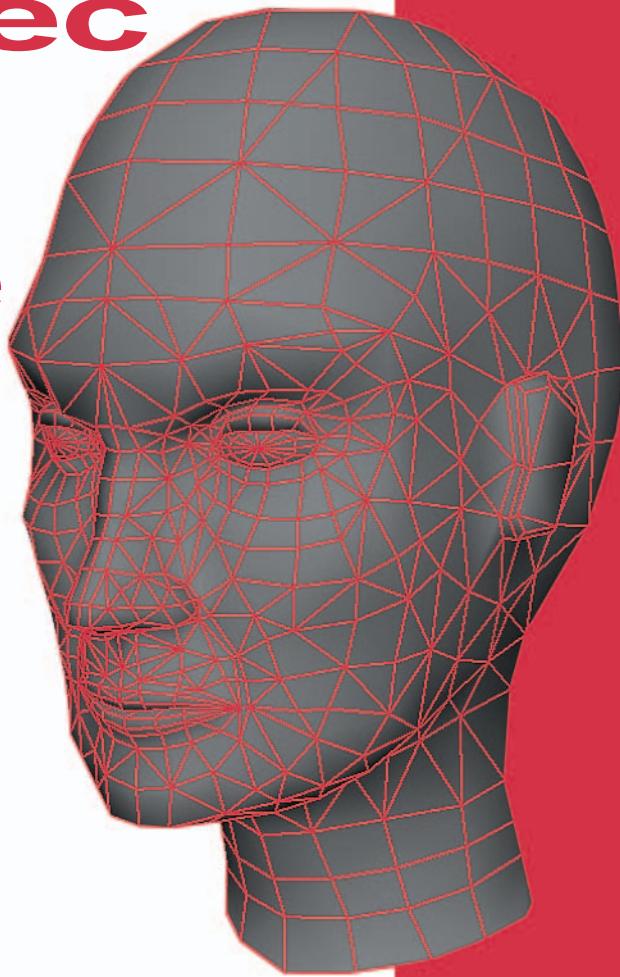


Cognitec & Viisage (ZN Vision)



PROFESSIONALS - to - PROFESSIONALS



CCTV

Российское издание журнала
по системам видеонаблюдения
и охранному телевидению

#6
2004

Издается "Media Focus"

<http://cctvfocus.ru>

focus



Тест-драйв: Системы распознавания лиц

Тест-драйв: Сетевые видеосервера

Тест-драйв: Domination

Теория: Беспроводные сети
Выставка "Охрана и Безопасность"
Цифровая запись как доказательство



Новые DVR и камеры Samsung

Ваша безопасность в надежных руках.



Системы безопасности Samsung. Заслуживают безусловного доверия.



SCC-C6405P

1/4-дюймовая ПЗС-матрица с повышенной чувствительностью в видимой ИК области спектра; с функцией WDR; 480 тв.л.; 22х оптическое и 10х цифровое увеличение; интерфейсы RS-485, RS-422; 360° горизонтальный обзор, 0-180° вертикальный обзор; быстрый обзор с максимальной скоростью 400°/сек.



SMT-171P, 190P

Размер рабочей области экрана 17 (19) дюймов, время отклика: 8 (12) мс, яркость (типичная): 300 (400) кд/м², коэффициент контрастности: 700:1 (400:1), угол обзора (В/Г): 150/120, интерфейс: аналоговый/цифровой, строчная частота: 31-82 кГц, имеющиеся цвета корпуса: черный.

SHR-4081, 4160

8 (16)-ти каналный видеорегистратор; MPEG 4; CIF 300 ips (режим Triplex); USB2.0 интерфейс; подключение внешних HDD, CD/DVD-RW, USB Flash Drive; подключение к сети Ethernet.



**SHR-2040, 2042,
2160, 2162**

4 (16)-х каналный видеорегистратор; MPEG 4; CIF 100 ips (режим Triplex); USB2.0 интерфейс; подключение внешних HDD, CD/DVD-RW, USB Flash Drive; подключение к сети Ethernet.



SAMSUNG

ELECTRONICS

Новые технологии SAMSUNG

Новые видеокамеры:

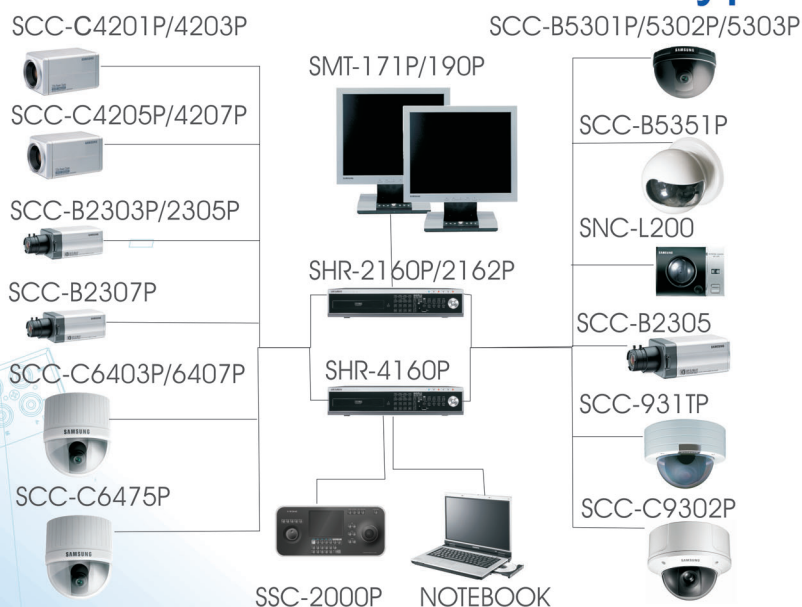
- 32x -оптическое увеличение (320-полное, 32x оптическое и 10x цифровое)
- 530/570 ТВЛ цвет/ч.б.
- Встроенный web-трансмиситтер



SCC-C6403P - самая дешевая роботизированная видеокамера с 32x оптическим увеличением!

“Виртуальная матрица” с системной клавиатурой SSC-2000P

- управление камерами
- управление регистраторами
- управление мультиплексорами
- управление сетевыми камерами
- организация “виртуальной матрицы”



Официальный партнер
SAMSUNG ELECTRONICS
в России и странах СНГ



От редакции

Заканчивается 2004 год, и мы предлагаем вашему вниманию последний в этом году номер журнала. Коллектив нашей редакции поздравляет всех читателей с наступающим, а для кого-то уже наступившим, Новым годом и желает творческих успехов и успешной реализации всех задуманных проектов. Подводя итоги текущего года, мы отметим, что нам не только удалось реализовать наши планы по увеличению информативности журнала, но также значительно расширить нашу читательскую аудиторию.

Конец года выдался очень урожайным на события и новинки, с которыми мы спешим познакомить наших читателей. Из событий мы особенно бы отметили проходившую с 9 по 11 ноября в Санкт-Петербурге выставку "Охрана и Безопасность", а из новинок, представленных в нашем журнале, мы рекомендуем обратить особое внимание на очень интересную телекамеру с разрешением до 21 мегапиксела, которую разработала компания Spectrum San Diego Inc. В этой новинке используется матрица ПЗС от Dalsa с технологией строчного сканирования для получения черно-белых изображений с что позволяет распознавать лица и автомобильные номера на больших расстояниях.

Особое внимание в этом номере мы уделили системам распознавания лиц. В рубрике "тест-драйв" мы представили две системы: ZN-SmartEye (теперь известная как Viisage FaceFinder), разработанная немецкой компанией ZN Vision Technologies AG, а также модуль распознавания лиц в интегрированной системе ITV Интеллект. Этот модуль распознавания лиц был разработан еще одной немецкой компанией Cognitec Systems GmbH. Тема тестирования систем распознавания лиц оказалась весьма интересной и неожиданно популярной, поэтому в следующих номерах мы продолжим знакомить наших читателей с другими системами, в том числе и с отечественными разработками, что является еще одним серьезным аргументом в пользу оформления годовой подписки на "ССТV Фокус". Кстати, подписку на 2005 год можно уже сейчас быстро оформить на нашем веб-сайте www.cctvfocus.ru.

По заказу правительства США и ряда других организаций проводилась серия тестирований (FERET, FRVT), которые, к сожалению, не только не сумели выявить серьезных преимуществ какой-либо из тестируемых систем, но и окончательно запутали ситуацию с системами распознавания лиц. Достаточно любопытно смотреть, как компании, предоставившие свои продукты для тестирования, выборочно публикуют те результаты тестирования, которые выставляют их системы распознавания лиц в наиболее выгодном свете. Последнее тестирование FRVT 2002 (Face Recognition Vendor

Tests) имело место более двух лет назад, и, судя по всему, его организаторы и заказчики разочаровались не только в тестировании, но и в самих технологиях распознавания лиц. По крайней мере, проводившееся с 1994 года с завидной регулярностью тестирование сейчас не осуществляется, и не слышно ничего о том, что оно будет проведено в ближайшем будущем. Мы не ставили перед собой задачу провести несколько миллионов сравнений различных фотографий, для того чтобы получить очевидные выводы. Для нас куда важнее было представить выбранные нами системы так, как если бы наши читатели находились вместе с нами в тестовой лаборатории и могли видеть все достоинства и недостатки этих продуктов, а также сделать заключение относительно применения таких систем на практике.

Все мы уже привыкли к тому, что все большее количество продуктов CCTV использует подключение по беспроводным сетям, число инсталляций с использованием беспроводных сетей также возрастает. За последние годы мы видели уже немало несовместимых между собой решений и неэффективных стандартов, но, наконец, индустрия определилась с поддержкой одной серии стандартов для беспроводных сетей, а именно серии стандартов 802.11. Впрочем, существует много вариаций стандартов 802.11. Некоторые из этих вариаций более "зрелые", чем другие. Сейчас все более важно не просто разбираться в номенклатуре этих стандартов, но и понимать, какими возможностями они обладают и какое практическое применение они имеют в охранном телевидении также, как и в других сферах. Чтобы помочь разобраться с этими стандартами, мы предлагаем вниманию читателей статью, рассказывающую о всем многообразии стандартов 802.11.

Хотя мы все в той или иной степени понимаем, что представляют собой аналоговые и цифровые сигналы, Джон Уоткинс из компании Snell&Wilcox в своей статье "От аналогового к цифровому" подробно объясняет теорию, на которой основывается приобретающий все большее значение мир цифрового видео.

И в заключение мы предлагаем нашим читателям ознакомиться с подборкой материалов, посвященной законности использования видеозаписи и техническим и юридическим аспектам ее использования при судебных разбирательствах. Данная подборка вобрала в себя несколько интервью и любезно предоставленные материалы как специалистов в области права, так и людей, непосредственно использующих системы видеонаблюдения и практически ежедневно решающих различные технические и юридические вопросы, связанные с ними.

№ 5 (11) сентябрь-октябрь 2004 года

Журнал зарегистрирован Министерством РФ по делам печати, телерадиовещания и средств массовых коммуникаций. Свидетельство о регистрации ПИ №77-14952.

Журнал выходит один раз в два месяца
(6 номеров в год)

Идея: Мурат Алтуев

Над номером работали:
Станислав Поздняков, Максим Черняков,
Евгений Шарапов, Азрет Тебердиев, Надежда
Франтова, Вадим Мытник, Марина Хайкова,
Анастасия Беленко-Франтова, Луиза
Шарапова, Эверест Мокаев

Рисунки: Нина Селиванова

Адрес редакции

115201, Москва, 1-й Котляковский
переулок, д. 3, офис 16 (м. Каширская).

Главный редактор

Станислав Поздняков
E-mail: editor@cctvfocus.ru

Заместитель главного редактора

Максим Черняков
E-mail: press@cctvfocus.ru

Технический редактор

Евгений Шарапов
E-mail: testdrive@cctvfocus.ru

Отдел рекламы

Эверест Мокаев
Тел.: +7 (095) 110-9975
E-mail: adv@cctvfocus.ru
Web: <http://cctvfocus.ru/adv>

Отдел дизайна

Вадим Мытник
E-mail: design@cctvfocus.ru

Оптовая продажа и распространение

Анастасия Горбанева
Тел.: +7 (095) 110-9975
E-mail: sub@cctvfocus.ru
Web: <http://cctvfocus.ru/distribution/>

Подписка на журнал

Анастасия Горбанева
Тел.: +7 (095) 110-9975,
Факс: +7 (095) 110-9975
E-mail: sub@cctvfocus.ru
Web: <http://cctvfocus.ru/subscription/>

Бухгалтерия

Татьяна Постникова
Тел.: +7 (095) 110-9975
E-mail: buh@cctvfocus.ru

РАСПРОСТРАНИТЕЛИ ЖУРНАЛА

Все страны:

ОЗОН — книжный интернет-магазин
<http://ozon.ru/context/detail/id/1495283>

МК-ПЕРИОДИКА

Тел.: +7 (095) 284-5008
<http://www.periodicals.ru>

ИНФОРМНАУКА

Подписной индекс 99001.
Тел.: +7 (095) 152-5481, 155-4342

Азербайджан: DEMONIK

Тел.: (99450)-6201370 (Фуад Айдаев)
370118, Баку, ул. Нахичеванского 67/51.

Белоруссия: ВАЛЮСИТ (Минск)

Тел.: +375 (17) 238-9775, 8-0296-333-691

Украина: АГЕНТСТВО КСС

тел.: (0352) 430427
<http://www.kss.kiev.ua/>

Москва и Московская область:

DSSL

Тел.: (095) 938-9492, 938-9493
<http://www.dssl.ru>

ITV

Тел.: (095) 775-1199
<http://www.itv.ru>

АЛЬГИС-СЕКЬЮРИТИ

Тел.: (095) 995-8809

<http://www.algis.ru>

АРМО-СИСТЕМЫ

Тел.: (095) 937-9056, 937-9057
<http://www.armosystems.ru>

АСТЕРО

Тел.: (095) 250-5387
<http://www.astero.ru>

ЛИНК, НПФ

Тел.: (095) 119-7499, 8 (0967) 67-4245
Подольский р-н. <http://www.link.podolsk.ru>

ОЗОН — лучший книжный интернет-магазин

Заказ по телефону **797-92-84** только для жителей Москвы и Московской области.
<http://ozon.ru/context/detail/id/1495283>

СПЕЦИАЛЬНЫЕ РЕШЕНИЯ И СИСТЕМЫ

Тел.: (095) 923-6097, 928-4818
<http://www.security-systems.ru>

ТАТРИС БЕЗОПАСНОСТЬ

Тел.: (095) 748-6888, 489-6025
<http://www.tatrissecurity.ru>

ТСО — Технические Средства Охраны

Тел.: (095) 363-3774, 165-9245, 165-4094
<http://www.tso.ru>

ГРОСС-ЭЛЕКТРО

Тел.: (095) 781-3660(многоканальный),

369-27-57

<http://www.perimetr.ru>

**НАЦИОНАЛЬНЫЕ ЛАБОРАТОРИИ
БЕЗОПАСНОСТИ**

Тел.: (095) 332-5588,
Тел.: (095) 332-5498
<http://www.security-market.ru>

Новокузнецк: ЭВРИКОМ-КУЗБАСС

Тел.: (3843) 46-7265, 46-7265
<http://www.evrikom.ru>

Санкт-Петербург: БИК-ИНФОРМ

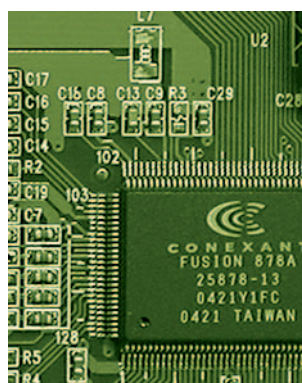
Тел.: (812) 252-2862, 252-7413, 118-5944
<http://bic-inform.spb.ru>

За достоверность рекламной информации ответственность несут рекламодатели. Рекламные материалы не редактируются и не корректируются.

Все права защищены. Никакая часть данного издания не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая запись на магнитный носитель, использование и хранение в базах данных и информационно-поисковых системах, без письменного разрешения редакции. Исключение составляют взятые в кавычки цитаты из журнала, приводимые в критических статьях и обзорах. Копирование любой части данного журнала с целью, отличной от Вашего личного использования, является нарушением закона об авторских правах.

В этом номере

Выставка "Охрана и Безопасность" в Санкт-Петербурге, 2004.	4
Выставка "Охрана. Спасение. Безопасность" в иркутском "Сибэкспоцентре".....	7
Вот, новый поворот... что он нам несет... ..	8
SentryScore - первая в мире система видеонаблюдения с разрешением до 21 мегапиксела	14
Тест-драйв сетевых видеосерверов	18
Тест-драйв видеосервера Domination	36
Беспроводные сети. Серия стандартов 802.11.....	46
Системы распознавания лиц и суровая действительность	52
Тест-драйв: ZN-SmartEye (Viisage FaceFinder).....	54
Тест-драйв: Модуль распознавания лиц в интегрированной системе ITV Интеллект (Cognitec Systems GmbH)	60
От аналогового к цифровому	68
Цифровая видеозапись как доказательство	77



Выставка “Охрана и Безопасность” в Санкт-Петербурге, 2004

Наш журнал с большим интересом следит за такими крупными событиями отечественной индустрии безопасности, каким, безусловно, является проходившая с 9 по 11 ноября в Санкт-Петербурге выставка “Охрана и Безопасность”. Хотелось бы донести свои впечатления от прошедшей выставки до наших читателей, которые по тем или иным причинам не смогли на ней присутствовать.

К сожалению, редакция нашего журнала из-за определенных сложностей не успела оформить самостоятельную заявку на отдельный стенд, и нам пришлось ютиться на небольшом столике на стенде другой компании, которая любезно предоставила нам часть своей площади.



Группа компаний “АРМО” была представлена региональным подразделением “АРМО-Петербург”.

Сразу отметим, что, несмотря на сложности, для нашего издательства эта поездка не стала убыточной и никаких разочарований и неприятных сюрпризов нам не принесла. Мы вполне окупили наш визит на выставку продажей книг и каталогов, хотя и не в полной мере выполнили задачу по повышению узнаваемости издательства и журнала.

Определенно, выставка “Охрана и Безопасность” является 3 выставкой по значимости на территории России. Она немного не дотягивает до уровня двух лидеров - форума “Технологии Безопасности” и MIPS, но при этом имеет свои отличительные от них положительные моменты.

Выставка отметила в этом году свой 8 день рождения. А это уже довольно солидный возраст для российского рынка безопасности и всего, что с ним связано. Как отмечали некоторые участники, в прошлом году посетителей было немного поменьше, будем надеяться на продолжение данной тенденции, но подождем, как говорят спортивные комментаторы, до объявления официальных результатов.

Перейдем непосредственно к впечатлениям от выставки.

Началось всё несколько сумбурно, что, впрочем, очень типично. Организация выставки была, как обычно, на всех выставках далека от идеала, но всё же на достаточном уровне.

По составу посетителей, да и участников, можно было заметить, что “Охрана и Безопасность” по-прежнему остается в первую очередь региональной выставкой, но при этом достаточно весомой. И это совсем не так плохо, как почему-то

у нас считают. По каким-то причинам региональные выставки часто недооценивают, считая достойными своего внимания исключительно крупнейшие. Но в регионах есть свои, и при этом очень значительные плюсы. Множество вполне достойных, хотя и небольших компаний могут показать свои новейшие разработки, представить услуги и при этом надеяться на всеобщее внимание, в том числе и столичных посетителей. Крупные московские компании могут более агрессивно выходить на региональные рынки как напрямую, так и с помощью своих местных партнеров.

Так на выставке “Охрана и Безопасность” многие крупные компании из других регионов (в основном из Москвы) напрямую не выставлялись, а работали на стендах своих представителей или, что чаще, своих партнеров.

Можно отметить и некоторые новинки, которые были анонсированы на выставке. Об их технических и потребительских свойствах мы говорить не будем - рынок рассудит. Так компания “ЭВС” из Санкт-Петербурга анонсировала свои мегапиксельные камеры (первые российские мегапиксельные телекамеры на нашем рынке). Стоит отметить их очень неординарный подход при разработке. Наш журнал собирается познакомить читателей с этими телекамерами в одном из ближайших номеров. Компания “ВИПАКС” из Перми представила свой продукт - цифровой видеорегистратор Domination, который вызвал столько споров. Необходимо отметить нестандартный подход к рекламной компании этого продукта: дерзкий и новый. Организаторам этой рекламной компании удалось охватить почти 100% мужского контингента выставки. За женскую половину сказать не можем, так как главный упор был сделан на размещении рекламных модулей в туалетах. На уровне глаз были расклеены плакаты, и волей-неволей все были вынуждены их прочесть. Мы далеки от того, чтобы разделять возмущенные, если не сказать завистливые, замечания относительно данной акции. Главная цель рекламной компании была достигнута, при этом грамотный подход не позволил ассоциировать продукт с местом размещения. Нам же со своей стороны остается только порадо-



Компания “СпецЛаб” была представлена на стенде их партнеров в данном регионе компании ALL SYSTEMS.

ваться, что хоть кто-то на нашем рынке безопасности сумел сделать что-то оригинальное и работающее в области маркетинга. О самом цифровом видеорегистраторе Domination вы также сможете прочитать в этом номере.

Определенный интерес вызвала и 21-мегапиксельная телекамера SentryScore, зарубежная новинка, представленная на нашем рынке компанией "СТА плюс". Подробнее о принципах работы этой телекамеры вы также сможете прочитать в этом номере журнала.

Компания "Пентакон" (бывшая "Росси-СП") представила последнее обновление VideoNet 8. ITV продемонстрировала систему распознавания лиц и систему контроля банкоматов.

Кроме этих новинок, выставка воспринималась бы посетителями как достаточно заурядное событие, если бы не один факт. Самым любопытным, помимо новинок, оказалось то, что трудно было найти стенды средней руки. Бросались в глаза стенды-гиганты и скромные, но самодостаточные стенды. Впрочем, среди остальных особенно выделялся стенд компании "ЛУИС+". Это то, что называется "СТЕНД" с большой буквы. Он действительно выделялся своими размерами и к тому же был двухэтажным. Также привлекательно смотрелись стенды компаний "Пентакон", "Равелин", "АРМО-Петербург" и еще нескольких других. А, в общем, все было, как обычно. Ничего нового с точки зрения привлечения клиентов - испытанный набор инструментов: девушки (иногда спящие, а иногда откровенно не понимающие, что же они рекламируют), каталоги, буклеты и различная полиграфическая продукция.

Отметим некоторые, на наш взгляд, недостатки. Выставка была неудачно разделена на три равных части. Каждая часть представляла собой отдельное здание, соединенное исключительно маленьким переходом. Неудивительно, что на третью часть внимания у посетителей уже фактически не оставалось. Причем вход в зал номер 1 находился дальше всего. Охрана, видимо, по распоряжению руководства выставки начала ограничивать выход посетителей через зал №1, искусственно выдавливая посетителей в зал №2 и №3. Да, что ни говори, по этому показателю, конечно, что MIPS с СК "Олимпийский", что "Охрана и Безопасность" с ЛенЭкспо уступают форуму Технологии Безопасности в экспоцентре "Крокус".

Вручение наград было намечено на самый конец выставки, и никто, конечно, не смог оценить по достоинству награжденных. Тем более что посетителей уже почти не было, а многие компании были больше заняты сборами.

Но плюсы тоже были. Вполне достойная организация, хоть и не высшего уровня. Растущее количество посетите-

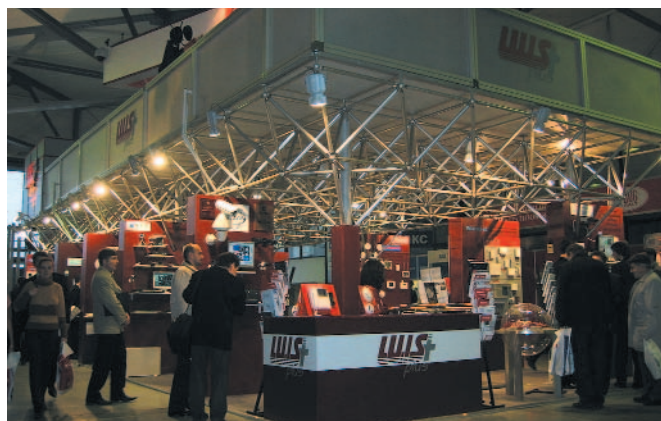
лей. Заметный рост общего бюджета компаний на выставочную и маркетинговую деятельность. Первые ростки свежих идей на рынке безопасности в области маркетинга. Рост общего уровня всех компаний.



Наши коллеги: журнал "Скрытая камера" ("Тинко-печать"), издательство "Все о вашей безопасности", журнал "Системы безопасности" издательства "ГРОТЕК". Наши петербургские коллеги: журналы "БДИ" и "Алгоритм безопасности".



Стенды-гиганты. Корпорация "Пентакон" и компания "ЛУИС+" поразили всех своими внушительными стендами.



Самый яркий стенд на выставке у компании ИТВ.



Наш партнер компания "ГРОСС-ЭЛЕКТРО". Скромно, но со вкусом.



Стенд компании ISS был оформлен в стиле их системы распознавания лиц.



Наш сосед по выставке - компания Ultra Star.



Компания "ВИПАКС" - самая оригинальная компания выставки.

Выставка "Охрана. Спасение. Безопасность" в иркутском "Сибэкспоцентре"



19-21 октября 2004 г. в Иркутском Международном выставочном комплексе "Сибэкспоцентр" были представлены системы охранно-пожарной сигнализации, системы охранного телевидения и наблюдения, системы ограничения и контроля доступа, досмотровое оборудование, специальный транспорт, средства обеспечения безопасности на транспорте, а также системы связи и оповещения.

Разделы выставки:

- Аварийно-спасательное оборудование и экипировка;
- Пожаро- и взрывобезопасность;
- Криминалистическая техника вооружения и тыловое обеспечение;
- Охранная и охранно-пожарная сигнализация;
- Системы охранного телевидения и наблюдения;
- Информационная безопасность;
- Системы связи и оповещения;
- Системы ограничения и контроля доступа, досмотровое оборудование;
- Специальный транспорт, безопасность на транспорте;
- Охрана здоровья, средства первой медицинской помощи;
- Подготовка кадров, учебные материалы, специализированные издания;
- Средства индивидуальной защиты, снаряжение, рабочая и форменная одежда;
- Охрана труда, социально-правовая защита;
- Страхование;
- Охранные услуги;
- Услуги и средства поддержки и обслуживания систем безопасности;

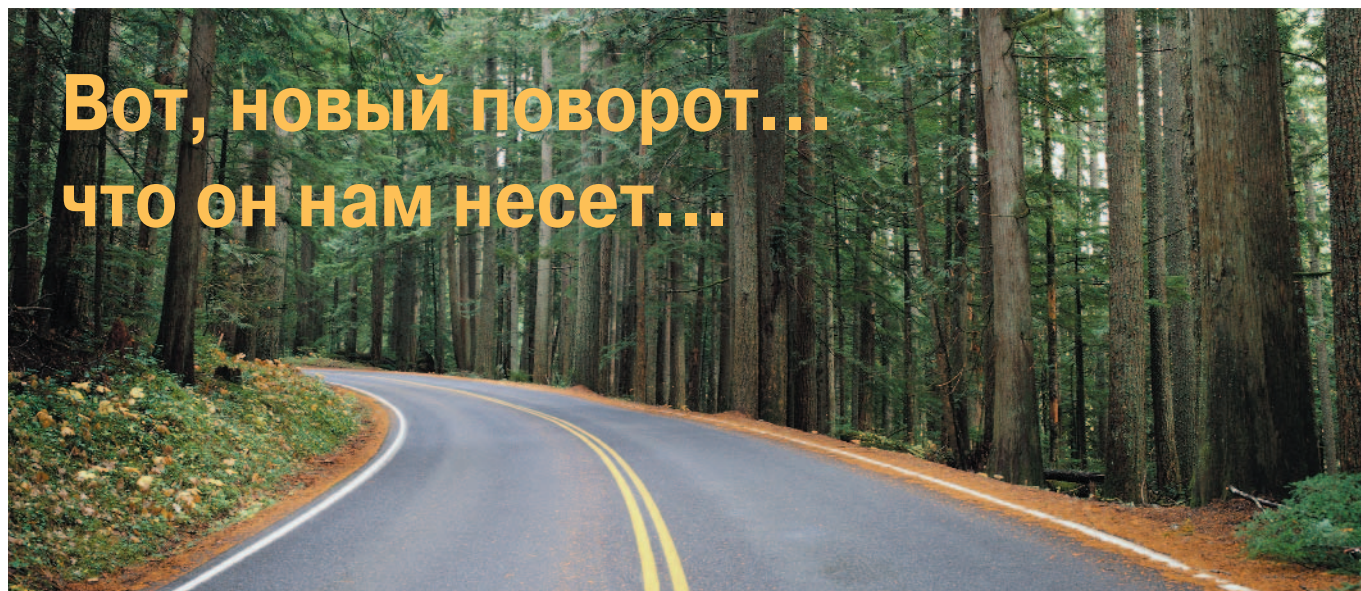
Радиационная и химическая безопасность;

Автоматизированные комплексы системы жизнеобеспечения и безопасности зданий.

Сибэкспоцентр - пожалуй, самый известный выставочный комплекс в Сибири, выставки проводятся в нем практически каждую неделю, и организаторы знают свое дело очень хорошо. Хотя многие участники жаловались все же о недостаточном интересе посетителей к выставке, что многие склонны объяснять недостаточной рекламой мероприятия в СМИ. По словам участников и гостей, данная выставка является наиболее крупной как по количеству экспозиций, так и посетителей в Сибири. Из трех основных павильонов выставочного комплекса под выставку "Охрана. Спасение. Безопасность" было выделено два.

Изюминкой выставки стала экспозиция группы компаний ЕВРААС, которая арендовала целый павильон в рамках выставки. Хочется отметить, что вся экспозиция одного павильона практически напоминала экспозицию всех остальных участников, разбросанных по второму павильону. Среди систем видеонаблюдения были представлены системы "Интеллект" (ITV), "АвтоИнспектор" (ISS), цифровые видеорегистраторы "Dalmeier". На стендах остальных участников выставки были представлены как традиционные системы на мультимедиа, так и завоевывающие российский рынок цифровые видеорегистраторы от корейских и китайских производителей, из цифровых систем в основном демонстрировались системы "Интеллект" и "Видео7" производства московской компании ITV, которая выступила генеральным спонсором выставки "Охрана. Спасение. Безопасность".





Вот, новый поворот... что он нам несет...

Наступает новый 2005 год. Неизвестно, как он сложится для каждого из нас, но уже сейчас можно с относительной уверенностью предположить те направления, по которым будет развиваться рынок CCTV, и где мы с вами увидим увлекательное представление, состоящее из отдельных акций и глобальных стратегий.

Но давайте вначале вспомним уходящий 2004 год. Чем же он нам запомнился?

По моему личному мнению, период 2003-2004 года был тем, который определил направление движения на ближайшие лет 5. Уже заложен фундамент. Еще начиная с 2000 года можно было наблюдать значительный рост объемов как производства, так и, соответственно, продаж. И пока места было достаточно для всех. Наши компании живут в условиях значительного роста внутреннего рынка и растущего спроса на российские товары из области CCTV за рубежом. Не секрет, что многие компании, я говорю сейчас о разработчиках и в меньшей степени о производителях, значительную часть доходов получают от экспорта. И пока, по всем прогнозам замедление роста рынка не предвидится.

Признаюсь честно, очень любопытно наблюдать за развитием этого рынка. Чувствуешь себя современником некоего таинственного развития чего-то, что в будущем, искренне верю, станет серьезным, с чем будут считаться. Интересно наблюдать становление этого малыша-переростка, гидроцефала со слабенькими ножками, у которого много самолюбия и при этом слишком недоразвитый организм. Он понимает, что у него зна-

чительное будущее, и даже сейчас о нем уже все больше и больше говорят. Но ему не хватает витаминов для полноценной деятельности.

Интересно наблюдать уже потому, что он развивается по своим, одновременно и понятным и загадочным законам. За этот год мы видели очень много интересного. Расколы отдельных компаний и последовавшие за этим войны, обиды и месть. Причем это неожиданно приобрело массовый характер. Как какой-то вирус. И наше издательство не стало исключением из этой массовой эпидемии. Что же можно еще отметить? Усиление конкуренции во всех областях, включая выставочные компании. Попытка впервые более или менее независимо измерить рынок... к сожалению, бесплодная. Препятствие отказываться (хотя бы для вида, большего и не требуется) от серости. Неприятие множества хороших идей. Проснувшийся интерес крупнейших зарубежных компаний к российскому рынку и многое другое.

Но главное, что мне хотелось бы отметить - это факт отсутствия на российском рынке CCTV компании, так скажем, с большой буквы. Великой компании, пусть и маленькой сейчас, но с большим будущим. Не видно компаний с амбициозными, значительными целями, которые практически невыполнимы. И если в области разработки программного обеспечения у нас еще намечается какой-то прогресс, и на своей территории российские разработчики заставляют неприятеля считаться с собой, то в области производства какого-либо оборудования мы несем всё новые и новые непоправимые потери. И мне

кажется это показательным. Просто посмотрите на Индию, и поймете, кто в конце концов выигрывает при таком развитии событий.

Сектор CCTV - сильно зависимый сектор от общего развития экономики страны. Он не может быть ни локомотивом, ни лидером - так как не может в принципе создать добавленную стоимость для продукта или услуги компании-потребителя в процессе своего использования. Это услуга, которая всегда будет включаться только в расходы. Но для многих компаний это необходимая услуга, и по мере появления свободных средств компании будут ограниченно вкладывать их в улучшения инфраструктуры безопасности. Многие поспорят, что, хотя этот рынок и не создает добавленной стоимости, говорить так не совсем корректно. Любая компания, принимающая решение об инвестировании в новые технологии, руководствуется исключительно соображениями экономической целесообразности, а именно сокращением издержек на поддержание безопасности. Но выходит, как и принято у нас в стиле "хотели как лучше, а получилось как всегда". А зависимость заключается в том, что компании обращают внимание на продукцию этого рынка пропорционально количеству свободных средств.

Относительно следующего года можно прогнозировать два наиболее вероятных сценария развития ситуации в секторе CCTV исходя из общей макроэкономической ситуации в стране.

Первый сценарий является оптимистическим сценарием развития всего рынка информационных технологий в

России, который основывается на предположении, что основные макроэкономические показатели (уровень инфляции, рост реальных доходов населения, положительное сальдо внешнеэкономической деятельности, уровень поступлений валютной выручки, инвестиции предприятий) увеличатся, либо останутся на прежнем уровне, а это более чем вероятно, так как на протяжении последних лет наблюдается замедление роста российской экономики, несмотря на небывалый уровень мировых цен на энергоносители и сырьевые материалы (основная статья российского экспорта).

Соответственно, стоит ожидать роста благосостояния всех экономических единиц, начиная от крупных компаний до отдельных граждан. В связи с увеличением свободных средств компании начнут вкладывать их в улучшение своей инфраструктуры. Выбор, естественно, будет отдаваться более современным и более дорогим продуктам во всех областях, в том числе и в CCTV. В выигрыше останутся компании, производящие продукты верхнего и среднего ценовых сегментов. Такая парадоксальная ситуация вполне возможна. Будут выбрасываться на рынок обновленные модели продуктов, технически не отличающиеся от своих предшественников, и чьей главной задачей будет увеличение маржи прибыли. Компании нижесреднего и нижнего ценового сегментов, стесненные сверху ограничением спроса, будут искусственно выдавливаться в массовый рынок. И если это произойдет, то мы станем свидетелями ни много ни мало революции в CCTV. Что будет потом,

когда компании побогаче осознают преимущества массового рынка - это уже 2006 год.

Также представляется интересным, как будут развиваться события в области финансирования и инвестирования рынка. Рано или поздно рынок столкнется с нехваткой инвестиций в область новых разработок. Нельзя отрицать тот факт, что наши специалисты способны разработать, да и уже разработали, достаточно конкурентоспособные продукты. Пока это строилось по большому счету исключительно на энтузиазме самих разработчиков, что свойственно молодому рынку. Но рынок зреет, а вместе с ним становятся более "жадными" и все участники этого рынка. Тем более этот рынок постоянно растет.

Зарубежные компании решают эти проблемы различными способами: проводят слияния между собой, поглощают другие компании, создают вертикально интегрированные холдинги (если их можно так назвать), заключают партнерские договоры, привлекают заемные средства, банковские кредиты и т.п. Но возможно ли всё это в России? Это по-прежнему остается вопросом без ответа. Последние события на нашем рынке говорят скорее об обратной тенденции. Пока у нас научились только прятать и молчать. Но "отнимать" от себя и вкладывать как-то не хотят.

Второй (и, кстати, менее вероятный) вариант развития событий связан со снижением экспортных поступлений от продажи сырья и, соответственно, со спадом макроэкономических показателей. Сектор CCTV как

зависимый элемент сферы услуг должен будет защищаться. Какие меры будут разрабатывать компании для сокращения издержек и возможности выстоять в конкурентной борьбе - это вопрос сугубо индивидуальный, так как компании, наверное, сами еще об этом не задумывались. Могу предположить, что многие компании-разработчики программного обеспечения сейчас чувствуют себя как за каменной стеной, дескать, это уж точно не про нас, а у нас всегда всё будет в порядке. Но уже сейчас можно наблюдать осязаемое усиление конкуренции, связанное с ростом количества участников-продавцов. А с сокращением спроса конкуренция неизбежно только усилится, и это, уверен, будет "неожиданностью" для многих, как наступление зимы в декабре для наших коммунальных служб. Все начнут сбивать цены на свою продукцию, и, естественно, пострадают представители низшего и среднего ценового сегмента, так как лимит для маневра у них более ограничен. Возможно ожидать сокращение штата сотрудников, как самого затратного элемента работы компаний, ограничение маркетинговых затрат и другие широко известные методы. Рассчитывать на другие, более оригинальные меры противодействия неудачному стечению обстоятельств не приходится.

В случае исполнения данного прогноза многие компании столкнутся не только с определенными финансовыми проблемами, но и трудностями, так сказать, психологического характера. После головокружительного роста многие компании переступят невидимую черту, за которой замедление приравнивается к остановке. А аппетит уже нагулял, и он, как известно, приходит во время еды. Многие компании и их руководители средней руки искренне хотят видеть себя сильными, успешными и в чем-то великими, но при этом не имеют ясной стратегии хотя бы на трехлетнюю перспективу. Многие сдадутся, другие будут бесплодно ожидать второго дыхания. Но вместо того, чтобы предпринять какие-либо шаги в этом направлении, менеджмент предпочитает оставаться в плену иллюзий, ожидая повторения стремительного роста.

Для многих российских компаний показательным примером компании A4Vision. Созданная двумя студентами и основанная на одном изобретении эта



компания сумела не только выжить, но и, набрав обороты, занять лидирующие позиции. Если кому-то не известно, то напомним, что сейчас эта компания базируется в США, хотя и считается российской. За 2003 год оборот этой очень молодой компании составил около \$1 млн. Полтора месяца назад контрольный пакет A4vision за \$8,5 млн. купил один из старейших венчурных фондов Силиконовой долины Menlo Ventures. Еще \$4,3 млн вложил консорциум под началом Menlo. А в конце октября совладельцем A4Vision стал Лари Эллисон, если кому-то неизвестно, то это президент и генеральный директор крупнейшего в мире разработчика корпоративного программного обеспечения Oracle. Как заявляет один отцов-основателей A4vision Артем Юхин, основная часть привлеченных денег компания вложит в работу над дальнейшими разработками. И можно быть в этом уверенным, так как участие венчурных фондов выступает гарантом правильного применения средств.

Очень хотелось бы отметить не только, так скажем, "раскрученность" работы вышеописанной компании, но и, по моему мнению, их грамотность в долгосрочной перспективе.

Любая компания в сфере что биотехнологий, что систем видеонаблюдения стремится получить глобаль-

ные заказы, будь они государственные или нет. У мелких компаний в индустрии безопасности почти нет шансов пробиться на самый верх. Глобальные заказы подразумевают и глобальных исполнителей.

Немного отвлечемся. Как правило, в сфере CCTV, по крайней мере в области разработки программного обеспечения, главный разработчик основного продукта является или полным владельцем, либо совладельцем значительной доли. Рынок CCTV - это не рынок отдельных частных пекарен, и быть маленьким здесь грозит полным исчезновением как самостоятельной единицы. И здесь работает, и в России скоро начнет работать, закон поглощения маленьких рыбешек крупными акулами. Поэтому наращивание капитализации, если такой термин вполне применим по отношению к российским компаниям, по моему мнению, является самой приоритетной задачей. Большую компанию можно и дороже продать. А продавать, возможно, придется уже в ближайшем будущем. Зарубежному капиталу или своим - это не столь важно. А тот, кто успеет стать больше и богаче к началу периода поглощений, будет сам поглощать, так как маленькое не может вместить большое.

Вывод компании, которая считается вроде бы российской, за рубеж кажется очень хорошей идеей с нескольких точек зрения. Во-первых, это позволяет более плодотворно находить источники финансирования. А во-вторых, для управления компанией ставятся люди, которые не "измучены российскими минеральными водами". Компания не подвержена российским политическим и экономическим рискам, но при этом может плодотворно оперировать и в России.

И в заключение мы приберегли относительно хорошие новости для вас. По сообщениям некоторых СМИ, 18 ноября правительство РФ поддержало и в целом одобрило общую концепцию развития рынка информационных технологий в

России на период до 2010 года. Но какие выгоды это может нести непосредственно для нашего многострадального сектора. Судите сами - поддержку нашли очень смелые решения, даже такие, как отмена таможенных пошлин на ввоз комплектующих для ПК, сокращение налогов на сектор информационных технологий и упрощение процедур экспорта программ. Вполне возможно, что эти меры начнут действовать уже с середины 2005 года. Если эти меры будут действительно введены, то выгоду при правильном подходе можно извлечь очень значительную.

По отчетам и оценкам влиятельной исследовательской международной компании IDC, с 2000 по 2003 год российский рынок IT вырос почти в два раза - до \$ 7.1 млрд. Объем рынка информационных технологий в России составляет всего 1,4% ВВП, тогда как, например, в США - 5%. На экспорт идет всего 14% российской IT-продукции - это намного меньше, чем в Израиле (70%) и Индии (80%). Определить тот процент, который занимает всё, что так или иначе связано с сектором CCTV, очень трудно. Можно, конечно, предположить, что он составляет около 0,05%, но и это может оказаться преувеличением.

Выше описанная концепция была разработана самим ведомством под руководством Леонида Реймана (министерство информационных технологий и связи) с участием компании McKinsey.

Особо интересны предложения министерства связанные со снижением фискального бремени на участников рынка. В частности, планируется упразднить таможенные пошлины на ввоз комплектующих для компьютеров, упростить процедуру таможенного оформления программ, идущих на экспорт, снизить ставку единого социального налога на IT-предприятия, себестоимость продукции которых более чем на 50% определяется затратами на оплату сотрудников.

Расходы самого государства и участников рынка на воплощение концепции составят около 10 млрд. рублей. При этом и отдача должна быть очень впечатляющей: в результате всех предусмотренных мер объемом российского рынка IT-рынка должен возрасти к 2010 году более чем в пять раз - до \$40 млрд.





Еще раз обращаясь к теме подведения итогов уходящего года, редакция журнала решила предоставить слово непосредственно тем компаниям, за успехами и неудачами которых мы следили с замирающим сердцем в течение всего года.

Компаниям был предложен ряд вопросов:

1. Как сложился год для вашей компании?
2. С какими трудностями столкнулась ваша компания в уходящем году?
3. Каких успехов в области охранного телевидения добилась ваша компания?
4. Какое событие в области охранного телевидения вы могли бы выделить в уходящем году?
5. Как, по вашему мнению, будет развиваться рынок охранного телевидения в следующем году и ваша компания?

Технический Директор "Сатро-Паладин" Сизов Алексей Юрьевич:

1. Этот год был достаточно удачным и успешным. В этом году нашей компании исполнилось 10 лет, компания продолжила свой рост и развитие благодаря комплексному подходу в обслуживании своих клиентов.

2. Основные трудности, если их так можно назвать - недобросовестная конкуренция и "черный PR". Это говорит о том, что нашу компанию уважают и боятся как сильного конкурента.

3. Основным успехом можно назвать то, что компания является одним из крупнейших поставщиков на российский рынок оборудования охранного телевидения. В ассортимент компании входят все востребованные рынком и самые популярные модели как видеосекьюрити, так и устройств обработки и видеорегистрации.

4. Стремительный рост цифровых технологий как в области обработки и записи информации, так и в области передачи данных.

5. Рынок продолжит свой рост и развитие. Цифровые технологии будут играть все большую роль на рынке. Также должен продолжиться рост в сетевых технологиях передачи видеосигнала.

Компания "Сатро-Паладин" поздравляет всех, кто так или иначе связан с рынком систем безопасности, с наступающим Новым Годом, в особенности, своих клиентов и партнеров! Хотелось бы пожелать всем стабильности, благополучия и счастья! Пусть Новый 2005 Год будет безопаснее, спокойнее и радостнее для всех!

Руководитель отдела маркетинга рекламы группы компаний "Роникс Стандарт" Горбункова Евгения:

1. Для группы компаний "Роникс", куда входят торговая компания "Роникс Стандарт" и монтажная компания "Роникс Секьюрити", 2004 год может быть охарактеризован как научно-плодотворный и экономически-успешный.

2. Основной проблемой, возникающей у поставщиков импортного оборудо-

ования, к которым относится компания "Роникс Стандарт", является падение курса доллара США к основным мировым валютам.

В настоящее время одной из приоритетных целей нашей компании является продвижение на российский рынок оборудование фирм Ikegami Tsushinki, Sunell, AvTech и антитеррористического видеоконтекста "SaveVision", реализованного на базе уникальных технологий компании "MegaPixel". Отличительной особенностью предложенных решений, являются нейроразличительные алгоритмы, а именно: высокоизбирательная помехоустойчивая детекция движения, Slow Down Detection - детектор оставленных/исчезнувших предметов, Slow Speed Filter - фильтр медленных скоростей. Система предназначена для решения задач наблюдения, охраны, регистрации и контроля доступа.

3. По итогам участия в международной конференции "Интерполитех 2004" компания "Роникс Стандарт" была награждена золотой медалью и дипломом "Гарантия качества и безопасности" за разработку и внедрение в МВД и

ФСБ России новых высокоэффективных технических средств для антитеррористической деятельности.

Решением общественного экспертного Совета смотров "Лучшие в России", "Лучшие в Москве" Российского Фонда Защиты Прав Потребителей России ООО "Роникс Секьюрити" награждено Дипломом за активное участие в формировании цивилизованного потребительского рынка в России.

4. На российском рынке появился антитеррористический видеокomплекс "SaveVision II", осуществляющий обработку видеоинформации в режиме "реального времени" (25 к/с на канал).

Появление на рынке IP-камер шведской компании AXIS и RAID-массивов различных компаний, т.к. в настоящее время необходимо оптимизировать большой объем видеоинформации.

5. Мировой рынок цифровых систем стремительно развивается, при этом качество оборудования улучшается, а цена не изменяется или становится меньше. Что касается России и СНГ, то прослеживается динамика перехода на цифровые записывающие устройства.

В тоже время в Северной Америке и Европе динамика развития направлена на переход телевидения с аналогового на цифровое.

Коллегам по бизнесу искренне желаем удачи, финансового благополучия и достижения намеченных целей.

Александр Пыпин. Руководитель отдела маркетинга G2Technology:

1. 2004 год стал одним из самых результативных в работе компании. Динамично развивались связи с региональными партнерами, открылись филиалы в Санкт-Петербурге и Ростове-на-Дону, переехал в более просторный офис украинский филиал.

Было выделено в отдельное подразделение направление по проектированию сложных систем безопасности. В нем теперь слаженно работают известные на рынке эксперты. Компания начала подготовку к выводу на рынок нового мощного программного продукта для систем предотвращения потерь. Развивались связи с иностранными поставщиками. На заводе HITRON было налажено производство новых моделей видеокамер под маркой G2Technology.

2. Как и другие компании самостоя-

тельно импортирующие оборудование из-за рубежа мы ощутили трудности в этой сфере, особенно на стадиях замены и ремонта оборудования.

3. Были реализованы крупные проекты на АЗС Лукойл и ВР, в торговых сетях Копейка, Рамстор, Перекресток, Лента. Один из сложнейших проектов был реализован в Перми - оборудование комплексной системой безопасности крупнейшего в регионе торгового объекта. Были установлены: система видеонаблюдения на более 80 видеокамер, система контроля кассиров на 32 кассы, система контроля доступа.

Наибольшее влияние в течение года на рост рынка охранного телевидения оказали террористические акты - многие компании и учреждения, ранее не задумывавшиеся об установке таких систем, стали обращаться с запросами. Во многих городах были приняты, а в ряде из них уже реализуются, программы по массовой установке систем в жилых домах, на транспорте, в учебных заведениях и больницах, на опасных производствах.

4. В следующем году динамично будет развиваться рынок массовой установки систем в местах проживания и досуга людей. Наша компания будет сохранять специализацию на установке систем видеонаблюдения и предотвращения потерь в местах досуга и работы людей - торговых предприятиях и развлекательных заведениях, офисах. Но главным событием станет выпуск на рынок интегрированного программно-го решения для управления сложными системами безопасности и системами предотвращения потерь.

Компания G2Technology поздравляет участников рынка безопасности с Новым Годом и желает им хорошо отдохнуть. До встреч в 2005 году.

Вадим Насыров, начальник отдела развития ЗАО "Терна-СБ":

1. В начале 2004 года руководством "Терна СБ" было принято решение максимальное усилие приложить к увеличению доли дистрибуции в компании. И уже сегодня можно сказать что в этом направлении были достигнуты серьезные успехи. Однако это не означает, что компания перестала уделять внимание проектному бизнесу. В уходящем году компания "Терна СБ" успешно реализовала ряд

крупных проектов. В целом, уходящий год сложился удачно и можно говорить о том, что компания вышла на новый уровень развития.

2. Если говорить о трудностях, то они были связаны в основном с рабочими моментами. Достаточно серьезная проблема, я думаю, для всех компаний - это отсутствие учреждения, которое готовило бы специалистов в области систем безопасности в общем и охранного телевидения в частности.

3. Как уже говорилось выше, "Терна СБ" посвятила этот год развитию дистрибуции в компании. И в итоге заняла достойное место в одном ряду с крупнейшими поставщиками оборудования на российском рынке. Также успехом можно назвать налаженные в уходящем году связи с крупными мировыми производителями оборудования охранного телевидения.

4. В уходящем году наблюдалось некоторое перераспределение рынка систем охранного телевидения между компаниями, работающими на этом рынке. Думаю, что сильно выросло количество монтажных организаций. Также показательным является появление специальных маркетинговых агентств. Это говорит о том, что рынок систем безопасности переходит в более зрелую стадию.

5. Однозначно рынок охранного телевидения в 2005 году будет расти. Думаю, все больше частных пользователей установят себе систему охранного наблюдения. А это приведет к увеличению доли дешевого азиатского оборудования на российском рынке. Однако и объем продаж оборудования известных брендов будет расти. Особенно в рамках антитеррористических мероприятий.

Коллектив компании "Терна СБ" сердечно поздравляет всех своих коллег по бизнесу с наступающим Новым Годом. Желаем всем добиться значительных успехов в следующем году, а также обеспечить растущий все еще молодой российский рынок охранного наблюдения лучшими отечественными и мировыми решениями.

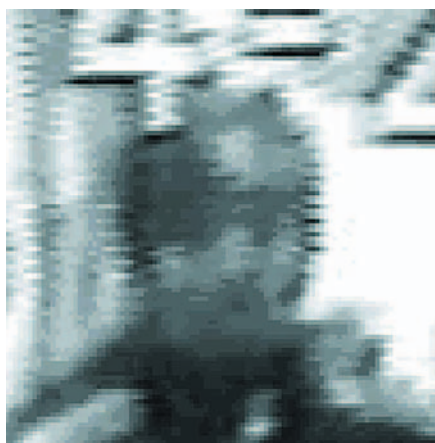
Редакция журнала искренне благодарит всех откликнувшихся участников опроса.

SentryScope - первая в мире система видеонаблюдения с разрешением до 21 мегапиксела

Очень интересную телекамеру представила компания Spectrum San Diego Inc. В этой новинке используется матрица ПЗС от Dalsa с технологией строчного сканирования (line scan) для получения черно-белых изображений с разрешением до 21 мегапиксела, что позволяет распознавать лица и автомобильные номера на больших расстояниях.

Вступление

Наверняка многие сталкивались с такой проблемой: случилось происшествие и требуется просмотреть его запись. Служба безопасности находит в архиве кадры с записью этого инцидента и увеличивает интересующие области кадра. К сожалению, изображение расплывается настолько, что его невозможно использовать для опознания, как, например, на приведенной фотографии.



Изображение неопознанного грабителя банка, полученное с помощью стандартной телекамеры

Стандартное разрешение кадра, которое используется в современном охранном телевидении, составляет 640x480 пикселей (NTSC). Для того чтобы уверенно распознать лицо человека на такой записи, разрешение кадра должно достигать 40 пикселей на фут (1 фут = 30 см). Разделив 640x480 пикселей на 40 пикселей на фут, мы получим максимальную зону обзора 16x12 футов (4.8x3.6м). Это означает, что запись сможет помочь в раскрытии преступления только в том случае, если телекамера была сфокусирована в правильном направлении на зоне 16x12 футов.

Эта проблема еще более обострилась с появлением цифровых видеорегистраторов (DVR). Для экономии архивного пространства цифровые видеорегистраторы часто записывают

кадры с меньшим разрешением, например, 320x240 пикселей. Если в этом случае нам нужно распознать лица и другие мелкие детали, то зона обзора уменьшается до 8 дюймов в ширину (2.4 м).

Для того чтобы преодолеть ограничения стандартных решений, используемых в охранном телевидении, требуется значительно более высокое разрешение. В этой статье мы расскажем об использовании технологии строчного сканирования, которая позволяет вести видеонаблюдение со сверхвысоким разрешением для большой зоны обзора, которая применяется в системе SentryScope. Также мы рассмотрим потенциальные сферы применения этой технологии в охранном телевидении.

Сегментация в охранном телевидении

Для того чтобы определить, где технология строчного сканирования может быть использована оптимальным образом, необходимо выделить определенные сегменты в сфере охранного телевидения. В целом, существует три рода операций видеонаблюдения:

1) В первом случае система видеонаблюдения полностью укомплектована персоналом. Операторы отслеживают ситуацию на мониторах. Если используются поворотные телекамеры, то ими управляют операторы. В случае происшествия персонал может быть немедленно отправлен на место этого происшествия. Таким образом обеспечивается очень высокий уровень безопасности, но это требует значительного количества персонала.

2) Во втором случае система видеонаблюдения укомплектована персоналом частично, который не проводит все свое время за мониторами. Например, может оказаться слишком много телекамер, персонал может также быть занят на патрульной службе, наблюдение за телекамерами может вестись только в определенные часы и т.д.

От внимания операторов сразу ускользают многие происшествия, которые обнаруживаются только позже. Архивные записи часто непригодны при расследовании этих происшествий, так как телекамеры не были правильно позиционированы.

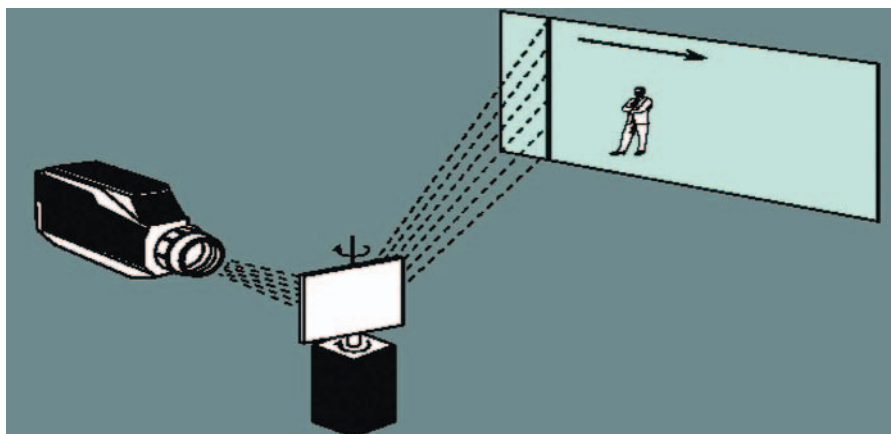
3) В третьем случае система видеонаблюдения работает в автономном режиме, и ведется постоянная запись с последующим просмотром подозрительных эпизодов. Эта альтернатива требует наименьшего количества людей, но поворотные телекамеры не используются, так как некому ими управлять.

