Журнал для руководителей предприятий и специалистов отрасли безопасности

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

№ 5 (20)
сентябрь-октябрь
2011

Безопасность многофункциональных и критически важных объектов

Информационная безопасность

Инженерно-техническая безопасность

Антитеррористическая защищенность зданий и сооружений

Каналы сопряжения и коммуникации, информационно-аналитические системы

AXIOM
SECURITY

Не требует доказательств

Оборудование охранного CCTV видеонаблюдения

УНП: 100972915

ОДО "Сфератрэйд"
ул. Машиностроителей 29-502, Минск 220118 Беларусь
info@secur.by www.secur.by

Тел./факс: +375 17 3415050
Velcom: +375 29 6415050
МТС: +375 29 5415050

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ, №5-2011
В НОМЕРЕ:

ОФИЦИАЛЬНЫЙ РАЗДЕЛ

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ (СВН)

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ (ОХРАНА ПЕРИМЕТРА)

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ (ПОЖАРНАЯ БЕЗОПАСНОСТЬ)

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ (СКУД)

АНТИТЕРРОРИСТИЧЕСКАЯ ЗАЩИЩЕННОСТЬ ЗДАНИЙ И СООРУЖЕНИЙ

КВОИ

КАНАЛЫ СОПРЯЖЕНИЯ И КОММУНИКАЦИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СПРАВОЧНАЯ ИНФОРМАЦИЯ

«ТЕХНОЛОГИИ БЕЗОПАСНОСТИ»
Производственно-практический журнал
№ 5 (20) 2011, сентябрь-октябрь 2011

Периодичность выхода: 1 раз в 2 месяца

Учредитель и издатель:
ООО «АэркомБел»

Главный редактор:
Сергей Адамович Драгун

Журнал зарегистрирован
в Министерстве информации
Республики Беларусь
Свидетельство о регистрации
№ 846 от 10.12.2009

Адрес редакции:
220073, г. Минск, ул. Гусовского, 6,
оф. 2.15.2
Тел./факс: (017) 310-40-41, 290-84-05

Отдел рекламы:
Тел./факс: (017) 310-40-41,
310-40-42, 290-84-05
e-mail: info@aercom.by
www.aercom.by

Отдел подписки:
Тел./факс: (017) 310-40-41, 290-84-05
e-mail: podpiska@aercom.by

Подписка через РУП «Белпочта»:
01248 — для индивидуальных подписчиков;
012482 — для предприятий и организаций.

Цена 35000 бел. руб. без НДС,
на основании п. 3.12 ст. 286
Особенной части Налогового Кодекса
Республики Беларусь

Подписано в печать — 19.12.2011 г.
Формат: 60x90 1/8
Бумага офсетная
Гарнитура Myriad Pro. Печать офсетная
Усл. печ. л. 8,5; Уч.-изд.л.8
Тираж: 800 экз.
Заказ _____

Отпечатано в типографии
ООО «Юстмаж»

Адрес типографии: г. Минск,
ул. Калиновского, д.6, Г 4/К, комн. 201
Лиц. ЛП №02330/0552734 от 31.12.2009,
Министерство информации РБ

ISSN 2221-8661

Данный номер журнала стал итогом конференции «Безопасность на многофункциональных и спортивных объектах», проведенной 2 ноября 2011 на базе Белорусского государственного университета информатики и радиоэлектроники.

Конференция получилась насыщенной и практически полезной для всех участников. Основная задача мероприятия — всестороннее рассмотрение методов и средств обеспечения комплексной безопасности, многофункциональных и критически важных объектов — успешно реализована. На мероприятии был представлен ряд уникальных докладов, часть которых обобщена и опубликована в журнале.

Основные выводы после проведения конференции можно сделать следующие:

- с точки зрения использования современных средств и систем безопасности многофункциональные и критически важные объекты являются наиболее перспективными в нашей стране (в т.ч. коммерчески перспективными);
- такого рода объекты требуют интеграции как технической (различных систем безопасности), так и организационной (взаимодействие различных силовых ведомств);
- требуется дальнейшая проработка национальной нормативной базы;
- необходимо повышение квалификации специалистов всех уровней (проектировщиков, инсталляторов, пользователей СБ, руководителей, представителей регуляторов и др.).

Опыт нашей работы, а также практика аналогичных изданий других стран говорят о том, что только специализированные издания (информационные площадки) могут сформировать мероприятия с глубоко проработанной концепцией. Именно такие мероприятия являются наиболее эффективными для знакомства специалистов с практическими решениями вопросов безопасности на объектах.

Хочу поблагодарить всех участников и организаторов конференции. В частности Департамент охраны МВД, специалистами которого была оказана основная методическая помощь в разработке концепции мероприятия. Отдельные слова благодарности выражаю руководству Белорусского государственного университета информатики и радиоэлектроники за помощь в подготовке мероприятия и предоставление современной материально-технической базы.

Мы намерены продолжать развивать профессиональное общение, создавая специализированные национальные информационные площадки. В планах журнала «Технологии безопасности» проведение в 2012 году ряда семинаров и специализированной белорусской выставки-форума по безопасности.

С уважением, Драгун Сергей Адамович,
главный редактор журнала

Научно-практическая конференция

Безопасность многофункциональных и спортивных объектов с массовым пребыванием людей

Организаторы:

Информационные партнеры:

Официальные партнеры, участники:

9 772221 866000 11005

• telecom • computers • bank • automation • security • software • electronic components •
• printing • digital printing • informatization • digital house • office technologies •

tibo 2012

19-ая МЕЖДУНАРОДНАЯ СПЕЦИАЛИЗИРОВАННАЯ ВЫСТАВКА И КОНГРЕСС

ТЕЛЕКОММУНИКАЦИИ. СЕТЕВЫЕ ТЕХНОЛОГИИ.
МОБИЛЬНАЯ И ФИКСИРОВАННАЯ СВЯЗЬ, РАДИОСВЯЗЬ. ОПЕРАТОРЫ СВЯЗИ
СИСТЕМЫ БЕЗОПАСНОСТИ.
СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ.
IT ТЕХНОЛОГИИ, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.
ПЕРИФЕРИЙНЫЕ УСТРОЙСТВА.
СИСТЕМЫ АВТОМАТИЗАЦИИ ПРОИЗВОДСТВА, ПРОЕКТИРОВАНИЯ И УПРАВЛЕНИЯ.
ЭЛЕКТРОПИТАЮЩИЕ УСТАНОВКИ, СИСТЕМЫ ЭНЕРГОСБЕРЕЖЕНИЯ, КОНДИЦИОНИРОВАНИЯ И ВЕНТИЛЯЦИИ.
АВТОМАТИЗАЦИЯ И ВСТРАИВАЕМЫЕ СИСТЕМЫ.
ИЗМЕРИТЕЛЬНАЯ ТЕХНИКА.
ТЕХНОЛОГИИ "УМНОГО ДОМА".

25-28 апреля 2012

ФУТБОЛЬНЫЙ МАНЕЖ

г. Минск, пр. Победителей, 20/2

ЗАО "Техника и коммуникации", Тел.: (375-17) 306 06 06, (375-29) 650 91 02
E-mail: tibo@tc.by, www.tibo.by

Разработка правовых основ обеспечения безопасности критически важных объектов информатизации

Перевалов Д.В., начальник кафедры ГУО «Институт национальной безопасности Республики Беларусь», кандидат юридических наук, доцент

В современных условиях все большую актуальность приобретает проблема обеспечения безопасности критически важных объектов информатизации (далее — КВОИ). В Республике Беларусь данному вопросу также придается особое значение. В частности, в Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 09.11.2010 № 575, отмечается, что основным национальным интересом в информационной сфере является обеспечение надежности и устойчивости функционирования критически важных объектов информатизации (п.14). Кроме того, в Концепции национальной безопасности Республики Беларусь в качестве основных направлений нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности предусмотрено обеспечение материально-технической основы безопасности функционирования КВОИ, а также разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное негативное воздействие на национальную безопасность (абз.5 п.51, абз.2 п.54[1]).

Одним из приоритетных направлений государственной политики в сфере обеспечения безопасности КВОИ, как представляется, является разработка правовых основ в данной области. Немаловажное значение это имеет и для обеспечения безопасности многофункциональных и спортивных объектов с массовым пребыванием людей, так как такие объекты достаточно часто содержат в себе КВОИ.

Правовая основа КВОИ должна представлять собой иерархически выстроенную систему нормативных правовых актов, состоящую из следующих уровней:

1) ***конституционный уровень***, который включает нормы Конституции Республики Беларусь, определяющие основные положения права собственно-сти, обеспечения экологической безопасности, деятельности государственных органов по обеспечению прав и свобод личности (*ст.ст. 13, 44, 46, 59*[2]);

2) ***базовый уровень***, который составляют нормы специального законодательного акта, определяющие правовой статус КВОИ, субъектов государственного управления в этой сфере и их функции, систему и содержание мер обеспечения безопасности КВОИ, порядок их применения, а также субъектов контроля и надзора в этой сфере и их функции (*ст.ст. 27-41 Закона Республики Беларусь об информации, информатизации и защите информации*»[3]);

3) ***функциональный уровень***, включающий нормы законодательных актов, указов Президента Республики Беларусь, постановлений Правительства Республики Беларусь, а также нормативных правовых актов уполномоченных государственных органов и собственников КВОИ, детализирующих вопросы реализации мер обеспечения их безопасности КВОИ (*например, Указ Президента Республики Беларусь «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» от 25.10.2011 № 486*[4]);

4) ***обеспечивающий уровень***, объединяющий нормы законодательных актов, непосредственно не регламентирующих обеспечение безопасности КВОИ, но определяющих полномочия государственных органов и иных организаций по реализации соответствующих мер в данной области, а также нормы указов Президента Республики Беларусь и постановлений Правительства Республики Беларусь по отдельным вопросам обеспечения безопасности КВОИ (*например, п.5, абз.5 п.51, абз.2 п.54 Концепция национальной безопасности Республики Беларусь*);

5) ***технико-технологический*** уровень, который составляют нормы различных технических стандартов, регламентирующие требования и правила обеспечения безопасности информационных технологий (*например, СТБ 34.101.1-2004*[5]).

Вместе с тем, при осуществлении правового регулирования обеспечения безопасности КВОИ возникает ряд проблем, основной из которых является сопряжение технических аспектов обеспечения безопасности

[1] Концепция национальной безопасности Республики Беларусь: Указ Президента Республики Беларусь от 09 нояб. 2010 г., № 575 // Нац. реестр правовых актов Респ. Беларусь. — 2010. — № 276. — 1/12080.

[2] Конституция Республики Беларусь, 15 марта 1994 года; с изменениями и дополнениями, принятыми на респуб. референдумах 24 ноября 1996 г. и 17 октября 2004 г. // Нац. реестр правовых актов Респ. Беларусь. — 1999. — № 1. — 1/0; 2004 — № 188. — 1/6032.

[3] Об информации, информатизации и защите информации: Закон Респ. Беларусь от 10 нояб. 2008 г., № 455-З // Нац. реестр правовых актов Респ. Беларусь. — 2008. — № 279. — 2/1552.

[4] О некоторых мерах по обеспечению безопасности критически важных объектов информатизации: Указ Президента Респ. Беларусь, 25 окт. 2011 г., № 486 // Нац. реестр правовых актов Респ. Беларусь. — 2011. — № 121. — 1/13026.

[5] Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель: СТБ 34.101.1-2004. — Введ. 21.07.04. — Минск: Госстандарт: Белорус. гос. ин-т стандартизации и сертификации, 2004. — 36 с.

КВОИ с закономерностями правовой регламентации данной сферы общественных отношений.

Наличие данной проблемы обусловлено следующими обстоятельствами:

– ***во-первых***, теми последствиями, которые влечет за собой включение деятельности по обеспечению безопасности КВОИ в сферу правового регулирования:

а) подчинение этой деятельности принципам правового регулирования (использование правовых дефиниций, определение правового статуса субъектов, определение вида и характера действий, установления процедурного порядка осуществления действий);

б) определение пределов осуществления деятельности по обеспечению безопасности КВОИ (осуществление действий только по технической защите информации или/и иных действий);

в) установление при осуществлении деятельности по обеспечению безопасности КВОИ общеобязательных и унифицированных правил поведения (невыполнение этих действий влечет административную или уголовную ответственность, например, нарушение правил защиты информации (*ст.22.7 Кодекса Республики Беларусь об административных правонарушениях*[1]) или умышленное нарушение правил эксплуатации компьютерной системы или сети (*ст.355 Уголовного кодекса Республики Беларусь*[2]);

– ***во-вторых***, спецификой деятельности по обеспечению безопасности КВОИ:

а) такая деятельность в большинстве своем регулируется различными техническими нормативными правовыми актами;

б) функционирование технических устройств, программно-аппаратных средств урегулировать нормативными правовыми актами невозможно.

Однако в настоящее время предпринята попытка решить проблему сопряжения технических и правовых аспектов обеспечения безопасности КВОИ и урегулировать данную сферу общественных отношений.

25 октября 2011 г. Главой государства принят ***Указ № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»***, проект которого был подготовлен специалистами Института национальной безопасности Республики Беларусь с привлечением специалистов Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь.

Данный нормативный правовой акт содержит следующие основные аспекты:

1) его положения устанавливают понятийно-категориальный аппарат в сфере обеспечения безопасности КВОИ — понятия и определения объекта информатизации, КВОИ, угрозы безопасности КВО;

2) определяется компетенция органов государственного управления в данной сфере — Совета Министров Республики Беларусь, Оперативно-аналитического центра при Президенте Республики Беларусь, владельцев КВОИ, государственных органов (организаций), в подчинении (составе, системе) которого находятся владельцы КВОИ;

3) порядок отнесения объектов информатизации к КВОИ и содержание деятельности по обеспечению безопасного функционирования КВОИ;

4) порядок исключения объектов информатизации из числа КВОИ.

Необходимо отметить, что работа над проектом Указа носила сложный характер, многие его положения носили компромиссный характер, ряд положений не в полной мере корреспондируется с положения технических нормативных правовых актов. Например, определение термина «объект информатизации» в Указе № 486 не совпадает с определением, которое дано в ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

В дальнейшем предполагается принятие целой группы нормативных правовых актов, которые должны урегулировать ряд вопросов в сфере обеспечения безопасности КВОИ (*п.4 Указа № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»*). В частности, будут разработаны и установлены Советом Министров Республики Беларусь отраслевые критерии отнесения объектов информатизации к КВОИ, определен порядок ведения Государственного реестра КВОИ.

Таким образом, можно сделать следующие выводы:

1) разработка правовой основы обеспечения безопасности КВОИ является актуальным направлением деятельности в данной сфере;

2) при осуществлении правового регулирования обеспечения безопасности КВОИ возникает ряд проблем, основной из которых является сопряжение технических аспектов обеспечения безопасности КВОИ и закономерностей правовой регламентации данной сферы общественных отношений;

3) решение указанной проблемы возможно только при учете как технических, так и правовых аспектов обеспечения безопасности КВОИ.

Список использованных источников

1. Конституция Республики Беларусь, 15 марта 1994 года; с изменениями и дополнениями, принятыми на респуб. референдумах 24 ноября 1996 г. и 17 октября 2004 г. // Нац. реестр правовых актов Респ. Беларусь. — 1999. — № 1. — 1/0; 2004 — № 188. — 1/6032.

2. Уголовный кодекс Республики Беларусь, 9 июля 1999 г., № 275-3 // Нац. реестр правовых актов Респ. Беларусь. — 1999. — № 76. — 2/50.

3. Кодекс Республики Беларусь об административных правонарушениях, 9 июля 1999 г., № 194-3 // Нац. реестр правовых актов Респ. Беларусь. — 2003. — № 63. — 2/946.

4. Об информации, информатизации и защите информации: Закон Респ. Беларусь, 10 нояб. 2008 г., № 455-3 // Нац. реестр правовых актов Респ. Беларусь. — 2008. — № 279. — 2/1552.

5. Концепция национальной безопасности Республики Беларусь: Указ Президента Республики Беларусь, 09 нояб. 2010 г., № 575 // Нац. реестр правовых актов Респ. Беларусь. — 2010. — № 276. — 1/12080.

6. О некоторых мерах по обеспечению безопасности критически важных объектов информатизации: Указ Президента Респ. Беларусь, 25 окт. 2011 г., № 486 // Нац. реестр правовых актов Респ. Беларусь. — 2011. — № 121. — 1/13026.

7. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель: СТБ 34.101.1-2004. — Введ. 21.07.04. — Минск: Госстандарт: Белорус. гос. ин-т стандартизации и сертификации, 2004. — 36 с. ■

[1] Кодекс Республики Беларусь об административных правонарушениях, 9 июля 1999 г., № 194-3 // Нац. реестр правовых актов Респ. Беларусь. — 2003. — № 63. — 2/946.

[2] Уголовный кодекс Республики Беларусь, 9 июля 1999 г., № 275-3 // Нац. реестр правовых актов Респ. Бела-русь. — 1999. — № 76. — 2/50.

