы для интерфейсов последовательных данных в системах передачи. Общие положения.

17. IEC 60839-7-2(2001) Системы тревожной сигнализации. Часть 7-2. Форматы сообщений и протоколы для интерфейсов последовательных данных в системах передачи. Общий протокол прикладного уровня.

18. IEC 60839-7-3(2001) Системы тревожной сигнализации. Часть 7-3. Форматы сообщений и протоколы для интерфейсов последовательных данных в системах передачи. Общий протокол уровня канала передачи данных.

19. IEC 60839-7-4(2001) Системы тревожной сигнализации. Часть 7-4. Форматы сообщений и протоколы для интерфейсов последовательных данных в системах передачи. Общий протокол транспортного уровня.

20. IEC 60839-7-5(2001) Системы тревожной сигнализации. Часть 7-5. Форматы сообщений и протоколы для интерфейсов последовательных данных в системах передачи. Интерфейсы систем с двухпроводной конфигурацией в соответствии с ИСО/МЭК 8482.

21. IEC 60839-7-6(2001) Системы тревожной сигнализации. Часть 7-6. Форматы сообщений и протоколы для интерфейсов последовательных данных в системах передачи. Интерфейсы систем, использующие рекомендации ITU-T V.24/V.28 для передачи сигналов.

22. IEC 60839-7-7(2001) Системы тревожной сигнализации. Часть 7-7. Форматы сообщений и протоколы для интерфейсов последовательных данных в системах передачи. Интерфейсы систем для сменных датчиков аварийных систем IEC 60839-7-11(2001) Системы тревожной сигнализации. Часть 7-11. Форматы сообщений и протоколы для интерфейсов последовательных данных в системах передачи. Последовательный

протокол, применяемый в цифровых системах связи, с использованием рекомендаций ITU-T V.23 для передачи сигналов на уровне интерфейсов с телефонной сетью общего пользования (PSTN).

23. IEC 60839-7-12(2001) Системы тревожной сигнализации. Часть 7-12. Форматы сообщений и протоколы для интерфейсов последовательных данных в системах передачи. Интерфейсы предприятий почтовой, телеграфной и телефонной связи для специализированных каналов связи с использованием рекомендаций ITU-T V.23 для передачи сигналов.

24. IEC 60839-7-20(2001) Системы тревожной сигнализации. Часть 7-20. Форматы сообщений и протоколы для интерфейсов последовательных данных в аварийных системах передач. Терминальные интерфейсы с использованием рекомендации ITU-T V.24/V.28 для передачи сигналов.

25. IEC 60839-10-1(1995) Системы тревожной сигнализации. Часть 10: Системы охранной сигнализации.

Среди последних тенденций в развитии СКУД в последнее время уделяется все больше внимания биометрическим решениям идентификации и радиочастотной идентификации. Предполагается, что при работе над новым стандартом по СКУД будут использованы положения МЭК/ИСО, касающихся биометрической идентификации международных стандартов. Ниже при веден перечень основных документов, на которые нужно обратить внимание.

1. ГОСТ Р ИСО/МЭК 14443-1-2004 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 1. Физические характеристики.
2. ГОСТ Р ИСО/МЭК 15693-1-2004 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия. Часть 1. Физические характеристики.
3. ГОСТ Р ИСО/МЭК 15693-2-2004 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия. Часть 2. Воздушный интерфейс и инициализация.
4. ГОСТ Р ИСО/МЭК 15963-2005 Автоматическая идентификация. Радиочастотная идентификация для управления предметами. Уникальная идентификация радиочастотных меток.
5. ГОСТ Р ИСО/МЭК 19794-2-2005 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца – контрольные точки.

6. ГОСТ Р ИСО/МЭК 19794-4-2006 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца.
7. ГОСТ Р ИСО/МЭК 19794-5-2006 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица.
8. ГОСТ Р ИСО/МЭК 19794-6-2006 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза.

Кроме того, имеется множество как отечественных, так и зарубежных документов, касающихся вопросов, связанных со СКУД – как непосредственно (например, ряд стандартов на замки и запирающие устройства с электрическим управлением, а также стандарты по методам идентификации), так и определяющие дополнительные вопросы применения СКУД (стандарты на автоматизированные системы управления, информационные системы и т.д.).

3. КЛАССИФИКАЦИЯ ОБЪЕКТОВ ЗАЩИТЫ

Классификация объектов осуществляется с целью установления дифференцированных требований к системам противокриминальной защиты, обеспечивающим минимально необходимые уровни **безопасности** имущества в соответствии с установленными классами объектов нахождения имущества, с учетом критериев оценки возможного ущерба интересам личности, общества и государства, который может быть нанесен в случае реализации криминальных угроз.

В зависимости от степени потенциальной опасности, а также возможных последствий в случае реализации криминальных угроз, объекты, их помещения и территории подразделяются на три основных группы:

I группа: критически важные и потенциально опасные объекты;

II группа: социально-значимые объекты;

III группа: объекты сосредоточения материальных ценностей.

В зависимости от вида и размеров ущерба, который может быть нанесен объекту, находящимся на нем людям и имуществу в случае реализации криминальных угроз, все объекты подразделяются на 3 класса:

- Класс 1 – (высокая значимость);
- Класс 2 – (средняя значимость);
- Класс 3 – (низкая значимость).

В целях определения класса объекта применяют методы многокритериальной оценки возможного ущерба от криминальных угроз, при этом качественные критерии, предельные значения количественных критериев для каждой группы объектов и выбор класса объекта устанавливаются Правительством Российской Федерации с учетом анализа рисков, криминальных угроз и размеров потенциального ущерба. Каждой группе объектов соответствует определенный класс (степень) защиты объекта техническими средствами обеспечения противокриминальной защиты (всего 4). В зависимости от класса защиты объекта определяется минимально необходимый состав средств инженерно-технической укрепленности и технических средств противокриминальной защиты.

Классификации подлежат все потенциально опасные в криминальном отношении объекты независимо от их организационно-правовых форм и форм собственности. Порядок классификации объектов определяется Правительством Российской Федерации. Основная часть регламента устанавливает функциональные требования к техническим средствам и системам противокриминальной **безопасности** объектов защиты: условия и порядок создания таких систем, принципы их построения, требования к проектированию, монтажно-наладочным работам, введению в эксплуатацию и эксплуатации, а также конкретные требования к средствам инженерно-технической укрепленности объекта и **техническим средствам охраны**.

Важной составляющей проекта технического регламента является раздел, посвященный вопросам подтверждения соответствия технических систем противокриминальной защиты требованиям регламента, которое устанавливается в двух формах:

- принятия декларации о соответствии,
- обязательной сертификации, что позволяет осуществлять действенный контроль за соответствием созданной **технической системы безопасности** объекта классу его защиты.

4. КЛАССИФИКАЦИЯ СРЕДСТВ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ СОГЛАСНО ГОСТ Р 51241-2008

Средства КУД подразделяют по:

- функциональному назначению устройств;
- функциональным характеристикам;
- устойчивости к НСД.

Средства КУД по функциональному назначению устройств подразделяют на следующие основные средства:

- устройства преграждающие управляемые;
- устройства исполнительные;
- устройства считывающие;
- идентификаторы (ИД);
- средства управления в составе аппаратных устройств и программных средств.

В состав СКУД могут входить другие дополнительные средства: источники электропитания; датчики (извещатели) состояния УПУ; дверные доводчики; световые и звуковые оповещатели; кнопки ручного управления УПУ; устройства преобразования интерфейсов сетей связи; аппаратура передачи данных по различным каналам связи и другие устройства, предназначенные для обеспечения работы СКУД.

В состав СКУД могут входить также аппаратно-программные средства - средства вычислительной техники (СВТ) общего назначения (компьютерное оборудование, оборудование для компьютерных сетей, общее программное обеспечение).

Средства КУД по функциональным характеристикам подразделяют на следующие группы:

УПУ - по виду перекрытия проема прохода:

- с частичным перекрытием (турникеты, шлагбаумы);
- с полным перекрытием (полноростовые турникеты, специализированные ворота);
- со сплошным перекрытием проема (сплошные двери, ворота);
- с блокированием объекта в проеме (шлюзы, кабины проходные).

УИ - по способу запирания:

- электромеханические замки;
- электромагнитные замки;
- электромагнитные защелки;
- механизмы привода дверей, ворот.

Идентификаторы и считыватели - по следующим признакам:

- виду используемых идентификационных признаков (идентификаторы и считыватели);
- способу считывания идентификационных признаков (считыватели).

По виду используемых идентификационных признаков идентификаторы и считыватели могут быть:

- механическими - представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);

- магнитными - представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т.д.);

- оптическими - представляют собой нанесенные на поверхность или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, голографические метки и т.д.);

- электронными контактными - представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи и т.д.);

- электронными радиочастотными - считывание кода с электронных идентификаторов происходит путем передачи данных по радиоканалу;

- акустическими - представляют собой кодированный акустический сигнал;

- биометрическими (только для считывателей) - представляют собой индивидуальные физические признаки человека (отпечатки пальцев, геометрию ладони, рисунок сетчатки глаза, голос, динамику подписи и т.д.);

- комбинированными - для идентификации используют одновременно несколько идентификационных признаков.

По способу считывания идентификационных признаков считыватели могут быть:

- с ручным вводом - ввод осуществляется с помощью нажатия клавиш, поворотом переключателей или других подобных элементов;

- контактными - ввод происходит при непосредственном, в том числе и при электрическом, контакте между считывателем и идентификатором;

- бесконтактными - считывание кода происходит при поднесении идентификатора на определенное расстояние к считывателю;

- комбинированными.

Классификация средств управления СКУД включает в себя:

- аппаратные средства (устройства) - контроллеры доступа, приборы приемно-контрольные доступа (ППКД);

- программные средства - программное обеспечение СКУД.

СКУД классифицируют по:

- способу управления;

- числу контролируемых точек доступа;

- функциональным характеристикам;

- уровню защищенности системы от несанкционированного доступа к информации.

По способу управления СКУД подразделяют на:

- автономные - для управления одним или несколькими УПУ без передачи информации на центральное устройство управления и контроля со стороны оператора;

- централизованные (сетевые) - для управления УПУ с обменом информацией с центральным пультом и контролем и управлением системой со стороны центрального устройства управления;

- универсальные (сетевые) - включающие в себя функции как автономных, так и сетевых систем, работающие в сетевом режиме под управлением центрального устройства управления и переходящие в автономный режим при возникновении отказов в сетевом оборудовании, центральном устройстве или обрыве связи.

По числу контролируемых точек доступа:

- малой емкости (не более 64 точек);

- средней емкости (от 64 до 256 точек);

- большой емкости (более 256 точек).

По функциональным характеристикам СКУД подразделяют на три класса:

1-й - системы с ограниченными функциями;

2-й - системы с расширенными функциями;

3-й - многофункциональные системы.

Классификация средств КУД по устойчивости к НСД основана на устойчивости к разрушающим и неразрушающим воздействиям по уровням устойчивости:

1) нормальной;

2) повышенной;

3) высокой.

УПУ классифицируют по устойчивости к разрушающим воздействиям.

Устойчивость УПУ устанавливают по:

1) устойчивости к взлому;

2) пулестойкости (только для УПУ со сплошным перекрытием проема);

3) устойчивости к взрыву.

Нормальная устойчивость УПУ обеспечивается механической прочностью конструкции без оценки по показателям устойчивости к разрушающим воздействиям.

Для УПУ повышенной и высокой устойчивости со сплошным перекрытием проема (сплошные двери, ворота) и блокированием объекта в проеме (шлюзы, кабины проходные) устанавливается классификация по устойчивости к взлому, взрыву и пулестойкости, как для защитных дверей, по ГОСТ Р 51072.

Классификация устройств исполнительных (замки, защелки) по устойчивости к разрушающим воздействиям в зависимости от конструкции - по ГОСТ Р 52582, ГОСТ Р 51053, ГОСТ 19091, ГОСТ 5089.

По устойчивости к неразрушающим воздействиям средства КУД в зависимости от их функционального назначения классифицируют по следующим показателям:

- устойчивости к вскрытию - для УПУ и исполнительных устройств (замков и запорных механизмов);
- устойчивости к манипулированию;
- устойчивости к наблюдению для считывателей ввода запоминаемого кода (клавиатуры, кодовые переключатели и т.п.);
- устойчивости к копированию (для идентификаторов);
- устойчивости защиты средств вычислительной техники (СВТ) средств управления СКУД от несанкционированного доступа к информации.

Классификацию по устойчивости к неразрушающим воздействиям: вскрытию, манипулированию, наблюдению, копированию устанавливают в стандартах и нормативных документах на средства КУД конкретного типа.

Классификацию СКУД к НСД определяют, как для систем с централизованным управлением по защищенности от несанкционированного доступа к информации ПО СКУД и средств СВТ, входящих в состав сетевых СКУД.

Классификацию систем КУД по защищенности от НСД к информации устанавливают, как для автоматизированных систем, в соответствии с [1] по Приложению А, таблица А.1, с учетом классификации средств СВТ, входящих в состав сетевых СКУД по устойчивости от НСД к информации в соответствии с [2] по Приложению Б, таблица Б.1.

Таблица А.1

ТРЕБОВАНИЯ К АВТОМАТИЗИРОВАННЫМ СИСТЕМАМ ПО ГРУППАМ

Подсистемы и требования	Группы и классы				
	3		2	1	
	3Б	3А	2Б	1Г	1В
1. Подсистема управления доступом 1.1. Идентификация, проверка подлинности и контроль					

доступа субъектов:					
- в систему	+	+	+	+	+
- к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-	-	+	+
- к программам	-	-	-	+	+
- к томам, каталогам, файлам, записям, полям записей	-	-	-	+	+
1.2. Управление потоками информации	-	-	-	-	+
2. Подсистема регистрации и учета					
2.1. Регистрация и учет:					
- входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+
- выдачи печатных (графических) выходных документов	-	+	-	+	+
- запуска/завершения программ и процессов (заданий, задач)	-	-	-	+	+
- доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	-	-	+	+
- доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	-	-	+	+
- изменения полномочий субъектов доступа	-	-	-	-	+
- создаваемых защищаемых объектов доступа	-	-	-	-	+
2.2. Учет носителей информации	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	+
2.4. Сигнализация попыток нарушения защиты	-	-	-	-	+
3. Подсистема обеспечения целостности					
3.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+
3.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+
3.3. Наличие администратора (службы) защиты информации в АС	-	-	-	-	+
3.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+
3.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+
3.6. Использование сертифицированных средств защиты	-	+	-	-	+

Примечание - Знак "+" означает наличие требований к данному классу, знак "-" - отсутствие требований к данному классу

Б.1. Показатели защищенности от НСД к информации

Таблица Б.1

Наименование показателя	Класс защищенности		
	6	5	4
1. Дискреционный принцип контроля доступа	+	+	+
2. Мандатный принцип контроля доступа	-	-	+
3. Очистка памяти	-	+	+
4. Изоляция модулей	-	-	+
5. Маркировка документов	-	-	+
6. Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+
7. Сопоставление пользователя с устройством	-	-	+
8. Идентификация и аутентификация	-	=	+
9. Гарантии проектирования	-	+	+

10. Регистрация	-	+	+
11. Целостность КСЗ	-	+	+
12. Тестирование	+	+	+
13. Руководство пользователя	+	=	=
14. Руководство по КСЗ	+	+	=
15. Тестовая документация	+	+	+
16. Конструкторская (проектная) документация	+	+	+

Примечание - Знак "-" означает отсутствие требований к данному классу, знак "+" - наличие новых или дополнительных требований, знак "=" - требования совпадают с требованиями к СВТ предыдущего класса

5. СЕТЕВЫЕ ВАРИАНТЫ СКУД

Сетевые варианты могут включать в себя различные элементы автономных систем контроля и управления доступом: считыватели, электромеханические замки, доводчики, турникеты, шлагбаумы, автоматические ворота и.т.д. Только все эти элементы будут собраны в единый комплекс, управлять и контролировать который сможет всего лишь один сотрудник с помощью компьютера. Типовой вариант исполнения сетевой версии СКУД включает следующие элементы:

1. **Головной контроллер.** Это центральное устройство в системе, которое контролирует работу остальных контроллеров;
2. **Второстепенные контроллеры.** Данные устройства подключаются к головному контроллеру с помощью интерфейса RS-485. К второстепенным контроллерам подключаются различные периферийные устройства;
3. **Периферийные устройства.** Это считыватели, турникеты, автоматические калитки, шлагбаумы, электромеханические замки и.т.д. Количество данных устройств зависит от количества дверей и пожеланий конкретного заказчика;
4. **Компьютер с установленным программным обеспечением.** Компьютеров в системе может быть несколько. Программное обеспечение может быть серверным и клиентским. Компьютер с серверным программным обеспечением подключается к головному контроллеру. Серверное программное обеспечение позволяет просматривать информацию со всех контроллеров, блокировать/разблокировать двери, открывать/закрывать двери, загружать поэтажные планы, следить за работой контроллеров с помощью этих планов, составлять картотеку сотрудников и.т.д. Остальные компьютеры по сети подключаются к компьютеру с серверным программным обеспечением. На них устанавливается клиентское программное обеспечение. Клиентское программное обеспечение не позволяет менять какие-либо настройки системы, а только просматривать информацию о состоянии системы.

6. АВТОНОМНЫЕ СКУД

Автономные системы контроля и управления доступом. Предназначены они в основном для санкционированного доступа сотрудников в здание организации. Как правило такие системы устанавливаются на центральные двери, либо на запасные выходы. Системы исполнения могут быть следующие:

1. Малая проходная для одной двери.

Данная система предназначена для малых организаций, штат которых включает не более 1000 сотрудников. Вариантов исполнения данной системы в основном бывает два.

Первый вариант - один автономный считыватель, электромагнитный замок, кнопка выхода. Считыватель может быть как обычным, который открывает замок при поднесении к нему карточки, так и с кодонаборником, который открывает замок при поднесении карточки и при наборе кода, либо просто при наборе кода. Сотрудник, имеющий карточку, сможет войти в свою организацию. Для выхода ему достаточно нажать на кнопку выхода. Такая система является простейшей, не позволяет контролировать сотрудников и не защищает организацию от внештатных ситуаций, т.к. любой человек может покинуть организацию, нажав на кнопку.

Собственно для этого существует второй вариант малой проходной для одной двери. Он состоит из следующих элементов: два считывателя, электромагнитный замок, кнопка выхода. Считыватели ставятся на обеих сторонах двери. Для входа и выхода надо иметь карточку. Если установить считыватели с кодонаборником, то для входа и выхода требуется иметь карточку и знать код. Кнопка выхода ставиться в каком – либо потайном месте. Охранник, используя данную кнопку, может выпускать из организации гостей, не имеющих карточки.

2. Малая проходная для одной двери с возможностью учёта рабочего времени.

Малая проходная с автономными считывателями имеет ограниченные возможности. Она конечно защищает организацию от проникновения в неё нежелательных лиц. Но её минусы очевидны. Карточку можно украсть, а код узнать. Для этого и существуют более сложные системы контроля и управления доступом. Состоит данная система из следующих элементов: контроллер, компьютер с установленным ПО, 2 идентичных считывателя, электромагнитный замок, кнопка выхода. В данном случае алгоритм доступа ничем не отличается от предыдущего, только охранник в данном случае с помощью компьютера и установленного на нём программного обеспечения может сравнивать лицо человека, прошедшего через дверь, с оригинальной фотографией владельца данной карты.

Установленное на компьютере программное обеспечение позволяет вести табельный учёт рабочего времени сотрудников, составлять расписание рабочей недели, праздников и выходных, блокировать/разблокировать проход через дверь, загружать в компьютер поэтажные планы для удобства контроля.