Современные решения в охранном телевидении подходят для первого случая, когда система видеонаблюдения полностью укомплектована персоналом. Разрешение телекамеры не является критичным, так как за мониторами постоянно следят, и в случае необходимости персонал может оперативно среагировать. Но ограничения современных решений в охранном телевидении становятся очевидны, как только персонал перестает следить за мониторами или невозможно выслать людей на место происшествия.

Разрешение телекамеры становится очень важным фактором для второго и третьего случая, когда система видеонаблюдения укомплектована персоналом лишь частично или работает в автономном режиме, а для расследования происшествий используются архивные записи. На этих записях необходимо идентифицировать лица людей, небольшие предметы, например, оружие или автомобильные номера, а также подозрительную деятельность.

Сверхвысокое разрешение с технологией строчного сканирования

Камеры с технологией строчного сканирования уже давно используются в сферах не связанных с охраным телевидением. Для создания изображений движущихся объектов в техноло-



Вращающееся зеркало проецирует сканирующую линейку по всей зоне обзора телекамеры

Компромиссы

Для первого из рассмотренных нами случаев с большим количеством персонала цвет зачастую считается очень критичным, тогда как в двух других случаях, для которых и предназначены телекамеры SentryScope, разрешение более важно. Обычно цветная телекамера имеет в 3-4 раза меньшее разрешение, чем черно-белая телекамера с таким же количеством пикселей. Для того чтобы получить максимально возможное разрешение, телекамеры SentryScope работают с черно-белым изображением.

Современные телекамеры, используемые в охранном телевидении, фиксируют до 30 кадров в секунду, что при просмотре на мониторе дает "живое" видео. Большинство спецвидеомагнитофонов и цифровых видеорегистраторов позволяют уменьшать скорость записи до 1-4 кадров в секунду для экономии архивного пространства. Поскольку технология строчного сканирования обрабатывает огромное количество пикселей, в телекамерах SentryScope скорость обновления кадров составляет 1 кадр в секунду.

В рамках архитектуры SentryScope скорость обновления кадров ограничивают следующие ключевые элементы:

- 1) Вычислительная мощность и скорость ввода/вывода процессора обработки изображений
- 2) Поворотное устройство с зеркалом, которое используется для скани-

гии строчного сканирования используется не матрица, а только одна сканирующая линейка пикселей. Одной из наиболее распространенных сфер применения камер с технологией строчного сканирования является контроль качества продукции на конвейерных линиях. Камеры с технологией строчного сканирования формируют изображения продуктов с высоким разрешением, что позволяет проводить очень тщательную дефектоскопию. Также эта технология применяется при сортировке писем на почте и в космической фотосъемке.

Чтобы адаптировать технологию строчного сканирования для видеонаблюдения вертикальная сканирующая линейка при формировании изображения должна обходить все поле обзора. На иллюстрации 2 показан один из способов того, как это может быть реализовано.

Поле обзора телекамеры со строчным сканированием проецируется на зеркало, которое установлено на оси с мотором. При вращении зеркала вертикальная сканирующая линейка формирует изображение из множества вертикальных линий.

В телекамере SentryScope от Spectrum San Diego, Inc. используется вертикальная сканирующая линейка, состоящая из 2048 пикселей, на основе ПЗС. Благодаря применению высокоточного оптического устройства сканирующая линейка формирует изображение из 10240 линий (максимально), что в итоге дает разрешение около 21 мегапикселя.

Какое разрешение нужно вам?

Как показано на иллюстрации 3, при 20 пикселях на фут распознавание ли-

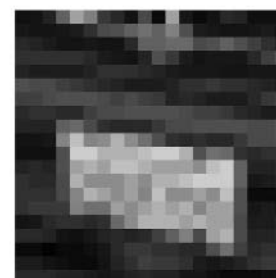
ца невозможно. При 40 пикселях на дюйм узнать лицо человека возможно, но распознавание автомобильных номеров затруднено. При 80 пикселях на дюйм (примерно 2.7 пикселя на сантиметр) лица и более мелкие детали становятся отчетливо различимы.

В качестве примера возьмем крупную стоянку автомашин, для которой необходимо распознавание автомобильных номеров. С помощью телекамеры SentryScope можно фиксировать до 10240 пикселей по горизонтали. Разделив 10240 на 80 пикселей на фут, получим поле обзора в 128 футов (около 40 м) только для одной телекамеры. Вся эта зона будет "прикрыта" одной телекамерой со сверхвысоким разрешением 100% времени. Это позволяет получить детальные записи событий для немедленного просмотра или последующего анализа.

80 pixels/ft.

40 pixels/ft.

20 pixels/ft.



Для распознавания лиц и ключевых деталей требуется 40-80 пикселей на фут (примерно 1.5-3 пикселя на см)

рования вертикальной линейкой поля обзора

3) Скорость передачи данных интерфейса телекамеры и внешних записывающих устройств

4) Вычислительная мощность и скорость ввода/вывода записывающего устройства

В качестве устройства обработки изображений в телекамерах SentryScope используется цифровой сигнальный процессор BlackFin производства Analog Devices. Этот новейший процессор может выполнять 600 миллионов операций в секунду. Сканирующее устройство с зеркалом, специально разработанное Spectrum San Diego, использует усовершенствованное цифровое управление для обеспечения высокоточного позиционирования. В качестве интерфейса между телекамерой и компьютером используется Fast Ethernet со скоростью до 100 мегабит в секунду. Этой скорости вполне достаточно для передачи сжатого видеоизображения сверхвысокого разрешения. И, наконец, для записи используется производительный компьютер с процессором 2 гигагерц и с объемом архива до 480 гигабайт. Все эти компоненты были тщательно отобраны для обеспечения оптимальной производительности при разумной цене. С развитием технологии и неизбежным снижением цен производи-

тельность телекамер SentryScope, вероятно, будет повышаться.

Потенциальный круг потребителей

Недавно появившиеся и, соответственно, более дорогие технологии обычно находят сбыт среди так называемых ранних последователей (люди, воспринимающие новинки быстро, но с осторожностью). Основная сфера применения телекамер SentryScope включает в себя видеонаблюдение за обширными зонами, за которыми невозможно постоянно вести наблюдение с применением существующих телекамер, и куда нельзя оперативно отправить людей в случае происшествия.

При скорости обновления кадров 1 к/с оперативное видеонаблюдение, возможно, не будет основной сферой применения этого продукта, но в двух рассмотренных нами случаях, когда система видеонаблюдения укомплектована персоналом частично или работает в автономном режиме, то есть когда обращение к архивным записям носит регулярный характер, применение будет вполне оправданно.

Ранние последователи этой технологии, скорее всего, будут из тех сфер деятельности, в которых нераскрытое преступление или террористический

акт могут оказаться катастрофическими по своим последствиям. Например:

Местные и федеральные органы власти
Аэропорты
Транспортные терминалы
Системы жизнеобеспечения
Порты и гавани
Развлекательные центры (стадионы, аттракционы, спорткомплексы)
Местные и федеральные органы охраны правопорядка
Автостоянки

Телекамеры могут быть расположены на самой автостоянке, по периметру, у входа или выхода или в любом другом месте, где требуется 100% покрытие зоны со сверхвысоким разрешением.

Впрочем, телекамеры SentryScope можно успешно использовать и там, где сейчас используются стандартные телекамеры. Некоторые "уязвимые" зоны, где традиционно высок риск, могут потребовать дополнительной защиты, а телекамеры SentryScope будут удачным дополнением к уже существующим системам видеонаблюдения. В этом случае можно взять лучшее от двух технологий: высокую скорость обновления кадров и цветное изображение от стандартной технологии и сверхвы-





SentryScope позволяет вести наблюдение за обширными зонами со сверхвысоким разрешением и увеличивать мелкие объекты

сокое разрешение для покрытия зон повышенного риска при низкой скорости обновления кадров от технологии строчного сканирования.

Что мы получим в результате?

Что оператор системы видеонаблюдения ожидает получить от телекамеры SentryScope? При просмотре архивных записей сверхвысокое разрешение позволяет увеличивать объекты, как это показано на иллюстрации 4. Можно будет отчетливо распознать лица и автомобильные номера. Традиционные телекамеры, используемые в охранном телевидении, покажут всего лишь то, что кто-то оказался в кадре. Телекамера SentryScope позволит идентифицировать человека и доказать это в суде.

Заключение

Вряд ли существует простой способ, позволяющий провести сравнение в ценовом отношении обычной телекамеры и SentryScope, так как при построении системы видеонаблюдения приходится учитывать слишком большое количество факторов. Но вполне справедливо будет сказать, что SentryScope может заменить более одной обычной поворотной телекамеры, управляемой человеком. Если же людей не хватает, чтобы следить за всеми телекамерами или система видеонаблюдения работает в автономном режиме, SentryScope может заменить несколько обычных телекамер без поворотного устройства.

Если перед вами стоит выбор использовать или не использовать SentryScope, то имеет смысл оценить

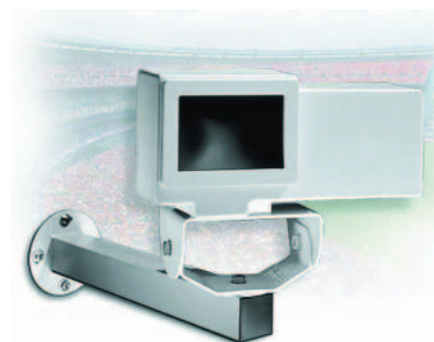
преимущества сверхвысокого разрешения при наблюдении за большими зонами:

Меньшие затраты на установку и эксплуатацию системы видеонаблюдения, так как требуется меньше телекамер.

Повышение производительности труда службы безопасности за счет уменьшения количества мониторов и записей, которые нужно просматривать.

Ускорение анализа и расследования преступлений

Решающим фактором при выборе может оказаться то, что если вам требуется наблюдение за критично важными зонами 100% времени со сверхвысоким разрешением, то возможности SentryScope значительно превосходят в этом обычные телекамеры, используемые в охранном телевидении.



Снимок сделанный с помощью телекамеры SentryScope



**MDW-100
VIP-10
AXIS-241S
AXIS-241Q**

Тестирование сетевых видеосерверов

Сейчас трудно кого-то удивить новинками из сферы высоких технологий. И уже давно не данью моде, а необходимостью, стало внедрение IP-решений во все сферы деятельности человека. Поскольку охранное телевидение также относится к сфере высоких технологий, то и ее не обходит стороной все новое и прогрессивное. Общество уже привыкло к компьютерам. И процессоры, которые считались самыми производительными еще буквально два года назад, уже можно найти разве только в комиссионных магазинах. Но в ПК для систем видеонаблюдения и видеорегистрации не все выполняемые задачи подразумевают работу большого количества приложений. Исходя из этого многие разработчики для оптимизации работы своих систем стараются организовать выполнение только необходимых приложений. Это легче реализовать на операционных системах с открытой архитектурой, когда на ПК установлено ядро операционной системы, необходимые приложения, драйверы и программное обеспечение. Понятно, что не все так просто, и это тема еще не одной статьи. И есть решения, в которых можно обойтись без операционной системы Windows. В большинстве случаев это устройства не на базе архитектуры Intel, то есть поп-PC, среди которых отдельную группу занимают сетевые видеосерверы. В эту группу входят как устройства с модулем для организации архива, так и без него. В свою очередь видеосервер является неотъемлемой составной частью сетевой телекамеры. То есть сетевые телекамеры уже подразумевают наличие встроенного видеосервера.

Что же такое видеосервер? Это устройство или модуль (в составе сетевых

телекамер), который используется в составе аналогово-цифровой системы видеонаблюдения и служит для преобразования аналогового видеосигнала в цифровой формат для последующей трансляции по каналу связи или записи на цифровой носитель.

Сетевые видеосерверы оцифровывают аналоговый видеосигнал и передают цифровое видеоизображение по сети, тем самым превращая обычные аналоговые телекамеры в сетевые.

Основное преимущество сетевых видеосерверов перед менее гибкими аналоговыми системами видеонаблюдения заключается в том, что они позволяют получить удаленный доступ к телекамерам в режиме реального времени, используя для этого локальные сети.

Остановимся на типовых особенностях сетевых видеосерверов.

На видеовходы, или видеовход видеосервера подается аналоговый видеосигнал. Многие видеосерверы работают также и со звуковым каналом. На видеосервер может подаваться как аналоговый аудиосигнал, так и уже оцифрованный на внешних, сопряженных с устройством, аудиомодулях. При этом аудио- и видеоканал могут быть как синхронизированными между собой, так и нет. Многие видеосерверы оборудованы входами для приема сигналов с внешних тревожных датчиков, и тревожными выходами с нормально замкнутыми или нормально разомкнутыми контактами.

Просмотр видеоизображения и управление поворотными телекамерами можно осуществлять с компьютера, подключенного к локальной сети, в стандартном веб-браузере. Тем не менее, многие компании-производители поставляют в комплекте с видеосервером программное обеспечение, кото-

рое служит для удаленного мониторинга, администрирования, управления поворотными телекамерами, а также конфигурирования и перепрограммирования видеосервера с возможностью загрузки новых драйверов и обновления программного обеспечения. Кроме этого, отдельные компании-производители для организации разветвленных сетей видеонаблюдения предлагают дополнительно приобрести как отдельные программы, так и целые программные пакеты.

Перед конфигурированием IP-адреса видеосервера и его предварительной настройкой организуется соединение между видеосервером и ПК администратора. Обычно канал связи устанавливается через интерфейс RS-232, в ряде случаев для этого используется и соединение по локальной сети, при этом достаточно нахождения обоих устройств в одной подсети. В качестве программного обеспечения используются встроенный в операционную систему Windows Hyper Terminal, протокол ARP или дополнительные утилиты.

Во многих видеосерверах организовано управление поворотными телекамерами и PTZ-устройствами, а также периферийными устройствами. Соединения устройств с видеосервером осуществляется через последовательные порты с интерфейсом (RS-232, RS-485, RS-422). Программная поддержка протоколов связи реализована в записанных в долговременную перезаписываемую память видеосервера драйверах.

Подключение видеосервера к локальной сети осуществляется посредством интерфейса 10BaseT/100BaseTX.

В видеосерверах приветствуется наличие встроенного детектора движения, возможность организации архива на локальном ПК, отсылка уведомле-

ний по электронной почте, TCP, HTTP, а также изображений на почтовый ящик, FTP- и HTTP-серверы либо в автоматическом режиме как по расписанию, так и по тревогам, либо вручную по команде оператора. Удобно, если на видеосервере организовано управление по триггерам, программируемым алгоритмам реакций на определенные события. В качестве инициаторов событий выступают как срабатывание по тревожным входам, так и по детектору движения, а также при потере видеосигнала на входе видеосервера и загрузка устройства. И не лишним в видеосервере является наличие буфера памяти, достаточного объема для хранения текущей видеоинформации, предотвращения и посттревожной записи.

Не будем описывать типовой алгоритм работы видеосерверов, используемые алгоритмы сжатия, разрешения, поддерживаемые сетевые протоколы, а плавно перейдем к тестированию выбранных для этого видеосерверов.

MDW-100

В скромной коробке из серого картона с надписями Web Camera и наклейками с краткой информацией о содержимом был упакован сетевой видеосервер. Кроме него, в коробке находились руководство пользователя в бумажном виде, компакт-диск с программным обеспечением и все тем же руководством, но уже в электронном виде и комплект кабелей. Наклейка на коробке информировала о названии упакованного устройства - Intelligent Network Transmitter MDW-100A. Также название модели устройства было написано на нижней части устройства, и из надписи следовало, что перед нами

модель MDW-100 производства компании MC Electronics (Южная Корея).

Сетевой видеосервер MDW-100 выполнен в виде миниатюрного устройства с черным покрытием, тремя информационными индикаторами на лицевой панели и вынесенными на заднюю часть корпуса разъемами. Вес устройства - 300 грамм, размеры - 53х58х110мм. На задней панели сетевого видеосервера расположены вход для подачи питания, стандартный разъем RJ-45, используемый для подключения устройства к сети Ethernet или Fast Ethernet и 8-штырьковый разъем последовательного порта RS-232. Там же расположены аудиовход и аудиовыход. Кроме вышеперечисленного, на заднюю панель видеосервера помещен 6-штырьковый разъем порта GPIO. На него выведены тревожные входы и тревожные выходы, а также композитный видеовход для подачи видеосигнала.

На компакт-диске записано руководство пользователя на английском языке и программное обеспечение. Не будем останавливаться на программном обеспечении для КПК с операционной системой Windows CE. Впрочем, при совместном использовании данного программного обеспечения и КПК (как вариант планшетного КПК) с модулем беспроводной связи пользователь может получить достаточно удобное мобильное рабочее место. Что касается программного обеспечения для ПК, то его установка прошла без осложнений, и в результате мы получили сразу несколько программных модулей: AdminTool 4.41, WebCamViewer 1CH 1.45, WebCamViewer 4CH 1.45 и WebCamPlayer 1.45, назначение которых становится понятным при переводе названий. Рассмотрим каждый из них по отдельности.



Любая система в первую очередь требует настройки и конфигурации, и именно в этом заключается основное назначение программного модуля AdminTool 4.41. Исходя из объема выполняемых задач, пользователь может самостоятельно выбрать вариант автоматически загружаемого интерфейса программы из трех предложенных на выбор: easy, medium и advanced. Конфигурация каждого из предложенных вариантов соответствует их переводу: минимальный, стандартный и вариант для продвинутых пользователей.

На первом этапе работы требуется обнаружить видеосервер в сети, для чего уточняется зона поиска, выбором одной из двух конфигураций. Поиск осуществляется в локальной сети и сети Интернет. Для этого необходимо ограничить зону поиска, заполнив пустые поля для IP-адреса и порты искомого видеосервера. Если же видеосервер находится в одной локальной сети с компьютером администратора, то в результате сканирования появится новое окно с MAC-адресом и IP-адресом найденного устройства. Строка с выведенной информацией одновременно является ссылкой в окно подменю настроек характеристик видеосигнала. В это же подменю можно переместиться из основного меню с ранее выбранным интерфейсом для продвинутых пользователей. Именно в данном окне назначается тип используемого видеостандарта и осуществляется настройка качества видеосигнала. Среди предлагаемых настроек - настройка яркости, контрастности, а так же настройки цветности. Из данного подменю возможен переход в подменю предварительного просмотра видеоизображения от обнаруженного источника видеосигнала. Также в подменю предварительного просмотра можно попасть и из основного меню, при условии что оно загружено в варианте для продвинутого пользователя. Кроме вышеперечисленных, существуют еще два подменю: подменю настройки интерфейсов RS-232C и RS-485, и отдельное подменю конфигурирования FTP-сервера и IP-сервера (с возможностью задания динамического IP-адреса для DHCP, или настройкой протокола PPPoE). Достаточный минимум алгоритмов записи был бы неполным без возможности работы по расписанию. С устройства организуется отправка кадров на выбранный для организации архива сервер в течение назначаемого промежутка времени.



По тому же сценарию осуществляется настройка видеосервера при его размещении в сети Интернет. Все описанные операции настроек требуют полномочий администратора с соответствующим паролем доступа (по умолчанию прописанный в устройстве пароль администратора приведен в руководстве пользователя на MDW-100). Для каждого из 9 пользователей можно задать индивидуальное имя и пароль, а также разрешить пользоваться функциями управления GPIO и SIO, которых мы коснемся позднее. Из меню настроек возможно переключение между устройствами, которые требуют изменения ранее заданных настроек. И еще одна важная функция. При необходимости, из AdminTool можно обновить версию прошивки сетевого видеосервера.

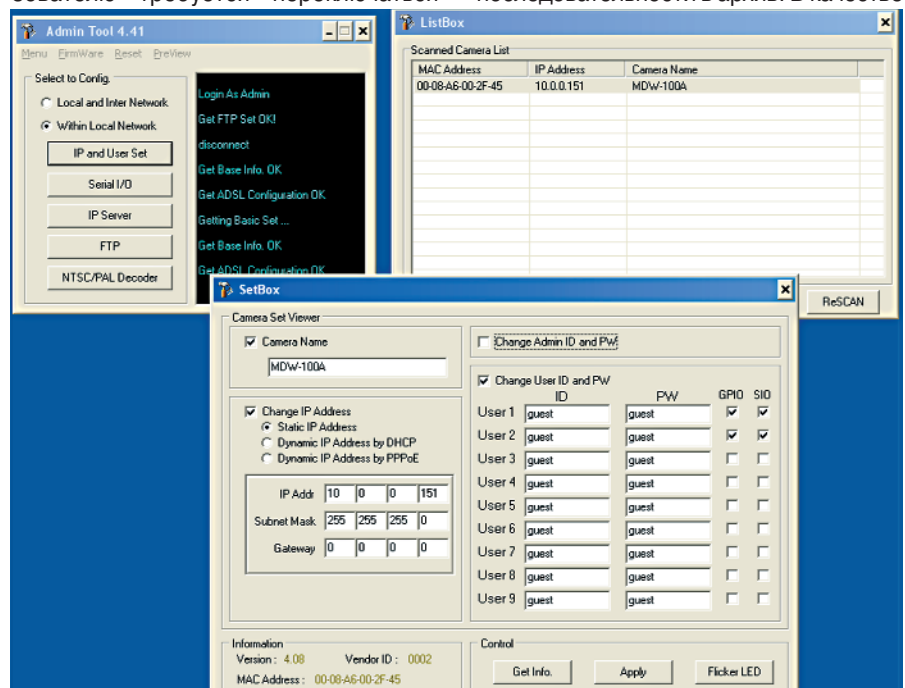
Программное обеспечение Web CamViewer1CH 1.45, являясь основной рабочей программой, предназначено для мониторинга, управления, а также для организации процесса записи видеопоследовательности на ПК (никакого дополнительного ПО для этого докуपा не придется). В программе WebCamViewer1CH 1.45 имеется возможность установить одновременное соединение только с одним видеосервером. Интерфейс основного окна программы можно условно разделить на четыре части. В информационном окне сообщений выводится отчет по событиям. При активизации следующего окна у оператора появляется возможность управления PTZ-устройствами посредством расположенных в окне кнопок управления. При неактивности данной опции, видимо, для уменьшения загруженности интерфейса кнопки управления скрываются. Аналогично организовано и окно GPIO, которое в активном виде

состоит из двух частей, одна часть которого предназначена для работы с тревожными входами, вторая - для работы с тревожными выходами. И, как и следовало ожидать, большая часть основного окна отведена под трансляцию видеоизображения. В нижней части окна на черном поле отображается рабочая статистика канала связи с сетевым видеосервером. Статистика включает в себя IP-адрес видеосервера, информацию об установлении соединения,

иконку об активности аудиоканала с возможностью изменения уровня звука, иконку изменения размера окна видеоизображения, статистику активности режима записи, скорости воспроизведения видеоизображения и параметрам видеопотока. Для удобства работы пользователя в отдельную строку вынесены кнопка соединения, кнопка включения режима записи и кнопка перехода в меню конфигурации настроек. В строке с наименованием соединения расположена иконка активизации канала аудио и кнопка Capture, используемая для сохранения изображения текущего видеокдра. Но кнопка Capture столь не приметна, что поначалу мы на нее даже не обратили внимания.

Что касается меню конфигурации настроек, то оно состоит из трех закладок. Окно первой закладки используется для конфигурации соединения. Если пользователь требует переключаться

между разными соединениями, то для упрощения процесса ввода конфигурации нового соединения достаточно один раз заполнить поля для данных по соединению и ввести их в адресную книгу. В дальнейшем после активизации строки с информацией по требуемому соединению двойным щелчком левой кнопки мыши данная информация заполнит поля для текущего соединения. Далее остается только принять настройки и осуществить соединение. Пользователю с правами администратора разрешена настройка параметров качества видеопотока. Он может наложить ограничение по скорости трансляции видеопотока, измеряемой в к/с, выбрав наиболее подходящий из восьми предложенных вариантов, подобрать размер видеопотока опытным путем, задать интервал между ключевыми кадрами в видеопоследовательности, а также установить максимальную и минимальную границы качества транслируемого видеоизображения. Поскольку данные настройки будут едины для всех соединений, придется выбирать оптимальный вариант для всех соединений сразу. Разработчики рекомендуют свои конфигурации настроек, которым соответствуют кнопки Best (наилучшее качество), Good (хорошее качество), Default (стандартное качество), Bad (плохое качество) и Worst (наихудшее качество видеоизображения). В этом же окне предлагается задать режим работы видеосервера: трансляция видеопотока по локальной сети с целью просмотра или режим с возможностью записи видеопоследовательности в архив. В качестве

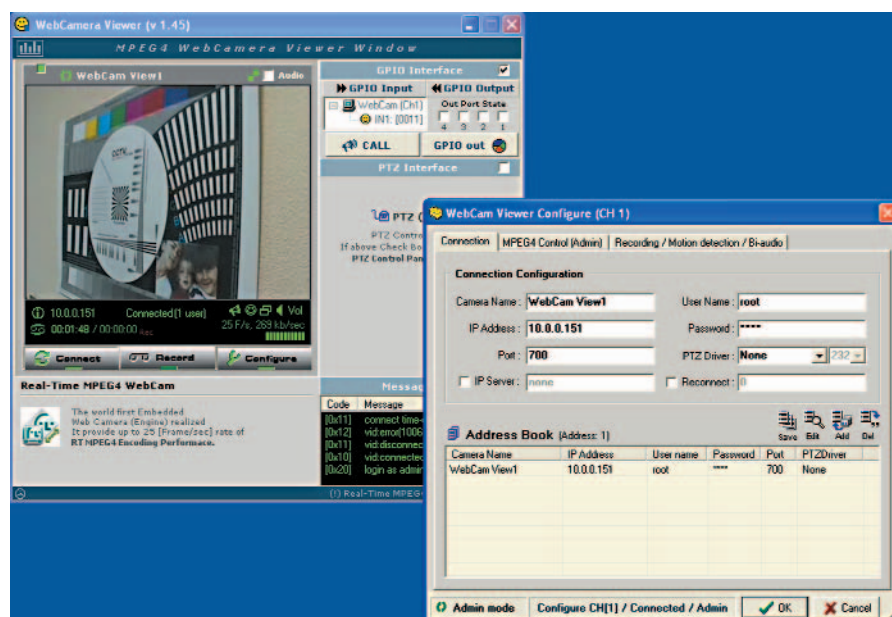


Конфигурирование видеосервера.

помощи по настройке качества записи, разработчики при каждом ползунке настройки разместили изменяющие цвет цифры. Числовое значение соответствует положению своего ползунка, а цвет цифр изменяется с черного на красный, если заданное значение параметра настройки выходит за границы рекомендуемых разработчиками значений. В устройстве предусмотрено три режима передачи кадров: mode 0 (в данном режиме передаются только ключевые кадры), mode 1 (в данном режиме передаются все кадры) и mode 2 (передаются все кадры, в которых обнаружено движение при условии, что они не попадают в категорию для mode 0).

Нам не удалось в руководстве пользователя обнаружить информацию по максимальному количеству одновременных соединений с видеосервером (позднее данная информация была найдена на сайте компании-производителя). Ограничение данного параметра было определено при тестировании. Данное число было получено путем одновременного подключения к видеосерверу пользователей с нескольких удаленных рабочих мест. Максимально с одним видеосервером нам удалось установить 10 соединений. При этом одно рабочее место подразумевало ПК, как с установленным одиночным соединением с видеосервером, так и с максимальным количеством одновременных соединений.

Действительно, на одном рабочем месте возможен одновременный запуск нескольких программ WebCamViewer 1CH и 4CH, но ввиду



Настройки соединения.

единичности образца MDW-100 попавшего в нашу тестовую лабораторию, установить их максимальное количество не представлялось возможным.

Программа WebCamViewer4CH является четырехканальным вариантом программы WebCamViewer1CH, и предназначена для организации одновременной работы уже с 4 аудио и видеоканалами. В остальном же принципиальных отличий между двумя программами нет.

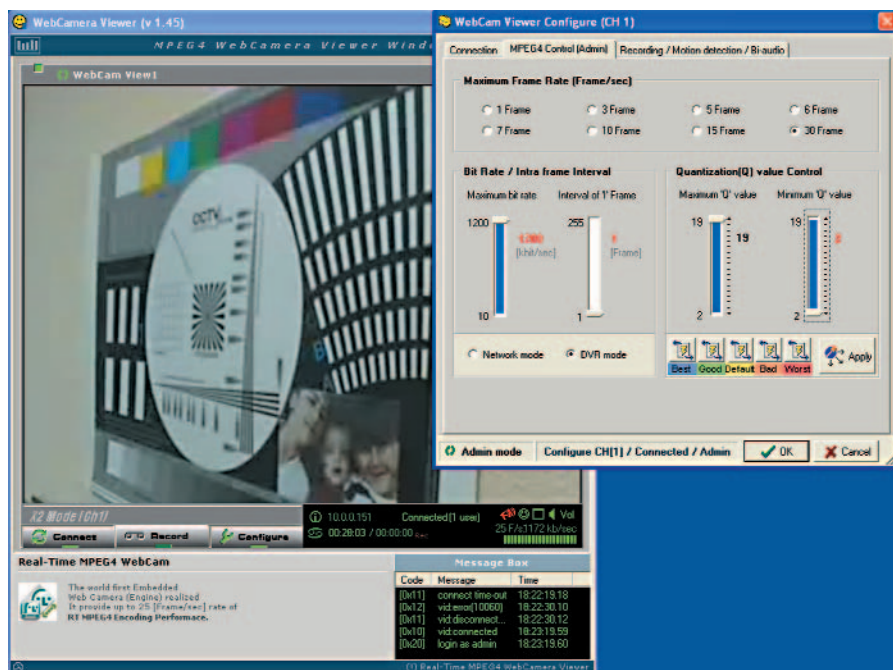
Программное обеспечение WebCamPlayer 1.45 служит для просмотра в отдельном окне одной выбранной из архива видеопоследовательности. В процессе просмотра ранее записанной видеопоследовательности можно включить режим наложе-

ния маски, при этом окно для вывода видеоизображения делится на 25 зон. Если одновременно активизировать режим маски и детектор движения, то результатом обнаружения движения будет изменение цвета границы зоны, в которой обнаружено движение, с черного на красный. Также в программе предоставлена возможность получения снимка активной части окна, в котором воспроизводится ранее выбранная видеопоследовательность.

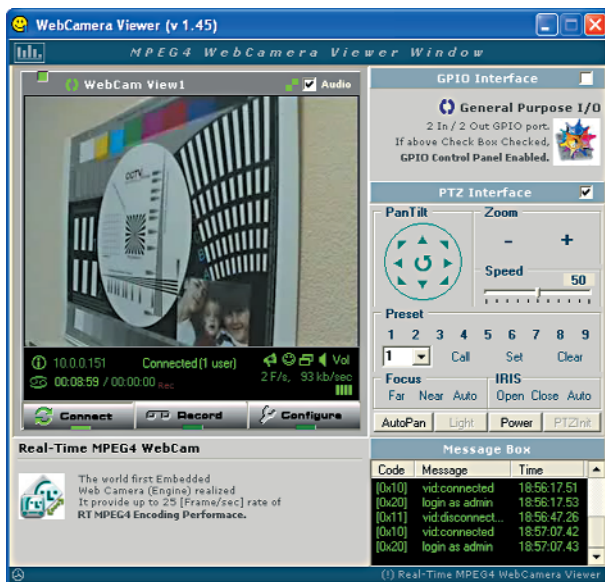
Перейдем непосредственно к самому процессу тестирования.

Подключившись к видеосерверу с правами администратора, а среди всех одновременно подключенных пользователей разрешается только одно соединение пользователя с данными полномочиями, мы получили полный доступ ко всем предложенным настройкам. Из рекомендуемых производителем, мы решили выбрать конфигурацию Best, которая подразумевает лучшее сочетание параметров и настроек, влияющих на качество компрессии MPEG-4.

При подключении одного пользователя максимальный поток составил 1172 КБ/с при назначенном 1200 КБ/с, а скорость отображения 25 к/с из назначенных 30 к/с. Возможно, данное максимальное значение скорости воспроизведения подразумевает использование стандарта NTSC, но для нас приоритетным все же является PAL. При увеличении количества подключаемых к видеосерверу пользователей от одного до 10, скорость воспроизведения падает до 18 к/с. В качестве недостатка данной конфигурации настроек



Настройки MPEG-4.



Управление PTZ - устройством.

можно отметить периодическое волнообразное изменение скорости отображения видеопотока. Данное явление наблюдается только в случае подключения максимально разрешенного количества пользователей, но скорость воспроизведения при этом не опускается ниже отметки 1 к/с, то есть происходит постоянное волнообразное колебание скорости отображения от 1 до 18 к/с.

При выборе конфигурации с наихудшим качеством Worst скорость воспроизведения практически не изменяется. Такие же значения параметров сохраняются и при организации процесса записи по всем видеоканалам.

Заметим, что конфигурация Worst подразумевает автоматическое активирование сетевого режима, в остальных конфигурациях подразумевается режим "цифрового видеорегистратора". Но при повторном входе в режим настроек, с ранее выбранной конфигурацией Worst, активизирован будет все-таки режим "цифрового видеорегистратора". Выбрав конфигурацию Worst и подключив максимальное количество пользователей, получим значение потока по каждому отдельному каналу 14 КБ/с, а скорость воспроизведения 4 к/с.

Возвращаясь к конфигурации Best, отметим, что при активизации режима записи связь видеосервер-пользователь уже не столь стабильна, наблюдаются случаи потери соединения и невозможности активизирования режима записи более чем 8 каналов на одном рабочем месте одновременно. Подобные недостатки замечены при активизации режима записи с ранее назначенной конфигурацией Worst. Если после критического падения качества

воспроизведения режим записи все-таки активизируется, записанная при этом видеопоследовательность в архиве хотя и сохраняется, но в программе WebCamPlayer 1.45 не воспроизводится. Повторное подключение канала, по которому наблюдалось пропадание соединения, не представляется возможным. В ряде случаев, даже при попытке повторного подключения, после принудительного отключения всех пользователей, первое соединение все-таки устанавливается, качество видеопотока при этом просто неприемлемое. Для восстановления качества воспроизводимого изображения требуется переконфигурация настроек в меню настроек видеопотока выбранной для работы программы (WebCamViewer1CH 1.45 или WebCamViewer4CH 1.45).

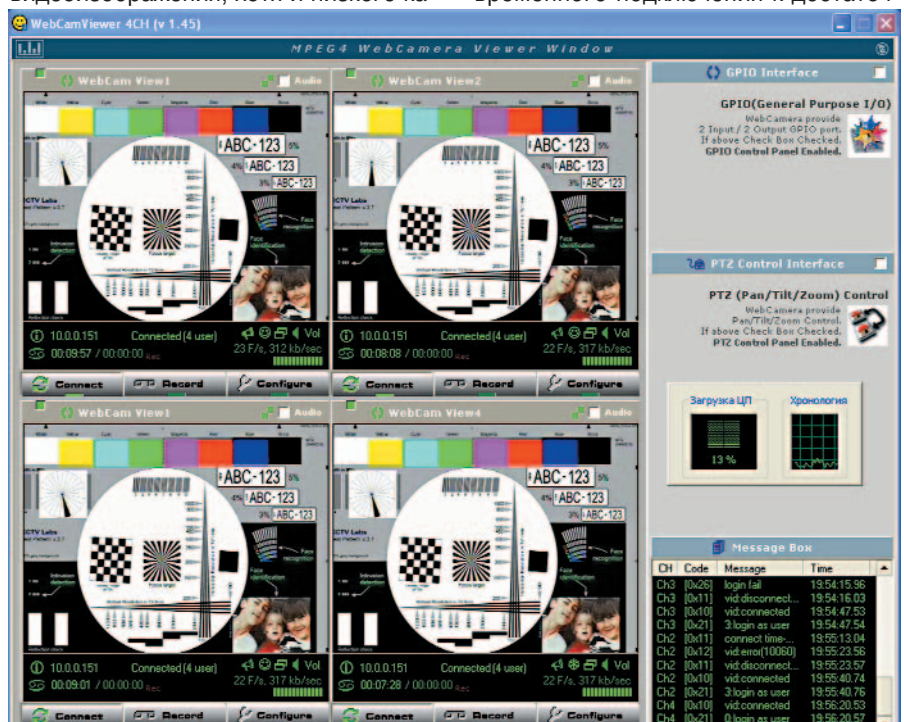
Исходя из всего вышесказанного, мы советуем быть более внимательными при использовании крайних режимов, предлагаемых производителем конфигураций настроек. И как замечание при работе с конфигурацией Worst. Если у первого подключившегося к видеосерверу пользователя, еще сохраняется стабильное воспроизведение видеопотока, хотя и низкого ка-

чества, не факт, что таким же качеством видеопотока будут наслаждаться и остальные пользователи.

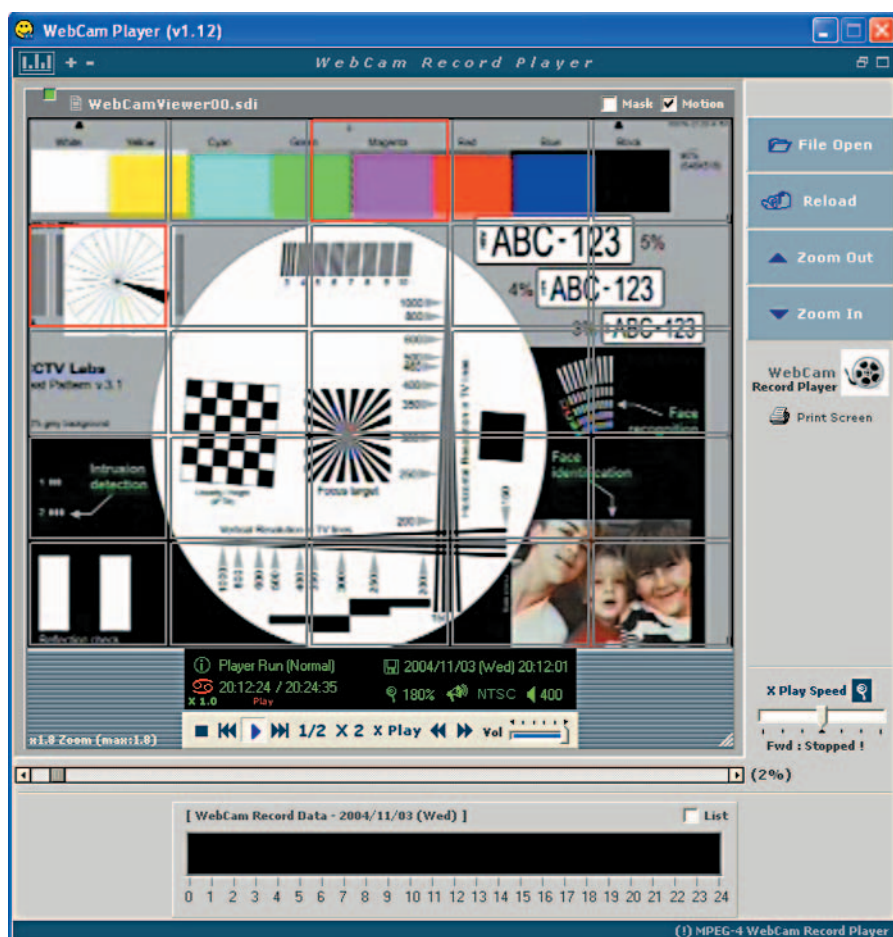
Так что конфигурация настроек является достаточно индивидуальным и не допускающим шаблонов процессом.

Разрешение для всех режимов настройки было около 200 ТВЛ. Качество изображения было наихудшим в конфигурации Worst, и примерно одинаковым в конфигурации Default и Good. Наилучшее качество наблюдалось в конфигурации Best, но и оно не сильно отличалось от качества в конфигурациях Default и Good. Поскольку этот сетевой видеосервер на самом деле работает с форматом кадра 320x240, то высокой разрешающей способности от него ожидать не приходится, а отображение 640x480 - это интерполированное разрешение кадра, и в расчет его принимать не следует, хотя такой формат кадра и упомянут на русскоязычном сайте. Существенным недостатком этого сетевого видеосервера оказалось неправильное отображение кадра PAL, так как происходит срезание части кадра в его левой и нижней части. Данный недостаток сохраняется и при просмотре видеоархива.

В целом, использование устройства с идущим в комплекте программным обеспечением позволяет построить разветвленную систему видеонаблюдения и записи. Конечному пользователю предоставлена возможность организации не более 10 рабочих мест, с возможностью одновременного подключения к достаточ-



Одновременный просмотр 4 каналов.



Просмотр видеоархива.

ному количеству видеосерверов. На каждом рабочем месте подразумевается организация режима записи по каждому стабильному соединению, включая организацию записи по детектору движения, для которого предусмотрена настройка чувствительности. Востребованы возможности организации видеоархива на FTP-сервере с отправкой видеопотока по индивидуальному расписанию, а также подключения к каждому видеосерверу PTZ- устройств, в том числе и поворотных телекамер, использующих любой из 13 предлагаемых на выбор протоколов связи. При работе с данным устройством можно организовать канал связи пользователь - видеосервер или видеосервер - пользователь с записью аудиосигнала. Добавьте ко всему вышеперечисленному специальную программу для работы с записанным архивом, поддерживающую многооконный запуск с назначением индивидуального задания по каждому окну, что не запрещает одновременный, но несинхронизированный просмотр одной записи во всех активных окнах.

Нам понравился достаточно простой и интуитивно понятный интер-

фейс всех программных модулей. Примечательно и миниатюрное исполнение самого видеосервера.

На компакт-диске находится дополнительное программное обеспечение, служащее для организации работы с HTTP-сервером. Для реализации возможности просмотра видеоизображения, передаваемого с видеосервера, в окне запущенного веб-браузера потребуется перепрограммировать видеосервер. Необходимые для этого

файлы можно найти на том же компакт-диске, а поэтапные шаги выполнения данной операции описаны в руководстве пользователя.

А теперь остановимся на особенностях устройства. Отметим полное отсутствие поддержки русского языка. В бумажной версии технической документации вообще ничего конкретного не было сказано про данную модель сетевого видеосервера. Этот документ является скорее общим руководством по программному обеспечению линейки сетевых телекамер и видеосерверов производства компании MC Electronics. Впрочем, это становится понятно только после ознакомления с электронной версией руководства пользователя. Недостаток информации можно восполнить при посещении веб-сайта компании-производителя MC Electronics. Что приятно, на сайте имеется ссылка на русскоязычный портал, практически полностью копирующий оригинальный сайт компании. На русскоязычном сайте можно найти дополнительную информацию о компании, ее продукции, и, конечно, техническую спецификацию на сетевой видеосервер MDW-100A.

Впрочем, при функциональности начального уровня это устройство имеет самую низкую цену среди всех протестированных для данного номера журнала сетевых видеосерверов, поэтому не стоит надеяться на более глубокую адаптацию данного видеосервера под российских потребителей. Хотя производители обещают совершенствовать возможности видеосервера, уже сейчас данное устройство можно воспринимать как вполне законченное решение.



Горизонтальное разрешение: 1-worst, 2-bad, 3-default, 4-good, 5-best.

VIP-10

Следующим по очереди тестированию подвергся сетевой видеосервер VIP 10 производства компании VCS Video Communication Systems AG. Как известно, с 5 июля 2004 года данная компания вошла в состав Bosch Security Systems Group.

Видеосервер VIP 10 упакован в коробку из белого картона. В комплекте с устройством поставляется блок питания, напряжение на выходе которого составляет 24 В постоянного тока, а к выведенным проводам подключена клемная колодка. Также в комплекте идут краткое описание в бумажном виде, кабель для подключения к последовательному порту и компакт-диск с полным описанием и дополнительным программным обеспечением Acrobat Reader, DirectX9.00b, MPEGViewer и MPEGActiveX.

Корпус видеосервера выполнен в виде параллелепипеда с пазами и выступающими элементами. Выступающие элементы имеют отверстия для жесткого монтажа устройства в стойку, шкаф, короб и т.д. На нижней части устройства размещены 4 резиновые накладки. При применении данных накладок можно понизить уровень внешней вибрации, а также исключить соприкосновение металлического корпуса устройства с поверхностью, в частности при настольной установке видеосервера.

Если быть точным, то VIP 10 - это не одиночное устройство, а представитель линейки оборудования, в состав которой входит два устройства. Тестируемая модель VIP 10S сконфигурирована как передатчик, так же существует устройство VIP 10E, которое выполняет функцию приемника и декодирует оцифрованный сигнал в аналоговый. Совместное использование устройств обоих типов позволяет строить системы безопасности без использования персональных компьютеров, но это уже за рамками данного тестирования, хотя подобная конфигурация типична для сетевых видеосерверов производства VCS.

Размер устройства - 65x27x108мм, вес без внешнего блока питания составляет 300 грамм.

Что касается поддерживаемых стандартов сжатия, то устройство VIP 10 использует компрессию MPEG-4 и кодирует звук в формате G.711. На лицевую панель видеосервера вынесены комбинированный видеовход с разъемом BNC и 9-



штырьковый разъем последовательного порта, поддерживающий последовательные интерфейсы RS-232/RS-485 (включая поддержку RS-422). На тыльной стороне корпуса устройства размещен разъем интерфейса USB 2.0, который, как сказано, на сайте компании-производителя, используется для организации записи архива на внешние носители, а также для подключения внешнего модуля связи по сети WLAN (пока неясно, как реализуются данные опции, и даже обновление ПО ясности в этот вопрос не внесло). Также на задней панели расположены три индикатора статуса работы устройства, 10-штырьковый разъем для подключения внешней колодки и разъем RJ-45 для подключения к сети Ethernet/Fast Ethernet. К 10-штырьковому терминалу кроме питания можно подключить 1 аудиосигнал и 2 тревожных сигнала. Что касается выходов, то они представлены 1 аудиовыходом и двумя тревожными выходами. Если посмотреть внимательно, то на задней панели можно найти отверстие. За данным отверстием скрыта кнопка перезагрузки устройства, используемая для сброса настроек и конфигурации сетевого видеосервера.

Руководство пользователя написано на английском языке и является общим для моделей серии VIP 10 и моделей серии VIP 1000. Для более удобной

навигации по руководству пользователя можно использовать не только содержание, но и алфавитный указатель. Большую часть информации из руководства пользователя можно найти в файле помощи.

Не будем нарушать принятый порядок тестирования устройств данного типа. Непосредственно этапу тестирования предшествует этап конфигурации и настройки. В первую очередь потребуется задать IP-адрес сетевого видеосервера. Видеосервер и компьютер между собой потребуются соединить посредством кабеля по последовательному интерфейсу. Для установления связи воспользуемся встроенными в операционную систему Windows средствами связи, а именно Hyper Terminal. Если данный процесс вызывает трудности, то стоит обратиться к руководству пользователя. В целом, процесс достаточно тривиален. Трудно сравнивать удобство данного способа задания IP-адреса и способа, при котором используются дополнительные утилиты. Скорее это дело привычки. Но способ, в котором для соединения с устройством используется локальная сеть, является более универсальным. Подчас дополнительное соединение может быть источником непредвиденных трудностей.

После того как соединение установлено, то при запуске видеосервера, в

окне Hyper Terminal загрузится информация о подключенном устройстве и приглашение к началу работы. Процесс настройки разрешен только пользователю Service. После принятия имени пользователя в окне Hyper Terminal загружается таблица меню. В данной таблице приведены группы настроек и соответствующий каждой группе символ, служащий уже для загрузки таблицы настроек выбранной группы. Аналогично построение и таблицы для выбранной группы, только символы уже соответствуют отдельным настройкам.

Для окончательной загрузки введенных настроек видеосервер необходимо перезапустить.

На этапе загрузки Live page пользователю предлагается установить дополнительное программное обеспечение ActiveX Control (размер данного файла порядка 5МБ), необходимое для декодирования передаваемых с видеосервера видеоизображений. Это программное обеспечение будет скачено в автоматическом режиме с сайта производителей. При отсутствии выхода в сеть Интернет или же при низкой скорости связи ActiveX Control можно установить из директории с аналогичным названием, расположенной на поставляемом с видеосервером компакт диске. На данном этапе мы столкнулись с целым рядом трудностей. Мы так и не смогли добиться воспроизведения видеоформата MPEG-4 в запущенных веб-браузерах на 4 ПК из 7. При этом конфигурация всех ПК соответствовала системным требованиям разработчиков. Что касается системных требований, то для работы с видеосервером на ПК должна быть установлена операционная система Windows 98, 2000, XP. В качестве веб-браузера рекомендуется использовать Internet Explorer версии 5.5 и выше. Пожалуй, стоит вспомнить тестирования других видеосерверов производства компании VCS Video Communication Systems AG. Материалы по данному тестированию можно найти в 4 номере нашего журнала за предыдущий год.

Загрузившись в окне веб-браузера основную страницу Live page можно условно разбить на несколько частей. В нижней части основной страницы расположены два окна: окно событий и окно сообщений. Верхнюю часть страницы Live page занимает баннер, который можно заменить на панорамное изображение от телекамеры. Данная опция реализуема только при ис-

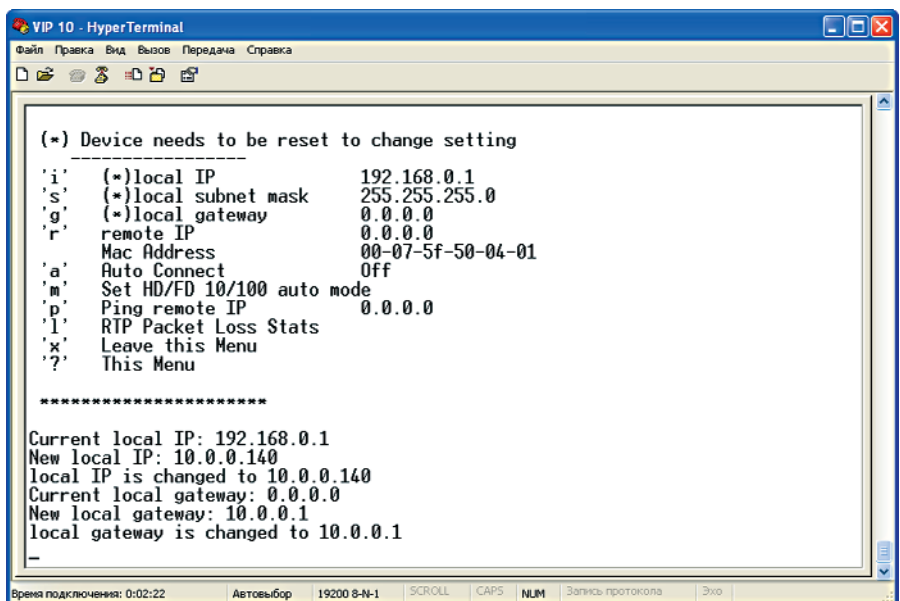


пользовании телекамер Sony EVI-D100 и Sony EVI-D30/31. Под баннером размещена строка с ссылками для активизации режима MPEG-4, активизации режима M-JPEG и ссылка перехода на страницу настроек. Также на основную страницу можно вынести индикаторы статуса реле и тревог и виртуальный пульт управления поворотной телекамерой. Центральную часть основной страницы занимает окно с выводимым видеоизображением. Под данным окном размещена строка с кнопкой, используемой для получения снимка активной части экрана, и кнопкой для активизации режима записи (в режиме M-JPEG отсутствует). Над окном с видеоизображением помещена строка с информацией о выбранном режиме воспроизведения видеоизображения (MPEG-4 или M-JPEG) и ссылки переключения между размерами активного окна (352x288 и 704x576).

Для настройки устройства предложено два режима: Wizard и Expert Mode. На этапе конфигурации и настройки видеосервера разработчики рекомендуют воспользоваться режимом Wizard. В данном режиме по мере заполнения своего рода анкет происходит автоматическая их смена, до тех пор пока ви-

деосервер не получит всю необходимую для настройки информацию. Кроме необходимых для заполнения полей, в каждом из окон существует зона, где выводится информация, упрощающая и разъясняющая этапы настройки. Всего требуется заполнить 18 основных окон, и несколько дополнительных. По окончании пользователь получает полностью сконфигурированное устройство. Второй режим рекомендуется использовать администратору и подготовленным пользователям. Он предназначен для подстройки и переконфигурирования видеосервера. Из режима Expert Mode также возможно обновление программного обеспечения.

Для удобства навигации по меню Expert Mode все настройки объединены в семь групп. Остановимся на отдельных из них. В группе Unit identification расположено пять подгрупп. В данной группе задается название устройства, назначаются пользователи, пользователям присваивается пароль. В видеосервере предусмотрена многоуровневая система доступа. Максимальными правами администратора, а также возможностью настраивать и конфигурировать видеосервер обладает пользователь Service. Кроме

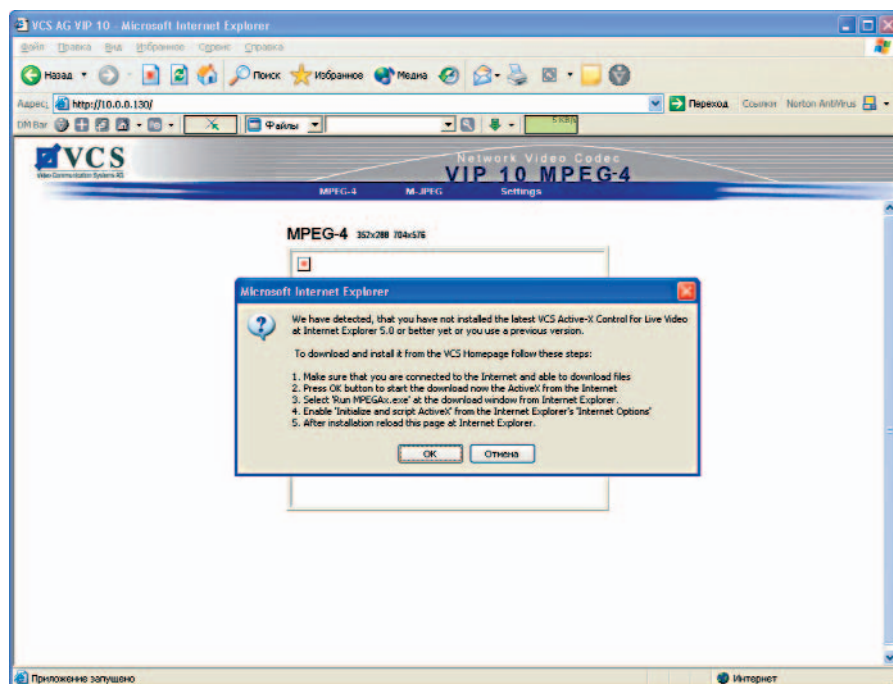


Конфигурация видеосервера в Hyper Terminal.

Service, существует еще две группы пользователей: User и Live. Пользователям из группы User разрешено работать с отдельными опциями и настройками, пользователи из группы Live могут только осуществлять мониторинг.

В видеосервере VIP 10 поддерживаются только два языка: немецкий и английский. Видимо, в качестве компенсации пользователю предоставлена возможность выбора формата даты и времени, накладываемых в виде титров на видеоизображение. На выбор предложено три формата: европейский, американский и японский. Пользователь может синхронизировать видеосервер с ПК или с назначаемым сервером.