Обеспечение защиты информации в системах безопасности объектов с массовым пребыванием людей

Барановский Олег Константинович, заместитель начальника испытательной лаборатории по науке Государственного предприятия «НИИ ТЗИ»

Справка ТБ

Барановский Олег Константинович. Образование высшее, радиофизик, в 1998 г. окончил Белорусский государственный университет. Имеет академическую степень магистра естественных наук, кандидат физико-математических наук. Опыт работы в области защиты информации — с 1998 г. по настоящее время.

Развитие информационных технологий, их использование в технологиях безопасности позволяет реализовывать все более сложные требования к качеству функционирования объектов с массовым пребыванием людей, например, спортивных комплексов. В последнее время в связи с задачей повышения экономической эффективности эксплуатации таких объектов наблюдается устойчивый тренд к их многофункциональности. Многофункциональные комплексы позволяют проводить, помимо спортивных, культурно-зрелищные, общественные и политические мероприятия. Характерной отличительной чертой таких мероприятий является совместное пребывание десятков тысяч людей в ограниченном закрытом пространстве.

Современные многофункциональные объекты — это сложные инженерные сооружения со своей специфической технологией и высокими эксплуатационными характеристиками. Основным показателем качества функционирования таких объектов является обеспечение безопасности их функционирования, особенно безопасности присутствующих людей.

Безопасное функционирование обеспечивается путем ввода в эксплуатацию ряда систем. В первую очередь к ним относятся:

- дежурно-диспетчерская система;
- охранная сигнализация;
- пожарная сигнализация;
- контроль и управление доступом;
- видеонаблюдение;
- пожарная автоматика (пожаротушение, противодымная защита, оповещение, эвакуация);
- связь с объектом;
- электроосвещение и электропитание;
- поддержание микроклимата (теплоснабжение, вентиляция, кондиционирование).

Так, объекты должны быть оборудованы комплексом систем оповещения, сообщающим о тревожном событии, порядке и путях эвакуации. Для обеспечения управления процессом эвакуации зрителей с трибун и прилегающей территории сооружения должны быть оборудованы системами видеонаблюдения, позволяющими вести оперативный контроль с помощью камер видеонаблюдения и совместно с системой оповещения координировать эвакуацию посетителей.

Помимо этого, система видеонаблюдения должна обеспечивать оперативный поиск подозрительных лиц или находящихся в розыске преступников в контрольно-пропускных точках доступа на объект с последующим сообщением в службу безопасности объекта или органы внутренних дел.

Немаловажное значение отводится и системе охранной сигнализации объекта с возможностью сообщения о тревожных ситуациях, как в службу безопасности объекта, так и на местные пульты органов внутренних дел или вневедомственной охраны.

Система пожарной сигнализации должна предполагать возможность оперативной передачи информации о тревожной ситуации в местные органы МЧС, а также обеспечивать взаимодействие с инженерными системами, отвечающими за дымоудаление и отключение подачи воздуха на территорию возгорания.

Охранные системы обязательно связаны со службами мониторинга параметров безопасности, которые получают всю информацию о текущей ситуации от различных систем безопасности комплекса в целом.

К современным спортивным сооружениям мирового уровня все чаще добавляют определение «умный». Это означает, что все подсистемы интегрированы в комплексную систему безопасности. Для посетителей плюсом такого объекта, прежде всего, является гарантия быстрой реакции на предотвращение последствий аварийных и других, связанных с безопасностью, ситуаций. Обслуживающему персоналу на «умных» объектах проще осуществлять контроль оборудования, поддерживать стабильность работы систем управления.

Проектирование и построение комплексных систем безопасности должно осуществляться с учетом модели угроз безопасности объекта, которая включает модель нарушителя.

Как правило, для такого рода объектов различают три модели нарушителей:

- хулиганство;
- криминал;
- терроризм.

Хорошо известны многочисленные случаи, когда хулиганы забрасывали бутылками, петардами, частями сидений спортивное поле или сцену, участвовали в массовых драках. Пользуясь значительным скоплением людей, увлеченно следящих за происходящим на спортивной арене, криминальные элементы совершают карманные кражи, похищают личные вещи, оставленные без присмотра. Любое массовое мероприятие может стать мишенью террористов. Причины очевидны. Во-первых, это всегда крупное скопление гражданского населения. Во-вторых, на таких мероприятиях могут присутствовать граждане других стран, высокопоставленные гости, в том числе и представители государственных органов высокого ранга. В третьих, мероприятия широко освещаются прессой.

Модель нарушителя безопасности — это совокупность его целей и возможностей, направленных или потенциально приводящих к нарушению безопасности людей и активов объекта.

Современные злоумышленники все чаще для достижения своих целей воздействуют на системы контроля и управления различными аспектами безопасности объектов.

Например, хулиганы в целях препятствования их идентификации могут ослеплять камеры наблюдения. Хулиганы-хакеры пытаются взламывать информационные системы объекта, препятствуя качественному оказанию информационных услуг как посетителям, находящимся во время мероприятия на объекте, так и внешним пользователям. Криминальные элементы будут заинтересованы в подделке и незаконной перепродаже электронных билетов, что может привести к конфликтным ситуациям при проходе посетителей через электронные системы пропуска. Целью террористов часто является создание паники путем нарушения режима штатного функционирования или вывода из строя систем видеоотображения, звукового сопровождения, пожарной автоматики, систем поддержания микроклимата и управления эвакуацией людей.

Обеспечение безопасности многофункциональных объектов, на которых проводятся мероприятия международного уровня, должно проводиться с учетом всех трех моделей.

В связи с этим, в продуктах и системах обеспечения штатного функционирования объекта должны быть предусмотрены механизмы безопасности, а комплексные системы безопасности объектов должны включать подсистемы защиты информации.

Кроме того, для поддержания безопасной эксплуатации объекта рекомендуется создать и ввести в действие систему менеджмента информационной безопасности. За основу может быть взята система стандартов ИСО/МЭК 27000. Данная методология позволяет создать надежную защиту активов объекта путем анализа угроз, планирования и реализации мер защиты, выполнения процедур оценки остаточных рисков нарушения безопасного функционирования объекта и их снижения до приемлемого уровня.

В качестве иллюстраций рассмотрим несколько типичных угроз и путей их решения.

1. Система пожарной или охранной сигнализации. Угрозой информации является нарушение целостности и (или) доступности контролируемых параметров среды. Например, ввиду применения незащищенных к взлому протоколов обмена, поступающий на пульт службы безопасности сигнал подменяется злоумышленником с посылкой некорректного идентификатора места события безопасности. При этом контроль сотрудником службы безопасности с применением системы видеонаблюдения места потенциального возгорания или нарушения периметра безопасности не подтвердит факт события безопасности. В результате, направление сотрудников службы безопасности для проверки ситуации приведет к потере времени на предотвращение и (или) устранение последствий инцидента. Для снижения риска реализации данной угрозы необходимо использовать системы сигнализации со стойкими протоколами аутентификации данных.

2. Система видеонаблюдения. Угрозой информации является нарушение целостности и (или) доступности видеосигнала. Передача видеосигнала без механизма аутентификации данных позволяет злоумышленнику подменить сигнал реального времени с видеокамер, а отсутствие механизмов подтверждения подлинности позволяет корректировать данные видеоархива. Для снижения риска реализации данной угрозы необходимо использовать механизм электронной цифровой подписи видеосигнала.

3. Система контроля доступа. Угрозами информации являются нарушение конфиденциальности, целостности, доступности данных разграничения доступа. Сбои штатного функционирования механизмов идентификации в системе контроля и управления доступом из-за перегрузок сети и потери доступа к серверу с настройками безопасности могут привести к затруднению перемещения сотрудников по территории объекта. Для снижения риска необходимо дублировать каналы связи или использовать выделенные линии связи.

Важным вопросом для обеспечения безопасного проектирования и эксплуатации объектов в республике является своевременность разработки и введения стандартов, регламентирующих все аспекты управления безопасностью многофункциональных сооружений с массовым пребыванием людей.

Это, во-первых, проверка используемых продуктов и систем безопасности на соответствие требованиям безопасности информации (конфиденциальность, целостность, доступность, сохранность) в рамках добровольной и обязательной сертификации. Характерной особенностью таких продуктов и систем является высокая сложность последующей интеграции в них механизмов защиты информации.

Во-вторых, обеспечение безопасной поддержки жизненного цикла комплексных систем безопасности. Другими словами, проектирование и создание систем, обеспечивающих безопасное функционирование объекта, должно осуществляться по утвержденным процедурам, а субъекты должны иметь сертификат подтверждения соответствия: система качества соответствует утвержденным критериям качества оказания услуг в области защиты информации.

В-третьих, аттестация или подтверждение соответствия подсистем защиты информации комплексных систем безопасности требованиям ТНПА в области защиты информации до введения объекта в постоянную эксплуатацию.

Сегодня проектирование и создание многофункциональных объектов проводится в условиях зависимости от импорта продуктов и систем обеспечения различных аспектов безопасного функционирования этих объектов, а в отдельных случаях и с привлечением иностранных подрядчиков, при этом процедуры подтверждения соответствия требованиям безопасности информации не достаточно развиты. ■

Актуальные вопросы обеспечения безопасности объектов различных категорий с использованием технических средств и систем охраны

Брель Игорь Данилович,
полковник милиции,
заместитель начальника
управления средств
и систем охраны
Департамента охраны МВД
Республики Беларусь

В республике проводится много организационных и технических мероприятий по обеспечению безопасности многофункциональных и спортивных объектов, в том числе предусмотренных государственной программой по борьбе с преступностью и решениями местных исполнительных и распорядительных органов. Вместе с тем, проблема сегодня, на мой взгляд, состоит в механизме их реализации.

Нормативное оформление требований к системам видеонаблюдения

Безопасность таких объектов должна быть комплексной, отвечающей интересам не только МВД, но и КГБ, Министерства здравоохранения, МЧС и многих других ведомств. Поэтому проведению каких-либо мероприятий по безопасности должно предшествовать нормативное оформление этих требований, согласованное всеми вышеперечисленными ведомствами, так как интересы ведомств иногда могут не совпадать в способах реализации мер безопасности. Например, МВД заинтересовано в установке решеток, турникетов, а МЧС, наоборот, — в отсутствии препятствий на путях возможной эвакуации людей. МВД и КГБ заинтересованы в том, чтобы телекамеры, установленные в местах массового пребывания людей, решали целевую задачу по идентификации лиц. МЧС и Министерство здравоохранения заинтересованы, скорее, в целевой задаче обнаружения и различения для получения информации о пожаре или количестве пострадавших, так как им необходимо спасать людей, а не устанавливать их личность. В октябре текущего года МВД подготовило технические условия по оснащению системами видеонаблюдения объектов с массовым пребыванием людей, но единого нормативного правового или технического нормативного правового акта до сих пор нет.

Вторая проблема тесно связана с первой и обусловлена некомпетентностью в области отдельных видов безопасности лиц, которым по долгу службы приходится контролировать соблюдение норм безопасности. Как участковый инспектор милиции, юрист может проверить соблюдение игорным заведением требований нормативных правовых актов по наличию «телевизионной системы видеонаблюдения высокого разрешения», если в Департамент охраны регулярно обращаются проектные организации за разъяснением этого, то есть технические специалисты в области охранного телевидения? Логика подсказывает, что должен быть не просто нормативный документ по обеспечению безопасности многофункциональных и спортивных объектов, но его требования должны быть конкретны и понятны всем лицам, ответственным за их реализацию.

Третья проблема состоит в необходимости совершенствования правового регулирования внедрения телевизионных систем видеонаблюдения.

Очевидно, что до реализации организационных и технических мер по обеспечению безопасности многофункциональных и спортивных объектов следовало бы сначала обратиться к зарубежному опыту. И прежде всего к опыту Великобритании — страны, которая более полувека находится в состоянии гражданской войны. Или Израиля, то есть к опыту тех стран, которые уже давно столкнулись с терроризмом, бесчинствами болельщиков и другими угрозами.

Данные страны идут по пути создания нормативно оформленных требований, и только затем их реализации, проверки эффективности, а не наоборот.

В Великобритании накоплен большой опыт в области нормирования безопасности многофункциональных и спортивных объектов. На основе стандартов Великобритании и ведомственных нормативных актов министерств и ведомств страны уже не первый год издаются европейские стандарты, например, BS EN-50132-7:1999 «Технические системы охраны. Системы охранные телевизионные. Руководство по применению».

Нормативные акты Великобритании имеют разную степень обязательности исполнения, но кто мешает в Беларуси ввести в качестве обязательных требования тех же руководящих документов полиции Великобритании в области применения телевизионных систем видеонаблюдения, выпускаемых HOSDB (Home Office Scientific Development Branch):

• Guidance Notes for the Procurement of CCTV for Public Safety at Football Grounds (Руководство по применению телевизионных систем видеонаблюдения для обеспечения безопасности публики на футбольных стадионах).

• Performance Testing of CCTV Perimeter Surveillance System (Тестирование качества систем периметрового видеонаблюдения). *Издано в 1996 г., ныне является основным документом, описывающим методики тестирования телевизионных систем видеонаблюдения не только на периметре, но и в любых других условиях.*

• CCTV Operational Requirements Manual (Руководство по написанию функциональных требований к телевизионным системам видеонаблюдения). *5-я версия документа выпущена в 2009 г. и включает в себя описание особенностей СОТ с IP-телекамерами.*

Или документы, издаваемые:

NSI (National Security Inspectorate \Национальной инспекцией по безопасности), например, «Counter Terrorism Protective Security Advice for Stadia and Arenas» («Рекомендации по защите от терроризма стадионов и спортивных арен»)

LDSA (London District Surveyors Association /Ассоциацией наблюдателей Лондонского округа), например, «Safety of Sports Grounds No 4 — Guide to Electrical and Mechanical Services in Sports Grounds», 1996 ; «Safety of Sports Grounds No 3 — Guide to Control over Concessionaire Facilities and Other Services at Sports Grounds»

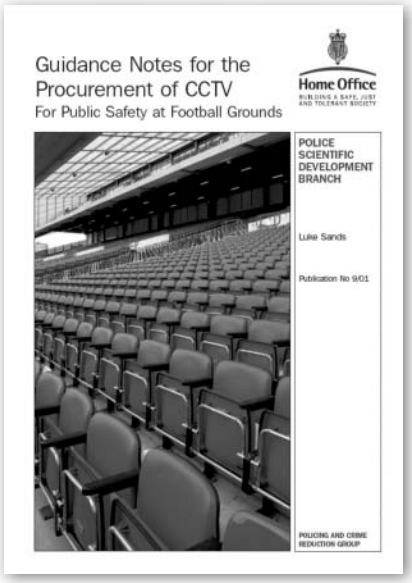
BSIA (British Security Industry Association \ Британской ассоциацией производителей охранной техники); **ACPO** (Association of Chief Police Officers \ Британской Ассоциацией полицейских), **DCMS** (Department for culture, media and sports \ Департаментом по культуре, средствам массовой информации и спорту), **NaCTSO** (National Counter Terrorism Security Office \ Национальной антитеррористической службой) **HSE** (Health and Safety Executive\ Исполнительным органом по здравоохранению и безопасности) и др.

Например, руководство, подготовленное Департаментом по культуре, средствам массовой информации и спорту (**DCMS**) «Guide to Safety at Sports Grounds, 2008, fifth edition \ «Руководство по обеспечению безопасности на спортивных объектах 2008, 5-я редакция»), — документ, который вполне годится для Беларуси, что актуально в сфере предстоящего чемпионата мира по хоккею, который будет проходить в Беларуси.

В этом документе подробно изложены требования к размещению

функциональных элементов спортивных объектов, к архитектурно-планировочным решениям, приведены расчеты безопасного наполнения объекта, требуемые расстояния между креслами, рядами, высота поручней, разделительных барьеров, требования к путям эвакуации и пр. (в интересах Минстройархитектуры, МЧС и других министерств), оснащению телевизионными системами видеонаблюдения, разделительными барьерами, механическими турникетами (в интересах МВД, КГБ, МЧС), а также описаны меры по обеспечению пожарной безопасности и оказанию первой медицинской помощи (в интересах МЧС, Минздрава) и пр.

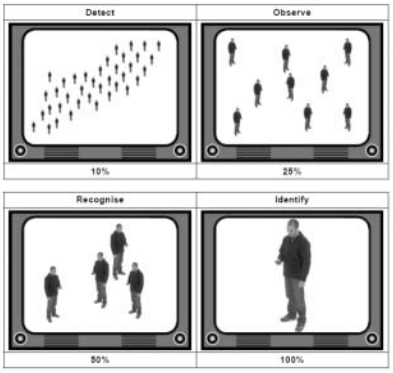
Руководство выдвигает конкретные требования перед проектировщиком по анализу возможных угроз, видеоизображению, которое следует получать от телекамер, планированию ответных мер на агрессию, террористические акты.



Относительно телевизионных систем видеонаблюдения Руководство требует соблюдения положений руководящего документа полиции Великобритании по обеспечению безопасности зрителей на футбольных стадионах, разработанных HOSDB.

При использовании аналоговых телекамер для сопровождения обнаруженной цели (мониторинга) — она должна занимать не менее 5 % высоты экрана, для обнаружения цели — 10 % высоты экрана, для различения (распознавания) — 50 %, для идентификации — 120 %.