Следует отметить, что в двух вышепредложенных схемах вместо двери могут быть использованы различные автоматические ворота, калитки, откатные двери, турникеты, шлагбаумы и.т.д. Наиболее распространёнными схемами исполнения СКУД являются системы с турникетом и шлагбаумом.

3. Автономная проходная с турникетом.

Как правило крупные офисные здания используют турникеты для удобства доступа посетителей и сотрудников. Стандартная схема автономной проходной включает в себя следующие элементы: контроллер, два считывателя, турникет, пульт для ручного управления турникетами.

4. **Автономная проходная со шлагбаумом.**

Сейчас практически всё современные здания имеют парковку. Для сокращения времени проезда данные парковки могут быть оборудованы автономными системами контроля и управления доступом. Они могут включать в себя следующие элементы: контроллер, два считывателя, которые считывают карточки на расстояния до 100 метров, сам шлагбаум и кнопку для ручного управления шлагбаумом.

7. ПРОЦЕДУРЫ, ВЫПОЛНЯЕМЫЕ СКУД

Процедуры, выполняемые СКУД, делятся на основные и дополнительные.

К основным процедурам относится санкционирование - присвоение каждому пользователю идентификатора, регистрация его в системе и задание для него временных интервалов доступа и уровней доступа.

Решение проблемы идентификации может осуществляться двумя раз личными путями:

- с использованием специализированных элементов-ключей;
- опознаванием конкретного лица по его неотъемлемым характеристикам.

В особенно ответственных случаях оба эти подхода могут быть использованы одновременно, хотя использование второго пути существенно ограничивается очень высокой стоимостью аппаратуры опознавания (по отпечаткам пальцев, голосу, рисунку сетчатки глаза и т.д.). Поэтому чаще всего используется первый подход.

При категорировании объектов доступа необходимо различать:

- доступ на некоторую интегрированную территорию - огороженную забором территорию предприятия;
- доступ в отдельно стоящее здание или отдельный этаж здания и т.д.;
- доступ в конкретное помещение, расположенное на этой территории.

В первом случае говорят о доступе в зону контроля, а во втором - о доступе в помещение.

Как правило, в автоматизированных системах контроля доступа сочетаются контроль обоих видов. При этом может происходить детализация понятия зоны контроля, при которой вся контролируемая территория может разбиваться на несколько непересекающихся зон контроля со своими особенностями доступа. Каждой зоне контроля и каждому помещению с контролируемым входом присущи свои ограничения на вход.

Общий принцип должен быть следующим: чем более ответственный уровень администрации дает права доступа к конкретному объекту (зоне, помещению) и чем меньше лиц имеют такие права, тем более ограниченным должен быть режим доступа и более строгими требования к идентификации.

Режим доступа для помещений должен быть, как правило, более жесткий, чем для зон контроля. Необходимо различать ситуации, когда вход и выход осуществляются по разным правилам.

Все режимы доступа, используемые при автоматизированном контроле, можно разбить на три группы:

- без ограничения доступа;
- доступ по праву доступа;
- запрет доступа.

Режимы свободного прохода применяются для помещений, доступ в которые должен быть постоянно или временно открыт для всего персонала или при аварийных ситуациях. Свободный проход может быть:

- абсолютным и бесконтрольным (фактически соответствует отключению системы контроля);
- абсолютным и контролируемым (проход не запрещается никому, но все проходящие регистрируются);
- условным (например, любой владелец ключа, используемого в системе типа, или любое лицо, знающее правила прохода), как контролируемым, так и неконтролируемым.

Режимы запрета доступа могут применяться в том случае, если необходимо предотвратить доступ ко всем или некоторым помещениям (зонам) на временной или постоянной основе всем, кроме ограниченного числа специально уполномоченных лиц.

Запрет доступа может быть плановым или экстренным, при возникновении особых ситуаций. Режимы доступа в соответствии с присвоенными правами являются основными в системах контроля доступа.

Способ предоставления конкретному лицу прав доступа существенным образом влияет на надежность контроля доступа в целом. Поэтому наиболее целесообразно предоставить такую возможность только одному сотруднику - Администратору Системы Контроля Доступа, который действует на основе принятых в организации административных процедур.

Должна быть исключена возможность изменения предоставленных прав другими лицами, в том числе и их владельцами. Применительно к автоматизированным системам это требует ограничения доступа к используемым техническим средствам.

Наряду с категорией доступа существенную роль играет понятие интервал времени ступа, который описывает часть (части) суток, в течение которых данному контроллеру вешается открывать данный электронный замок. Текущие версии многих автономных СКУД использует два типа интервалов доступа:

- индивидуальные;
- групповые.

И те, и другие назначаются независимо для каждого дня недели. Для каждого дня моет быть назначен более чем один интервал доступа. В таком случае определяемые интервалы не должны пересекаться.

Индивидуальные интервалы доступа используются при работе с сетевыми электронными замками. Они назначаются независимо для каждого контроллера относительно каждого конкретного электронного замка для каждого дня недели.

Групповые интервалы назначаются независимо для каждого электронного замка во всей группе контроллеров, имеющих к нему доступ. Возможности регулирования доступа с помощью групповых интервалов доступа менее гибки, чем при использовании индивидуальных интервалов доступа. При их назначении должны быть соблюдены определенные требования.

Контроль соблюдения режима доступа является важнейшей частью мероприятий по обеспечению безопасности. Он может быть:

- оперативным;
- периодическим.

При оперативном контроле о любых попытках нарушения установленного режима доступа немедленно сообщается специальному лицу - дежурному системы контроля доступа.

При периодическом контроле такие попытки фиксируются и уполномоченное лицо (Дежурный или Администратор), в произвольный момент времени, может ознакомиться с соответствующими записями. В первом случае обеспечивается более высокая степень защищенности контролируемых объектов. И в первом и во втором случае желательно обеспечивать также фиксацию лиц, имеющих право на санкционированный доступ в контролируемые помещения (зоны).

Разрешение доступа или отказ в доступе - выполняется на основании результатов анализа предыдущих процедур;

Регистрация - протоколирование всех действий в системе;

Реагирование - реакция системы на несанкционированные действия (подача предупреждения, тревожных сигналов, отказ в доступе).

К дополнительным процедурам относятся:

- сбор и обработка информации о перемещениях персонала или предметов по объекту;
- организация и учет рабочего времени;
- управление освещением, лифтами, вентиляцией и другой сервисной автоматикой;
- управление приборами телевизионного наблюдения.

9. ИДЕНТИФИКАТОРЫ И СЧИТЫВАТЕЛИ В СКУД

Устройство идентификации доступа (идентификаторы и считыватели) считывает и расшифровывает информацию, записанную на индентификаторах разного типа и устанавливает права людей, имущества, транспорта на перемещение в охраняемой зоне (объекте).

Контролируемые места, где непосредственно осуществляется контроль доступа, например, дверь, турникет, кабина прохода, оборудуются считывателем, устройством исполнительным и другими необходимыми средствами.

Идентификатор - предмет, в который (на который) с помощью специальной технологии занесена кодовая информация, подтверждающая полномочность прав его владельца и служащий для управления доступом в охраняемую зону. Идентификаторы могут быть изготовлены в виде карточек, ключей, брелков и т.п.

Считыватель - электронное устройство, предназначенное для считывания кодовой информации с идентификатора и преобразования ее в стандартный формат, передаваемый для анализа и принятия решения в контроллер. Считыватель - устройство, расположенное, как правило, на стене рядом с дверью или другим преграждающим устройством и предназначенное для чтения идентификационного кода с карт пользователей. В корпусе считывателя может быть установлен светодиод для индикации приглашения к входу в случае успешного считывания кода.

В СКУД существует порядка десяти видов идентификаторов и считывателей, использующих различные способы записи, хранения и считывания кодовой информации, обеспечивающие разный уровень секретности и имеющие существенно отличающиеся цены.

9.1. **Биометрические системы распознавания**

При работе подобных систем считываются и сверяются с базой данных основные биометрические показатели того или иного индивидуума. Чаще всего проверке подвергаются следующие биометрические признаки: отпечатки пальцев, трехмерное изображение головы человека, сетчатка, голос. Самые дорогие и самые точные системы контроля доступа – именно биометрические.

Наиболее перспективным направлением в системах идентификации в настоящее время признаны технологии биометрической идентификации. Устройства биометрической идентификации в системах контроля доступа до недавнего времени были достаточно редким и экзотическим элементом этих систем из-за своей сложности и высокой цены. Однако их главное преимущество перед другими способами идентификации — аутентификация личности, т. е. установление подлинности человека по его физическим признакам, а также развитие современных технических средств, привели к появлению на рынке относительно недорогих и качественных средств биометрического контроля доступа.

При идентификации по индивидуальным биометрическим признакам определяется именно человек — носитель этих признаков, а не выданный ему документ — карта, код, ключ, пароль и т. п. Это является основным отличием данных систем от любых других идентифицирующих устройств.

Системы контроля доступа, использующие подобную идентификацию, начали внедряться с середины 90-х годов. Поскольку стоимость подобных систем в то время была

весьма велика, они применялись лишь в тех местах, где было необходимо обеспечить наивысшую степень защиты. Однако в последние годы с появлением недорогих и мощных микропроцессорных устройств и развитием компьютерных методов анализа образов подобные системы стали применяться все чаще.

Инфракрасный брелок передает идентификационный код в инфракрасном диапазоне. Возможность перехвата для таких устройств ниже, потому что существует конкретная направленность сигнала. Однако такие устройства не слишком широко распространены в России.

9.2. Карта Виганда (Wigand)

Эта пластиковая карта имеет вкрапления из специального магнитного сплава. Магнитная головка считывателя определяет индивидуальный код карты при правильном позиционировании карты по отношению к считывателю. То есть принцип действия схож с магнитными картами, но такие ключи менее подвержены внешним факторам.

Форматом Wiegand нередко называют стандартный 26-битный формат, который характеризуется специфическим расположением двоичных данных. Карты, метки и брелки компании HID могут быть запрограммированы в этом формате.

Сам по себе 26-битный формат — открытый. Являясь промстандартом, этот формат работает почти со всеми системами контроля доступа HID. Он произошел от технологии кодирования данных Wiegand.

9.3. Карта со штрих-кодом

Штрих-код - закодированная с помощью штрихов буквенно-цифровая информация, предназначенная для считывания сканером и дальнейшей компьютерной обработки данных. Пока это самая дешёвая технология изготовления карточек с кодом.

Штрих-код печатается чёрным цветом предпочтительно на белом, золотом или серебряном фоне - фон другого цвета может снизить качество считывания. Минимальный размер штрих-кода - 1 см по высоте и 2,5 см по ширине.

Расположение штрих-кода на пластиковой карте может быть выбрано произвольно, но не ближе 3-х мм от края карты. Возможно горизонтальное или вертикальное ориентирование. Но, разумеется, он не должен запечатывать нанесённую на карту текстовую или графическую информацию.

Нанесение штрих кода на классические пластиковые карты производится двумя способами: на готовую карту с помощью сублимационного термопринтера либо наносится на основу пластиковой карты под специальный защитный слой.

Первый способ относительно быстр и дешев. Термосублимационная печать обеспечивает довольно надёжное закрепление краски на пластике. Как правило, во избежании истирания штрих-кода, сверху пластиковая карта дополнительно покрывается защитным лаком, что существенно сказывается на цене.

При печати же на пластиковой основе штрих-код остается под защитным слоем, как и все изображение и надежно защищен от механических повреждений.

Чаще всего штрих-коды используют для дисконтных карт, подарочных сертификатов, идентификационных и топливных карт.

Отметим, что такая персонализация имеют смысл при наличии как минимум одного компьютера с неким программным обеспечением.

Применение в этих системах штрих-кодирования сводится лишь к приобретению и подключению устройства для считывания штрих кодов под названием сканер штрих-кода.

Нанесением самого штрих-кода на товары или на дисконтные карточки клиентов (карточки постоянных клиентов), предпочтительно пластиковые, пусть занимаются специалисты.

Вариантов физического подключения сканеров к компьютеру не много. Основные это подключение

- через COM-порт, USB-порт и
- в разрыв клавиатуры.

Как правило, к сканеру прилагается драйвер для его работы с компьютером. Но иногда и в драйвере нет необходимости, например, если сканер подключен в разрыв клавиатуры. В этом случае сканер, при считывании штрих кода, автоматически введет в компьютер буквы и цифры кода, вместо ручного введения каждого символа с клавиатуры. Если сканер подключен через COM-порт, такого же эффекта можно достичь, программно назначив его альтернативным устройством ввода:

(Пуск – Настройка - Панель управления - Специальные возможности – Общие -, Поставить "галочку" в альтернативные устройства, нажать "настройка", "ОК", "Применить").

Каждый штрих - код (символика) разработан с точки зрения оптимизации следующих параметров: :

- высокая информационная плотность, или высокое разрешение. Очень маленькие коды

могут быть отпечатаны и использованы на изделиях, где место для крепления ограниченно, например, печатные платы;

- оптимальное расположение данных, когда возможность ошибок чтения практически нулевая;

- легкость дешифровки. Некоторые штрих коды используют простую технологию кодирования и широко поддерживаются производителями сканеров.

Штрих кодыимеют точно определенное содержание данных. Они структурируются для обеспечения удобства большого количества пользователей. Некоторые штрих коды разработаны с поддержкой значительного количества наборов символов, тогда как другие поддерживают только цифровые данные.

Некоторые форматы имеют механизм контроля корректности, заключающийся в вычислении одной части кода по другой. В России используются в основном форматы EAN-13 (EAN-8). Одним из основных компонентов этой технологии является использование сканеров штрих-кодов. Сканеры штрих-кодов различаются как по способу подключения к компьютеру, так и по возможностям. В настоящий момент практически все выпускаемые сканеры способны считывать наиболее популярные форматы кодов, включая EAN-13 (EAN-8), UPC A, UPC E, ITF, Code 39, ISBN. При считывании сканеры автоматически разбирают сканируемый код, проверяют его корректность и могут различными способами модифицировать код (например, производить перекодировку из одного формата в другой). В качестве результата сканеры выдают строку символов, представляющих штрих-код в форме, понятной для человека. По способу подключения сканеры делятся на подключаемые в COM-порт компьютера или в разрыв клавиатуры. В последнем случае сканер имитирует работу клавиатуры и, вследствие этого, к строке со считанным штрих-кодом необходимо добавлять специальные символы в случае, если необходимо отличать ввод штрих-кода от простого набора на клавиатуре.

Технология штрихового кодирования подразумевает уникальность штрих кода для каждого товара, поэтому необходимо централизованное распределение штрих-кодов. Для решения этой задачи в 1977 г. была создана международная некоммерческая и неправительственная организация EAN International, представителем которой в России является "Ассоциация автоматической идентификации ЮНИСКАН/EAN Россия".

Приказом Госстандарта России №92 от 30.04.93 на базе ЮНИСКАН/EAN РОССИЯ образован Технический комитет по стандартизации ТК 355 “Автоматическая идентификация”. Одним из направлений деятельности ТК 355 является разработка, рассмотрение, согласование и подготовка к утверждению государственных стандартов

Российской Федерации. В настоящее время Госстандартом России приняты следующие нормативные документы по стандартизации:

10. ГОСТ Р 51001-96 "Автоматическая идентификация. Штриховое кодирование. Требования к символике "2 из 5 чередующийся" (EN 801);

11. ГОСТ Р 51002-96 "Автоматическая идентификация. Штриховое кодирование. Требования к символике "Код 39" (EN 800);

12. ГОСТ Р 51003-96 "Автоматическая идентификация. Штриховое кодирование. Требования к символике "Код 128" (EN 799);

13. ГОСТ Р 51201-98 "Автоматическая идентификация. Штриховое кодирование. Требования к символике "ЕАН/ЮПиСи" (EN 797).

14. ГОСТ Р 51294.1-99 "Автоматическая идентификация. Кодирование штриховое. Идентификаторы символик".

15. ГОСТ Р 51294.2-99 "Автоматическая идентификация. Кодирование штриховое. Описание формата требований к символике".

16. ГОСТ Р 51294.3-99 "Автоматическая идентификация. Кодирование штриховое. Термины и определения".

17. ГОСТ Р 51294.4-2000 (ИСО/МЭК 15459-1-99)"Автоматическая идентификация. Международная уникальная идентификация транспортируемых единиц. Общие положения".

18. ГОСТ Р 51294.5-2000 (ИСО/МЭК 15459-2-99) "Автоматическая идентификация. Международная уникальная идентификация транспортируемых единиц. Порядок регистрации".

19. ГОСТ Р 51294.6-2000 (ИСО/МЭК 16023-2000) "Автоматическая идентификация. Кодирование штриховое. Спецификация символики MaxiCode (Максикод)".

20. ГОСТ Р 51294.7-2001 (ИСО/МЭК 15416-2000) "Автоматическая идентификация. Кодирование штриховое. Линейные символы штрихового кода. Требования к испытаниям качества печати" с датой введения 1 октября 2001 г.

21. Р 50.1.20-99 (ЕНВ 1649-95) "Автоматическая идентификация. Кодирование штриховое. Факторы, влияющие на считывание символов штрихового кода" (ENV 1649).

9.4 Кодовая клавиатура

Определение пользователя происходит путем набора персонального кода - последовательности цифр - на клавиатуре кодонаборной панели. Обычно данный способ

идентификации используется также в комбинациях с другими, для повышения надежности систем.

Клавиатурные считыватели, хотя и считаются недостаточно защищенными от манипуляций (подбор кода, наблюдение), имеют определенные достоинства, например, разрядность кода может быть выбрана произвольно, код может устанавливаться самим пользователем и произвольно им изменяться, быть неизвестным оператору системы.

Индивидуальный код присваивается каждому из сотрудников. Эта система защищена от утраты вследствие физической потери, однако крайне ненадежно в случае осуществления давления или добровольной передачи постороннему лицу. Улучшить ситуацию могут системы, позволяющие препятствовать подбору кода и тому подобным операциям. Системы с кодовым набором – наиболее дешевые из всех, но ненадежные, поэтому часто комбинируются с другими типами СКУД, например, картами.

9.5. Магнитная карта

Этот тип карт имеет магнитную полосу, которая определенным образом прикладывается к считывателю. Это и является главным камнем преткновения: осуществить это за пару секунд не удастся. К тому же подобные карты и их считыватели подвержены порче под влиянием внешних факторов (размагничивание, загрязнение и т.п.).

Карты с магнитной полосой уже более 20 лет используется в системах контроля доступа. Кредитные карты, билет на проезд в общественном транспорте или посадочный талон на самолёт - применения технологии карт с магнитной полосой очень разнообразны. Магнитные карты срабатывают при проведений в определённом направлении и с определённой скоростью по щели считывателя. Магнитная полоса наносится на одну из сторон пластиковый карточки. После этого её кодируют - записывают информацию.

Магнитная полоса содержит закодированную запись данных владельца карты. Считывающее устройство мгновенно расшифровывает информацию, содержащуюся на магнитной полосе.

Магнитная полоса на карте имеет три дорожки. Карты с магнитной полосой делятся по типу полосы на LoCo - низкоэрцитивная магнитная полоса (на 300 эрстед), HiCo - высокоэрцитивная магнитная полоса (помехозащищенные, до 4000 эрстед) и MeCo - около 2750 эрстед. Эти виды характеризуется разной степенью устойчивости к магнитным полям.

На магнитные дорожки возможна запись только латинских букв, буквы кириллицы вызывают ошибку в работе записывающего устройства.

- первая дорожка хранит имя держателя карты;
- вторая дорожка хранит номер карты и срок годности карты;
- третья дорожка позволяет записывать дополнительную информацию (используется редко)

Достоинства:

- существенным преимуществом магнитных карт является их невысокая стоимость.