В группе Video/Audio setting настраиваются параметры аудио и видеоканалов. Отдельная страница отведена под настройки конфигураций для компрессии видеопотока MPEG-4. Пользователю предложено настроить две конфигурации, а в дальнейшем осуществлять быстрое переключение между ними. На этапе настройки можно выбрать любую из восьми предложенных на выбор предустановок. Данные предустановки подразумевают взаимную конфигурацию нескольких параметров, среди которых ограничение пропускной способности сети, настройка качества и компрессии видеопотока, задание интервала между ключевыми кадрами, выбор разрешения видеоизображения между Low 176x144 (QCIF), Standard 352x288 (CIF) и High 704x288 (2CIF). На выбор пользователю предложены следующие предустановки: high quality (CIF), с разрешением 352x288; high res. (2CIF), с разрешением



Видеоизображение в формате сжатия MPEG-4 без установки ActiveX не воспроизводится.

704 x 288; low res. (QCIF) с разрешением 176 x 144; DSL, для DSL соединений с размером видеопотока 500 КБ/с; ISDN (2B), для ISDN соединений с 2 В-каналами; ISDN (1B), для соединений ISDN с одним В-каналом; MODEM, для соединений с аналоговым модемом и размером видеопотока 20 КБ/с и GSM, для соединений с GSM модемом.

Группа Alarm setting отведена под настройку тревожных событий и реакций на них. В качестве тревожных событий в видеосервере рассматриваются потеря видеосигнала, срабатывание по детектору движения и тревожным входам, а также изменение контрастности видеоизображения.

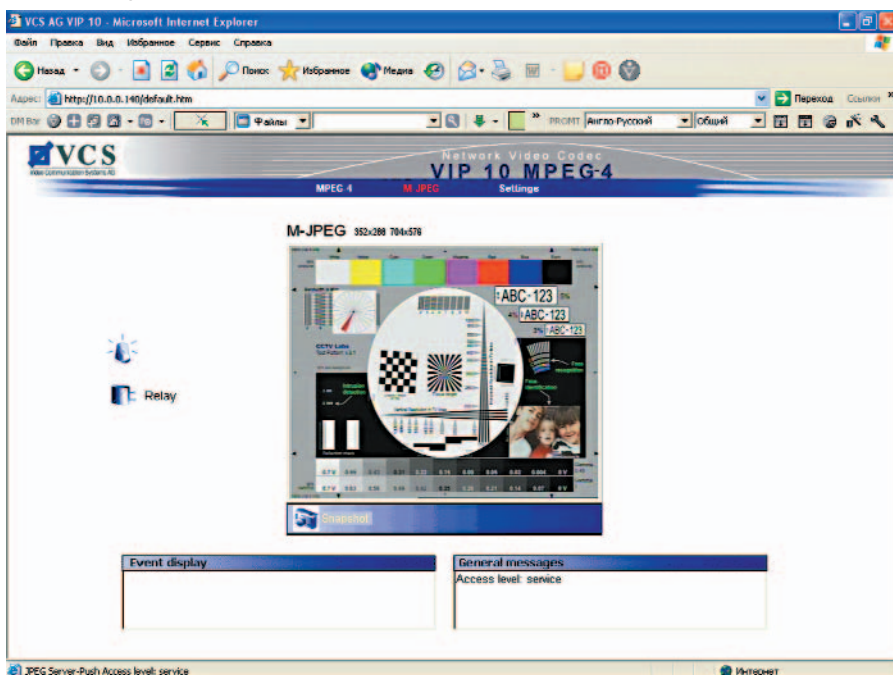
В следующей группе настраиваются реакции по тревожным событиям. Например, в качестве реакции выступает замыкание реле.

В группе Interface setting размещены настройки, служащие для конфигурации последовательного порта. Видеосервер VIP 10 поддерживает 13 протоколов управления поворотными телекамерами, что позволяет пользователю управлять подключенной к видеосерверу поворотной телекамерой, при условии если поворотная телекамера поддерживает любой из заданных протоколов.

И в отдельную группу выведены сервисные настройки. В данной группе можно конфигурировать сетевые настройки, узнать о версии программного обеспечения и при необходимости обновить его, а также настроить конфигурацию Live page. Примечательно наличие настройки Multilink-Multicast, которая позволяет дублировать видеопоток сразу на несколько клиентов на уровне сетевого оборудования, тем самым снижая нагрузку на видеосервер.

Остановимся на отдельных моментах тестирования.

В результате выбора в подменю MPEG-4 Encoder конфигурации high quality (CIF) строка настройки качества автоматически принимает значение 8. Данный параметр можно изменить как в сторону ухудшения до Low с численным значением 31, так и в сторону увеличения High с численным значением 4. Но видимого изменения в качестве видеоизображения при этом не происходит. Возможно, данная опция рабо-



Воспроизведение видеоизображения в формате M-JPEG.



Меню настроек.

тает только в автоматическом режиме.

Отметим еще одну особенность видеосервера. Независимо от выбора конфигурации выводимого на Live page видеоизображения, а качество изображения действительно изменяется в соответствии с настройками, во всех конфигурациях полученные снимки активного окна (при помощи кнопки Snapshot) являлись файлами формата JPEG с разрешением 352x288 и, независимо от выбранной конфигурации, с одинаковым качеством.

При выборе режима воспроизведения M-JPEG, а в видеосервере отдельных настроек для данного режима не предусмотрено, при размере окна 704x576, скорость воспроизведения для одной сессии в среднем составляет 1 кадр в 1,5-2с. Значение скорости воспроизведения с выбранным размером окна 352x288 уже находится в пределах 1к/с. Для максимального количества одновременно установленных сессий скорость воспроизведения достигает 1 к/мин. Максимальное количество соединений в режиме M-JPEG, установленное эмпирическим путем, составляет 9 сессий. На 10 сессии обновление видеоизображений прекращалось. Возвратить видеосервер в рабочий режим удавалось только после перезагрузки.

Для режима воспроизведения MPEG-4 максимальное число одновременно установленных соединений равняется 5 сессиям. Данное количество соединений было установлено с ПК, находящимся в одной локальной сети с видеосервером VIP 10. И даже в таких условиях, видеоизображение воспроиз-

водилось с разной задержкой. Максимальная задержка равнялась 7 минутам! Но надо отметить, что скорость воспроизведения видеоизображений при этом составляет 25 к/с, а пропуск кадров не наблюдается. И важен тот факт, что по первому соединению изображение воспроизводится в режиме "живое видео".

Горизонтальное разрешение для конфигурации high res. (2CIF) достигает 360 ТВ-линий, но при этом на изображении наблюдаются артефакты в виде областей с наложением цветовой мозаики, а также цветковые шумы. В этой же конфигурации записанный файл продолжительностью в 1 минуту имеет размер 17.6 МБ

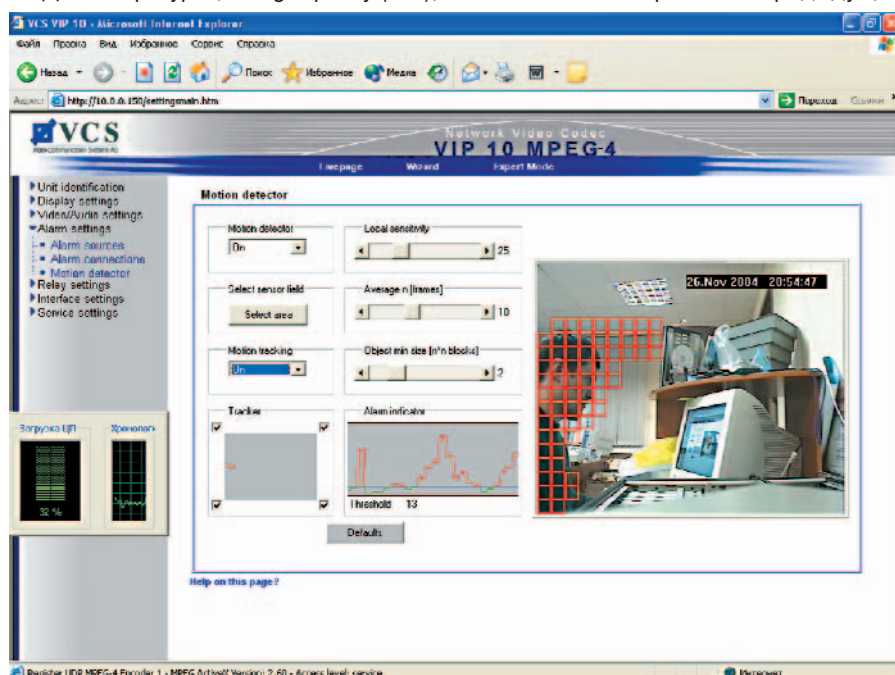
Для конфигурации high quality (CIF),

впрочем, как и для остальных конфигураций, горизонтальное разрешение менее 200 ТВЛ. Записанный файл продолжительностью в 1 минуту имеет размер 3.1 МБ

Для просмотра записанного видеоархива разработчики предлагают воспользоваться MPEGViewer. Данную утилиту можно найти на компакт-диске. В принципе, пользователю не предлагают ничего особенного. На компьютерах, где ранее не установился драйвер для декодирования MPEG-4, MPEGViewer работать не будет.

И краткие выводы по тестированию. Видеосервер VIP10 тестировался в одинаковых условиях со всеми остальными. При этом он оказался самым требовательным к организации рабочего места пользователя. Но нельзя забывать об особенностях и возможностях видеосервера VIP 10S. В полной мере о них можно говорить только при совместном использовании VIP 10S с VIP 10E. А что касается построения разветвленных систем видеонаблюдения, то компания VCS Video Communication Systems AG для этих целей предлагает целый программный продукт Vidos, состоящий из нескольких модулей.

В ряде линеек оборудования данного производителя сохраняются типовые особенности, это не обошло стороной и видеосервер VIP 10S. В компании VCS Video Communication Systems AG принята своя концепция в отношении видеосерверов, для ее понимания мы рекомендуем посмотреть статью о тестировании предыдущей



Настройка детектора движения.

линейки видеосерверов данного производителя, напечатанную в 4 номере нашего журнала за прошлый год. И в завершении отметим, что полученные при тестировании видеосервера VIP 10S результаты говорят о том, что в компании VCS Video Communication Systems AG принято делать больший акцент на возможности организации разветвленных сетевых решений нежели на построение небольших локальных систем.

AXIS-241S/AXIS-241Q

Шведская компания Axis Communication безусловно является законодателем моды на рынке сетевых решений для охранного телевидения. И было бы нелогично, если бы тестирование сетевых видеосерверов обошлось без ее новых решений. Именно решений, так как речь пойдет сразу о двух моделях, а если быть более точными, о четырехканальном видеосервере Axis 241Q и его одноканальном варианте Axis 241S. В рубрике "тест-драйв" третьего номера нашего журнала за прошлый год мы уже останавливались на более ранней четырехканальной модели данной линейки, видеосервере Axis 2400, а также касались его одноканального варианта Axis 2401. С тех пор прошло достаточно времени, и мы восполним недостаток информации, протестировав как одноканальный видеосервер Axis 241S, так и его 4-канальный собрата, видеосервер Axis 241Q.

Для компании-производителя уже в правилах хорошего тона стало каждую модель упаковывать в индивидуальную картонную коробку с яркой глянцевой обложкой, где кроме дополнительной информации размещена фотография



Горизонтальное разрешение: 1-worst, 2-bad, 3-default, 4-good, 5-best.

вложенного изделия. Так было и с данными моделями. В комплект поставки входят: видеосервер, подробная инструкция пользователя (на английском языке), гарантийный талон, крепление для монтажа в стойку и компакт-диск с информацией о партнерах компании Axis Communication и о ранее выпущенной продукции.

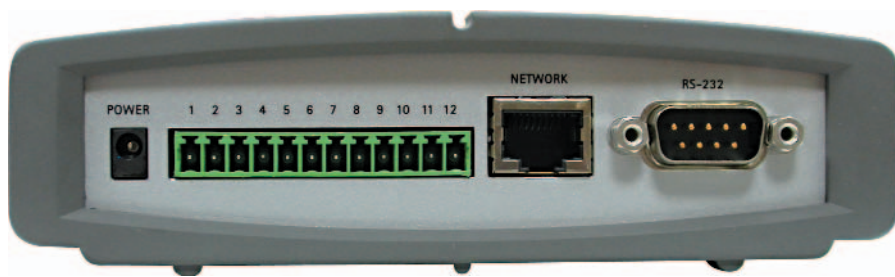
Видеосерверы Axis 241S и Axis 241Q имеют одинаковую довольно нестандартную форму в виде неправильного параллелепипеда с пазами, вырезами и скатами. Размеры корпуса - 42x140x155 мм, а вес без блока питания составляет 540 грамм. При поверхностном монтаже устройства опираются на выступающие ребра пластичных элементов, расположенных на передней и задней зонах конструкции корпуса. Элементы выполнены из эластичного пластика. Так что не составит особого труда снять данные элементы и в специальные пазы вдоль боковых поверхностей корпуса установить упоры, к которым приворачиваются креп-

ления, служащие для жесткого монтажа видеосервера на рабочий стол, шкаф, в короб или в стойку.

На лицевую панель устройства вынесены три статусных индикатора, переключатели согласованной нагрузки 75 Ом, 4 композитных видеовхода для четырехканальной модели и один композитный видеовход со сквозным композитным видеовыходом для модели Axis 241S. На задней панели расположены вход для подачи питающего напряжения, стандартный разъем RJ45, служащий для подключения устройства к локальной сети и терминал, используемый для подключения клеммной колодки. Там же размещен 9-штырьковый разъем последовательного порта RS-232, используемый для подключения PTZ-устройств.

На плате видеосервера мы обнаружили 32-битный RISC-процессор AXIS ETRAX 100LX, микросхема AXIS ARTPEC-2 с 8/16 МБ памяти (241S/241Q), а также 32/64 МБ оперативной памяти (241S/241Q) и 8 МБ флэш-памяти. В





обоих устройствах для записи событий, предшествовавших тревоге и последовавших за ней, выделяется 9 МБ оперативной памяти. В отдельной части энергонезависимой перезаписываемой памяти хранятся файлы настройки и драйверы для PTZ-устройств.

Сценарий установки, инсталляции и подключения видеосерверов вполне применим к большинству устройств подобного типа. Достаточно подсоединить устройство к локальной сети, подать видеосигнал и питающее напряжение. Далее нужно присвоить IP-адрес, используя протокол ARP, или заранее скачанную с веб-сайта компании производителя утилиту Axis IP Installer. Необходимым для выполнения данной операции является знание MAC-адреса видеосервера. Данная информация помещена на наклейке сетевого видеосервера.

После присвоения IP-адреса можно подключаться к устройству и переходить к этапу настройки. При первом обращении ко встроенному в видеосервер веб-серверу устанавливается дополнительное программное обеспечение, позволяющее отображать в окне веб-браузера видеопоток, передаваемый в формате M-JPEG. Видеосервер использует встроенную операционную систему Linux с ядром 2.4.

В устройстве предусмотрена многоуровневая система доступа, а нас в первую очередь интересует доступ с максимальными правами для администрирования. По умолчанию это пользователь "root". Заданный по умолчанию пароль для данного пользователя прописан в прилагаемом к устройству руководстве пользователя в бумажном виде. После принятия имени пользователя и соответствующего ему пароля будет завершена полная загрузка основной страницы, которая будет сконфигурирована в соответствии с полномочиями пользователя, установившего данное соединение. В дальнейшем на этапе соединения с видеосервером можно отключить опцию запроса имени пользователя и назначенного пароля. Но процедура

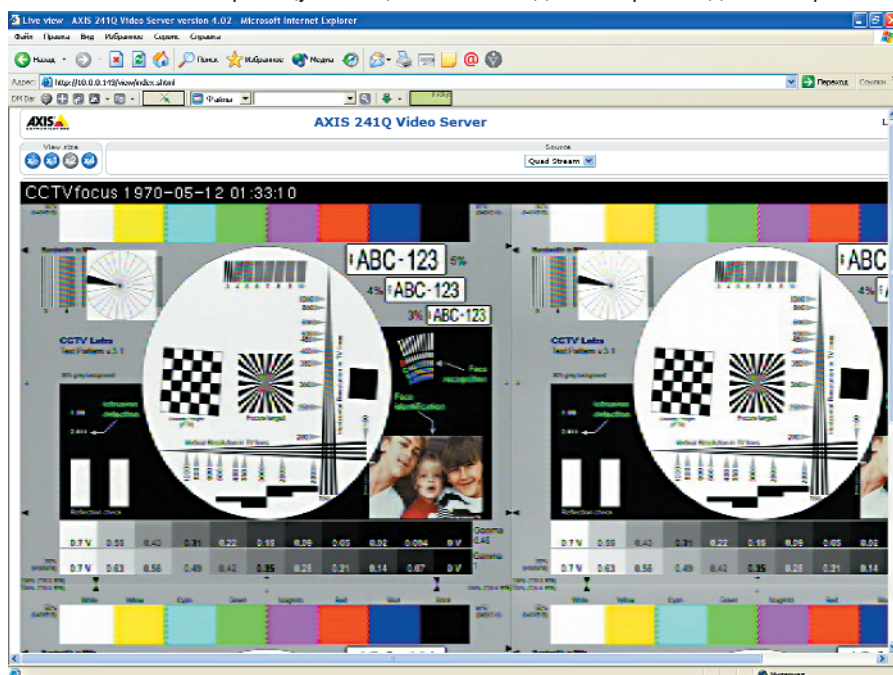
идентификации необходима при использовании опций видеосервера, подразумевающие принадлежность пользователя к группе с соответствующими на то правами и полномочиями. В центре загрузившейся странице расположено окно с видеоизображением.

По умолчанию над данным окном размещен ряд кнопок, служащих для изменения масштаба выводимого видеоизображения. При желании данное окно можно развернуть на весь экран монитора. Кнопка с соответствующей функцией расположена в отдельном ряду под окном с видеоизображением. В этом же ряду находится кнопка для получения стоп-кадра и кнопка сохранения захваченного кадра в отдельной папке в виде изображения в формате JPEG. По желанию данный ряд кнопок убирается со страницы Livepage. Кроме отмеченных, на основную страницу можно вывести и другие кнопки, а также кнопки для управления PTZ-устройствами. Это реализуется из меню настроек страницы Setup. Чтобы переместиться на данную страницу, необходимо воспользоваться ссылкой с соответствующим названием. Кроме страницы настроек, с основной страницы можно попасть на страницу помощи.

При каждом тестировании оборудования компании Axis Communication нами отмечалось удачное структурирование файла помощи Help, а также его достаточная информативность. Данная особенность не обошла стороной и модели Axis 241S и 241Q.

Что касается меню настроек, то для удобства работы все настройки объединены в пять групп. Группа Basic Configuration имеет четыре закладки. В закладке User администратор может назначить новых пользователей, задать им пароль и назначить их в ту или иную группу. Всего предусмотрено три группы пользователей: Viewer с возможностью просмотра (имеет смысл только при отключении анонимного просмотра), Operator - пользователь с возможностью изменять настройки просмотра, Administrator - администратор с максимальными правами и полномочиями. Соответственно права и полномочия пользователя определяются его принадлежностью к одной из перечисленных групп пользователей. На этой же странице дается разрешение на управление PTZ-устройствами как пользователям с именем и паролем (Operator, Administrator), так и анонимным пользователям (Viewer). Количество одновременно подключенных к видеосерверу конечных пользователей не может быть более 20.

Закладка настроек TCP/IP служит для конфигурации IP-адреса видеосервера, там же осуществляется настройка DNS-сервера и выставление ограничения по пропускной способности сети. В закладке настройки даты и времени,



Вывод видеоизображений в режиме quadro.

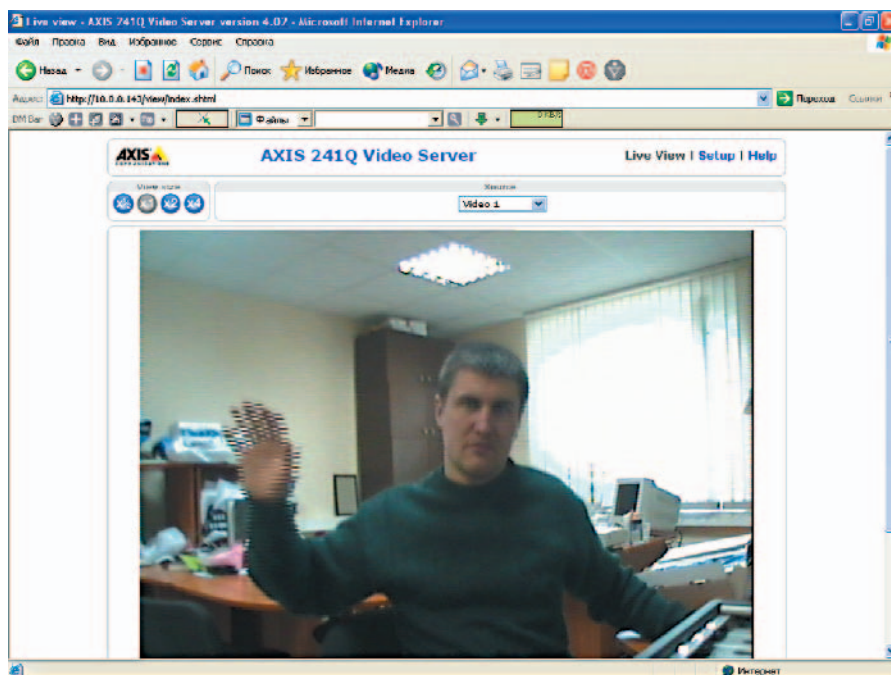
кроме стандартных настроек, предусмотрено назначение NTP-сервера для синхронизации по времени. В той же группе размещена закладка настройки видеоизображения, под которую выделена целая последующая группа.

После общей настройки видеосервера настройки данной группы представляют для нас наибольший интерес. Пользователь имеет возможность задать необходимое разрешение из пяти возможных: 4CIF (768x576), 2CIF Expanded (интерполированный до разрешения 768x576), 2CIF (768x288), CIF (384x288) и QCIF (192x144). Здесь можно назначить уровень компрессии от 0 до 100, выбрать черно-белое или цветное изображение, а также наложить ограничение на размеры видеопотока.

В следующей группе Live View Config настраивается конфигурация рабочего окна с выводимым нем изображением. Можно воспользоваться предложенной по умолчанию конфигурацией либо перенастроить интерфейс по собственному усмотрению. При данной настройке не следует убирать галочку из пункта Show setup link, иначе будет невозможно напрямую попасть со страницы Livepage в меню настроек и для этого придется использовать ссылку <http://IP-адрес/ operator/ basic.shtml>.

Что примечательно, разработчики предлагают поместить на Livepage еще 4 настраиваемые ссылки, чем мы непременно решили воспользоваться. Мы проверили их работоспособность, поместив ссылки еще на четыре видеосервера.

На закладке HTML Examples можно

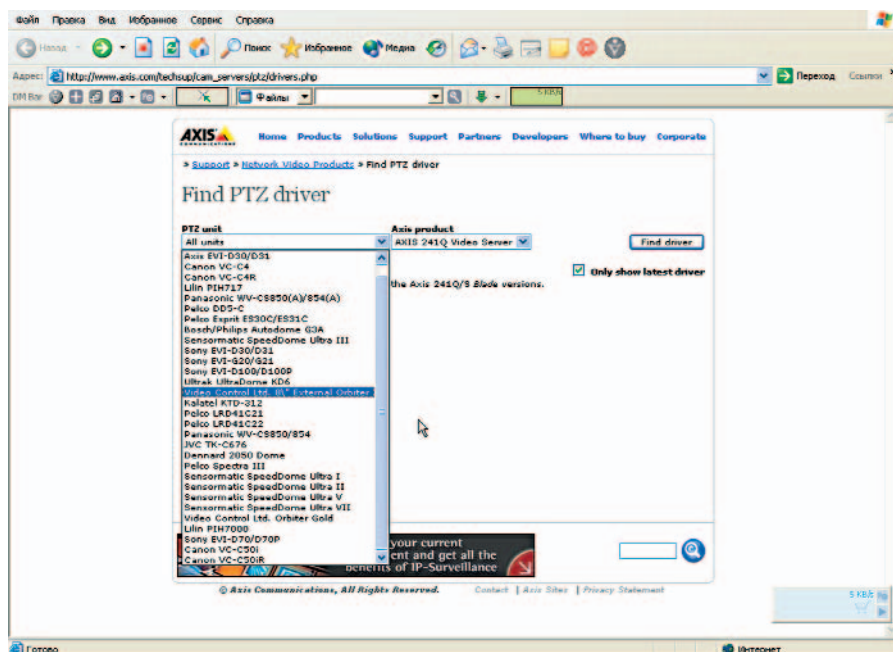


Эффект гребенки на полнокадровом изображении.

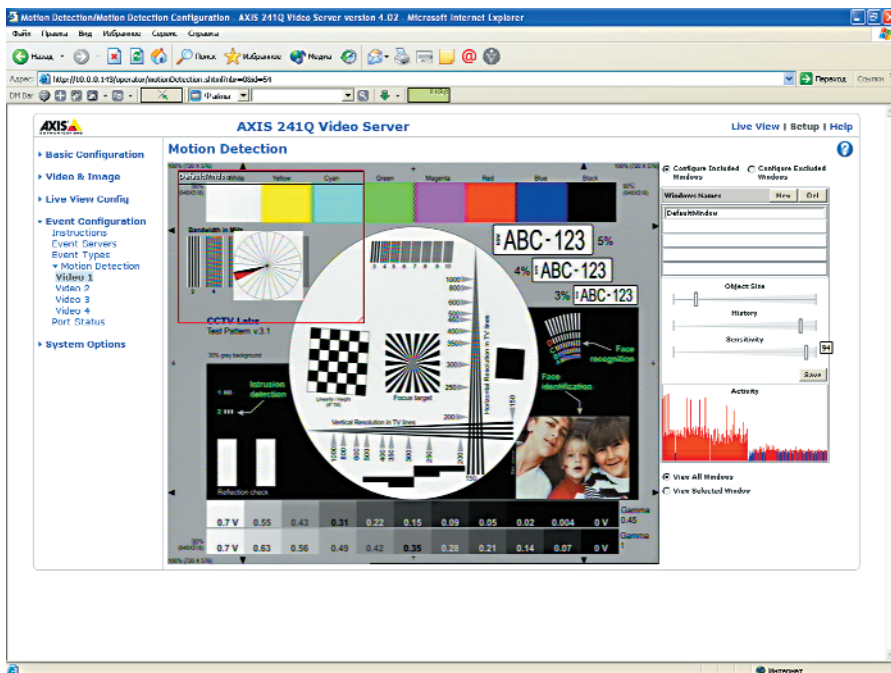
задать разрешение, настроить компрессию, выставить цветность и назначить титры. После этапа настройки автоматически генерируется код Java-скрипт. Применение данного кода позволит выводить ранее настроенное изображение на странице собственного сайта. На выбор предложено несколько форматов для вывода изображения (JPEG, Motion JPEG, Java Applet Motion JPEG video и Java Script update image).

Следующая группа полностью выделена под конфигурацию работы по событиям. На первом этапе настройки меню конфигураций по событиям требуется задать и настроить TSP, HTTP, FTP-серверы. Далее настраивается

событие (задается его название и выбирается приоритет). Следующим этапом настраивается период реакции триггера (всегда, по расписанию в установленный промежуток времени заданного дня, отсутствие реакции). Предлагается на выбор 5 инициаторов событий: внешнее срабатывание по 4 тревожным входам, команда оператора, потеря видеосигнала, срабатывание детектора движения и загрузка устройства. Если в качестве реакции на события выбрать отправку видеоизображения, то далее назначается пункт получения. При выборе в качестве адресата FTP-сервера потребуются назначить основной и дополнительный FTP-сервер, задать буфер предзаписи с выбором длительности промежутка между кадрами, буфер дозаписи с выбором длительности промежутка между кадрами, продолжительность сеанса отсылки с заданием времени или по активности триггера с выбором длительности промежутка между кадрами. По желанию, можно выбрать вариант названия кадра. Отсылаемое изображение может отличаться от текущего, и иметь другое качество. Возможность данной настройки также реализуется в описываемой закладке. Еще одной настраиваемой реакцией на событие может быть активизация тревожного выхода в течение задаваемого промежутка времени. Следующим шагом настраивается отсылка сообщений на адрес электронной почты, HTTP-сервер, или TCP-сервер с заданием адреса получателя и вводом



Дополнительные драйвера для PTZ-устройств доступны на сайте Axis Communication.



Настройка детектора движения.

текста сообщения. И в завершение задается предустановка для PTZ-устройства. PTZ-устройство будет автоматически обрабатывать данную предустановку при возникновении настраиваемого тревожного события.

Отдельное окно отведено под настройку реакций по расписанию, алгоритм настройки которых аналогичен вышеописанному.

Настройка детектора движения подразумевает выполнение стандартных для данной опции операций. Разработчики предлагают сконфигурировать до 10 активных зон, задавая их размер и перемещая по всему окну с видеоизображением. При необходимости зона может располагаться как внутри заданной границы, так и вне ее, исключая площадь внутри границы. Настройки детектора движения представлены настройкой чувствительности, настройкой минимального размера объекта и настройкой History, которая учитывает скорость перемещения объекта (длительность нахождения объекта в зоне поиска движения). График активности можно посмотреть в окне "Активность". Для большей точности мы предлагаем воспользоваться рекомендациями разработчиков в файле помощи.

И последней, но не менее важной группой, является группа системных настроек. По многим настройкам она дублирует предыдущие группы. Среди новых настроек отметим возможность фильтрации IP-адресов, более

подробные сетевые настройки, конфигурацию интерфейсов RS-232 и RS-455. В этой же группе предусмотрена возможность приведения видеосервера к заводским установкам и получения статистики по целому ряду параметров.

Возможны случаи, когда в используемом пользователем веб-браузере вводятся не все настройки, или выводятся, но в некорректной форме и не в полном объеме (это возможно при выборе веб-браузеров, на которые не распространяются рекомендации разработчиков, а так же при работе на КПК). В данном случае следует воспользоваться закладкой Plain Config, в

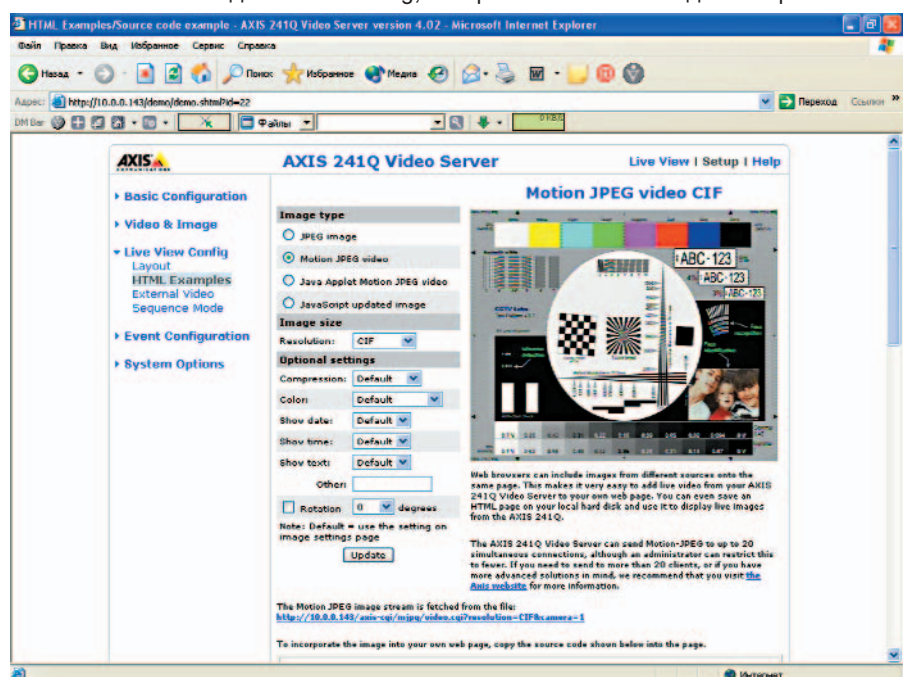
которой также доступны все ранее описанные настройки.

И не менее удобной является возможность самостоятельного редактирования всех скриптов встроенного веб-сервера. Конечно, данной опцией стоит пользоваться только опытным пользователям.

В данных видеосерверах реализована поддержка полнокадрового режима воспроизведения. Для полноценной работы рекомендуется использовать ПК с операционными системами Windows 98, Windows 2000, а также Windows XP. Более ограничены по возможностям будут пользователи операционных систем Linux, Unix, Mac OS и Mac OS X. В качестве веб-браузеров рекомендуется использовать Microsoft Explorer и Mozilla. Ограничения по функциональности накладываются на веб-браузеры Netscape и Opera.

Для приблизительного расчета выделяемого под видеоархив пространства разработчики в технической спецификации поместили график зависимости размера кадра от выбранной компрессии и разрешения видеокadra.

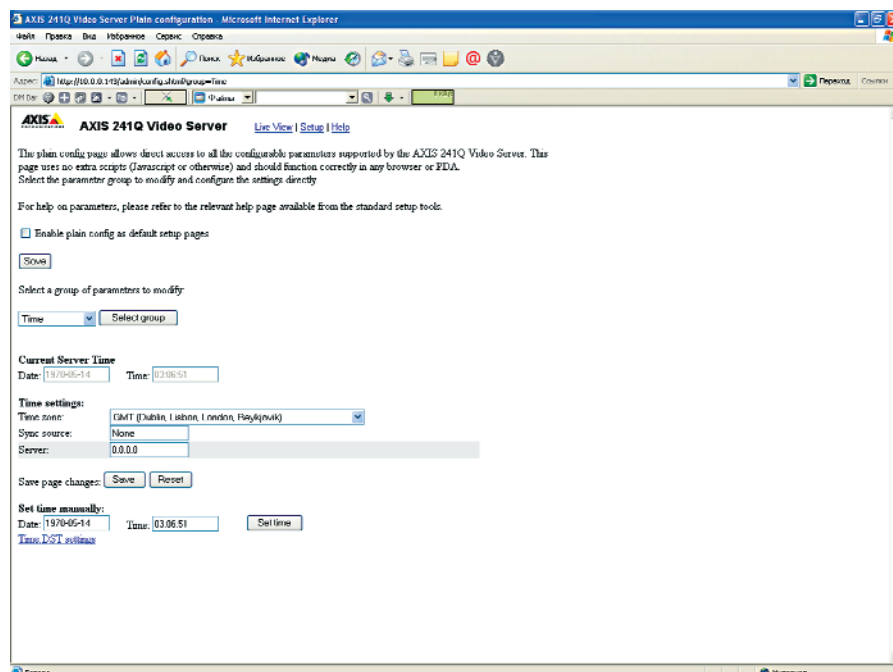
Что касается четырехканального видеосервера Axis 241Q, то факт наличия четырех видеовходов подразумевает его работу в режиме "квадро". Помимо данного режима, устройство поддерживает работу и в режиме переключения изображения от назначенных каналов и, соответственно, все свойственные Axis 241S режимы. Время задержки, в течение которого будет транслироваться только видеоизображение от



Страница настройки HTML Examples.

установленного канала, для каждого канала задается индивидуально. На странице Liverage добавилась возможность вывода изображения от всех четырех каналов одновременно в одном окне.

Для переключения в режим вывода изображения по выбранному каналу требуется выделить любой кнопкой мыши один канал из четырех, выводимых в режиме "квадро" либо выбрать его в выпадающей строке новой группы кнопок под заголовком Source. Там же размещена кнопка включения режима перелистывания и кнопка отмены данного режима. Для выводимого в режиме "квадро" видеоизображения добавилась новая закладка Quad Stream в группе настройки видеоизображения основного меню настроек. В этой закладке пользователь может назначить разрешение 4CIF (704x576) или CIF (352x288), а также выбрать требуемый уровень компрессии из пяти предложенных: Very low, Low, Medium, High, Very high. Кроме отмеченного, в закладке Quad Stream можно наложить ограничение на размер видеопотока и его скорость воспроизведения. В этой же группе добавились индивидуальные закладки для отдельной настройки каждого видеоканала, те же изменения произошли и в группе Basic Configuration. В группе Live View Config добавилась закладка Sequence Mode, в которой выбираются видеоканалы, от которых будет выводиться видеоизображение в активизированном режиме перелистывания, а также настраивается время переключения между каналами. Все настройки для каждого канала индивидуальны. Что касается настройки детектора движения в закладке Motion Detection группы Event Configuration, то теперь под данную настройку для каждого канала до-



Все настройки доступны на странице Plain Config.

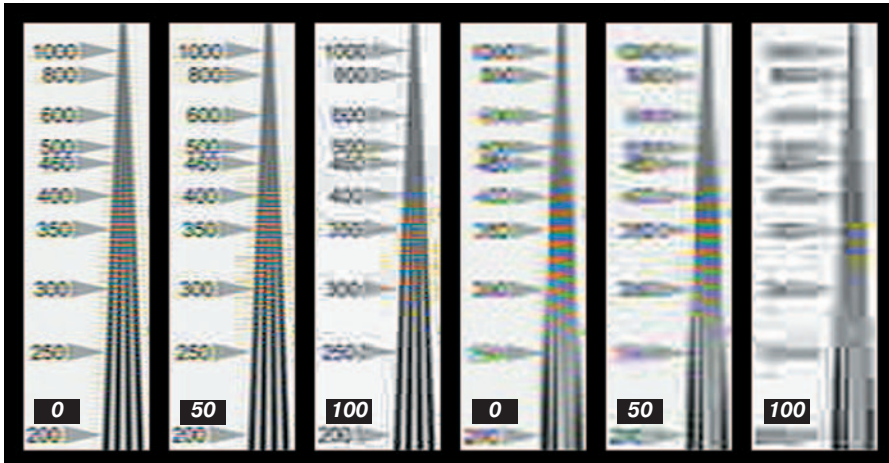
бавилась персональная страница.

Среди всех тестируемых видеосерверов Axis 241S и Axis 241Q позволили получить максимальное количество сессий с вполне приемлемыми показателями. Данные по тестированию Axis 241S сведены в отдельную таблицу.

Приведем данные по тестированию видеосервера Axis 241Q. С одной подключенной сессией, в режиме перелистывания интервал между выводами изображений от камер достигал 3с. Для режима "квадро" с разрешением 4CIF (704x576) при разных уровнях компрессии скорость воспроизведения имела следующие значения: 13 к/с для Very low, 12 к/с для Low, 11 к/с для Medium, 8 к/с для High и 7 к/с для Very high. Для режима "квадро" с разрешением 4CIF (704x576) при выборе монохромного изображения скорость воспроизведения была равна 16 к/с для Very low, 15 к/с для Low,

13 к/с для Medium, 11 к/с для High и 9 к/с для Very high. Разрешение выводимого цветного изображения по одному каналу при 4CIF (768x576) для уровня компрессии 0% и 50% составляет около 330 ТВЛ, для уровня компрессии 100% - около 310 ТВЛ.

В качестве итога, скажем, что компания Axis Communication и на этот раз не разочаровала нас. Тестируемым видеосерверам присуще большое количество возможностей, включая поддержку огромного числа протоколов связи управления поворотными телекамерами. Информацию по протоколам, как и дополнительные драйверы, выложена на сайте компании Axis Communication. Видеосерверы Axis 241S и Axis 241Q можно использовать как для локальных систем видеонаблюдения и архивации видеоданных, так и для построения распределенных систем. И этому способствует дополнительное программное обеспечение Axis Camera Explorer, Axis Camera Recorder, предлагаемое компанией Axis Communication. Большинство разрабатываемых устройств наделяет одинаковыми возможностями и практически идентичным интерфейсом программного обеспечения. Так что много дополнительной информации, отчасти относящейся и к данным видеосерверам можно почерпнуть из наших ранних публикаций.



Горизонтальное разрешение: размер кадра 768x576, уровень компрессии 0, 50, 100; размер кадра 384x288, уровень компрессии 0, 50 100.

MDW-100A

Название:	MDW 100A Web transmitter
Производитель:	MetaCom Electronics (MC Electronics)
Страна:	Корея
Сайт:	http://www.mcctv.ru (http://www.mcctv.com)
Видеовходы/видеовыходы:	1 BNC
Разрешение:	QVGA (320X240)
Стандарт видеосжатия:	MPEG-4
Скорость передачи:	25 к/с
Кол-во сетевых соединений:	10
Входы/выходы тревоги:	четыре/четыре
Разъемы:	RS-232/RS-485 (опция)
Сетевое подключение (протоколы):	10Base-T (TCP/IP, HTTP, SMTP, ARP, DNS, PPPoE, ICMP, FTP)
Безопасность:	Защита паролем на уровне пользователя, фильтрация IP-адресов
Системные требования:	Нет данных (тестировалось на Windows XP)
Програмное обеспечение:	Internet Explorer с ActiveX, AdminTool 4.41, WebCamViewer1CH 1.45, WebCamViewer4CH 1.45 и WebCamPlayer 1.45
Дополнительные возможности:	ПО для КПК с операционной системой WindowsCE, встроенный видеодетектор движения, 2 аудиоканала (прием/передача), PTZ-управление.
Размеры:	53x58x110мм
Источник питания:	12 В DC, внешний
Дополнительное ПО:	-

Формат сжатия	Разрешение кадра	Настройки качества	Скорость отображения к/с	Разрешение ТВЛ	Размер кадра
MPEG-4	320X240	Best	25	<200	82КБ
		Good	25	<200	46КБ
		Default	25	<200	13КБ
		Bad	25	<200	6КБ
		Worst	25	<200	3,5 КБ

VIP-10S

Название:	VIP 10S Network Video Server (VIP 10 Video Sender)
Производитель:	VCS Video Communication Systems AG
Страна:	Германия
Сайт:	http://www.vcs.com
Видеовходы/видеовыходы:	1 BNC
Разрешение:	Low 176 x 144 (QCIF), Standard 352 x 288 (CIF) и High 704 x 288 (2CIF)
Стандарт видеосжатия:	MPEG-4, Motion JPEG
Скорость передачи:	25 к/с для компрессии MPEG-4 при разрешении 704 x 288 (2CIF)
Кол-во сетевых соединений:	Не заявлено
Входы/выходы тревоги:	два/один
Разъемы:	RS-232/RS-422/RS-485, USB 2.0
Сетевое подключение (протоколы):	10/100Base-Tx (RJ-45)(RTP, Telnet, UDT, TCP, IP, HTTP, IGMP, ICMP, ARP, SNMP)
Безопасность:	Защита паролем на уровне пользователя
Системные требования:	Windows 9x/NT/2000/XP
Програмное обеспечение:	Internet Explorer v5.5 и выше, MPEGViewer (просмотр видеоархива), ActiveX Control
Дополнительные возможности:	разъем USB2.0 (планируется использовать для организации записи на внешний USB Flash Drive, для подключения внешнего модуля связи по сети WLAN), вывод панорамного изображения в верхней части Live page (для телекамер Sony EVI-D100 и Sony EVI-D30/31), 1 аудиоканал, PTZ-управление, настройка Multilink-Multicast (позволяет дублировать видеопоток сразу на несколько клиентов)
Размеры:	65x27x108мм
Источник питания:	24 В DC, внешний
Дополнительное ПО:	Комплект ПО VIDOS

Формат сжатия	Разрешение кадра	Скорость отображения к/с	Разрешение ТВЛ	Размер кадра
MPEG-4	Low 176 x 144 (QCIF)	25	<200	1.45КБ
	Standard 352 x 288 (CIF)	25	<200	2.1КБ
	High 704 x 288 (2CIF)	25	360	12КБ
M-JPEG	704x576	0.5	<200	26,4 КБ
	352x288	1	<200	26,4 КБ

В результате сохранения кадра при помощи кнопки snapshot, независимо от формата сжатия и заданного разрешения видеозображения, создается файл формата JPEG с разрешением 352x288, независимо от выбранной конфигурации с одинаковым качеством, разрешением менее 200ТВЛ и средним размером 26,4 КБ.

AXIS-241Q

Название:	AXIS 241Q Video Servers
Производитель:	Axis Communication
Страна:	Швеция
Сайт:	http://www.axis.com
Видеовходы/видеовыходы:	4 BNC
Разрешение:	4CIF (768x576), 2CIF Expanded (интерполированный до разрешения 768x576), 2CIF (768x288), CIF (384x288), QCIF (192x144); для режима Quad Stream 4CIF (704x576), CIF (352x288)
Стандарт видеосжатия:	Motion JPEG
Скорость передачи:	25 к/с (см. таблицу)
Кол-во сетевых соединений:	20
Входы/выходы тревоги:	четыре/четыре
Разъемы:	RS-232 (DB-9) и RS-485 (терминальный блок)
Сетевое подключение (протоколы):	10BaseT/100Base-TX (RJ-45) (TCP/IP, HTTP, FTP, SMTP, NTP, DHCP, ARP, BOOTP, HTTPS)
Безопасность:	Защита паролем на уровне пользователя, фильтрация IP-адресов, HTTPS криптографическая защита
Системные требования:	Windows 9x/NT/2000/XP, Linux, UNIX, Mac OS, Mac OS X
Програмное обеспечение:	Microsoft Explorer, Mozilla
Дополнительные возможности:	Поддержка WatchDog, PTZ-управление, поддержка UPnP, AXIS Dynamic DNS, встроенный видеодетектор движения, 64 МБ буфер предзаписи, 4 настраиваемые ссылки на Liveness, генерация кода на Java-скрипт для вывода видеоизображения на требуемой странице, отправка группы кадров на FTP-сервер, отсылка сообщений на e-mail, HTTP-сервер, TCP-сервер.
Размеры:	42x140x155 мм
Источник питания:	9В DC, внешний
Дополнительное ПО:	Axis Camera Explorer, Axis Camera Recorder

Разрешение кадра		4CIF (768x576) Цветной		4CIF (768x576) ч/б	
Формат сжатия	Компрессия	Разрешение ТВЛ	Скорость отображения к/с	Разрешение ТВЛ	Скорость отображения к/с
M-JPEG	Very low	<200	7	<200	9
	Low	<200	8	<200	11
	Medium	<200	11	<200	13
	High	<200	12	<200	15
	Very high	<200	13	<200	16

В режиме перелистывания интервал между выводами изображений от телекамер достигает 3с. Результаты тестирования приведены для режима "кадро", так как результаты тестирования одного канала полностью совпадают с результатами AXIS-241S.

AXIS-241S

Название:	AXIS 241S Video Servers
Производитель:	Axis Communication
Страна:	Швеция
Сайт:	http://www.axis.com
Видеовходы/видеовыходы:	1 S-Video, 1 BNC/1 BNC
Разрешение:	4CIF (768x576), 2CIF Expanded (интерполированный до разрешения 768x576), 2CIF (768x288), CIF (384x288), QCIF (192x144)
Стандарт видеосжатия:	Motion JPEG
Скорость видеопередачи:	25 к/с (см. таблицу)
Кол-во сетевых соединений:	20
Входы/выходы тревоги:	четыре/четыре
Разъемы:	RS-232 (DB-9) и RS-485 (терминальный блок)
Сетевое подключение (протоколы):	10BaseT/100Base-TX Интернет (RJ-45) (TCP/IP, HTTP, FTP, SMTP, NTP, DHCP, ARP, BOOTP, HTTPS)
Безопасность:	Защита паролем на уровне пользователя, фильтрация IP-адресов, HTTPS криптографическая защита
Системные требования:	Windows 9x/NT/2000/XP, Linux, UNIX, Mac OS, Mac OS X
Програмное обеспечение:	Microsoft Explorer, Mozilla
Дополнительные возможности:	Поддержка WatchDog, PTZ-управление, поддержка UPnP, AXIS Dynamic DNS, встроенный видеодетектор движения, 32 МБ буфер предзаписи, 4 настраиваемые ссылки на Liveness, генерация кода на Java-скрипт для вывода видеоизображения на требуемой странице, отправка группы кадров на FTP-сервер, отсылка сообщений на e-mail, HTTP-сервер, TCP-сервер.
Размеры:	42x140x155 мм
Источник питания:	9 В DC, внешний
Дополнительное ПО:	Axis Camera Explorer, Axis Camera Recorder

Разрешение кадра		4CIF (768x576)		2CIF Expanded		CIF (384x288)	
Формат сжатия	Компрессия	Разрешение ТВЛ	Скорость отображения к/с	Разрешение ТВЛ	Скорость отображения к/с	Разрешение ТВЛ	Скорость отображения к/с
M-JPEG	0	330	18	330	23	<200	25
	50	320	24	320	25	<200	25
	100	300	25	300	25	<200	25



Видеосервер Domination

У каждой компании-производителя есть особые дни в году. Например, юбилеи или, скажем, выставки. Выставку можно сравнить с олимпиадой. К ней все подходят ответственно, готовятся задолго до её начала. И фавориты всегда заранее всем известны. А вот кто из "серых лошадок" завоюет олимпийские медали, предсказать никто не берётся. Вот и до форума "Охрана и безопасность 2004" в Санкт-Петербурге никто не знал компанию "ВИПАКС" из Перми как серьёзного производителя цифровых систем видеонаблюдения. И вручение премии "Эталон Безопасности 2004" их видеосерверу Domination для всех стало полной неожиданностью. Именно тестированию этой новой для российского рынка системы видеонаблюдения и посвящена наша статья.

Компания "ВИПАКС" существует на рынке систем безопасности с 1996 года и достаточно известна в качестве поставщика оборудования электронных систем безопасности в Пермской области. До международного форума "Охрана и безопасность 2004", данная компания продвигала на рынке охранного телевидения продукцию других производителей, в том числе и компаний, бренды которых у всех на слуху. А на последнем международном форуме "Охрана и безопасность 2004" компа-

ния "ВИПАКС" представила продукт собственного производства. И сразу же их новинку ожидал успех. Диплом победителя конкурса "Эталон безопасности 2004" в номинации "Охранное телевидение и наблюдение" - неплохой старт.

Компания "ВИПАКС" предлагает линейку многоканальных видеосерверов Domination на 4, 6, 8, 16 видеоканалов. В дополнение к этому, потребитель получает еще по паре аудиоканалов на каждом из устройств.

В компании "ВИПАКС" любезно откликнулись на наше предложение провести тестирование многоканального видеосервера Domination.

В нашу тестовую лабораторию в оперативном порядке были доставлены целых два устройства: шестиканальный видеосервер Domination MV-6 и восьмиканальный видеосервер Domination MV-8.

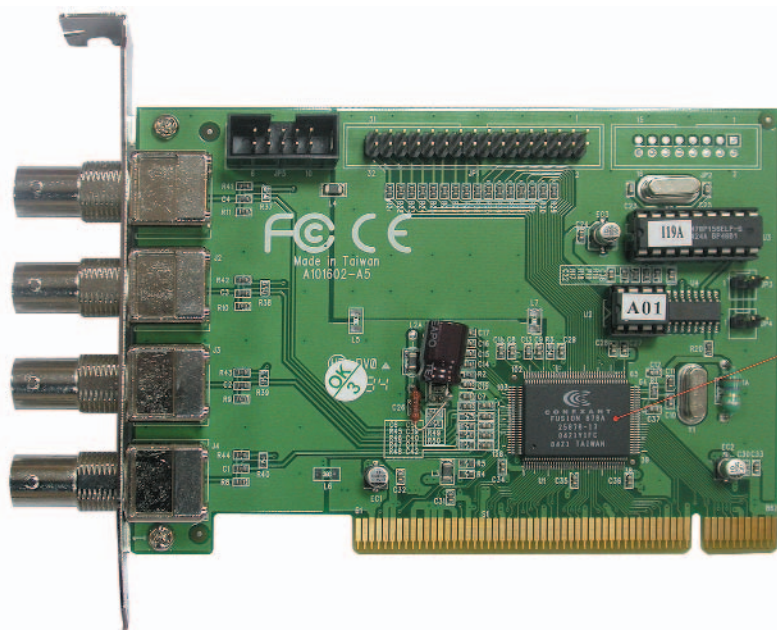
Цифровые видеосерверы выполнены на базе ПК, MV-6 - в корпусе Slim PC (формат Flex ATX), а MV-8 - в настольном корпусе.

В видеосервере MV-6 установлено 3 двухканальные платы видеоввода, на каждой из которых находится по 2 композитных видеовхода с разъемами RCA и по одному входу S-Video, который является опцией и не используется. Для оцифровки видеопотока ис-

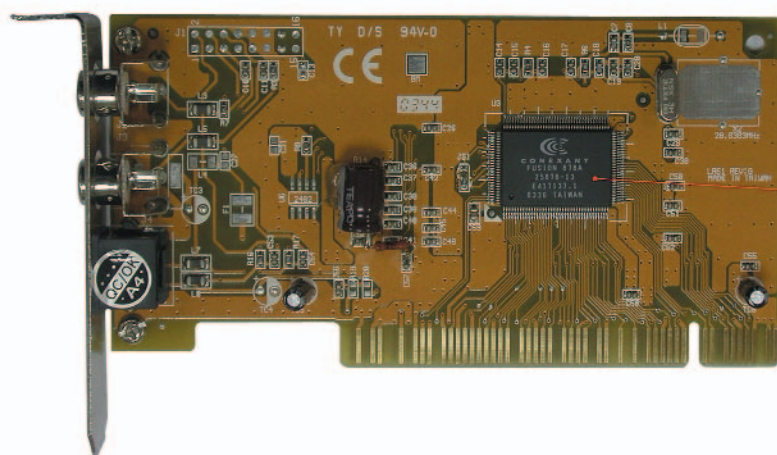
пользуются установленные на каждой плате по одному АЦП Fusion 878A производства компании Conexant.

В видеосервере MV-8 установлено уже 4 четырехканальные платы видеоввода и оцифровки, на каждой из которых размещено по 4 композитных видеовхода с разъемами BNC и по одному АЦП Fusion 878A производства компании Conexant.

Внутри корпуса каждого видеосервера установлен флэш-носитель и USB-ключ защиты. Программное обеспечение видеосервера и операционная система Linux находятся на флэш-носителе. Флэш-память, в отличие от жестких дисков, не подвержена механическому износу в процессе эксплуатации. Кроме физических повреждений, возможны сбои в файловой системе диска (например, из-за проблем с электропитанием), и, как следствие, сбой в программном обеспечении или операционной системе. Флэш-носитель разбит на два раздела. На первом разделе, с которого разрешено только чтение информации (а значит, исключено возникновение сбоя файловой системы), находятся операционная система и программное обеспечение, а на следующий раздел записываются все настройки видеосервера. На USB-ключе защиты записан программный код, который является ключом, служа-



АЦП Conexant Fusion 878A



АЦП Conexant Fusion 878A

щим для авторизованного доступа к цифровому видеосерверу.

Встроенный архив восьмиканально-го видеосервера MV-8 может размещаться на 4 жестких дисках и составлять 800 гигабайт. Есть также версия видеосервера MV-8 со съемным жестким диском (но тогда используется только один жесткий диск и устанавливается пользователем). На шестиканальном видеосервере MV-6 объем архива уже определяется емкостью жесткого диска, который пользователь может самостоятельно поместить в устройство. В шестиканальном видеосервере MV-6 имеется только специальный отсек, в который устанавливается съемный контейнер с помещенным в него жестким диском. На всех жестких дисках используется файловая система ext3. Для чтения видеоархива, ранее записанного на помещенный в съемный контейнер жесткий диск, производитель предлагает дополнительное устройство (Play Module). Данный модуль является са-

мостоятельным устройством. Используя его, пользователи получают такие же возможности для работы с архивом, как если бы жесткий диск с записанным на нем архивом размещался в самом видеосервере.

Что касается требований к клиентскому компьютеру для работы с видеосервером Domination, то они следующие:

- Операционная система Windows XP Professional или Windows 2000 с установленным DirectX версии 8.1 и выше;
- Процессор - Celeron 1.7 ГГц (рекомендуется Celeron 2.6 ГГц);
- Оперативная память - 256 МБ;
- Свободное место на диске - 200 МБ;
- Видеокарта - 32 МБ с поддержкой 32-битного цвета;
- Сетевая плата - 10/100 Мбит/с;
- Звуковая карта - если требуется звуковое сопровождение работы ПО Domination.