Данные требования понятны не только для проектировщика, но и для участкового инспектора милиции — для проверки соблюдения таких требований не требуется специального образования. Это — отличительная черта руководящих документов полиции Великобритании. Для наглядности в руководящих документах требования сопровождаются иллюстрациями, например, такими, как в «CCTV Operational Requirements Manual. 2009» («Руководство по написанию функциональных требований к телевизионным системам видеонаблюдения»).



Данные изображения иллюстрируют требования к телевизионным системам видеонаблюдения для обычных объектов, а не для спортивных. Представленные иллюстрации не требуют никаких комментариев.

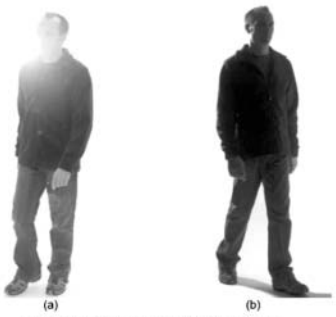
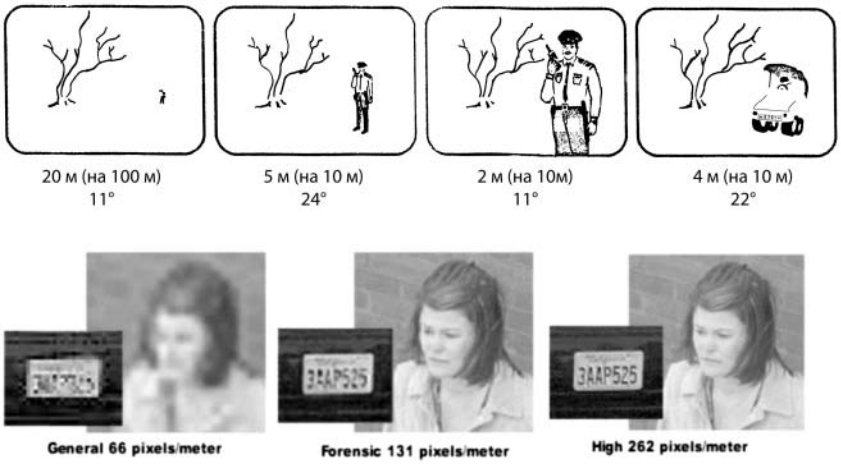


Figure 8: (a) effect of flare and (b) silhouette effect



Рекомендации Департамента охраны по выполнению системами охранного телевидения целевых задач, разработанные на основе документов Великобритании и России, выглядят следующим образом:

«При использовании аналоговых телекамер разрешением не менее 450 телевизионных линий по горизонтали (ТВЛ) для реализации целевых задач:

- для обнаружения человека его изображение должно составлять не менее 10 % высоты экрана (поле зрения по горизонтали 20 м);
- для различения или идентификации знакомого человека его изображение должно составлять не менее 60 % высоты экрана (поле зрения не более 5 м);
- для идентификации незнакомого человека его изображение должно составлять не менее 120 % высоты экрана (поле зрения — 2 м);
- для чтения государственного номера изображение легкового автомобиля должно быть не менее 50 % высоты экрана (поле зрения около 4 м).

Эти требования не трудно пересчитать и для IP-камер, которые широко используются в настоящее время. На прошлой конференции требования для решения целевых задач видеонаблюдения с помощью IP-камер озвучивала компания «Монтажные технологии»:

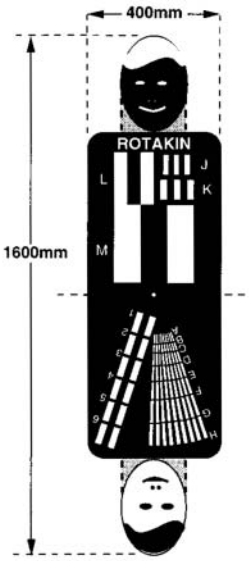
- для реализации целевой задачи **«обнаружения»** цель должна занимать не менее **66** пикселей на 1 м по горизонтали;
- для реализации целевой задачи **«различения»** — не менее **131** пикселя на 1 м по горизонтали;
- для реализации целевой задачи **«идентификации»** (высокой детализации) — не менее **262** пикселей на 1 м по горизонтали **для человека и госномера автомобиля**; а также **1100** пикселей — **для денежных купюр**.

Возвращаясь к «Guidance Notes for the Procurement of CCTV for Public Safety at Football Grounds» («Руководство по применению телевизионных систем видеонаблюдения для обеспечения безопасности публики на футбольных стадионах»), следует отметить, что Руководство не ограничивается только требованиями по вычислению размеров цели в процентах к высоте экрана, а требует использовать еще и манекен Rotakin, устанавливаемый в наиболее удаленной точке видеонаблюдения, как того требует и евростандарт BS EN50132-7. Манекен Rotakin — высококонтрастная тестовая цель в виде плоской фигуры 1,6 м х 0,4 м, с обеих сторон имеющей форму человеческой , а также ряд контрастных черно-белых полос.

Манекен устанавливается на границе зоны контроля телекамеры (на максимальном удалении от нее), при необходимости он поворачивается, чтобы имитировать движения человека. Дальше по изображению на мониторе оценивается распознаваемость деталей манекена. Если вы видите манекен, то, соответственно, вы увидите и человека — решите задачу идентификации, обнаружения или различения (распознавания).

На основе белорусского опыта монтажа и эксплуатации телекамер на «Минск-Арене», накопленного компанией «Новатех», а также такими компаниями, как «Спецэлектро», «Монтажные технологии», «Сатурн-Инфо» и др., можно дать следующие рекомендации:

1. При установке телекамер вблизи дорог, на площадях необходимо учитывать возможную вибрацию опор, на которых установлена телекамера, и повышенный уровень пыли, создаваемой транспортом, поэтому необходимо использовать телекамеры с функцией стабилизации видеоизображения. Кроме того необходимо применять герметичные



Rotakin Scale	mm/cycle on target	TV Lines/picture height for 100%R image
A	6,4	500
B	7,1	450
C	8,0	400
D	9,1	350
E	10,07	300
F	12,8	250
G	16,0	200
H	21,3	150
J	32,0	100
K	40,0	80
L	80,0	40
M	160,0	20

кожухи для телекамер со стеклоочистителями, иначе придется регулярно вызывать автовышку для протирки объектива.

2. При установке телекамер на стадионах необходимо предусматривать принудительное ограничение скорости телекамер, потому что при ее перемещении вручную легко «заблудиться» — заполненные трибуны (секторы) мало отличаются одна от другой.

3. Помимо управляемых телекамер, на стадионах и площадях (в интересах служб безопасности, МВД, КГБ, а также МЧС и Минздрава) обязательно необходимы фиксированные камеры, дающие обзорное изображение.

4. Следить за обстановкой на трибунах или во время массовых мероприятий необходимо визуально — никакие компьютерные программы не помогут (программы типа «Интеллект» лишь подсказывают о фиксации лиц, хранящихся в базе данных, помогая оператору, или позволяют обрабатывать созданный массив видеозаписи), поэтому нужно предусматривать большое количество рабочих мест для операторов. Это не ведет, однако, к необходимости создавать большой штат — на период проведения спортивных мероприятий в качестве операторов могут выступать сотрудники милиции, обеспечивающие общественный порядок.

5. Необходимо крайне осторожно применять цифровые системы с межкадровой компрессией типа MPEG, MJPEG, так как при быстром движении поворотной камеры они могут не обеспечить разборчивую видеозапись.

6. На крупном объекте всегда должен быть один главный центр мониторинга, куда будет стекаться вся информация о безопасности, касающаяся как нарушений общественного порядка, так и пожаров, других угроз безопасности, а в определенных местах могут быть установлены постоянные или временные удаленные рабочие места операторов, дополнительные центры мониторинга или просто индикаторные панели.

Правовое регулирование применения телевизионных систем видеонаблюдения

Если говорить о проблеме правового регулирования применения телевизионных систем видеонаблюдения, то в первую очередь необходимо обратить внимание на имеющуюся проблему законности видеонаблюдения вообще за гражданами, автотранспортом.

Если применение охранного телевидения разрешено Законом «Об охранной деятельности в Республике Беларусь», то остальное замкнутое телевидение («технологическое», «прикладное») при попадании в объектив человека или автомобиля оказывается вне закона, так как этим нарушаются конституционные права граждан, требования Закона «Об оперативно-розыскной деятельности», а при установке на предприятии — еще и требования «Трудового кодекса».

С охранным телевидением другая крайность: оно разрешено к применению без каких-либо ограничений, что тоже не совсем правильно, так как не каждому гражданину понравится, что за ним наблюдают скрыто установленной на абсолютно законных основаниях (по проекту) телекамерой, например, в кабинке для переодевания в супермаркете (для охраны товара от хищения).

Сегодня для наблюдения за зрителями на стадионах или в местах массового пребывания людей видеоизображение выводится на пост службы безопасности, которая не имеет права заниматься оперативно-розыскной деятельностью, охранять общественный порядок. Единственный выход — оформлять телевидение как охранное. Но тут граждане могут задать вопрос: «А что ж вы охраняете, кресла? А возле стадиона — тротуарную плитку?»

За рубежом с этого начинали. Именно оттуда пришли таблички, предупреждающие о ведении видеосъемки, но и они применяются только в случаях, установленных законодательством. Я в своих выступлениях часто в качестве примера того, как соблюдается законодательство по видеонаблюдению за рубежом, привожу случай с посещением белорусской делегацией центра мониторинга дорожного движения в Канаде. Центр представляет собой кинозал, но с экраном, состоящим из множества мониторов, в зале расположены операторы, причем за действиями нескольких операторов наблюдает контролер, а за контролерами еще контролеры — своеобразная пирамида.

Один из членов делегации спросил у сопровождающего, можно ли с помощью телекамер увидеть номерной знак автомобиля или лицо сидящего за рулем. В ответ делегату предложили самому это установить с помощью джойстика, управляющего трансфокатором телекамеры. В тот момент, когда изображение на экране увеличилось настолько, что можно было попытаться различить номер автомобиля, экран погас... Его отключил контролер. Как потом объяснили, действие сочли попыткой нарушения законодательства, защищающего права граждан: гражданин не давал согласия на съемку, данный акт считается вторжением в частную жизнь гражданина. Для контроля дорожной обстановки достаточно и наблюдавшейся ранее картинки. Однако делегат удивился: «А зачем же тогда трасфокатор?». — «В случае аварии оператору необходимо видеть, есть ли пострадавшие, имеется ли потребность в вызове ГАИ, скорой помощи, службы эвакуатора и т.п.»

К такому уважению закона надо стремиться и нам, а пока юристы по вопросу применения видеонаблюдения предлагают дождаться судебного прецедента. Что ж, подождем…

Ввоз и сертификация систем видеонаблюдения в Республике Беларусь

Согласно Указу Президента № 459 «О порядке лицензирования видов деятельности, связанных со специфическими товарами (работами, услугами)», на Государственный военно-промышленный комитет возложена функция лицензирования деятельности, связанной с продукцией военного назначения. Государственный военно-промышленный комитет и Государственный таможенный комитет издали постановление от 28.12.2007 г. № 15/137 (в ред. от 1.04.2009 г. № 5/23) «Об утверждении перечней специфических товаров (работ, услуг)», согласно которому к специальным технических средства для негласного визуального наблюдения и (или) документирования, то есть к вооружению, отнесли ... все телекамеры!

Читаем внимательно пункт 2.2 б) приложения 8 Постановления, согласно которому к специальным техническим средствам для негласного визуального наблюдения и (или) документирования относятся телекамеры **«без визира»**, то есть без функции просмотра отснятого изображения, которой нет ни в одной телекамере — это атрибут бытовых видеокамер. Далее — телекамеры, «работающие при низкой освещенности объекта (0,01 лк и менее) или при освещенности чувствительно-

го элемента 0,0001 лк и менее». Во-первых, стандарт Беларуси требует указывать чувствительность телекамеры (минимальную освещенность) только на сцене (на объекте), а не на чувствительном элементе. Во-вторых, постановление не разъясняет при каких условиях должна измеряться данная освещенность, то есть теряется смысл установления требований как таковых. В-третьих, получается, качественные телекамеры известных производителей с хорошей чувствительностью (лучше 0,01 лк) ввозить в Беларусь нужно так же, как и зенитно-ракетные комплексы. Аналогично следует ввозить и программное обеспечение типа «Интеллект», позволяющее производить поиск изображений людей в массиве видеозаписи.

Благо, что ни таможенники, ни военные не выполняют требование разработанного ими постановления, ограничивая ввоз только телекамер с вынесенным зрачком (pin-hole). А если начнут? Кстати, Закон «Об охранной деятельности не запрещает использовать телекамеры с объективом типа «pin-hole» в охранных целях (ими укомплектованы видеодомофоны, банкоматы), нет запрета на их использование ни в России, ни в других странах, так как задачи оперативно-розыскной деятельности могут решаться и обычными телекамерами, в том числе закамуфлированными под бытовые предметы.

Если это так актуально для Беларуси, то следует внести изменения в законодательство или ограничить п. 2.2 б) приложения 8 телекамерами, «закамуфлированными под бытовые предметы»?

Защита прав потребителей технических средств видеонаблюдения

Сегодня покупка телекамеры — это кот в мешке. Технические средства видеонаблюдения обязательной сертификации не подлежат и, зная позицию Госстандарта, регулярно сокращающего перечень товаров, подлежащих обязательной сертификации, не будут в ближайшее время. Такая позиция правильная: проблемы с защитой прав потребителей в области безопасности во всем мире решает не государство, а сами производители и поставщики средств безопасности, объединяющиеся в ассоциации. Для производителей и поставщиков средств безопасности потерять сертификат принадлежности к ассоциации систем безопасности равносилен банкротству. При оценке производства в рамках сертификации производители всегда показывают данный сертификат, а когда узнают, что требуется предоставить и сертификат соответствия, удивляются и начинают его лихорадочно искать. Ассоциации инициируют и разработку стандартов, не позволяющих присутствовать на рынке недобросовестным производителям и поставщикам.

30 дБ 20 дБ 15 дБ

У нас не только нет современного стандарта, но даже и органа по сертификации, способного в рамках добровольной сертификации выдать документ, подтверждающий технические характеристики телекамеры, хотя что-то можно проверить, руководствуясь ГОСТ 23456-79 и СТБ ГОСТ Р 51558-2003. Как без этого могут работать конкурсные («тендерные») комиссии, производящие закупку телекамер? Только верить паспорту, изготовленному на компьютере. В результате, как в анекдоте «джентельменам верят на слово — тут мне карта и пошла…», посмотрите на фантастические цифры, приводимые в паспортах на телекамеры.

Для решения проблемы можно также обратиться к зарубежному опыту. В Европе действует BS EN-50132-2-1:1998 «Технические системы охраны. Системы охранные телевизионные. Часть 2 . Раздел 1. Черно-белые телекамеры». В отличие от СТБ ГОСТ Р 51558-2003 по нему чувствительность может указываться как минимальная освещенность на чувствительном элементе либо на сцене (на объекте).

Но при указании чувствительности на сцене, как требует и СТБ ГОСТ Р 51558-2003, производитель обязан указать, при каких условиях она достигается, причем при отключенной АРУ. Например, чувствительность телекамеры «0,3 лк при светосиле объектива F 1,4 и пропусканием 0,9, пиковой отражательной способности объекта 60 %, при освещении, перпендикулярном объекту, и при выходном сигнале с соотношением сигнал/шум 40 дБ (*или в единицах IRE, что допускает BS EN-50132-2-1:1998*)». В качестве эксперимента возьмите прайс-листы, паспорта или пройдитесь по стендам выставок «Человек и безопасность», «Тибо» и посмотрите, кто подобным образом указывает чувствительность телекамер в паспортах, то есть соблюдает СТБ ГОСТ Р 51558-2003. Мне, например, наиболее часто отвечают: «А что это такое?..». Обидно за страну .

Продавцы телекамер в основной своей массе не в состоянии даже ответить, где измерена минимальная освещенность телекамеры, указанная в паспорте: на чувствительном элементе или на сцене, хотя цифры освещенности на сцене и на чувствительном элементе могут отличаться от 10 до 200 единиц при их взаимном переводе по правилу «большого пальца» или формулам, приведенным в учебнике Нэила Каминга (Neil Cumming). «Security: A Guide To Security System Design and Equipment Selection and Installation, Second Edittion»

Согласно BS EN-50132-2-1:1998, если производитель приводит чувствительность телекамеры как минимальную освещенность на сцене, рекомендуется, чтобы она приводилась с объективом F1.4, пиковой отражающей способностью объекта 0,89, пропусканием объектива 0,9 и освещением, перпендикулярным объекту. В таком случае чувствительность «на объекте» отличается от чувствительности «на ПЗС-матрице» ровно в 10 раз.

Как «вводят в заблуждение» покупателей телекамер, наглядно показывает приведенная ниже иллюстрация из журнала «Безопасность News № 15-1997 г ., демонстрирующая изображение, полученное от трех телекамер с «одинаковой» чувствительностью без указания соотношения сигнал/шум выходного сигнала, при котором она измерена.