Недостатки:

- магнитная карта ограничена по объёму информаций, которая может быть записана на магнитной ленте;
- низкая безопасность данных;
- магнитная карта достаточно чувствительна к внешним воздействиям – загрязнениям, царапинам, влаге;
- точное позиционирование в считывателе.

Средний срок службы магнитных карт 1 – 2 года, затем магнитный слой стирается. Магнитные карты применяют, как правило, в системах, где предусмотрена частая замена карт. С другой стороны это недорогая и легко внедряемая технология.

Магнитная лента имеет три вида коэрцитивности (определяет коэффициент намагничиваемости):

- низко коэрцитивной силой LoCo (300 эрстед)
- средней коэрцитивной силой MeCo (2750 эрстед)
- высоко коэрцитивной силой HiCo (4000 эрстед).

Кодировка магнитной ленты осуществляется по трём дорожкам.

Номер дорожки	Количество знаков	Кодируемые данные	
Первая дорожка	76 знакомест	Цифры, буквы, знаки	QWERTYUIOPASDFGHJKLZXCVBNM1234567890 : ; = + ( ) – ‘ " ! @ # ^ & * < > / / Латинские буквы ЗАГЛАВНЫЕ. " % " – начало записи, " ? " – конец записи в строке, при считываний не отображаются.
Вторая дорожка	37 знакомест	Цифры, знаки	1234567890 = Знак = отображает пробел " ; " – начало записи, " ? " – конец записи в строке, при считываний не отображаются.
Третья дорожка	104 знакомест	Цифры	1234567890 = " ; " – начало записи, " ? " – конец записи в строке, при считываний не отображаются.

Считыватель для магнитных карт своим внешним видом и размерами напоминает пачку сигарет с прорезью, а функционально представляет собой магнитный тракт магнитофона - магнитную головку, к которой специальный ролик прижимает магнитную карту. Для считывания кода с магнитной карты пользователю следует провести ею в

прорези считывателя вдоль всей ее магнитной полосы. Наиболее развитые магнитные считыватели имеют PIN-клавиатуру и позволяют программировать функции считывателя.

9.6. Бесконтактная карта (Proximity)

Главное удобство такой карты – отсутствие необходимости четкого позиционирования ее по отношению к считывателю. Различные модели считывателей карт проксимити имеет рабочее расстояние от 5 см до 2 м. Важным преимуществом также является высокая скорость прохода через устройство контроля доступа, что очень удобно при большом потоке посетителей. Также можно не беспокоиться о сохранности карты – она мало подвержена влиянию окружающей среды; ее можно только потерять. Существуют тонкие и более толстые карты, которые допускают возможность нанесения изображения, в том числе и фото владельца, а также ключи в виде брелоков, автомобильных ключей и т.д.

Считыватель Proximity генерирует электромагнитное излучение определенной частоты (обычно 125 кГц) и при внесении Proximity-карты в зону действия считывателя это излучение через встроенную в карту антенну подпитывает электронику карты. Получив необходимую энергию для работы, карта пересылает на считыватель свой идентификационный номер с помощью электромагнитного импульса определенной формы и частоты. Длительность такого цикла составляет обычно около 0,1 с.

Основной характеристикой Proximity - считывателя является расстояние, на котором происходит уверенное считывание кода, которое для распространенных и недорогих считывателей равно 6 - 10 см. Лучшие и достаточно дорогие считыватели обеспечивают расстояние считывания до 60 - 80 см. На таких расстояниях можно вообще не вынимать идентификатор из кармана: система допустит вас в защищенное помещение просто при подходе к двери. (Здесь следует учесть, что вы можете просто пройти рядом с дверью, не имея намерения заходить в защищенное помещение, блокировка с исполнительных механизмов двери при этом будет снята.)

9.7. Радиочастотная идентификация (RFID-системы)

Изначально, технология RFID использовала диапазон низких частот, поэтому LF (Low Frequency) – технология, принятая для самого старого варианта RFID, которая использовалась главным образом в производстве и сельскохозяйственных направлениях деятельности. ISO 11784 и ISO 11785 - два широко распространенных стандарта в области низких частот (125 кГц), которые широко использовались и используются в области идентификации и слежения за животными. При этом ISO 11784 определяет структуру данных признака животных (в этом стандарте, животные могут быть идентифицированы

кодом страны и уникальным национальным удостоверением личности). ISO 11785 был посвящен техническим аспектам коммуникации.

Но в скором времени развитие самой технологии (выход на новые частоты) и областей ее применения (структура данных, протоколы обмена) настолько ускорило темп, что число стандартов ISO значительно выросло (таблица 3).

Таблица 3. Стандарты ISO/IEC в области RFID

Стандарт ISO/IEC	Название	Статус
ISO 11784	Радиочастотная идентификация животных. Структура информации.	Изданный стандарт 1996
ISO 11785	Радиочастотная идентификация животных. Техническая концепция.	Изданный стандарт 1996
ISO/IEC 14443	Карты идентификации. Бесконтактные карты с интегральной схемой. Proximity-карты	Изданный стандарт 2000
ISO/IEC 15693	Карты идентификации. Бесконтактные карты с интегральной схемой. Vicinity-карты.	Изданный стандарт 2000
ISO/IEC 18001	Информационная технология. Технология AIDC. RFID для управления объектами. Требования к приложениям.	Изданный стандарт 2004
ISO/IEC 18000-1	Интерфейс радиосвязи (часть 1).Общие параметры каналов связи для разрешенных частотных диапазонов.	Изданный стандарт 2004
ISO/IEC 18000-2	Интерфейс радиосвязи (часть 2). Параметры интерфейса радиосвязи с частотой до 135 кГц	Изданный стандарт 2004
ISO/IEC 18000-3	Интерфейс радиосвязи (часть 3). Параметры интерфейса радиосвязи на частоте 13.56 МГц	Изданный стандарт 2004
ISO/IEC 18000-4	Интерфейс радиосвязи (часть 4). Параметры для интерфейса радиосвязи на частоте 2.45 ГГц	Идет заключительное утверждение как мирового стандарта
ISO/IEC 18000-5	Интерфейс радиосвязи (часть 5). Параметры для интерфейса радиосвязи на частоте 5.8 ГГц	Идет заключительное утверждение как мирового стандарта
ISO/IEC 18000-6	Интерфейс радиосвязи (часть 6). Параметры для интерфейса радиосвязи в диапазоне частот 860-930 МГц	Изданный стандарт 2004
ISO/IEC 18000-6	Интерфейс радиосвязи (часть 6). Параметры для интерфейса радиосвязи на частоте 433.92 МГц	Идет заключительное утверждение как мирового стандарта
ISO/IEC 15960	Синтаксис данных. Требования к прикладному сообщению.	Изданный стандарт 2004
ISO/IEC 15961	RFID для управления объектами. Протокол передачи данных - прикладной интерфейс	Изданный стандарт 2004
ISO/IEC 15962	RFID для управления объектами. Протокол правил кодировки данных и логических функций памяти	Изданный стандарт 2004
ISO/IEC 15963	RFID для управления объектами. Уникальная идентификация радиочастотной метки.	Идет заключительное утверждение как мирового стандарта

В настоящее время для каждого из выделенных частотных диапазонов действуют свои стандарты со своей степенью проработки. В настоящее время выделяются следующие диапазоны частот, для которых существуют международные стандарты ISO: 125-135 кГц, 860-930 МГц, 13.56 МГц и 2.45 ГГц (диапазоны 5.8 ГГц и 433.22 МГц в настоящее время практически не используется). На каждом из выделенных диапазонов работают приложения и прикладные системы, схожие по функциям (Таблица 4).

Таблица 4. Стандарты ISO по частотному диапазону

Рабочая частота	Стандарт	Приложения
125 кГц 135 КГц	ISO 14223 ISO 11784 ISO 11785 ISO 18000-2	Разработаны для идентификации животных (в т.ч. домашнего скота), но используются достаточно широко, например, в автомобильных иммобилайзерах
13.56 МГц	ISO 14443 ISO 15693 ISO 10373 ISO 18000-3	Бесконтактные смарт-карты для широкого круга приложений. Бесконтактные метки для приложений логистики, идентификации товаров и т.д. Методы тестирования Proximity и Vicinity карт для диапазона 13.56 МГц
860-930 МГц	ISO 15961 ISO 15962 ISO 15963 ISO 18000-6	Бесконтактные метки для приложений логистики, идентификации товаров со средней дальностью
2.45 ГГц	ISO 15961 ISO 15962 ISO 15963 ISO 18000-4	Бесконтактные метки для приложений логистики, идентификации товаров с увеличенной дальностью

Ниже приведены параметры, соответствующие наиболее распространённым стандартам RFID для HF-диапазона частот.

Таблица 5. Стандарты ISO по частотному диапазону

Характеристика	ICODE 1	ISO 15693	ISO 14443 A	ISO 14443 B
Серийный номер, bit	64	64		
Длина ключа, bit			48	48
Скорость обмена, кБод	26,5	53	106	106
Модуляция	10% ASK	10% или 100% ASK	100% ASK	10% ASK
Метод кодирования	Pulse position modulation	Pulse position modulation	Модифицированный код Миллера	NRZ-L код
Частота поднесущей, кГц	423	423	847	847
Модуляция поднесущей	-	100% ASK	ON/OFF keying	PSK
Кодирование	Манчестерский код	Манчестерский код	Манчестерский код	NRZ-L код

поднесущей				
Длина CRC, bit	8	16		
Механизм антиколлизии	Временные слоты	Временные слоты	Бит-ориентированный	Ответ по запросу

Кроме широко известных стандартов ISO, широкое распространение и популярность получили стандарты EPC Global. EPC Global стала заниматься стандартизацией после того, как основанная в 1999 году при Массачусетском университете Auto ID Labs, занимавшаяся вопросами определения стандартов в области сверхвысоких частот (UHF), закрылась в октябре 2003 года. Чтобы завоевать рынок и быть понятной потребителям RFID компания EPC Global начала с того, что выделила определенные функциональные группы меток, назвав их классами. Еще при Auto ID Labs были выделены следующие группы (классы):

- Класс 0. Группа пассивных меток для идентификации объекта (Passive Identity Tag). Эти метки содержат только так называемый «электронный код продукта» (Electronic Product Code, EPC) в неизменяемом виде и использующий проверку CRC для обнаружения ошибок.
- Класс 1. Группа пассивных меток с функциональными возможностями (Passive Functional Tag). Эта большая группа меток содержит все метки, имеющие какие либо дополнительные функции, отличающие их от первой группы. Примером таких функции могут быть перезаписываемый EPC, шифрование данных и т.п.
- Класс 2. Группа «полупассивных» меток (Semi-Passive Tag). К этой группе были отнесены все метки, использующие дополнительно источник питания. При этом основным источником питания должен являться считыватель, а точнее, излучаемая им энергия.
- Класс 3. Группа активных меток (Active Tag). Эти метки содержат встроенный источник питания, полностью обеспечивающий метку необходимой энергией вне зависимости от считывателя.
- Класс 4. Группа активных RFID-меток (RFID Tag). Эти метки не только содержат встроенный источник питания, но и набор определенной логики, позволяющей метке обмениваться данными с такой же меткой или обычным считывателем.

В настоящее время существует два поколения стандартов EPC (Generation 1, Generation 2). В первом поколении были определены только метки класса 0 и класса 1(Class 0, Class1). Метки класса 0 (C0g1) программировались во время изготовления и получали атрибут «только чтение («R/O»). В метки класса 1 (C1g1) информация могла быть записана пользователем только один раз, они получили атрибут «одна запись, множественное чтение («WORM»). Класс 0 и класс 1 имеют различные протоколы для

работы со считывателем. Следует упомянуть и о модификациях классов, которые поддерживаются так называемыми «открытыми» стандартами EPC Global.. Наиболее широко используемые модификации это класс 0+ (C0+g1) –отличается размером памяти (96 бит вместо принятых изначально 64 бит) и класс 1b (C1bg2), где всего 128 бит, 96 (код EPC) из которых доступно для многократной записи.

Толчком к созданию меток класса 2 поколения послужил спрос на метки, содержащие большее количество информации и имеющие возможности множественной записи («WMRM»). Ответом EPC Global стали метки первого поколения класса 2 (C2g1), поддерживающие оба протокола обмена данными со считывателем.

Однако, развитие RFID-технологий шло такими высокими темпами, что в 2003 EPC Global, чтобы угнаться за столь быстро развивающейся отраслью начинает выпускать второе поколение стандартов. Чтобы избежать проблем, возникающих при работе с метками первого поколения, EPC Global ввела общий протокол обмена данными для всех продуктов второго поколения. Протокол изначально разрабатывался для меток класса 1 второго поколения, но должен быть пригоден для работы с разрабатываемыми в перспективе классами (планируется создать метки класса 2, 3 и 4).

В настоящее время, метки класса 0 и класса 1 доступны для коммерческого использования. 96-битовый EPC обеспечивает уникальные идентификаторы для 268 миллионов компаний. Каждый изготовитель может иметь 16 миллионов классов объекта и 68 миллиардов регистрационных номеров в каждом классе. Есть и новые схемы нумерации, которые начинаются 128-битовыми и 256-битовыми регистрационными номерами, чтобы обеспечить совместимость с новыми выпускаемыми стандартами второго поколения.

Сеть EPC, или как ее еще называют UCCNET, отслеживает теговые объекты EPC, в процессе их движения через цепь поставки из источника к потребителю. Сеть EPC состоит из следующих основных компонентов, которые используются в системе стандартов:

- ONS (Object Naming Services) -службы именования объектов, аналог DNS (Dynamic Named Services) типичной компьютерной сети. Каждый признак EPC привязан к детальной информации об объекте через локальную сеть (LAN) или Web
- Savant - технология программного обеспечения, служащая «нервной системой» для сети, управляющая потоком данных между метками и считывателями.
- PML (Physical Markup Language) – язык физического обозначения, поднабор из XML-языка, который был определен как стандартная платформа развития для сети EPC

Индустрия RFID быстро движется вперед, расширяя текущие стандарты и создавая новые, требуемые для международного внедрения технологии. ISO - глобальная власть в

области стандартизации, и EPC Global - главная сила на рынке RFID, располагающая большой поддержкой промышленности и потребителей, в настоящее время больше соперничают, чем сотрудничают, что приводит к малоэффективной политике управления мировыми стандартами. Так, в настоящее время, стандарты EPC Global охватывают следующие области (Таблица 6).

Таблица 6. Стандарты EPC Global

Стандарт EPC Global	Название, содержание
Стандарты данных метки EPC	Определенные схемы шифрования номера объекта для версии EAN.UCC Global Trade (GTIN®), а также следующих стандартизованных данных: EAN.UCC Serial Shipping Container Code (SSCC®), EAN.UCC Global Location Number (GLN®), EAN.UCC Global Returnable Asset Identifier (GRAI®), EAN.UCC Global Individual Asset Identifier (GIAI®), General Identifier (GID).
Спецификации класса 0 UHF	Коммуникационный протокол и интерфейс для класса 0 на чатоте 900 МГц
Спецификации класса 1 UHF	Коммуникационный протокол и интерфейс для класса 1 на частоте 860 - 930 МГц
Спецификации класса 1 UHF, второе поколение	Коммуникационный протокол и интерфейс для класса 1 на частоте 860 - 930 МГц, основанный на первом поколении класса 1
Спецификации класса 1 HF	Коммуникационный протокол и интерфейс для класса 1 на частоте 13.56 МГц
Протокол считывателя	Обмен сообщениями сообщений и протокол между считывателями меток и поддерживающим EPC программным обеспечением
Спецификация Savant	Спецификация для служб Savant, выполняющих запросы приложений в пределах сети EPC Global
Спецификация ONS	Спецификация для использования ONS, при извлечении информации, связанной с EPC
Спецификация ядра PML	Спецификация для общего набора словарей, который используется в пределах глобальной сети EPC, обеспечивающая стандартизированный формат данных, полученных считывателями.

Наиболее интересны стандарты EPC Global второго поколения (Gen 2), позиционируемые компанией как единый мировой стандарт.

Gen 2 – результат процесса стандартизации, управляемого EPC Global, дочерней компанией Uniform Code Council и EAN International, международных организаций по стандартизации, ответственных за широкое внедрение штрих-кода (Universal Product Code UPC). Так Symbol - член-учредитель EPC Global, поддерживает обе технологии Gen 1 и Gen 2, выпуская считыватели, которые уже сейчас можно программно перевести на Gen 2, и метки Gen 2, которые скоро поступят в продажу.

Ожидается, что протокол EPC Global Gen 2 станет лидирующим стандартом для RFID с рабочей частотой систем в UHF диапазоне 900 МГц, который преодолевает многие ограничения решений EPC Global Class 0 и Class 1 первого поколения.

Gen 2 представляет собой концепцию с улучшенными качествами и стандартами работы, такими как функционирование нескольких считывателей в непосредственной

близости друг от друга, соответствие всем нормам мировых регулирующих органов, высокий уровень качества считываемости меток, высокая скорость считывания, возможность многоразовой записи информации на метки и повышенный уровень безопасности.

Радиоканальное устройство позволяет считывать идентификационный код на большом расстоянии, но может быть легко взломано, как любое устройство, работа которого основана на использовании радиочастот. Поэтому есть необходимость применения схем «блуждающих» кодов.

Карта со встроенным чипом и контактами для считывателя, хорошо защищена от взлома. В последнее время применяется не слишком часто. Считыватели радиоканальных карт установлены на предприятиях, засекреченных менее основательно, нежели вышеозначенные. Это самые распространенные объекты, безопасность которых, несомненно, важна, но скорее на бытовом, нежели на государственном уровне. Существуют различные протоколы передачи информации, используемые при работе радиоканальных считывателей: Em-Marin, Deis-ter, Hitag1/Hitag2, HID. Все они предполагают использование при работе частоты в 125 кГци при проведении сеанса связи между считывателем и картой передают в открытом виде UIN карты. Основной сильной стороной считывателей, основывающихся на работе с радиоканалами, это отсутствие задержек при идентификации, работа на расстоянии от 0 до 1 метра, невысокая стоимость и предельная простота в обслуживании. Но простой доступ к радиоканалу в момент открытой передачи UIN позволяет легко перехватить эту информацию, которую позже можно будет использовать для незаконного доступа на объект. В этом случае может использоваться функция запрета повторного прохода. Это может стать проблемой для личностей, планирующих несанкционированный визит, однако от копирования карты и ее дальнейшего использования злоумышленником не защитит. В целях обеспечения безопасности именно от копирования идентификационных данных используется новая Smart-технология. Для сеанса связи между считывателем и Smart-картой и используется частота 13,56 МГц. Smart-протоколы бывают следующих видов: Legic, Mifare, iC-lass. Общей особенностью перечисленных протоколов является то, что каждая Smart-карта оснащена встроенной памятью с несколькими секторами и вычислительным процессором. Чем выше частота передачи, тем больше скорость обмена данными между считывателем и картой. Плюс к тому, в отличие от обыкновенного радиоканального считывателя, обмен данными происходит в три этапа, каждый из которых представляет собой посылку разнообразной по содержанию информации. Это препятствует копированию идентификационного номера карты. Например, карта

стандарта Mifare при попадании в рабочее поле Smart-считывателя отправляет ему не только UIN, но и случайное число. Считыватель отправляет обратно в карту обработанное число; такой обмен происходит еще раз. После второго вычисления со считывателя на контроллер УПУ направляется номер карты, который, в случае совпадения с данными контроллера, служит ключом для пропускного устройства. Исходная информация для вычислений меняется раз от раза. Таким образом гарантируется подлинность карты стандарта Mifare, а не использование ее копии. Исходя из этого, можно сказать, что копирование данных путем вторжения в радиоканал будет бесполезным. Причем из-за разбиения памяти на сектора Smart-карты могут обеспечивать доступ к различным отделам и помещениям охраняемого объекта: ведь ту информацию, которая в случае радиоканальной идентификации пришлось бы записывать на разные карты, в памяти Smart-карты разносятся в разные сектора. Контроллеры таких систем контроля и управления доступом при этом могут быть не связаны между собой. Когда система состоит из автономных контроллеров, Smart-карта связывает оператора СКУД и недоступные для него пункты доступа. Оператор может внести изменения в Smart-карту, а не в удаленный контроллер. Такая централизованность позволяет экономить человеческие и материальные, а также временные ресурсы. Еще эта характеристика Smart-карт может обеспечивать системность СКУД и связывание их в единую сеть с единым головным рабочим местом оператора, которая может быть значительно разнесена по пространственным характеристикам. Таким образом, можем сделать следующие выводы: по результатам нашего анализа особенностей радиоканальной, биометрической и Smart-технологий обеспечения безопасности объектов, выбор требуемой системы контроля и управления доступом должен основываться на уровне требований к безопасности охраняемого объекта. Радиоканальные карты удобны для использования на предприятиях с большим количеством работников, имеющих доступ в закрытую зону, а также с требованиями в плане безопасности, близкими к стандартным, так как они наименее хорошо защищены от перехвата данных и передачи. Smart-технологии обеспечивают большую безопасность, но все же они не гарантируют невозможность передачи карт посторонним лицам. Биометрические же системы необходимо применять на объектах с высокой секретностью, так как могут наиболее достоверно идентифицировать личность входящего там, где их применение в связи с высокой стоимостью аппаратуры будет оправдано.