Перечислим заявленные компанией-производителем возможности сис-

темы видеонаблюдения Domination:

- Триплексная система. Одновременная запись видеоинформации на жесткий диск, просмотр текущей видеоинформации и просмотр архива.
- Собственный алгоритм покадрового сжатия видеоизображение на основе компрессии JPEG.
- Триплексная система. Одновременная запись видеоинформации на жесткий диск, просмотр текущей видеоинформации и просмотр архива.
- Высокое качество записи видеоинформации с разрешением до 768x576 точек с возможностью регулировки скорости записи и степени сжатия.
- Запись аудиоинформации.
- Видеосервер комплектуется сетевым программным обеспечением с лицензией на неограниченное количество рабочих мест.
- Возможность объединения в локальную сеть практически неограниченного количества видеосерверов.
- Программное обеспечение видеосервера и ОС Linux находятся на

флэш-носителе, жесткий диск используется только для записи видеоархива, что исключает возможность выхода сервера из строя по причине сбоя диска.

- Мультизонный детектор движения (432 зоны), настраиваемый для конкретной задачи по чувствительности и области обнаружения.

- Съёмный диск для создания архива видеoinформации.

- Регламентированный многопользовательский доступ к ресурсам системы.

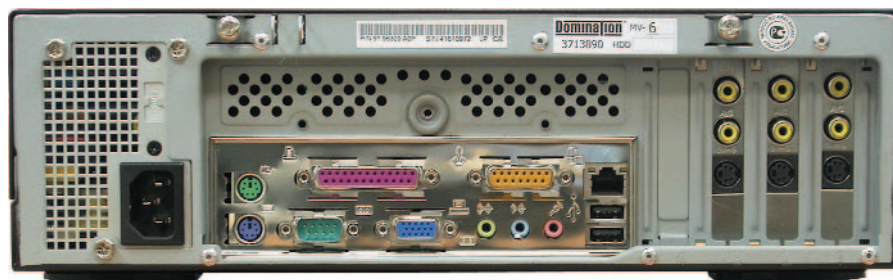
- Возможность настройки яркости, контрастности, цветности как при просмотре "живого" видео, так и при воспроизведении архива.

- Экспорт записей с видеосервера за любой промежуток времени.

- Быстрый поиск в архиве видеозаписей по дате и времени. Ускоренное и замедленное воспроизведение видеозаписи вперед и назад.

- Управление поворотными устройствами и скоростными купольными камерами с компьютера-клиента.

Архитектурно система видеонаблюдения Domination состоит из нескольких цифровых видеосерверов и локальных ПК с установленным на них клиентским ПО. При этом добавление нового цифрового видеосервера в систему видеонаблюдения возможно в любой момент и не требует никаких изменений в уже существующей структуре. Это позволяет строить как простейшие локальные системы видеонаблюдения, так и сложные распределенные.



Основная задача видеосервера при этом заключается в одновременной передаче видеоизображений от различных источников видеосигналов множеству компьютеров-клиентов.

Различные пользователи испытывают несовпадающие потребности в просмотре тех или иных телекамер. Каждый компьютер-клиент имеет свою производительность (которая вследствие трудоемкости задач декомпрессии зачастую оказывается недостаточной для вывода всех видеоизображений с максимальной скоростью) и пропускную способность канала связи, соединяющего клиента с видеосервером. Как следствие, видеопотоки, передаваемые цифровым видеосервером различным клиентам, в общем случае не совпадают как по содержанию, так и по скорости.

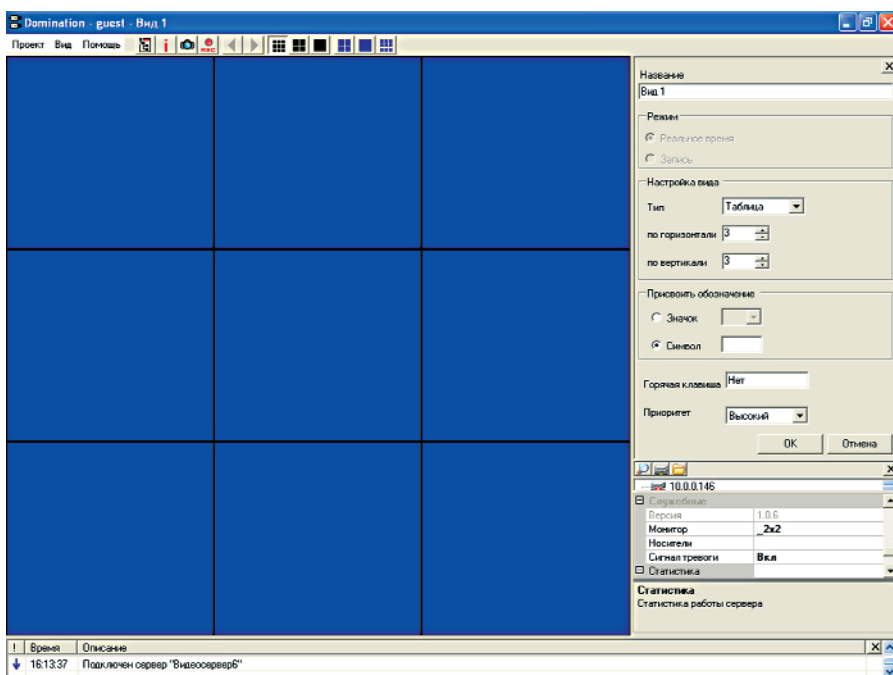
Отличительной особенностью данной системы является то, что видеопоток с видеосервера передается на каждый компьютер-клиент без уменьшения разрешения изображения. А пользователь на локальном рабочем месте имеет возможность в частном порядке настроить выводимое на клиентском ПО изображение в соответствии с ин-

дивидуальными потребностями, а также возможностями своего ПК.

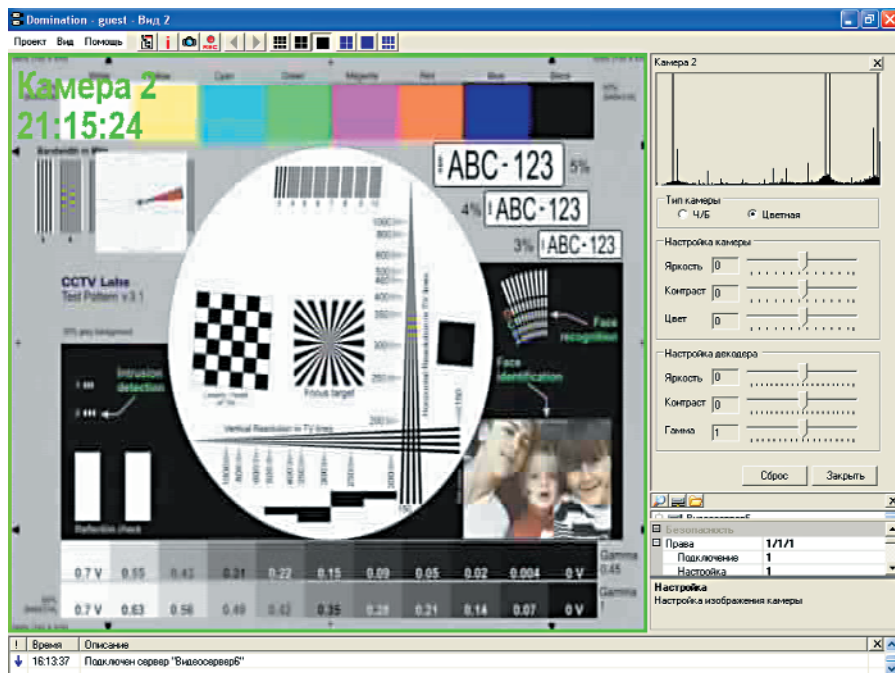
Для каждого видеоканала пользователь может ограничить скорость просмотра, снизив при этом число получаемых кадров, а значит и нагрузку на сеть. Благодаря этому число видеосерверов, к которым одновременно подключен пользователь на локальном рабочем месте, и число просматриваемых видеоканалов можно регламентировать в соответствии с решаемыми на рабочем месте задачами.

Ядро операционной системы видеосервера не содержит ничего лишнего и оптимизировано под выполнение только поставленных задач, а значит, более устойчиво к сетевому взлому. Все действия пользователей по настройке системы могут быть жестко регламентированы, вывести видеосервер из строя или уничтожить видеоархив можно только путем непосредственного физического воздействия. Видеоархив перезаписывается автоматически, "по кругу", и даже администратор системы не может удалить или подменить какую-либо часть видеоархива.

В многоканальном видеосервере Domination сетевая производительность обеспечивается программным обеспечением, работающим под управлением ОС Linux и в большей мере зависит от пропускной способности подключенного канала связи. Все операции по просмотру изображений и настройке системы осуществляются с компьютера-клиента, что освобождает некоторые ресурсы сервера от необходимости обслуживания графического интерфейса. В программном обеспечении как видеосервера, так и видеоклиента широко используются технологии MMX. Это позволяет достичь высоких скоростей цифровой обработки видеoinформации. Благодаря использованию журналируемой файловой системы и реализации алгоритмов быстрого восстановления структуры данных, находящихся на жестком диске. В случае пропадания электропитания из видеоархива "выпадает" лишь



Настройка вида.



Настройка изображения

та часть времени, которая требуется на загрузку сервера.

В отдельных случаях клиентское рабочее место можно использовать лишь для настройки видеосервера и просмотра/экспорта видеоархива. Видеосервер предоставляет возможность организации рабочего места наблюдателя (путем подключения к нему монитора). При этом интерфейс локального пользователя жестко защищен от вмешательства в работу системы, а пользователю предоставляются только функции видеонаблюдения в реальном масштабе времени.

Многоканальный видеосервер Domination является законченным, полностью готовым к работе устройством. Все операции по установке сводятся к подключению источников видеосигнала и кабеля компьютерной сети к видеосерверу. Видеосервер комплектуется сетевым ПО с лицензией на неограниченное количество рабочих мест.

На первом этапе установки клиентского ПО устанавливается платформа Microsoft .NET Framework. Microsoft .NET Framework - это платформа, упрощающая создание распределенных приложений.

Компания "ВИПАКС" предложила нам две версии клиентского ПО Domination (версии 1.1.7 и 1.1.8). И хотя в версии 1.1.8 еще были недоработки, нам вдвойне было интересно протестировать именно данную версию ПО.

С помощью ПО Domination можно просматривать видеoinформацию и

прослушивать звук, осуществлять настройку видеосервера, распределять права доступа.

Перед установкой клиентского ПО мы внимательно ознакомились с руководством пользователя, а в ходе установки программного обеспечения, нами были учтены и выполнены все требования разработчиков, включая закрытие всех антивирусных программ.

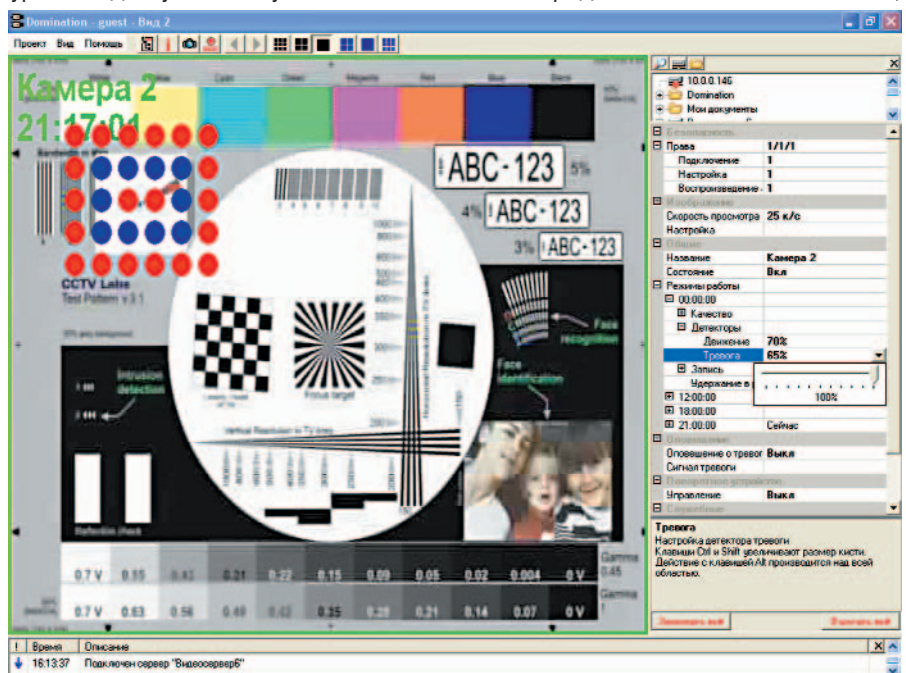
Установка программного обеспечения прошла без осложнений.

При запуске программного обеспечения появится диалоговое окно авторизации пользователя. Минимальными правами обладает пользователь с уровнем доступа 1. По умолчанию его

имя и пароль будут guest. Максимальный уровень доступа 11. По умолчанию это пользователь с именем root и паролем masterkey. Уровень доступа на все ресурсы системы предварительно установлен равным 1. Таким образом, при первом запуске программы Domination, независимо от того под каким из имен входит пользователь, ему будут доступны все настройки системы (кроме возможности добавлять новых пользователей при авторизации под именем guest).

Основную часть рабочего окна программы занимает окно для отображения телекамер. Под данным окном располагается окно событий, справа - окно панели управления, а сверху - строка с кнопками вызова подменю и функциональными кнопками.

На первом этапе работы требуется создать так называемый вид, в котором пользователь должен сконфигурировать основной рабочий интерфейс и осуществить настройки для назначенных телекамер по заданным или найденным цифровым видеосерверам и локальным хранилищам архива. Создаются отдельные виды для разных конфигураций окон выбранных видеоканалов как для работы с "живым видео", так и для работы с архивами. После создания и настройки вида, осуществляется автоматический поиск видеосерверов, находящихся в пределах локальной сети. Если видеосервер находится в сети Интернет, то для подключения к нему требуется указание его IP-адреса. Далее определяются активные каналы,



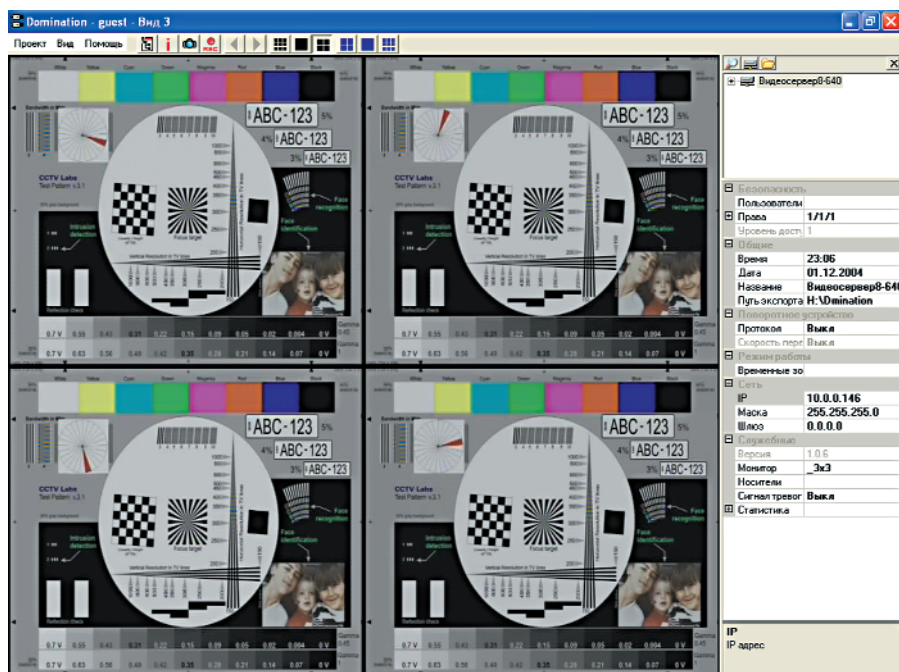
Настройка чувствительности для тревоги.

которым назначаются окна для вывода видеоизображения. Это можно осуществить путем перетаскивания мышкой иконки с требуемым видеоканалом на рабочий стол. Таким же способом можно менять расположение окон с выводимым видеоизображением в основном окне и изменять порядок расположения иконок видов.

Клиентское программное обеспечение выполнено в виде одиночного приложения, в котором позволено просматривать как "живое" видео, так и воспроизводить архив. Из него же осуществляются и все настройки системы.

Важной особенностью интерфейса программы является то, что служебные окна никогда не заслоняют видеоизображение. При вызове меню настроек окно вывода видеоизображения лишь смещается, и оператор системы не теряет из поля зрения ситуацию на объекте. Расположение на экране клиента окон с выводимым видеоизображением является совершенно произвольным.

Само программное обеспечение Domination работает в режиме "поверх всех окон". Для вывода на экран любого другого приложения необходимо свернуть окно программы Domination. Режим работы "поверх всех окон" позволяет пользователю одновременно с выполнением задачи видеонаблюдения работать с различными офисными приложениями. Данная функция необходима пользователям, для которых видеонаблюдение является второстепенной задачей. В программном обес-



Настройка вида.

печении реализованы алгоритмы автоматической адаптации к производительности компьютера-клиента, чтобы работа программного обеспечения Domination не мешала работе в других приложениях.

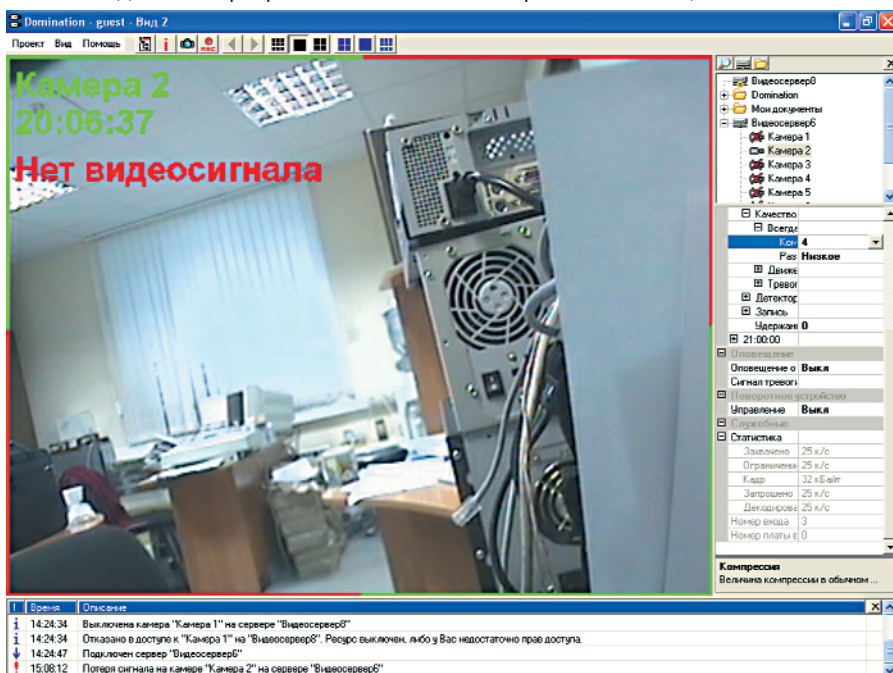
Клиентское программное обеспечение также может работать в полноэкранном режиме, когда выводятся только ячейки с видеоизображениями (переход по Alt+Enter) и в режиме, при котором вся площадь экрана, кроме верхних двух строк с кнопками управления, занята ячейками с видеоизображениями. В этом режиме недоступным становится лишь осуществление настроек системы, а все основные

действия (переключения от одного вида к другому, цифровое увеличение, управление поворотными камерами, ведение "горячей записи", сохранение снимков) пользователь может выполнять, не меняя режима.

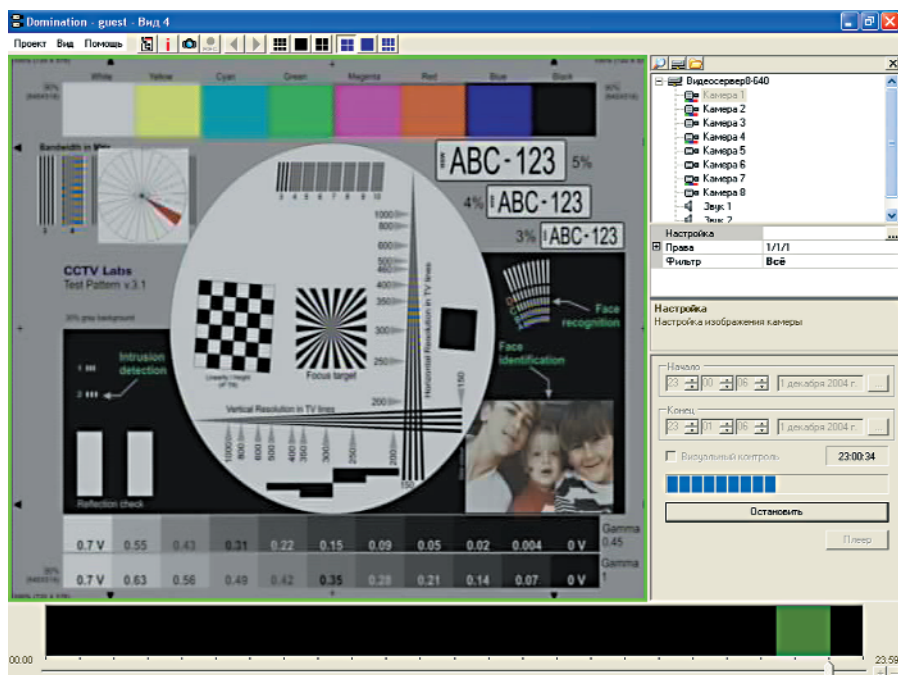
В отдельно сконфигурированном для этого виде пользователь может просматривать видеоархив с цифрового видеосервера, а также экспортировать его на требуемый носитель с возможностью дальнейшего просмотра.

В то время как запись видеоизображений на видеосервере ведется по настройкам телекамер, пользователь может также запустить (путем нажатия кнопки "REC" или горячей клавиши R) "горячую" запись только выбранной телекамеры. Архив при этом будет записан на жесткий диск компьютера-клиента. "Горячая запись" никак не связана с записью, которая осуществляется на видеосервере, и ведется со скоростью получения кадров клиентом. Это удобно, когда пользователь в процессе мониторинга решил заархивировать наблюдаемое им событие и не уверен в том, что на цифровом видеосервере организована непрерывная запись.

В последнее время обязательным атрибутом систем видеонаблюдения является возможность управления поворотными телекамерами. В клиентском программном обеспечении Domination управление поворотными телекамерами осуществимо как с клавиатуры, так и с помощью мыши. Использование мыши очень удобно: смещение курсора от



Потеря видеосигнала.



Экспорт видеоархива.

центра изображения задает направление, а величина смещения - скорость поворота. Также с помощью мыши доступно управление функцией приближения и фокусировкой телекамеры. С клавиатуры, помимо функций управления, доступна ещё и работа с предустановками. Из клиентского программного обеспечения возможна и работа со встроенным меню телекамеры. При данных возможностях отпадает необходимость в приобретении дорогостоящего пульта управления.

Для выполнения действий по настройке системы пользователь должен авторизоваться под именем с достаточным уровнем доступа. Большая часть настроек системы выполняется из основной панели настроек.

Основная панель настроек вызывается и убирается с помощью кнопки в строке меню программы. Основная панель настроек делится на две части: в верхней отображаются видеосерверы Domination, присутствующие в сети, и подключенное к ним оборудование, в нижней - доступные настройки в зависимости от выбранного объекта. Положение раздвигательной черты между верхней и нижней частью может быть настроено с помощью мыши. Так же может быть изменена ширина панели настроек.

Панель настроек имеет привычную древовидную структуру. Нажатие на значок "+" открывает подчиненные пункты, нажатие на значок "-" - сворачивает.

Отдельно настраивается видеосер-

вер, отдельно - телекамеры и аудиоканалы. Кратко перечислим основные настройки: настройка прав доступа к серверу и списка пользователей, настройка расписания работы цифрового видеосервера (временные зоны), сетевые настройки цифрового видеосервера, настройка монитора сервера (задается вид мультикартины на мониторе, подключенном непосредственно к серверу), просмотр состояния встроенных носителей.

Что касается основных настроек телекамеры, то они представлены разграничением прав доступа к телекамере, параметрами изображения, общими настройками телекамеры, настройками видеодетектора движения и тревоги, настройками степени компрессии и разрешения, настройками режимов записи телекамеры и настройками длительности удержания в режиме тревоги.

Отдельно настраиваются аудиоканалы и ряд других параметров. Пользователь может сохранить все настройки и конфигурации.

Особо следует отметить, что в клиентском ПО настройки яркости/контраста осуществляются отдельно для цифрового видеосервера и для клиента. Настройки декодера клиента никак не влияют на изображение записываемое или передаваемое другим клиентом, зато позволяют подстроить изображение под субъективные пожелания пользователя.

Непрерывное ведение записи на встроенный архив видеосервера орга-

низовано по "кольцевому" способу, когда самая первая запись затирается, а ее место занимает текущая.

Каждый видеокادر захватывается в оперативную память, после чего, если необходимо, выводится на монитор видеосервера (режим Overlay при этом не используется), записывается на диск или передается по сети на удаленные рабочие места с установленным клиентским ПО. Настройка компрессии одинакова для записи и клиентов. Изображение сжимается с установленным качеством, после чего записывается и передается всем запрашивающим его клиентам.

В видеосервере существует возможность настройки автоматического изменения разрешения, степени сжатия и скорости записи индивидуально для каждого видеоканала, в зависимости от событий и текущего времени, что позволяет гибко подобрать соотношение качество/размер архива согласно потребностям пользователя.

Пользователю предоставлена возможность экспорта записей из оперативного архива видеосервера за любой промежуток времени на любой носитель информации, что позволяет создавать архивы длительного хранения на компьютерах-клиентах, файловых серверах и т.п., а в дальнейшем просматривать экспортированный архив. В клиентском ПО Domination данный архив называется локальным хранилищем.

ПО видеосервера и видеоклиента обеспечивает быстрый поиск записей по дате, времени, событиям, мгновенный выход на заданную точку воспроизведения. Пользователю доступно ускоренное, замедленное, синхронное, пок кадровое воспроизведение записи вперед-назад. Еще одной особенностью системы видеонаблюдения Domination является обеспечение синхронизированного воспроизведения записей не только между телекамерами, но и между несколькими видеосерверами, а также экспортированными архивами. Эта функция незаменима, например, при анализе событий, когда объект перемещался из поля зрения телекамер одного сервера в поле зрения телекамер, подключенных к другому серверу.

Что касается организации записи, то в системе видеонаблюдения Domination предложена следующая концепция.

Пользователь задает до 4 временных зон. Несколько временных зон

позволяют в дальнейшем индивидуально для каждой из них настроить работу детектора движения, скорость записи и отображения и ряд других параметров.

Для выбранной временной зоны можно задать любой из трех режимов записи: "Всегда", "Движение", "Тревога". Далее задается требуемая скорость записи, разрешение и уровень компрессии. И это все по каждому видеоканалу в отдельности. К примеру, требуется организовать охрану автомобиля. В настройках видеодетектора движения задается зона по всей площади автомобиля, зона-тревога, а вокруг автомобиля обрисовывается зона-активность. Далее мы можем настроить видеоканал таким образом, что вся активность вокруг автомобиля записывается с одним качеством и скоростью, а при тревоге качество и скорость записи увеличиваются. Таким образом, мы имеем записанные в архив все действия, предшествующие тревоге и после нее. Также отдельно задается время удерживания режима тревоги.

Просмотр записи, которая велась с высокой скоростью, немного медленнее вследствие ограничений, накладываемых каналом связи и ограниченности ресурсов сервера. Когда ведется просмотр архива, остальные задачи (захват, компрессия, запись, передача по сети другим клиентам) не останавливаются. При этом зачастую запись воспроизводится неравномерно. Неравномерности легко избежать, принудительно установив скорость просмотра.

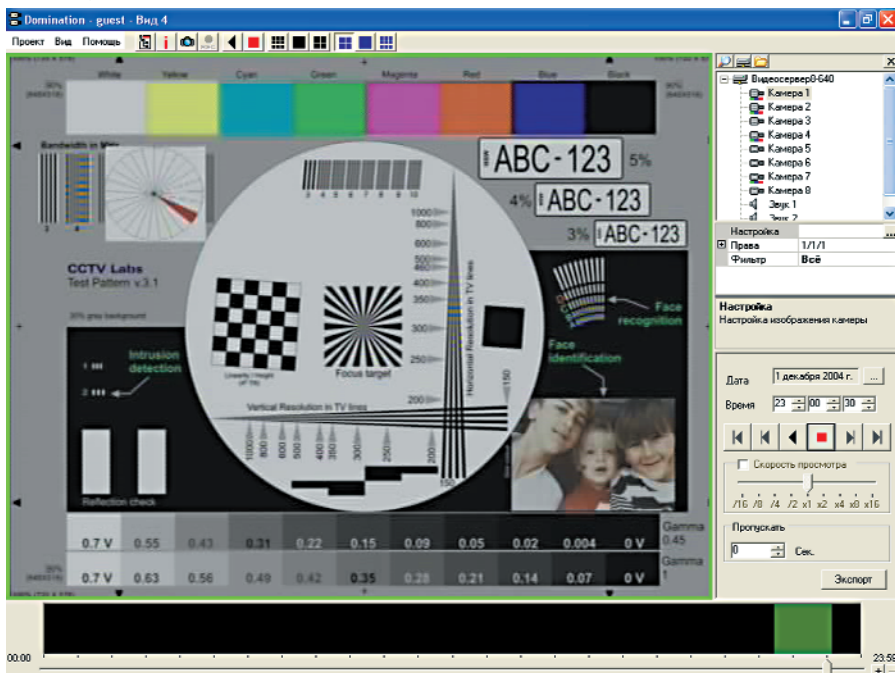
При тестировании многоканальных видеосерверов мы использовали видеосигнал с тестового генератора со статичным изображением тестовой таблицы и динамическое видеоизображение с телевизионной телекамеры. Поскольку при равных условиях оба цифровых видеосервера по одинаковым параметрам давали одинаковые результаты, мы решили провести более глубокое тестирование цифрового видеосервера MV-8.

Установленные в видеосервер платы видеоввода и оцифровки поддерживают только режим мультимплексирования, что дает суммарную скорость 16 к/с на один чип оцифровки. Система выполняет автоматический деинтерлейсинг. Работая с одним видеоканалом при выбранном разрешении "Высокое" (768x576 пикселей), клиентское ПО декодирует видеоизображение с максимальной скоростью 12 к/с. Такая же скорость и при отображении видеоизображения. При этом эффект гребенки не наблюдается, а максимальное горизонтальное разрешение цветного изображения составляет 340 ТВ-линий. При выборе "Среднего" разрешения (768x288 пикселей) скорость декодирования, как и скорость отображения, возрастает до 25 к/с. В данной конфигурации горизонтальное разрешение остается без изменения, а вертикальное соответственно падает ввиду того. Выбирая значение разрешения "Низкое" (384x288 пикселей), пользователь получает все ту же скорость 25 к/с на декодировании и на отображение, а также и горизонтальное

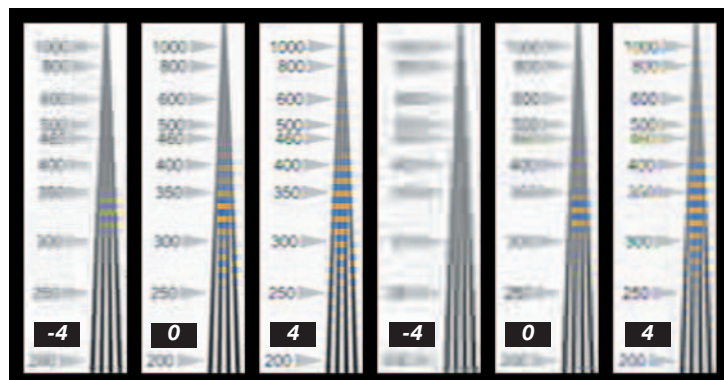
разрешение около 200 ТВ-линий. Для каждого из разрешений можно выбрать индивидуальный уровень компрессии из 9 предложенных, что отразится на качестве видеоизображения и размере кадра.

Результаты тестирования сведены в отдельную таблицу. При этом можно сказать, что все они оказались вполне предсказуемыми и стабильными. Система, как и предполагалась, всецело зависит от пропускной способности сети, загруженности ресурсов как самих видеосерверов, так и клиентских рабочих мест. Что касается горизонтального разрешения, то максимальное значение в 340 ТВ-линий является хорошим результатом при использовании режесторного фильтра для видеостандарта PAL. По сведениям, полученным от разработчиков, в перспективе планируется переводить систему на платы видеоввода, на которых будут установлены АЦП с гребенчатым фильтром для видеостандарта PAL. Переключение в настройках видеоканала с цветного видеоизображения на черно-белое на результатах тестирования не отразилось. По всем тестируемым параметрам, остались такие же значения, которые имели место для цветного видеоизображения.

Мы высоко оценили логичное построение и алгоритмы взаимной работы многоканальных видеосерверов и клиентских рабочих мест с установленным на них ПО Domination. Интерфейс программного обеспечения прост и интуитивно понятен. Предоставляя удобное рабочее место оператора, производители также постарались максимально сократить возможность влияния человеческого фактора, переводя работу системы в автоматический режим. Хотелось отметить оперативность ответов представителей компании на заданные нами вопросы, а также достаточную информативность всех предоставленных материалов. И особенно поблагодарить ведущего программиста проекта Domination Новикова Сергея за проведение телефонных консультаций по функциональности как тестируемых видеосерверов, ПО, так и системы в целом. Отдельную благодарность мы выражаем руководству компании "ВИПАКС" в лице Осина Андрея за оперативно предоставленное для тестирования оборудование.



Просмотр видеоархива.

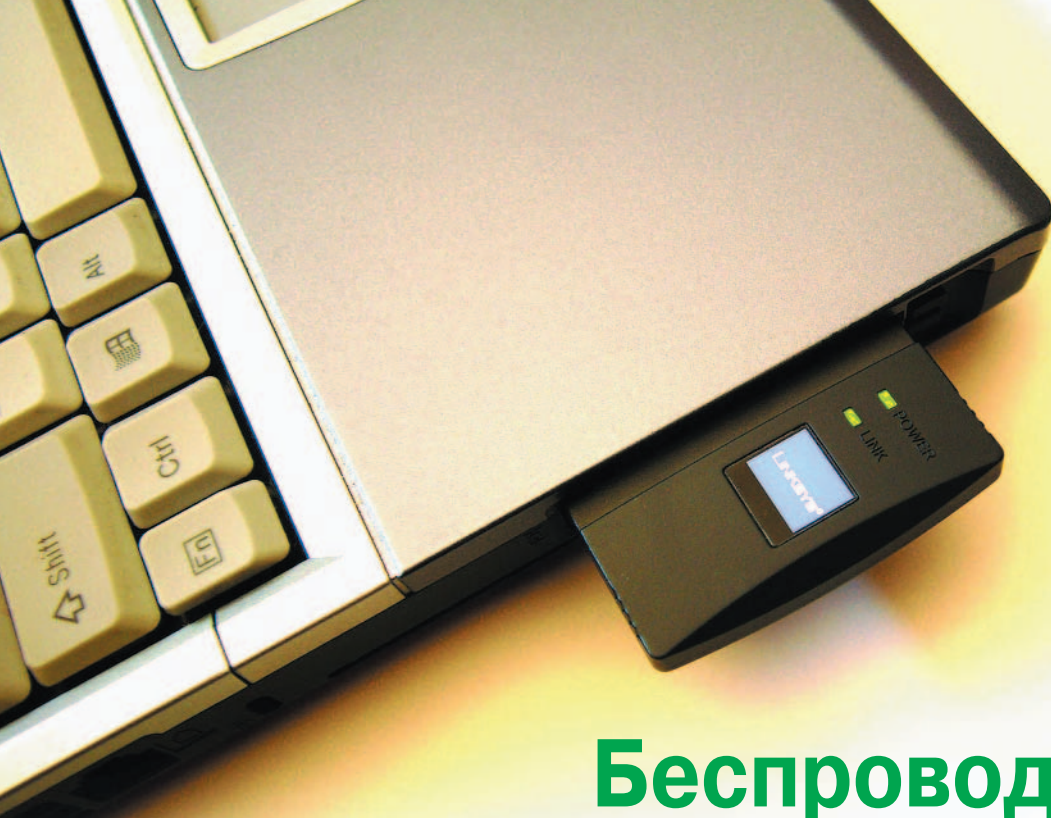


Горизонтальное разрешение:
размер кадра 768x576,
уровень компрессии - 4 (наибольшая), 0, 4 (наименьшая);
размер кадра 384x288,
уровень компрессии - 4 (наибольшая), 0, 4 (наименьшая).

Для разрешения Высокое (768x576 пикселей) горизонтальная разрешающая способность составляет порядка 340 ТВ-линий.
Для разрешения Низкое (384x288 пикселей) - менее 200 ТВ-линий.

Реальная сцена							
Количество каналов	Уровень компрессии	Разрешение					
		Высокое		Среднее		Низкое	
		скорость отображения к/с	размер кадра КБ	скорость отображения к/с	размер кадра КБ	скорость отображения к/с	размер кадра КБ
1	-4	12	19	25	9	25	5
	-3	12	24	25	12	25	6
	-2	12	28	25	14	25	8
	-1	12	31	25	15	25	9
	0	12	36	25	17	25	10
	1	12	41	25	21	25	12
	2	12	48	25	26	25	15
	3	12	74	25	36	25	21
	4	12	145	25	70	25	42
8	-4	2	21	7	10	8	6
	-3	2	28	7	13	8	8
	-2	2	31	7	15	8	9
	-1	2	35	7	17	8	10
	0	2	41	7	20	8	12
	1	2	49	7	24	8	14
	2	2	55	7	28	8	17
	3	2	77	7	39	8	23
	4	2	161	7	78	8	46

Тестовая таблица							
Количество каналов	Уровень компрессии	Разрешение					
		Высокое		Среднее		Низкое	
		скорость отображения к/с	размер кадра КБ	скорость отображения к/с	размер кадра КБ	скорость отображения к/с	размер кадра КБ
1	-4	12	24	25	12	25	6
	-3	12	29	25	15	25	8
	-2	12	35	25	17	25	10
	-1	12	40	25	20	25	11
	0	12	44	25	22	25	13
	1	12	51	25	26	25	15
	2	12	60	25	30	25	18
	3	12	80	25	40	25	25
	4	12	150	25	78	25	47
8	-4	2	28	3	14	7	8
	-3	2	35	3	17	7	10
	-2	2	41	3	20	8	11
	-1	2	46	3	23	8	13
	0	2	52	3	26	8	15
	1	2	60	3	30	8	18
	2	2	69	3	35	8	21
	3	2	91	3	46	8	28
	4	2	167	3	85	8	52



Беспроводные сети.

Серия стандартов 802.11.

Все мы уже привыкли к тому, что все большее количество продуктов CCTV использует подключение по беспроводным сетям (Wireless LAN - WLAN), число инсталляций с использованием беспроводных сетей также возрастает. Популярность и удобство беспроводных коммуникаций между компьютерами, маршрутизаторами и цифровыми устройствами захвата и обработки видео заставляют производителей выпускать более совершенные и дешевые решения с завидной частотой. За последние годы мы видели уже немало несовместимых между собой решений и неэффективных стандартов, но, наконец, индустрия определилась с поддержкой одной серии стандартов для беспроводных сетей, а именно серии стандартов 802.11, разработанной Институтом инженеров по электротехнике и электронике (IEEE, Institute of Electrical and Electronics Engineers). Эти новые стандарты определяют передачу по беспроводным сетям (wireless Ethernet, WLAN), по отношению к ним также употребляется термин Wi-Fi (Wireless Fidelity).

Впрочем, существует много вариаций стандартов 802.11. Некоторые из этих вариаций более "зрелые", чем другие. Сейчас все более важно не просто разбираться в номенклатуре этих стандартов, но и понимать, какими возможностями они обладают и какое практическое применение они

имеют в охранном телевидении, также, как и в других сферах. Продажи растут, так как все большее количество компаний оценили преимущества беспроводных сетей.

Росту их популярности также способствовала ассоциация WECA (the Wireless Ethernet Compatibility Alliance), которая обеспечивает тестирование совместимости и взаимодействия оборудования различных производителей. Эта группа, в которую входят более 130 компаний, уже вынесла положительное заключение о соответствии стандарту 802.11b 185 продуктам, выдав им свой фирменный знак "Wi-Fi".

Другие организации, занимающиеся стандартизацией, тоже уделяют внимание стандартам беспроводных сетей. Европейский институт стандартов по телекоммуникациям ETSI (European Telecommunications Standards Institute) разработал стандарт HyperLAN/2 для беспроводных сетей 5 ГГц. Этот стандарт соответствует нормам работы в диапазоне радиочастот, который в Европе традиционно используется радаром, хотя еще и не сумел завоевать рынок, как стандарты IEEE.

В Японии группа MMAC (Multimedia Mobile Access Communication) разрабатывает спецификации для усовершенствованных типов беспроводных систем. Впрочем, поскольку IEEE внедряет дополнительные стандарты для

соответствия требованиям японских регулирующих организаций, то шансы самой группы MMAC на столь же широкое распространение ее стандартов существенно уменьшаются.

В рамках серии стандартов IEEE's 802.11 существует несколько спецификаций, часть из которых находится еще в процессе разработки. Пользователям необходимо сделать свой выбор, производителям решить, какие стандарты применять в своей продукции, дистрибьюторам выбрать, какие продукты поддерживать и рекомендовать покупателям, а инсталляторам определиться с тем, какое оборудование устанавливать на объектах.

Что такое 802.11?

IEEE 802.11 или Wi-Fi определяет набор стандартов для беспроводных сетей, разработанный группой 11 IEEE 802. Иногда термин используют для обозначения первоначального стандарта, который во избежание ошибок также именуют традиционным 802.11 (802.11 legacy).

В настоящее время семейство 802.11 включает три отдельных протокола кодирования (a, b, g). Изначально функции безопасности были включены в эти протоколы, но в дальнейшем они развивались как отдельные стандарты (например, 802.11i). Другие стандарты в этом семействе (с-f, h-j, n) являются сервисными улучшениями и дополне-

ниями или исправлениями предыдущих спецификаций. Первым стандартом, который получил широкое распространение, оказался 802.11b. За ним, как это ни странно, последовали стандарты 802.11a и 802.11g. Частоты радиоволн, используемые в серии стандартов 802.11, принадлежат к СВЧ-диапазону и в большинстве своем подлежат минимальному регулированию со стороны контролирующих органов. В большинстве стран для использования этого спектра радиочастот не требуются специальные разрешения.

Традиционный стандарт 802.11 (802.11 legacy)

Первоначальная версия стандарта IEEE 802.11, появившаяся в 1997 году и иногда называемая 802.1у, определяла две скорости передачи данных (1 и 2 Мбит/с). Передача должна была осуществляться в инфракрасном диапазоне или на полосе частот 2.4 ГГц, предназначенной для использования в промышленных, научных и медицинских целях. В последующих версиях стандарта отказались от инфракрасного диапазона, поскольку реального применения этот диапазон не нашел в стандарте, а сам стандарт не мог конкурировать с устоявшимся протоколом IrDA. Традиционный стандарт 802.11 был быстро заменен стандартом 802.11b.

Стандарт 802.11b

Дальность действия стандарта составляет около 50 метров при использовании ненаправленных антенн с малым усилением, которые обычно применяются в устройствах 802.11b. Максимальная пропускная способность - 11 Мбит/с. Впрочем, значительная часть ее расходуется на непроизводительные затраты, а максимальная пропускная способность на практике составляет около 5.5 Мбит/с. Металл, вода и толстые стены способны поглощать сигналы 802.11b и существенно уменьшают дальность действия. Стандарт работает на полосе частот 2.4 ГГц и использует в качестве метода доступа к среде передачи множественный доступ с контролем несущей и предотвращением конфликтов CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

При использовании внешних антенн с высоким коэффициентом усиления этот протокол можно применять для установления двухточечного соединения с дальностью действия до 8 кило-

метров, хотя некоторые утверждают, что им удавалось добиться дальности действия до 80-120 километров в зоне прямой видимости.

Обычно это делается для замены дорогих выделенных линий или очень громоздкого микроволнового коммуникационного оборудования. Современные сетевые карты поддерживают передачу данных со скоростью 11 Мбит/с, но автоматически снижают скорость до 5.5, а затем до 2 и 1 Мбит/с при падении мощности сигнала.

Для протокола 802.11b предусмотрен ряд расширений (например, объединение каналов (channel bonding) и пакетная передача данных (burst transmission)) для увеличения скорости передачи данных до 22, 33 и 44 Мбит/с. Все эти расширения протокола являются разработками отдельных компаний, которые используют их в своем оборудовании, и, соответственно, официально расширения не поддерживаются со стороны IEEE. Многие компании называют эти улучшенные версии протокола



802.11b+.

Первое широко распространенное коммерческое применение стандарта 802.11b было реализовано компанией Apple Computer под торговой маркой AirPort.

Стандарт 802.11a

В 2001 году на рынке стал доступен более скоростной стандарт 802.11a, хотя утвержден он был еще в 1999 году. Этот стандарт оперирует в частотном диапазоне 5 ГГц с максимальной скоростью 54 Мбит/с. На практике максимально достижимая скорость составляет около 25 Мбит/с. При необходимости скорость уменьшается до 48, 36, 34, 18, 12, 9 и 6 Мбит/с. В стандарте 802.11a используются 12 неперекрывающихся между собой каналов: из них 8 предназначены для работы внутри помещения, а 4 для построения двухточечного соединения.

В разных странах имеются различные идеи по поводу регулирования использования радиочастот, хотя проведенная в 2003 году международная конференция по вопросам радио- и телекоммуникаций несколько упростила дело в этой сфере. В середине 2003 года решением Федеральной комиссии связи США был расширен диапазон частот, доступных каналам стандарта 802.11a.

Этот стандарт не получил широкого распространения из-за популярности стандарта 802.11b, а также из-за ограниченного радиуса действия, так как в частотном диапазоне 5 ГГц 802.11a не может работать на таком же расстоянии, как 802.11b, при прочих равных (например, те же самые ограничения по мощности передатчика); сигнал стандарта 802.11a также более легко поглощается препятствиями.

Большинство производителей оборудования 802.11a, чтобы хоть как-то компенсировать непопулярность стандарта на рынке, начали выпускать сетевые карты, поддерживающие два диапазона и два или три стандарта. Эти сетевые карты могут работать в сетях 802.11a и b или

802.11a, b и g, автоматически определяя нужный стандарт. Также доступны точки доступа, одновременно поддерживающие все эти стандарты.

Стандарт 802.11g

В июне 2003 года был принят третий стандарт 802.11g. Как и 802.11b, этот стандарт работает в частотном диапазоне 2.4 ГГц, но со скоростью 54 Мбит/с, что на практике дает примерно 24.7 Мбит/с, как и в стандарте 802.11a. 802.11g полностью обратно совместим с 802.11b, используя те же самые частоты. Процесс принятия стандарта затянулся в основном из-за необходимости сделать 802.11g совместимым с 802.11b. Впрочем, присутствие оборудования 802.11b авто-

матически снижает скорость передачи сети 802.11g до скорости стандарта 802.11b.

Стандарт 802.11g будоражил умы любителей новинок еще с января 2003 года, то есть задолго до принятия. Корпоративные пользователи выжидали, а Cisco и другие крупные производители оборудования ждали принятия стандарта. К лету 2003 года анонсы стали появляться один за другим. Большинство двухдиапазонных продуктов 802.11a/b превратились в двухдиапазонные и трехстандартные, поддерживая a, b и g на одной сетевой карте или точке доступа.

Теперь некоторые точки доступа поддерживают новую возможность под названием Super G, которая за счет объединения каналов (channel bonding) способна повысить скорость передачи до 108 Мбит/с. Эта возможность может препятствовать работе других сетей, а также быть несовместимой с некоторыми сетевыми картами стандартов b и g. Кроме того, технология пакетной передачи данных (burst transmission) также доступна в некоторых продуктах и чипсетах, что значительно повышает скорость передачи данных. Продукты с этой технологией также могут быть несовместимыми с некоторым оборудованием.

Первым крупным производителем, внедрившим стандарт 802.11g в свои продукты, снова оказалась компания Apple, которая использовала для этого стандарта торговую марку AirPort Extreme.

Каналы и совместимость в международном масштабе

Канал	МГц	США X10	Канада X20	Европа ETSI X30	Испания X31	Франция X32	Япония X40	Япония X41
1	2412	x	x	x				x
2	2417	x	x	x				x
3	2422	x	x	x				x
4	2427	x	x	x				x
5	2432	x	x	x				x
6	2437	x	x	x				x
7	2442	x	x	x				x
8	2447	x	x	x				x
9	2452	x	x	x				x
10	2457	x	x	x	x	x		x
11	2462	x	x	x	x	x		x
12	2467			x		x		x
13	2472			x		x		x
14	2484						x	

802.11b и 802.11g делят весь частотный диапазон на 14 перекрывающихся каналов по 22 МГц каждый. Каналы 1, 6, 11 и 14 имеют минимальное перекрытие, и их (или аналогичный ряд неперекрывающихся каналов) можно использовать, когда несколько сетей мешают работе друг друга. Только каналы 10 и 11 могут работать во всех частях света, так как Испания и Франция не разрешили использование на своей территории каналы с 1 по 9 для стандарта 802.11b. Приведем полный список частот из IEEE STD 802.11b-1999/Cor 1-2001.

Стандарт 802.11n

В январе 2004 года IEEE анонсировал разработку нового стандарта для глобальных беспроводных сетей. Реальная скорость будет 100 Мбит/с (даже 250 Мбит/с на физическом уровне), что в 4-5 раз быстрее чем у 802.11g и, может быть, в 50 раз быстрее чем у 802.11b. Предполагается, что 802.11n также повысит и дальность действия по сравнению с существующими стандартами. Принятие стандарта ожидается к концу 2005 года.

Кто первым сойдет со сцены

IEEE 802.11a, оперирующий в частотном диапазоне 5 ГГц, без каких-либо помех и ограничений может работать в США и Японии. В странах ЕС этому стандарту пришлось дольше ждать разрешения, так как европейские регулирующие инстанции рассматривали возможность применения европейского стандарта HIPERLAN. 802.11a был разрешен к использованию в Европе примерно в середине 2002 года.

802.11a также предоставляет большую скорость передачи данных в 54 Мбит/с, но несовместим с 802.11b, если не брать тех случаев, когда в оборудовании поддерживаются оба стандарта.

Сертификация

Поскольку IEEE только устанавливает спецификации стандартов, но не тестирует оборудование на соответствие им, торговая группа Wi-Fi проводит программу сертификации, которую оплачивают ее участники. Теоретически все компании, производящие оборудование стандартов 802.11 являются участниками программы сертификации. Торговая марка Wi-Fi, принадлежащая группе и использующаяся только на совместимом оборудовании, должна гарантировать взаимную совместимость. В настоящее время Wi-Fi может обозначать любой из стандартов 802.11a, b или g. С осени 2003 года Wi-Fi также включает в себя стандарты защиты информации WPA (Wi-Fi Protected Access). Потом маркой Wi-Fi также будут обозначать оборудование, в котором применяется стандарт защиты информации 802.11i (WPA2). На продуктах с торговой маркой Wi-Fi обязательно должен быть указан частотный диапазон, в котором они работают: 2.4 или 5 ГГц.

Небольшие беспроводные сети

С быстрым распространением кабельных модемов и DSL появляется все больше людей, которые хотят построить небольшие сети у себя дома, чтобы предоставить свой высокоскоростной доступ в Интернет в общем пользование.

Беспроводные офисные сети зачастую ничем не защищены или защищены только WEP, а этот протокол защиты информации достаточно прост для взлома. Эти сети часто позволяют "людям с улицы" получить доступ в них и в Интернет. То же самое относится и к небольшим домашним сетям.

Защита информации

В 2001 году группа из университета Беркли (Калифорния) представила документ описывающий уязвимость в стандарте 802.11b (Fluhrer, Mantin, and Shamir "Weaknesses in the Key Scheduling Algorithm of RC4"). За этим вскоре последовали публичные заявления Адама Стабблфилда (Adam Stubblefield) и компании AT&T, под-

Следующие стандарты и группы существуют в рамках рабочей группы IEEE 802.11

- IEEE 802.11 - Первоначальный стандарт (2 Мбит/с, 2.4 ГГц)
- IEEE 802.11a - 54 Мбит/с, 5 ГГц стандарт (1999, на рынке с 2001)
- IEEE 802.11b - Усовершенствованный 802.11 с увеличением скорости 5.5 и 11 Мбит/с (1999)
- IEEE 802.11d - Стандарт определяет требования к передаче информации от точек доступа на пользовательские устройства по разрешенным радиоканалам и с допустимым уровнем мощности сигнала.
- IEEE 802.11e - Дополнительные улучшения: QoS, в т.ч. Пакетная передача
- IEEE 802.11f - Inter-Access Point Protocol (IAPP) Стандарт 802.11f содержит рекомендации по применению протоколов обмена информацией между точками доступа."
- IEEE 802.11g - 54 Мбит/с, 2.4 ГГц стандарт (обратно совместим с b) (2003)
- IEEE 802.11h - пополнит возможности стандарта IEEE 802.11a функциями управления мощностью передатчика (TPC) и динамического выбора канала/частоты (DCS/DFS).
- IEEE 802.11i - and Transmit Power Control (TPC) for European compatibility
- IEEE 802.11i (принят 24 июня 2004) - содержит описание новых функций, предназначенных для защиты информации
- IEEE 802.11j - Набор рекомендаций для использования на территории Японии
- IEEE 802.11n - Усовершенствования для повышения скорости передачи данных

тверждающие возможность взлома. В результате им удалось перехватить передаваемые данные и получить несанкционированный доступ к беспроводной сети.

IEEE выделила отдельную рабочую группу для разработки нового стандарта защиты информации 802.11i. Прежде такие работы велись в рамках разработки более широкого стандарта 802.11e, призванного оптимизировать уровень контроля доступа к среде (MAC-уровень). Группа Wi-Fi анонсировала промежуточную спецификацию под названием WPA (Wireless Protected Access), которая основывалась на черновых набросках из IEEE. Эта спецификация стала появляться в продуктах с середины 2003 года. Стандарт 802.11i (WPA2) был принят в июне 2004 года и использует улучшенный стандарт шифрования AES (Advanced Encryption Standard) вместо RC4, который использовался в WEP и WPA.

А что же Bluetooth?

Если предложить создать локальную беспроводную сеть, то большинство специалистов по информационным технологиям остановят свой выбор на оборудовании стандарта 802.11b, и лишь немногие подумают о технологии Bluetooth, которая также предназначена для передачи по радиочастотам на небольшое расстояние.

Причина такого пренебрежения заключается в том, что Bluetooth всегда позиционировалась как технология для соединения таких устройств как мобильные телефоны, телефонные гарнитуры, компьютеры, цифровые фотоаппараты и другая периферия, но не для построения локальных сетей.

Впрочем, технология Bluetooth мо-

жет стать серьезной альтернативой для построения беспроводных локальных сетей, так как в ближайший год будет выпущено много устройств с поддержкой Bluetooth. Впрочем, специалистам по информационным технологиям придется подумать дважды, прежде чем использовать Bluetooth, так как 802.11b и Bluetooth используют одинаковый частотный диапазон для передачи данных, то возможность взаимных помех нельзя не учитывать.

Такая ситуация заставляет многих специалистов по информационным технологиям очень осторожно оценивать возможность использования устройств Bluetooth в беспроводных сетях до тех пор пока этот стандарт не укоренится более глубоко. Питер Джадж (Peter Judge), аналитик компании Infonetics, утверждает: "Вряд ли компании, устанавливающие беспроводные локальные сети, всерьез рассчитывают на применение технологии Bluetooth в ближайшее время. Многие специалисты подумают дважды, прежде чем устанавливать оборудование стандарта 802.11b в тех местах, где предполагается использовать большое количество устройств Bluetooth".

Появление концентраторов, способных обрабатывать оба типа трафика могло бы решить проблему. Такие кон-

центраторы располагались бы рядом с персональным компьютером и обрабатывали бы обычный и беспроводной трафик. Компания 3Com уже разрабатывает такую систему концентраторов.