Ответьте себе, на какое изображение вы рассчитывали, покупая телекамеру? Разве это не обман потребителей? Сегодня каждая уважающая себя охранная фирма вынуждена создавать испытательную лабораторию, чтобы не быть обманутой при покупке телекамеры. Не проще ли все эти вопросы решить на уровне белорусской ассоциации производителей и поставщиков охранной техники? ■

Практическое применение систем видеонаблюдения для повышения пожарной безопасности объектов и территорий

Воробьев С.Ю., Есипович Д.Л.,
НИИ ПБ МЧС Республики Беларусь
Катковский Л.В., НИИ ПФП БГУ им. А.Н. Севченко

Развитие и применение систем контроля технологий производства, охранного телевидения, контроля доступа показывают, что видеотехнологии могут успешно решать и задачи обеспечения пожарной безопасности объектов и территорий. Видеодетекторы могут обнаруживать пожар в помещении и на открытых площадках автоматически по таким специфическим признакам, как: задымленность, открытое пламя, характерные движения и частоты колебаний объекта на изображении. В то же время это позволяет при необходимости оператору визуально оценивать ситуацию на объекте.

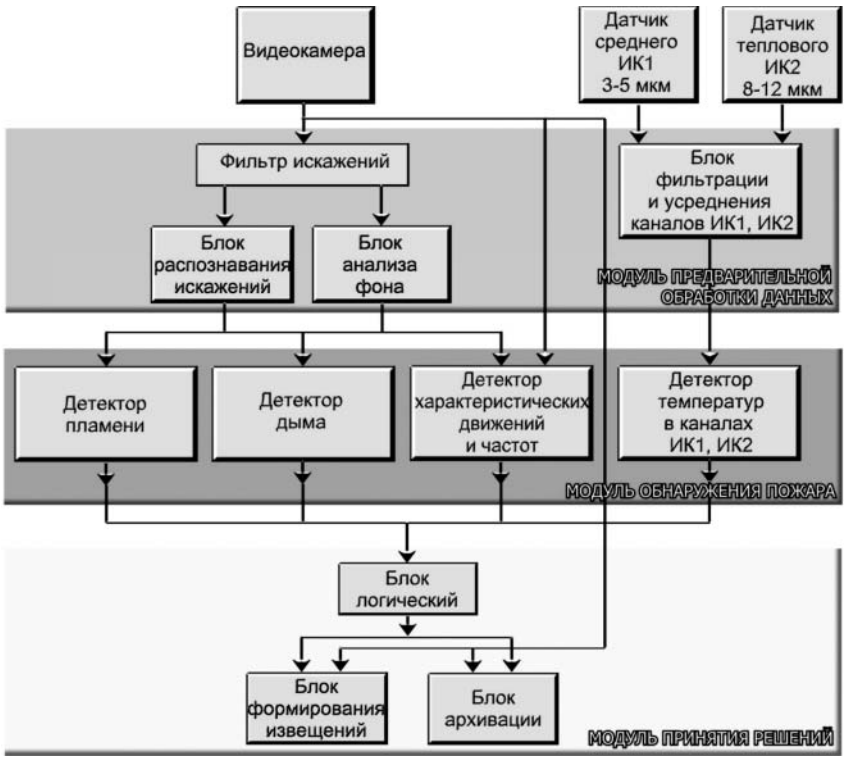
Традиционные сигнализаторы пожара, как правило, производят анализ выборки частиц или температур и проверку прозрачности воздуха. Эти устройства требуют близкого расположения к очагу пожара и не всегда надежны, так как большинство из них реагирует на дым, который не обязательно является результатом возгорания. Видеодетекторы могут использоваться в тех случаях, когда обычные сигнализаторы пожара не применимы. Системы видеонаблюдения могут успешно использоваться на объектах электроэнергетики, промышленных объектах, автомобильных и железнодорожных тоннелях, метрополитене, в лесном хозяйстве.

Трагические события 2010 г. в Российской Федерации, когда горели леса почти по всей территории России, заставили начать внедрение в лесных массивах систем видеонаблюдения. Министерство лесного хозяйства Республики Беларусь второй год осуществляет программу оснащения лесов Беларуси системами видеонаблюдения. Среди аналогичных систем можно назвать систему «Лесной дозор» (Российская Федерация), автоматическую систему обнаружения ландшафтных пожаров и экологического мониторинга «GoldenEye» (Латвия), а также две отечественные наземные системы обнаружения лесных пожаров, разработанные в НИИ ядерной физики и НИИ ПФП Белгосуниверситета соответственно.

В настоящее время за рубежом все большую актуальность получают видеодетекторы дыма, интегрированные в системы сетевого видеонаблюдения. Они применяются в системах пожарной безопасности дорожных, железнодорожных и эксплуатационных тоннелей. Установка подобной системы производства компании D-Tec в дорожном туннеле гавани Сиднея являет собой пример возможностей по обеспечению оперативного обнаружения потенциального источника возгорания. В рассматриваемом примере система видеонаблюдения с видеодетектором дыма была подключена к 40 телекамерам, установленным в тоннеле, что позволило гарантировать раннее обнаружение дыма. В тоннеле была организована серия контролируемых возгораний автомобилей, чтобы проверить, как вытяжная система справится с удалением дыма, а также протестировать на практике способности точечных извещателей пожарной сигнализации и системы пожаротушения.

На этих испытаниях, когда горели реальные автомобили, температура в тоннеле превышала 500° С. Система видеонаблюдения с видеодетекто-

Блок-схема видео-теплового аппаратно-программного комплекса обнаружения пожара



Продолжение см. стр. 14

Использование изображений, полученных системами видеонаблюдения, при проведении криминалистических экспертиз

Артюшин Алексей Альбертович, начальник 5-го управления ГЭКЦ МВД Республики Беларусь

Экспертно-криминалистическими подразделениями МВД Республики Беларусь осуществляется экспертная идентификация личности людей по зафиксированным объективным материальным отображениям признаков внешности, а также исследуются изображения иных объектов с целью их идентификации.

Сравнительные методы исследования

Специфика экспертной портретной идентификации личности, в частности относительно высокая субъективность в оценке признаков внешности, обуславливает большое количество методов сравнительного исследования, применяемых для идентификации личности.

Все традиционные методы сравнительного исследования можно подразделить на три группы:

- методы сопоставления;
- методы совмещения;
- методы наложения.

В первую группу методов входят:

- визуальное (простое) сопоставление с последующей разметкой признаков;

методы совмещения

Начало см. стр. 13

ром дыма сделала запись, а первый сигнал тревоги она подала уже через 14 секунд после того как появились первые видимые признаки дыма, до возникновения видимого пламени. В течение всего времени испытаний система подала 30 сигналов тревоги. При этом во время испытаний ни одна из обычных систем пожарной сигнализации не заметила возгорание в тоннеле.

В настоящее время специалистами НИИПФП им. А.Н. Севченко БГУ совместно с НИИ ПБиЧС МЧС РБ в рамках выполнения задания Государственной программы научных исследований «Научное обеспечение безопасности и защиты от чрезвычайных ситуаций» на 2011-2015 гг. запланирована разработка макетного образца аппаратно-программного комплекса для дистанционного обнаружения и мониторинга пожаров со стационарных объектов и подвижных носителей. Основанием для разработки послужило изучение опыта Западной Европы и Российской Федерации.

В результате будет создан макетный образец автоматической системы дистанционного обнаружения и мониторинга пожаров в реальном времени со стационарных пунктов и подвижных носителей, а также методика измерений, обнаружения и мониторинга пожаров с использованием созданной системы. Система позволит обеспечить высокое качество данных дистанционных измерений, в реальном времени обрабатывать данные, вести мониторинг пожара, прогнозировать его развитие, что приведет к снижению затрат при обнаружении и ликвидации пожаров, минимизации наносимого ущерба.

Макетный образец системы пройдет полигонные испытания, будет разработан регламент ее применения. Предполагается выполнение системы на современном научно-техническом уровне, что позволит повысить качество и оперативность принимаемых решений по ликвидации обнаруженных пожаров, а также решать задачи мониторинга объектов и территорий в интересах МЧС РБ, Минлесхоза, других министерств и ведомств. Основные планируемые технические характеристики:

- Определение малоразмерного пожара сразу же после его начала (несколько секунд).
- Вероятность правильного обнаружения пожара должна составлять не менее 98%.
- Система должна пройти испытания и аттестацию в НИИ ПБ МЧС РБ. ■

визуальное (простое) сопоставление с последующей разметкой признаков

сопоставление с использованием «масок»

сопоставление биологической асимметрии

сопоставление с помощью аппликаций (композиций)

- сопоставление с использованием «масок»;
- сопоставление с помощью наложения координатных сеток;
- сопоставление относительных величин;
- сопоставление биологической асимметрии;
- сопоставление с помощью аппликаций (композиций).

Ко второй группе методов сравнения (методам совмещения) относятся:

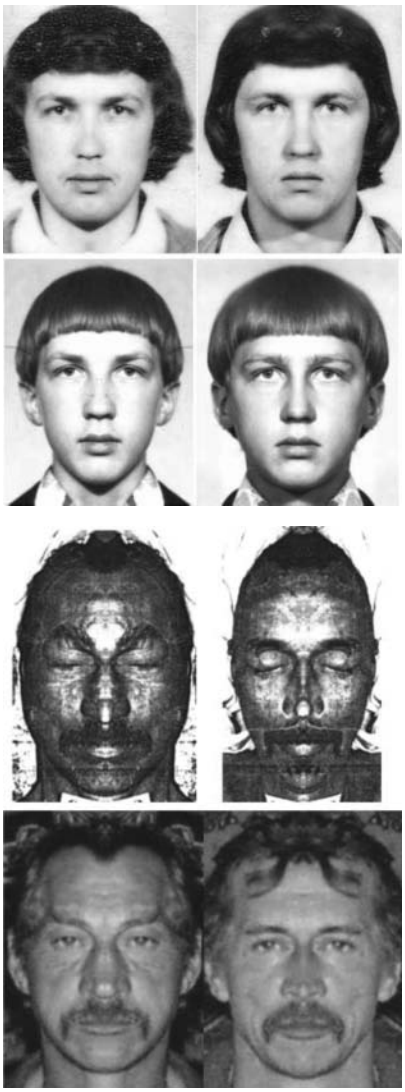
- совмещение изображений по прямым линиям;
- совмещение по ломаной линии, т.е. монтаж одного изображения с частью другого.

В ходе применения методов совмещения оценивается цельность, естественность полученного изображения, т.е. являются ли элементы одного лица продолжением элементов другого.

Третью группу традиционных методов сравнительного исследования составляют методы наложения изображений, подразделяющиеся на:

- наложение путем сложения (накладываются друг на друга либо позитивные, либо негативные изображения и, при совпадении, усиливается контраст одноименных элементов ввиду сложения плотностей, а различающиеся признаки выглядят неотчетливо);
- наложение путем вычитания (когда позитивное изображение накладывается на негативное. При этом, совпадающие элементы «вычтут» друг друга и дадут нейтральный серый фон, а различия выглядят ярким светлым ореолом вокруг них).

Кроме указанных традиционных методов сравнительного исследования могут применяться и другие. Например, проективно-геометрические,



наложение путем сложения

основанные на выявлении на изображениях лиц, так называемых, константных точек или точек-ориентиров, которые затем должны использоваться для различных геометрических построений (метод АГИ — алгоритм графический идентификационный, предложенный Р.Э. Эльбуром; аналитический метод — Н.С. Полевой; метод угловых измерений — Н.В. Зависист).

Однако специально проведенные эксперименты показали, что объекты, предлагаемые в качестве константных точек, таковыми не являются, поскольку из-за возрастных изменений внешнего облика человека, а также вследствие известной подвижности элементов лица, на которых они находятся, обладают значительной по величине областью расположения. В связи с этим определение точного места их расположения практически невозможно и поэтому не исключено повторение их системы на изображении другого лица. В связи с этим проективно-геометрические методы

не нашли широкого применения в судебно-портретной экспертизе.

Для оценки результатов сравнительного исследования может быть применен вероятностно-статистический метод. Однако последний также имеет ряд ограничений (в настоящее время применяется только для мужчин, европеоидного антропологического типа).

вероятностно-статистический метод

Выбор методов исследования признаков внешности на изображениях обусловлен в каждом конкретном случае качеством отображения признаков и возможностями самого метода. Решение об использовании того или иного метода при проведении портретного исследования остается за экспертом.

В то же время, существуют общие ограничения, обуславливающие возможность экспертной портретной идентификации личности, для которой необходимо качественное изображение идентифицируемых и идентифицирующих объектов, сопоставимые ракурс и условия освещения.

Качество видеоинформации

Использование правоохранительными органами видеоинформации для экспертной идентификации личности выявило ряд проблем, связанных в первую очередь, с качеством исследуемых экспертами-криминалистами видеоматериалов.

Качество видеоинформации определяется, в свою очередь, техническими свойствами систем видеонаблюдения и тактикой их применения. Очень часто полученное системами видеонаблюдения и направляемое для проведения экспертизы портретной идентификации изображение оказывается непригодным для идентификации зафиксированных на видеозаписях людей, т.к. не отображает в необходимой мере их анатомические особенности внешности.

Информация о недостатках систем видеонаблюдения и о требованиях к видеоизображению для проведения экспертно-криминалистическими подразделениями экспертиз портретной идентификации личности, а также осуществления поисковых операций с использованием АСПИ, была опубликована в выпуске журнала «Технологии безопасности» №2 за 2010 год.

В последнее время к нам часто обращаются для решения вопроса, изображен ли на представленном фрагменте видеозаписи камеры наружного наблюдения тот или иной человек, имеется ли изображение автомобиля определенной модели, его регистрационного номера и т.д. Но здесь наши возможности не безграничны, мы напрямую зависим от качества предоставляемого материала. Если на интересующий нас объект на изображении приходится 2-3 пикселя, то в этом случае ни о какой идентификации речь вести невозможно.

Идеология построения систем видеонаблюдения в некоторых случаях направлена на получение обзорной съемки местности, какого-то участка местности, она не ориентирована на получение качественного изображения людей, которых потом потребуется идентифицировать. Существуют некоторые объекты, на которых обязательно должны стоять камеры видеонаблюдения и средства, которые ориентированы именно на получение изображений человека, его портрета для последующей идентификации. В первую очередь это банки, банкоматы, заправочные станции и другие объекты, на которых происходит расчет платежными средствами, и в свою очередь именно там имеют место случаи мошенничества, манипуляции с различными платежными картами, в том числе и поддельными.

На наш взгляд, в тех системах видеонаблюдения, в которых есть большая вероятность возникновения задач идентификации человека или иных объектов, совершенно необходимо устанавливать камеры видеонаблюдения с перспективой решения именно таких задач. Большое значение имеет не просто установка достаточно качественных видеокамер, но их грамотная эксплуатация. Примером может служить расследование мошенничества при расчетах на АЗС. На экспертизу предоставили видеозапись с камеры наружного наблюдения, изъятую при выемке и видеозапись, полученную при проведении следственного эксперимента участием подозреваемого. Использована одна и та же видеокамера, условия съемки близкие. Но на съемке, осуществленной в день преступления, номер автомобиля не виден, а на видеосъемке следственного эксперимента почему-то номер виден достаточно хорошо. Тут влияние, вероятно, оказала скорость видеозаписи, режимы, в которых работало это оборудование. На таких объектах целесообразно применять те режимы видеозаписи, такую аппаратуру, чтобы можно было рассмотреть конкретный номер автомобиля. По делу о взрыве в Минском метро многие доводы защиты строятся на том, что на изображениях видеокамер метрополитена нельзя категорично сказать, что на них изображены именно Коновалов и Ковалев. При проектировании систем видеонаблюдения должны целенаправленно выбираться точки съемки с последующей перспективой идентификации личности. ■

Практическое применение систем безопасности на инфраструктурных объектах

Христофоров Андрей, директор по корпоративным продажам компании ITV|AxxonSoft

Я очень часто сталкиваюсь с тем, что различные системы безопасности — пожарная, охранная сигнализация, система контроля доступа, видеонаблюдение — никак между собой не связаны. Иногда некоторые части системы дублируют друг друга, создавая избыточность инфраструктуры безопасности и увеличивая ее стоимость. Если удается объединить в рамках одной информационной инфраструктуры данные от различных систем безопасности, то комплекс этих систем становится «информационно прозрачным», что позволяет находить лучшие решения, более эффективные компромиссы. Чтобы обеспечить эту «информационную прозрачность» мы и начали разработку платформы «Интеллект» как инструмента для создания больших комплексных систем безопасности. Системы безопасности, которые я буду приводить в качестве примера, основаны именно на этой платформе.

Безопасный город

Так называемая система «Безопасный город» — одна из самых непонятных и сложных структур. Я сталкивался в Интернете с информацией, что вокруг одного дома устанавливается 10 камер и утверждается, что построена система «Безопасный город» . Так происходит потому, что понятие «Безопасный город» документально не зафиксировано. То, что построено в различных городах, может включать следующие компоненты:

- интеллектуальная транспортная система;
- система управления нарядами и средствами (милиция);
- система управления городским транспортом;
- подсистема видеонаблюдения жилого фонда;
- подсистема видеонаблюдения местами массового скопления людей ;
- подсистема интеллектуальной обработки информации;
- система голосовой экстренной связи;
- системы обеспечения эксплуатации жилого фонда;
- геоинформационная система;
- система контроля работоспособности.