9.8. Электронный ключ

Такое устройство непременно должно иметь контакты, необходимые для работы считывателя. Через них в момент контакта передается идентификационный код. Широко распространена система "touch memory" (фирма Dallas Semicindactor). Сам чип находится в стальном корпусе небольших размеров. При соприкосновении корпуса со считывателем происходит передача кода. В основном имеют вид брелока, но могут применяться и в виде карточек. Устойчивость к изнашиванию и вредным факторам большая.

Аппаратные ключи защиты состоят из собственно ключа, подключаемого к LPT или COM-порту компьютера (недавно анонсированы ключи, подключаемые к USB-шине), и программного обеспечения (драйверов для различных операционных систем и модуля, встраиваемого в защищаемую программу).

Аппаратная часть таких ключей выполнена на микросхемах FLASH-памяти, на PIC-котроллерах или на заказных ASIC-чипах. Эта элементная база отличается очень низким энергопотреблением, поэтому для питания ключей используются выводы, изначально для этого не предназначенные (-AUTO FEED, -INIT, -SLCT IN, -STROBE или одна из информационных шин для LPT-порта; DTR, RTS для COM-порта). Информационный обмен между ключом и компьютером происходит, обычно, в последовательном виде, с использованием стробирующего сигнала, формируемого драйвером. В качестве выходных информационной и стробирующих линий используются вышеперечисленные выводы, а в качестве входной линии используются сигналы –STROBE, -ACK, BUSY, PE, SLCT или ERROR для LPT-порта и DSR, CTS для COM-порта.

Конечно, аппаратные ключи, подключаемые к LPT- и COM-портам, должны обеспечивать “прозрачный” режим обмена по стандартным для этих портов протоколам. Например обмен с ключами, подключаемыми к LPT-порту, будет вестись только при пассивном уровне сигнала –SLCT IN (т.е. “принтер не выбран”), а обмен с ключами для COM-портов будет происходить только при пассивном уровне DTR (“Data terminal ready”). Впрочем, эти ухищрения все равно не помогают избежать конфликтов со стандартными устройствами, предназначенными для подключения к данным портам (последними моделями принтеров и сканеров, использующих двунаправленный обмен по параллельному порту или с манипуляторами типа “мышь” и модемами, подключаемыми к последовательному порту). От подобных недостатков должны быть свободны ключи, подключаемые к USB-шине, но пока их серийное производство только начинается.

Самый простой и самый легко взламываемый - ключ на основе FLASH-памяти. Основная его идея в том, чтобы перед продажей защищаемого программного обеспечения записать в ключ некоторые данные и/или части программного кода, а на этапе проверки легальности использования ПО считать эти данные из ключа. Ломается защита примерно

так: определяется алгоритм обмена информацией между компьютером и ключом, считывается информация из FLASH-памяти ключа и пишется соответствующий эмулятор (драйвер, который подменяет собой штатный драйвера электронного ключа и - вместо обмена с реальным устройством - передает прикладной программе заранее подготовленные данные). Кроме того, такие ключи обладают наименьшей степенью прозрачности для стандартных протоколов обмена (т.к. данные, не предназначенные для ключа, теоретически могут быть восприняты им как команда на чтение или запись FLASH-памяти, что приведет либо к порче хранимой информации, либо к нарушению протокола обмена с другим устройством, подключенным к тому же порту компьютера).

Ключи, сделанные на основе PIC или ASIC-чипов, имеют на порядок большую устойчивость к взлому и “прозрачность” для штатных протоколов обмена. Обе эти микросхемы представляют собой контроллеры, содержащие в себе процессор, некоторое количество оперативной памяти, FLASH-память команд и память для хранения микропрограммы. Микропрограмма и внутренняя память обычно защищается от внешнего считывания, так что сделать аппаратную копию ключа довольно проблематично. Основное отличие PIC-ключей от ASIC-ключей в том, что PIC-чипы программируются разработчиком ключей (т.е. он может относительно легко изменить алгоритмы работы), а ASIC-чипы являются заказными микросхемами (т.е. алгоритмы жестко задаются на этапе производства микросхем). Поэтому ASIC-ключи получаются более дешевыми, чем собранные на основе PIC-чипов, но по этой же причине защита на их основе менее надежна (определив алгоритм обработки данных в одном из ASIC-чипов, можно написать эмулятор ключа для всей партии, которая - в силу особенностей производства - обычно бывает достаточно большой). Широко известен случай, когда был определен алгоритм работы электронного ключа производства компании “Aladdin Software Security R.D.” (как оказалось, данная функция может быть реализована одной строкой на языке C), после чего появилось большое количество эмуляторов ключей данной фирмы. И разработчики ничего не могли с этим поделать, так как для изменения алгоритма им пришлось бы заказывать производство новой партии микросхем.

Программная часть защитного комплекса состоит из драйвера аппаратного ключа и модуля, встраиваемого в прикладную программу.

1. Драйвер ключа.

Так как ни одна уважающая себя операционная система не позволит прикладной программе напрямую общаться с портами ввода/вывода, требуется наличие драйвера, выполняющегося в режиме ядра ОС. Это условие является обязательным для всех клонов Unix, Novell Netware, MS Windows NT.

Задача драйвера – обеспечить самый низкий уровень обмена данными между ключом и прикладной программой. Для ключей, подключаемых к COM- и LPT-портам, драйвер отвечает за формирование синхронизирующих и информационных сигналов на выходах соответствующих разъемов и за расшифровку последовательного кода, получаемого от аппаратного ключа. Кроме того, для PIC- и ASIC-ключей драйвер формирует инициирующую последовательность (данные, приняв которые, ключ начинает обрабатывать все последующие данные по заданному алгоритму).

2. Встраиваемый модуль.

Как уже было сказано выше, для ключей на основе FLASH-памяти защита заключается в считывания из ключа некоторых данных и/или участков программного кода. Для PIC- и ASIC-ключей защита строится по принципиально другому методу. На этапе программирования ключа (или производства ASIC-чипа) в него записывается микропрограмма, реализующая некоторую функцию $y = F(x1,x2,\ldots xn)$, где $x1\ldots xn$ – входные параметры, а y – выходной параметр. Обычно один или несколько параметров $x1\ldots xn$ представляют собой случайные числа (для затруднения определения вида функции F), один из параметров – уникальный номер ключа (“серийный номер”), еще один - идентификатор защищаемого программного обеспечения, и т.п.

После обработки ключом входных параметров он формирует и выдает в компьютер выходное значение y. Это значение передается в модуль, интегрированный в прикладную программу, где над этим значением и параметрами x1…xn производится преобразование вида $y' = f(y,x1,x2\ldots xn)$.

Результирующим значением y’ могут быть константы, необходимые для работы программы, участки программного кода, адреса подпрограмм и т.п. При этом необходимое условие - невозможность восстановления функции $F(x1,x2\ldots xn)$ по функции $f(y,x1,x2\ldots xn)$, которую довольно легко получить, реассемблировав участок прикладной программы, отвечающий за проверку данных, полученных от ключа.

При наличии в ключе энергонезависимой памяти и/или таймеров можно добавить их текущие значения в качестве аргументов функции F(x1,x2…xn), что расширяет возможности построения систем защиты.

Для обеспечения защиты от взлома применяются:

- защита от реассемблирования (условные и безусловные переходы по содержимому регистров или ячеек памяти, после которых ставятся несколько байт, реассемблируемых в реальную команду процессора; “размывание” программного кода путем размещения его в разных местах программного модуля с выполнением безусловных или неочевидных условных переходов после каждой ассемблерной команды),

- защита от трассировки (перехват INT1 и INT3, издевательства над регистрами SS/SP/ESP, работа в режиме запрещенных прерываний и т.п.),
- защита от отладчиков (проверка их наличия через API-функции),
- проверка изменения кода драйвера ключа или встраиваемого модуля (проверка контрольной суммы, проверка по контрольным точкам и т.п.).

Если система защиты обнаруживает попытку взлома, работоспособность прикладной программы намеренно нарушается. Это может проявляться и как невозможность запуска прикладной программы, и как ее неправильное функционирование. В последнем случае взлом защищаемой программы становится еще труднее, т.к. не понятно, на каком этапе сработала защита.

10 . ИНТЕРФЕЙСЫ СКУД

Классические контроллеры СКУД подключаются по интерфейсу RS-485, причем до нескольких десятков на одну линию интерфейса.

При относительно низкой стоимости и простоте интерфейс имеет достаточно хорошие характеристики, в большинстве случаев достаточные для решения задач обмена информацией между компонентами СКУД.

RS-485 существует и применяется давно, но говорить о том, что он морально устарел, пока, наверное, всё-таки еще рано. Нет проблем с поставкой аппаратных драйверов. Интерфейс знаком огромному количеству разработчиков, понятно как с ним работать. Самый существенный недостаток RS 485 – невысокая пропускная способность и большие ограничения при организации сетей типа «мастер-ведущий» для взаимного межконтроллерного обмена. Проектировать на основе этого интерфейса мощные современные системы с большим объемом передаваемой информации и развитой логикой межкомпонентного «общения» достаточно проблематично. Еще одно ограничение – необходимость прокладки выделенных линий связи и дальность чуть более километра (далеко не все системы устойчиво работают при использовании дополнительных промежуточных усилителей сигнала). Если, например, объект, на котором установлен какой-то сегмент системы, удален на большее расстояние или нет возможности для прокладки дополнительного кабеля, объединять компоненты системы по этому интерфейсу бывает весьма сложно.

По своей природе RS-485 – это интерфейс типа «ведущий – ведомый», где ПК поочередно опрашивает подключенные на линию контроллеры.

На каждый запрос предполагается ответ, а если его по какой-то причине нет, то контроллер считается неисправным. Тайм-аут ожидания ответа на может быть слишком большим, чтобы скорость реакции системы при наличии не отвечающего контроллера оставалась адекватной. Обычно тайм-аут не превышает удвоенной длительности ответа контроллера, что составляет примерно 50–100 миллисекунд. Если ответа нет дольше, значит, контроллер неисправен.

Вместе с тем задержки до нескольких десятков миллисекунд в цепочке компьютер – драйвер виртуального порта – стек TCP/IP – сеть Ethernet – маршрутизатор (коммутатор) – асинхронный сервер – контроллер могут случаться достаточно регулярно, что приводит к фактической неработоспособности рассматриваемого решения.

Таким образом, без переделки ПО самого контроллера работоспособную систему получить сложно. Квалифицированное решение выглядит иначе: в контроллере устанавливается контроллер Ethernet (аналог сетевой карты в ПК), с которым напрямую взаимодействует микропроцессор контроллера СКУД. Естественно, что ПО контроллера в части обмена с ПК кардинально меняется. Таким образом, СКУД с Ethernet – это достаточно сложная новая разработка, и компания-производитель должна быть на нее мотивирована рыночной ситуацией.

Появившись в СКУД относительно недавно, интерфейс Ethernet получил широкое распространение, и эта экспансия продолжается. Что, в общем-то, не удивительно, ведь по оценкам экспертов примерно 80 процентов объектов, которые нуждаются в оборудовании системами контроля и управления доступом, - это современные офисные, промышленные и прочие здания. Сегодня на всех таких объектах уже существует инфраструктура локальной сети. И использовать её на подобных объектах – это логично, удобно и очень выгодно с точки зрения материальных затрат. В самом деле, зачем прокладывать дополнительные кабели, если можно подключить систему к уже существующей сети. Это – одно из основных достоинств интерфейса. Также нельзя не отметить и его высокую пропускную способность. Сегодня скорости в 100 Мбит – обыденное явление, поэтому не вызывает проблем необходимость обмена большими объемами информации, по сравнению с тем же RS 485. Кроме того, нет ограничений и препятствий для организации обмена информацией между компонентами системы (например, между контроллерами) Безусловно, есть и недостатки, как же без них? Первый заключается в том, что стандартная дальность Ethernet составляет 100-150 м. Для обеспечения большей дальности связи нужно использовать оптоволокно с конверторами, либо через каждые 150 метров ставить усилители сигнала.

Еще более важный момент – защита передаваемых данных по сети. Подключение оборудования в общую локальную сеть предприятия требует принятия дополнительных мер по обеспечению информационной безопасности. Я имею в виду шифрование данных, передаваемых от контроллеров к серверу и обратно, а также грамотное администрирования трафика. Понятно, что, если контроллер подключен к обычной корпоративной сети, и кто-то из сотрудников «перекачивает» полнометражный фильм, то данный сегмент сети будет какое-то время физически перегружен, и информация от контроллера до сервера может дойти с задержкой по времени.
На сегодняшний день существует множество специализированных программ, которые позволяют перехватывать информацию, передаваемую по локальной сети. В этом случае, для обеспечения безопасности передаваемых данных в рамках СКУД необходимо либо использовать шифрование данных (например, использовать передачу данных по защищенным VPN-соединениям), либо используемые для системы безопасности каналы выделять в отдельные подсети.

Вообще надо заметить, и статистика эксплуатации СКУД на объектах, где нет повышенных требований к вопросам безопасности, это подтверждает, что информация, циркулирующая по системе контроля и управления доступом, злоумышленникам малоинтересна. В самом деле, зачем в обычном офисе кому-то перекрывать вход в помещения соседям по этажу. Или знать, кто из них и во сколько пришел на работу. Если же речь идет об объектах с повышенным режимом секретности, то существует масса апробированных технологий защиты информации.

UDP – самый быстрый и ненакладный протокол. Позволяет обмениваться пакетами размером не более одного Ethernet-кадра (примерно 1500 байт). Но нам и этого за глаза хватит – в СКУД контроллер редко обменивается с ПК-пакетами размером более 100 байт. Таким образом, за счет скорости и простоты UDP – первый кандидат на использование в системе реального времени. Не случайно многие сетевые протоколы систем промышленной автоматизации работают именно на нем. Недостаток UDP – отсутствие гарантированной доставки сообщений – легко обходится теми же методами, что и при работе с RS-485: квитированием, т. е. передачей подтверждения приема каждого пакета.

TCP/IP - данный протокол обеспечивает гарантированную доставку, сам умеет на передающей стороне «резать», а на приемной «склеивать» большие пакеты данных, но это нам не очень нужно. Зато он менее расторопен и намного более накладен в программной реализации. Преимущество его только в том, что чаще всего по умолчанию проходит через корпоративные коммутаторы и маршрутизаторы.

Http - это самый медленный из протоколов, он «надстроен» над TCP/IP и используется в качестве основного в WEB, т. е. именно с его помощью мы получаем информацию из Internet. Из этого следует, что он проходим практически в мировом масштабе, в чем его определенное преимущество. Но в системах реального времени его применение практически невозможно из-за медлительности.

Главный плюс промышленных интерфейсов – это возможность построения многоранговых сетей с обменом между контроллерами системы. Протоколы очень надежны с точки зрения доставки информации, обеспечивают высокую скорость обмена данными между компонентами системы. Основной минус – пока еще недостаток опыта у российских разработчиков в разработке устройств под данные интерфейсы. Нюансов, с которыми столкнется разработчик, гораздо больше, чем при использовании того же RS 485.

Промышленные протоколы – открытые. В них есть четкая стандартизация. Производитель, разработав выходной интерфейс в данном стандарте, сможет легко подключается к этой шине. Достаточно иметь драйвер, который будет программировать это устройство и им управлять. Точно так же, кстати, как и Ethernet. Нужна библиотека драйверов для компьютера, который будет общаться с этим устройством, и всё. Потому что интерфейс стандартизован.

Стандарты промышленных сетей активно используются в интеллектуальных зданиях, системах автоматизации каких-то технологических процессов, то есть везде, где повышенные требования к быстроте и гарантированной передаче данных. Тот же CAN массово применяется в автомобильной промышленности, - вся электрика, начиная от лампочек и заканчивая системами ABS, - в современных автомобилях подключается именно по этому протоколу.

Интерфейсы беспроводных сетей в некоторых случаях незаменимы. Существует достаточно большое разнообразие беспроводных сетей, разработанных для тех или иных целей с вытекающими из этого конкретными характеристиками. Рассмотрим те из них, которые пригодны так или иначе для СКУД.

Wi-Fi – считают, что этот канал связи единственный, который может быть применим в профессиональных СКУД. С точки зрения компонентов СКУД (контроллеров, компьютеров) это полный аналог проводного Ethernet, и подключенные к беспроводным коммутаторам устройства даже не отличат одну среду передачи от другой. Как абсолютно нормально использовать сеть Ethernet для подключения контроллеров к системе, так же естественно использовать и беспроводные каналы связи на базе Wi-Fi. Это

освобождает от необходимости прокладки параллельных коммуникаций для связи компонентов при использовании традиционного RS-485.

Вся разница только в том, как на данном предприятии или части его территории построена локальная сеть: на витой паре, оптоволокне или с применением радиоканала. Таким образом, если говорить о Wi-Fi, то это в чистом виде замена только среды передачи без каких-либо других изменений. Скорости передачи практически одинаковые, внутренние протоколы тоже. Но до точки доступа все равно придется дотягиваться кабелем.

Реализация может быть и иной – оснастить сам контроллер доступа радиоканалом и соответствующим программным стеком, но о таких разработках я, например, пока даже не слышал. Главная причина, видимо, в том, что они будут достаточно затратны в производстве, особенно если учесть изначально невысокую тиражность оборудования. Понятно, что контроллеры СКУД, наверное, никогда не будут выпускать миллионными тиражами.

Bluetooth - у этого канала связи несколько иное назначение. К тому же Bluetooth имеет небольшой радиус действия, собственные протоколы. Использовать его нужно на обеих сторонах: и со стороны компьютера, и со стороны контроллера. Скоростей передачи было бы достаточно, но при малом радиусе действия смысл использовать Bluetooth в профессиональных системах теряется. Основное назначение данного интерфейса – связать что-то в рамках хотя бы одного помещения. Надежно соединить контроллер с сервером, который стоит через 5 дверей, нереально, такая система просто не будет работать. ZigBee - это одна из самых быстроразвивающихся беспроводных технологий. Но для использования в системах контроля и управления доступом она тоже не очень подходит прежде всего потому, что изначально разрабатывалась как низкоскоростной канал связи для объединения в сеть различных датчиков. Применительно к безопасности это могут быть датчики охранной и пожарной сигнализации.