Джадж также считает, что до сих пор неясно, будет ли Bluetooth серьезной проблемой. "Возможно, что всплески активности Bluetooth будут редки и не смогут напрямую мешать объемному трафику 802.11b".

В ближайшее время незначительный радиус действия устройств Bluetooth будет существенно увеличен. TDK Systems тестирует новую керамическую антенну, которая увеличит радиус действия устройств Bluetooth с 10 до 50 метров, что позволит сравняться с устройствами 802.11b. Но TDK, которая также производит и компоненты для беспроводных сетей, надеется, что даже в этом случае Bluetooth не составит конкуренции стандарту 802.11b. Как говорит Ник Ганн (Nick Hunn), директор отдела исследований и разработок в TDK Systems Europe: "Радиус действия - достаточно неточный параметр. Куда важнее учитывать скорость передачи данных, которая в беспроводных сетях в настоящее время легко достигает 3-4 Мбит/с, что несравнимо с 200 Кбит/с у Bluetooth. Уверен, что в будущем Bluetooth в офисах будет использовать-

Стандарт	Метод передачи	Частоты	Скорость передачи данных (Мбит/с)
802.11	FHSS, DSSS, ИК	2.4 ГГц, ИК	1, 2
802.11b	DSSS, HR-DSSS	2.4 ГГц	1, 2, 5.5, 11
802.11b+ (нестандартизован)	DSSS, HR-DSSS (PBCC)	2.4 ГГц	1, 2, 5.5, 11, 22, 33, 44
802.11a	OFDM	5.2, 5.5 ГГц	6, 9, 12, 18, 24, 36, 42, 48, 54
802.11g	DSSS, HR-DSSS, OFDM	2.4 ГГц	1, 2, 5.5, 11; 6, 9, 12, 18, 24, 36, 42, 48, 54

ся в основном для передачи голосового трафика, а 802.11b - для передачи данных". Ганн также подчеркнул, что существуют возможности взаимодействия различных сетей и миграции от одной технологии к другой. По его мнению, большое количество телефонных аппаратов с поддержкой Bluetooth сделает стандарт более популярным и приведет к более быстрому по сравнению со

стандартом 802.11b снижению цен на устройства и компоненты Bluetooth.

Spectralink, производитель, который специализируется на производстве голосовых продуктов для беспроводных сетей, уверен, что конкуренция со стороны Bluetooth не представляет угрозы. "В лагере сторонников Bluetooth допускают, что это не сетевой протокол", - заявляет Бен Гудериан (Ben

Guderian), директор по маркетингу компании Spectralink - "Проблема конфликта при передаче данных будет решена. Специалисты по информационным технологиям уже давно не придерживаются мнения "поживем - увидим", так как они знают, что беспроводные сети 802.11b уже широко доступны сейчас".

Стандарт	Скорость передачи данных и диапазон	Модуляция	Защита	Преимущества/Недостатки
IEEE 802.11	до 2 Мбит/с, 2.4 ГГц	FSSS или DSSS	WEP и WPA	Получил дальнейшее развитие в 802.11b
IEEE 802.11a (Wi-Fi)	до 54 Мбит/с, 5 ГГц	OFDM	WEP и WPA	Продукты, которые соответствуют этому стандарту получают сертификат Wi-Fi. 8 доступных каналов. Менее подвержены радиочастотным помехам чем 802.11b и 802.11g. Лучше чем 802.11b поддерживают мультимедийные видео- и аудиоприложения при большом количестве пользователей. Меньший чем у 802.11b радиус действия. Несовместим с 802.11b.
IEEE 802.11b (Wi-Fi)	до 11 Мбит/с, 2.4 ГГц	DSSS с CCK	WEP и WPA	Продукты, которые соответствуют этому стандарту получают сертификат Wi-Fi. Несовместим с 802.11a. Для покрытия больших зон требуется меньше точек доступа чем в 802.11a. Высокоскоростной доступ в пределах 100 метров от базовой станции. 14 каналов, из которых только 3 непересекаются.
IEEE 802.11g (Wi-Fi)	до 54 Мбит/с, 2.4 ГГц	DSSS с CCK при скорости менее 20 Мбит/с, OFDM при скорости более 20 Мбит/с	WEP и WPA	Продукты, которые соответствуют этому стандарту получают сертификат Wi-Fi. Может заменять 802.11b. Улучшенная защита по сравнению с 802.11. 14 каналов, из которых только 3 непересекаются.
Bluetooth	до 2 Мбит/с, 2.45 ГГц	FHSS	PPTP, SSL, VPN	Нет встроенной поддержки IP, поэтому плохая поддержка TCP/IP и беспроводных сетей. Лучше всего подходит для соединения КПК, мобильных телефонов и компьютеров на небольшом расстоянии.
Home RF	до 10 Мбит/с, 2.4 ГГц	FSSS	Независимые IP-адреса для каждой сети. Данные шифруются 56-битным ключом.	Home RF более не поддерживается ни одним производителем или рабочей группой. Предназначен для использования в домашних, но не корпоративных, сетях. Оборудование относительно недорого для установки и эксплуатации. Качество голосовой передачи всегда сохраняется высоким за счет резервирования части полосы пропускания для голосовых сервисов. Хорошая защита от помех.
HiperLAN/1 (Европа)	до 20 Мбит/с, 5 ГГц	CSMA/CA	Шифрование каждой новой сессии и индивидуальная аутентификация	Используется только в Европе. Только в режиме ad-hoc, не требуется конфигурирования и центрального контроллера. Не обеспечивает реальной синхронности сервисов. Достаточно дорого для установки и обслуживания. Нет гарантированной полосы пропускания.
HiperLAN/2 (Европа)	до 54 Мбит/с, 5 ГГц	OFDM	Улучшенная защита с шифрованием каждой новой сессии и индивидуальной аутентификацией.	Используется только в Европе. Разработан для передачи пакетов IP, FireWire, ATM и оцифрованного голоса от мобильных телефонов. Лучшее качество сервиса, чем HiperLAN/1. Гарантированная полоса пропускания.



Системы распознавания лиц и суровая действительность

Распознавание лиц - достаточно тривиальная задача, с которой мы сталкиваемся регулярно, но автоматизация этого процесса, как и многих других процессов, характерных для высшей нервной деятельности является крайне сложной задачей, которая, возможно, никогда не будет решена полностью.

В настоящее время на рынке доступно достаточное количество систем распознавания лиц, чтобы не говорить о них как об уникальном явлении. Все они могут получать изображения лица с кадров от телекамеры или из статичной фотографии. При этом на начальном этапе происходит локализация лица в кадре, а затем после предварительной обработки специальные алгоритмы выделяют набор параметров, по которому происходит сравнение полученной фотографии с наборами параметров других фотографий, содержащихся в базе данных.

Системы распознавания лиц уже перешагнули тот порог, который отделяет область научной фантастики от практической сферы применения, но до сих пор существование подобных систем окружено некой мистической завесой. Несмотря на то, что системы распознавания лиц в настоящее время можно встретить практически на любой более-менее крупной выставке, посвященной безопасности, и каждый желающий может ознакомиться с демонстрацией их возможностей, до сих пор господствуют два диаметрально противоположных мнения относительно применимости данных систем на практике.

С одной стороны, многие энтузиасты новых, и в первую очередь информационных, технологий готовы часами

увлеченно рассказывать о преимуществах систем распознавания лиц, разделяя эти технологии совершенно фантастическими возможностями. Такие энтузиасты готовы верить любым рекламным сказкам и с полной серьезностью рассуждать о возможности использования систем распознавания лиц для таких актуальных для систем распознавания лиц задач, как поиск террористов в метро. Список этих задач можно продолжать до бесконечности, но рассказы о том, как "космические корабли бороздят просторы Большого театра" или "вовремя закупленные в достаточном количестве системы распознавания лиц способны были предотвратить американскую трагедию 11 сентября" находятся в одном логическом ряду. Самое любопытное, что такие утверждения не являются досужими домыслами самих энтузиастов, а активно подпитываются недобросовестной рекламой. Можно с уверенностью утверждать, что такая недобросовестная реклама целиком и полностью лежит на совести нечистоплотных менеджеров по продажам и рекламе систем распознавания лиц, а сами разработчики не имеют к этому ни малейшего отношения. Вполне понятное желание менеджера побыстрее продать товар, не вдаваясь в подробности и руководствуясь принципом: "Не обманешь - не продашь". Но при этом ради сиюминутной выгоды в жертву приносится не только репутация самого продавца, но также, как правило, и разработчика системы. Не останавливаясь на достигнутом, такие специалисты рекламного дела продолжают свои рекламные компании, которые на практике превращаются в компании по долгосрочной дискреди-

тации самой идеи автоматического распознавания лиц.

Парадоксально, но те же самые люди во многом способствовали и формированию противоположного мнения о системах распознавания лиц как о "дорогих игрушках", не имеющих практического применения. Этот скептицизм является своего рода защитной реакцией потребителя на недобросовестную рекламу.

Мы не придерживаемся ни того, ни другого мнения. Как это часто бывает, истина находится где-то посередине. Системы распознавания лиц имеют свои сферы применения, может быть и не столь широкие, как хотелось бы многим, но в этих сферах автоматическое распознавание уже зарекомендовало себя как удобный инструмент.

Практически каждый разработчик систем распознавания лиц имеет уже готовое решение в сфере контроля доступа. И это закономерно, так как контроль доступа изначально является сферой, для которой и разрабатывались технологии автоматического распознавания лиц.

Целью любой системы контроля доступа является предоставление людям, имеющим соответствующие права, возможность доступа в определенные зоны, поэтому использование систем распознавания лиц для идентификации или аутентификации абонентов вполне закономерно и имеет то преимущество перед другими биометрическими системами, которые используют отпечатки пальцев, узор радужной оболочки или сетчатки глаз, расположение кровеносных сосудов, голоса и т.д., что не требуют установки дополнительного оборудования для идентификации, кроме телекамер, и работа-

ют относительно незаметно для пользователя, не требуя от него дополнительных действий. Функция распознавания лиц, применяемая в сфере контроля доступа, может быть основной, то есть система распознавания лиц полностью отвечает за контроль доступа (режим идентификации, при котором происходит сравнение полученной фотографии со всеми фотографиями, содержащимися в базе данных системы). Но также функция распознавания лиц может быть вспомогательной, когда используются дополнительные средства для установления личности, чаще всего карточка (режим верификации, при котором происходит сравнение полученной фотографии с одной из фотографий базы данных). Эти два сценария применения систем распознавания лиц для контроля доступа можно назвать классическими, и они уже с успехом зарекомендовали себя, так как низкий уровень ошибок обусловлен тем, что люди, пытающиеся получить доступ, заинтересованы в том, чтобы система распознала их лицо, но так может быть далеко не всегда.

Например, еще одним вариантом применения систем распознавания лиц может быть использование их в ситуации прямо противоположной рассмотренной выше, то есть не для пропуска "нужных" людей при ограниченном доступе, а для блокирования доступа нежелательных посетителей при общем неограниченном доступе. Наиболее распространенным примером, иллюстрирующим такое применение, является установка систем распознавания лиц в казино, клубах и других увеселительных и публичных заведениях для отсева нежелательных посетителей. В этом случае количество ошибок распознавания будет значительно выше, так как корректные условия работы для системы не всегда удастся обеспечить, а сами посетители, тем более попадающие в группу нежелательных посетителей, постараются максимально затруднить работу системы распознавания лиц, как только узнают о ее существовании или даже заметят установленные телекамеры.

Еще одной перспективной сферой применения систем распознавания лиц является борьба с подделкой документов. В настоящее время в США в некоторых департаментах полиции устанавливаются системы распознавания лиц для контроля выдачи водительских прав. Но для установления

по-настоящему эффективного контроля выдачи документов потребуется устанавливать системы распознавания лиц в масштабах целой страны, а до этого еще далеко.

Зачастую продавцы систем распознавания лиц (в отличие от самих разработчиков) на первое место ставят такие второстепенные факторы, как одобрение системы пользователями (то есть система не должна вызывать у пользователя чувства дискомфорта и быть простым в использовании), забывая о том, что система должна точно выполнять свою основную функцию, то есть находить в базе данных соответствующую фотографию и не путать разные фотографии. Все остальные факторы играют второстепенную роль и не могут служить доказательством работоспособности системы, если сам алгоритм распознавания лиц имеет существенные недостатки.

В качестве показателей надежности систем распознавания лиц могут служить вероятности ошибок первого и второго рода. Эти показатели изначально использовались для характеристики биометрических систем контроля доступа, но так как системы распознавания лиц в первую очередь применяются именно в системах контроля доступа, то использование этих показателей вполне закономерно.

Ошибки первого рода определяют вероятность ложного отказа (FRR, False Rejection Rate), то есть система распознавания лиц не сумела найти правильное соответствие в базе данных, хотя нужная фотография в ней содержится. Ошибка второго рода отвечает за вероятность ложного сравнения (FAR, False Acceptance Rate) и проявляется в том случае, когда система, грубо говоря, обозначалась, то есть утверждает идентичность фотографий двух разных лиц. Также системы распознавания лиц можно характеризовать уровнем равной вероятности ошибок первого и второго рода (EER, Equal Error Rates) - точкой, в которой вероятность ошибки первого рода равна вероятности ошибки второго рода. Например, уровень равной вероятности ошибок первого и второго рода в один процент означает, что из 100 попыток распознавания в одном случае система не сможет распознать то лицо, которое она должна узнавать, или ошибочно распознает одно лицо. Впрочем, такая методика не отражает массы факторов, которые могут влиять

на работу системы распознавания лиц.

А все эти системы в большей или меньшей степени чувствительны к освещению, но особенно требовательны они к повороту или наклону головы. В идеальных условиях человек должен "предъявлять" свое лицо системе, как документы: "прямо и в развернутом виде". При этом системе потребуется некоторое время, для того чтобы получить несколько фотографий лица и выбрать из них фотографию с наиболее удачным ракурсом. Обычно допустимый поворот или наклон лица не превышает 15-20 градусов, в противном случае вероятность распознавания лица резко снижается. Что бы не утверждали сами разработчики, любая система распознавания лиц будет в той или иной мере чувствительна к изменению лица с возрастом, а также к наличию бороды, усов и очков, а вероятность распознавания будет неизбежно снижаться. Впрочем, здесь уже многое будет зависеть от конкретного алгоритма распознавания лица, кроме того, задача распознавания лица в этом случае значительно возрастает и для человека, не говоря уже о самих системах.

Сейчас во многих странах ведутся исследования того, как человек распознает лица, и то, каким образом это происходит, до сих пор доподлинно неизвестно. Но одно с уверенностью можно сказать, в процессе распознавания лиц в мозгу не производятся трудоемкие вычисления, также как и не происходит построение сложной математической модели лица, то есть принципы работы систем распознавания лиц и человеческого мозга различны. Поэтому сейчас технологии автоматического распознавания лиц только пытаются приблизиться по эффективности распознавания к возможностям человеческого мозга, но до этого еще очень далеко. Сейчас можно точно сказать, что технологии автоматического распознавания лиц, несмотря на очевидные успехи, еще только делают первые шаги, и впереди предстоит огромная работа по их совершенствованию, возможно, даже по пути подражания работе мозга человека. До тех пор пока этого не произойдет, системы распознавания лиц будут иметь очень ограниченную сферу применения, обусловленную очень жесткими требованиями, которые такие системы предъявляют к изображению лица.



ZN-SmartEye (Viisage FaceFinder)



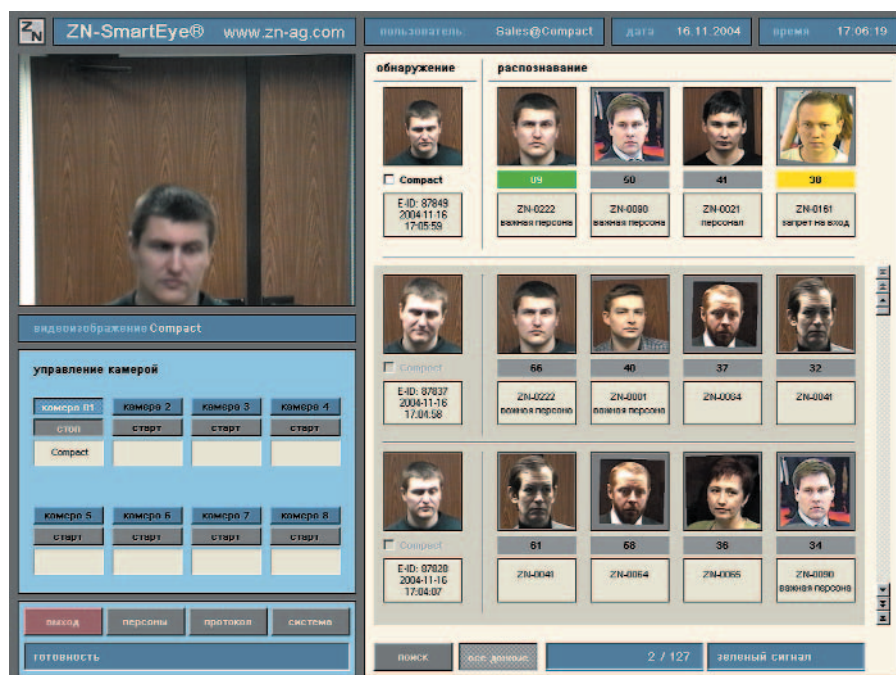
Первой системой распознавания лиц, с которой мы хотели бы вас познакомить, была выбрана SmartEye, производства немецкой компании ZN Vision Technologies AG. Компания была основана в 1993 году на базе Рурского университета (Бохум, Германия) и Южно-Калифорнийского университета (Лос-Анджелес, США). Кстати, уже через три года после основания, в 1996 году, ZN получила премию немецкой промышленности за инновации. Не так давно американская компания Viisage, также специализирующаяся на технологиях распознавания лиц, приобрела ZN, которая стала ее филиалом в Европе, поэтому в настоящее время рассматриваемую систему можно встретить на рынке под новым названием Viisage FaceFinder. Впрочем, пусть это никого не смущает, так как кроме логотипа компаний и названий никаких серьезных изменений в этом продукте не произошло.

Система распознавания лиц SmartEye способна находить лицо в кадре телекамеры и проводить проверку на совпадение с уже имеющимися фотографиями в базе данных. В качестве потенциальной сферы применения SmartEye можно перечислить такие заведения, как клубы, казино, а также общественные места, например, аэропорты, стадионы, и т.д. Этот список можно значительно расширить, так как систему можно применять везде, где есть возможность установки телекамеры для получения четких снимков лиц входящих людей. Очевидно, что в мес-

те установки системы необходимо постоянно контролировать доступ и вести мониторинг системы, иначе никакой пользы, кроме сбора статистики посещений, от установленной системы не будет. Впрочем, это достаточно очевидные требования, присущие практически всем системам распознавания лиц, о более специфических требованиях мы расскажем немного позже, сейчас же посмотрим, что представляет собой система SmartEye.

Система распознавания лиц SmartEye поставляется не в виде отдельного программного обеспечения, как это можно было ожидать, а в виде

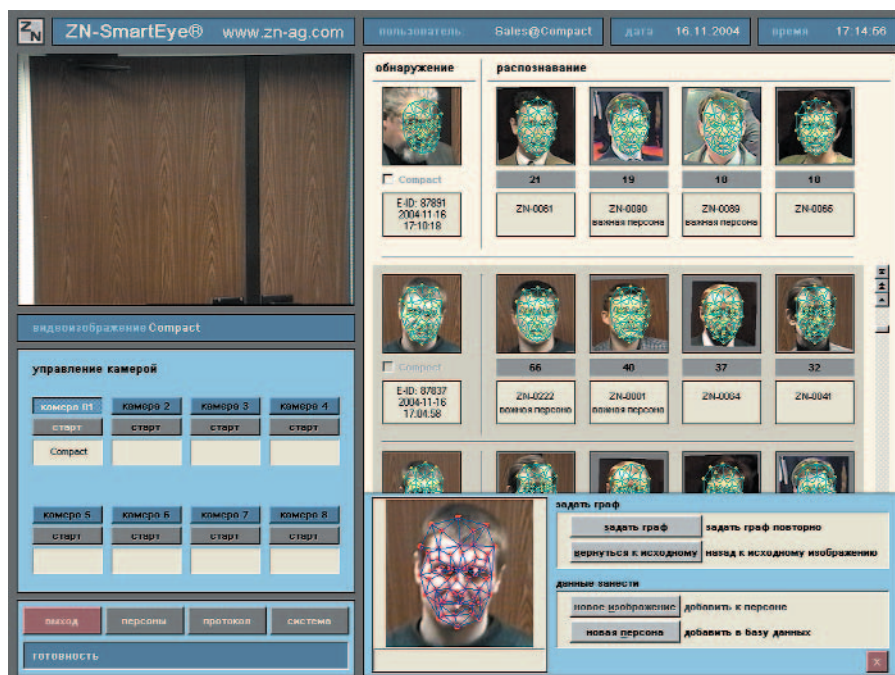
готовых системных блоков, что значительно облегчает процесс установки. Более того, компания-производитель готова поставлять вместе с системой SmartEye все необходимое для ее работы, включая телекамеры и мониторы. Такое решение также позволяет не заниматься подбором оптимальной конфигурации, а полностью доверить этот выбор разработчикам системы. Сама система SmartEye фактически представляет собой обычный компьютер, хотя и серверной конфигурации (в нем имеется даже стример для резервного копирования данных), работающий под управлением операционной системы



Пример удачного распознавания лица. Вероятность совпадения составляет 89 %. Но, как видно, две предшествующие попытки были менее удачными.

семейства Windows. Для ввода сигнала от телекамеры используется одноканальная плата видеоввода. Эта плата достаточно проста по сравнению с теми платами видеоввода, к которым мы привыкли, но для такой задачи как распознавание лиц, вероятно, не требуется особо сложное устройство для ввода видеоизображения. На самой плате фактически установлен только АЦП BT848 с режекторным фильтром, последствия работы которого видны невооруженным глазом. Впрочем, вопрос о качестве изображения в данном случае является второстепенным, так как его вполне хватает для того, чтобы получить отчетливую фотографию лица.

В нашем распоряжении оказалась конфигурация предыдущей версии системы SmartEye, сделанная на базе двухпроцессорного компьютера с процессорами Intel Pentium III, тогда как в настоящее время предлагаются и многопроцессорные конфигурации на базе Intel Pentium 4. На новых моделях устанавливается операционная система Windows XP, хотя в нашем случае компьютер работал под управлением операционной системы Windows NT. Версия программного обеспечения SmartEye была одна из последних (ZN-SmartEye 2.0.1). Также следует заметить, что мы имели дело с самой простой конфигурацией, в которой все процессы исполнялись на одном компьютере, но существуют многоканальные конфигурации с более сложной распределенной архитектурой, в рамках которой поиск лица и построение



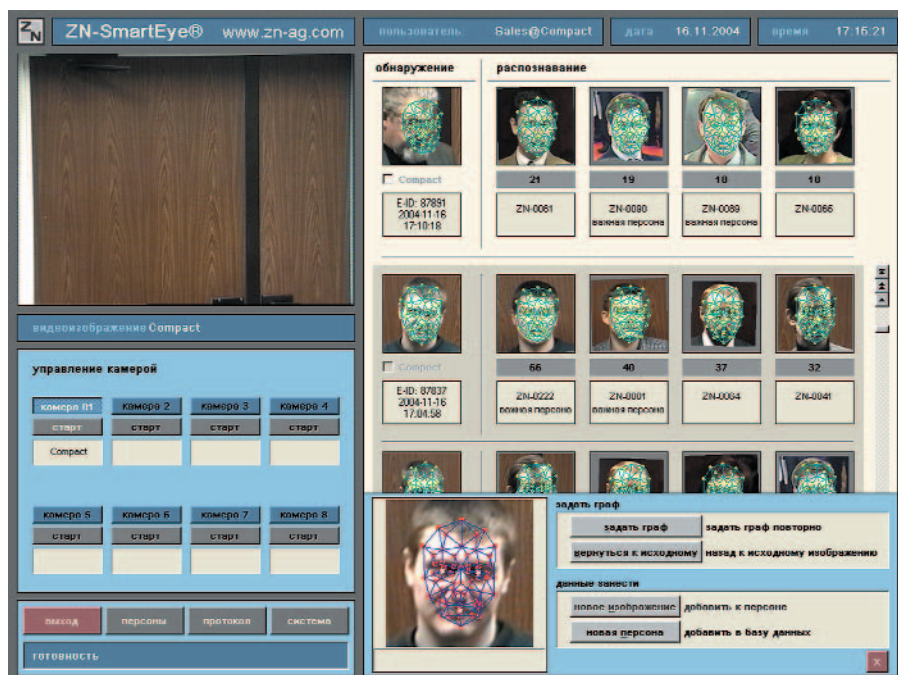
Построение графов в системе распознавания лиц ZN-SmartEye. Как видно на фотографии внизу, базовые точки графа определены системой не вполне корректно (смещены из-за наклона лица).

трехмерной модели выполняется на клиентских компьютерах, а сравнение лиц - на сервере. Также могут присутствовать и отдельные станции для просмотра результатов и администрирования системы. Взаимодействие между компонентами осуществляется по сети. В стандартной конфигурации максимально предусмотрено 8 клиентских компьютеров, причем, это не предел, и возможны нестандартные конфигурации под заказ.

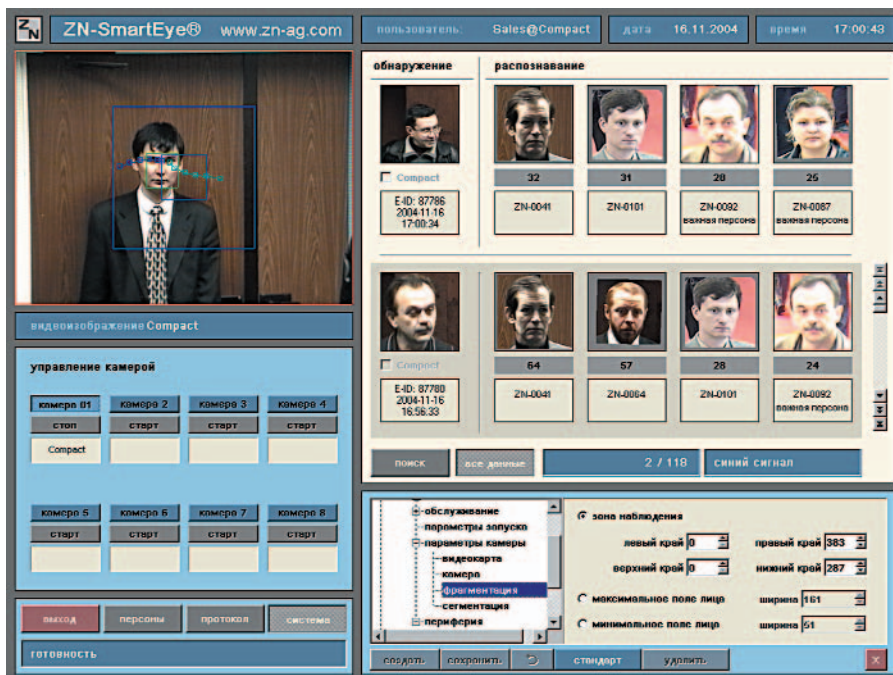
Принципы работы системы распознавания лиц SmartEye достаточно просты и очевидны, но за ними стоит

очень сложная математика, которая и требует мощных многопроцессорных конфигураций. Весь процесс распознавания лица можно разбить на 3 этапа: обнаружение лица в кадре, построение трехмерной модели лица, которая здесь называется "графом", по двумерной фотографии и сравнение полученного графа с графами фотографий, содержащихся в базе данных. Кстати, если посмотреть в администраторских настройках системы, то можно увидеть 3 программных модуля, которые соответственно называются "обнаружение", "моделирование лица" и "распознавание". Четвертый программный модуль "рабочее место" выполняет функцию оболочки для первых трех модулей.

На первый взгляд все выглядит достаточно просто, но это обманчивое впечатление, и, если вы подумали, что SmartEye сделана по популярному в операционных системах семейства Windows принципу Plug'n'Play, то, скорее всего, вас ждет разочарование. Забегая вперед, скажем, что система распознавания лиц SmartEye требует очень точной настройки для адаптации к внешним условиям, таким как освещение и фон. А если эти условия меняются, то каждый раз придется проводить дополнительную подстройку системы, что, учитывая большое количество различных опций и настроек, может оказаться достаточно долгим процессом. Поэтому, если у вас не было опыта общения с анало-



Пример неправильного построения графа. Несмотря на то, что базовые точки определены правильно, граф значительно меньше размеров лица.



Элементы визуализации настройки системы распознавания лиц.

гичными системами, то при настройке потребуется помощь квалифицированного специалиста, несмотря на то, что в SmartEye предусмотрен очень удобный интерфейс с элементами визуализации настройки (можно сравнить с аналогичными элементами визуализации, например, выделение контуром, которые используются при настройке детектора движения).

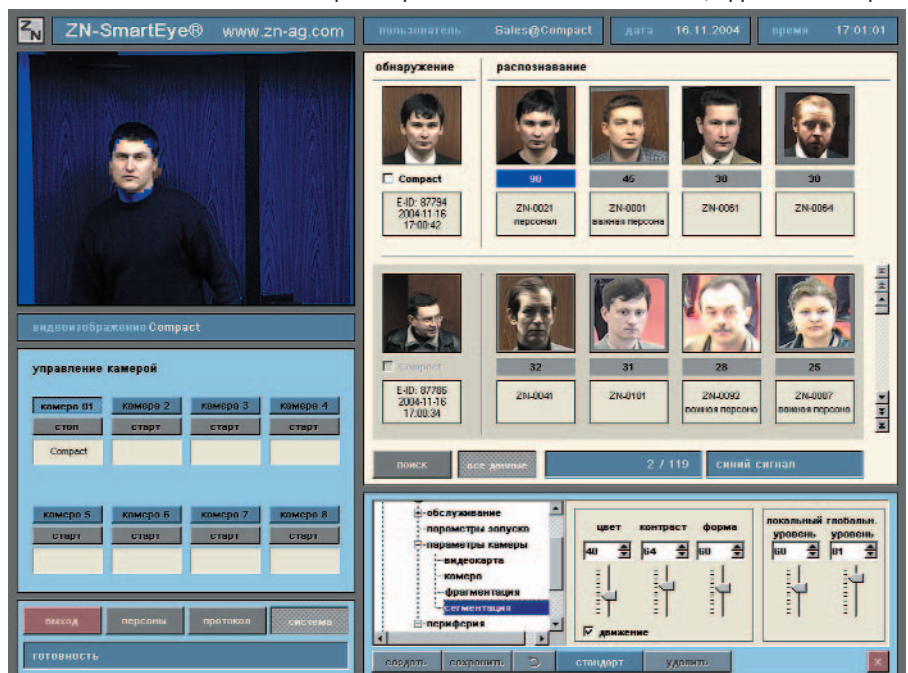
На первом этапе система постоянно ведет анализ содержания кадра и пытается найти в нем любые предметы, хотя бы отдаленно напоминающие человеческое лицо. Чтобы облегчить эту задачу системе, так как процесс весьма ресурсоемкий в пункте меню настроек "фрагментация" можно задать зону наблюдения, то есть зону, в которой система будет искать лица, а также указать максимальный и минимальный размер лица, то есть два квадрата, которые может занимать лицо в кадре. Как видим, аналогии с настройкой детектора движения продолжают, что, впрочем, неудивительно, так как в поиске лица задействован детектор движения, чтобы исключить возможность ложного распознавания фотографии вместо живого лица, хотя проверку на движение можно и отключить. В процессе настройки видно, что система в первую очередь обращает внимание на движущиеся объекты примерно круглой формы. В режиме настройки видно, что система "отрабатывает" не только лицо, но и другие области в кадре, такие как

белая рубашка, блики на двери, что выражается в дополнительной нагрузке процессора, но в итоге система правильно определяет лицо и не ошибается.

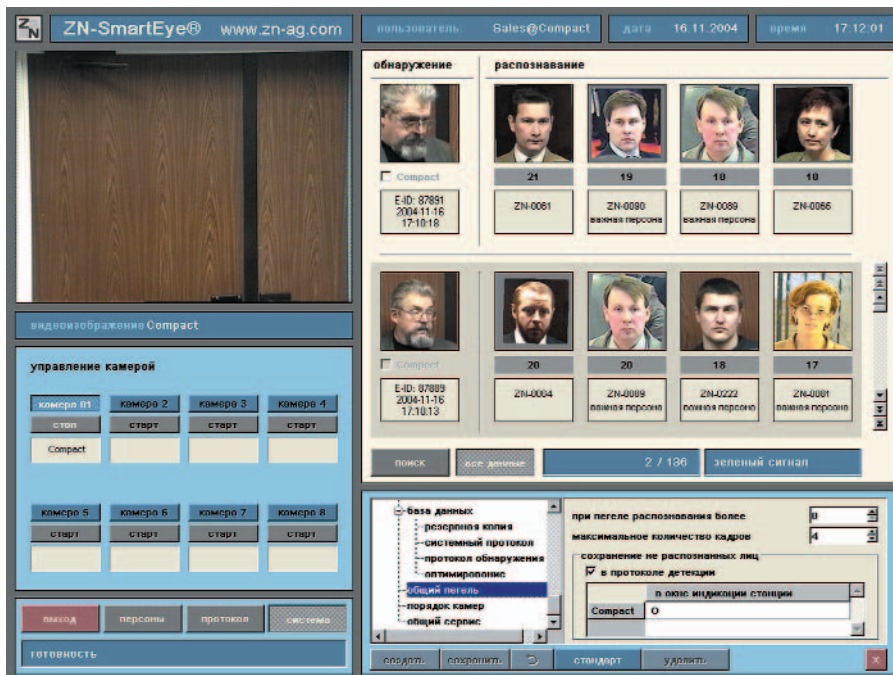
Впрочем, для корректного "захвата" лица потребуется еще провести дополнительную настройку в пункте меню "фрагментация" (параметры "цвет", "контраст", "форма", а также локальный и глобальный порог срабатывания). Эти параметры достаточно очевидны, за исключением, пожалуй, формы лица (этот параметр позволяет адаптировать систему для распознавания неевропеоидных лиц), но чтобы освоиться с этими параметра-

ми потребуется немного практики.

Построение трехмерной модели лица начинается с поиска опорных точек. В графе используется три опорные точки: два зрачка и середина рта. Все остальные точки (а их примерно 60), используемые в графе, вычисляются, по трем опорным точкам, а также по другим особенностям лица. Использование небольшого количества точек, по сравнению со значительно более сложной структурой лица, позволяет нивелировать влияние различного рода причесок, бороды, усов и очков на распознавание лица, хотя очевидно, что челка, спадающая на глаза, или очень густая борода могут создать серьезную проблему, так как будет прикрыта одна из опорных точек. При добавлении новых фотографий в базу данных необходимо внимательно следить за тем, чтобы система правильно строила граф. Если же граф был построен неправильно, то он может охватывать не все лицо или наоборот выходить за пределы лица. Такую фотографию нельзя добавлять в базу данных, так как она может значительно ухудшить возможность распознавания лица. В этом случае можно задать три опорные точки вручную, и если граф после этого будет построен правильно, то фотография может быть добавлена в базу данных. Для улучшения качества распознавания рекомендуется добавлять несколько фотографий в базу данных под одним именем. Также для добавления можно использовать оцифрованные фо-



Элементы визуализации настройки системы распознавания лиц.



Настройка общего порога распознавания.

тографии, при этом сохраняются все те же требования, которые предъявляются к фотографии лица, взятой из видеопоследовательности.

Особое требование система распознавания лиц предъявляет к ракурсу лица. Лицо человека для успешного распознавания должно быть направлено строго в телекамеру. Допустимые отклонения лица влево/вправо и вверх/вниз не должны превышать 15 градусов. В противном случае SmartEye не сможет построить правильный граф, и исправить ситуацию не удастся, даже если вручную задать три опорные точки. Здесь уже потребуется помощь оператора, которому придется просматривать все нераспознанные фотографии. Они сохраняются в специальный журнал с пометкой о дате и времени, когда было зафиксировано лицо.

Исходя из упомянутой особенности, для работы системы распознавания лиц нужно создавать условия, когда человек хотя бы ненадолго (примерно 1 секунда) посмотрит в объектив телекамеры, для того чтобы получить качественную фотографию анфас. Также для работы системы нужно исключить возможность быстрого перемещения лица в кадре, так как если слишком быстро пройти перед телекамерой, не говоря уже о том, чтобы пробежать, то система может вообще ничего не зафиксировать. Эти условия можно обеспечить, но об этом нужно позаботиться до установки системы SmartEye.

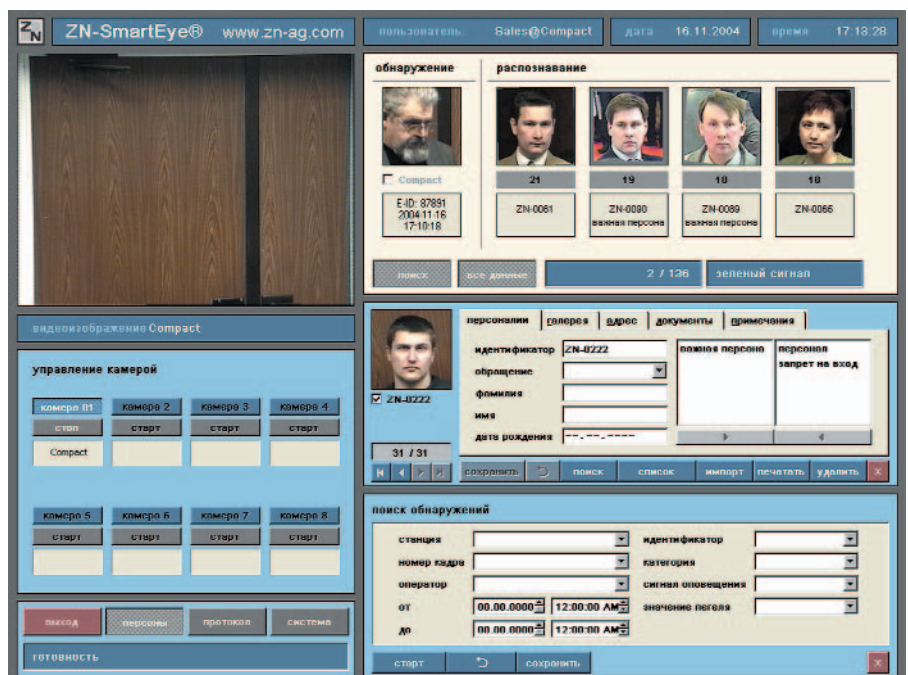
Еще одно наше замечание касается выбора фотографии для сравнения из последовательности кадров. Было замечено, что система далеко не всегда выбирает лучший из возможного ракурс, так как обычно выбираются первые кадры, и если среди них не окажется кадра в фас, то распознавание будет невозможно, хотя в дальнейшем человек может повернуть лицо в сторону телекамеры.

Впрочем, первые кадры отображаются на мониторе, а система продолжает работать со всеми кадрами, которые она получает от телекамеры. Если же замечено, что сравнение лица происхо-

дит с одной и той же персоной, то новые кадры не отображаются, хотя и участвуют в процессе распознавания лица.

Особое внимание нужно обратить на требования к освещению, которые достаточно строгие. Освещение должно быть равномерным, и лицо не должно быть слишком ярким или слишком затемненным. Это, впрочем, очевидно, так как по слишком темной или засвеченной фотографии и человек трудно будет распознать, но учитывая особенности алгоритма распознавания, это еще более критично. Более того, если освещение неравномерно, допустим, одна часть лица хуже освещена, чем другая, а это в первую очередь касается нижней половины лица, когда источник света находится сверху, как это обычно и бывает, то лицо с большой долей вероятности не будет опознано. Блики от очков, даже небольших, тоже влияют на качество распознавания, хотя сами очки не оказывают значительного влияния. Следует также избегать резких перепадов в освещении и прямых источников света в кадре. Дополнительные движущиеся объекты в кадре, как, например, те же блики, также затрудняют процесс распознавания.

Еще один интересный момент, на котором хотелось бы остановиться, это то, каким образом система выводит результаты сравнения. В процессе поиска полученный граф сравнивается с имеющимися в базе, и затем на выбор выдаются похожие фото-



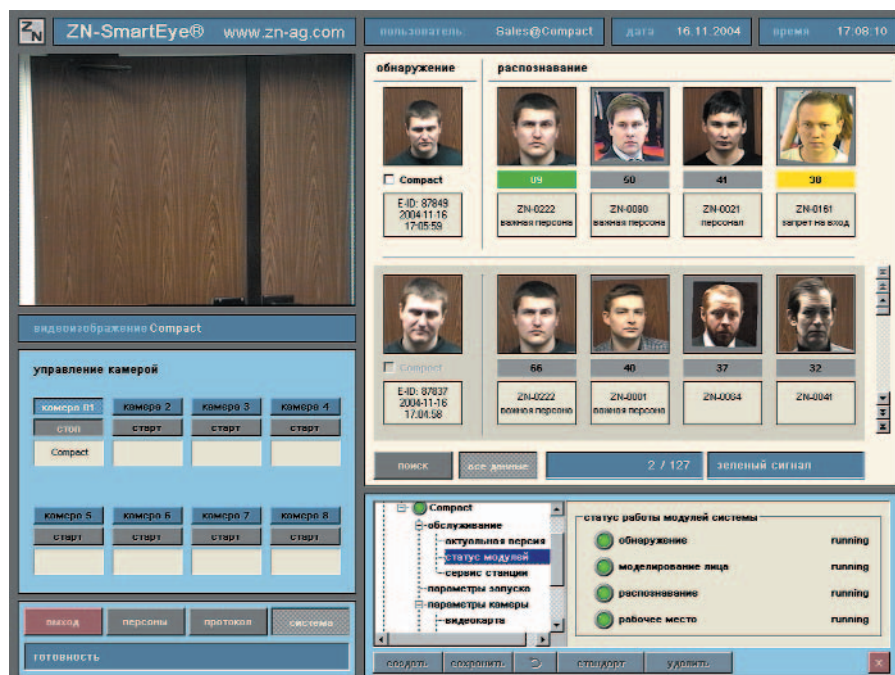
Поиск в базе данных.

графии, под которыми указывается процент соответствия.

При неудачном стечении обстоятельств (плохой ракурс и освещение, несоответствующее требованиям) из 4 фотографий, предложенных на выбор, может не оказаться ни одной даже приблизительно похожей с точки зрения человека фотографии, хотя система будет "настаивать" на идентичности с вероятностью до 50 процентов. Также нужная фотография может иметь наименьшую вероятность соответствия из всех остальных фотографий, предложенных на выбор.

Впрочем, мы рассматривали условия работы системы далекие от идеальных. Если же обеспечить корректные условия для работы системы распознавания лиц SmartEye, то поиск и сравнение в базе производятся достаточно уверенно. Система находит в базе лица с уверенностью распознавания 70-90%. На практике можно ставить порог срабатывания 70%, и ошибка ложного распознавания будет исключена, хотя возможность нераспознавания в любом случае будет сохраняться, так как нельзя гарантировать того, что человек обязательно будет смотреть в телекамеру и не крутить при этом головой достаточно продолжительное для распознавания время.

В итоге после знакомства с системой мы пришли к выводу, что

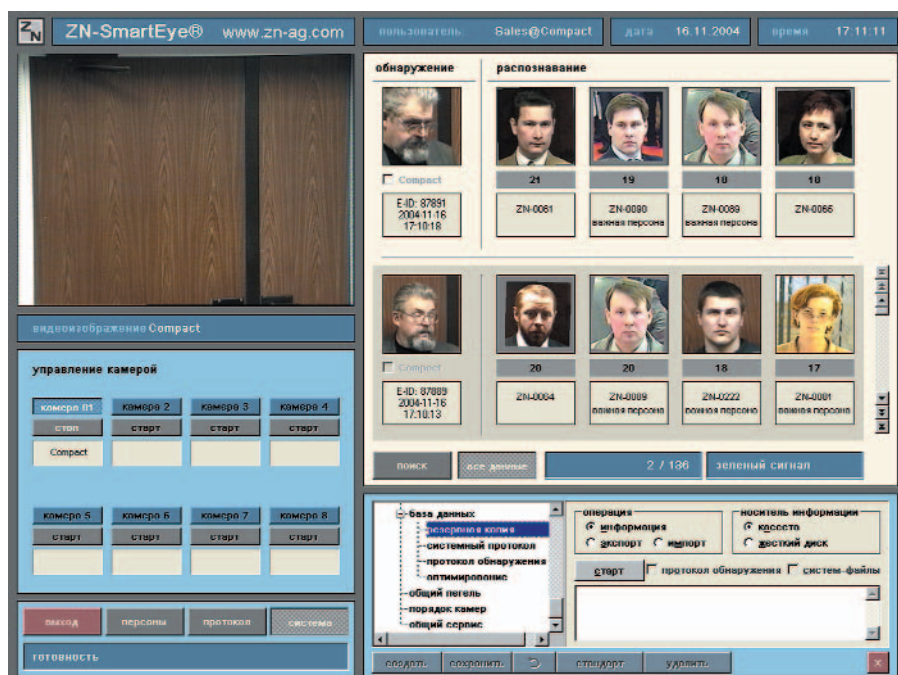


Статус работы модулей системы.

SmartEye вполне функциональная и работоспособная система, которую вполне можно применять для ограничения доступа нежелательных лиц. Основные требования системы к освещению и ракурсу лица накладывают определенные ограничения на сферу применения системы SmartEye, то есть систему не получится применить для поиска лиц в толпе, так как там не удастся создать идеальные условия ее работы, и качество распознавания будет на очень низком уровне. Если же удаст-

ся создать идеальные условия, а в первую очередь это касается даже не требований к освещению, которые достаточно несложно обеспечить, а получение качественного снимка лица в фас, то SmartEye сможет полностью раскрыть все свои возможности.

Для того чтобы повысить вероятность получения качественной фотографии лица в фас, можно предложить следующий вариант. Телекамера, подключенная к системе распознавания лиц, устанавливается на стойку или стол рядом с сотрудником службы безопасности или любым другим сотрудником, который будет обращаться ко всем входящим с определенным вопросом. При ответе посетитель обычно смотрит спрашивающему прямо в лицо, и в этот момент правильно расположенная телекамера, допустим, слева или справа от спрашивающего, может переслать системе хороший снимок. Очевидно, что для работы с такой системой потребуются обученный персонал, который в случае неуверенного распознавания лица будет принимать сам решения на основе предложенных системой на выбор фотографий, а не соглашаться с первой предложенной. Также следует всегда помнить о необходимости иметь качественную базу фотографий и производить очень тщательную настройку системы (или прибегнуть для этого к услугам квалифицированного специалиста).



Система распознавания лиц предоставляет несколько возможностей для резервного копирования данных. В данном случае копирование возможно на жесткий диск и на встроенный стример.

Модуль распознавания лиц в интегрированной системе ITV Интеллект (Cognitec Systems GmbH)

Мы выбрали столь сложное название для нашего тест-драйва вовсе не из любви к громоздким наименованиям, которых предостаточно на отечественном рынке систем безопасности, а для точности. Ни для кого уже, наверное, не секрет, что компания ITV сейчас активно занимается интегрированием в свою систему Интеллект разнообразного оборудования и технологий, доступных на рынке.

Это стремление, конечно, похвально, но, как правило, приводит к тому, что, сделав ставку на одну технологию, компания, занимающаяся интеграцией, "забывает" о других технологиях, конкурирующих с первой. Даже если изначальная ставка на определенную технологию и была верна, расстановка сил достаточно быстро меняется особенно в сфере интеллектуальных технологий, к которой, безусловно, относятся технологии распознавания лиц. Не исключено, что спустя некоторое время выбранная технология, бывшая прежде одним из лидеров, утратит свои позиции и окажется в хвосте прогресса. В результате конечный пользователь лишается свободы выбора и приобретает, фактически навязанную ему связку продуктов, которая не всегда является оптимальной для его целей.

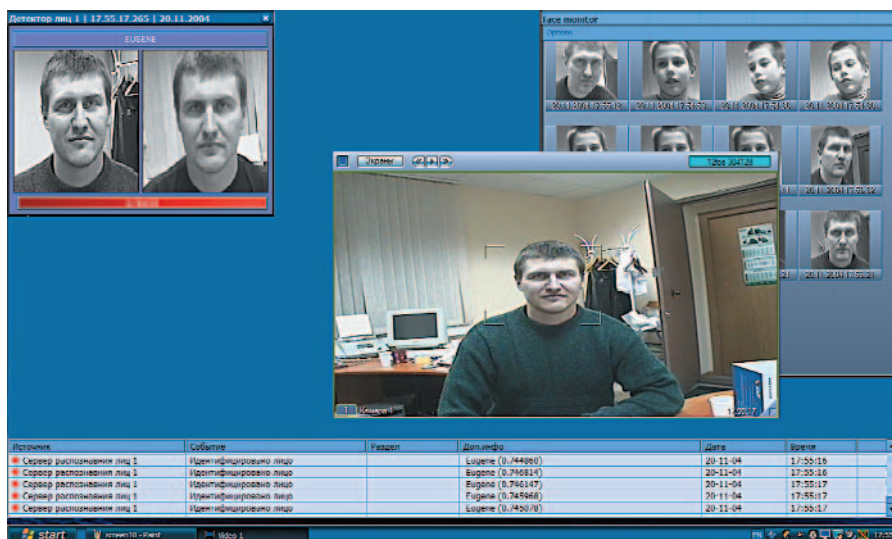
Впрочем, оставив в стороне грустные размышления о последствиях технического прогресса, нужно заметить, что в систему Интеллект в настоящее время интегрировано два модуля распознавания лиц, что позволяет пользователю сделать хотя бы какой-то выбор. Первый

модуль, разработанный компанией Asia Software из Казахстана, был интегрирован в систему Интеллект первым и уже достаточно давно находится в продаже. Его работу демонстрировали на разнообразных выставках и, поэтому для нашего тестирования мы выбрали второй модуль распознавания лиц, разработанный немецкой компанией Cognitec. Здесь мы снова оказались, как говорится, "впереди планеты всей", и наши читатели смогут одними из первых познакомиться с работой модуля распознавания лиц от Cognitec, интегрированного в систему Интеллект.

Сама система предоставляет только удобный интерфейс для модуля распознавания лиц, но сама по себе никакой новой функциональности ему не добавляет и не участвует в процессе распознавания.

Принципы работы модуля распознавания достаточно просты, если отбросить стоящую за ними математику. Остановимся подробнее на принципах работы этой патентованной технологии от Cognitec, которая называется FaceVACS. Обработываются 8-битные черно-белые изображения (256 градаций яркости). Цветные изображения предварительно приводятся к этому формату. Весь процесс распознавания лиц разбивается на следующие этапы.

1. Локализация лица. При этом производится анализ изображения, где определяются размер и положение одного или более лиц. Для простоты объяснения далее будет предполагаться, что система обнаружила только одно лицо на изображении. Для локализации лица формируется так называемая пирамида изображений, которая пред-



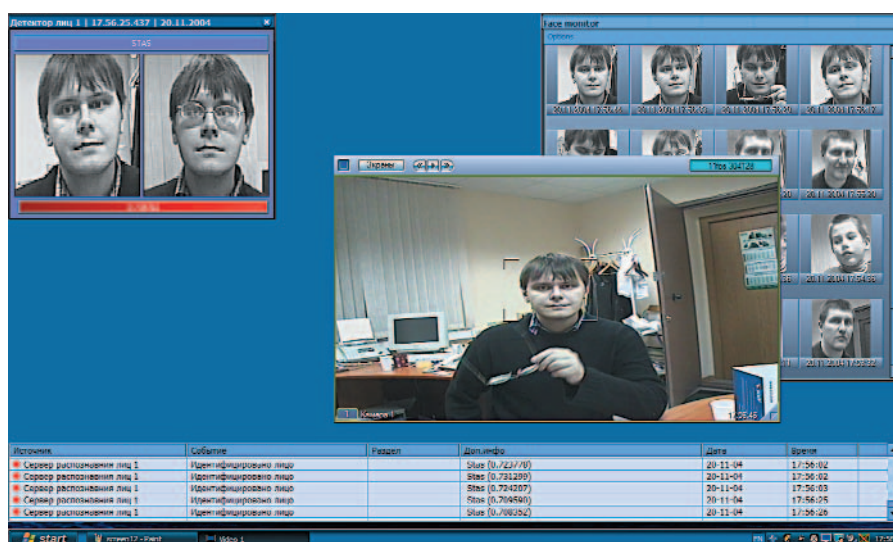
Пример удачного распознавания лица

ставляет собой несколько копий исходного изображения с различным разрешением. Эти копии изображения сканируются специальной маской, которая определяет вероятность нахождения лица в каждой позиции маски. Если эта вероятность достаточно велика, то предполагается, что в данной позиции маски на копии определенного разрешения исходного изображения присутствует лицо. Исходя из данных о позиции лица и разрешения копии, рассчитывается позиция и размер лица на исходном изображении.

2. Локализация глаз. Определяется положение центров глаз. Они и будут опорными точками при дальнейшем анализе лица. Первое определение положения глаз рассчитывается приблизительно на локализованном на предыдущем этапе лице. Затем по соседству с двумя приблизительными позициями производится поиск точного положения глаз. Этот поиск очень похож на поиск положения лица за исключением того, что копии изображения в пирамиде имеют более высокое разрешение, чем копии в пирамиде для поиска лица. Позиции, которые имеют наибольшую вероятность того, что в них находятся глаза, и берутся за основу для последующих расчетов.

3. Оценка качества. Проверяется качество лицевой фотографии, чтобы установить, возможны ли следующие шаги. Чтобы фотография оказалась пригодной, она должна соответствовать ряду критериев. Например, фотография лица не должна быть слишком размытой или слишком зашумленной. Если качество фотографии окажется неподходящим, то распознавание лица прекращается.

4. Нормализация. Фотография лица



Очки особо не влияют на вероятность удачного распознавания лица

вырезается из основного изображения, масштабируется и разворачивается таким образом, что полученная фотография имеет стандартные размеры и положение центров глаз для удобства последующего сравнения. То есть зрачки глаз располагаются на одной заранее определенной горизонтальной линии, которая будет одинакова для всех таких фотографий. Кроме того, фотография выравнивается по центру таким образом, что ее центр лежит на половине отрезка, соединяющего центры двух глаз на фотографии. В параметрах конфигурации модуля можно задавать минимальное и максимальное расстояние между глазами.

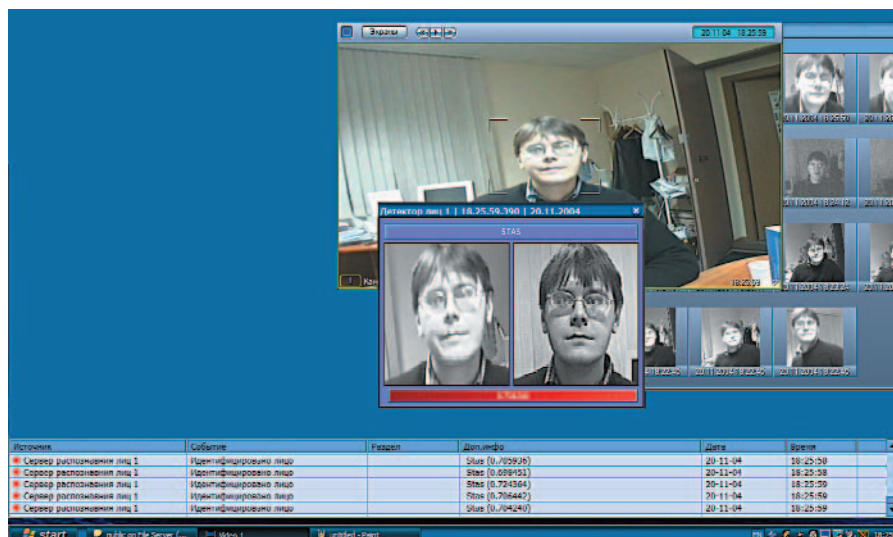
5. Предварительная обработка. Нормализованное изображение проходит предварительную обработку стандартными методами, такими как гистограммная эквализация, нормализация яркости и т.д.