Как управлять всей этой информацией и строить всю эту систему? Наш опыт показывает, что операторы, которые смотрят в мониторы 24 часа в сутки, неэффективны. Точнее, они эффективны в первые полчаса. Но в случаях, когда что-то действительно происходит, и мы думаем, что оператор должен это видеть и реагировать, на деле часто получается, что он не видит и не реагирует. Поэтому для создания большой и в то же время эффективной системы недостаточно вывести в центр мониторинга изображения с сотен камер и посадить операторов, которые будут за ними следить. Здесь необходимо правильно организовать алгоритм работы системы, в том числе с применением видеоаналитики. Как и где в больших системах может использоваться видеоаналитика, я сейчас расскажу.

Контроль дорожного движения

Контроль дорожного движения делится на две части — это некий «кнут» и «пряник». С одной стороны, это фискальная часть, фиксация правонарушений и выписка штрафов, а с другой стороны, это составляющие, улучшающие нашу жизнь — сбор информации о пробках и возможность оптимизации дорожного движения в рамках города. Например, на Северном Кавказе в городе Нальчик на основе «Интеллекта» реализована комплексная система, которая решает множество задач, начиная от фиксации правонарушений и заканчивая автоматическим управлением дорожным движением — сюда входит изменение режимов работы светофоров в зависимости от текущей дорожной ситуации, а также управление нарядами, силами и техническими средствами.

Видеоаналитика решает в рамках такой системы две основные задачи: распознавание номеров автомобилей для автоматической фиксации правонарушений и для целей розыска, а также сбор данных о дорожной ситуации для целей адаптивного регулирования дорожного движения. Хочу

отметить, что, помимо фиксации нарушений скоростного режима, нами уже создана система, определяющая проезд на запрещающий сигнал светофора.

Распознавание лиц

Технологии распознавания лиц сегодня очень требовательны к условиям, в частности, к ракурсу съемки. Фактически, в толпе они малоэффективны, поэтому при создании систем с применением этих технологий приходится придумывать различные ухищрения, чтобы привлечь внимание человека и заснять его лицо с оптимального ракурса. Эту задачу можно решать при помощи выбора правильного места установки камеры, например, в турникете метрополитена. Проходя через турникет и прикладывая карточку, человек, как правило, смотрит в одну точку — на датчик, к которому прикладывается карта. Благодаря этому вероятность захватить и распознать лицо существенно повышается. Можно повысить эффективность распознавания, увеличив количество рубежей контроля. Или просто с помощью административного ресурса.

Технологию распознавания лиц можно использовать и для работы с архивом. Для этого строятся и сохраняются векторные биометрические характеристики всех лиц, попавших в кадр, по которым впоследствии можно производить поиск похожих лиц. Это не отменяет распознавания в реальном времени: по данной характеристике можно попытаться сразу идентифицировать человека.

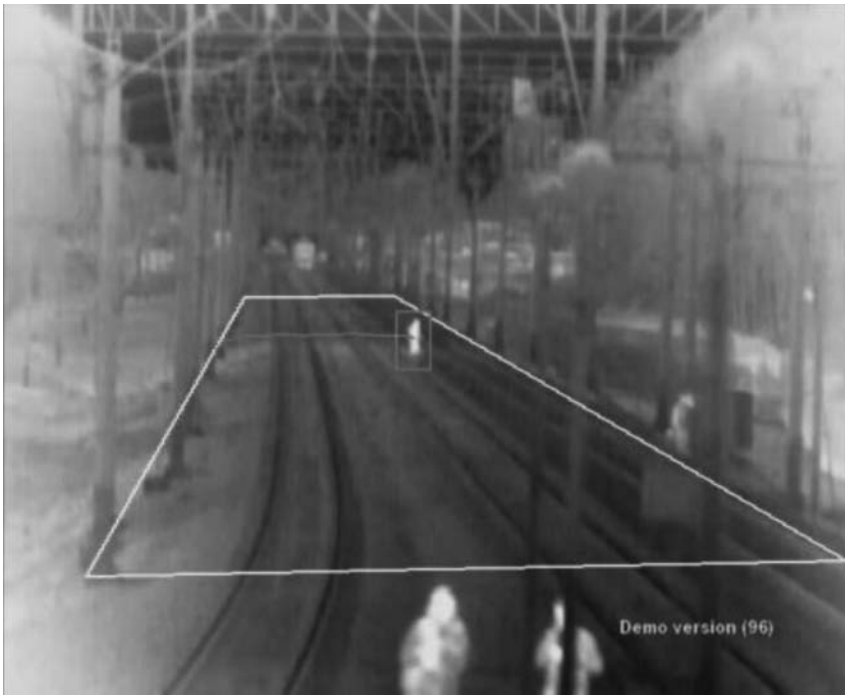
Как именно работает наша система? Предположим, что мы ищем какое-то определенное лицо — у нас есть фотография, фрагмент видеоархива или даже грамотно построенный фоторобот. И мы хотим понять, когда и где появлялось это лицо. Изображение передается в систему и запускается поиск. Результаты поиска выводятся оператору в виде списка лиц, похожих на заданное, по убыванию степени сходства. Затем оператор может выбрать одно из найденных лиц и повторить поиск уже по нему — и так до тех пор, пока не будет найдена фотография, которую можно отправить на распознавание и идентифицировать. Либо получить статистические данные: где и когда, с определенной долей вероятности, этот человек появлялся. Таким образом, мы создали инструмент, позволяющий существенно ускорить поиск интересующего нас лица в архиве.

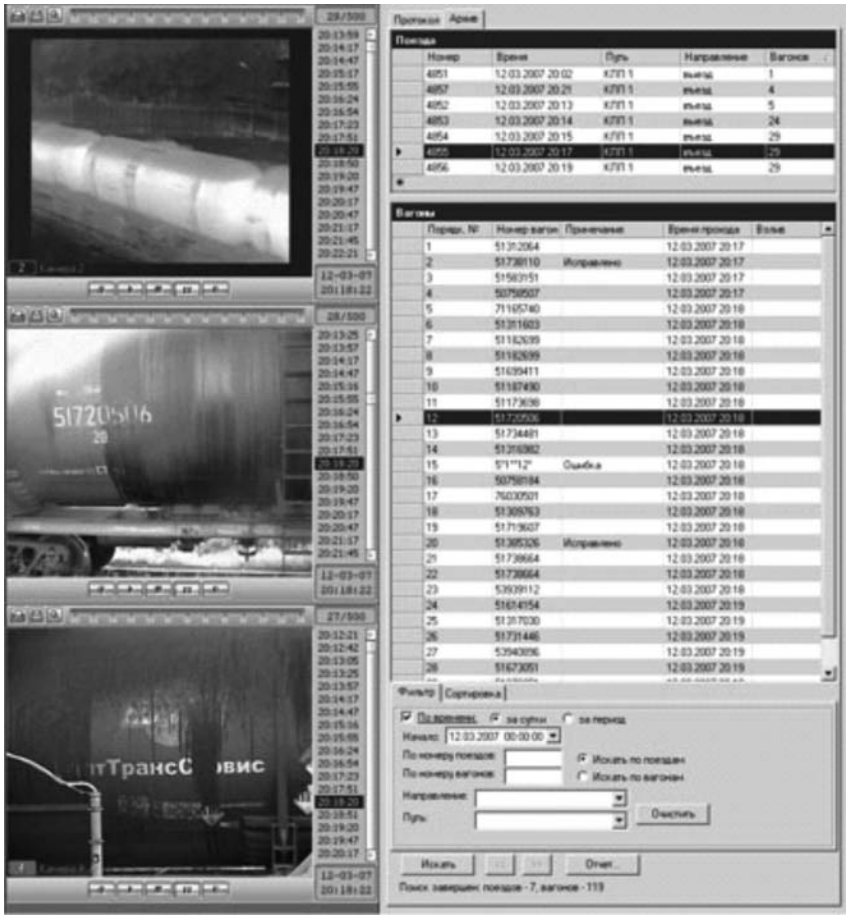
Он может быть полезен в системах класса «Безопасный город» при проведении оперативно-розыскных мероприятий.

Железная дорога

Довольно крупный и интересный с точки зрения технологий проект — это скоростная трасса Санкт-Петербург — Москва. На некоторых участках поезд идет со скоростью 200 км/ч. За время существования трассы уже погибло несколько человек. Вдоль путей построен забор, к тому же, существуют официальные переходы и переезды, однако людей это не останавливает. Для комплексного повышения безопасности системы было принято решение о строительстве системы видеонаблюдения. При этом ставилась задача не только записывать архив, чтобы потом разбираться, что именно произошло, а работать в реальном времени: зафиксировать на рельсах в данный момент посторонний объект, предпринять соответствующие действия, предотвратить катастрофу и гибель людей.

Как вы понимаете, скорость реакции здесь имеет огромное значение, кроме того, количество установленных вдоль путей камер велико. Поэтому было принято решение использовать видеоаналитику для помощи операторам и исключения пресловутого человеческого фактора. Она





привлекает внимание оператора, чтобы он не пропустил момент появления кого-то или чего-то на полотне. Нами была интегрирована сторонняя видеоаналитика, встроенная в тепловизоры Bosch и «Гардлайнер», которые применены в проекте. Эта видеоаналитика позволяет создавать «стерильную зону». Если в этой зоне появляется некий объект, запускается алгоритм, который выдает тревогу при определенных условиях. Например, если объект вошел в зону и вышел — реакции нет, а если задержался на какое-то время — выдается оповещение оператора.

Для вокзалов также актуальна детекция оставленных предметов. Сейчас мы используем детектор оставленных предметов нового поколения, который работает на базе трекинга. Еще одна технология, востребованная, в частности, для вокзалов , — это подсчет людей в очереди. Она была разработана для того, чтобы оценивать загруженность билетных касс и оптимизировать логику их работы. Но данная технология может применяться и для подсчета людей в толпе.

Наша разработка для железной дороги «ЖД-Интеллект» оказалась очень востребованной на нефтеперерабатывающих комбинатах. «ЖД-Интеллект» производит распознавание номеров вагонов и цистерн и подсчет вагонов в составе. Система адаптивная, интеллектуальная, самообучаемая. Если в течение недели обучать систему, исправляя возникающие ошибки, то она практически перестанет ошибаться. В системе используются 2 камеры и пара оптических датчиков. Датчики отмечают промежутки между вагонами, таким образом производя их подсчет. Камеры с двух сторон снимают номера вагонов для дальнейшего распознавания. Две камеры применяется для того, чтобы выбрать наилучшую гипотезу: часто бывает так, что с одной стороны номер плохо читается, например, залит нефтепродуктами, а с другой — чистый и читается хорошо. Таким образом, применение пары камер может существенно повысить качество распознавания. Еще одна камера, тепловизионная, используется для определения так называемого уровня взлива жидкости в цистернах. Любая цистерна, даже если она долго простояла на холоде, все равно имеет градиент температуры, по которому и определяется уровень взлива. И еще один элемент, интегрированный в нашу систему, — это железнодорожные весы.

Вся информация может передаваться в «1С:Бухгалтерию», экспортироваться в натурные листы. По данным, поступающим с объектов, внедрение системы «ЖД-Интеллект» позволило в несколько раз уменьшить время формирования состава.

Time Compressor

Технология Time Compressor в данный момент находится на завершающей стадии разработки. Она позволяет быстро просмотреть все события за выбранный период времени, при этом ускоренное воспроизведение не применяется. Скорость просмотра достигается за счет того, что на экран выводится одновременно несколько движущихся объектов, которые попадали в кадр на протяжении выбранного периода в разные моменты времени. При этом алгоритм работает так, что объекты не перекрывают друг друга надолго и на экране одновременно отображается не более заданного количества объектов. Time Compressor позволяет быстро найти интересующий нас объект и, кликнув по нему мышкой, перейти в обычный режим просмотра видеозаписи непосредственно к интересующему нас моменту.

Time Compressor будет эффективен там, где за длительный период времени появлялось не очень большое количество объектов. В этом случае при обычном просмотре архива нам может потребоваться несколько часов, чтобы найти момент появления интересующего нас объекта, тогда как в режиме Time Compressor объект может появиться уже через несколько минут.

Заключение

Многие заказчики и даже инсталляторы не до конца понимают, на что способна видеоаналитика. Кто-то ждет от нее чудес, кто-то, может быть, однажды разочаровавшись, считает, что видеоаналитика хорошо работает только на выставочных стендах. Конечно же, и то и другое не верно. Но только грамотная постановка задачи и понимание того, что мы хотим получить, позволяет существенно повысить эффективность системы видеонаблюдения при помощи видеоаналитики.

ООО «АкссонСофт»
220100, г. Минск, ул. Куйбышева, 40, офис 3.
Тел.: (017) 292-66-11, 292-66-99
E-mail: minsk@axxonsoft.com
Сайт: www.axxonsoft.by

Видеоаналитика компании «Синезис»

Хилькевич Сергей,
технический директор
компании «Синезис»

Справка ТБ

Хилькевич Сергей. Образавание, 1991-1996 гг. — Военная академия Республики Беларусь; с 2005 г. — Технический директор SYNESIS.

– Что такое видеоаналитика компании «Синезис», какие задачи она позволяет решать?

– Видеоаналитика (ВА) — очень широкое понятие, включающее в себя обнаружение, сопровождение объектов, распознавание штатных/нештатных ситуаций и прочее.

Мы специализируемся на обнаружении и сопровождении объектов в условиях динамически изменяющегося фона (деревья, кусты, водная поверхность и т.п.). Это является базисом, на основании которого мы реализовали Rules (Правила) и Tempering Detectors (Сервисные детекторы). На данный момент у нас реализованы два правила — TripWare (Сигнальная Линия) и Field Region (Зона Интереса), а также шесть сервисных детекторов — Camera Redirected (Камера смещена) , Camera Obstructed (Обзор ограничен), ImageTooDark (Изображение затемнено), ImageTooBlure (Изображение расфокусировано), ImageTooBright (Изображение засвечено), ImageTooNoisy (Изображение зашумлено). Умелая комбинация Правил и Сервисных Детекторов позволяет решать очень широкий спектр прикладных задач. Например, пересечение границы, движение в зоне, подсчет людей, оставленный предмет, праздношатание, остановка на месте дольше определенного времени, бег выше определенной скорости, движение в заданном направлении.

– В реализации каких сценариев вы наиболее сильны?

– В обнаружении объектов на сложном меняющемся фоне, в сопровождении и распознавании ситуаций. Это подтверждено сертификатом i-LIDS (Imagery library for intelligent detection systems) лаборатории в научном подразделении МВД Великобритании, которая занимается тестированием технических средств обнаружения и сертифицирует оборудование для государственных проектов. Сертификат i-LIDS является общепризнанным стандартом качества видеоаналитики в отрасли. Встроенная видеоаналитика SYNESIS одобрена i-LIDS как система первичного обнаружения для формирования оперативных тревог и для записи событий в приложениях видеонаблюдения стерильной зоны.

– Существуют ли у вас разработки по работе с большим скоплением людей?

– До последнего времени это не было нашим приоритетом. Видеоаналитика для большого скопления людей сильно отличается от наших предшествующих разработок, как с точки зрения подходов анализа, так и с точки зрения необходимой производительности аппаратного обеспечения. В этом году мы начали заниматься данным направлением и разработали модуль видеоаналитики для подсчета людей и измерения параметров очереди. Модуль определяет количество людей, прошедших в заданном направлении, с точностью до 95%. При установке в местах массового скопления людей модуль определяет количество субъектов в каждый момент времени, а также время нахождения каждого человека в поле зрения камеры.

Основное отличие данной разработки от предшествующих состоит в том, что новые алгоритмы оптимизированы для анализа видео с фиксированных купольных камер, установленных на потолке. В алгоритмах используется детектор голов, который позволяет выделять людей (пассажиров, покупателей) в плотной очереди или потоке. Детектор голов также повышает точность работы видеоаналитики при появлении теней от бокового освещения. Кроме того, модуль может быть использован как детектор толпы, срабатывающий при превышении порогового количества людей.

Как происходит обработка информации в дальнейшем?

– Наша компания разработала и выпускает двухканальный видеосервер MagicBox со встроенной видеоаналитикой. Результаты работы видеоаналитики поступают на СВН по протоколу ONVIF. Приняв результат работы видеоаналитики, СВН обеспечивает оперативную реакцию, а также сохраняет результаты в архив, что поможет в дальнейшем вести интеллектуальный поиск.

– В чем преимущества компоновки ВА на конечном устройстве?

– Следует отметить, что сегодня обработка видеопотока на большинстве СВН происходит в серверной части (т.н. серверная видеоаналитика), что довольно накладно с точки зрения загрузки трафика. Одна из тенденций развития видеоаналитики — все больший «уход» на конечное устройство. Камеры и видеосерверы делаются достаточно интеллектуальными, способными работать как в режиме управления извне, так и в автономном режиме. Это происходит, несмотря на мощность современных серверных платформ, ведь все равно существует их конечная мощность.

Кроме того, задача СВН — это все-таки не видеоаналитика, а удобство использования этих систем. Раньше анализ видеопотока существовал только на стороне сервера, была постоянная связь, непрерывный прием потока. Сейчас в принципе, когда видеоаналитика уходит на устройства, нет необходимости постоянно принимать весь поток от устройства. Вы можете принимать информацию выборочно, опираясь на метадан-

ные, которые вы получаете от самого устройства. В результате происходит снижение объема трафика в каналах связи. Аналитика будет работать только по заданному каналу и по вашим настройкам.