Возможно, в скором времени ZigBee потеснит многие из существующих сегодня радиоканальных ОПС. Ведь почти все они разработаны вне каких-либо стандартов. У каждого производителя – свои протоколы обмена, и заменить имеющиеся на объекте беспроводные датчики на оборудование другого производителя невозможно.

Если стандарт ZigBee получит распространение, что вполне вероятно, то заказчик получит возможность использовать в системах ОПС практически любые датчики на выбор. Тем более что стандартные профили (спецификации наборов команд и протоколов обмена) для конкретных приложений в области автоматизации зданий и систем

безопасности разработаны, опубликованы, и все это вместе взятое гарантирует совместимость оборудования разных производителей.

Этот стандартхорош для соединения центрального узла с периферией, которая размещается территориально распределенно, причем за счет включения в систему ретрансляторов территория покрытия может быть весьма большой. Теоретически можно использовать ZigBee и в СКУД. Но этот канал имеет небольшую скорость передачи данных и небольшую дальность. Согласитесь, нерационально строить длинную цепочку ретрансляторов ради соединения контроллера с компьютером. Есть много более простых, а главное, дешевых и надежных способов.

GSM - исторически эта беспроводная сеть начала применяться в системах безопасности первой. У GSM-каналов есть очень большое преимущество: сеть обеспечивает практически сплошное покрытие. Все пространство, где живет человек, находится в зоне действия сети. Методы передачи информации в сети GSM – это SMS-сервис, голосовой канал, а также технология передачи данных GPRS.

SMS-сервис позволяет передавать короткие текстовые сообщения. Если есть необходимость передавать не текстовую информацию, ее нужно перекодировать, тогда допустимый объем этого сообщения будет уменьшаться.

Главный применительно к системам безопасности недостаток в том, что это не on-line сервис. А для профессиональных СКУД on-line мониторинг просто необходим. То есть в режиме реального времени информация должна поступать в службу реагирования, и в таком же on-line режиме команды от оператора или компьютера должны поступать на контроллер. Сервис не гарантирует время доставки, сообщение вообще может затеряться. Конечно, потери могут быть в любых протяженных каналах связи – за счет помех, шумов, наводок и т. д. Искаженная информация – потерянная информация. С этой проблемой можно бороться. Для того чтобы обеспечить гарантированную доставку, используется подтверждение, на чем, как известно, основана работа протокола TCP. Аналогичный механизм можно было бы использовать в SMS. Но сервис не дает гарантий оперативной доставки сообщений, и это принципиально не позволяет применять его для работы в реальном времени. Использовать SMS как резервный канал связи – вполне нормально и допустимо. Как основной – только в непрофессиональных системах.

Голосовой канал чаще всего используются для управления, например, домашней автоматикой и системой безопасности через голосовые меню, и этим область его применения, пожалуй, исчерпывается.

В GSM-каналах можно использовать GPRS или EDGE – специализированные службы, которые предназначены для обмена информацией на сравнительно высоких скоростях. С

использованием этих служб можно удаленно подключать IP-оборудование. Но вновь возникает вопрос: насколько такой подход рационален для профессиональных систем? Распределенные удаленные офисы почти всегда подключены к Интернету, причем подключены через готовые каналы связи с минимальной платой за трафик. Использовать для этих целей параллельный беспроводной канал не очень интересно и достаточно накладно. Если у пользователя есть коммуникатор с приличным дисплеем, можно по дороге на работу набрать номер своего сервера и посмотреть, например, отчет о рабочем времени.

В качестве основного канала связи в профессиональных СКУД могут использоваться только те беспроводные технологии, которые эквивалентны по функционалу, назначению и стоимости стандартной проводной компьютерной сети предприятия, – это Wi-Fi, Wi-Max и аналогичные беспроводные сети.

Технологии сенсорных сетей типа ZigBee, Z-Wawe и многие аналогичные должны использоваться по своему прямому назначению – для получения информации от различных датчиков без прокладки проводов на ограниченной (локальной) территории. Такая привлекательная сеть, как GSM, может использоваться либо в домашних системах, либо как дополнительный канал удаленного доступа к серверу СКУД для получения отчетов и аналогичных действий.

11. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СКУД

В системах контроля и управления доступом аппаратными средствами являются контроллеры. В них хранятся базы данных персонала, контроллер сам знает, кого, когда и через какую точку (если он обслуживает несколько точек) пропускать, он готов очень оперативно отреагировать на любое происшедшее в системе событие. Основная задача софта компьютера, то есть, программного обеспечения верхнего уровня, – возможность конфигурирования системы, оперативный мониторинг, различные прикладные функции: отчеты, учет рабочего времени. Но перекладывать на софт задачи, связанные с логикой работы системы, никогда не было чертой профессиональных систем, а сегодня тем более, потому что развитие техники позволяет реализовывать любой функционал, от которого зависит живучесть системы, на базе аппаратных устройств.

Многие современные контроллеры работают на своей операционной системе, как правило, на Unix (Linux), и, по сути, представляют собой компьютеры на базе промышленных ПК. Для них пишутся прикладные задачи, которые реализуют функционал возможностей контроллера. С точки зрения развития техники и технологий охотно это допускаю. С точки зрения здравого смысла возникают вполне закономерные,

на мой взгляд, вопросы. Понятно, что современная элементная база позволяет сделать практически всё, что угодно. Но возможно ли обеспечить конкурентоспособную цену такого оборудования? Ведь очевидно, что, например, размеры памяти контроллера, которому предстоит работать под операционной системой типа Linux, нужно увеличить на порядки по сравнению с контроллерами, не использующими ОС общего назначения. Минимум, что требуется для работы самой Linux, это мегабайт программной памяти и мегабайт – оперативной. Между тем, самый серьезный и многофункциональный контроллер СКУД, построенный на базе микроконтроллера, требует не более 64 кбайт программной памяти и не более – 32 кбайт оперативной памяти. А еще нужно учитывать, что Linux, как правило, привносит все проблемы доступных операционных систем. Например, может существенно увеличиться время реакции на некоторые события. Согласитесь, если контроллер ищет в базе данных пользователя не 0,2 секунды, а секунду или более, это ни в коем случае не свидетельствует о хорошей работе системы.

С одной стороны, понятно стремление разработчиков использовать такую операционную систему как Linux, потому что упрощается процесс создания самого ПО контроллера, - операционная система обеспечивает весь базовый функционал ввода/вывода, файловую систему, Ethernet стеки TCP/IP, - всё это является встроенными функциями любой нормальной операционной системы, в том числе и Linux. С другой стороны, для систем реального времени, с учетом потока событий долгая реакция системы вряд ли допустима. У многих заказчиков сегодня уже есть определенное мнение о том, как должна работать СКУД, и не нужно его ухудшать.

Наиболее распространенным вариантом является СКУД, в состав которой входят контроллеры доступа, оборудование, подключенное к контроллерам, и программное обеспечение (ПО), которым оснащены компьютеры общего назначения. Посредством ПО реализуются те функции СКУД, которые не поддерживаются контроллерами доступа в силу множества экономических и технологических причин. Все функции могут быть условно разделены на четыре категории: работа с пропусками, конфигурирование, мониторинг и управление, расширение технических возможностей контроллеров.

Ниже представлен типовой «набор» программного обеспечения СКУД.

1. Работа с пропусками.

Выдача и удаление пропусков - выполнение функции выдачи и удаления пропусков требует довольно больших временных затрат, поэтому для реализации данной процедуры используют ПО, упрощающее и ускоряющее ее. В современных программах оформления пропусков для формирования учетных карточек пользователей могут применяться html-страницы.

Ввод номера карты со считывателя – для избежания ошибок, многие программные продукты обеспечивают возможность ввода номера карты в систему непосредственно со считывателя, установленного в пункте выдачи пропусков.

Ведение базы данных пропусков - контроллеры доступа имеют ограниченное количество памяти и могут сохранять только минимальную информацию по действующим пропускам. Историю пропусков, данные по изъятым, а также дополнительную информацию по использующимся в настоящий момент пропускам (должность пользователя, подразделение, дата рождения, документ, удостоверяющий личность, и т.д.) контроллеры не содержат. С помощью ПО хранение подобных сведений, объем которых практически не ограничен, обеспечивается на серверах баз данных (БД) - MS SQL, Inter-base, Oracle, MS JET, FoxPro и т.д.

Отчеты по пропускам - информацию, находящуюся в БД, можно применять для формирования разнообразных отчетов, в частности, о количестве разовых посетителей, о числе выданных пропусков за неделю и пр.

Печать пропусков - в тех случаях, когда на пропуск наносится фотография, ФИО, должность и отдел его владельца, требуется специализированное ПО с редактором форм, поддерживающим принтеры для печати карт. Кроме того, зачастую ПО может обеспечить пакетную печать, а также печать различных форм для разных категорий пропусков и т.п.

Работа с несколькими контроллерами - если СКУД обслуживается не одним, а несколькими контроллерами доступа, то без применения ПО каждый пропуск потребовалось бы вводить в каждый контроллер отдельно. При использовании ПО информацию с пропуска достаточно ввести лишь в один контроллер, а затем разослать в остальные. Такой же механизм действует при удалении пропуска или изменении данных в нем,

Документооборот - выдача или удаление пропусков обычно предполагает составление заявки, подписание ее у определенных должностных лиц, передачу заявки в бюро пропусков. На каждом из этапов в пропуск добавляется та или иная информация, поэтому поддержка ПО документооборота позволяет снизить временные затраты на выдачу пропусков.

Интеграция с системами планирования и учета ресурсов предприятия - ПО для СКУД, как правило, строится по тем же принципам, что и ERP-система (*Enterprise Resource Planning System - система управления ресурсами компании*): использование операционной системы, сервера БД, серверов приложений и т.д. Поэтому СКУД и ERP-систему весьма просто интегрировать в единый комплекс, в результате чего система

контроля доступа обеспечивается данными из ERP об увольнении и приеме новых сотрудников, а в ERP-систему поступают данные учета рабочего времени.

Смена PIN-кода - некоторые владельцы пропусков, особенно материально-ответственные лица, должны иметь возможность регулярно менять свой PIN-код. Программное обеспечение упрощает этот процесс и может предоставлять даже Web-интерфейс для смены PIN-кода. В результате владелец пропуска способен делать это в любой момент времени со своего рабочего места.

2. Конфигурирование СКУД .

Конфигурирование контроллеров - контроллер доступа имеет множество настроек: таблицы временных зон и интервалов, праздников, уровней доступа, считывателей и т.д. Наличие удобного графического интерфейса позволяет ускорить процесс конфигурирования и снизить вероятность ошибки.

Многопользовательская работа - конфигурирование контроллера, создание пропусков, анализ отчетов и другие действия выполняются разными людьми. Именно с помощью ПО можно обеспечить одновременную работу нескольких человек с одним и тем же контроллером доступа прямо со своих рабочих мест дистанционно.

Восстановление после сбоев - в случае выхода из строя контроллера доступа и его замены возникает задача конфигурации нового устройства и загрузки в него всех пропусков. ПО позволяет осуществить эту операцию быстро и без особых трудностей.

3. Мониторинг и управление.

Мониторинг - стандартной функцией ПО СКУД является визуализация протоколов событий, включающих в себя события отказа доступа, взлома двери, удержания двери открытой и пр. Отображение подобных событий на поэтажных планах помогает контролировать ситуацию и вовремя предпринимать необходимые действия.

Управление - ПО обеспечивает возможность управления работой СКУД (блокировать/открывать двери и шлюзы, переводить их в различные режимы работы и т.д.) как для отдельных точек прохода, так для помещений, этажей и здания в целом.

Фотоидентификация - зачастую от оператора необходимо получать подтверждение разрешения о доступе, выданного контроллером СКУД. Для этого на проходной устанавливается ПО, которое автоматически показывает данные о человеке, предъявившем пропуск. Получив эти сведения, оператор может либо заблокировать проход, если данные неверны, либо разрешить проход в случае предъявления верной информации.

Слежение за перемещением - на основании данных о событиях доступа с помощью ПО можно контролировать, в каком помещении находится тот или иной сотрудник.

Отчеты по событиям - как правило, вся информация, регистрирующаяся в журнале событий СКУД, хранится в БД. Современное ПО позволяет оператору автоматизировать процесс поиска необходимых сведений в БД, которые могут быть отсортированы по источникам событий, владельцам пропусков, времени и прочим критериям.

Учет рабочего времени - функция учета рабочего времени позволяет определить число опозданий, прогулов, уходов с работы, количество отработанных часов за месяц для каждого конкретного сотрудника.

Интеграция с системами видеонаблюдения, охранной и пожарной сигнализации - ПО позволяет проводить анализ информации о событиях, происходящих в СКУД, совместно с данными системы видеонаблюдения и охранной сигнализации. То есть по событию СКУД оператору будет автоматически показано изображение от требуемых видеокамер. Причем управляемая видеокамера может автоматически позиционироваться для нахождения наилучшего ракурса. Создавая отчеты событий СКУД, можно организовать их сопровождение видеофрагментами. При интеграции СКУД с охранной сигнализацией можно автоматически ставить помещения на охрану при уходе последнего сотрудника или снимать помещения с охраны по приходе первого сотрудника. Интеграция СКУД с пожарной сигнализацией обеспечивает возможность автоматического открытия дверей на выход в случае пожара. Алгоритмы интеграции СКУД с другими системами зависят от конкретных задач на объекте.

4. Расширение технических возможностей контроллеров

Сложные алгоритмы прохода - на некоторых объектах требуется реализовывать специфические алгоритмы доступа, например разрешать доступ в помещение только при наличии в нем как минимум одного уполномоченного сотрудника. Для решения такой задачи разрабатывается специальное ПО. Сменный режим доступа На многих предприятиях требуется не только ограничение доступа нежелательным лицам, но и управление временем доступа сотрудников. Последнее не всегда можно осуществить с помощью контроллеров СКУД в организациях с круглосуточным производством, со сменным или гибким режимом работы, так как логика работы большинства контроллеров СКУД основана на модели, в которой временные интервалы доступа формируются для конкретных дней недели (понедельник-воскресенье) плюс несколько типов праздников. Для автоматизации гибкого графика логика работы контроллеров должна быть иной. Однако алгоритмически скользящий режим гораздо более ресурсоемок и для микропроцессорного устройства его реализация очень нетривиальна.

Стоит отдельно упомянуть о надежности программных устройств управления СКУД, то есть программного обеспечения (ПО), установленного на компьютерах управления,

серверах баз данных, дополнительных рабочих местах и т.д. Чаще всего сам компьютер (если говорить начистоту, то и ПО, установленное на нем) является самым ненадежным элементом СКУД. При выходе компьютера из строя (даже если система в полном объеме сохраняет работоспособность) теряются такие важные функции, как отображение информации, поступающей к операторам, и возможность управления техническими средствами СКУД вручную. Для устранения влияния данного фактора можно, как и в случае с центральными контроллерами, применять "горячий" резерв. Однако если в системе очень много компьютеров, на которых хранятся базы данных, или управляющих компьютеров, то "горячее" резервирование каждого из них обойдется слишком дорого. В таких случаях допустимо создание "холодного" резерва. С этой целью один из компьютеров собирает сведения об изменениях конфигурации (составе баз данных и т.д.) со всей системы. При выходе из строя какого-либо элемента сети производится замена из ЗИПа, а далее вся необходимая конфигурация "заливается" из компьютера "холодного" резерва.

Надежность программных устройств управления следует рассматривать и с точки зрения обеспечения необходимого уровня защиты от несанкционированного доступа к информации, а также возможности разграничения полномочий доступа и прав операторов. Для этого могут использоваться не только опции, встроенные в операционные системы, но и специализированные инструменты, которые реализованы либо программными, либо программно-аппаратными средствами. Необходимо обратить внимание на лицензии и сертификаты таких средств и выбирать те, которые соответствуют требованиям оснащаемого объекта.

12. Защита от несанкционированного управления и физического воздействия на устройства СКУД.

Расположение устройств ввода идентификационных признаков вне зоны, которая становится безопасной благодаря их работе, делает их уязвимыми для попыток несанкционированного управления ими. Нарушитель может просто сломать считыватель и беспрепятственно проникнуть в защищаемую зону или воспользоваться незащищенной

линией связи, не взламывая стену, а также похитить устройство. В том случае, если связь между устройством контроля доступа и собственно контроллером не наблюдается в реальном времени, как интерфейс Wie-gand, то оператор окажется в полном неведении об утрате прибора. Беззащитную линию связи можно заставить реализовать открытый протокол, после чего воспользоваться симулятором номеров карт и получить доступ к защищенной зоне. Если вы против такого развития событий, то вам стоит обеспечить перманентный мониторинг линии связи «контроллер – считыватель», закрытый протокол передачи информации или, в крайнем случае, оградить линию связи от вторжения саботажной линией, а собственно устройство ввода идентификационных параметров - тамперным контактом, запрограммированным на распознание отрыва или вскрытия.

Можно попытаться защитить считыватель с помощью помещения его внутрь стены. Приемно-передающая антенна, правда, должна в любом случае находиться снаружи. Однако если это будет выдавать присутствие системы, то демонтировать вмурованный в кладку прибор будет значительно сложнее, чем ничем не защищенный. Оправданно также использование уличных кожухов с повышенной взломоустойчивостью.

Самым главным негативным последствием кражи устройства ввода идентификационных признаков является доступ к хранящейся в его памяти базе данных всех имеющих доступ к закрытой зоне сотрудников. Само собой разумеется, что объекты с повышенной секретностью или государственной важности не имеют право так подставлять себя и свой коллектив. Поэтому при создании системы контроля и управления доступом лучше создать базу данных биометрических и иных параметров не в памяти считывателя, а в хранилище контроллера. К тому же это позволяет расширить такую базу, поскольку кроме нахождения контроллеров внутри защищенной зоны и, как следствие, недосягаемости для злоумышленников, память контроллера существенно больше памяти собственно УВИП. Это помогает сохранять большое число данных без опасности попадания их не в те руки. Контроллеры с подобными функциями уже разработаны и позволяют увеличить размер базы данных до 100 000 идентификационных признаков в режиме автономной работы. Естественным следствием разработки такой системы стала усовершенствованная защита связи внутри системы «считыватель-контроллер», кодирование передаваемых данных и перманентный контроль над линией связи.

Подмечено, что радиоканальная технология идентификации обладает значительным минусом – возможностью копирования идентификационных номеров карт. Для этого всего лишь требуется оборудование для съема данных по открытому радиоканалу, что

позволяет копировать номера карт, находящихся на связи со считывателем. Возможно и по-другому скопировать информацию с карты: при этом используется специальное устройство, которое карта воспринимает как считыватель, и данные копируются в любом месте, например, на улице, а не только на режимном объекте. Если подобное устройство обладает достаточно мощным передатчиком и высокотехничной антенной, рабочее поле его копировальных способностей может достигать метра. Против появления двойных карт может помочь либо использование Smart-устройств, либо комплексные средства идентификации. И, естественно, стоит защитить связь "считыватель-контроллер", иначе применяемые средства безопасности не приведут к должному результату.

12. ИНТЕГРИРОВАННЫЕ СКУД

СКУД может быть интегрирована другими системами безопасности. Грамотная интеграция СКУД с системой видеонаблюдения позволяет полностью контролировать ситуацию на объекте. В случае возникновения внештатной ситуации данная совокупность систем позволяет в рекордные сроки выявить нарушителя. Благодаря наличию тревожных входов и выходов СКУД может быть интегрирована с системой охранной сигнализации. Данная совокупность позволяет при проникновении в помещение включать сирену, светодиодную лампу и.т.д. Также СКУД может быть интегрирована с системой пожарной сигнализации. Данная совокупность позволяет разблокировать двери, открыть ворота, опустить турникеты в случае пожара для эвакуации персонала.