6. Выделение характерных черт лица. В обработанном изображении лица

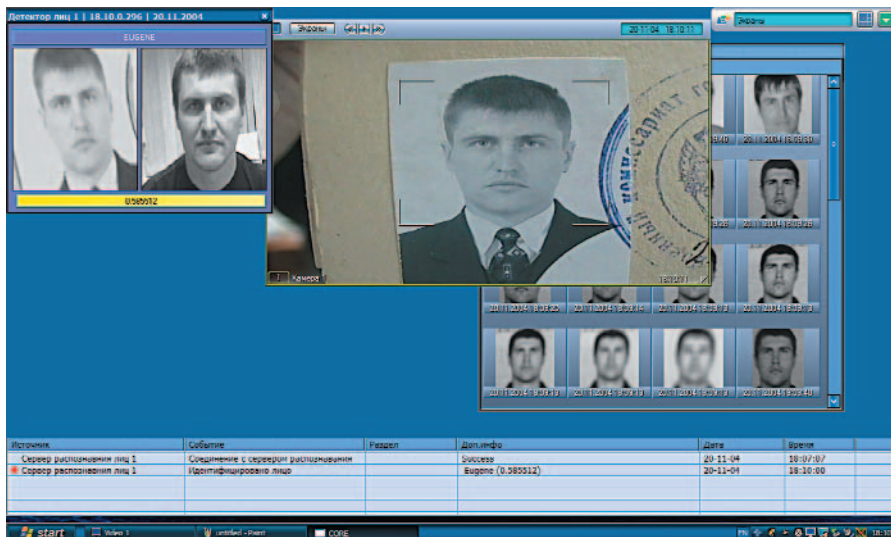
выделяются характерные черты, по которым можно отличить одно лицо от другого. Выделение характерных признаков начинается с того, что к заданным зонам фотографии лица применяются преобразования (например, амплитуды определенных пространственных частот в заданных зонах лица), достаточные для того, чтобы по ним можно было различать разные лица. Результаты сводятся в векторной форме. К полученным результатам применяется глобальное преобразование. Параметры этого преобразования были определены экспериментально на основе большой базы данных фотографий, чтобы уверенно отличать разные фотографии и в то же время, определять сходство разных фотографий одного лица с учетом реальных условий. Результаты глобального преобразования также выражаются в векторной форме в многомерном пространстве.

7. Создание набора признаков. В процессе регистрации характерных черт лица (обычно по нескольким фотографиям) они собираются в набор признаков, который также называется "биометрический шаблон". В генерируемый набор признаков могут входить несколько фотографий (до 5) для того, чтобы учесть возможные ракурсы лица. Полученный набор признаков представляет собой центры кластеров результатов предшествующего глобального преобразования. Эти усредненные значения и используются в последующем сравнении.

8. Сравнение. Сама функция сравнения наборов признаков достаточно проста, что ускоряет вычисления и позволяет проводить быстрое срав-



Распознавание возможно даже при неудачном освещении



Распознавание по фотографии возможно, но не всегда проводится успешно

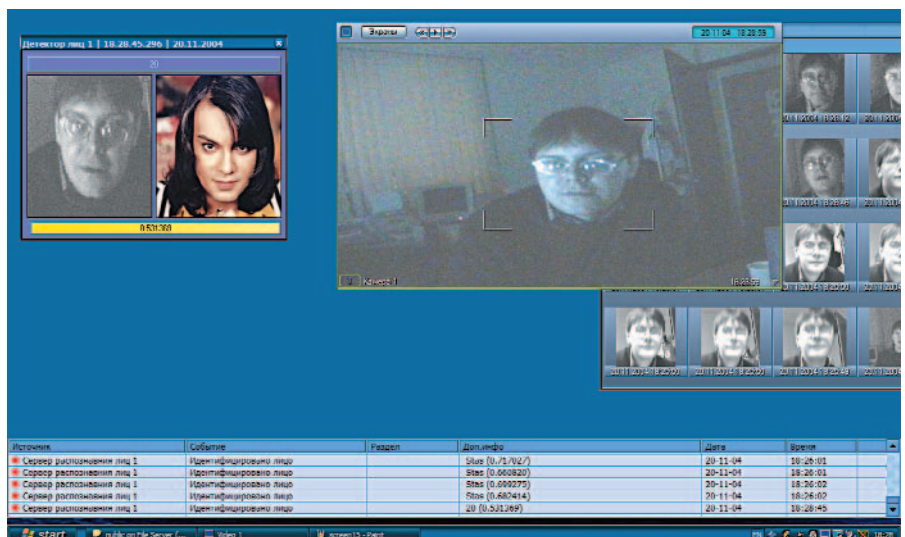
нение даже по очень большим базам данных. При идентификации один набор признаков, полученный из изображения, сравнивается с наборами признаков, которые содержатся в базе данных. При верификации полученный набор признаков сравнивается только с одним набором признаков, который содержится в базе данных. В обоих случаях из базы данных выбирается тот набор признаков, который имеет наибольшую вероятность совпадения с полученным набором признаков. Порог сравнения, то есть наименьшая вероятность совпадения, задается пользователем.

Переходя к самому тестированию, мы пропустим вопросы, связанные с установкой модуля и конфигурированием его по следующим причинам. Разработчики из ITV предоставили в распоряжение нашей тестовой лаборатории уже готовую систему распознавания лиц. Но даже если бы это было не так, добавление одного модуля в систему не представляется серьезной проблемой. Что касается конфигурирования модуля распознавания лиц, то, к сожалению, мы вынуждены заметить, что настроек обнаружить не удалось, так как разработчики из ITV в процессе интеграции модуля в систему Интеллект решили не делать их доступными для пользователей и ограничились только самыми необходимыми параметрами. Мотивация этого решения была самая что ни на есть благородная, поскольку разработчики стремились максимально облегчить жизнь пользователю, но это значительно сужает возможности по адаптации системы к различным условиям эксплуатации.

После запуска системы Интеллект с интегрированным модулем распознавания лиц помимо основного окна, в котором выводится изображение телекамер, мы видим еще и дополнительное окно Face monitor, в котором выводятся все изображения, зафиксированные системой лиц. Вначале это окно пустое, но при появлении людей в кадре станет быстро заполняться, так как модуль распознавания лиц выбирает не один предположительно самый удачный кадр, а набирает несколько кадров с разными ракурсами лица, что упрощает поиск соответствия в базе. При этом в основном окне процесс обнаружения и отслеживания лиц показывается визуально рамкой, очерчивающей границы лица. В случае обнаружения совпадения появляется еще одно всплывающее окно, в правой части которого находится фотография из базы данных, а в левой - фотография лица, обнаруженного в кадре. Под ними указана вероятность совпадения (число,

принимающее промежуточные значения от 0 до 1). Цвет фона этого поля зависит от того, насколько высока вероятность совпадения. "Зеленый" - вероятность очень низка. "Желтый" - вероятность совпадения достаточно высока, но возможна ошибка. "Красный" - очень высокая вероятность совпадения. В верхней части окна выводятся название фотографии в базе данных и время обнаружения. Это окно будет присутствовать на экране до тех пор, пока пользователь его не закроет или система не обнаружит новое совпадение, после чего появится то же окно, но с новыми фотографиями. Также интерфейс модуля распознавания лиц позволяет просматривать содержащиеся в базе данных фотографии, подключать новые базы данных, добавлять новые фотографии из тех, что попали в кадр или импортировать фотографии из файлов. Как уже было сказано выше, сам модуль распознавания лиц работает с черно-белыми фотографиями, но это не значит, что цветные фотографии нельзя добавлять в базу данных. Независимо от того, цветная или черно-белая фотография, на стадии обработки будет "вырезано" черно-белое изображение. Для удобства самого пользователя мы бы рекомендовали добавлять из файла именно цветные фотографии, так как цвет лица тоже может быть отличительным признаком (например, в США, где таким образом можно сразу визуально отличать европеоидов, негроидов и монголоидов). Хотя цвет лица и не учитывается системой при сравнении, сам пользователь все же будет его различать.

Как видно на иллюстрации, пользовательский интерфейс сделан максимально простым. Настолько же про-



Недостаточное освещение может привести к ошибочному распознаванию

ста и настройка модуля распознавания лиц, которая осуществляется в меню конфигурации системы Интеллект. В пункте меню "Оборудование" добавляется сервер распознавания лиц, которому можно указать, какой модуль использовать (от Cognites или Asia Software). Также можно указать минимальный порог при сравнении фотографий. В нашем случае один сервер распознавания лиц поддерживал 4 детектора лиц, которые настраиваются отдельно. При их настройке можно указать, к какой телекамере осуществить привязку детектора лиц, и задать обработку всех кадров или только каждого 2, 3 и т.д. Это снижает нагрузку на центральный процессор компьютера, но может привести к тому, что системе потребуется больше времени для того, чтобы захватить нужное для сравнения количество кадров. Здесь же можно определить размеры площади, которое может занимать в кадре лицо (от 1.0 до 3.0). Рекомендованное значение 1.4 прекрасно подходит для большинства случаев, но если лицо человека оказывается слишком близко к телекамере и может занимать значительную часть кадра, то это значение лучше увеличить. Хотелось бы, конечно, видеть больше возможностей для настройки модуля распознавания лиц, и, в первую очередь возможность настройки нескольких зон обнаружения, таких как, например, в привычных всем детекторах движения, но таких возможностей нет. Также имело бы смысла для определенных сфер применения выводить не одну, наиболее похожую фотографию, а несколько в порядке убывания вероятности совпадения. Не исключено, что все это



За лицо система может принять любой объект отдаленно напоминающий лицо, но ошибочного распознавания не происходит



Добавление фотографий в базу данных

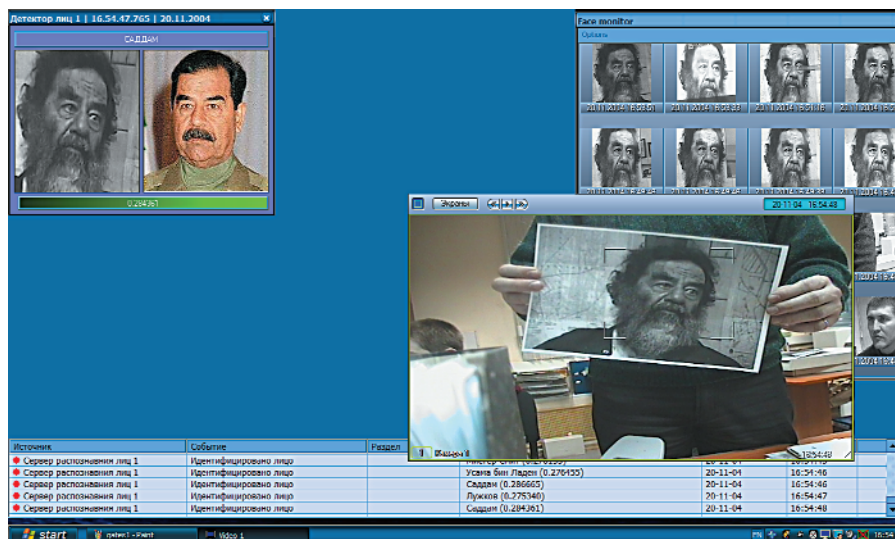
появится в следующих версиях. Как говорится, "поживем - увидим".

Модуль распознавания лиц мы решили тестировать в помещении при искусственном освещении. Конфигурация тестового компьютера была

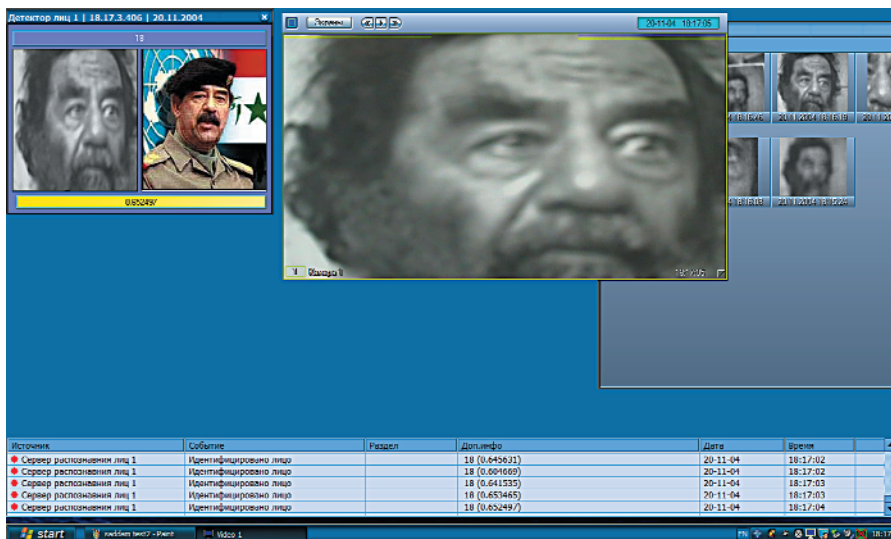
следующая:

Процессор Intel Pentium 4 3.00 ГГц
512 МБ оперативной памяти
Видеокарта Radeon 9950
Системная плата Asus P4P800SE
Операционная система Microsoft Windows XP Professional Version 2002 Service Pack 2

Поскольку любое тестирование в нашем журнале носит исключительно практический характер, мы поставили перед системой следующую задачу. Допустим, мы хотим ограничить доступ в нашу тестовую лабораторию, разрешив его только определенным сотрудникам, а все остальные лица приравниваются к нежелательным посетителям. Делается это таким образом. Каждый сотрудник, которого необходимо занести в базу, садится напротив телекамеры и смотрит в нее. Система получает несколько снимков лица в разных ракурсах, из которых выбирается лучший, то есть такой, где ли-



Пример неудачного сравнения фотографий



Пример удачного сравнения фотографий

цо отчетливо видно, повернуто ровно в сторону телекамеры, выражение лица естественное. Таким образом, мы вводим 10 фотографий. Чтобы несколько усложнить задачу, мы вводим в базу данных еще 20 фотографий (цветных) известных политиков, звезд эстрады и кино. Вряд ли кто-нибудь из них мог оказаться в нашей тестовой лаборатории и помешать эксперименту.

Все фотографии, попавшие в базу данных, соответствовали минимальным требованиям, предъявляемым к фотографиям для успешного распознавания: фотография четкая, расстояние между зрачками превышает 32 пиксела, контраст лица и фона превышает 64 градации. Эти требования оказались вполне обоснованными. Так как при небольшом размере лица в кадре фотографии (то есть примерно менее 50 пикселей в ширину модуль распознавания лиц продолжает отслеживать лицо, но сравнение лиц не производится, хотя фотографии и остаются в системе. Впрочем, чтобы несколько усложнить задачу, мы добавили в базу данных и два рисунка, сделанных от руки, а также две размытые фотографии, так как в реальности при работе с большими базами данных в них может оказаться фотографии самого разного качества.

Еще одно требование, предъявляемое к фотографиям, связано с максимально допустимым углом поворота головы. Как и многие другие системы распознавания лиц, модуль от Cognitec допускает поворот головы влево или вправо на 15 градусов. Если этот угол будет превышен, то модуль все равно локализует лицо (окончательно он его потеряет только при угле

поворота 90 градусов), но распознавание будет невозможно. Что касается наклона головы, то к нему система в целом менее чувствительна, чем к повороту головы. Это, вероятно, связано с тем, что при подъеме или наклоне головы изменяется освещенность лица, а к изменению освещения модуль распознавания лиц от Cognitec оказался малочувствителен, что можно оценивать как значительный плюс в первую очередь именно этого алгоритма распознавания лиц.

В рамках тестирования мы вводили в базу данных и засвеченные фотографии, и специально засвечивали лицо в кадре, при этом вероятность совпадения не снижалась более 5 процентов, хотя, например, человеку уже сложно было опознать даже свое собственное лицо по такой фотографии, так как человек не видит промежуточного кадра после этапа предварительной обработки.

Головные уборы, очки не оказывают

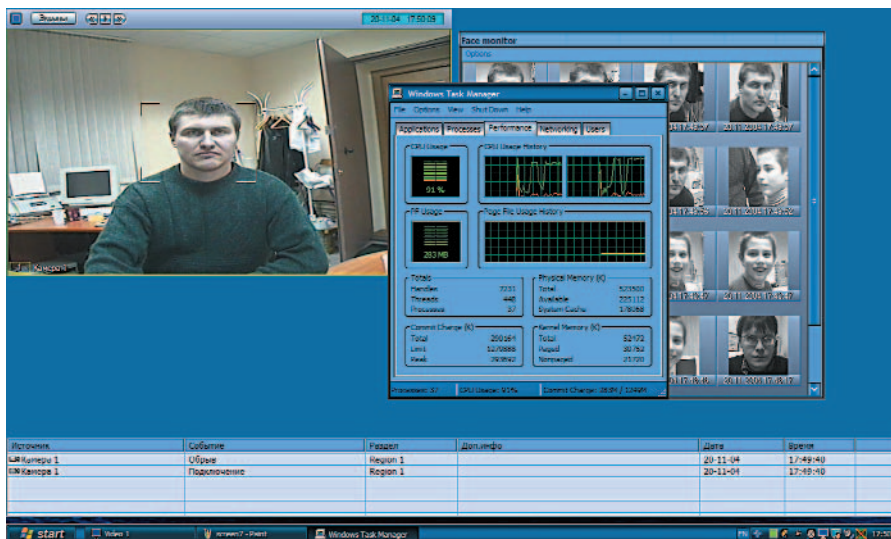
влияния на уверенность распознавания (снижение вероятности распознавания в пределах 3%). Как с очками, так и без них, система распознавала лицо практически одинаково, хотя солнцезащитные очки или постоянные блики в обычных очках не дадут провести сравнение, так как система не найдет зрачки. Это уже неизбежно, так как модуль распознавания лица требуется точно определить положение зрачков.

Разработчики из Cognitec утверждают, что их модуль может распознать даже частично прикрытое или заслоненное лицо. Мы не сумели найти подтверждения их словам и пришли к выводу, что лицо должно быть обязательно открыто. Кроме того, даже незначительное изменение мимики лица (улыбка, закрытые глаза) немного снижает уверенность распознавания (в пределах 5 процентов), если же изменения в мимике будут более значительными (гримасы), то модуль может обнаружить с уверенностью до 50% сходство лица с фотографией, ничего общего на первый взгляд с таким лицом не имеющее.

Также выяснился ряд любопытных моментов. Во-первых, система не столь уж чувствительна к резкости фотографии: мы специально вводили фотографии из кадра, полученного с расфокусированной телекамеры, и качество распознавания снижалось совсем незначительно (до 10% при самом размытом изображении). Конечно, если полностью расфокусировать объектив телекамеры, то не только система распознавания лиц, но и человек ничего не увидит. Во-вторых, некачественное изображение с большим количеством шумов особенно при недостаточном освещении делает невозможным рас-



Загрузка процессора невелика в режиме поиска лица



При появлении лица в кадре загрузка процессора резко возрастает

познавание, хотя человек без проблем опознает лицо в кадре. В этом аспекте требования к качеству изображения будут такими же, как у многих ярких детекторов движения.

В процессе тестирования модуль распознавания очень уверенно сравнивал всех наших сотрудников с их фотографиями, но при этом на практике никогда нельзя получить 100% или даже 90% вероятности совпадения. Вероятности варьируются в следующих пределах: 15-40% (фотографии непохожи либо ракурс выбран неудачный), 40-55% (фотографии немного похожи, но ошибка вероятна), 55-70% (фотографии очень похожи, ошибка маловероятна), 70-75% (полное совпадение, ошибка исключена). Разработчики рекомендуют устанавливать порог распознавания 50% (0.5). Впрочем, в результате тестирования мы пришли к выводу, что для целей точного распознавания можно поставить порог 70% (0.7), хотя для этого человеку придется немного дольше находить перед телекамерой. Любопытно, что интервал вероятности распознавания при сравнении человека с его фотографией, сделанной незадолго до этого, оказывается один и тот же (70-75%).

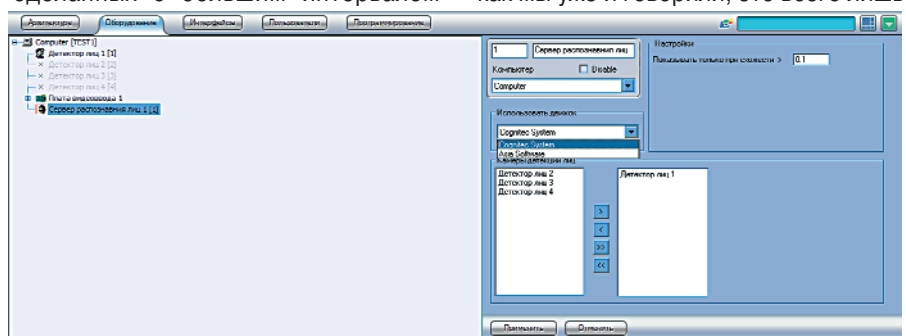
Технология FaceVACS от Cognitec поддерживает дополнительную проверку на "объемность" изображения в кадре, чтобы исключить распознавание фотографии, поднесенной к телекамере. В нашем случае эта проверка была отключена, поэтому при поднесении фотографии к телекамере, система опознает фотографию как лицо, хотя и не так уверенно, как настоящее лицо. Вероятность распознавания будет ниже. Более того, если взять листок

бумаги и нарисовать на нем схематично лицо, а потом поднести листок телекамере, то и его система воспринимает как лицо человека, хотя, конечно, и не спутает его ни с одной фотографией в базе данных.

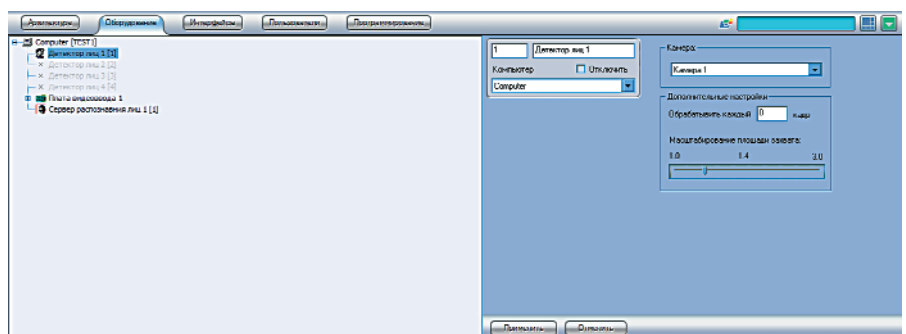
Чтобы посмотреть, как система работает с различными возрастными изменениями на фотографиях, мы пытались сравнивать старые и новые фотографии (в пределах 10 лет) с документов. Впрочем, стабильных результатов получить нам не удалось. В редких случаях уверенность сравнения у системы доходила до 50%. Но все же можно с уверенностью сказать, что все рассказы о том, как различные системы распознавания лиц уверенно находят совпадения на фотографиях, сделанных с большим интервалом

времени - это не более чем рекламный миф. То есть это возможно, но в тех случаях, когда лицо не изменилось, или изменилось незначительно, но такие совпадения будут скорее исключением, чем правилом.

В заключение мы провели еще один достаточно любопытный и показательный тест. В базу данных были введены 2 фотографии иракского диктатора Саддама Хусейна. Первая была сделана достаточно давно, вероятно, еще времен так называемой "войны в Заливе" в 1991 году, вторая - накануне последней войны в Ираке. Между фотографиями присутствует легко видимая человеческим глазом разница, но любой уверенно скажет, что на фотографии изображен один и тот же человек. Модуль распознавания лиц ничего общего между ними не нашел. Тогда мы взяли третью фотографию, сделанную в то время, когда американские военные захватили в плен Саддама. Эта фотография обошла весь мир, и, многие помнят изображенного на ней иракского диктатора с огромной бородой. Думаю, не каждый человек тогда смог бы уверенно сказать, что американцы захватили именно Саддама Хусейна. Когда мы поднесли эту фотографию к объективу телекамеры системы уверенно сравнила фотографию с более поздней (65%), лишней раз подтвердив, что был захвачен все таки иракский диктатор. Впрочем, система не сочла его похожим на более раннюю фотографию (всего только 28%). Но как мы уже и говорили, это всего лишь



Настройки позволяют выставить распознавание лиц по 4 каналам



Меню конфигурации модуля распознавания лиц

исключение из правила и не стоит даже думать о серьезном применении системы распознавания лиц в криминалистике для идентификации.

Отдельно следует сказать о загрузке процессора. Мы ожидали, что алгоритм распознавания лиц будет весьма ресурсоемким, так как обязательно будет требовать огромного количества вычислений. Но загрузка центрального процессора превзошла даже все наши смелые предположения. Она оказалась просто гигантской. На тестовом компьютере, который оказался в нашем распоряжении, был установлен вполне современный центральный процессор Intel Pentium 4 с частотой 3 ГГц и поддержкой технологии Hyper-Threading, которую, кстати, поддерживала и сама система распознавания лиц, иначе бы никакой пользы от этой технологии не было. До тех пор пока в кадре не появлялся объект, который система интерпретировала как лицо, загрузка процессора была минимальной. С появлением в кадре лица загрузка моментально возрастала до 90%. То есть, казалось бы, загрузка процессора достаточно высока, но си-

стема еще справляется с обработкой 1 канала. На самом деле, хотя в настройках системы было указано обрабатывать каждый кадр темп ввода кадров составлял не 25 к/с, а только 12 к/с. Хотя это не оказывало существенного влияния на процесс распознавания, но для работы модуля распознавания лиц на каждом кадре при скорости ввода 25 к/с даже на одном канале потребуются вдвое более производительный процессор, не говоря о том, чтобы вести распознавание лиц по 4 каналам одновременно. Можно, конечно, снижать темп ввода кадров или обрабатывать модулем распознавания не все кадры, а только, допустим три кадра в секунду. Но при этом нужно учитывать, что слишком низкая скорость обработки кадров модулем распознавания лиц затрудняет его работу, так как алгоритму потребуется больше времени для получения удачных с точки зрения распознавания ракурсов.

По информации от разработчиков, загрузка процессора мало зависит от самого процессора, так как модуль всегда дает загрузку около 90-100% даже в случае с двухпроцессорными

конфигурациями (возможно, скорость обработки автоматически регулируется в модуле). Но при этом обеспечивается нормальная работа других модулей. Также не рекомендуется устанавливать на одном компьютере модули захвата лиц и модуль распознавания лиц, то есть рекомендуется создавать распределенные конфигурации.

Также нужно учитывать, что модуль распознавания лиц, если соблюдены все требования, способен одновременно находить в кадре более одного лица (удалось находить 4-5 лиц), но при этом системе потребуется больше ресурсов, так как количество вычислений будет возрастать пропорционально количеству распознаваемых лиц.

Сама компания Cognitec в первую очередь применяет свою патентованную технологию распознавания лиц в системах контроля доступа, и, разумеется, FaceVACS в первую очередь оптимизирована именно для этой сферы применения, как это и подтвердили результаты тестирования. Попытки применения в другой сфере потребуют значительной адаптации и оптимизации этого модуля.

От аналогового к цифровому

Хотя мы все в той или иной степени понимаем, что представляют собой аналоговые и цифровые сигналы, Джон Уоткинс (John Watkins) из компании Snell&Wilcox в этой статье подробно объясняет теорию, на которой основывается приобретающий все большее значение мир цифрового видео.

Мир телевидения и телевидения становится цифровым. Есть существенные причины, по которым это происходит, и которые мы рассмотрим здесь. Просто так никто не переходит на цифровые технологии. Возможно, это сейчас считается престижным, но должны быть более серьезные причины, например, экономические. Здесь все достаточно просто: правильно спланированная система цифрового телевидения обходится дешевле в повседневной эксплуатации, чем аналоговая система, выполняющая те же самые функции. Цифровая система имеет меньшее время простоя и требует меньше запланированного и незапланированного технического обслуживания.

Экспериментальная фаза завершена, и теперь, когда цифровые технологии достигли зрелости, что выразилось в разработке надежного и экономически эффективного оборудования, именно аналоговые технологии неожиданно оказались нерентабельными. Меняется не просто оборудование, изменяется сама природа телевидения.

Мир телевидения изменился с изобретением видеомagneтофонов. Зрители смогли записывать телепередачи и просматривать их позже или покупать видеокассеты по своему выбору. Так появилась ранняя форма видео по запросу (Video-on-Demand). Когда наступило время конкуренции от кабельного и спутникового телевидения, снова произошли изменения. Сейчас на какой-то период времени все успокоилось.

Соотношение сторон кадра изменилось с 4:3 на 16:9. На экранах наших телевизоров появились более качественные изображения за счет улучшенных стандартов сигналов. По экономическим выкладкам, новое телевидение вынуждено будет использо-

вать компрессию, а это означает, что оно будет цифровым.

Технологии массового хранения из компьютерной области в сочетании с технологиями сжатия видеоизображения позволяют создавать полноценное видео по запросу, где выбор телезрителей передается на сервер по обратной связи. Эта обратная связь дает возможность осуществлять покупки, не выходя из дома, и устраивать интерактивные телепередачи. Персональные компьютеры уже сейчас способны принимать телевизионное изображение и воспроизводить диски со сжатым видеоизображением.

Поэтому, если вы только не собираетесь открыть овцеферму, то вопрос об использовании цифровых технологий для вас не существует. Здесь скорее стоит вопрос, когда и до какой степени их использовать.

С помощью цифровых технологий можно выполнить ту же работу, что и с помощью аналоговых, но несколько иным образом и с большим удобством. Если относится к цифровому оборудованию как к аналоговому, то ничего хорошего из этого не выйдет, а удобство в работе пропадет. Если относится к нему правильно, то вы пожнете все плоды. Одной из задач этой статьи объяснить, что значит "правильно".

Мир цифровых технологий сложен, и математики могут неплохо пораз-

влекаться, засыпав слушателей формулами и терминами, которые имеют смысл только для специалистов по космическим технологиям. Эта статья не для них. Она написана для обычных людей, которые хотят самостоятельно принимать решения, но не оказаться погребенными под лавиной деталей. Поэтому здесь нет никакой математики, а специальная терминология используется только тогда, когда можно объяснить, что она обозначает, а не для того, чтобы показать, каких успехов мы добились на этой стезе.

Что значит "оцифрованный"

Оцифрованный телевизионный сигнал - это всего лишь еще одно представление телевизионного сигнала, то есть сигнал представлен в цифровом виде. На рисунке 1 показано, как обычная аналоговая телевизионная система разбивает время на кадры и поля, а затем разбивает поля на строки. Оба эти процесса называются дискретизацией: представление чего-либо непрерывного через периодические дискретные измерения. В цифровом телевидении мы просто продолжаем процесс дискретизации в третье измерение таким образом, что телевизионные линии разбиваются на точки, которые называются пикселями. На рисунке 1b показано, каким образом телевизионная строка разбивается на пиксели.

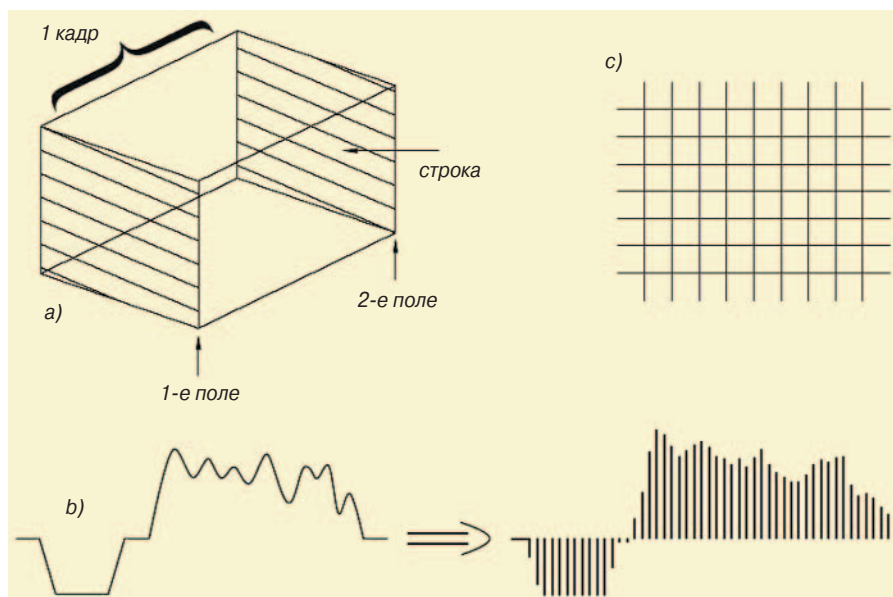


Рис. 1а. В аналоговом телевидении время разбивается на поля, и каждое поле разбивается вертикально на строки. Если разбить каждую строку (b), то формируется матрица пикселей. Такая матрица пикселей получается из аналогового телевизионного сигнала при дискретизации строки по времени (с).

Обычный кадр (NTSC) содержит примерно 1/3 миллиона пикселей. В компьютерной графике размеры пиксела по горизонтали и вертикали зачастую совпадают, что дает так называемый "квадратный пиксел". В вещательных телевизионных системах пиксели не совсем квадратные по причинам, которые мы изложим ниже. После того как кадр разбит на пиксели, значение каждого пиксела представляется числом. На рисунке 1с показано, как оцифровывается аналоговая телевизионная строка. Это похоже на рисование на бумаге в клетку. Горизонтальная ось отображает количество пикселей на экране. Вертикальная ось показывает размах видеосигнала.

График нашего видеосигнала теперь можно передать куда угодно, последовательно указав только значения по вертикальной оси для каждого пиксела. В результате видеосигнал будет представлен последовательностью целых чисел, иначе говоря, потоком данных.

Таким образом может быть оцифрован любой сигнал. В случае с аналоговым телевизионным сигналом присутствует только один сигнал на канал. Когда оцифровывается телевизионный сигнал, то он, включая цветность, просто выражается числами. Цифровое телевидение по-прежнему имеет такие же характеристики, как и аналоговое.

Если используется аналоговый компонентный видеосигнал, то будут присутствовать три синхронных сигнала на канал. Потребуется три конвертора для получения трех потоков данных для представления RGB или цветоразностных компонент.

После преобразования видео- или аудиосигналов в данные мы можем использовать различные информационные технологии хранения, обработки и передачи данных. Цифровая передача данных имеет преимущество перед аналоговой в том, что она позволяет избавиться от шумов и дрожания сигнала. Если мы конвертируем целые числа представляющие видеосигнал в двоичный формат, как это показано на рисунке 2, то получившиеся в результате двоичные цифры, то есть биты, могут быть 0 или 1. Эти два состояния могут быть представлены в любой системе (электрической, оптической, магнитной или механической), в которой существует два состояния. На рисунке 3 изображено, каким образом двоичное число может быть

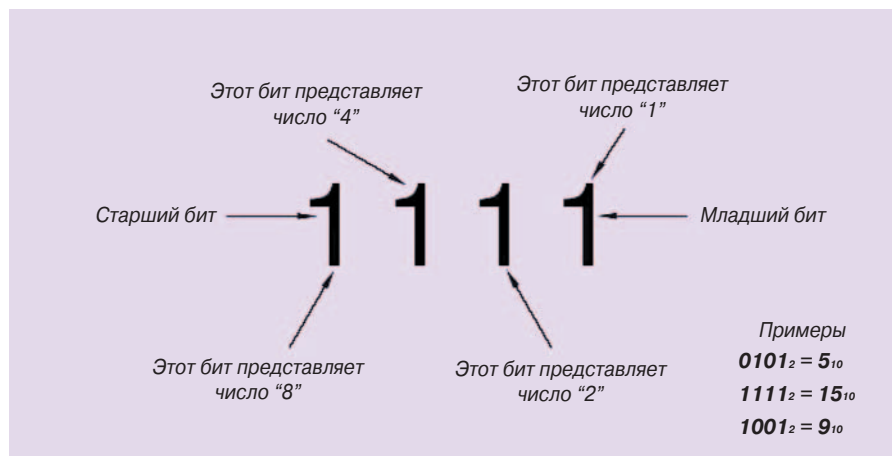


Рис. 2. В двоичном формате можно хранить и передавать любое число в тех системах, которые могут иметь два состояния.

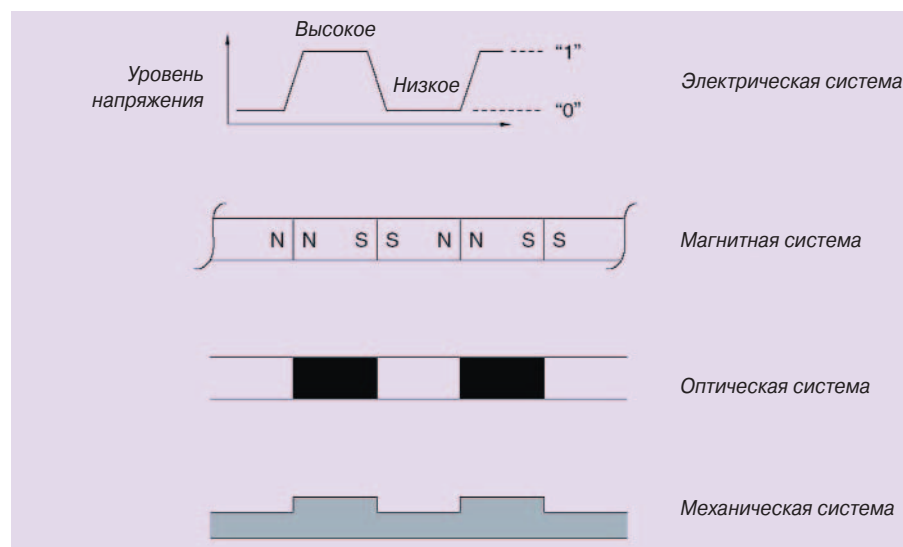


Рис. 3. На рисунке три показано несколько способов представления двоичного потока данных.

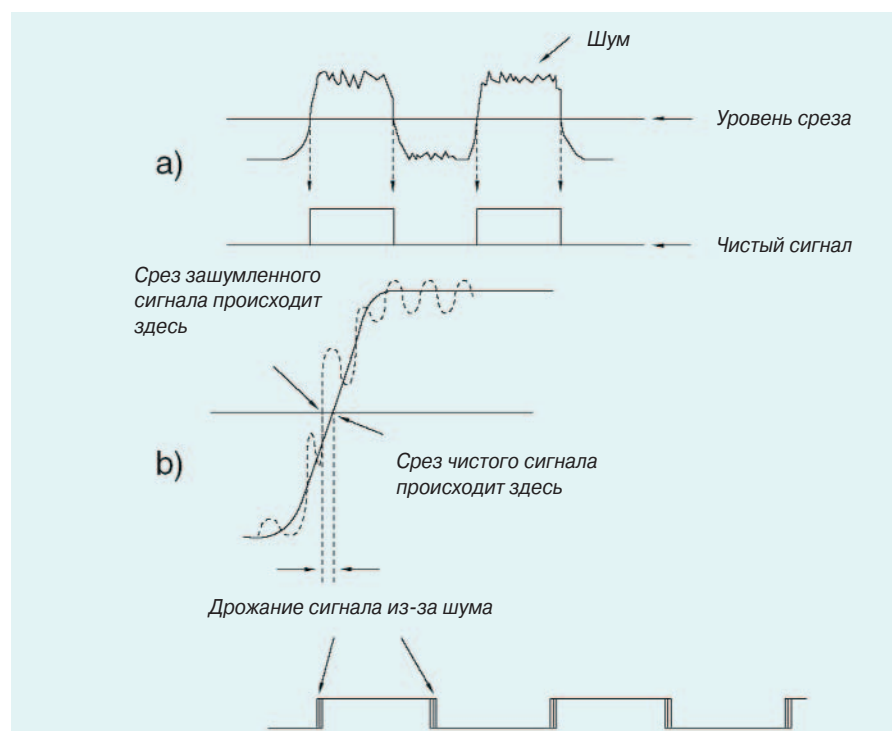


Рис. 4. Преимущество сигнала в двоичном формате заключается в том, что за счет сравнения напряжения сигнала с эталонным значением отбрасывается значительная часть шумов. В результате остается только дрожание сигнала, которое устраняется схемой фазовой синхронизации.

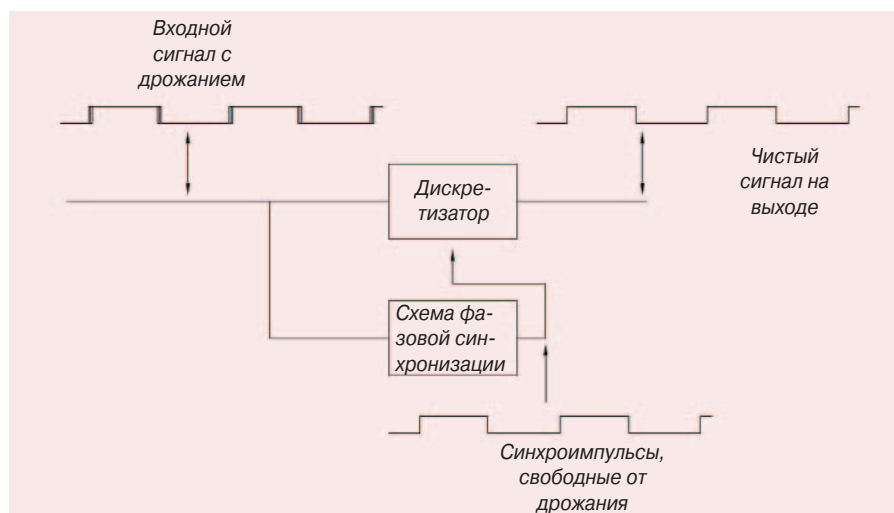


Рис. 5. В результате работы такой схемы на выходе получается сигнал, идентичный тому, который был в передатчике.

представлено электрическим способом (двумя разными напряжениями), магнитным (различным намагничиванием), оптическим (чередованием прозрачных и непрозрачных зон в записи) и механическим (углубления на поверхности лазерного диска).

Так как присутствует только два состояния, то шум легче отфильтровать, чем в любой другой системе. На рисунке 4 это показано на примере электрического интерфейса. Хотя изначально сигнал поступает чистым, но когда он дойдет до приемника, то в нем появятся шум и дрожание. В приемнике происходит сравнение напряжения сигнала с эталонным значением, которое находится посередине между максимальным и минимальным значением. Любое напряжение выше эталонного уровня рассматривается как 1, ниже - как 0. В этом процессе отбрасывается значительная часть шумов, и сигнал снова восстанавливается в первоначальном двоичном формате.

Но таким способом мы сможем отфильтровать только шум, но не дрожание сигнала. Для этого потребуются другой способ. На рисунке 4b показано, как дрожание сигнала искажает его, случайным образом производя смещения по временной оси в его колебаниях. Впрочем, среднее время большого количества колебаний останется неизменным. Схема фазовой синхронизации позволяет усреднить время большого количества колебаний и воссоздать стабильный сигнал. Принцип работы примерно такой же, как и у маховика с поршнем. Маховик усредняет импульсы от поршня, чтобы обеспечить плавное вращение.

Фильтрация шума с ограничением по максимуму и минимуму в сочетании со схемой фазовой синхронизации в англоязычной литературе называется "reclocker". В результате работы такой схемы на выходе получается сигнал, идентичный тому, который был в передатчике. Шум и дрожание исключаются, поэтому потери данных при передаче не происходит. Кроме того, эти схемы мы можем использовать в паре или каскадно и в любом случае на выходе у нас будет чистый сигнал, как показано на рисунке 5.

В цифровых системах такие схемы используются повсеместно. В цифровых видеомагнитофонах они отфильтровывают шум и дрожание сигнала. Также они используются в жестких дисках, проигрывателях компакт-дисков, маршрутизаторах и т.д. Причина такой популярности заключается в том, что они предотвращают ошибки при регенерации сигнала.

Одна из основных причин применения цифровых систем заключается в том, что качество сохраняется в независимости от количества этапов записи и передачи. Впрочем, это справедливо в том случае, если мы не используем компрессию данных. На рисунке 6 показана простейшая система с ана-

логовыми входами и выходами, аналого-цифровым преобразователем (АЦП), цифрово-аналоговым преобразователем (ЦАП) и цифровым видеомагнитофоном с цифровыми входами и выходами. Сигнал, выходящий из АЦП восстанавливается и записывается цифровым видеомагнитофоном на пленку. При воспроизведении с пленки сигнал снова восстанавливается для устранения шумов пленки и дрожания. Вся информация, считанная с пленки и имеющая потери данных, перед отправлением на ЦАП будет восстановлена благодаря системе коррекции ошибок. На ЦАП происходит окончательное восстановление данных, и полученный сигнал будет идентичен тому, который выходил из АЦП.

В результате качество видеоизображения системы определяется только качеством АЦП и ЦАП. АЦП может быть соединен напрямую с ЦАП, то есть цифровой видеомагнитофон будет работать в сквозном режиме в обход пленки. При этом качество изображения не изменится. Это будет верно в том случае, если не используется компрессия изображения, а информация не испорчена избыточным шумом и потерями настолько, что восстановление сигнала и коррекция ошибок станут невозможными в цифровом видеомагнитофоне.

Таким образом, имея дело с цифровыми системами, следует обращать внимание на следующие две вещи:

1. ЦАП и АЦП определяют качество изображения, поэтому нужно использовать самые лучшие из доступных. Экономия на ЦАП и АЦП ни к чему хорошему не приведет.

2. ЦАП и АЦП определяют качество изображения только в том случае, если нет ошибок данных, поэтому всегда нужно следить за целостностью данных.

Целостность данных невозможно измерить с помощью обычного аналогового измерительного оборудования.

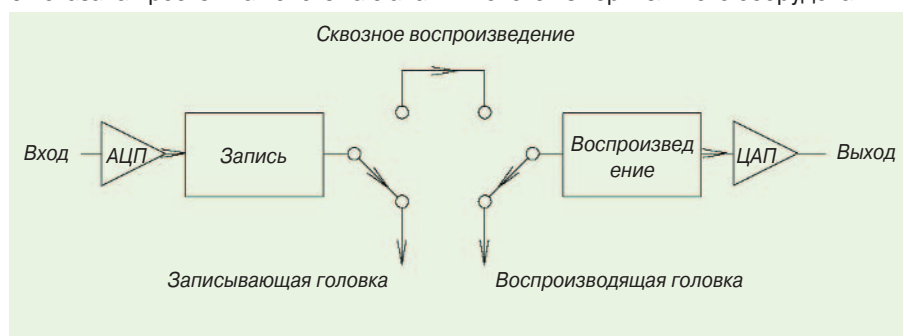


Рис. 6. В простом цифровом видеомагнитофоне с коррекцией ошибок качество изображения при воспроизведении записи будет таким же, как и при сквозном воспроизведении.

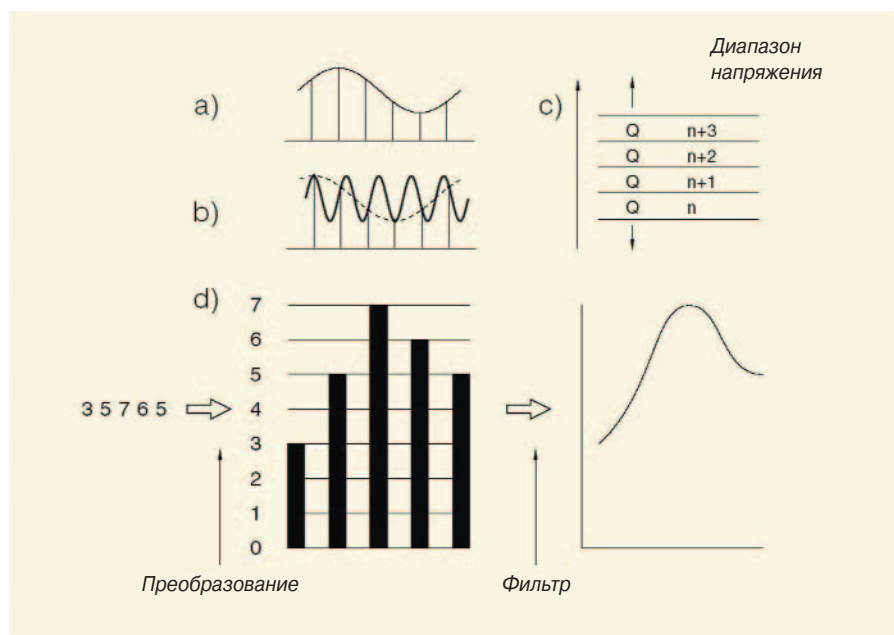


Рис. 7. Интуитивно понятно, что высокой частоты дискретизации будет достаточно. При низкой частоте дискретизации происходит алиасинг, как на рисунке b). При квантовании (рисунок c) диапазон напряжения сигнала разбивается на равные интервалы Q . Квантователь выдает число, соответствующее интервалу, в которое попадает значение аналогового сигнала. d) Числа преобразовываются обратно в импульсы напряжения, а фильтр восстанавливает непрерывный сигнал.

Как преобразовать из аналогового в цифровой вид?

В этой главе мы расскажем об аналогово-цифровом преобразовании, которое во многом определяет качество изображения в цифровых системах. В преобразователях применяются три фундаментальных процесса: фильтрация, дискретизация и квантование.

На рисунке 7a вы видите, что происходит при правильной дискретизации. Форма сигнала сохраняется.

На рисунке 7b показано, что происходит, если взят сигнал, частота которого слишком велика для выбранной частоты дискретизации. В результате получен сигнал неправильной формы. Полученное в результате неправильного выбора частоты дискретизации ложное отображение информации называется алиасингом (aliasing). Этот эффект заметен в кино, когда крутящиеся колеса визуально останавливаются и начинают крутиться обратно. Частота, с которой крутятся спицы колес, слишком высока по сравнению со скоростью обновления кадров.

Алиасинг необходимо предотвратить еще в преобразователях, что достигается за счет использования специальных фильтров до дискретизации сигнала. Этот фильтр отбрасывает частоты, которые выше половины частоты дискретизации, что исключает появление алиасинга.

Помимо процесса дискретизации в АЦП требуется квантователь для преобразования дискретных значений аналогового сигнала в двоичные числа. На рисунке 7c показано, как квантователь разбивает весь диапазон изменения напряжения аналогового сигнала на фиксированное число равных интервалов, каждый из которых представлен числом. Квантователь выдает число, соответствующее интервалу, в которое попадает значение аналогового сигнала.

Точное положение аналогового сигнала в этих интервалах теряется, таким образом может появиться ошибка, называемая ошибкой квантования. Так как ошибка не может превышать интервал квантования, то ошиб-

ку можно минимизировать, выбрав достаточное количество интервалов. В 8-битном преобразователе имеется 256 интервалов квантования, потому что это количество интервалов можно выразить 8-битным числом. Это позволяет получить невзвешенное соотношение сигнал/шум около 50 дБ. 10-битный преобразователь дает 1024 интервала и соотношение сигнал/шум на 12 дБ больше.

Оборудование отличается в зависимости от формата данных, с которым оно может работать. Более старое оборудование, работающее только с форматом D1, обрабатывает 8-битные значения. Более современное - 10-битные.

На рисунке 7d показано, что для обратного преобразования из аналогового вида в цифровой потребуются две операции.

Сначала генерируется напряжение пропорциональное каждому двоичному значению, которое пропускается через восстанавливающий фильтр. Этот фильтр восстанавливает из дискретного сигнала в непрерывный сигнал. Функции этого фильтра понятны из его названия. Таким образом, в любой цифровой системе видеоизображение, которое мы видим, проходит через два аналоговых фильтра. На практике сигнал из цифрового в аналоговый вид и наоборот может конвертироваться несколько раз по определенным причинам. При каждом новом преобразовании накладываются еще два фильтра, и любой недостаток в них будет суммироваться и нарастать. Поэтому необходимо использовать самые лучшие из доступных фильтры. Поэтому нет никакого смысла использовать дешевые

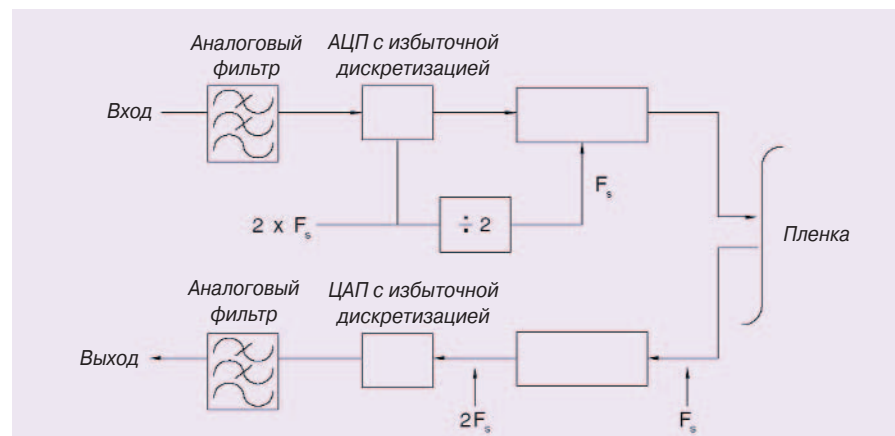


Рис. 8. В преобразователе с избыточной дискретизацией частота дискретизации временно увеличивается, чтобы облегчить работу аналоговых фильтров. Частота дискретизации увеличивается и уменьшается на этапе цифровой обработки, где фильтрация проще.

фильтры, так как все их дефекты тут же передадутся цифровой системе.

Одним из способов борьбы с недостатками этих фильтров является избыточная дискретизация. Как показано на рисунке 8, это может быть применено и к АЦП, и к ЦАП. При избыточной дискретизации в АЦП частота дискретизации временно удваивается и аналоговый фильтр анти-алиасинга отбрасывает сигналы с частотой вдвое превышающую ту, которую он бы отбросил без удвоения. Вследствие избыточной дискретизации цифровой фильтр анти-алиасинга более корректно выполнит свои функции, чем смог бы любой аналоговый фильтр. После этого частота дискретизации возвращается к стандартному значению

Каким образом работают цифровые интерфейсы

В этой главе мы рассмотрим стандарты существующие для обмена и передачи данных, представляющих собой оцифрованные компонентные и композитные видеосигналы. Также будут рассмотрены вопросы состыковки компонентных и композитных видеосигналов. Для стандартного цифрового композитного видеосигнала используется частота дискретизации, которая в четыре раза выше частоты поднесущей. Для NTSC частота дискретизации будет приблизительно равна 14.32 МГц. Это упрощает разделение яркостных и цветоразностных компонент цифровыми фильтрами. На рисунке 9 показан сигнал, с учетверенной частотой дискретизации. Обратите внимание, что оцифровка производится с начала активной строки, так как цифровые видеоманитроны, работающие с композитным видеосигналом (D-2 и D-3), не записывают строчные интервалы гашения, а восстанавливают их искусственно. Впрочем, цифровые интерфейсы могут записывать и весь видеосигнал. На рисунке 10 показано, каким образом полный сигнал NTSC укладывается в 8 и 10-битные диапазоны квантования. Дискретизация производится по осям I и Q, и полученные значения не пересекаются с сигналами цветовой синхронизации.

Дискретизация компонентных сигналов производится иначе, чем композитных. Для совместимости в обоих форматах 525/60 и 625/50 была вы-

брана одна частота дискретизации, привязанная к частоте строчной синхронизации. Для дискретизации яркостного сигнала чаще всего используется частота 13.5 МГц. За такую совместимость приходится расплачиваться тем, что пиксели не будут квадратными. Обратите внимание, что в компонентных цифровых системах записывается и передается только активная строка. В оцифрованной активной строке содержится 720 пикселей, что немного превышает длительность аналоговой активной строки, поэтому в оцифрованную строку попадает и часть интервала гашения (для NTSC).

В компонентных системах цветоразностные сигналы имеют меньшую полосу пропускания. В аналоговых компонентных системах (например, Betacam) цветоразностные сигналы имеют половину пропускной способности яркостного сигнала, поэтому при дискретизации можно использовать вдвое меньшую частоту, чем при дискретизации яркостного сигнала, то есть 6.75 МГц. Также используется в четыре раза меньшая частота, чем при дискретизации яркостного сигнала, и эта частота, то есть 3.375 МГц, которой присвоено значение 1, является самой низкой из используемых на практике.