– Какова схема и возможности работы сервера с метаданными?

– Во-первых, сервер, опираясь на метаданные, может обеспечивать оперативную реакцию. Т.е. нужное изображение будет автоматически вам предоставлено на основании метаданных от устройства. Во-вторых, с помощью метаданных можно индексировать архив, который ведет СВН, а затем очень удобно осуществлять поиск.

Как это может выглядеть? Существует поток метаданных, архив проиндексирован, вы можете просто задать условия поиска: «меня интересуют люди в желтых майках, которые пересекали обозначенную линию такого-то числа, в какой-то промежуток времени». При использовании данного метода (т.н. интеллектуальной разметки) поиск будет осуществлен очень оперативно. Если же этого нет, придется проигрывать весь архив. Вот почему сейчас многие компании и пользователи стали поворачиваться лицом к ВА возможностям. Еще 3 года назад не было полного понимания возможностей работы с архивом, сейчас все сценарии ВА «созрели». Медленно, но верно они идут к коммерческому использованию.

– Какая программная среда используется для анализа метаданных?

– На сегодняшний день это продукт «Интеллект» компании ITV. Если речь идет о базовой функциональности, то поддерживается любая VMS-система, которая поддерживает открытый стандарт ONVIF. Говоря о поддержке стандарта ONVIF, я бы подчеркнул, что почти все производители поддерживают его больше для «галочки». Стандарт еще довольно молодой, находится в доработке, кроме того, не все сценарии использования покрывались. Только с выходом версии 2.2, ONVIF стал приемлемым для использования в коммерческих системах; сейчас он позволяет решать практически любые задачи, которые можно решить с помощью СВН.

– Ваша компания активно работает с тепловизорами. Какова специфика работы с такими устройствами?

– Тепловизоры являются сейчас популярной темой. Для нас работать с информацией от тепловизора даже проще, т.к. если мы говорим об обычном оптическом диапазоне, то в нем существует масса факторов, влияющих на работу аналитики: тени, отражения и пр. Качество аналитики определяется тем, насколько адекватно можно фильтровать все эти факторы. Тяжело работать с информацией от обычных камер ночью, когда идет засветка фарами и в оптическом диапазоне картинка разваливается. Однако такие факторы не влияют на работу видеоаналитики в тепловом диапазоне.

Мы специально создали одноканальную версию нашего видеосервера. Реализуем его в виде плат, которые производители телевизоров вставляют и подключают в свое устройство — получается цифровой тепловизор с аналитикой в одном корпусе.

– Какова дальность работы ВА в тепловизорах?

– Зависит только от качества тепловизора, от качества картинки, которую мы получаем. В худшем случаи — это 100-200 метров, в лучшем — 800-900 метров.

– Каковы ваши возможности настройки (написания дополнительных функций) продукта по ВА под специфику объекта?

– Мы выполняем работы по настройке продукта под специфику использования на объектах. Например, ВА на железной дороге не должна реагировать на проходящие поезда, пограничный комитет, это классический случай сценария стерильная зона . Там ничего менять не надо. Конечно, под каждую отрасль делаются доработки, возможности для этого есть.

– Каковы основные современные тенденции и тренды на рынке аналитики?

– Во-первых, специализация. Это значит, что будет востребована аналитика, решающая конкретные отраслевые задачи (торговые центры, железная дорога и т.д.).

Во-вторых, многокамерная видеоналитика. Это и многокамерное слежение, и стереоскопическое зрение, и многокамерная панорамная сшивка, мультисенсорная видеоналитика (совместное использование телевизионных и тепловизионных каналов).

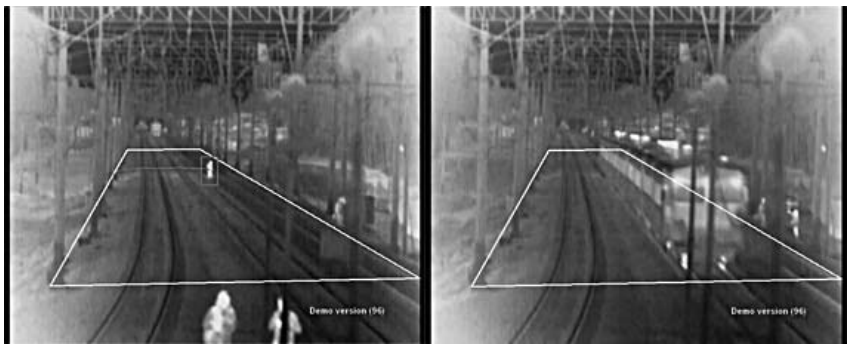
В-третьих, работа с архивом метаданных.

В-четвертых, распределенная видеоаналитика, когда часть задач будет решаться на конечных устройствах, а часть на серверах.

А также стандартизация (ONVIF 2.2).

– Назовите мировых лидеров в ВА?

– Всех тяжело назвать. Например, английская компания VCA Technology, Bosch. ■



Справка

Справка: ONVIF (Open Network Video Interface Forum). Отраслевой стандарт ONVIF определяет протоколы взаимодействия таких устройств, как IP-камеры, энкодеры, видеорегистраторы и системы управления видео. На начало 2010 года число компаний-участников форума ONVIF превысило отметку 100. Стандарт определяет следующие аспекты взаимодействия IP-камеры с системами управления или видеозаписи (DVR): конфигурирование сетевого интерфейса; обнаружение устройств по протоколу WS-Discovery; управление профилями работы камеры; настройка поточной передачи медиа-данных; обработка событий; управление приводом PTZ; видеоаналитика; защита (управление доступом, шифрование). Важным преимуществом стандарта ONVIF является хорошая поддержка видеоаналитики, встраиваемой в конечные IP-устройства, например, камеры и энкодеры.

ООО «Синезис»
220043, г. Минск, пр-т Независимости, дом 95, пом. 12, офис 316
Тел./факс: (017) 281-77-85, 281-77-91
E-mail: s@synesis.ru
Сайт: www.synesis.ru

УНП: 190950894

PELCO
by Schneider Electric

Системы видеонаблюдения для спортивных и других объектов с массовым пребыванием людей на базе оборудования Pelco by Schneider Electric

В современных условиях системам безопасности на объектах с массовым пребыванием людей уделяется особое внимание. Трудно переоценить роль грамотно и профессионально построенной системы видеонаблюдения на подобных объектах.

Такую систему можно с уверенностью назвать «глазами», а при использовании соответствующего мощного программно-аппаратного комплекса видеоаналитики, обработки и хранения информации — даже «сердцем и мозгом» общей системы безопасности объекта (контроля доступа, пожарной и охранной сигнализации, оповещения и т.д.)

Применение систем видеонаблюдения Pelco by Schneider Electric на различных спортивных объектах

Компания Pelco by Schneider Electric является одним из мировых лидеров, производителей логически законченных, монобрендовых, неограниченных по масштабу систем видеонаблюдения. Системы и компоненты виденаблюдения Pelco by Schneider Electric открыты для интеграции с системами виденаблюдения всех основных производителей такого оборудования.

Перечень объектов спортивного назначения, оборудованных системами видеонаблюдения, включает в себя футбольные стадионы, хоккейные арены, бейсбольные залы, олимпийские объекты, многофункциональные объекты, гоночные трассы которые расположены в разных странах мира.

Гордостью нашей страны является многофункциональный культурно-спортивный комплекс (МКСК) «Минск-арена». Это масштабный спортивный комплекс, включающий в себя универсальный зал-арену, велодром, конькобежный стадион, единый паркинг, объекты обслуживания посетителей, конференц-залы и т.д.

Система видеонаблюдения МКСК «Минск-арена» построена на оборудовании Pelco by Schneider Electric и состоит из более 800 камер, объединенных на базе ip-платформы Endura.

Основные функции системы видеонаблюдения на спортивных объектах

Система видеонаблюдения спортивного сооружения призвана выполнять две основные функции: контроль и документирование поведения болельщиков во время спортивных мероприятий и круглосуточная охрана зданий и сооружений объекта. Помимо самого здания с многочисленными рекреациями и спортивной арены, подконтрольными являются также прилегающая территория и автостоянка. Специфика спортивных сооружений — размеры и значительное число зон контроля — требует особого подхода к выбору оборудования и созданию системы видеонаблюдения.

Система должна отвечать нескольким важным принципам:

- использование видеокамер высокого разрешения, т.к. принципиально получение не только «общей картинки», но и детального изображения, позволяющего получать качественные фотографии болельщиков, в том числе и из архива:

• обеспечение «живого» онлайн-видео без задержек. Динамические спортивные игры требуют высокой степени реакции службы безопасности. При чрезвычайном происшествии, охрана должна реагировать незамедлительно;

• обработка больших потоков видеоданных, что предусмотрено требованием к высокому разрешению видеоизображения;

• защита оборудования от вандализма;

• возможность системы строить большие операторские комнаты с большим числом рабочих мест для операторов, видеостенами и т.п.

Endura

С учетом вышеизложенных требований и особенностей наиболее оптимальным видится использование ip-платформы Endura производства Pelco by Schneider Electric (США).

Система базируется на сетевом протоколе TCP/IP, является распределенной, с отсутствием выделенных серверов или иных критических узлов, с возможностью создания неограниченного числа постов наблюдения и центров хранения, с возможностью построения иерархической системы доступа и управления.

Endura не имеет ограничений ни по числу камер, ни по количеству создаваемых постов видеонаблюдения, ни по территориально-географическому распределению компонентов.

Система гибкая, мобильная, легко расширяемая и модифицируемая, децентрализованная, открытая и интегрируемая с другими инженерными системами объекта.

Ip-платформа Endura предназначена для создания системы видеонаблюдения на основе сетевых протоколов и ОС Linux, что обеспечивает универсальность и широкие функциональные возможности в сочетании с высоким быстродействием, максимальной надежностью и безопасностью.

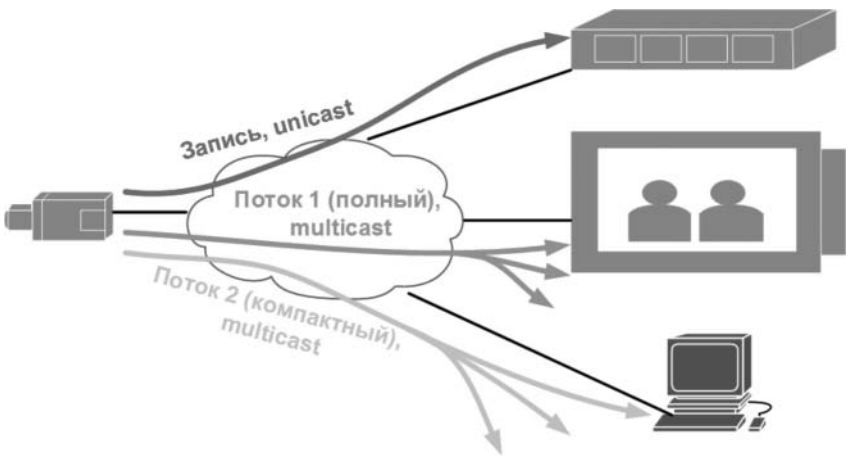
Описание применяемых видеокамер

Из продуктовой линейки Pelco можно подобрать камеру практически под любую задачу. В линейке есть аналоговые и ip-камеры, стандартного разрешения и мегапиксельные, фиксированные и PTZ, стандартного, купольного, антивандального исполнения и т.п.

В качестве PTZ ip-камеры предлагается использовать скоростной поворотный ip-купол Spectra IV IP. Spectra является самой продаваемой в мире купольной камерой. На сегодня продано более 1 млн. куполов в более чем 160 странах мира. Бескомпромиссными плюсами этой модели являются широкий модельный ряд, включающий исполнение из нержавеющей стали, антивандальное исполнение, модель с наполнением инертным газом, создающим избыточное давление, а также большой выбор опций — кронштейнов, узлов крепления, встроенных конверторов, блоков питания и т.п.

В доступных модификациях поставляется оптика с оптическим зумом 23, 27 или 35 крат. Температура эксплуатации от -51°C до +60 °C, класс защиты IP67. Оптика камер Spectra прекрасно решает задачи оптического увеличения. Но зачастую требуется получать панорамное изображение более высокого разрешения. Например, для выделения на фоне общей картинки противоположной трибуны окна с цифровым увеличением (так называемые «зоны интересов»). В этом случае правильнее использовать новинку — камеру Spectra HD — новую купольную PTZ ip-камеру с разрешением 1 МПк и 18-кратным трансфокатором.

Для контроля трибун можно использовать специальное исполнение Spectra Horizont. В отличие от классической Spectra эта камера позволяет смотреть выше уровня горизонта (на 18 градусов). Это полезная возможность, если требуется, например, наблюдать за противоположной трибуной, а камера установлена не на самой высокой точке.



Там, где требуется защита от вандализма (а это, например, все подтрибунное пространство арены), имеет смысл использовать камеры антивандального исполнения или защищать камеры специальными кожухами.

В качестве небольших антивандальных камер Pelco предлагает серию IM-V. Это миникупол диаметром 3 дюйма с корпусом, выполненным из металла, и поликорбанатным пластиковым колпаком, с разрешением до 1.3 МПк, компрессией H.264 и минимальной чувствительностью 0,03 лк.

Для защиты камер в классическом исполнении в линейке Pelco присутствует широкая гамма антивандальных, уличных и специальных кожухов.

При необходимости использовать вандалозащищенную поворотную камеру мы рекомендуем камеру Spectra в вандалозащищенном исполнении. Эта модификация имеет усиленный корпус и специальную решетку, защищающую плафон.

Многоадресная передача сигнала

Ip-камеры и аппаратные ip-кодеры Pelco имеют возможность передачи видеоинформации на несколько (неограниченное число) адресов одновременно, поддерживая мультикаст сетевые протоколы адресации. Мультикаст — это возможность сетевых устройств одновременно передавать данные от одного источника на неограниченное число приемников. Это очень важно для возможности видеть и писать видеосигнал сразу на нескольких постах. И при этом не допускать увеличения нагрузки на сеть. В противном случае будет невозможно одновременно смотреть один видеосигнал с нескольких рабочих мест, или же сеть быстро заполнится ненужным трафиком.

Хранение информации в системе Endura

Endura обеспечивает эффективное хранение видеозаписи и ведение видеозаписи в режиме реального времени на несколько серверов одновременно. Регистраторы могут располагаться в любом месте, при условии обеспечения требуемой пропускной способности сетевой инфраструктуры.

Производительность одного сетевого регистратора NSM5200 (способность одновременно обрабатывать видеопотоки с различных источников видеоинформации) составляет 250 Мбит/с, что эквивалентно потоку от более чем 125 ip-камер с разрешением 4CIF и 25 кадрами в секунду.

Для эффективного заполнения дисков и обеспечения отказоустойчивости си-

стемы записи есть возможность балансировки загрузки серверов хранения данных с целью равномерного заполнения. В случае отказа одного из устройств хранения система автоматически переключит записываемые видеопотоки на другое устройство записи.

Запатентованная технология EnduraStor оптимизирует систему хранения данных, значительно увеличивая продолжительность записи при минимизации расходов на хранение. Например, при необходимости можно вести круглосуточную запись со всех камер 25 кадров в секунду с последующим автоматическим прореживанием через 7 дней до 6 кадров в секунду, тем самым освобождая значительные дисковые пространства.

Регистраторы NSM5200 имеют 12 встроенных дисковых накопителей RAID 6 общей емкостью до 36 ТБ на регистратор, с возможностью объединения до 20 регистраторов в пул.

Регистраторы имеют резервные источники питания, резервные вентиляторы для надлежащего охлаждения, дисковый массив RAID6, обеспечивающий сохранение записанной видеоинформации даже при одновременном отказе двух дисков. NSM5200 использует платформу на основе ОС Linux, что обеспечивает максимальную надежность и безопасность. В случае выхода из строя регистратора камеры автоматически должны распределяться между другими регистраторами.

Организация рабочих мест пользователей

Рабочие места пользователей получают видеоинформацию от IP-камер и аппаратных ip-кодеков напрямую, минуя устройства регистрации. Ограничений по количеству или по разнесению рабочих мест нет. В системе может быть неограниченное число устройств видеовывода.

В качестве устройств для создания постов видеонаблюдения и рабочих мест используется:

WS5070 — аппаратное рабочее место на базе Windows 7 с возможностью подключения до 2 мониторов, с функциями администрирования системы;

WS5200 — программное обеспечение, аналогичное WS5070, для установки на компьютеры третьих производителей;

VCD5202 — виртуальная матрица, специальное решение для оператора без функций администрирования, под Linux и с клавиатурой с джойстиком для управления PTZ-устройств;

NET5402HD — декодер на 2 монитора, способный декодировать до 32 видепотоков, используется для расширения рабочего пространства оператора (добавление оператору мониторов) или для создания видеостен.

Дополнительно существует программный модуль WS5200-MAP, позволяющий отображать планы контролируемого объекта с нанесенными условными обозначениями камер и других устройств. Условный знак на плане позволяет по нажатию выполнять действия по управлению камерами, видеовыводу и т.п.