При анализе технических характеристик современных цифровых (компьютерных) систем видеоконтроля следует различать характеристики собственно системы видеоконтроля от обычных характеристик современной компьютерной техники, на базе которой такие системы собраны. Например, тип (EIDE, SCSI) и емкость (10-80 G) жесткого диска имеет смысл анализировать только в блочных системах, выпускаемых с ограниченной номенклатурой жестких дисков. Аналогично следует относиться к разрешению видеомонитора, обычным коммуникационным и сетевым интерфейсам (RS-232, Ethernet IEEE 802.3 и т.д.) и прочим компьютерным комплектующим и компьютерной периферии (CD-ROM, ZIP, DAT-накопители, тип процессора, объем оперативной памяти и т.п.). Как правило, все эти характеристики имеют смысл сравнивать только для систем, поставляемых в жестко заданных конфигурациях. Большинство же цифровых систем видеоконтроля выпускаются как в блочном, так и в так называемом OEM-исполнении, т.е. допускают использование практически любых компьютерных

комплектующих и PC-платформ, наиболее подходящих для каждой конкретной цифровой системы видеоконтроля, востребованной Заказчиком.

Из характеристик собственно систем видеоконтроля следует отметить следующие.

1. Очень важная характеристика, определяющая "лицо" системы и удобство ее управления/администрирования - ***интерфейс управления/администрирования системы***. К сожалению, большинство цифровых систем видеоконтроля обладают Windows-подобным интерфейсом, который при всем его преимуществе в офисных приложениях, для профессиональных систем видеоконтроля является очень серьезным недостатком, т.к. неэффективно использует доступную для отображения площадь экрана монитора, позволяет произвольно закрывать, в т.ч. случайно, окна управления и отображения, имеет очень много повторяющихся панелей управления одними и теми же функциями и т.п. Иногда такой интерфейс для организации нормальной работы требует использования нескольких мониторов, что также является серьезным недостатком (например, видеоотображение - на одном мониторе, а работа с видеоархивом - на другом). Некоторые цифровые системы видеоконтроля, обладая специализированным, и, на первый взгляд "красивым" интерфейсом, тем не менее также неэффективно используют доступную площадь экрана монитора системы видеоконтроля (часть панелей управления системой фиксировано занимают часть площади монитора). Профессиональные цифровые системы видеоконтроля должны иметь максимально простой, рациональный интерфейс, с количеством настроек и органов управления, минимально необходимых и достаточных для их эффективного использования.

2. **Допустимые форматы видеокадров**, которые используются при видеообработке и видеозаписи. Существует множество форматов, используемых современными цифровыми (компьютерными) системами видеоконтроля. Профессиональные цифровые системы, как правило, работают со всеми максимально допустимыми для цифровой обработки видеоформатами: 768x576, 720x576 и 768x288. Иногда, по совокупности остальных показателей, к профессиональным относят цифровые системы видеоконтроля, работающие с форматами 704x576, 640x512 и иногда 640x480 (в основном для зарубежных систем, обычно работающими с меньшими форматами, чем отечественные профессиональные цифровые системы видеоконтроля). Остальные обычно довольствуются разрешениями от 640x480 до 640x256, 384x288, 320x256, 320x240 и даже 192x144, 160x120, 80x60. С учетом так называемого Kell-фактора и известной пропорции телевизионного изображения - аспекта (3/4), формат 384x288 (или аналогичные по количеству пикселов по горизонтали) соответствует разрешению около 250-280 телевизионных линий по горизонтали (качество VHS), а форматы 768x288 и 768x576 (или

аналогичные) - разрешению 500-600 линий по горизонтали для черно-белого изображения и 300-400 - для цветного (качество S-VHS). Современные видеокамеры, как правило, имеют следующие форматы ПЗС-матриц: монохромные высокого разрешения - 782x582, 768x576, стандартного - 512x582, 512x576, цветные высокого разрешения - 752x582, стандартного - 500x582. Поскольку в системах видеоконтроля, как правило, используются черно-белые видеокамеры высокого и стандартного разрешения, для профессиональных цифровых (компьютерных) систем видеоконтроля очень важны именно форматы 768x288 и 768x576 (или аналогичные им по количеству пикселей по горизонтали/вертикали), поскольку только они позволяют получать максимально информативные для последующей цифровой обработки видеокадры, с минимальной потерей исходного разрешения входного видеосигнала.

3. **Разрешение канала видеообработки/записи**, измеряемое в телевизионных линиях (ТВЛ). Принято считать, что профессиональные системы должны обеспечивать разрешение канала видеообработки по горизонтали 500-600 ТВЛ для черно-белого изображения и 350-400 ТВЛ - для цветного. Разрешение канала видеообработки связано как с форматом видеокадра, уже упоминаемым выше, так и с методами цифровой обработки видеосигналов. Для цветных композитных видеосигналов именно цифровая обработка является определяющей в ограничении максимального разрешения канала обработки (выделение сигнала цветности из общего спектра видеосигнала), что накладывает жесткие ограничения на максимально возможное разрешение по горизонтали не более, чем 350-400 ТВЛ (обычно 78-100 ТВЛ на 1 МГц полосы видеосигнала). Более высокие разрешения (400-500 ТВЛ и выше) для цветных изображений возможны только в случае работы с компонентным цветным сигналом: Y:C, RGB и пр. Естественно, в этом случае необходимо использовать и соответствующие видеокамеры с раздельными выходами яркостного (Y) сигнала и сигнала цветности (C). Не менее важна и характеристика разрешения по вертикали, которая очень сильно связана с допустимыми форматами видеокадров системы: для формата 768x576 речь идет о реальном разрешении по вертикали в 400-450 линий (теоретически - не более 576), для формата 640x480 - 360-400 линий (теоретически - не более 480) а для формата 384x288 - 200-250 линий (теоретически - не более 288). Пересчет формата из пикселей в ТВЛ и обратно обычно выполняется с помощью так называемого расширенного Kell-фактора (который равен 0,7-0,85 по горизонтали и 0,7-0,8 - по вертикали). Kell-фактор позволяет выполнять такой пересчет при любом переходе от черезстрочной развертки входных видеосигналов в прогрессивную развертку компьютерных (цифровых) мониторов. Отдельно следует выделять разрешение канала видеозаписи, которое может широко варьироваться в

зависимости от степени компрессии (сжатия) видеосигнала. В профессиональных системах даже хорошо сжатое изображение должно обеспечивать достаточно высокое разрешение (150-250 ТВЛ), приемлемое по качеству, при минимальном объеме отдельного видеокадра (от 1-2 кбайт до 5-10 кбайт). На практике разрешение канала обработки/записи и по горизонтали, и по вертикали удобно проверять с помощью специальных измерительных таблиц, например, EIA1956.

4. **Метод и степень компрессии (сжатия) видеосигнала.** Как правило, в цифровых (компьютерных) системах видеоконтроля используются следующие методы компрессии (сжатия) видеоизображений: WAVELET-подобные (WL, DELTA-WL и т.д.), JPEG и M-JPEG/MPEG - подобные (MPEG-1, MPEG-2, MPEG-4 и т.д.). При этом последние пришли или из обычной компьютерной техники сжатия статических изображений (JPEG), или позаимствованы из бытовой цифровой видеозаписи потокового видео (MPEG), что накладывает некоторые особенности на их использование в системах видеоконтроля. Дело в том, что JPEG очень плохо сжимает потоковое видео (видеопоследовательности), а M-JPEG/MPEG - подобные методы компрессии работают на основе так называемых опорных кадров и практически перестают работать при мультиплексировании видеосигналов, когда могут возникать задержки между отдельными видеокадрами до 100-200 мс и более, что соответствует скорости обработки до 5-10 FPS (frame per second, кадров/с). С другой стороны, M-JPEG/MPEG - подобные методы компрессии при больших степенях компрессии (32:1 и более) дают очень заметные искажения характерной формы (блоккинг-эффект, мозаичный эффект, искажения типа ступеньки и т.п.), что делает практически невозможным использование больших степеней компрессии для целей осуществления более компактной цифровой видеозаписи и организации оперативных видеоархивов большой емкости. От этих недостатков почти свободны методы компрессии, которые базируются на WAVELET - преобразованиях, т.е. на так называемой математике "волновых всплесков". Здесь искажения, как правило, носят визуально менее выраженный характер, что очень плодотворно сказывается на качестве хорошо компрессированных видеокадров (т.е. на разрешении канала записи/воспроизведения). Иногда в цифровых системах видеоконтроля используются MPEG-подобные, оптимизированные по скорости, алгоритмы компрессии h.261 и h.263 (с модификациями h.261+, h.263+), в основном предназначенные для реализации видеоконференций и видеотелефонии по сетям ISDN, без особых требований к качеству сжатых видеокадров (это, кстати, делает их малопригодными в профессиональных системах видеоконтроля). По степени компрессии они занимают промежуточное положение между WAVELET и M-JPEG/MPEG и встречаются в цифровых системах

видеоконтроля довольно редко. Как правило, при одинаковых степенях сжатия WAVELET опережает по качеству методы компрессии на базе JPEG/MPEG, и, тем более, h.261 и h.263, а при одинаковом или сопоставимом качестве - имеет существенно меньший размер сжатого кадра: 1-3 Кбайт для WAVELET против 5-10 Кбайт для M-JPEG/MPEG. А это, как правило, соответствует степени компрессии (сжатия) для WAVELET от 10 до 100 раз (максимум - до 200 и даже в 300 раз), а для M-JPEG/MPEG - от 5 до 20 раз (максимум - до 50-70 раз). Следует также понимать, что степень компрессии принципиально не может иметь какого-то заранее заданного значения, т.к. очень сильно зависит от характера реальных видеоизображений (однородно белые стены внутри офиса сжимаются куда сильнее, чем осенняя листва деревьев или кустарников во всем ее цветовом многообразии и движении). Некоторые системы используют модификации алгоритмов компрессии на основе так называемой "дельта-компрессии" (DELTA), которая за счет передачи лишь изменений между отдельными кадрами видеоизображений позволяет обеспечить дополнительную степень компрессии до 5:1 и выше (при различиях между смежными кадрами - до 20% и меньше), что может быть очень важно для передачи видеоизображений по низкоскоростным каналам связи (при скоростях от 9,6 до 56 Кбайт/с). Кстати, видеоизображения, записанные в форматах на базе стандартных JPEG/MPEG-преобразований, как правило, можно просмотреть любыми внешними программными средствами (стандартными просмотрщиками). С этой стороны закрытые алгоритмы кодирования на базе WAVELET для средств обеспечения безопасности куда более предпочтительны, т.к. принципиально не позволяют получать свободный внешний доступ к видеоархиву (в этом случае для преобразования в формат AVI, например, надо использовать специальные конверторы). В последнее время в некоторых профессиональных цифровых системах видеоконтроля наметилась тенденция перехода на аппаратную поддержку компрессии WAVELET, что дает таким системам неоспоримые преимущества в повышении общего быстродействия и качества всей системы в сочетании с уменьшением требований к компьютерной платформе, в отличие от уже сравнительно давно используемой дорогой и не очень подходящей для систем видеоконтроля аппаратной компрессии MPEG.

5. **Тип платы видеозахвата (схема ввода)** - это характеристика системы, которая объясняет количество немультиплексированных/мультиплексированных входов и каналов обработки на одну плату (например, схема ввода 4x4 - это 4 немультиплексированных входа и 4 канала/микросхемы обработки, 16x1 - 16 мультиплексированных входов и 1 канал/микросхему обработки, 16x4 - 16 мультиплексированных входа и 4 канала/микросхему обработки и т.д.).

6**. Скорость обработки/записи немультиплексированных изображений.** Как правило, современные цифровые системы видеоконтроля обрабатывают немультиплексированные изображения со скоростью до 25 FPS. Здесь и далее характеристики скорости обработки приведены для стандарта PAL, наиболее широко распространенного на отечественном рынке видеокамер. Скорость обработки 25 FPS соответствует качеству "живого видео" ("live-video"). К сожалению, для многих цифровых видеорегистраторов скорость приводится без указания формата обрабатываемых видеокадров (768x576, 768x288, 384x288 и т.д.) и их цветности (черно-белые или цветные). Именно отсюда очень много некорректностей в сравнении. Как правило, все характеристики цифровых систем видеоконтроля указываются для формата видеокадра 384x288 (или аналогичных форматов), а для многочисленных корейских систем - и того меньших форматов. Но отсутствие привязки скорости обработки/записи к формату и цветности видеокадра может привести к тому, что характеристики систем, обрабатывающих со скоростью 25 FPS кадры форматов 768x576 и 640x480, могут отличаться значительно. Следует также понимать существенную разницу между скоростью обработки и записи, которые могут очень сильно отличаться друг от друга. На скорость записи очень влияет используемый алгоритм компрессии и способ ее реализации (программная или аппаратная).
7. **Скорость обработки/записи мультиплексированных изображений** - это еще более сложный для понимания параметр, вокруг которого еще больше некорректностей и манипулирования цифрами при указании конкретных технических характеристик цифровых систем видеоконтроля. Все современные системы видеоконтроля, за очень небольшим исключением, работают с асинхронными аналоговыми или гибридными (с цифровой предобработкой) видеокамерами, имеющими самые обычные аналоговые композитные видеовыходы. А это означает, что любой цифровой системе видеоконтроля требуется время (как правило, 60-80 мс) для синхронизации с видеопотоками разных камер при их переключении. Именно поэтому скорость обработки мультиплексированных видеосигналов для профессиональных систем соответствует 12,5-16 FPS на один канал цифровой обработки, а для остальных - 8-10 FPS. Причем для некоторых цифровых систем видеоконтроля (например, захватывающих видеосигнал с помощью микросхем Philips SAA71XX), время синхронизации может быть величиной непостоянной, сильно зависящей от типа и марки конкретных видеокамер. В результате - вместо декларируемых 12,5 FPS можно в реальности получить 8-10 FPS, причем конкретное значение будет зависеть даже от конкретного экземпляра внешне совершенно одинаковых видеокамер одной и той же фирмы одной и той же марки. Следует отметить, что для достижения

более высокой скорости обработки 16 FPS четкий захват четных или нечетных полукадров не контролируется, что внешне приводит к характерному подергиванию изображения на экране вверх-вниз. Более реально - это 12,5 FPS стабильного видеозахвата для любых видеокамер. Для плат, выполненных, например, по схеме 16x4 (использующих четыре микросхемы видеозахвата и мультиплексор для 16-ти видеовходов) это значение может составлять до 50 FPS на одну плату (12,5 x 4 = 50 FPS). Именно так работают профессиональные системы. Естественно, что скорость обработки/записи мультиплексированных изображений обязательно должна указываться в строгой привязке к формату и цветности видеокадра. Для мультиплексированных изображений разница между скоростью обработки и записи обычно не такая значительная, как для немультиплексированных, хотя для некоторых систем разница также может быть значительной.

8. Емкость видеоархива - еще одна из характеристик, вокруг которой всегда идут баталии взаимного непонимания, споров и полной несопоставимости показателей разных систем. В технических характеристиках цифровых систем видеоконтроля можно встретить указание емкости видеоархива как в часах (днях, сутках), так и в количестве записываемых кадров. И первый, и второй подход имеют как доводы за, так и против. Рассмотрим первый пример. Пусть для какой-либо цифровой системы видеоконтроля указано, что она обеспечивает время записи от 2 до 1642 часов, с примечанием, что это в зависимости от интервала (скорости) записи и степени компрессии. Можно встретить и такое: "...при видеокомпрессии до 30 Кбайт для каждого изображения видеозапись в реальном времени может происходит в течение 75 дней для каждой из 36 камер". Второй пример: "при коэффициенте сжатия 1:80, среднем количестве движения на объекте 20% и емкости диска 1 Гбайт будет записано 781 250 кадров, что равно 54 часам непрерывной записи изображений от 4 ТВ камер с частотой записи 1 кадр в секунду для каждой ТВ камеры". Впечатляет? Не очень, если принять во внимание, что ни в первом, ни во втором примере совершенно не указывается, для каких форматов кадра, цветности и какого качества записи указываются эти технические характеристики емкости видеоархива. А если принять во внимание, что реальные степени сжатия очень сильно зависят от характера конкретного видеоизображения, становится понятно, что емкость видеоархива - это характеристика, очень сомнительная для использования в целях сравнения различных систем, к тому же использующих совершенно различные алгоритмы компрессии и реализующие видеозапись с совершенно разным качеством. Из этого можно сделать вывод, что более корректно для целей сравнения следует указывать конкретные размеры сжатых видеоизображений одинаковых форматов и одинакового качества, например, с

помощью видеозаписи специальных тестовых таблиц (EIA1956, например). Поскольку для современных цифровых систем видеоконтроля конкретные объемы жестких дисков практической роли не играют (как правило, существует очень широкий их выбор), приняв за единицу измерения условный 1 Гбайт, характеристики и времени, и количества кадров, например, легко можно получить с учетом конкретной скорости видеозаписи и объема отдельного видеокадра заданного сопоставимого формата (качества). Например, для кадров формата 384x288 с размером 2 Кбайта и скорости записи 25 кадров/с для одной видеокамеры: 1 Гбайт : 2 Кбайт/кадр = 500 000 кадров / 1 Гбайт, 500 000 кадров : 25 кадров/с = 20 000 с или 5,6 часа / 1 Гбайт. Соответственно, для жестких дисков в объемом 60 Гбайт общая емкость видеоархива будет составлять 5,6 часа * 60 = 336 часов для скорости записи 25 кадров/с. Для скорости 50 кадров/с (две камеры по 25 FPS или 4 платы по 12,5 FPS) будет 168 часов, а для 12,5 кадров/с (для 16 мультиплексированных видеокамер на одну плату видеозахвата с одним каналом обработки), например, - 672 часа или 28 суток. Стоит заметить, что увлекаться подобными расчетами не следует, поскольку прогнозировать степень компрессии в реальных условиях конкретного объекта заранее невозможно.

9. **Наличие дополнительных средств архивирования видеоинформации.** Как правило, все цифровые системы видеоконтроля имеют только оперативный видеоархив на системном жестком диске (иногда - в дополнительном специализированном системном блоке), организованный по принципу безостановочной кольцевой видеозаписи. Это приводит к тому, что при полном заполнении жесткого диска самые ранние записи стираются. С целью организации долговременного видеоархива некоторые профессиональные системы имеют дополнительные средства архивирования, которые позволяют переносить оперативный видеоархив или отдельные его фрагменты на любые внешние носители (сетевые диски, стриммеры и т.п.). Отдельные профессиональные системы имеют дополнительные средства архивирования, позволяющие выполнять сетевое архивирование с удаленных систем видеоконтроля (удаленных видеосерверов), в т.ч. по коммутируемым каналам связи.