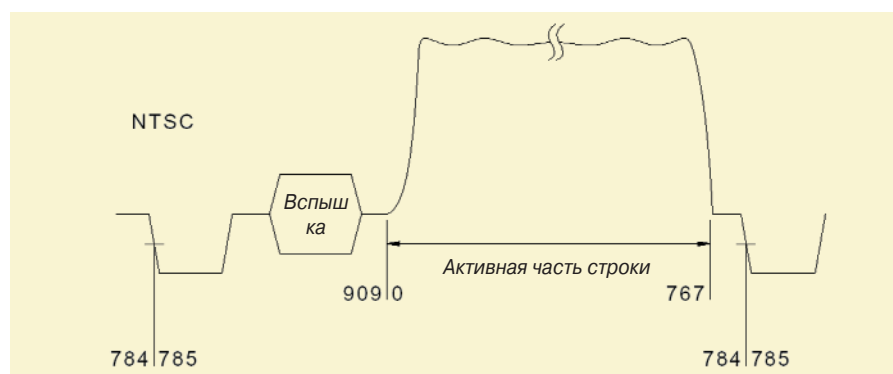


Рис. 9. Пример оцифрованной строки NTSC

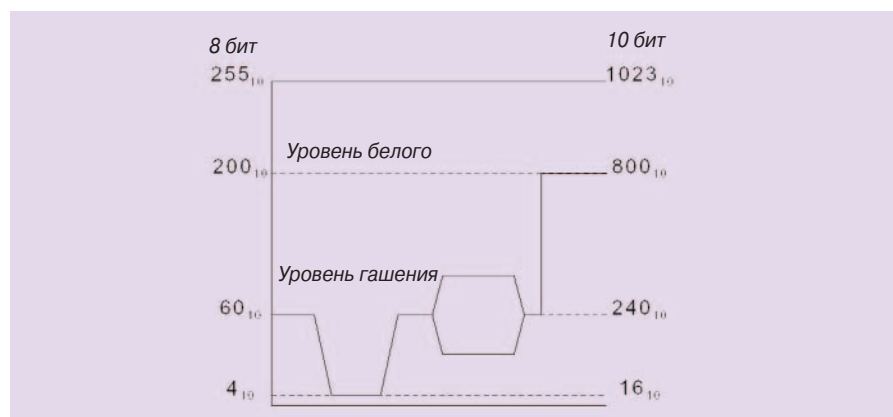


Рис. 10. Как полный сигнал NTSC укладывается в 8 и 10-битные диапазоны квантования.

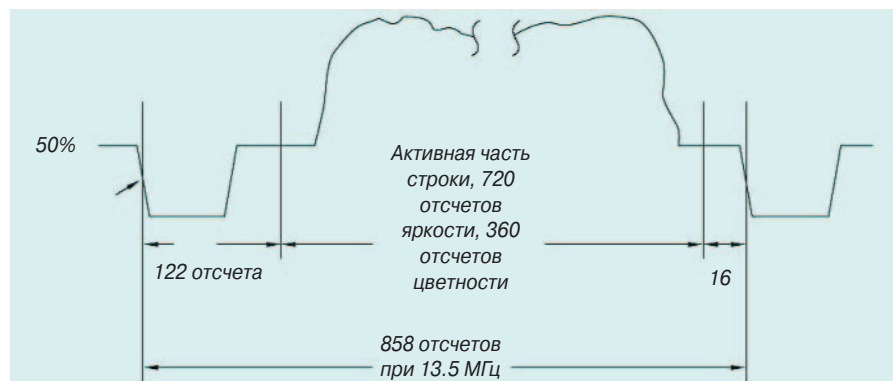


Рис. 11. Цифровой компонентный сигнал.

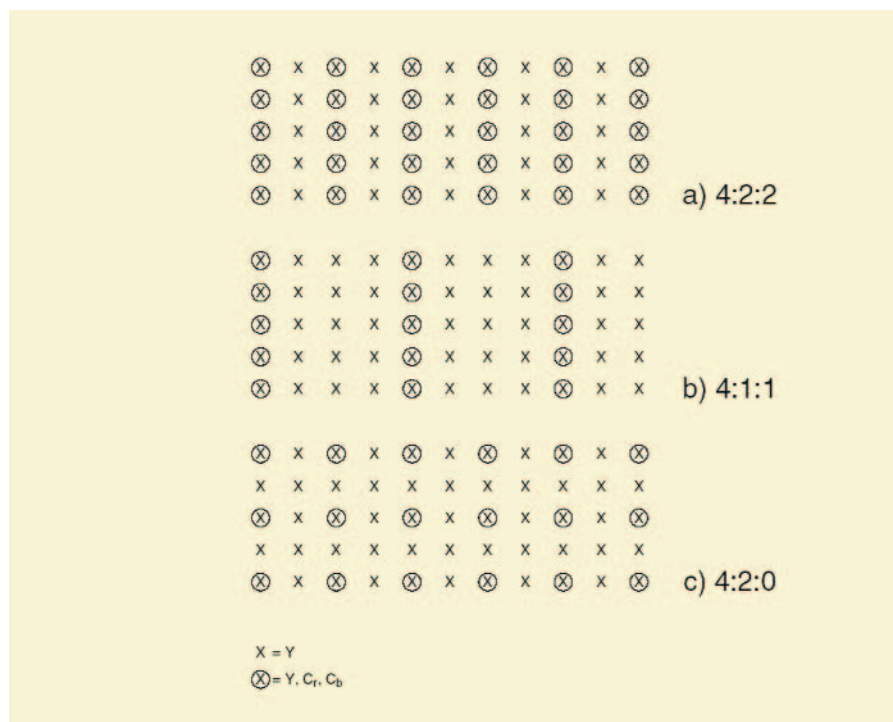


Рис. 12. а) Формат оцифровки 4:2:2.

б) Формат оцифровки 4:1:1 уменьшает горизонтальное цветовое разрешение.

в) Формат оцифровки 4:2:0 сохраняет горизонтальное цветовое разрешение, но теряет вертикальное цветовое разрешение.

Частоте дискретизации 6.75 МГц соответственно присвоено значение 2, а частоте 13.5 МГц - 4.

Большинство компонентного цифрового оборудования использует формат дискретизации 4:2:2. В этом формате записывают стандарты D-1, D-5 и Digital Betacam. Его поддерживает и цифровой последовательный интерфейс SDI (serial digital interface). На рисунке 12а показано, как выглядит формат дискретизации 4:2:2 в двухмерном пространстве. В каждом пикселе представлена только яркостная компонента. Цветоразностный сигнал представлен только в каждом втором пикселе по горизонтали. Два других формата дискретизации применяются в основном в системах, использующих компрессию. На рисунке 12б при формате дискретизации 4:1:1 цветоразностный сигнал представлен только в каждом четвертом пикселе по горизонтали. На рисунке 12с изображен формат дискретизации 4:2:0, где расположение отсчетов цветоразностного сигнала по горизонтали такое же как и по вертикали, что дает более "квадратный" цветной пиксел.

Рисунок 13 показывает, каким образом компонентный видеосигнал укладывается в 8- и 10-битное квантование. Сигналы синхронизации могут уходить ниже 0 этой шкалы, так как мы используем только активную строку.

Цветоразностные сигналы смещены вверх, поэтому положительные и отрицательные значения могут быть представлены в нашем диапазоне двоичных чисел.

Стыковка цифровых потоков может быть осуществлена двумя способами: параллельным и последовательным.

Параллельные интерфейсы используют 25-штырьковый разъем типа B и тяжелый многожильный кабель. Это старая технология, которая не позволяет передавать далее 50 метров, так как в противном случае биты в приемник не будут поступать синхронно. Но, вероятно, хуже всего то, что параллельный интерфейс коммутирует каждый бит и сигналы синхронизации отдельно, а устройства, использующее такой интерфейс, на самом деле весьма сложные по организации и имеет 11

уровней, то есть такие устройства очень дороги и не выпускаются в больших объемах. Как только стали доступными наборы микросхем для построения последовательного интерфейса, параллельный интерфейс стал устаревшим, но только очень новое оборудование имеет входы и выходы последовательного интерфейса как стандартные. Если у вас есть старое оборудование, в котором используется только параллельный интерфейс, то и в этом нет ничего страшного, так как достаточно добавить переходник, преобразующий параллельный интерфейс в последовательный.

Цифровой последовательный интерфейс (SDI) позволяет передавать компонентный или композитный цифровой видеосигнал по обычному коаксиальному кабелю. Вместо того чтобы пересылать все биты одновременно по нескольким жилам кабеля, интерфейс SDI пересылает все биты по очереди по единственному проводу кабеля. Такой режим передачи требует высокой частоты - 270 миллионов бит при формате дискретизации 4:2:2. При такой частоте даже обычная последовательная пересылка битов представляет сложность, так как некоторые последовательности битов составляют такие сигналы, которые тяжело обработать. В качестве решения этой проблемы используется технология под названием "скремблирование", которая разбивает и преобразовывает "неудобные" последовательности битов перед отправкой. В приемнике применяется обратный процесс, который называется дескремблирование и полностью восстанавливает изначальную последовательность битов. Сигналы интерфейса SDI имеют очень высокую частоту, и уже в самом кабеле может случиться значительное ослабление сигнала. Чем больше длина, тем сильнее ослабевает сигнал, и тем больше бу-

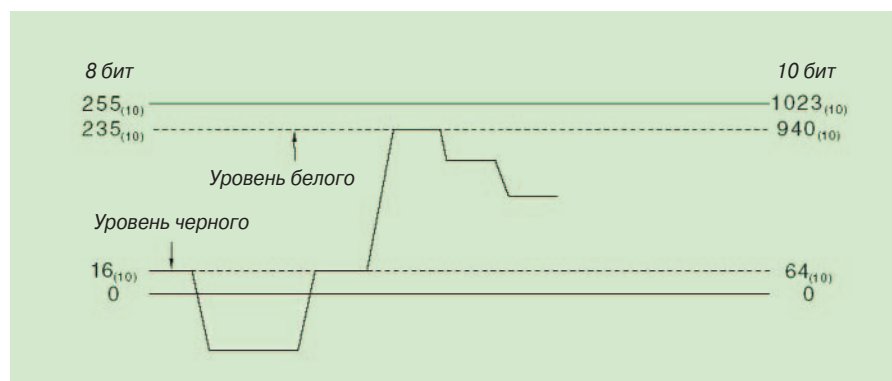


Рис. 13. Как компонентный видеосигнал укладывается в 8 и 10-битном диапазоне квантования.

дет проявляться дрожание сигнала. Это вполне нормально, так как сигнал будет восстановлен, как это было описано в предыдущей главе. Впрочем, для восстановления сигнала, необходимо, чтобы сигнал не был ослаблен настолько, чтобы нельзя было определить высокий или низкий уровень. На рисунке 14а показано, какие длины кабелей используются для интерфейса SDI. Превышения не допускаются, и на рисунке 14b видно, что происходит при превышении максимальной длины кабеля. После определенного порога качество передачи по интерфейсу резко снижается, поэтому для надежности лучше оставлять некоторый запас по длине кабеля. На практике этот запас определить очень просто. Достаточно удлинить каждый кабель на 15 метров, если после этого система продолжает работать, то запаса хватает. В противном случае потребуется заменить кабель или установить повторитель, но прежде нужно проверить, насколько правильно настроена схема фазовой синхронизации в приемнике. Последовательный цифровой видеосигнал сам по себе несовместим с компонентным и композитным видеосигналами, так как они аналоговые. Впрочем, интерфейс SDI представляет собой всего лишь поток данных, и в этом смысле отличие касается только скорости передачи. Поэтому вполне возможно создать оборудование двух стандартов, которое будет работать с композитным и компонентным интерфейсом SDI. Такие устройства уже существуют. Обычно, для того чтобы перейти от композитного к компонентному сигналу, потребуется только нажать кнопку, которая изменит частоту. Это означает, что если вы обновляете композитную систему до цифровой, то в будущем вы сможете перейти и на компонентный сигнал.

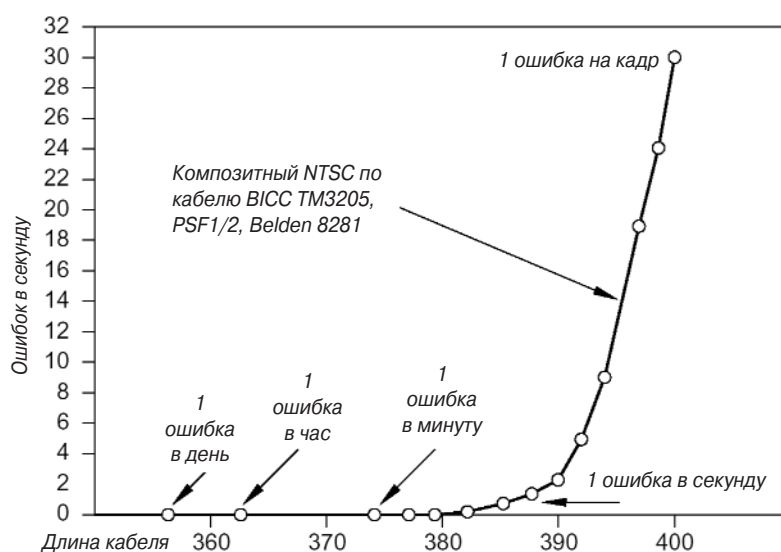
Интерфейс SDI обрабатывает цифровой видеосигнал, который представляет собой оцифрованный аналоговый сигнал и имеет те же интервалы, то есть в цифровом сигнале будут пробелы в данных там, где у аналогового сигнала будут интервалы гашения. Эти пробелы можно использовать для передачи дополнительных данных вместе с видеосигналом. Эта передача осуществляется абсолютно "прозрачно", а устройства, обрабатывающие только видеосигнал, игнорируют дополнительные данные. Более функциональные устройства опреде-

а)

Стандарт	Предел длины кабеля	Оптимальная длина кабеля
Композитный NTSC	400 м	320 м
Композитный PAL	360 м	290 м
Компонентный 601	290 м	230 м
Компонентный 16:9	210 м	170 м

Тип кабеля: BICC TM3205, PSF1/2, Belden 8281 или любой другой с потерей 8.7 дБ/100 м при 100 МГц

b)



Частота ошибок	NTSC	PAL	Компонентный 601	Компонентный 16:9
1 ошибочный бит / поле	4.2×10^{-7}	4.2×10^{-7}	4.2×10^{-7}	4.2×10^{-7}
1 ошибочный бит / секунда	4.2×10^{-9}	4.2×10^{-9}	4.2×10^{-9}	4.2×10^{-9}
1 ошибочный бит / минута	4.2×10^{-10}	4.2×10^{-11}	4.2×10^{-11}	4.2×10^{-11}
1 ошибочный бит / час	4.2×10^{-12}	4.2×10^{-12}	4.2×10^{-13}	4.2×10^{-13}
1 ошибочный бит / день	4.2×10^{-14}	4.2×10^{-14}	4.2×10^{-14}	4.2×10^{-14}
1 ошибочный бит / месяц	4.2×10^{-15}	4.2×10^{-15}	4.2×10^{-15}	4.2×10^{-16}
1 ошибочный бит / год	4.2×10^{-16}	4.2×10^{-16}	4.2×10^{-16}	4.2×10^{-17}

Рис. 14. а) Максимальная длина кабеля, используемого с интерфейсом SDI. Превышать ее не рекомендуется. б) После определенного порога качество передачи резко снижается, поэтому для надежности лучше оставлять некоторый запас по длине кабеля.

ляют код, сигнализирующий о передаче дополнительных данных, и привлекают их из видеосигнала. Дополнительные данные можно помещать и в оцифрованный композитный сигнал, хотя они будут ограничены по времени интервалом синхронизации.

Почему декодирование столь сложно?

В идеальной аналоговой телевизионной системе процесс композитного кодирования тесно перемешивает частоты яркости и цветности в трех измерениях: по вертикали, по горизонтали и во времени. Композитные сигналы, с которыми приходится сталкиваться на практике, зачастую далеки от идеала.

Редактирование видеоизображения и резкие цветовые переходы создают такие высокие частоты, которые смешиваются отнюдь неидеально.

Такие сигналы практически и теоретически невозможно декодировать правильно, так как частоты яркости и цветности вторглись в пространство друг друга и полностью разделить их не удастся. Композитный видеосигнал на самом деле является своего рода сжатием с потерями, так как позволяет передавать цветное видеоизображение в той же полосе частот, что и черно-белое. Эти случающиеся время от времени композитные сигналы, которые невозможно правильно декодировать, можно сравнить с артефактами, возникающими при сжатии видеоизображения.

Оставляя в стороне технические подробности, отметим, что точное декодирование композитных видеосигналов, встречающихся на практике, далеко не всегда возможно. Более того, нет ни одной технологии декодирования, которая была бы идеальной. Различные технологии декодирования имеют свои сильные и слабые стороны, поэтому нет ничего удивительного в том, что существует большое количество разнообразно оборудования для декодирования. Искусство декодирования заключается в том, чтобы выбрать правильный декодер для определенной задачи исходя из бюджета.

В композитном сигнале произошло смешение в трех измерениях. Полное разделение яркости и цветности воз-

можно только в том случае, если оно тоже производится в трех измерениях. Некоторые декодеры умеют делать и это. Для фильтрации во временном измерении необходимо иметь одновременный доступ к нескольким полям, что требует больших объемов памяти и соответственно удорожает стоимость оборудования. Такие технологии могут применяться только на стабильном видеосигнале, так как нестабильность нарушает фазовые отношения сигнала цветности в полях. В этом случае будет присутствовать запаздывание видеосигнала, что для некоторых задач неприемлемо. Кроме того, спектр композитного сигнала близкий к идеальному может быть получен только при отсутствии быстрого движения, а любое редактирование сигнала нарушает его трехмерный спектр. Любой декодер, сравнивающий несколько полей, будет воспринимать редактирование в видеоизображении как ненормально быстрое движение, что создает определенные сложности.

Если трехмерная фильтрация по какому-либо причинам не подходит для

них строках, когда фазовые соотношения от строки к строке нарушены, что приводит к потере вертикальной четкости, сопровождаемой появлением помехи от неотфильтрованной поднесущей цветности (так называемые "висящие точки"). Обычно в декодерах эта проблема решается возвратом к режекторной фильтрации, что, впрочем, приводит к снижению разрешения.

В компании Snell and Wilcox разработали и альтернативный способ фильтрации Gate (Gate circuit), который заключается в том, что специальная схема Gate помещается после гребенчатого фильтра. Эта патентованная система содержит режекторный фильтр настроенный на частоту поднесущей, глубина и ширина которой может варьироваться в широких пределах. "Щель" (notch) в спектре сигнала яркости контролируется в зависимости от "прорыва" в него сигнала цветности за счет отдельного гребенчатого фильтра. Таким образом, высокочастотная составляющая яркостного сигнала не обязательно утрачивается. Разделение яркости и цветности не

может проводиться при сравнении полей или строк при нестабильных сигналах, как например от видеомангитофонов. В этих случаях обычные фильтры отключаются, и для разделения яркости и цветности используется только фильтр Gate.

На практике может потребоваться не только декодирование, но дополнительная кадровая синхронизация, так как вход-



нашей задачи, то можно использовать подход с вертикальной фильтрацией, который заключается в вычитании двух соседних строк одного поля. При этом произойдет подавление сигнала яркости (если предположить, что соседние строки не сильно отличаются по цветности) и в результате останется поднесущая цветности удвоенной амплитуды. Такой гребенчатый фильтр позволяет достаточно успешно разделить яркостную и цветностную компоненты сигнала без заметной задержки.

Впрочем, известно, что такой гребенчатый фильтр не работает при резких переходах цветности в двух сосед-

ные сигналы могут оказаться далеко не идеальными. В большинстве случаев композитные видеосигналы будут аналоговыми, но также может потребоваться обработка цифровых сигналов формата D-2 или D-3. В процессе обработки все чаще используются компонентные видеосигналы с форматом дискретизации 4:2:2, поэтому в декодер будет уместным включить и аналого-цифровое преобразование. Если это преобразование производится сразу после поступления сигнала в декодер, то фильтрация может вестись полностью в цифровом виде.

Цифровая видеозапись как доказательство

Данная статья представляет собой подборку материалов, посвященную законности использования видеозаписи и техническим и юридическим аспектам ее использования при судебных разбирательствах. В дальнейшем, по мере накопления заслуживающих вашего внимания фактов, мы постараемся осветить данную проблему более широко со всех точек зрения, привлекая специалистов из сфер деятельности, связанных с рассматриваемой проблематикой. Данная подборка вобрала в себя несколько интервью и любезно предоставленные материалы как специалистов в области права, так и людей непосредственно использующих системы видеонаблюдения и практически ежедневно решающих различные технические и юридические вопросы, связанные с ними. Надеемся, в следующих статьях мы подробно осветим непосредственно сам процесс экспертизы видеозаписи рассмотрим ряд дополнительных аспектов, связанных с законностью разных схем скрытой видеозаписи. И, наконец, мы получим ряд материалов по уже законченным уголовным делам, где одним из доказательств служила видеозапись (сейчас они еще не закончены).



Иванов Павел Юрьевич, старший научный сотрудник экспертно-криминалистического центра МВД РФ. Данное интервью открывает нашу подборку материалов. В нем освещены как технические, так юридические аспекты рассматриваемой проблемы.

В настоящее время сложилась практика, когда системы наблюдения входят в комплексы охраны объектов и выполняют функции обнаружения опасных ситуаций (функции телевизионной сигнализации). Другие функции - слежение за объектами наблюдения и документирование ситуации становятся второстепенными. Регламентация функционирования систем наблюдения осуществляется ГОСТом Р 51558-2000 "Системы охранного телевизионного". Данные требования носят общий характер и не учитывают криминалистические рекомендации по получению и записи изображений, пригодных для рассле-

дования преступлений. Это приводит к невозможности в большинстве случаев проведения криминалистических исследований и установления личности преступников.

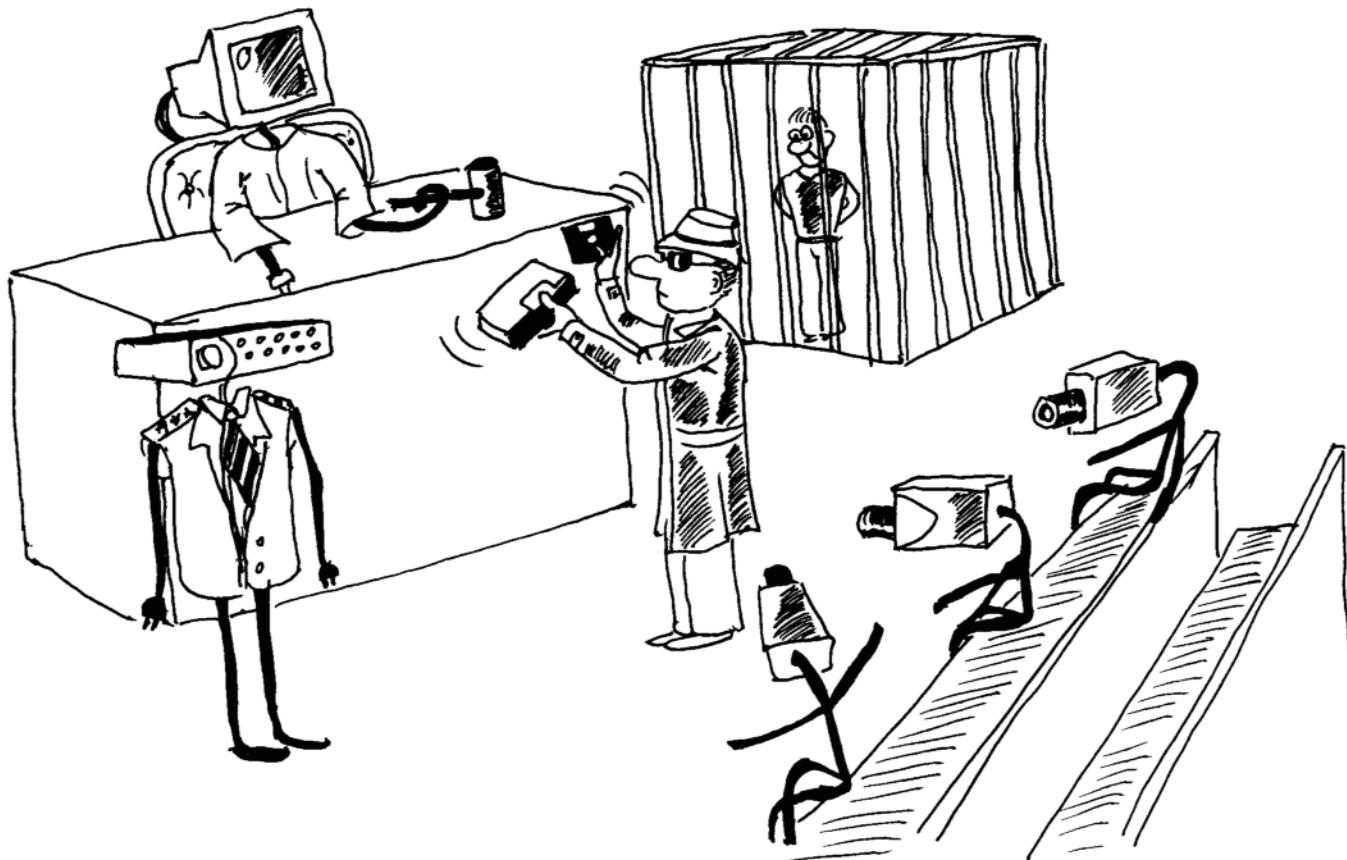
Криминалистические требования к телевизионным системам наблюдения были разработаны ЭКЦ МВД России в 1999 году по предложению ряда организаций. Экспериментальные исследования проводились в одном из отделений Сбербанка при технической поддержке концерна России, который предоставил телевизионное оборудование и аппаратно-программный комплекс ROSSI-MEGASENSE. Результаты этих исследований были опубликованы в информационном письме (см. приложение 2).

Полученные видеозаписи и цифровые изображения могут использоваться в ходе расследования и раскрытия преступлений. Для этого проводится криминалистическое исследование фото и видеодокументов. Экспертиза фото и видеодокументов

выполняется в ЭКЦ МВД России, ФСБ России, РФЦСЭ Минюста России. Методики исследования цифровых видеозаписей и изображений в настоящее время находятся в стадии разработки. **(Редакция журнала пыталась связаться с ЦСЭ при Минюсте, но безрезультатно. Может быть, с выходом этого номера, ответственные лица в Минюсте опровергнут данное утверждение. - от ред.)**

Видеозапись может использоваться в качестве инструмента при ОРМ и как улика при рассмотрении дела в суде. В контексте данной статьи имеет смысл подробно остановиться только на втором аспекте использования видеозаписей. Практика показывает, что использование видеозаписи широко практикуется в российских следственных и судебных органах в качестве доказательства в рамках уголовного процесса.

Использование видеозаписи в качестве доказательства по уголовному



делу допускается статьями 74, 81 и 84 УПК РФ. (Что касается других кодексов, то такие нормы существуют в ГПК (Ст. 55 ч. 2), в КоАП (Ст. 26.7 ч. 2) и в АПК (Ст. 64 ч. 2)).

Статья 84 УПК РФ определяет различные виды и формы информации, и её носителей. Допускается как аналоговая, так и цифровая форма визуальной информации. Правда, отсутствует их дифференциация, что создает определенные трудности при правоприменительной практики.

Видеозаписи могут изыматься в ходе производства процессуальных действий или представляться потерпевшими и прочими лицами. В соответствии со статьями 84 УПК РФ видеозаписи, признанные вещественными доказательствами изымаются по постановлению и приобщаются к уголовному делу. Порядок изъятия определяется статьями 183 УПК РФ.

На этапе проведения следственного действия и изъятия видеозаписи или отдельных изображений существует проблема отсутствия методики их изъятия.

В нормативных документах не указано, на каком носителе должна предоставляться цифровая видеoinформация на экспертизу. Допускается передача как на жестком диске, так и на других носителях (CD-R/RW, флэш - память). Ведь, в ряде случаев

невозможно изъять оригинальную видеозапись (жесткие диски организованы в RAID - массив, на них стоит необходимое для видеозаписи ПО и т.д.), поэтому, иногда, могут изыматься копии видеозаписи.

Разумеется, изъятие видеозаписи должно происходить в порядке установленном УПК. Но так делается далеко не всегда. Как правило, решение о том, изымать жесткий диск с оригинальной видеозаписью, а то и весь видеосервер целиком, или ограничиться ее копией принимается в каждом конкретном случае на основе множества различных факторов. В целом, изъятие всей системы наблюдения редко бывает целесообразно, однако изъятие одного лишь носителя бывает недостаточно для решения вопросов, поставленных перед экспертом. Поэтому необходимо определение объектов, подлежащих изъятию, порядка изъятия, а также уточнения функций эксперта-криминалиста. Работа над методическими рекомендациями по данным направлениям активно ведется в ЭКЦ МВД. Исходя из практики, предпочтение отдается носителям CD-R (копиям видеоматериалов), дабы дополнительно подстраховаться от возможности фальсификации.

Для приобщения фото и видео документов и их использования в качестве

доказательств в соответствии со статьей 88 УПК РФ необходимо оценить их относимость, допустимость и достоверность.

Зафиксированная визуальная информация позволяет установить процесс совершения преступления, его участников (преступников и пострадавших), а также предметы, относящиеся к совершению преступления. Здесь возможно использование метода **портретного сравнения** (см. ниже).

При установлении относимости видеодокументов выявляется время совершения зафиксированных действий, личности участников событий и другие фактологические данные.

При установлении допустимости и достоверности источника получения информации необходимо установить (помимо времени) место и обстоятельства проведения съемки, ее точку, а также перечень технических средств, применявшихся при видеосъемке. Дополнительно необходимо установить операции, проводившиеся (или не проводившиеся) с видеозаписью в дальнейшем. То есть ответить на вопросы: "Есть ли признаки монтажа видеозаписи" и "Прерывалась ли видеозапись".

При рассмотрении дела в суде мнение эксперта очень весомо. Судья практически всегда безоговорочно до-

веряет ему. Поэтому на эксперте лежит огромная ответственность за те выводы, которые он оглашает в суде. Но существует и обратная сторона медали. Если эксперт при решении идентификационной задачи дает вероятностный ответ (пусть даже с большой степенью вероятности), то этот ответ может и не учитываться в суде.

Существует и специфическая проблема, характерная для цифровых видеозаписей: отсутствие унификации видеоплатформатов. Нередко формат, записанный на оборудовании (или при помощи ПО) одного производителя не воспроизводится стандартными видеопроигрывателями. Такое бывает, несмотря на то, что большинство современных систем охранного видеонаблюдения записывают в наиболее распространенные форматы. Поэтому очень хотелось бы получать вместе с видеозаписью и оборудование, аналогичное тому на котором она была сделана: это уже предложения к производителям ПО и аппаратной части систем охранного телевидения. Концерн ROSSI, с которым мы давно сотрудничаем, сделал именно так. В дальнейшем необходимо создание рабочей группы, в которую вошли бы предста-

вители крупных организаций охранного видеонаблюдения, для разработки универсальных стандартов в области охранного видеонаблюдения.

Необходимо отметить ряд трудностей, с которыми сталкиваются эксперты при производстве экспертиз по видеозаписям и изображениям, полученных телевизионными системами наблюдения. Прежде всего, они относятся к идентификационным исследованиям.

Для идентификации объектов необходимо иметь совокупность признаков, характерную только для данного объекта, и их относительную устойчивость. В **портретной идентификации** в качестве признаков используются форма, размер, положение, цвет элементов внешности. При идентификации транспортных средств, в качестве признаков, используются форма, размер, положение символов номера. Чем больше индивидуальных признаков, тем выше вероятность опознавания. Однако для изображений, полученных телевизионными системами наблюдения, характерно сжатие информации, в результате которого индивидуальные признаки теряются. К постоянным

факторам относятся: низкое качество используемых телекамер, неправильная установка телекамер, неправильное освещение объектов в поле зрения телекамер (в том числе фоновая засветка и неравномерная освещенность снимаемого объекта), использование мультиплексирования кадров с нескольких телекамер, потери в тракте передачи видеосигнала, потери информации при оцифровке видеопотока. При воздействии случайных факторов, например, быстром перемещении объекта, происходит очень значительное искажение (смаз) признаков.

В целом, можно сказать, что только около 20% видеозаписей подходят для криминалистического анализа, а 80% имеют настолько плохое качество, что практически не имеет смысла даже браться за исследование таких видеозаписей.

На предварительной стадии анализа изображений методы цифровой обработки помогают выделить контура или выявить часть признаков, но улучшение изображения не всегда результативно. Поэтому требуется совершенствование методик идентификационных исследований, которое

может происходить в нескольких направлениях: 1. объединение информации об одном объекте из разных видеок кадров; 2. использование функциональных признаков в портретной идентификации; 3. использование метрических вычислений по изображению для определения реальных размеров объектов.

Другой проблемой производства экспертизы является отсутствие методик для решения диагностических задач анализа изображений. Традиционные подходы не позволяют анализировать цифровые изображения и их носители. Поэтому создание методик проведения диагностических исследований с использованием математических методов значительно повысит точность исследований. В основу новой методики **определения условий съёмки**, расположения источников и характера освещения могут быть положены методы моделирования процесса съёмки, применение метода трассирования лучей и имитации отражающих свойств поверхности. В основе метода **трассирования лучей** лежит воспроизведение в математической форме лучей от источника света к объекту и от объекта к светочувствительному приёмнику. Понятие "трассирование лучей" происходит от слова "путь", что связано с моделированием геометрического пути каждого светового луча, участвующего в построении изображения. Процесс моделирования основывается на законах геометрической оптики (преломления, отражения, прямолинейности и др.). Основная идея метода сводится к повторению всех геометрических преобразований, которые бы совершил каждый световой луч на пути источник==>объект==>приёмник. **(Однако, средств для разработки и внедрения методики Иванова нет. Комплект программного обеспечения и графической станции SGI стоит несколько десятков тысяч долларов. -от ред.).**

А вот слова доктора юридических наук **Ильи Александрова**: "На сегодняшний день известной нам практики с анализом видеозаписей, произведенных цифровой техникой, не имеется. В связи с широкими возможностями манипуляций цифровыми видеозаписями процесс доказывания факта подлинности цифровой видеозаписи, будет гораздо слож-

нее, нежели аналоговой".

Елена Герасимова, руководитель юридического департамента компании Лигас, обобщает юридические нормы, содержащиеся в Конституции, Уголовном и Трудовом кодексах касающиеся сбора и распространения видеoinформации.

Конституция РФ в ст. 24 устанавливает запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Федеральный Закон "Об информации, информатизации и защите информации" в статье 11 (Информация о гражданах (персональные данные)) категоризирует такую информацию как персональные данные и относит ее к разряду конфиденциальной информации.

Право на неприкосновенность частной жизни обеспечивает гражданину возможность находиться вне службы в состоянии известной независимости от государства и общества и выражается в свободе общения между людьми на неформальной основе.

Данное право обеспечивается установленной в ст. 137 УК РФ ответственность за нарушение неприкосновенности частной жизни. Эта статья запрещает незаконный сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия. Федеральным законом от 8 декабря 2003 г. № 162-ФЗ "О внесении изменений и дополнений в Уголовный кодекс Российской Федерации" в УК РФ были внесены существенные изменения, в данную статью. Изменены диспозиции некоторых норм Особенной части Уголовного кодекса. Так, из признаков состава ч. исключена корыстная цель (либо иная личная заинтересованность), а также необходимость наступления вредных последствий для привлечения к ответственности. Данная поправка сделана для того, чтобы еще больше защитить частную жизнь индивида от каких бы то ни было посягательств извне.

Стоит рассмотреть вопрос может ли установка системы видеонаблюдения в организации нарушить неприкосновенности частной жизни.

Во-первых, в данном случае отсутствует объект преступления. Сфера профессиональной деятельности не относится к частной жизни лица.

Объективная сторона состава преступления будет отсутствовать, даже если в процессе будет собрана информация, касающаяся личной сферы индивида, так как в упомянутой статье речь идет только о незаконном сборе и распространении сведений, а система видеонаблюдения к таковым не относится.

Во-вторых, не вся информация, касающаяся частной жизни лица, является его личной тайной, например, в силу ее общеизвестности. К личной тайне можно отнести только сведения, не подлежащие, по его субъективному мнению, которого они касаются, оглашению. Поэтому он вправе отнести к личной тайне любые сведения. Но если информация передана непосредственно самим лицом (умышленно и добровольно), то ее сбор не является незаконным. То есть отсутствует обязанность, насилие, угроза, введение в заблуждение и принуждение работника проявлять обсто- ятельства частной жизни на рабочем месте. Аналогичная норма статье 137 УК РФ существует и в Трудовом Кодексе РФ (статья 86). Уточняя, что в случаях непосредственно связанных с вопросами трудовых отношений, при условии письменного согласия работника, работодатель вправе получать и обрабатывать данные о его частной жизни. Но в соответствии в ТК РФ организация обязана:

- учитывать права работника по отношению к своим персональным данным (ст. 89);
- довести до сведения работников порядок обработки их персональной информации (п. 7 ст. 86);
- обеспечивать защиту информации от неправомерного ее использования или утраты;
- соблюдать правила передачи персональной информации работника (ст. 88).

То есть для того, чтобы исключить инкриминирование ст. 137 УК к организации осуществляющий сбор информации посредством видеонаблюдения, необходимо уведомить лиц о том, что таковое ведется и получить их согласие. Но распространение собранной видеoinформации без согласия передавшего ее (записанного в видеоматериале) лица уже может быть квалифицировано по упомянутой статье.

Итак, для того чтобы установленная система видеонаблюдения соответствовала всем правовым нормам, мы

рекомендуем придерживаться следующей стратегии. Видеонаблюдение должно вестись максимально открыто, не выходя из рамок требуемых для достаточного обеспечения производственного процесса. То есть необходимо проинформировать всех сотрудников о установленной системе видеонаблюдения, дополнительно разместив при входе в организацию соответствующее объявление. Его содержание может быть приблизительно таким: "В соответствии приказом № ... на территории организации в целях обеспечения режима безопасности сотрудников и сохранности имущества ведется видеонаблюдение, сведение персонального характера, попавшие в поле зрения системы видеонаблюдения не являются информацией о частной жизни лица, составляющей его личную или семейную тайну".

В качестве завершения хочется привести слова доктора юридических наук Ильи Александрова: "Действующим российским законодательством производство видеозаписи в местах общего пользования напрямую не запрещено".

А теперь стоит рассмотреть взгляд практиков на эту проблему: пользователя системы видеонаблюдения и ее инсталлятора. **Андрей Волошенко, начальник Службы безопасности сети магазинов СПАР.**

По статистике воровства в магазинах, то, что касается нашей сети, распределение выглядит приблизительно так: 20% приходится на покупателей, а 80% - на скрытое и открытое воровство персонала. Например, автомобиль с товаром, просто не приезжает в магазин (сговор с менеджерами и ответственными по складу), но если машина все же подъехала к "дебаркадеру", то разгружалась ли она очень хорошо можно отследить с помощью установленных там телекамер. Сразу можно выяснить: кто работал в эту смену, что за поставщик. Эта информация сразу передается правоохранительным органам.

Если случается происшествие, зафиксированное телекамерами, тот тут же оператор передает информацию охране на кассовом узле и задерживается правонарушитель, другие покупатели выступают как свидетели. Что касается территориальных границ, где уже можно зафиксировать правонарушение или преступление, то эта граница проходит через кассовый узел.



На данный момент суммы хищений, превышающих 600 рублей квалифицируются по УК, меньшие суммы - по КоАП. В последнем случае, правонарушитель не останется безнаказанным, так как в правоохранительных органах ведется архив таких правонарушений, в котором присутствуют свидетельские показания других покупателей. Наша сеть супермаркетов достаточно либерально относится к людям, совершившим такое в первый раз: просто заставляем оплатить или вернуть товар. Но милицию, все равно вызываем в профилактических целях. Разумеется, ведется собственный фотоархив всех людей (правонарушителей, свидетелей и т. д.), которые были задействованы в каждом случае.

Монитор, отображающий изображение с телекамер расположенных на входе и над кассовым узлом, выполняет две функции: предупреждает покупателей о том, что ведется видеонаблюдение и осложняет так называемый "рывок", то есть быстрое движение от кассового узла к выходу.

Очень непросто вести видеонаблюдение в зимнее и темное время. Из-за большого количества одежды (капюшоны, шарфы) бывает трудно идентифицировать конкретного человека. Но и здесь есть выход - необходимо, просто, более внимательно относиться к людям, одетым подобным образом.

Был один очень интересный случай. Однажды в магазин зашла хорошо одетая женщина среднего возраста, долго ходила по магазинам, выбирая товары. При этом, очень активно демонстрировала крупную сумму денег в валюте под разными предлогами. Затем она неожиданно закричала, что, мол, у меня пропали деньги. Магазины

невыгодно, чтобы у покупателей что-либо пропадало во время посещения магазина. Поэтому мы уделили особое внимание этому случаю, хотя проблемы, возникающие у покупателей с третьими лицами, выходят за компетенцию службы безопасности. Просмотрев видеозапись, обнаружилось следующее. В один из моментов женщина передала кошелек молодому человеку, который быстро вышел из магазина. Просмотрев запись с телекамер, расположенных на автостоянке, мы увидели, что они оба приехали на одной машине, потом женщина вошла в магазин. Пристыдив эту женщину, мы ее отпустили. К сожалению, ничего инкриминировать ей было нельзя: она сама передала кошелек, нет состава преступления предусмотренного статьей о краже. Гипотетически можно применить статью о мошенничестве, но крайне сложно. Вообще, такие уловки могут пройти в маленьких магазинчиках, где владелец постоянно живет в страхе возможных проверок. А такой инцидент, звонок в торговую инспекцию, людей промышляющих данным видом деятельности может привести к комплексной проверке торговой точки. И дешевле бывает вернуть, якобы пропавшие деньги покупательнице, чем отбивать атаки многочисленных проверяющих органов.

Артем Лекарев, коммерческий директор Группы компаний Национальные Лаборатории Безопасности.

Одним из наиболее ярких примеров, когда видеозапись помогла не только зафиксировать факт преступления, но и установить преступников, был неоднократный поджог аптечного склада недалеко от станции метро "Университет". Что запомнилось, со-

жгли табличку с надписью, что ведется видеонаблюдение. Оказалось, что это была группа подростков, причем некоторые из них специально позировали перед телекамерами, наверное, надеясь, что это муляжи.

Из преступлений и правонарушений наиболее часто фиксируются пьяные драки ночью, попытки угона автомобилей с автостоянок, мошенничество и вскрытие касс.

Необходимо помнить, что на экспертизу не принимаются копии видеозаписей на носителях отличных от жестких дисков. То есть записать информацию на диск CD-R/RW нельзя, приходится специально покупать жесткие диски для передачи на экспертизу. А сейчас найти диски объемом меньше 30 Гб очень непросто, да и накладно это получается.

Что касается сроков передачи видеоматериалов правоохранительным органам, то здесь нет никаких жестких временных рамок. В некоторых случаях копию видеозаписи можно передать и через 2 дня. Также нет никаких ограничений по длительности (нижнему пределу) передаваемых видеозаписей. То есть все зависит от длительности зафиксированного события, что, впрочем, очевидно.

Экспертиза видеозаписей на наличие цифровых водяных знаков не проводится, тем более, далеко до какой-либо их систематизации и стандартизации.

Из организационных моментов стоит отметить, что существует постановление московского правительства, обязывающее супермаркеты, оснащать системами видеонаблюдения, прилегающие к ним территории.

Тактическое расположение телекамер производится таким образом (см рекомендации - прим. ред.), чтобы попадающие в их поле зрения лица людей можно было достаточно уверенно идентифицировать.

Пока что не было прецедентов, когда человек возмущался фактом его видеозаписи, ссылаясь на тот или иной правовой документ. Поэтому, даже в тех организациях, где мы устанавливали системы охранного телевидения, не везде стоят таблички, предупреждающие, что "ведется видеонаблюдение".

В заключение хотим привести некоторые рекомендации, которые на наш взгляд, могли бы быть полезны при выборе системы видеонаблюдения

и ее использовании, а также тактическом применении видеозаписей в качестве доказательной базы. Как говорится: узелок на память.

Тяжелая артиллерия - свидетели

Наличие свидетелей свершившегося факта резко увеличивает вес видеозаписи данного события в суде. Чем их будет больше, тем, разумеется, лучше. Мы понимаем те сложности, с которыми придется столкнуться при их поиске: программы защиты свидетелей у нас нет, да, и поговорка: "моя хата с краю" очень уместна в данном случае. Не зря же у следователей бытует другая поговорка: "легче убедить невиновного раскаться, чем найти свидетеля".

Аналог или цифра ?

Существует одно распространенное заблуждение, имеющее, правда, под собой некоторые основания, что лучше предоставить аналоговую запись, чем цифровую. Дело в том, что доверия к цифровой записи будет больше. Действительно, криминалистический анализ цифровых видеозаписей не всегда возможен, и не всегда эксперты за него берутся. Поэтому, некоторые люди специально переводят цифровую видеозапись, на аналоговый носитель для предъявления в суде. Закон не предусматривает деления на цифровые и аналоговые носители.

А у вас часы песочные ?

При наложении даты и времени предпочтительнее использовать устройства, которые накладывают данную служебную информацию непосредственно на видеопоток, а программно (оверлей).

Телекамер много не бывает

Очевидно, что чем больше скорость записи, разрешение и формат кадра, тем лучше. К этому стоит добавить, что чем больше установлено телекамер, тем тоже лучше. Если событие будет зафиксировано несколькими телекамерами, то это, во-первых, увеличит вероятность опознания преступника, а во-вторых, увеличит доверие к вашей видеозаписи.

Пишите в один файл

При выборе системы видеонаблюдения учитывайте тот факт, что видеодокумент, полученный с помощью системы, записывающей всю информацию в один файл значительно сложнее уличить в подделке.

Кто делает быстро - делает дважды

Банальности не стоит говорить, но

все же. Если вдруг вы захотите подделать запись, помните, есть определенные временные рамки, после которых к вашей улике будут относиться весьма настороженно.

Подделка: краткий курс выживания

Среди наиболее часто встречающихся схем подделки видеозаписей можно выделить следующие: изменение меток даты/времени на видеозаписи; "чистка" кадров; "введение объектов"; "наложение другого фона".

Первую схему мы уже рассмотрели выше. Что касается второй, то здесь тоже нет никакого секрета - "ломать - не строить". "Введение объектов", как уже упоминалось выше, можно осуществить "размытием" их контуров. А вот на четвертой схеме имеет смысл остановиться чуть подробнее.

Тут сразу возникает ряд сложностей. Перечислим их: необходимо достаточная однородность заднего фона, минимум присутствующих оттенков (оптимально, вообще, ч/б изображение), минимальными временными изменениями яркости и контрастности. Таких условий добиться нелегко, особенно если моделировать (то есть подделывать) наиболее распространенные (то есть далеко не идеальные) ситуации. Помимо этого, необходимо соблюдать пропорциональность размеров и геометрических форм, в том числе во времени (при наличии движения). Зачастую уже на этапе подготовки такого материала возникает вопрос: "А стоит ли игра свеч?".

Что позволено Юпитеру, не позволено быку

Данный постулат напрямую вытекает из предыдущего абзаца. Суд может задать вопрос эксперту: "А сколько бы стоило изготовить подделку данной видеозаписи в таком же качестве, при тех же условиях?". И будет руководствоваться теми данными, которые предоставит эксперт. Предположим, если данная сумма значительно превосходит ваши потенциальные финансовые возможности (разумеется, с некоторым допущением), то не стоит очень уж волноваться. Это правило может иметь несколько исключений, например, дела, затрагивающие публичных людей (политиков, крупных бизнесменов и т. д.).

Запас карман не тянет

Эта рекомендация для тех, кто держит определенную видеозапись, что называется "про запас". Если вы не хотите обнаружить некоторые данные непо-

средственно сейчас, но боитесь, что со временем их могут не принять в качестве улики, опасаясь обвинения в их подделке, поместите носитель с видеозаписью в банковскую ячейку. В таком случае, вам придется вносить записи в так называемую книгу учета доступа к ячейке. Вот в ней должна быть только одна запись, зафиксировавшая тот момент, когда вы положили ценный груз в ячейку.

Законность записи

Достаточно тонкий момент, общих рекомендаций здесь быть не может.

Если видеозапись сделана в пределах вашей частной собственности (практически любые ситуации можно мотивировать защитой жизни), то такая запись абсолютно законна.

Скорее всего, суд примет к рассмотрению видеозапись угроз, шантажа или вымогательства. Сложнее будет обстоять дело, если вы зафиксировали факт передачи взятки.

Если у вас уже есть видеозапись, но сделана она не вполне законно, то здесь можно посоветовать формально устроиться в одно из средств массовой информации. Закон в "некоторых случаях" (на практике очень часто) позво-

ляет журналистам производить скрытую аудио- и видеозапись.

А КАК ОБСТОИТ ДЕЛО ЗА РУБЕЖОМ.

Казахстан

Определение Коллегии по гражданским делам Верховного Суда

Республики Казахстан от 28 февраля 2001 года N 5к-27-01

В кассационной жалобе истец ставит вопрос об отмене состоявшегося судебного постановления, указав, что основанием для привлечения его к дисциплинарной ответственности явилась видеозапись. Данная запись судом не исследовалась. В основу решения положены показания работников таможенных органов, которые являлись свидетелями наличия такой записи и просматривали ее, однако не видели самого факта получения вознаграждения. Видеозапись осуществлялась в рамках ОРМ. Указанная видеозапись ни судом, ни лицами, участвующими в деле, предметом исследования и оценки не была. ...Видно, что видеозапись производилась видеокамерой, установленной в области груди водителя, передававшие-

го деньги. В момент их передачи и беседы этого человека с истцом лица его видно не было, поэтому ссылка суда о правомерности действий МВД об отказе в предоставлении видеозаписи или ее части нельзя признать убедительной.

Материалы, полученные в результате оперативно-розыскных мероприятий, до облечения их в форму, предусмотренную уголовно-процессуальным законодательством, либо при отсутствии возможности ввести их в уголовный процесс, никаких правовых последствий не влекут.

Приведенные требования закона при рассмотрении дела не учтены, не проверено, какие основания имелись у органов МВД для проведения оперативно-розыскных мероприятий, не разрешен вопрос о возможности и допустимости указанной видеозаписи в качестве доказательства по гражданскому делу.

А вот что может быть, если на запись не накладывается информация о дате и времени...

Из приказа о наложении на истца дисциплинарного взыскания видно, что правонарушение было совершено в 10 часов 40 мин. 11 сентября 2000 года.

А из пояснений истца следует, что 11 сентября 2000 года они заступили на пост в 11 часов 30 минут.

При таких обстоятельствах решение суда первой инстанции по этому делу нельзя признать законным и обоснованным.

Украина

Скрытая видеозапись может быть доказательством

Несколько цитат из речи спикера Генпрокуратуры Украины.

"По делу проведена видеофонограммная экспертиза. Установлено, что запись является оригиналом, сделанным непрерывно. Какой-либо монтаж не производился. Запись звука и изображения сделаны одновременно". "...сделал скрытую видеозапись, после того как ему начали угрожать физической расправой ...при таких условиях видеозапись является допустимым доказательством в деле".

Германия

Вопрос об использовании видеозаписей в Германии законодательно не урегулирован. Но, разумеется, существует судебная практика. Немецкие суды при рассмотрении уголовных дел признают доказательствами видеозаписи, если они не затрагивают личную сферу запечатленных на них лиц, а также третьих лиц и способствуют выяснению обстоятельств совершения преступления. В целом, скрытая видеозапись может повлечь за собой иск о возмещении морального вреда. Поэтому желательно заранее информировать людей об установленной системе видеонаблюдения.

До недавнего времени использование видеозаписей в гражданском процессе в качестве доказательств отрицалось. Но сейчас ситуация стала меняться. Показательным примером является Решение немецкого Федерального Трудового Суда № 2 AZR 51/02 от 27 марта 2003 г. Суть заключается в следующем: кассира одного супермаркета уволили на основании потери доверия начальника к нему после установления с помощью видеозаписи факта мелкой кражи денег из кассы магазина. Кассир в исковом заявлении ссылаясь на недопустимость использования видеозаписей, произведенных скрытыми видеокameraми, но суд посчитал его аргументы неубедительными. Решение обосновывалось тем, что другим способом доказать факт кражи в супермаркете было невозможно.

Интересно, что в решении суда никак не отражены факты экспертизы видео-

записи на предмет ее подлинности. В вышеупомянутом случае использовалась аналоговая видеотехника. К сожалению, что касается цифровых видеозаписей, то еще нет достоверных данных по судебной практике.

США

В США на федеральном уровне действуют Правила доказательства в редакции 2003 года. Согласно Правилу № 1001 видеозапись может являться доказательством по гражданским и уголовным делам. Но только в том случае, если ей не наносится моральный ущерб гражданину путем вторжения в его частную жизнь. Ст. 273 Федерального УПК разрешает использовать запись видеоконференции в качестве доказательства. На основании судебной практики разработано специальное юридическое понятие - "квазиочевидец". Это тот человек, который наблюдал за происходящим удаленно (например, на мониторе).

Информации, касающейся сертификации оборудования для систем видеонаблюдения, а также экспертизы оборудования и видеозаписей найти в открытых источниках не удалось.

При цифровой видеозаписи суду необходимо предоставить цифровую копию на любом носителе и объяснение как была произведена запись. Случаев, когда требовалось бы предоставить суду весь видеосервер или видеорегистратор практически не зафиксировано. Что касается объяснения способа цифровой видеозаписи, то здесь часто на помощь приходят производи-

тели или инсталляторы данной системы охранного видеонаблюдения.

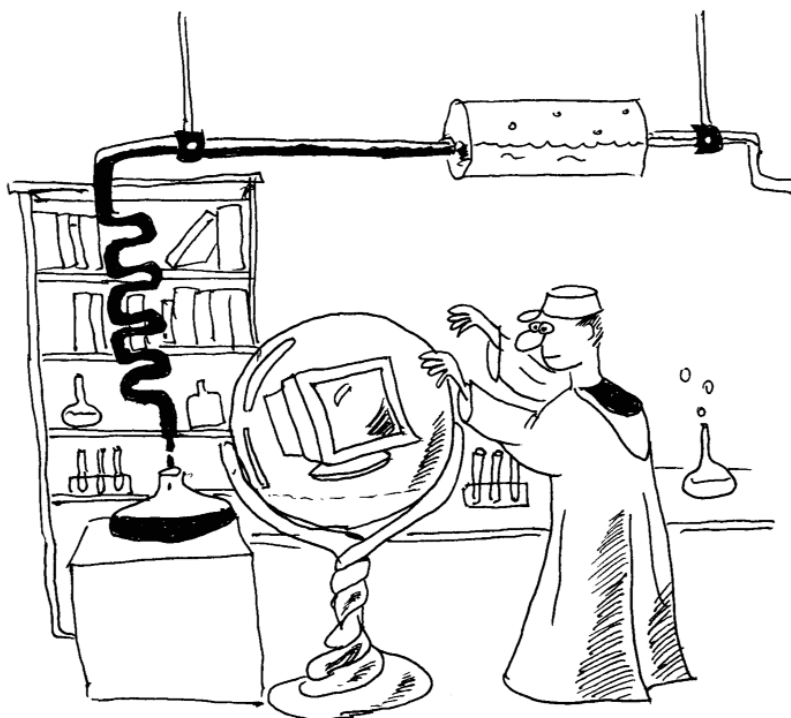
Беларусь

Согласно процессуальным кодексам РБ (ст. 100, 103 УПК РБ; ст. 74 ГПК РБ; ст. 74 ХПК РБ) видеозапись может являться доказательством. В рамках гражданского и хозяйственного процесса видеозаписи, полученные в нарушение законодательства скрытым путем, не могут использоваться в качестве доказательств. Пока достаточной судебной практики по вопросам установления факта подлинности видеозаписей в Беларуси не существует.