В зависимости от конкретных задач формируются посты видеонаблюдения, оснащенные по необходимости средствами коллективного доступа к видеоинформации. Для оперативного управления ситуацией и эффективного принятия решения в центре видеомониторинга стадиона, как правило, формируется единое пространство с установкой широкоформатных мониторов в видеостену. Вывод видеоданных на мониторы видеостены осуществляется оператором или автоматически. Видеопотоки выводятся на мониторы/видеостену напрямую с ip-камер или ip-кодеров, видеорегистраторы для видеовывода не задействуются. Просмотр видео из архива осуществляется с видеорегистраторов по запросу в соответствии с правами доступа.

Надежность системы видеонаблюдения

Для обеспечения отказоустойчивости системы существует механизм мониторинга состояния элементов системы, а также возможность подключения резервного оборудования, работающего в горячем резерве. Переход на резервное оборудование может осуществляться автоматически. Механизм ручной «горячей» замены осуществляется как на уровне регистраторов, так и на уровне дисков. В критически важных устройствах предусмотрено дублирование по питанию путем использования дублирующих блоков питания.

Endura поддерживает протокол UPnP. Все события отказов и сбоев оборудования, а также события, связанные с изменением настроек оборудования, такие как отказ видеокамеры, несанкционированное изменение зоны обзора видеокамеры, полное или частичное перекрытие зоны обзора видеокамеры посторонними предметами, все действия персонала регистрируются.

Благодаря применению СВН от Pelco by Schneider Electric на многофункциональном объекте заказчик получает стабильно работающую систему прекрасно зарекомендовавшую себя на многочисленных объектах по всему миру. ■

ЗАО «БЕЛНЭТЭКСПЕРТ»
220036, г. Минск, ул. Волоха, 1, ком. 407
Тел./факс: (017) 286-20-03, 286-20-04
E-mail: info@netexpert.by
Сайт: www.netexpert.by

Новая линейка IP-камер от EverFocus

При построении системы видеонаблюдения на многофункциональных объектах одним из важных критериев выбора конечного решения является высокое разрешение используемых камер. Применение мегапиксельных IP-камер в данном случае необходимо рассматривать неразрывно с гибким, полнофункциональным программным обеспечением, которое позволило бы оператору оперативно и с легкостью обеспечить детализацию того или иного объекта.

Евдокимов Сергей Александрович, аккаунт-менеджер компании EverFocus Electronics Corp.

Компания EverFocus рада представить вашему вниманию новую линейку IP-камер, которые совместно с программным обеспечением PowerFocus позволяют обеспечить безопасность объектов различной сложности!

В линейке новых IP-камер представлены четыре модели стационарных камер (EAN2150, EAN2350, EAN2218, EDN2245), а также две модели поворотных камер (EPN2218, EPN2218i).

EAN2150

Отличительной особенностью данной модели является использование высокочувствительной ПЗС-матрицы — 1/3" Sony Progressive CCD, которая обеспечивает стабильную работу камеры при минимальном освещении. Цвет: 0.03 Люкс @ F=1.2; Ч/Б: 0.001 Люкс / F=1.2. Для удобства настройки в камере есть композитный выход (BNC-разъем) для подключения сервисного монитора. Запись с камеры может осуществляться также локально, для этого в EAN2150 предусмотрен слот для Micro SD-карты. Максимальное разрешение изображения — 1280x960 (1.3Mpx).

EAN2350

Если есть необходимость в высокой детализации изображения, то камера EAN2350 является идеальным выбором. Максимальное разрешение — 2048x1536 (3Mpx). Несмотря на то, что в основе модели лежит КМОП-матрица — 1/2.7" Progressive CMOS, камера имеет достаточно высокие показатели чувствительности. Форматы сжатия MJPEG и H.264 дают пользователю возможность параллельно использовать их для различных целей, например, MJPEG — для записи, H.264 — для трансляции по сети. Встроенная функция детектора движения является удобной опцией и при совместном использовании с тревожными выходами камеры обеспечивает интеграцию IP-камеры с уже существующей охранной системой.

EAN2218

Одной из наиболее интересных моделей является камера EAN2218. Наличие встроенного трансфокатора (18X оптический зум, f= 4.7~84.6мм) предоставляет возможность использовать данную камеру для решения различных задач: охрана периметра, чтение номеров автомобилей и т.д. Максимальное разрешение — 1920 x 1080 (2Mpx).

EDN2245

Для уличного применения хорошим решением является купольная IP-камера с ИК-подсветкой 30 м — EDN2245. В данной модели есть встроенный варифокальный объектив

(f=3~9мм), минимальная освещенность составляет: Цвет: 0.2Люкс @ F=1.4; Ч/Б: 0.02Люкс / F=1.4. Класс Защиты IP66 и встроенный обогреватель обеспечивают возможность инсталляции камеры в различных погодных условиях. Максимальное разрешение — 1920 x 1080 (2Mpx).

EPN2218/EPN2218i

В линейке моделей IP камер представлены 2 поворотные камеры (наружное и внутреннее исполнение). К основным параметрам данной серии можно отнести: максимальное разрешение 1920 x 1080 (2Mpx), 18x оптический и 8x цифровой зум, поддержка двунаправленного аудио, цифровое понижение шума, детектор движения и т.д.

PowerFocus

PowerFocus for Network Video Recording

Бесплатная версия данного программного обеспечения (ПО) дает возможность организовать полноценный центр управления 64-мя IP-камерами, с возможностью создания локального архива. Разнообразные режимы отображения видео, создание виртуальной стены, дружественный интерфейс пользователя — все это позволяет спроектировать гибкую IP-систему среднего масштаба! Если же требования к системе более жесткие, то, приобретая дополнительную лицензию, можно расширить функционал ПО — версия клиент-сервер с функцией видеоаналитики. Счетчик людей, детектор оставленных вещей, детектор чужих предметов, детекция направления движения — это только некоторые возможности видеоаналитики EverFocus.

Более подробную информацию о новой продукции EverFocus вы можете получить у официальных дилеров компании EverFocus в Республике Беларусь.

Everfocus Electronics Corp.12F, No.72, Sec.1, Shin-Tai Wu Rd, Taipei, Taiwan
Тел.: +375 29 355 66 45
E-mail: sergey@everfocus.com.tw
Сайт: www.everfocus.by

Официальный дилер
СООО «САТУРН-ИНФО»
220015, г. Минск, ул. Пономаренко, 35а, офис 616
Тел./факс: (017) 251-62-06; 256-25-23
(029) 656-17-50, (029) 756-17-18
E-mail:saturn@saturn-info.com
Сайт: www.saturn-info.com

УНП: 100063951

Системы видеонаблюдения высокого разрешения. Опыт использования на спортивных объектах

Владимир Пеганов, директор компании «Легион безопасности», официального дистрибутора MOBOTIX AG в Республике Беларусь

Одна из лучших и современных систем видеонаблюдения на спортивных объектах установлена в Донецке на стадионе «Донбасс Арена», торжественное открытие которого состоялось 29 августа 2009 года. «Донбасс Арена» — первый стадион в восточной Европе, удовлетворяющий требованиям комитета УЕФА к стадионам категории Elite. В 2012 году здесь пройдут важные игры чемпионата Европы по футболу, в том числе полуфинал. Новый домашний стадион донецкого футбольного клуба «Шахтер», завоевавшего кубок УЕФА в 2009 году, вмещает более 51 000 тысячи зрителей.

Великолепное оснащение и безопасность

В здании стадиона расположено три ресторана, четыре бара, зона отдыха, фитнес-центр, кафе для болельщиков Fan-Café, музей ФК «Шахтер», магазин и 53 стенда быстрого питания. Этот стадион подходит не только для спортивных мероприятий, но и для организации концертов и различных шоу. При проведении массовых мероприятий основное внимание уделяется обеспечению безопасности. Чтобы занять все 51 504 места на стадионе, зрителям понадобится около часа, однако экстренная эвакуация заполненного стадиона занимает всего 8 минут. «Мы хотим, чтобы зрители чувствовали себя комфортно и в полной безопасности. Поэтому мы используем самую современную систему видеонаблюдения», — подчеркнул директор стадиона Александр Атаманенко. Впечатляет количество камер, обслуживающих стадион, что неудивительно, принимая во внимание масштабы строения: 528 камер MOBOTIX и 18 PTZ-камер Bosch полностью контролируют все помещения стадиона и прилегающую территорию. На стадионе установлено 4 территориально разнесенных сетевых хранилища (NAS) емкостью 210 Tb, которые соединены между собой по Fiber Channel. Массивы емкостью 210 Тб записывают все камеры на протяжении одного месяца.

В опасных зонах — безопасность без компромиссов. Высокое разрешение решает все...

Система видеонаблюдения, обеспечивающая безопасность стадиона «Донбасс Арена», выполняет четко определенные задачи. Во-первых, это распознавание людей на входе, выходе и на территории стадиона. Во-вторых, наблюдение за потоками зрителей и их направлением в критических точках — на входах и выходах, у входов на трибуны и в парк, где было высажено более 281 дерева и 35 000 кустов роз. Камеры установлены и в других важных зонах — в ресторанах, на автостоянках и в магазине для болельщиков. «Мы выбрали камеры MOBOTIX из-за целого ряда достоинств, — поясняет начальник службы безопасности «Донбасс Арены» Сергей Бургела. — Прежде всего — качество изображения. Вот смотрите: увеличив изображение потенциального нарушителя, получаем снимок с детальным изображением его лица. Теперь можно отправить этот снимок в полицию для опознания». Таким образом, камеры используются для профилактики беспорядков, позволяя службе охраны выпроводить «возмутителей спокойствия» с территории стадиона еще до начала игры. И даже если нежелательные события все-таки произошли, благодаря системе видеонаблюдения можно установить личности нарушителей порядка и тем самым оказать неоценимую услугу полиции.

... и низкие расходы

В отличие от традиционных камер с низким разрешением, камеры высокого разрешения, оснащенные 3,1 мегапиксельными датчиками, не только позволяют получать четкое изображение, но и вести видеонаблюдение на большей площади меньшим числом камер. «Предложение MOBOTIX включало меньшее число камер, чем решения других производителей», — отмечает С. Бургела. Кроме того, системы MOBOTIX

позволяют использовать уже имеющуюся информационную инфраструктуру. Все 528 камер получают электропитание через PoE-коммутаторы и объединены в крупнейшую сеть Украины, насчитывающую более 6000 портов.

Устойчивость к погодным воздействиям и ночная съемка

Работа под открытым небом и в ночное время выдвигает жесткие требования к системе видеонаблюдения. В данном случае устойчивость к погодным воздействиям и отсутствие механических компонентов — дополнительные аргументы в пользу камер MOBOTIX. Данные камеры не нуждаются в обогреве или охлаждении, а значит, и в обслуживании. Камеры имеют два отдельных датчика высокого разрешения — цветной для дневной съемки и высокочувствительный черно-белый для ночной съемки, и позволяют получать четкое изображение круглые сутки. Уникальная техника DualNight надежно работает без механического переключения и обеспечивает высокую светочувствительность. По ночам стадион «Донбасс Арена» ярко освещен и сияет, как алмаз. В таких условиях нужны датчики изображений с коррекцией контрового света — именно такие используются в камерах MOBOTIX.

Децентрализованная запись и простота монтажа

«Самым убедительным доводом для меня стала концепция децентрализации», — говорит Евгений Коноваленко, старший технический специалист службы безопасности. Обработка изображения и управление событиями происходят в самой камере. Это не только значительно разгружает компьютерную сеть, но и позволяет одновременно проводить прямую трансляцию, запись и поиск событий. «На четыре рабочих

места производится передача живых изображений на 42-дюймовые мониторы, кроме того, два 19-дюймовых монитора используются для поиска в архиве», — сообщает Коноваленко.

Встроенное ПО

«На каждом рабочем месте установлена программа MxControlCenter, которая имеет очень удобный интерфейс, понятный для персонала службы безопасности», — поясняет старший технический специалист. Важная особенность: программное обеспечение MOBOTIX прилагается к камерам бесплатно, обновления можно загрузить в Интернете. Это профессиональное ПО для управления системами видеонаблюдения на основе IP-камер поддерживает децентрализованную архитектуру и позволяет сократить число серверов в десять раз. Поэтому для записи мегапиксельных видеоклипов высокого разрешения, транслируемых со 100 камер, понадобилось всего три сервера. «Это еще один важный аргумент в пользу системы MOBOTIX», — отмечает С. Бургела. Поэтому решение MOBOTIX как нельзя лучше подходит для оснащения крупных сооружений, например стадионов: оно экономичнее и требует меньших трудовых затрат. Для обслуживания обычной системы видеонаблюдения, включающей 100 камер высокого разрешения без встроенной «логики», требуется 20 серверов.

MOBOTIX. Сделано в Германии: новаторская техника и снижение расходов

С момента основания в 1999 году немецкое акционерное общество MOBOTIX AG утвердилось не только как кузница технологий в области сетевых камер. Концепция децентрализации сделала практическое использование видеосистем высокого разрешения экономически выгодным.

Высокая точность изображения означает снижение числа камер

Благодаря применению датчиков высокого разрешения с 1536 строками одной камеры оказывается достаточно для полного охвата помещения. **Минимальные затраты на установку независимо от удаленности камеры** Подключение к компьютерной сети позволяет использовать недорогие сетевые компоненты для передачи информации по медным и волоконно-оптическим кабелям или беспроводной связи.

Современная технология сохранения данных снижает число накопителей

Благодаря децентрализованной архитектуре систем MOBOTIX записывающее устройство способно обслужить в 10 раз больше камер.

Управление по событиям снижает затраты на хранение данных

Автоматическое изменение настроек изображения (кадровой частоты, размера) при регистрации движения, шума или получении сигналов позволяет сократить потребность в ширине пропускного канала и в объеме запоминающего устройства.

Низкое энергопотребление, отсутствие необходимости в дополнительных системах обогрева

Защита от запотевания без подогрева позволяет подавать электропитание через сетевой или двухжильный кабель независимо от времени года (стандарт PoE), а также отказаться от использования кабеля питания.

Сокращение расходов на резервное питание до 80%

Малая потребляемая мощность (4 Вт) круглогодично (подогрев не требуется) позволяет организовать централизованное бесперебойное питание через сетевой кабель.

Прочность и отсутствие техобслуживания

Армированный стекловолокном прочный корпус со скрытым кабельным вводом и отсутствие механических деталей (нет автодиафрагмы) обеспечивают долгий срок службы.

В комплекте — ПО для управления произвольным количеством камер и запоминающих устройств

Для каждой задачи — свое ПО: MxEasy — для небольших систем видеонаблюдения, MxControlCenter — для профессиональных систем безопасности.

Произвольное расширение системы и защита инвестиций

Камеры и накопители можно добавлять в систему в процессе эксплуатации. Формат изображения, частота кадра и параметры записи настраиваются индивидуально для каждой камеры.

Встроенные дополнительные функции

В комплект включены: звуковое оборудование, объектив, крепление для установки на стену и погодозащитный корпус (от -30 °С до +60 °С). Большинство моделей имеет встроенный микрофон и динамик.

Таким образом, системы видеонаблюдения на крупном спортивном объекте призваны решать сложные технические задачи. Благодаря полученному опыту эксплуатации на такого рода объектах мы можем с уверенностью утверждать: оборудование MOBOTIX благодаря своим инновационным свойствам полностью справляется со своей работой и является очень удачным решением, позволяющим выполнять сложные и ответственные операции.

ООО «Легион безопасности»
220118, г. Минск,
ул. Машиностроителей, 29-117, офис 7
Тел./факс: (017) 340-42-17
E-mail: info@mobotix.by
Сайты: www.mobotix.by

Мировой опыт компании HIKVISION в построении систем видеонаблюдения на многофункциональных объектах

Компания «АВАНТ-ТЕХНО» уже 3 года предлагает на рынке Республики Беларусь продукцию одного из крупнейших мировых производителей систем безопасности HIKVISION. За это время в нашей стране реализовано немало интересных проектов с применением оборудования HIKVISION. Высокое качество и великолепные технические характеристики продуктов позволяют выполнять сложнейшие проекты по всему миру. Компанией HIKVISION немало сделано и для безопасности спортивных объектов. Самые знаковые спортивные проекты — олимпийский стадион в Пекине и центральный футбольный стадион в Аргентине.

Один из самых интересных за последние годы — проект «безопасный город» в Шанхае (EXPO 2010). Следует особо поблагодарить компанию HIKVISION за любезно предоставленную информацию о данном проекте, т.к. не часто удается узнать детали проекта такого уровня. Особенно интересен данный проект уникальным сочетанием современных технологий видеонаблюдения — применены сверхчувствительные аналоговые видеокамеры, способные передавать качественное изображение в условиях тумана, также видеоустройства, работающие в формате HD CCTV и IP, — камеры разрешением до 5 МПк. Применение 3-х различных технологий детально обосновано для каждого конкретного случая в целях достижения максимального эффекта. К сожалению, у нас подобные решения встречаются нечасто — когда предлагается применить наряду с IP еще и аналог. Считается, что аналог — «устарело», во всем мире делают серьезные проекты «только на IP». Объясняется это простым недостатком профессионализма. Мы надеемся на данном примере показать положительный опыт построения гибридных систем, дающих более высокое качество, нежели применение только одной технологии.