10. **Наличие многоканального детектора движения (активности).** Большинство современных цифровых (компьютерных) систем видеоконтроля обязательно имеют многоканальные детекторы активности. Профессиональные цифровые системы видеоконтроля обязательно должны использовать многоканальные детекторы движения. Если детекторы активности используют достаточно простые разбиения поля изображения, как правило, на 8-16 (очень редко - более) областей, которые используются только для анализа активности (как правило, на основании измерения относительных изменений

яркости/контраста в этих зонах), без определения реальных характеристик движения объекта, то истинно профессиональные детекторы движения дополнительно к обычному обнаружению активности, определяют как характеристики собственно детектируемого объекта (форму, контур, размер, контраст и т.д.), так и характеристики его движения (скорость, изменения скорости и т.д.). Основное отличие профессиональных детекторов от обычных - это возможность их настройки в реальных условиях охраны объектов именно на обнаружение движения объектов, с предельной минимизацией ложных срабатываний (фильтрацией помех), а также задания гибкой логики обработки тревог ("горячая" тревожная запись, пред- и пост-запись, управление по срабатыванию детектора остальным охранным оборудованием, например - подсистемой аудиоконтроля). Под ложными срабатываниями обычно понимаются срабатывания детектора на естественные оптические помехи (блики, естественные или некоторые искусственные колебания освещенности в зоне контроля, усредненно-стохастические изменения в зоне контроля, например, от листвы деревьев, помехи от дождя, снега и т.п.), а также срабатывания на объекты с характеристиками, отличными от требуемых (по форме, размеру, контрасту, скорости движения, ее изменению и т.д.). Так, например, с помощью профессиональных детекторов движения вполне можно отстроиться от помех, вызванных пролетом птиц, падающей листвы, некоторых домашних животных (кошек, собак, домашней птицы и пр.), и от бликов, отражающихся в обычных лужах, водоемах и т.п. Обычным детекторам активности это не под силу - обязательно будут ложные срабатывания, со всеми вытекающими последствиями. Именно поэтому наличием профессионального детектора движения профессиональные системы отличаются от обычных цифровых систем видеоконтроля, оснащенных обычным детектором активности. Некоторые профессиональные детекторы движения имеют несколько отдельно анализируемых зон (обычно не более 8...16-ти), каждая со своими настройками, что позволяет реализовывать ряд дополнительных функций детектирования и реакций на движение.

11. Количество немультиплексированных видеоканалов на один системный блок (одну плату) - очень важная характеристика цифровых систем, для которых важна организация многоканального высококачественного видеоконтроля со скоростью до 25 FPS. Как правило, одна плата видеозахвата позволяет обрабатывать 1, 2 или 4 немультиплексированных видеосигнала одновременно. Поскольку в системный блок обычно можно установить до 4-х плат видеозахвата, одним системным блоком цифровой системы видеоконтроля возможна параллельная обработка (организация видеонаблюдения и видеозаписи одновременно) от 4-х до 16-ти немультиплексированных видеоизображений со скоростью обработки до 25 FPS. При этом следует понимать, что

видеообработка и видеозапись со скоростями до 25 FPS более требовательна к ресурсам PC-платформы и значительно уменьшает глубину оперативного видеоархива. Кроме этого, указание количества немультиплексированных видеоканалов на один системный блок (плату) обязательно требует указания этого параметра в строгой привязке к скорости обработки/записи, к формату и цветности видеокадра. Иногда вместо общего количества немультиплексированных видеоканалов указывают суммарную скорость обработки/записи немультиплексированных видеоизображений, например 25 FPS, 50 FPS, 100 FPS и т.д.

12. Количество мультиплексированных видеоканалов на один системный блок (одну плату). Как правило, для организации профессионального видеоконтроля вполне достаточно обеспечить среднюю скорость обработки на один видеоканал от 1-3 FPS до 6-7 FPS, с возможностью динамического выделения тревожному видеовходу ресурса до 12,5-25 FPS. Для этого обычно используют или встроенные прямо на плату видеозахвата, или внешние мультиплексоры видеосигналов. Количество мультиплексированных видеоканалов на одну плату может составлять от 4-х (так называемая схема 4x1, с одной микросхемой видеозахвата) до 16-ти (16x1, 16x4, с одной или четырьмя микросхемами видеозахвата). Соответственно для одного системного блока цифровой системы видеоконтроля можно получить от 16 до 64 мультиплексированных видеоканалов обработки. По аналогии с немультиплексированными видеоизображениями, иногда вместо общего количества мультиплексированных видеоканалов указывают суммарную скорость обработки/записи мультиплексированных видеоизображений на системный блок, например, 12,5 FPS, 25 FPS, 50 FPS, 100 FPS, 200 FPS и т.д. Соответственно, в этом случае очень просто получить среднюю скорость обработки для любого количества мультиплексированных видеоканалов. Например, для суммарной скорости обработки 50 FPS и 32-х задействованных видеоканалов получаем 50 : 32 = 1,56 FPS на один видеоканал, как правило, с возможностью динамического выделения для тревожного видеоканала ресурса горячей записи/видеоотображения вплоть до 12,5 и даже 25 FPS.

13. **Наличие и количество тревожных входов/выходов (цифровых входов / выходов управления).** Для организации интеграции с внешним охранным оборудованием современные цифровые системы видеоконтроля, как правило, оснащаются специальными тревожными входами типа "сухой контакт" и специальными, как правило, релейными (или цифровыми) выходами управления. Обычно можно встретить системы с количеством тревожных входов от 8 до 64-х и релейных выходов от 8 до 32-х. Профессиональные системы видеоконтроля, как правило, должны обеспечивать гибкую логику обработки событий с тревожных входов и выдачи соответствующих управляющих сигналов на

выходы управления. Обычные системы видеоконтроля имеют очень простую логику обработки тревожных событий (включить запись по срабатывании тревожного входа или по срабатыванию видеодетектора движения/активности выдать управляющий сигнал на выход и т.д.).

14. **Возможность управления поворотными устройствами и объективами видеокамер (телеметрического управления).** Управление поворотными устройствами и объективами видеокамер для некоторых объектов является одним из обязательных требований к системе видеоконтроля. Именно поэтому большинство современных систем оснащаются средствами управления поворотными устройствами и объективами видеокамер, а для профессиональных систем видеоконтроля это требование является практически обязательным. Как правило, такое управление осуществляется по интерфейсам RS-485, что обычно требует использования в системах видеоконтроля соответствующих преобразователей интерфейсов RS-232/RS-485. Количество каналов телеметрического управления в цифровых системах видеоконтроля может быть самым разнообразным - от 4 / 8 / 16-ти фиксированных до 32 / 64-х и более расширяемых. Функциональность средств телеметрического управления видеокамерами цифровых систем видеоконтроля обычно соответствует функциональности обычных аналоговых средств управления.

15. **Возможность ведения объектно-ориентированных карт-схем охраняемых объектов.** Речь идет о возможности отображения на картах-схемах (как правило, многоуровневых иерархических) охранного оборудования, в т.ч. оборудования видеоконтроля, и режимов его работы (тревога, режим записи, режим охраны, обрыв и т.п.). Профессиональные системы дополнительно к простому отображению позволяют осуществлять управление охранным оборудованием прямо с плана-схемы. Особое значение для охраны больших объектов (многоэтажные здания, территориально распределенные объекты и т.п.) имеет возможность удобной навигации между отдельными элементами многоуровневых иерархических планов с целью быстрой локализации тревожной зоны и оперативного управления охранным оборудованием.

16. **Возможность многоканальной синхронной аудиозаписи (аудиоконтроля).** Как известно, синхронная с видео аудиозапись (аудиоконтроль) может очень существенно дополнять видеоконтроль анализом звуковой обстановки на охраняемом объекте. Обычно это очень помогает принятию решения о наступлении тревожного события или дает дополнительный канал информации, позволяющий отсеять ложное срабатывание системы видеоконтроля, например. Как правило, современные цифровые системы видеоконтроля имеют от 1-го - 2-х до 16-ти и более синхронных с видео аудиоканалов. Профессиональные системы, кроме обычной синхронной записи по срабатывании

детектора движения, должны обеспечивать еще аудиозапись по акустопуску, а также комбинированный режимы работы и возможность задания гибкой (интеллектуальной) логики обработки тревожных событий, связанных с синхронной записью звука и детектированием движения в системах видеоконтроля.

17. Наличие и общее количество аналоговых видеовыходов на один блок (одну плату). Как правило, скорее по традиции лучшего восприятия изображения на аналоговых мониторах, современные цифровые системы видеоконтроля имеют аналоговые выходы, к которым можно подключить обычные аналоговые видеомониторы (для организации дополнительного видеонаблюдения) или видеомагнитофоны (для организации дополнительной видеозаписи). На эти выходы, соответственно, можно выводить или сквозные видеоканалы, тревожную (тревожные) видеокамеру (видеокамеры), а также, просто наблюдать за заранее выбранным видеоканалом. Профессиональные системы, как правило, дополнительно к вышеописанному, могут позволять листать последовательно все тревожные видеоканалы и выводить их последовательно на аналоговый выход (выходы), а также задавать определенную гибкую логику обработки тревожных событий и вывода на аналоговые выходы любых видеоканалов в самых различных режимах просмотра (или видеозаписи).

18. Возможность экспорта видеоинформации. Очень полезная функция для документирования тревожных событий или преобразования видеоданных из внутреннего формата цифровой обработки и/или компрессии во внешние, как правило, широко распространенные форматы для дальнейшего их анализа и использования. Как правило, видеоряд преобразуется в широко распространенный формат AVI (или MPEG), а отдельные видеокадры - в формат JPEG (BMP). Такое преобразование обычно можно производить или в автоматическом, или ручном режимах в режиме "on-line" просмотра, а также при работе с видеоархивом.

Таблица 7. Сравнительные характеристики цифровых систем видеоконтроля

Модель		**Goal 6.0**	**Sivineya**	**NISS-VideoInspector**
Операционная система сервера / клиента	Win9x/Me	- / -	+ / +	+ / +
	WinNT	+ / -	+ / +	+ / +
	Win200	- / -	+ / +	+ / +
	Linux	- / -	- / -	- / -
Интерфейс системы	Win-подобн./ специализир.	+ / -	+ / -	- / +
Тип компрессии	(аппар. / прогр.)	Intel Indeo, MPEG-4	JPEG	Delta-Wavelet ап.-прогр.
Минимальный размер информ.	Кбайт	3-20	5-15	1-20

кадра для формата 3XX x 2XX				
Емкость видеоархива на 1G для формата 3XX x 2XX для скорости 25 FPS	кадров (часов), для справки	200 000 (2,2)	150 000 (1,7)	500 000 (5,6)
Формат видеокадров при обработке (записи)	пикселей (гор.) x (верт.)	640 x 480 320 x 240	640 x 480 320 x 240 160 x 120	768 x 576 768 x 288 384 x 288
Тип платы видеозахвата	(схема ввода)	3x1, 4x1	4x4, 2x1, 4x1	16x1,8x1,16x4
Стандарт цветности	PAL/NTSC/SEC	+ / - / +	+ / - / +	+ / + / -
Количество каналов со скоростью обраб. / записи до 25 FPS формата 3XX x 2XX	на 1 плату	1	4	4
	на блок	4	4, 8, 12, 16	4, 8, 12, 16
Количество каналов со скоростью обраб. /записи до 25 FPS формата 6XX x 2XX	на 1 плату	1	4	4
	на блок	4	4, 8, 12, 16	16
Количество мультиплекс. каналов обработки	на 1 плату	3, 4	16	16
	на блок	3-24	2, 4, 8, 16-96	4, 6, 8, 10,12, 16
Скорость обраб./записи немультиплексированных видеоизображений, FPS, для форм. 3XX x 2XX / 6XXx3XX	на 1 плату	25 / 25	100 / 100	200 / 200
	на блок	50 / 25	100 / 50	400 / 400
Скорость обраб/записи мультиплексированных видеоизображений, FPS, для форм. 3XX x 2XX / 6XXx3XX	на 1 плату	12,5 / 12,5	10 / 10	50 / 50
	на блок	50 / 25	40 / 40	100 / 100
Установка приоритетов по видеокамерам	обработка	+	+	+
	запись/гор.запись	+ / -	+ / -	+ / +
Одновременная запись/ отображение архива	(триплекс)	+	+	+
Видеодетектор активности/движения	активности / движения	+ / -	+ / -	+ / +
	компенс.помех	+	-	+
	чувтвит.	+	+	-
	разм./ контраст	- / -	- / -	+ / +
	управление по детектору	+	+	+
Управление телеметрией	(RS-485)	-	-	-
Тревожные входы	кол.	4	-	32
Выходы управления	кол.	-	-	32
Наличие (синхронного) аудиоконтроля	кол. каналов	4	-	16
Аналоговые выходы	кол.	-	-	12
	управление	-	-	+
Работа в сети TCP/IP	кол. серверов	1	1 +	-
	кол. клиентов	1	1 +	-
Архитектура сети	клиент/сервер	-	-	-
	файл/сервер	+	+	-
Экспорт видеоинформации	AVI (MPEG) /	- / -	- / +	- / +

	JPEG			
Оповещение, в т.ч. по коммут. линиям связи	дозвон / сообщ./ E-Mail / SMS	+ / + / - / -	- / - / - / -	+ / + / + / +
Удаленный мониторинг / администрирование сист.	сетев. клиент	- / -	+ / +	-
	Интернет	- / -	+ / -	+
Наличие протокола внешн./ внутр. событий в системе	внешн./ внутр.	+ / -	- / -	- / -
Карта-схема объекта	отобр./ управл.	+ / +	- / -	- / -
Средства архивирования	лок.ал. / удален.	- / -	- / -	- / -
Наличие средств программирования системы	макросы / язык программир.	+ / -	- / -	- / -
Встроенные средства защиты и безопасности системы	простые / многоуровнев.	+ / -	+ / -	+ / -
Интеграция с СКД, ОПС, АК и другими системами	возможность / наличие	- / -	- / -	- / -
Наличие спец. средств разработки ПО интеграции	(SDK)	-	-	-
Поддержка клиентов со стороны производит. / дилера	конс./обучение/ Интернет	- / - / +	+ / + / +	+ / + / +

Таблица 8. Сравнительные характеристики цифровых систем видеоконтроля

Модель		**AVer-S MP200**	**CTEC DVR-5600**	**Video Spider**
Операционная система сервера / клиента	Win9x/Me	+ / +	+ / +	- / +
	WinNT	- / -	+ / +	+ / +
	Win200	+ / +	- / -	- / -
	Linux	- / -	- / -	- / -
Интерфейс системы	Win-подобн./ специализир.	- / +	- / +	- / +
Тип компрессии	(аппар. / прогр.)	M-JPEG	JPEG, M-JPEG	MPEG, MPEG1
Минимальный размер информ. кадра для формата 3XX x 2XX	Кбайт	5-10	3-15	5-10
Емкость видеоархива на 1G для формата 3XX x 2XX для скорости 25 FPS	кадров (часов), для справки	150 000 (1,7)	200 000 (2,2)	150 000 (1,7)
Формат видеокадров при обработке (записи)	пикселей (гор.) x (верт.)	320 x 240	640 x 240 160 x 120	320 x 240 160 x 120
Тип платы видеозахвата	(схема ввода)	4x4	4x4	8 x 1
Стандарт цветности	PAL/NTSC/SEC	+ / + / -	+ / + / -	+ / + / -
Количество каналов со скоростью обраб. / записи до 25 FPS формата 3XX x 2XX	на 1 плату	4	-	8 *
	на блок	4	-	32 *
Количество каналов со скоростью	на 1 плату	-	4	-

обраб. /записи до 25 FPS формата 6XX x 2XX	на блок	-	16	-
Количество мультиплекс. каналов обработки	на 1 плату	-	-	8
	на блок	-	-	32
Скорость обраб./записи немультиплексированных видеоизображений, FPS, для форм. 3XX x 2XX / 6XXx3XX	на 1 плату	100 (/ 48 з)	100 (/12,5 з)	- / -
	на блок	64 (/ 32 з)	400 (/ 50 з)	- / -
Скорость обраб/записи мультиплексированных видеоизображений, FPS, для форм. 3XX x 2XX / 6XXx3XX	на 1 плату	-	- / 12,5	25 / -
	на блок	-	- / 50	100 / -
Установка приоритетов по видеокамерам	обработка	-	-	+
	запись/гор.запись	- / -	+ / -	+ / -
Одновременная запись/ отображение архива	(триплекс)	-	-	+
Видеодетектор активности/движения	активности / движения	+ / -	+ / -	+ / -
	компенс.помех	-	-	-
	чувтвит.	+	+	+
	разм./ контраст	- / -	- / -	- / -
	управление по детектору	+	+	+
Управление телеметрией	(RS-485)	-	+	+
Тревожные входы	кол.	16	16	5, 13
Выходы управления	кол.	12	4	-
Наличие (синхронного) аудиоконтроля	кол. каналов	-	-	-
Аналоговые выходы	кол.	-	-	+
	управление	-	-	+
Работа в сети TCP/IP	кол. серверов	1	1	1 +
	кол. клиентов	1	1	1 +
Архитектура сети	клиент/сервер	-	-	+
	файл/сервер	+	+	-
Экспорт видеоинформации	AVI (MPEG) / JPEG	- / -	- / +	+ / -
Оповещение, в т.ч. по коммут. линиям связи	дозвон / сообщ./ E-Mail / SMS	- / - / - / -	- / - / - / -	- / - / - / -
Удаленный мониторинг / администрирование сист.	сетев. клиент	+ / -	+ / -	+ / +
	Интернет	+ / -	- / -	- / -
Наличие протокола внешн./ внутр. событий в системе	внешн./ внутр.	+ / -	- / -	- / -
Карта-схема объекта	отобр./ управл.	-	- / -	- / -
Средства архивирования	лок.ал. / удален.	- / -	- / -	+ / -
Наличие средств программирования системы	макросы / язык программир.	- / -	+ / -	- / -
Встроенные средства защиты и безопасности системы	простые / многоуровнев.	+ / -	+ / -	+ / +

Интеграция с СКД, ОПС, АК и другими системами	возможность / наличие	- / -	- / -	- / -
Наличие спец. средств разработки ПО интеграции	(SDK)	+	-	+
Поддержка клиентов со стороны производит. / дилера	конс./обучение/ Интернет	+ / + / +	+ / - / -	- / - / +

Примечание: * - реальная скорость ввода составляет от 0,6 до 12,5 FPS по каждой камере и упаковывается в MPEG-1 поток 25 FPS одновременно по 8-ми каналам; (/ з) - скорость записи (в некоторых системах значительно меньше скорости обработки).

Таблица 9. Сравнительные характеристики профессиональных цифровых систем видеоконтроля.