Швейцария

В Швейцарии вопрос о допустимости видеозаписи в качестве доказательства законодательно не урегулирован. Согласно ст. 37 Федерального Закона о федеральном гражданском процессе 1947 года данный вопрос решается судом на основании внутреннего убеждения. Местные суды рассматривают видеозаписи в качестве полноценных доказательств. Вопрос с вторжением в частную жизнь человека решен аналогично немецкой практике.

Следует подчеркнуть, что по отдельным видам преступлений, например, нанесение тяжких телесных повреждений или убийств, вопрос о вторжении в частную жизнь человека не ставится. То есть подозреваемый фактически лишается возможности опротестовывать допустимость использования против него практически любой видеозаписи.



ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ ОХРАННЫЕ ТЕЛЕВИЗИОННЫЕ

Общие технические требования и методы испытаний

Television systems of security.
General technical requirements and test methods.

Дата введения 01/01/2001 г.

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт распространяется на вновь разрабатываемые и модернизируемые охранные телевизионные системы (далее - системы), предназначенные для использования в целях защиты людей и имущества на охраняемых объектах от преступных посягательств, и устанавливает общие технические требования и методы испытаний.

Требования настоящего стандарта в части 4.2 (требования к функциональным характеристикам), 4.3 (требования к техническим характеристикам), 4.4 (требования к электромагнитной совместимости), 4.5 (требования по устойчивости к несанкционированным действиям), 4.8 (требования к электропитанию), 4.9 (требования безопасности) являются обязательными.

2. НОРМАТИВНЫЕ ССЫЛКИ

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ 8.326-89 Государственная система обеспечения единства измерений. Метрологическая аттестация средств измерений

ГОСТ 12.1.005-88 Система стандартов безопасности труда. Общие санитарно-гигиенические требования к воздуху рабочей зоны

ГОСТ 12.1.006-84 (МЭК 65-85) Система стандартов безопасности труда. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля

ГОСТ 12.1.010-76 Система стандартов безопасности труда. Взрывобезопасность. Общие требования

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

ГОСТ 12.1.040-83 Система стандартов

безопасности труда. Лазерная безопасность. Общие положения

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

ГОСТ 12.2.006-87 (МЭК 65-85) Безопасность аппаратуры электронной сетевой и сходных с ней устройств, предназначенных для бытового и аналогичного общего применения. Общие требования и методы испытаний

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

ГОСТ 15.001-88 Система разработки и постановки продукции на производство. Продукция

производственно-технического назначения

ГОСТ 27.002-89 Надежность в технике. Основные понятия. Термины и определения ГОСТ 27.003-90 Надежность в технике. Состав и общие правила задания требований по надежности

ГОСТ 27.410-87 Надежность в технике. Методы контроля показателей надежности и планы контрольных испытаний на надежность

ГОСТ 7845-92 Система вещательного телевидения. Основные параметры Методы измерений

ГОСТ 12997-84 Изделия ГСП. Общие технические условия

ГОСТ 13109-97 Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения

ГОСТ 13699-91 Запись и воспроизведение информации. Термины и определения ГОСТ 14192-96 Маркировка грузов

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

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

ГОСТ 16962.1-89 (МЭК 68-2-1-74) Изделия электротехнические. Методы испытаний на устойчивость к климатическим внешним воздействующим факторам

ГОСТ 16962.2-90 Изделия электротехнические. Методы испытаний на устойчивость к механическим внешним воздействующим факторам

ГОСТ 17516-72 Изделия электротехнические. Условия эксплуатации в части воздействия механических факторов внешней среды

ГОСТ 17516.1-90 Изделия электротехнические. Общие требования в части стойкости к механическим внешним воздействующим факторам

ГОСТ 21879-88 Телевидение вещательное. Термины и определения

ГОСТ 23456-79 Установки телевизионные прикладного назначения. Методы измерений и испытаний

ГОСТ 27484-87 (МЭК 695-2-2-80) Испытания на пожароопасность. Методы испытаний. Испытания горелкой с игольчатым пламенем

ГОСТ 27570.0-87 (МЭК 335-1-76) Безопасность бытовых и аналогичных электрических приборов. Общие требования и методы испытаний

ГОСТ 27924-88 (МЭК 695-2-3-84) Испытания на пожароопасность. Методы испытаний. Испытания на плохой контакт при помощи накаливаемых элементов

ГОСТ 29073-91 Совместимость технических средств измерения, контроля и управления промышленными процессами электромагнитная. Устойчивость к электромаг-

гнитным помехам. Общие положения

ГОСТ 29192-91 Совместимость технических средств электромагнитная. Классификация технических средств

ГОСТ Р 8.563-96 Государственная система обеспечения единства измерений. Методики

выполнения измерений

ГОСТ Р 8.568-97 Государственная система обеспечения единства измерений. Аттестация испытательного оборудования. Основные положения

ГОСТ Р 50009-92 Совместимость технических средств охранной, пожарной и охранно-пожарной сигнализации электромагнитная. Требования, нормы и методы испытаний на помехоустойчивость и промышленные радиопомехи

ГОСТ Р 50627-93 Совместимость технических средств электромагнитная. Устойчивость к динамическим изменениям напряжения сети электропитания. Технические требования и методы испытаний

ГОСТ Р 50725-94 Соединительные линии в каналах изображения. Основные параметры. Методы измерений

ГОСТ Р 50775-95 (МЭК 839-1-1-88) Система тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения

ГОСТ Р 50776-95 (МЭК 839-1-4-89) Система тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию

ГОСТ Р 50862-96 Сейфы и хранилища ценностей. Требования и методы испытаний на

устойчивость к взлому и огнестойкость

ГОСТ Р 51121-97 Товары непродовольственные. Информация для потребителя. Общие требования

ГОСТ Р 51241-98 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний

ГОСТ Р 51242-98 Конструкции защитные механические и электромеханические для дверных и оконных проемов. Технические требования и методы испытаний на устойчивость к разрушающим воздействиям

ГОСТ Р 51318.14.1-99 (СИСПр 14-1-93) Совместимость технических средств электромагнитная. Радиопомехи промышленные от бытовых приборов, электрических инструментов и аналогичных устройств. Нормы и методы испытаний

3. ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящем стандарте применяются следующие термины с соответствующими

определениями:

3.1 телевидение: По ГОСТ 21879.

3.2 вещательное телевидение: По ГОСТ 21879.

3.3 замкнутое телевидение: Телевидение, используемое в различных отраслях науки и техники и, в отличие от вещательного, не предназначенное для массовой аудитории зрителей.

3.4 телевизионная система замкнутого типа: Совокупность технических средств, обладающих конструктивной, параметрической, информационной, программной и эксплуатационной совместимостью и обеспечивающих реализацию замкнутого телевидения.

3.5 система охранная телевизионная (СОТ): Телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений (со звуковым сопровождением или без него) служебной информации и извещений о тревоге с охраняемого объекта.

3.6 техническое средство СОТ (ТС СОТ): Конструктивно и функционально законченное (аппаратно-программное) устройство, входящее в состав системы.

3.7 охраняемый объект: Территория, здание, сооружение или помещение, оборудованные действующими средствами охранной сигнализации и охраняемые специальными подразделениями

3.8 охраняемая зона: По ГОСТ Р 50775.

3.9 пункт автономной охраны: Пункт, расположенный на охраняемом объекте или в непосредственной близости от него, оборудованный техническими средствами отображения информации о проникновении или/и пожаре в контролируемых помещениях (зонах) объекта для непосредственного восприятия человеком.

3.10 пункт централизованной охраны (ПЦО): По ГОСТ Р 50775.

3.11 сцена: Часть охраняемой зоны либо прилегающей к ней территории, анализ изображения которой производится одной телевизионной камерой.

3.12 цель: Находящийся в пределах сцены объект (человек, имущество), поведение (состояние) или индивидуальные характеристики которого могут быть определены оператором с помощью системы.

3.13 стандартная цель: Человек весом от 50 до 70 кг, ростом от 165 до 180 см, одетый в белый хлопчатобумажный халат.

3.14 тревога: По ГОСТ Р 50775.

3.15 тревожное событие: Проявление угрозы на охраняемом объекте.

3.16 работоспособное состояние: По ГОСТ 27.002.

3.17 неисправное состояние: По ГОСТ 27.002.

3.18 состояние тревоги: Состояние СОТ, которое является результатом реагирования системы на тревожное событие.

3.19 состояние наблюдения: Состояние системы, при котором она выполняет функции, достаточные для просмотра сцены оператором либо ручного сопровождения цели.

3.20 состояние охраны: Состояние системы, при котором она выполняет функции, достаточные для автоматического и, при необходимости, ручного сопровождения цели.

3.21 время реагирования системы на тревожное событие (время реагирования): Время от фактического пересечения границы сцены стандартной целью до момента выдачи системой извещения о тревоге.

3.22 сопровождение цели: Получение изображения движущейся в пределах сцены цели качеством, достаточным для определения оператором поведения (состояния) или индивидуальных характеристик цели.

3.23 ручное сопровождение цели: Сопровождение цели путем использования оператором органов управления технических средств системы.

3.24 автоматическое сопровождение цели: Сопровождение цели без участия оператора (или при минимальном его участии).

3.25 несанкционированные действия (НСД): Преднамеренные действия, направленные на нарушение правильности функционирования системы.

3.26 телевизионный анализ изображения (анализ изображения): По ГОСТ 21879.

3.27 синтез телевизионного изображения (синтез изображения): По ГОСТ 21879.

3.28 телевизионная камера (ТК): По ГОСТ 21879.

3.29 видеомонитор: По ГОСТ 21879.

3.30 видеонакопитель: По ГОСТ 13699.

3.31 последовательный переключатель: Устройство, позволяющее последовательно автоматически или вручную подключать источники видеосигнала к входу видеомонитора на определенное время.

3.32 квадратор: Устройство, позволяющее одновременно выводить на экран видеомонитора изображения от четырех источников видеосигнала, размещая их в соответствующих сегментах экрана.

3.33 мультиплексор: Устройство, позволяющее записывать сигналы от нескольких ТК на один видеоманитофон (мультиплексирование) путем записи последовательно по одному кадру изображения от каждой ТК, воспроизводить мультиплексированное изображение и обрабатывать сигналы извещения о тревоге.

3.34 матричный коммутатор: Многофункциональное устройство, позволяющее подключать любой вход к любому выходу системы, управлять ТС системы и обрабатывать сигналы извещения о тревоге по определенной программе.

3.35 обнаружитель движения: Устройство, формирующее сигнал извещения о тревоге при обнаружении изменений, обусловленных движением (появлением) цели на сцене.

3.36 видеопринтер: Устройство, позволяющее печатать кадры изображения на специальной бумаге.

3.37 видеоусилитель: Устройство, предназначенное для усиления и коррекции сигнала изображения, а также сложения его с различными сигналами, несущими служебную информацию.

3.38 кожух для телевизионной камеры: Устройство, предохраняющее ТК от внешних воздействий (перепадов температуры, влажности, осадков, НСД и др.).

3.39 видеозапись: По ГОСТ 13699.

3.40 видеозвукозапись: По ГОСТ 13699.

3.41 воспроизведение (информации): По ГОСТ 13699.

3.42 видеоманитофон: По ГОСТ 13699.

3.43 разрешение: По ГОСТ 21879.

3.44 телевизионный видеосигнал: По ГОСТ 21879

3.45 видеограмма: По ГОСТ 13699.

3.46 видеофонограмма: По ГОСТ 13699.

3.47 откат видеограммы (видеофонограммы): Возврат к предшествующей части видеограммы (видеофонограммы).

3.48 кадр: По ГОСТ 21879.

3.49 стоп-кадр: Режим работы технического средства СОТ (видеоаппарата, мультиплексора и др.), при котором циклически воспроизводится один кадр видеосигнала.

3.50 рабочий диапазон освещенностей: Диапазон освещенностей сцены (от минимальной до максимальной), в котором разрешение и отношение сигнал/шум телевизионной камеры не менее заданных.

3.51 чувствительность: Нижняя граница рабочего диапазона освещенностей сцены.

3.52 видеоканал: Совокупность технических средств системы, обеспечивающих телевизионный анализ, обработку, передачу и синтез телевизионного изображения от одной телевизионной камеры.

4. ОБЩИЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

4.1 Общие положения

4.1.1 Системы должны разрабатываться

(модернизироваться) в соответствии с требованиями настоящего стандарта, ГОСТ Р 50775, ГОСТ Р 50776, ГОСТ 15.001, технических условий (ТУ) и/или другой технической документации на конкретные системы.

4.1.2 Системы должны обеспечивать возможность круглосуточной работы.

4.1.3 Технические средства, предназначенные для построения систем, должны обладать конструктивной, информационной и эксплуатационной совместимостью. Параметры и требования, определяющие совместимость ТС, должны устанавливаться с учетом их назначения и условий применения в технической документации на конкретные системы.

4.1.4 Системы классифицируют в зависимости от их функциональных характеристик по следующим группам: с ограниченными функциями, расширенными функциями, многофункциональные; по категориям устойчивости к НСД: нормальной, повышенной и высокой устойчивости.

4.2 Требования к функциональным характеристикам систем

4.2.1 Обязательными для всех систем являются следующие функциональные характеристики-

- телевизионный анализ изображений с помощью одной или нескольких ТК;
- синтез телевизионных изображений, полученных от всех ТК;
- сопровождение цели;
- приоритетное отображение тревожных событий;
- сигнализация о несанкционированных действиях.

4.2.2 В зависимости от группы системы должны обеспечивать выполнение функциональных характеристик, указанных в таблице 1.

4.2.3 Система может иметь функциональные характеристики, не указанные в таблице 1. Такие характеристики должны указываться в ТУ и/или другой технической документации на конкретные системы.

4.3 Требования к техническим характеристикам

4.3.1 Технические характеристики систем

4.3.1.1 Значение разрешения системы должно соответствовать значению, указанному в ТУ и/или другой технической документации на конкретные системы. Разрешение системы должно быть указано для каждого видеоканала системы в телевизионных линиях (ТВЛ).

4.3.1.2 Значение времени реагирования системы на тревожное событие должно соответствовать для каждого видеоканала системы значению, указанному в ТУ и/или другой технической документации на конкретные системы.

кретные системы.

4.3.2 Технические характеристики телевизионных камер, приведенные ниже, и их значения должны соответствовать значениям, указанным в эксплуатационной документации на конкретные устройства:

- разрешение;
- рабочий диапазон освещенностей;
- отношение сигнал/шум.

4.3.3 Технические характеристики устройств обнаружения движения, приведенные ниже, и их значения должны соответствовать значениям, указанным в эксплуатационной документации на конкретные устройства:

- минимальный размер обнаруживаемой цели;
- минимальный контраст обнаруживаемой цели относительно фона;
- диапазон скоростей движения цели.

4.3.4 Технические характеристики видеонакопителей, приведенные ниже, и их значения должны соответствовать значениям, указанным в эксплуатационной документации на конкретные устройства:

- разрешение;
- отношение сигнал/шум;
- вид входного сигнала извещения о тревоге: тревога путем замыкания или размыкания контактов (увеличением или уменьшением тока).

4.3.5 Технические характеристики устройств управления и коммутации видеосигналов, приведенные ниже, и их значения должны соответствовать значениям, указанным в эксплуатационной документации на конкретные устройства:

- разрешение;
- отношение сигнал/шум;
- вид входного сигнала извещения о тревоге: тревога путем замыкания или размыкания контактов (увеличением или уменьшением тока);

- параметры сигнала оповещения о тревоге: максимальные коммутируемые напряжение и ток.

4.3.6 Технические характеристики видеомониторов, приведенные ниже, и их значения должны соответствовать значениям, указанным в эксплуатационной документации на конкретные устройства:

- разрешение;
- максимальная яркость изображения;
- геометрические и нелинейные искажения изображения.

4.3.7 Технические характеристики линий связи в каналах изображений должны соответствовать ГОСТ Р 50725.

4.4 Требования к электромагнитной совместимости

4.4.1 В соответствии с ГОСТ 29192 системы и входящие в них устройства относят-

ся по классификации технических средств к категории 4, по условиям эксплуатации - к группе Е.

4.4.2 В соответствии с ГОСТ 29073 системы и входящие в них устройства должны обеспечивать функционирование по критерию качества А или В в условиях воздействия электромагнитных помех. Степени жесткости систем и входящих в них устройств по ГОСТ Р 50009 должны быть следующие:

- вторая степень - при нормальной устойчивости;
- третья степень - при повышенной устойчивости;
- четвертая или пятая степень - при высокой устойчивости.

4.4.3 Уровень промышленных помех, создаваемых системой, не должен превышать норм, установленных ГОСТ 23511 и ГОСТ Р 50009.

4.5 Требования по устойчивости к НСД

4.5.1 ТС систем должны изготавливаться в исполнении, обеспечивающем защиту от прогнозируемых НСД, и/или размещаться в помещениях, местах (сейфах, боксах и др.), защищенных от этих действий.

4.5.2 Системы должны быть устойчивы к следующим воздействиям:

- разрушающим механическим НСД;
- несанкционированному доступу к программному обеспечению.

4.5.3 Требования по устойчивости к разрушающим механическим НСД распространяются на:

- кожухи и поворотные устройства телевизионных камер;
- сейфы, шкафы и др. для размещения устройств записи, управления и коммутации и т. д. Степень устойчивости ТС СОТ к НСД приведена в таблице 2.

4.5.4 Требования по устойчивости систем от несанкционированного доступа к информации - по ГОСТ Р 51241. При этом категория защиты системы от несанкционированного доступа к информации в соответствии с ГОСТ Р 51241 должна соответствовать:

- для систем нормальной устойчивости - классу Н;
- для систем повышенной устойчивости - классам ЗА, ЗБ, ЗВ;
- для систем высокой устойчивости - классам 1Г и 1В.

Категория защиты ТС должна соответствовать:

- для ТС нормальной устойчивости - классу Н;
- для ТС повышенной устойчивости - классу 5 или 6;
- для ТС высокой устойчивости - классу 4.

4.6 Требования надежности

В ТУ и/или другой технической документации на конкретные системы должны быть установлены показатели надежности в соответствии с ГОСТ 27.002 и ГОСТ 27.003.

4.7 Требования по устойчивости к внешним воздействующим факторам.

4.7.1 Исполнения ТС систем для различных климатических районов, категории размещения, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды должны соответствовать ГОСТ 15150.

4.7.2 В зависимости от условия применения в части воздействия механических нагрузок ТС систем должны обеспечивать требования по прочности и устойчивости при воздействии этих нагрузок. К ТС систем, не предназначенным для функционирования в условиях воздействия механических нагрузок, предъявляют требования только по прочности при воздействии этих нагрузок.

Требования по устойчивости в части воздействия механических факторов устанавливают в ТУ и/или другой технической документации на конкретные виды ТС в соответствии с требуемой группой условий эксплуатации по ГОСТ 17516 и степенью жесткости изделий по ГОСТ 16962.

4.8 Требования к электропитанию

4.8.1 Основное электропитание системы должно осуществляться от сети переменного тока по ГОСТ 13109.

Электропитание отдельных ТС допускается осуществлять от других источников с иными параметрами выходных напряжений, требования к которым устанавливают в эксплуатационной документации на конкретные ТС.

4.8.2 Система, в зависимости от группы по функциональным характеристикам, должна иметь резервное электропитание при пропадании напряжения основного источника питания. В качестве резервного источника питания может использоваться резервная сеть переменного тока или источники питания постоянного тока.

Номинальное напряжение резервного источника питания постоянного тока выбирается из ряда: 12; 24 В.

Переход на резервное питание должен происходить автоматически, без нарушения установленных режимов работы и функционального состояния системы.

При переходе на резервное электропитание должен выдаваться световой и/или звуковой сигнал.

4.8.3 Резервный источник питания должен обеспечивать выполнение основных функций системы, указанных в ТУ и/или

другой технической документации на систему, при пропадании напряжений в сети на время не менее 0,5 ч.

4.8.4 При использовании в качестве источника резервного питания аккумуляторных батарей должен выполняться их автоматический подзаряд.

4.8.5 При использовании в качестве источника резервного питания аккумуляторных или сухих батарей должна быть световая или звуковая индикация разряда батареи ниже допустимого предела. Сигнал разряда батарей может передаваться на ПЦО.

4.9 Требования безопасности

4.9.1 Система должна удовлетворять общим требованиям безопасности по ГОСТ 12.2.007.0 и ГОСТ 12.2.006.

4.9.2 Монтаж и эксплуатация ТС, требующих электропитания, должны отвечать требованиям безопасности по ГОСТ 12.2.003.

4.9.3 Система должна удовлетворять общим требованиям пожарной безопасности по ГОСТ 12.2.006.

4.9.4 Уровни излучений системы должны соответствовать нормам и требованиям безопасности, установленным ГОСТ 12.1.006, ГОСТ 12.1.040.

4.10 Требования к конструкции

4.10.1 Габаритные размеры ТС систем должны обеспечивать возможность транспортирования через типовые проемы зданий, а также сборку, установку и монтаж на месте эксплуатации.

4.10.2 Конструкция системы должна обеспечивать:

- взаимозаменяемость сменных однотипных составных частей;
- удобство технического обслуживания, эксплуатации и ремонтпригодность;
- защиту от несанкционированного доступа к элементам управления параметрами;
- санкционированный доступ ко всем элементам, узлам и блокам, требующим регулирования или замены в процессе эксплуатации.

4.10.3 Конструкционные, электроизоляционные материалы, покрытия и комплектующие изделия должны обеспечивать:

- механическую прочность;
- выполнение требований по устойчивости к несанкционированным действиям;
- безопасную работу в заданных условиях эксплуатации.

4.11 Требования к маркировке и упаковке

Маркировка ТС систем должна быть выполнена в соответствии с ГОСТ Р 50775, ГОСТ Р 51121 ГОСТ 12.2.006, ГОСТ 14192.

5. МЕТОДЫ ИСПЫТАНИЙ

5.1 Общие положения

5.1.1 Испытания систем проводят по методам, установленным настоящим стандартом и другими нормативными документами, а также по методикам, аттестованным согласно ГОСТ Р 8.563.

Объем и последовательность испытаний устанавливают в программе испытаний на конкретные системы.

5.1.2 Не допускается проводить испытание системы при одновременном воздействии предельных значений нескольких внешних воздействующих факторов, за исключением случаев, указанных в ТУ и/или технической документации на конкретные системы.

5.1.3 Перед началом испытаний органы регулирования, предназначенные для конечного пользователя, устанавливают в положение, соответствующее наилучшему визуальному восприятию изображения.

5.1.4 Во время проведения испытаний запрещается подстраивать и регулировать параметры системы с помощью органов регулирования и управления, не предназначенных для конечного пользователя, а также подтягивать крепежные детали.

5.1.5 Для проведения испытаний применяют средства измерений, имеющие свидетельства о поверке. Используемые для испытаний нестандартные средства измерений должны быть аттестованы по ГОСТ 8.326, а испытательное оборудование - по ГОСТ Р 8.568.

5.1.6 При проведении испытаний должны быть обеспечены требования техники безопасности и другие условия в соответствии с требованиями используемых нормативных документов.

Безопасность проведения работ, использования приборов, инструментов и оборудования - по ГОСТ 12.1.005, ГОСТ 12.1.006, ГОСТ 12.1.010, ГОСТ 12.1.019, ГОСТ 12.2.003.

Помещения для проведения испытаний должны соответствовать необходимому уровню безопасности работ, а приборы и оборудование должны использоваться в соответствии с предусмотренными ин-

струкциями.

5.1.7 Образцы, предназначенные для проведения испытаний, должны иметь нормативную и/или техническую документацию в объеме, необходимом для проведения испытаний, и быть полностью укомплектованы в соответствии с этой документацией.

5.1.8 Все испытания, кроме климатических, проводят в нормальных климатических условиях испытаний:

- температура окружающего воздуха (25 ± 10) °C;

- относительная влажность воздуха (65 ± 15) %;

- атмосферное давление 84-106 кПа.

5.2 Испытания на соответствие общим техническим требованиям

5.2.1 Испытания на соответствие систем требованиям к функциональным характеристикам (4.2) проводят путем проверки по специально разработанным методикам наличия функций в системе, указанных в 4.2, с последующим присвоением системе одной из трех групп по функциональным характеристикам.

5.2.2 Измерение разрешения систем (4.3.1.1) проводят по специально разработанным методикам и/или с использованием ГОСТ 23456.

5.2.3 Измерение времени реагирования (4.3.1.2) проводят путем имитации следующих тревожных ситуаций:

- появление стандартной цели в охраняемой зоне;

- отключение питания ТК;

- отключение линии связи ТК.

5.2.4 Измерение технических характеристик ТС систем (4.3.2-4.3.7) проводят по разработанным методикам и/или ГОСТ 7845, ГОСТ 23456, ГОСТ Р 50725.

Примечание - Допускается проводить испытания с использованием рабочих мест и стендов, состав и конфигурация которых должны указываться в ТУ и/или другой технической документации на конкретные системы.

5.2.5 Испытания на электромагнитную совместимость систем (4.4) проводят по ГОСТ Р 50009 и ГОСТ 23511.

5.2.6 Испытания по устойчивости ТС си-

стем к разрушающим механическим НСД (4.5.4) проводят по методам испытаний ГОСТ Р 50862 и ГОСТ Р 51242.

5.2.7 Испытания по устойчивости ТС от несанкционированного доступа к информации (4.5.5) проводят по ГОСТ Р 51241.

5.2.8 Установление соответствия системы требованиям надежности (4.6) проводят по методикам, разработанным с учетом положений и требований ГОСТ 27.410. Программу и периодичность испытаний разрабатывает предприятие-изготовитель и утверждает их в установленном порядке.

5.2.9 Испытания на устойчивость ТС систем к внешним воздействующим факторам (4.7) проводят по следующим методам испытаний:

- в части устойчивости к внешним климатическим воздействиям - по ГОСТ 16962, ГОСТ 16962.1, ГОСТ 23456;

- в части устойчивости к внешним механическим воздействиям - по ГОСТ 16962, ГОСТ 16962.2, ГОСТ 17516, ГОСТ 17516.1, ГОСТ 23456.

Примечание - Перечень ТС систем, предъявляемых для испытаний на устойчивость к внешним воздействующим факторам, должен быть указан в ТУ и/или другой технической документации на конкретные системы.

5.2.10 Испытания на соответствие систем требованиям к электропитанию (4.8) проводят по специально разработанным методикам испытаний с учетом методов испытаний по ГОСТ Р 50627 и ГОСТ 23456.

5.2.11 Испытания по обеспечению требований безопасности (4.9) проводят по специально разработанным методикам с учетом методов испытаний по ГОСТ 12.2.006, ГОСТ 12997, ГОСТ 27570.0; по пожарной безопасности - по ГОСТ 27484, ГОСТ 27924 и НПБ 247; по способам защиты человека от поражения электрическим током - по ГОСТ 12.2.007.0.

5.2.12 Оценку соответствия требованиям конструкции (4.10), маркировке и упаковке (4.11) следует проводить по специально разработанным методикам с учетом методов испытаний по ГОСТ Р 51121 и ГОСТ Р 50775.

Таблица 1

Техническое средство	Нормальная устойчивость	Повышенная устойчивость	Высокая устойчивость
Кожух и поворотное устройство телевизионной камеры	нет	Устойчивость к удару тяжелым предметом (энергия удара - 90 Дж)	1 Устойчивость к удару тяжелым предметом (энергия удара - 150 Дж) 2 Устойчивость к колюще-рубящему удару (не менее 30 ударов)
Сейф	нет	Класс устойчивости к взлому I (по ГОСТ Р 50862)	Класс устойчивости к взлому II (по ГОСТ Р 50862)

Функциональные характеристики систем	Группа систем		
	Ограниченные функции	Расширенные функции	Много-функциональные
1 Передача сигналов			
1.1 Передача изображений из охраняемого объекта на ПЦО	нет	нет	нет/да
1.2 Передача сигналов управления системой с ПЦО	нет	нет	нет/да
2 Запись и воспроизведение изображений			
2.1 Запись изображений в следующих режимах:			
- режим длительного времени записи	нет	нет/да	да
- режим записи в реальном времени	нет	да	да
2.2 Автоматическое переключение из режима длительного времени записи в режим записи в реальном времени, при получении извещения о тревоге, и обратно в режим длительного времени записи по истечении заданного времени	нет	нет/да	да
2.3 Наличие аудиоканала *	нет/да	нет/да	нет/да
2.4 Одновременная запись на один видеонакопитель изображений или изображений и звука** от нескольких ТК	нет	нет/да	нет/да
2.5 Одновременная запись текущего изображения или изображения и звука и воспроизведение ранее записанных изображений или изображений и звука**	нет	нет/да	нет/да
2.6 Откат видеороликов (видеофотоснимков)	нет	нет/да	да
2.7 Вывод стоп - кадра на отдельный видеомонитор без остановки записи:			
- вручную оператором	нет	нет/да	да
- автоматически при переходе системы в состояние тревоги	нет	нет/да	нет/да
3 Управление и коммутация видеосигналов			
3.1 Наличие энергонезависимой памяти для хранения установленных параметров при пропадании напряжения питания	нет	да	да
3.2 Организация нескольких пунктов автономной охраны	нет	нет/да	нет/да
3.3 Передача информации на устройства сбора информации или ЭВМ	нет	нет/да	да
3.4 Автоматическое сопровождение цели***	нет	нет/да	нет/да
3.5 Управление фокусным расстоянием объектива и диафрагмой (электронным затвором)***			
- ручное	нет	нет/да	да
- автоматическое	нет/да	нет/да	да
3.6 Компенсация***			
- прямых засветок объектива	нет	нет/да	да
- засветок цели сзади	нет/да	да	да
3.7 Автоматический контроль работоспособности ТС СОР и линий передачи информации с выдачей сигнала "авария" или "тревога" при неисправном состоянии системы	нет	нет/да	да
3.8 Резервирование электропитания СОР	нет/да	да	да
3.9 Переключение из состояния наблюдения в состояние охраны:			
- ручное	нет/да	да	да
- автоматическое программируемое	нет	нет/да	да
4 Вывод на экран видеомонитора служебной информации			
4.1 Состояние наблюдения:			
- текущее время	нет	нет/да	да
- текущая дата	нет	нет/да	да
- номер и/или имя телекамеры****	да	да	да
- режим записи	нет	нет/да	да
4.2 Состояние охраны:			
- дата и время перехода системы в состояние тревоги	нет	да	да
- текстовые указания оператору и план зоны, в которой произошло тревожное событие*****	нет	нет/да	да
- планы охраняемых зон*****	нет	нет/да	да

* При использовании телевизионных камер с аудиоканалом.

** При наличии аудиоканала в системе.

*** Возможно не для всех видеоканалов системы.

**** При наличии в составе СОР более 2 телевизионных камер.

***** Выводятся на экран компьютера, входящего в систему.

Примечание: В таблице приняты следующие обозначения:

"+" - наличие и проверка функции обязательны;

"-" - наличие функции не предусматривается;

"-/+" - возможны отсутствие и наличие функции, причем в последнем случае ее проверка обязательна.

КРИМИНАЛИСТИЧЕСКИЕ ТРЕБОВАНИЯ НА УСТАНОВКУ И ЭКСПЛУАТАЦИЮ ТЕЛЕВИЗИОННЫХ СИСТЕМ НАБЛЮДЕНИЯ

(выдержки из информационного письма "Криминалистические требования на установку и эксплуатацию телевизионных систем видеонаблюдения". - М.: ГУ ЭКЦ МВД России, 2001. Авторы Иванов П. Ю., Поставин В. И., Суржиков М. Л.)

Критерии качества изображений, пригодных для проведения идентификации

С помощью ТСН можно получить внешнее описание любого объекта. Это описание состоит из структурных, поверхностных и динамических характеристик. Так, например, описание внешнего вида человека включает заметные детали внешнего строения, предметов одежды и обуви, функциональные особенности. Для идентификации объектов необходимо иметь совокупность признаков, характерную только для данного объекта, и их относительную устойчивость. Тогда в пространстве признаков будет всего одна точка, соответствующая этому объекту. Человек обладает индивидуальностью (неповторимостью) внешнего вида и относительной устойчивостью признаков.

Процесс идентификации заключается в сравнении двух (или нескольких) совокупностей признаков между собой. Поэтому для идентификации необходимо выделить эти признаки. Для описания внешности человека крупными элементами лица, обладающими криминалистически значимыми признаками, являются: волосной покров головы, лоб, брови, глаза, веки, щеки, нос, носогубный фильтр, губы, зубы, подбородок, ушные раковины. Однако в крупном элементе при углубленном его изучении можно выделить составные части: при описании глаз это - строение глазной щели, выступание глазных яблок, вид внутренних углов глаз; при описании носа - переносье, спинка носа, основание носа, крылья носа. При этом каждый элемент внешности может характеризоваться следующими признаками: формой, размером, положением, цветом. Парные элементы также имеют симметрию или асимметрию. Каждый признак имеет три значения выраженности (два крайних и одно среднее). По мнению В.А. Снеткова, "общее число людей, из которых может быть выделено каждое лицо по совокупности этих признаков, будет равно 950" (Снетков В.Л. Габитоскопия: Учебник. - Волгоград: ВСШ МВД СССР, 1979.)

Однако на практике из-за влияния различных факторов количество признаков сокращается, а их отображение изменяется. Полноту отображения признаков можно

выразить в количестве признаков или вероятностью опознавания. Если отобразилось количество признаков, достаточное для категоричного ответа, то вероятность опознавания равна 1. Полнота отображения зависит от следующих характеристик изображения: резкости, пространственного разрешения, контрастности, глубины цвета, наличия и уровня шума, которые определяют качество изображения. На изменение отображения признаков влияют расположение источников света и характеристика освещенности, ракурс объекта.

Изображение не может быть резче, чем сам объект. Относительное движение камеры и предмета уменьшает резкость, образовывается "смаз". Самые резкие снимки получаются при условии неподвижности объекта и четкой фиксации камеры (отсутствие дрожания). Вследствие низкой контрастности объекта или мягкого освещения снимок может выглядеть менее резким. Отсутствие резкости возможно из-за неточной фокусировки или из-за аберраций объектива. Резкость зависит от разрешающей способности и остроты контуров.

Пространственное разрешение - очень важный параметр, который влияет на отображение деталей в первую очередь. Для выбора необходимого разрешения используется критерий, который определяет минимальное значение пространственного квантования. Указанное теоретическое значение было определено еще в 1928 году инженером американской телефонной компании AT&T Гарри Найквистом (позднее была сформулирована теорема Котельникова). Им были сформулированы критерии для оцифровки сигналов. Из этих критериев следует, что искажения информации будут отсутствовать, если число замеров по меньшей мере вдвое превышает число деталей. Для изображений это означает, что элемент изображения должен быть такого размера, чтобы на самую малую деталь объекта приходилось не менее двух элементов изображения. Если этот критерий не выполняется, говорят об избыточном или недостаточном квантовании. При недостаточной частоте квантования в изображении не только пропадают мелкие детали, но и появляется шум, искажающий изображение. Этот шум вызван наложением спектров. Недостаточная частота квантования приводит к появлению ложных низкочастотных гармоник. Эти ложные частоты имеют термин aliasing (англ.). В оптике это явление называют муар - эффектом.

На точность пространственного квантования влияют три значения: 1) размер све-

точувствительного элемента; 2) расстояние между светочувствительными элементами; 3) общее количество светочувствительных элементов. Первые два значения определяются технологией производства микросхемы - светочувствительной поверхности. Третье значение, как правило, указывается в технических характеристиках и измеряется либо в DPI (dot per inch) - количество точек на дюйм, либо в LPI (line per inch) - количество точек (линий) на отрезке прямой длиной в дюйм. Чем больше элементов на единицу длины, тем выше разрешающая способность.

Квантование яркости оказывает влияние на точность передачи полутонов. Диапазон значений яркости задается двумя параметрами - максимальным количеством градаций яркости (глубина точки) и максимальным значением яркости. Так как изображения, полученные ТСН, будут использоваться для проведения визуального исследования, то необходимое количество уровней серого определяется способностью человеческого восприятия изображения. По некоторым оценкам, человеческий глаз способен различать приблизительно 64 уровня серого. Однако необходимо иметь избыточность по двум причинам: из-за ошибок квантования и различия между кривыми чувствительности электронных элементов и глаза человека. При ошибках квантования в минимально оцифрованном изображении может появиться шум из-за статистического разброса измеряемого значения яркости. Визуально шум представляет собой мелкие вкрапления, хаотично разбросанные по изображению, и сильнее проявляется на темных участках.

Чувствительность глаза человека имеет логарифмическую зависимость (т.е. количество различаемых им полутонов в светлой и темной областях различно). Чувствительность цифрового устройства линейна, поэтому число необходимых градаций соответствует максимально требуемому в темной части тонового диапазона. Таким образом, для полутоновых изображений необходимо иметь не менее 256 градаций серого цвета, а для цветных изображений - по 256 градаций на каждый цвет.

Максимальное количество градаций яркости (глубина точки) связано с другим параметром - диапазоном оптических плотностей. Глубина точки показывает физическую возможность воспринимать большой диапазон оптических плотностей, а действительный диапазон приемного устройства еще зависит и от чувствительности считывающего устройства, и от электроники, и от

механики, применяемой в устройстве. Диапазон оптических плотностей является логарифмической производной, измеряется в относительных единицах от нуля до максимального значения, которое приводится в технических характеристиках.

Рельеф поверхности (в том числе лица) воспроизводится на изображении светлыми и темными полутонами, которые зависят от направления (боковое, верхнее, нижнее, переднее и заднее) и характеристики (направленное, рассеянное, нормальное) освещения. Элементы лица обладают различной способностью отражать падающий на них свет (Орлов П.Г. Идентификация личности по фотокарточкам. - М.: ВШ КГБ при СМ СССР, 1974). Светлые и темные тона с одной стороны выявляют рельеф лица, с другой - делают незаметными мелкие детали. В светлых тонах эти детали оказываются высветченными, в темных - затемненными. Образование, расположение и степень градации темных, светлых и средних тонов, резкость перехода между ними на лице или его изображении зависят от яркости и расположения источников света, светочувствительности приемников света.

При направленном освещении (например, солнечном) на изображении лица образуются тени в глазных впадинах, у основания носа, на верхней губе, подбородке, нижней челюсти и шее. При рассеянном освещении (например, при освещении в пасмурный день или при съемке в тени в солнечный день) выраженные тени отсутствуют, части лица передаются только различием светлых и средне светлых тонов. Наиболее правильно особенности лица отображаются в изображении, полученном при нормальном (комбинированном) освещении, которое предполагает не менее двух-трех источников света. Один из них является основным и устанавливается перед объектом; другие (дополнительные) располагаются с правой или левой стороны. Основным источником выявляет рельеф лица, дополнительные источники используются для подсветки теневых частей лица.

Вращение объекта относительно нормального положения вносит изменения в признаки идентификации. В портретной идентификации учитывают вращения в трех плоскостях: в вертикальной плоскости, параллельной плоскости изображения, - боковой наклон; в вертикальной плоскости, перпендикулярной плоскости изображения, - прямой наклон; в горизонтальной плоскости - поворот головы. Изменение угла бокового наклона не вызывает каких-либо изменений в отображении особенностей лица, поскольку вращение головы происходит в плоскости, параллельной плоскости изображения. При изменении угла прямого

наклона, независимо от того, рассматривается ли лицо в фас или в профиль, изменяются отображения особенностей лица, относящихся к форме, положению и вертикальным размерам. Горизонтальные размеры частей лица не изменяются. Поворот головы приводит к изменению в отображении только горизонтальных размеров. Вертикальные размеры остаются постоянными. При повороте лица в сторону от положения анфас до полного профиля ширина лица будет изменяться неодинаково, ближняя к наблюдателю половина будет сокращаться медленнее, чем дальняя, а также уменьшается расстояние между глазами.

Описанные изменения в отображении особенностей сохраняются, если голова остается в исходном положении, а меняется положение камеры относительно объекта наблюдения. Наиболее отчетливо отображаются особенности лица в плоскости изображения, когда объект наблюдения расположен на минимально допустимом расстоянии, определяемом фокусным расстоянием объектива. При этом четко отображаются форма, контуры, контраст и цветовая насыщенность частей лица, а также мелкие детали, имеющие первостепенное значение для индивидуализации объекта. Для лица такими деталями являются морщины, родинки, бородавки. В то же время, чем ближе объект к камере, тем больше искажения истинных соотношений размеров различно удаленных от камеры частей. Необходимо учитывать кривизну поля изображения и дисторсию.

Кривизна поля изображения - создаваемое сферической линзой изображение в плоскости, перпендикулярной оптической оси, не является плоским и имеет форму искривленной поверхности. В зависимости от линзы поверхность может быть выпуклой либо вогнутой. Наиболее сильно искажаются края.

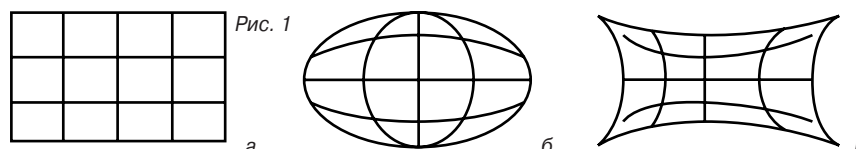
Дисторсия - нарушение закона подобия, различное увеличение частей одного изображения. Искажение зависит от расстояния точки до оптической оси.

В зависимости от расположения диафрагмы различают два вида дисторсии (рис. 1).

Рис. 1. Виды дисторсии: а - исходный; б - бочкообразный; в - подушкообразный

Если диафрагма впереди линзы - бочкообразная (увеличение больше в центре), а если диафрагма позади линзы - подушкообразная (увеличение больше по краям).

С удалением объекта от камеры на сним-



ке теряются мелкие детали лица, но более правильным становится отображение размерных соотношений крупных частей лица.

Для проведения идентификации необходимо выделить идентификационные признаки, которые в своей совокупности обладают индивидуальностью (или выделительной способностью). Выделительная способность определяется частотой встречаемости. Чем реже встречается признак, тем больше его идентификационная значимость. Имеется перечень особенностей лица, которые являются устойчивыми и относительно редкими. Частота встречаемости особенностей, указанных в перечне от 0,01 до 0,2. Экспериментальные данные показали, что такие признаки как искривление спинки носа, плоский подбородок и т.д. имеют большое идентификационное значение. Наиболее редкими признаками являются особые приметы (морщины, родинки и шрамы). Частота их встречаемости от 0,001 до 0,006. Общая частота совместной встречаемости входящих в совокупность независимых признаков определяется произведением их отдельных частот встречаемости. По оценкам П.Г. Орлова и З.И. Кирсанова, "комплекс совпадающих признаков внешности можно считать индивидуальным, если совместная частота встречаемости входящих в него признаков будет не более 10⁻⁷".

Причины ухудшения качества изображений, полученных при стационарном телевизионном наблюдении.

На качество изображений влияют следующие причины: ограничения, связанные с принципами построения ТСН, и искажения, вносимые в ходе передачи и записи изображений; режимы функционирования и условия эксплуатации.

Цветное изображение по своей природе более подвержено воздействию искажений, чем черно-белое, а существующие системы цветного ТВ по принципу действия вносят определенные ограничения качества.

Задачи получения, обработки и фиксации информации в процессе наблюдения для служб безопасности и криминалистических подразделений различны, поскольку первые занимаются наблюдением в режиме реального времени для предотвращения преступления и используют устройства отображения информации, а вторые работают с видеоматериалами, полученными ТСН, уже зафиксировавшими факт преступления или правонарушения.

В первом случае особое внимание уде-

ляется непосредственному наблюдению (без видеозаписи) оператором изображения со всех камер и лишь в случае необходимости или в ночное время производится видеозапись. Отсюда возникают требования к составу системы в целом и к параметрам составляющих ее устройств. Система должна быть с большим числом телекамер (с разрешением 350-420 твл), коммутатором, квадратором, обязательно качественным мультиплексором и среднего разрешения видеомагнитофоном (с разрешением до 350 твл). Естественно, изображение, переданное телекамерой и записанное подобным видеомагнитофоном, да еще в режиме мультиплексирования, для дальнейшей идентификации будет заведомо непригодно. Необходимо отметить, что интересующая информация может быть вообще не записана при неправильно выбранном режиме работы камер и магнитофона, или вследствие преднамеренных действий преступника, учитывая кратковременность включения камеры.

Во втором случае для фиксации информации (видеозаписи) необходимы только телекамеры (желательно с вариообъективом) и видеомагнитофоны - на каждую из них. Причем для получения изображения, пригодного для криминалистической идентификации, все устройства должны быть максимально высокого качества.

Минимально допустимая площадь наблюдаемого объекта представляет собой минимальную площадь изображения объекта в кадре, достаточную для проведения идентификации объекта. По предварительным результатам экспериментальных исследований, минимально допустимая площадь объекта (например, лица) составляет 1/7 площади кадра. Исходя из минимального размера площади наблюдаемого объекта в кадре, зафиксированного ТСН, выбирается объектив камеры (угол обзора, фокусное расстояние) с таким учетом, чтобы при любых условиях площадь изображения наблюдаемого объекта в кадре была больше минимально допустимой.

Минимально допустимая площадь изображения наблюдаемого объекта накладывает определенные требования на состав и режимы работы устройств ТСН. В отдельных случаях для охраны наиболее ответственных объектов требуется установка дополнительного оборудования для получения более качественного изображения (например, дополнительные камеры и видеомагнитофон). При использовании нескольких камер (в том числе с вариообъективом) для фиксации одного и того же объекта необходимо четко согласовать режимы работы коммутатора, мультиплексора и видеомагнитофона, а также устройства, управляющего варио-

объективом. Нежелательно одновременно записывать изображение от более чем четырех телекамер (мультикартина), поскольку площадь изображения наблюдаемого объекта в кадре будет меньше минимально допустимой и оно станет непригодно для проведения идентификации.

Результирующая (общая) разрешающая способность складывается из разрешающих способностей каждого из устройств, входящих в ТСН. По мнению авторов, наиболее слабым звеном (с точки зрения разрешения) ТСН является видеомагнитофон, на который в конечном итоге записывается изображение наблюдаемого объекта. Обзор рынка современных видеомагнитофонов, применяемых в ТСН, показывает, что лучшие модели способны записывать черно-белое изображение с разрешением 400 твл. Естественно, они являются наиболее дорогостоящими. Для получения изображения, пригодного для проведения идентификации, возможно использование магнитофонов с разрешением 240-380 твл. В этом случае предъявляются более жесткие требования к объективам, разрешению телекамер, их расположению и освещенности объектов. Например, в данном случае объектив надо выбирать с тем расчетом, чтобы угол обзора и фокусное расстояние позволяли получать изображение объекта в кадре максимально возможной площади, а разрешение телекамеры должно быть не менее 480 твл. Можно использовать вариообъектив, когда возникает необходимость наблюдения одной и той же камерой, как охраняемого пространства, так и видеозаписи (фиксации) отдельного объекта, находящегося в данном пространстве. При этом нет необходимости непрерывно записывать изображение всего охраняемого пространства, а достаточно кратковременно произвести видеозапись интересующего объекта крупным планом.

При использовании квадратора в режиме записи на видеомагнитофон записываются изображения сразу со всех четырех телекамер, но так как изображение занимает лишь четверть кадра, то качество записи существенно ухудшается и часто становится непригодным для дальнейшей идентификации. Ухудшение качества изображения можно компенсировать путем подбора более качественных параметров объектива и телекамеры, а также увеличением площади изображения наблюдаемого объекта в кадре, о которых рассказано выше. Разрешение квадраторов колеблется в интервале от 640х480 до 1024х512 пикс, что в определенной степени позволяет компенсировать указанное ухудшение качества изображения.

При записи изображений с нескольких камер с помощью мультиплексора кадры

пишутся на магнитофон целиком без ухудшения результирующего разрешения. Этого удалось достичь благодаря последовательной записи кадров со всех камер на видеокассету. Однако при выводе на монитор изображения с нескольких камер (мультикартина) движение объектов на экране получается дискретным, "дерганым", т.к. при цифровой обработке мультиплексор теряет часть информации. Мультикартина удобна при воспроизведении ранее записанной информации, во время наблюдения ее использовать нецелесообразно (изображение с одной камеры составляет 1/16 экрана). Для наблюдения за реальной ситуацией лучше применять квадраторы или матричные коммутаторы.

ТСН в зависимости от многообразия выполняемых задач будут включать в себя разные по составу и количеству функциональные устройства. Каждое устройство, входящее в состав ТСН, имеет свои функциональные особенности и режимы работы, поэтому вопрос выбора наиболее эффективного (для получения изображения, пригодного для идентификации) режима работы как всей системы в целом, так и отдельных устройств, приобретает первостепенное значение. Несогласованный, неправильный выбор режима работы хотя бы одного устройства ТСН приводит не только к ухудшению качества конечного (записанного на видеоленту) изображения, но и к потере информации вообще. Например, даже в случае получения качественного изображения, пригодного для идентификации, необходимо выбрать такой режим работы устройств ТСН, при котором была исключена возможность преднамеренного сокрытия идентифицирующих признаков наблюдаемого объекта. Иными словами, наблюдаемый объект должен относительно продолжительное время находиться перед объективом телекамеры, с которой в данный момент производится запись изображения на видеомагнитофон. Это требует соответствующей (весьма проблематичной при использовании многокамерной ТСН) настройки режима работы коммутатора либо добавления в систему дополнительного оборудования (вариообъектива и устройства управления вариообъективом и/или видеомагнитофона).

В случае непродолжительного нахождения объекта перед камерой, по мнению авторов, для получения качественной конечной картинки с каждой из телекамер системы наблюдения, должно записываться не менее пяти фреймов изображения наблюдаемого объекта, что позволит исключить возможные дефекты изображения (такие, как "смазы", расфокусировку изображения и т.д.).

Физическое размещение телекамер имеет большое значение как для выбора

оптимального состава ТСН, так и для получения качественного изображения. Приобретение дорогостоящих и высококачественных устройств ТСН станет бесполезным, если телекамера будет установлена неправильно. Из-за неудачного расположения камеры в охраняемом пространстве возможны следующие ситуации, ведущие к потере качества и информативности получаемых изображений: телекамера (при правильно выбранном фокусном расстоянии и угле обзора объектива) не охватывает необходимое охраняемое пространство; изображение наблюдаемого объекта становится меньше минимально допустимого размера изображения, пригодного для идентификации; телекамера выдает изображение наблюдаемого объекта в ракурсе, непригодном для проведения идентификации; близость к источникам радиоэлектронных помех, искажающих выдаваемое камерой изображение; наличие препятствия между объективом камеры и наблюдаемым объектом (стекло, прозрачная пленка, сетка и т.д.).

К ухудшению качества изображения, получаемого ТСН, приводит неудачное расположение телекамеры относительно источников естественного и искусственного освещения в охраняемом пространстве.

Ухудшение качества изображения наблюдается при следующих условиях: недостаточная освещенность помещения, в котором расположена камера; недостаточная освещенность наблюдаемого объекта; избыточная освещенность помещения, в котором расположена камера; избыточная освещенность наблюдаемого объекта; расположение источника света такое, что у наблюдаемого объекта искажаются индивидуализирующие признаки, появляются блики, тени и т.д.; фоновая засветка (постоянная или периодически возникающая); размещение и работа телекамеры в условиях, в которых по техническим параметрам данная модель не предназначена к использованию.

Рекомендации по установке и эксплуатации телевизионных систем наблюдения.

Организация стационарного наблюдения заключается в определении задач наблюдения, исходя из стратегии безопасности, в выборе системной конфигурации и параметров устройств систем наблюдения, их установке и соединении, а также в создании оптимальных условий освещенности и режимов работы.

При выборе системной конфигурации необходимо обратить внимание на следующие особенности: при фиксации визуальной информации посредством видеозаписи в процессе приема, передачи и обработки сигнала задействованы не все ус-

ройства системы. Изображение, полученное камерой, может передаваться через мультиплексор или коммутатор на видеоманитон; в сложной системе экономического подкласса - через квадратор на видеоманитон. Выше было отмечено, что идеальным случаем системной конфигурации для видеозаписи является подключение видеоманитона непосредственно к камере. Тогда в системе необходимо иметь для каждой камеры свой видеоманитон, что не реально.

При выборе параметров устройств основное внимание должно уделяться их разрешению. Результирующее разрешение системы будет зависеть от разрешения устройств, входящих в нее. Высокое разрешение камеры и низкое разрешение манитона, или наоборот, приводят к общему снижению разрешения системы. В результате экспериментальных исследований установлено, что для фиксации объектов с мелкими деталями, к которым относятся лицо человека, номер автомашины, текст документа, необходимо разрешение около 500 твл.

При выборе камеры необходимо согласовать освещенность объектов наблюдения и светочувствительность камеры. Ориентировочная освещенность объектов на широте г. Москвы следующая: безоблачный солнечный день (угол солнца 55°) - 100000 люкс; солнечный день с легкими облаками - 70000 люкс; пасмурный день - 20000 люкс; раннее утро - 500 люкс; сумерки - 4 люкс; ясная ночь, полная луна - 0,2 люкс; ясная ночь, неполная луна - 0,02 люкс; ночь, луна в облаках - 0,007 люкс; ясная, безлунная ночь - 0,001 люкс; безлунная ночь с легкими облаками - 0,0007 люкс; помещение без окон - 100-200 люкс; хорошо освещенные помещения, офисы - 200-1000 люкс.

Для повышения чувствительности камеры используются приборы ночного видения (например, электронно-оптические преобразователи). Чувствительность при использовании ПНВ увеличивается в 100 - 10000 раз. Однако за ними необходим специальный уход - не включать днем, всячески предохранять от выгорания катод ЭОП.

Другой путь повышения чувствительности - это приобретение дорогостоящих камер (например, производства Sony). В данных камерах установлена ПЗС - матрица Нурег HAD, в которой для каждого светочувствительного элемента устанавливается миниатюрная прецизионная собирающая линза, что позволяет сконцентрировать световой поток без лишнего его рассеивания. В результате вдвое возрастает чувствительность матрицы.

Для обеспечения качественной работы в условиях переменной яркости изображения и различных уровней фоновых засветок со-

временные камеры оснащаются подсистемами компенсации этих воздействий. Функция съемки при низких уровнях освещенности позволяет получать изображения с хорошим цветовым балансом при минимальной освещенности без увеличения шума. Если условия освещения существенно изменяются, то необходимо применение автоматической диафрагмы или электронного затвора. Это необходимо, например, в помещении, в котором освещение изменяется в разное время суток. В случае, когда требуется максимальная глубина резкости или четкость границ ярких объектов, необходимо применение автоматической диафрагмы.

При установке ТСН особое значение имеет правильное расположение камеры. Оно определяется углом и высотой установки камеры, расстоянием до объекта, исходя из минимального размера объекта в кадре и критичного ракурса объекта. Чтобы изображение объекта занимало максимальную площадь кадра, необходимо подобрать фокусное расстояние по формуле 2, приведенной в п. 1.2. В качестве размеров изображения объекта указываются параметры матрицы.

В зависимости от плана помещения выбирают объектив с необходимым углом зрения. Для максимального угла обзора устанавливают широкоугольные объективы с фокусным расстоянием 3,5 мм. При этом угол зрения будет около 90°. Длиннофокусные объективы с фокусным расстоянием 12 мм и углом зрения 30° используют при наблюдении периметра объекта.

При съемке с одной и той же точки объективами с различными фокусными расстояниями масштаб изображения изменяется прямо пропорционально величине фокусного расстояния. Изображения близко расположенных объектов при использовании короткофокусных объективов будут более контрастными и резкими в сравнении с изображением удаленных объектов при использовании длиннофокусных объективов. Короткофокусный объектив при небольшом диафрагмировании обладает большой глубиной резкости. Длиннофокусный объектив при съемке удаленных объектов имеет ограниченную глубину резкости.

При съемке объектов отклонение оптической оси объектива от горизонтального положения приводит к появлению нежелательных перспективных искажений. Это явление особенно заметно при использовании короткофокусных объективов. Поэтому отклонение оптической оси от горизонтального положения должно быть минимальным.