Модель		**DigiEye**	**Mitsubishi DS-200**	**NISS-Inspector+**
Операционная система сервера / клиента	Win9x/Me	- / -	- / -	+ / +
	WinNT	- / -	+ / +	+ / +
	Win200	- / -	- / -	+ / +
	Linux	- / -	- / -	+ / -
Интерфейс системы	Win-подобн./ ециализир.	- / +	+ / -	- / +
Тип компрессии	(аппар. / прогр.)	Delta, JPEG	MPEG-2	Delta-Wavelet ı.-прогр.
Минимальный размер адра для формата 3XX x	Кбайт	3 - 30	5-60	1-20
Емкость видеоархива на рмата 3XX x 2XX и 25 FPS	кадров (часов), для справки	250 000 (2,8)	100 000 (1,1)	500 000 (5,6)
Формат видеокадров при (записи)	пикселей ь.) x (верт.)	640 x 480 640 x 240 320 x 240	704 x 576	768 x 576 768 x 288 384 x 288
Тип платы видеозахвата	(схема ввода)	-	-	16x1,8x1,16x4
Стандарт цветности	PAL/NTSC	+ / +	+ / +	+ / +
Количество каналов со обраб. / записи до 25 FPS XX x 2XX	на 1 плату	-	-	4
	на блок	-	-	16
Количество каналов со обраб. /записи до 25 FPS XX x 2XX	на 1 плату	-	-	4
	на блок	-	-	16
Количество мультиплекс. бработки	на 1 плату	-	-	4 - 16
	на блок	16	64 *	4 - 64
Скорость обраб/записи лексированных	на 1 плату	-	-	100 / 100
	на блок	-	-	400 / 400

ражений, FPS, для XXx2XX / 7XXx2XX				
Скорость обраб/записи ксированных ражений, FPS, для XXx2XX/7XXx2XX	на 1 плату	-	-	50 / 50
	на блок	25 / 25	- / 25(50)	200 / 200
Установка приоритетов амерам	обработка	-	-	+
	запись/гор.запись	- / -	- / -	+ / +
Одновременная запись/ ие архива	(триплекс)	+	-	+
Видеодетектор	активности / вижения	+ / -	+ / -	+ / +
	компенс.помех	-	-	+
	число зон детект.	1	1	1
	разм./ контраст	+ / +	+ / +	+ / +
	управление по етектору	+	+	+
Управление телеметрией	(RS-485)	+	-	+
Тревожные входы	кол.	24	+	4 - 64
Выходы управления	кол.	24	-	4 - 64
Наличие (синхронного) роля	кол. каналов	-	-	1, 2, 4, 5, 8, 16
Аналоговые выходы	кол.	4	1	1, 3, 6, 9, 12
	управление	+	-	+
Работа в сети TCP/IP	кол. серверов	1 +	1	1 +
	кол. клиентов	1 +	1	1 +
Архитектура сети	клиент/сервер	-	-	+
	файл/сервер	+	+	+
Экспорт рмации	AVI/ JPEG(BMP)	- / +	- / -	+ / +
Оповещение, в т.ч. по иниям связи	дозвон / сообщ./ Mail / SMS	+ / - / + / -	- / - / - / -	+ / + / + / +
Удаленный мониторинг / ирование сист.	сетев. клиент	+ / +	+ / -	+ / +
	Интернет	- / -	- / -	+ / +
Наличие протокола утр. событий в системе	внешн./ внутр.	+ / -	- / -	+ / +
Карта-схема объекта	отобр./ управл.	- / -	- / -	+ /+
Средства архивирования	лок.ал. / удален.	+ / +	+ / -	+ / +
Наличие средств ирования системы	макросы / язык ограммир.	+ / -	- / -	+ / +
Встроенные средства безопасности системы	простые / огоуровнев.	+ / +	+ / +	+ / +
Интеграция с СКД, ОПС, ими системами	возможность / наличие	- / -	- / -	+ / +
Наличие спец. средств и ПО интеграции	(SDK)	-	-	+
Поддержка клиентов	конс./обучен./ Интернет	- / - / +	- / - / +	+ / + / +

Таблица 10. Сравнительные характеристики профессиональных цифровых систем видеоконтроля.

Модель		VideoNet	Видео-ИКС	CVS_NT
Операционная система сервера / клиента	Win9x/Me		- / -	+ / +
	WinNT	+ / +	+ / +	- / +
	Win200	+ / +	+ / +	- / -
	Linux	- / -	- / -	- / -
Интерфейс системы	Win-подобн./ специализир.	+ / -	+ / -	+ / -
Тип компрессии	(аппар. / прогр.)	h.261+	Wavelet	JPEG
Минимальный размер информ. кадра для формата 3XX x 2XX	Кбайт	2-20	7-30	3-40
Емкость видеоархива на 1G для формата 3XX x 2XX и скорости 25 FPS	кадров (часов), для справки	330 000 (3,7)	150 000 (1,7)	150 000 (1,7)
Формат видеокадров при обработке (записи)	пикселей (гор.) x (верт.)	768 x 576 384 x 288 192 x 144	720 x 576 720 x 480	768 x 576 768 x 288 384 x 288
Тип платы видеозахвата	(схема ввода)	4 x 4, 4 x 1	8 x 1, 32 x 1 *	1 x 1, 4 x 1 *
Стандарт цветности	PAL/NTSC	+ / +	+ / +	+ / +
Количество каналов со скоростью обраб. / записи до 25 FPS формата 3XX x 2XX	на 1 плату	4	-	1
	на блок	16	-	1
Количество каналов со скоростью обраб. /записи до 25 FPS формата 7XX x 2XX	на 1 плату	4	1	1
	на блок	8	4	1
Количество мультиплекс. каналов обработки	на 1 плату	4 - 16 *	8	-
	на блок	4 - 64 *	16, 32	4-32 *
Скорость обраб/записи немультиплексированных видеоизображений, FPS, для формата 3XXx2XX / 7XXx2XX	на 1 плату	100 / 100	25 / 25	25 / 25
	на блок	300 / 150	50 / 50	25 / 25
Скорость обраб/записи мультиплексированных видеоизображений, FPS, для формата 3XXx2XX/7XXx2XX	на 1 плату	50 / 50	50 / 50	16-25 / 16-25*
	на блок	200 / 150	50 / 50	16-25 / 16-25*
Установка приоритетов по видеокамерам	обработка	+	+	-
	запись/гор.запись	+ / -	+ / +	+ / -
Одновременная запись/ отображение архива	(триплекс)	+	-	+
Видеодетектор	активности / движения	+ / +	+ / -	+ / +

	компенс.помех	-	+	+
	число зон детект.	1	1	8
	разм./ контраст	+ / +	+ / +	+ / +
	управление по детектору	+	+	+
Управление телеметрией	(RS-485)	+	-	-
Тревожные входы	кол.	256	16	32
Выходы управления	кол.	256	1	1
Наличие (синхронного) аудиоконтроля	кол. каналов	8, 16	-	-
Аналоговые выходы	кол.	-	5	3
	управление	-	+	+
Работа в сети TCP/IP	кол. серверов	1	1	1 +
	кол. клиентов	1 +	1 +	1 +
Архитектура сети	клиент/сервер	-	-	+
	файл/сервер	+	+	+
Экспорт видеоинформации	AVI/ JPEG(BMP)	- / -	- / +	- / +
Оповещение, в т.ч. по коммут. линиям связи	дозвон / сообщ./ E-Mail / SMS	- / - / - / -	- / - / - / -	- / - / - / -
Удаленный мониторинг / администрирование сист.	сетев. клиент	+ / +	+ / +	+ / +
	Интернет	- / -	- / -	- / -
Наличие протокола внешн./ внутр. событий в системе	внешн./ внутр.	+ / +	+ / +	+ / +
Карта-схема объекта	отобр./ управл.	-	- / -	+ / -
Средства архивирования	лок.ал. / удален.	-	+ / -	+ / -
Наличие средств программирования системы	макросы / язык программир.	+ / -	- / -	- / -
Встроенные средства защиты и безопасности системы	простые / многоуровнев.	+ / -	+ / +	+ / -
Интеграция с СКД, ОПС, АК и другими системами	возможность / наличие	- / -	- / -	- / -
Наличие спец. средств разработки ПО интеграции	(SDK)	-	+	+
Поддержка клиентов	конс./обучен./ Интернет	+ / + / +	+ / + / -	+ / + / +

Примечание * - с внешними модулями мультиплекирования, коммутации или сопряжения.

Как правило, практически все современные цифровые системы видеоконтроля позволяют осуществлять удаленный видеомониторинг и/или удаленное администрирование системы. Для этого обычно используются или специальные сетевые клиенты, или самые обычные браузеры типа Microsoft Internet Explorer, Netscape, Opera и т.п. Практически все системы работают в сети по протоколу TCP/IP. Некоторые имеют встроенные средства автодозвона и работы по обычным телекоммуникационным линиям.

Профессиональные цифровые системы видеоконтроля, как правило, отличает от обычных систем возможность работы неограниченного количества видеосерверов и сетевых клиентов в одной сети любого масштаба (включая низкоскоростные сегменты сети), возможность организации перекрестного видеонаблюдения, использование архитектуры клиент-сервер, ведения единого протокола для всего сетевого комплекса в целом, а также возможность распределения охранных функций в пространстве сети и задание гибкой логики обработки тревожных событий. Таким образом, преимуществом профессиональных сетевых систем является отсутствие каких-либо количественных ограничений на общее количество видеоканалов обработки, а также общее количество охранного оборудования, включенного в единую сеть. К сожалению, далеко немногие цифровые системы видеоконтроля, претендующие на рынок профессионального оборудования в части сетевых свойств, таковыми на самом деле являются. Поскольку на возможность работы в сети, особенно по низкоскоростным каналам связи, очень сильно влияет средний размер видеокадра заданного формата и определенного качества (например, 1-2 Кбайт для кадра формата 384x288), то очень многие системы, реально работающие с небольшими степенями компрессии, при заданном уровне качества отдельных кадров (например, 5-10 Кбайт для того же кадра формата 384x288), реально неспособны эффективно работать в сложном сетевом окружении, и, особенно, при наличии сегментов сети с низкоскоростными телекоммуникациями. Так, например, отличие размера кадра в 5 раз дает аналогичное отличие и в максимальной скорости передачи видеосигналов по сети, а иногда - практическую невозможность такой работы на реальных объектах.

Как и любая другая компьютерная система безопасности, современная цифровая система видеоконтроля, кроме выполнения своих прямых функций, должна обеспечивать необходимый уровень собственной безопасности. Как правило, в обычных системах видеоконтроля дело ограничивается простым вводом идентификатора оператора (администратора) и пароля. Профессиональные системы, кроме этого, предоставляют более гибкие многоуровневые механизмы защиты - от сокрытия доступного оборудования и ограничения прав на администрирование основных элементов системы - до запрета на выгрузку как самой системы, так и ее интерфейсов. Кроме этого, некоторые профессиональные цифровые системы видеоконтроля, используя сетевые свойства и свойства администрирования операционных систем, на базе которых они выполнены, позволяют осуществлять очень гибкую политику собственной безопасности, интегрированную в общую политику безопасности охраняемого объекта (различные мониторы безопасности, использование дополнительных средств шифрования, единых

средств администрирования и т.д.). К сожалению, все вышесказанное нельзя отнести к некоторым блочным цифровым системам, поставляемым в заранее сконфигурированном виде, не допускающим вмешательства на уровне ее общесистемного программного обеспечения.

Очень важная характеристика, т.к. во многом определяет сетевые свойства, стабильность и надежность всей цифровой системы видеоконтроля, а также возможности ее интеграции в общую информационную систему и компьютерную сеть охраняемого объекта. Как правило, современные цифровые системы видеоконтроля выполнены на следующих операционных системах: Windows98/Me, Windows NT, Windows 2000 и Linux. Самые стабильные и надежные операционные системы - это Windows NT, Windows 2000 и Linux. Обычно базовой системой является Windows NT, как одна из самых устоявшихся и давно сертифицированных во всем мире по условиям безопасности не ниже класса C2. Системы на базе Linux пока встречаются еще редко, однако эта операционная система является одной из самых перспективных, в связи с открытостью ее кода и возможностью компиляции ядра со строго определенными свойствами, что очень важно для обеспечения безопасности и упрощения возможности сертификации цифровой системы видеоконтроля в целом.

Как правило, все системы видеоконтроля позволяют задавать определенную логику обработки тревожных событий (по расписанию, по характеру тревожных событий). Обычно все сводится к определению реакций на срабатывание детектора движения (активности), обработке состояний тревожных входов и выдаче соответствующих управляющих сигналов. Обычно такое программирование реализуется на уровне написания специальных макросов, которые представляют собой очень простые средства программирования. Отдельные профессиональные системы, дополнительно к возможности макропрограммирования имеют мощные встроенные средства программирования специальных скриптов, что позволяет, как правило, на любое событие в системе видеоконтроля определить любую доступную реакцию всех исполнителей, входящих в систему видеоконтроля. Для интегрированных систем такое программирование позволяет обрабатывать все события во всех подсистемах (СКД, ОПС, АК и т.д.) и вырабатывать для них все допустимые реакции управления. Такие системы принято считать интеллектуальными, т.к. они позволяют реализовать достаточно сложные алгоритмы реакций и управления, подобные человеческой логике принятия решений. Иногда, с целью предоставления возможности самостоятельно, без вмешательства разработчиков системы видеоконтроля, разрабатывать специализированные приложения и модули интеграции, некоторые системы, как правило профессиональные, могут

поставляться со специальными средствами разработки прикладного программного обеспечения (так называемые SDK). Для интегрированных систем наличие таких средств является просто необходимым для реализации возможности интеграции с любым внешним охранным оборудованием, включая СКД и ОПС.

ЛИТЕРАТУРА

1. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. – М., 2001 – 496 с.
2. Ярочкин, В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. – М.: Академический проект: Трикста, 2005. – 544 с.
3. Барсуков, В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2000. – 496 с., ил.
4. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия –Телеком, 2000. - 452 с., ил
5. Компьютерная преступность и информационная безопасность / А.П. Леонов [и др.]; под общ. Ред.А.П. Леонова. – Минск: АРИЛ, 2000. – 552 с.

Перечень нормативных документов

1. ГОСТ Р 8.568-97. Государственная система обеспечения единства измерений. Аттестация испытательного оборудования. Основные положения
2. ГОСТ Р 15.201-2000. Система разработки и постановки продукции на производство. Продукция производственно-технического назначения
3. ГОСТ Р ИСО/МЭК 7810-2002. Карты идентификационные. Физические характеристики
4. ГОСТ Р ИСО/МЭК 7811-1-2003. Карты идентификационные. Способ записи. Часть 1. Тиснение
5. ГОСТ Р ИСО/МЭК 7811-2-2002. Карты идентификационные. Способ записи. Часть 2. Магнитная полоса малой коэрцитивной силы
6. ГОСТ Р ИСО/МЭК 7811-3-2003. Карты идентификационные. Способ записи. Часть 3. Расположение рельефных символов на картах формата ID-1

7. ГОСТ Р ИСО/МЭК 7811-6-2003. Карты идентификационные. Способ записи. Часть 6. Магнитная полоса большой коэрцитивной силы

8. ГОСТ Р ИСО/МЭК 7816-1-2002. Карты идентификационные. Карты на интегральных схемах с контактами. Часть 1. Физические характеристики

9. ГОСТ Р ИСО/МЭК 7816-2-2002. Информационная технология. Карты идентификационные. Карты на интегральных схемах с контактами. Часть 2. Размеры и расположение контактов

10. ГОСТ Р ИСО/МЭК 7816-4-2004. Информационная технология. Карты идентификационные. Карты на интегральных схемах с контактами. Часть 4. Межотраслевые команды для обмена

11. ГОСТ Р ИСО/МЭК 7816-6-2003. Карты идентификационные. Карты на интегральных схемах с контактами. Часть 6. Элементы данных для межотраслевого обмена

12. ГОСТ Р ИСО/МЭК 7816-10-2004. Карты идентификационные. Карты на интегральных схемах с контактами. Часть 10. Электронные сигналы и ответ на восстановление у синхронных карт

13. ГОСТ Р ИСО/МЭК 10373-1-2002. Карты идентификационные. Методы испытаний. Часть 1. Общие характеристики

14. ГОСТ Р ИСО/МЭК 10373-2-2002. Карты идентификационные. Методы испытаний. Часть 2. Карты с магнитной полосой

15. ГОСТ Р ИСО/МЭК 10536-2-2004. Карты идентификационные. Карты на интегральных схемах бесконтактные. Часть 2. Размеры и расположение зон связи

16. ГОСТ Р ИСО/МЭК 10536-3-2004. Карты идентификационные. Карты на интегральных схемах бесконтактные. Часть 3. Электронные сигналы и процедуры восстановления

17. ГОСТ Р ИСО/МЭК 11693-2004. Карты идентификационные. Карты с оптической памятью. Общие характеристики

18. ГОСТ Р ИСО/МЭК 11694-1-2003. Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Часть 1. Физические характеристики

19. ГОСТ Р ИСО/МЭК 11694-2-2003. Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Часть 2. Размеры и расположение оптической зоны

20. ГОСТ Р ИСО/МЭК 11694-3-2003. Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Часть 3. Оптические свойства и характеристики

21. ГОСТ Р ИСО/МЭК 15693-1-2004. Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия. Часть 1. Физические характеристики

22. ГОСТ Р ИСО/МЭК 15693-2-2004. Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия. Часть 2. Воздушный интерфейс и инициализация

23. ГОСТ Р ИСО/МЭК 15963-2005. Автоматическая идентификация. Радиочастотная идентификация для управления предметами. Уникальная идентификация радиочастотных меток

24. ГОСТ Р ИСО/МЭК 19794-2-2005. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца - контрольные точки

25. ГОСТ Р ИСО/МЭК 19794-4-2006. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца

26. ГОСТ Р ИСО/МЭК 19794-5-2006. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица

27. ГОСТ Р ИСО/МЭК 19794-6-2006. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза

28. ГОСТ Р 50009-2000. Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний

29. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

30. ГОСТ Р 51053-97. Замки сейфовые. Требования и методы испытания на устойчивость к криминальному открыванию и взлому

31. ГОСТ Р 51072-2005. Двери защитные. Общие технические требования и методы испытаний на устойчивость к взлому, пулестойкость и огнестойкость

32. ГОСТ Р 51112-97. Средства защитные банковские. Требования по пулестойкости и методы испытаний

33. ГОСТ Р 51330.0-99 (МЭК 60079-0-98). Электрооборудование взрывозащищенное. Часть 0. Общие требования

34. ГОСТ Р 52436-2005. Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний

35. ГОСТ Р 52582-2006. Замки для защитных конструкций. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому

36. ГОСТ Р 52931-2008. Приборы контроля и регулирования технологических процессов. Общие технические условия

37. ГОСТ Р МЭК 60065-2005. Аудио-, видео- и аналогичная электронная аппаратура. Требования безопасности

38. ГОСТ 2.601-2006. Единая система конструкторской документации. Эксплуатационные документы

39. ГОСТ 2.610-2006. Единая система конструкторской документации. Правила выполнения эксплуатационных документов

40. ГОСТ 12.1.004-91. Система стандартов безопасности труда. Пожарная безопасность. Общие требования

41. ГОСТ 12.1.006-84. Система стандартов безопасности труда. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля

42. ГОСТ 12.1.019-79. Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты

43. ГОСТ 12.2.003-91. Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности

44. ГОСТ 12.2.007.0-75. Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности

45. ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения

46. ГОСТ 27.003-90. Надежность в технике. Состав и общие правила задания требований по надежности

47. ГОСТ 5089-2003. Замки и защелки для дверей. Технические условия

48. ГОСТ 14192-96. Маркировка грузов

49. ГОСТ 14254-96 (МЭК 529-89). Степени защиты, обеспечиваемые оболочками (код IP)

50. ГОСТ 15150-69. Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды

51. ГОСТ 16962-71. Изделия электронной техники и электротехники. Механические и климатические воздействия. Требования и методы испытаний

52. ГОСТ 19091-2000. Замки и защелки для дверей. Методы испытаний

53. ГОСТ 26828-86. Изделия машиностроения и приборостроения. Маркировка.

54. РД 78.36.003-2002 «Инженерно-техническая укреплённость. Технические средства охраны. Требования и нормы проектирования по защите объектов отпреступных посягательств».

55. СНиП 3.01.01-85* «Организация строительного производства», изд. 1995 с изм. 1,2;

56. СНиП 1.04.03-85* «Нормы продолжительности строительства и задела в строительстве предприятий, зданий и сооружений», изд. 1991;

57. СНиП 5.01.06-86 «Нормы расхода материалов, изделий и труб на 1 млн. руб. сметной стоимости строительно-монтажных работ по объектам электроэнергетики»;

58. СНиП 3.02.01-87 «Земляные сооружения, основания и фундаменты»;

59. СНиП 3.05.06-85 «Электротехнические устройства»;

60. СН 494-77 «Нормы потребности в строительных машинах»;

61. Руководящие материалы «Временные сооружения для строительства электросетевых объектов», №12575 тм;

62. Сборники нормативных показателей расхода материалов в строительстве;

63. Сборник «Расчетные нормативы для составления проектов организации строительства» часть IV, ЦНИИ ОМТП Госстроя СССР, 1973;