ЭКСПО 2010

Официальное название — EXPO 2010 Shanhai China. Всемирная выставка, проходившая с 1 мая по 31 октября 2010 года в г. Шанхае. Тема данного мероприятия: «Лучше город — лучше жизнь». Выставка предлагала концептуальные решения

проблем, касающихся сокращения ресурсов, снижения уровня преступности и сохранения окружающей среды посредством моделирования городов будущего.

В выставке приняли участие 192 государства и 50 международных организаций. Было установлено три исторических рекорда — по численности посетителей и площади экспозиции, а также была установлена новая, более высокая планка по безопасности и культуре проведения последующих выставок.

Выставка занимала площадь 5.28 кв. км, и за время работы ее посетили 73 миллиона человек (более 500 000 в день). Для проведения такого масштабного мероприятия была проведена широкая модернизация городской инфраструктуры.

В соответствии с масштабом мероприятия для обеспечения безопасности была построена **самая крупная в мире городская видеосистема высокой четкости — 13 000 видеокамер**. Уникальность проекта не только в его размерах, но и в том, что полиция получила возможность осуществлять наблюдения и запись в формате FULL HD 1080 — в режиме реального времени (наблюдение 25 fps).

Техническое задание и предложенные решения

В предварительно разработанном техническом задании на систему было указано, что камеры должны предоставить возможность отслеживать и увеличивать изображение людей или транспортных средств для распознавания личности или номера автомобиля на всей территории выставки и в прилегающих районах. Получить четкие кадры с уже существующих систем наблюдения было довольно сложно, что затрудняло работу полицейских при уголовных расследованиях и анализе транспортных происшествий.

Предложенные для установки новейшие камеры HIKVISION с поддержкой Full HD1080 позволили повысить четкость изображения в 6 раз по сравнению с аналоговой камерой и передавать изображение в режиме реального времени со скоростью 25 к/с. Например, ранее на перекрестке требовалась установка трех или четырех камер для мониторинга транспортных потоков на несколько полос. Одна камера Full HD покрывает весь перекресток с лучшей детализацией изображения.

После детального изучения всей территории было определено техническое решение и разработан проект, в результате которого инсталлировано 13 002 камер. В том числе 965 аналоговых камер и 12 037 цифровых с разрешением Full HD1080 (11 526 фиксированных и 511 поворотных). Также были оборудованы:

– 42 полицейских участка;

– 6 окружных контрольных центров наблюдения;

– 1 главный контрольный пункт с центром хранения и обработки изображений.

Комплекс основывается на трех различных системах: аналоговых, цифровых HD SDI (HD CCTV), IP — системах.

Было применено 3 различных способа передачи сигнала.

Аналоговая подсистема

В системе установлено 965 аналоговых камер, 844 камеры использовано для наиболее важных перекрестков, 121 камера — для мониторинга дорожного трафика, остальные — для общего обзора с господствующих высот. Аналоговые камеры помогли эффективно проконтролировать места, выходящие непосредственно к реке и отличающиеся частыми плотными туманами, а также для общего мониторинга во время дождя или снега.

На стадии разработки проекта было определено, что на важных перекрестках камеры должны различать изображения транспортных средств и пешеходов

на расстоянии от 5 до 50 метров. Для мониторинга дорожного трафика камеры должны распознавать автомобили и велосипеды на расстоянии от 10 до 100 метров.

Для общего обзора с господствующих высот камеры также должны были иметь функцию наблюдения в тумане и специальную оптику для мониторинга транспортных средств и людских потоков на расстоянии до 10 КМ с последующим подробным увеличением.

Для обработки и записи видеосигналов в полицейских участках были использованы 8-канальные цифровые видеорегистраторы реального времени с архивом на 8 ТБ и встроенным видеосервером двойного кодирования в форматах H.264 и MJPEG

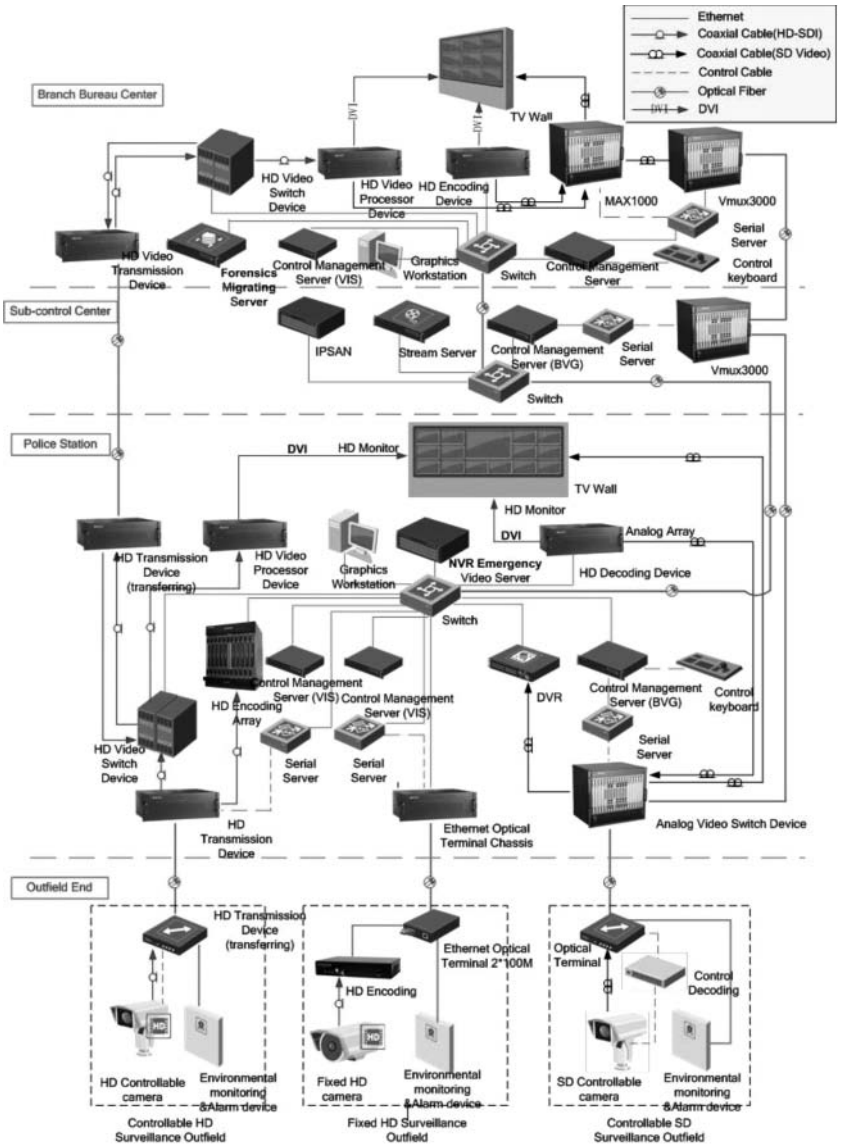
Описание подсистемы HD камер

Всего установлено 11 526 стационарных HD-камер, которые используются для наблюдения определенных сцен на расстоянии от 10 до 100 метров.

Также было установлено 511 HD управляемых камер, которые патрулируют в режиме реального времени, линии безопасности, запретные зоны и площади в пределах расстояний от 10 до 250 метров. Благодаря применению для данных целей видеокамер HD CCTV **удалось достигнуть предельно малой задержки команд управления (менее 250 миллисекунд)**, что позволило организовать более оперативное управление поворотными камерами.

Стационарные камеры передают сжатое цифровое Full HD1080 изображение с мест установки в центр наблюдения полицейского участка. Для наблюдения и локальной записи изображение отображается и записывается в реальном времени со скоростью — 25 fps в формате H.264, **параллельно все изображения передаются в окружной контрольный центр для записи и хранения в формате MJPEG со скоростью — 5 fps**.

Поворотные камеры передают не сжатое Full HD1080 изображение в формате HD SDI непосредственно в полицейские участки и в окружной контрольный центр. (Этот стандарт используется для передачи некомпрессированных и некодированных цифровых видеосигналов).



Общая структура системы

Система имеет четыре уровня:
1. Объектовое оборудование.
2. Полицейский участок.
3. Окружной контрольный центр.
4. Главный контрольный центр.

Применяется три вида видеосистем:
1. Аналоговое SD видео.
2. IP Full HD видео.
3. Незжатое HD SDI видео.

Две сети передачи данных:

1. 1 уровень — коаксиальный кабель или 1GB Network + оптическая система передачи данных.

2. 2 уровень — **впервые для систем безопасности была построена 10G IP Network**.

Для **главного контрольного центра также впервые были применены сервера хранения IP-SAN (ISCSI)** на 48 HDD, количество серверов — 696 шт.

Была разработана **единая интегрированная программная платформа** для всех уровней контроля, управления и хранения информации

Из-за большого масштаба видеосистемы было также применено ПО интеллектуальной видеоаналитики, что в значительной степени повысило эффективность контроля такого сложного объекта.

Учитывая престижность и актуальность мероприятия, данная система стала заметным проектом с одним из самых высоких уровней безопасности в Китае и по всему миру.

На международной выставке IFSEC 2011 (Германия) в номинации «Лучший проект в области безопасности 2010г.» проект системы видеонаблюдения для World Expo 2010 (Шанхай) был отмечен высшей наградой IFSEC и признан лучшим в мире проектом 2010 года.

ОДО «АВАНТ-ТЕХНО»
220004, г. Минск, ул. Короля , 45- 16в
Тел./факс: (017) 200-01-09, 226-43-52
E-mail: contact@avant.by
Сайт: www.avant.by

Использование тепловизоров в системах охранного наблюдения. Вопросы экономической эффективности

Дащинский Александр,
ОДО «Атомиум-Секьюрити»

Справка ТБ

Дащинский Александр Григорьевич — заместитель директора ОДО «Атомиум-Секьюрити». Образование высшее — инженер-радиотелемеханик. Опыт работы в сфере систем безопасности — 29 лет.

Расчет эффективности применения тепловизионных камер в системах охранного наблюдения на том или ином объекте производится при оценке критериев возможной угрозы или экономических потерь.

При правильном подходе к расчетам эффективности необходимо учитывать не начальную стоимость системы, а конечную, куда включены, например, расходы на электричество, обслуживание, простои и ремонт, а также некоторые другие эксплуатационные расходы.

Наиболее продуманная с точки зрения экономики и безопасности система сочетает в себе комплекс технических средств, каждое из которых технико-экономически подходит именно для своего участка.

В таком случае суммарный показатель эффективности вложенных в систему средств стремится к точке экстремума, в которой обеспечивается максимальное удовлетворение запросов Заказчика.

Одним из важных факторов при определении конечных затрат является расчет **стоимости потребляемой электроэнергии за период эксплуатации**. Простейший анализ расчетов конечных затрат условных участков охраны протяженностью 1 км (на одном установлена одна тепловизионная камера на поворотном устройстве, на другом — 10 видеокамер и освещение участка осуществляется лампами накаливания, на третьем — 10 видеокамер с ИК-прожекторами) с учетом только этого фактора показывает, что **конечные затраты системы охранного наблюдения на базе тепловизионных камер оказываются одинаковыми с системой охранного наблюдения, построенной на базе видеокамер с ИК-прожекторами, и в 1,4 раза дешевле системы охранного наблюдения, использующей лампы накаливания для освещения охраняемого участка**.

Немаловажную роль при построении системы охранного наблюдения играет и автоматизированное рабочее место (АРМ) оператора системы. На протяженных периметрах актуально применение только **интеллектуального наблюдения** (человек вообще не в состоянии одновременно наблюдать и оценивать более 10-12 изображений).

При сравнительной экономической оценке систем интеллектуального наблюдения на протяженных рубежах необходимо также учитывать, что большое количество изображений от видеокамер требует от системы передачи, обработки и регистрации видеоизображения (в т.ч. автоматического определения движущихся объектов) значительных ресурсов и, следовательно, **применения мощных и дорогих компьютерных сетей и высокопроизводительных серверов**.

Исходя из вышесказанного, в качестве примера произведем предварительные расчеты первоначальных и конечных затрат на оборудование условного периметра объекта (рис.1) протяженностью 4 км системами тепловизионного охранного наблюдения (вариант 1 — тепловизионные камеры, установленные фиксировано, вариант 2 — тепловизионные камеры на поворотных устройствах), а также системой видеонаблюдения с ИК-прожеторами (вариант 3).

Обобщенные результаты расчетов приведены в Таблице 1.

Из таблицы видно, что затраты на оснащение периметра тепловизионной системой охранного наблюдения по варианту 2 дешевле системы видео-

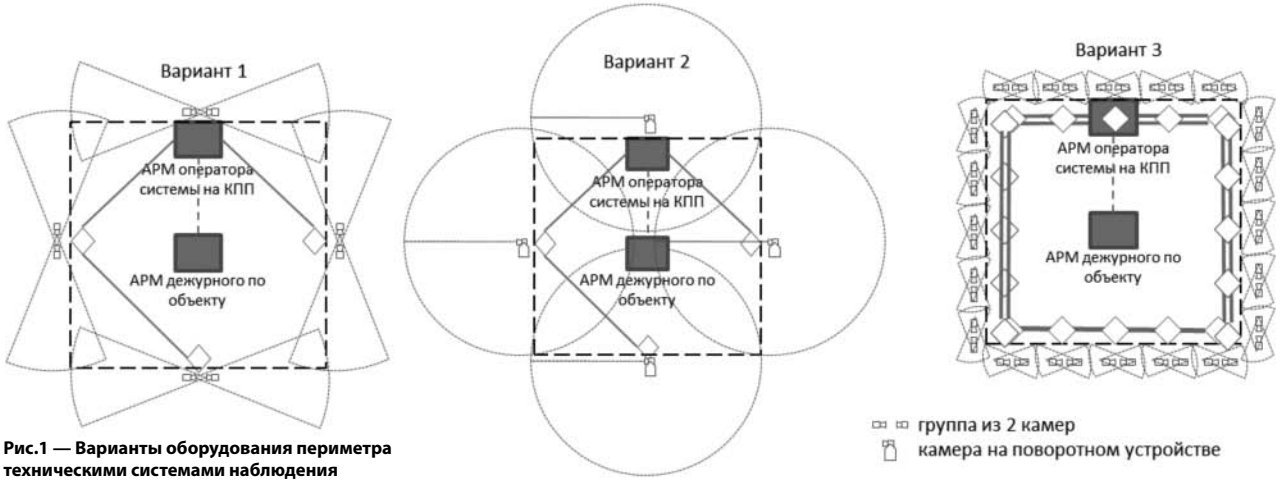


Рис.1 — Варианты оборудования периметра техническими системами наблюдения

Таблица 1. Расчеты затрат по вариантам 1-3

Наименование оборудования, работ	Затраты (по вариантам), у.е.					
	вариант 1		вариант 2		вариант 3	
	кол-во	стоимость	кол-во	стоимость	кол-во	стоимость
Тепловизионная камера КТН384/07-35	8 ед.	124 000	4 ед.	62 000		
Поворотное устройство			4 ед.	12 000		
IP-видеокамера					40 ед.	16 000
ИК-прожектор					40 ед.	8 000
Дополнительное оборудование и материалы	к-т	18 720	к-т	13 680	к-т	38 000
АРМ оператора	1 к-т	6 520	1 к-т	5 020	1 к-т	24 020
Итого (оборудование и материалы)		**149 240**		**92 700**		**86 020**
Монтаж камер, прожекторов и оборудования		2 400		1 200		14 000
Всего начальных затрат		**151 640**		**93 900**		**100 020**
Стоимость электроэнергии за срок службы (10 лет)		303		525		11 100
Стоимость замены расходных мате-риалов для ИК-прожекторов (10 лет)						24 000
Конечные затраты за 10 лет эксплуатации*		**151 943**		**94 425**		**135 120**

** без учета затрат на техническое обслуживание и замену расходных материалов системы*

наблюдения, кроме того, значительно меньшее (в 21 раз) энергопотребление, что существенно снижает конечные затраты Заказчика при эксплуатации системы. Преимуществом тепловизионной системы построенной по варианту 2, кроме дешевизны, является и то, что оператор может вручную управлять поворотом тепловизионных камер, повышая тем самым возможности системы в обнаружении объектов на подступах к охраняемому рубежу и сопровождению обнаруженных целей.

Конечный выигрыш тепловизионных систем наблюдения по сравнению с телевизионными на протяженных периметрах будет заметно ощутимее (чем больше протяженность, тем выше выигрыш).

Если же еще учесть эксплуатационные затраты Заказчика, такие как стоимость трудозатрат на техническое обслуживание, на привлечение квалификационного персонала и т.п. (на 4 единицы средства наблюдения они будут значительно меньше, чем на 40 единиц), то уже через 3-4 года эксплуатации **конечные затраты оснащения** объекта системой видеонаблюдения даже **на малых объектах превысят** конечные затраты оснащения системой тепловизионного наблюдения.

Не стоит забывать также и об аппаратурной **надежности системы** в целом, которая тем выше, чем меньше в системе составных частей, элементов.

В заключение напомним **наиболее значимые преимущества систем тепловизионного наблюдения**:

1. Видеокамеры (и приборы ночного видения) работают по принципу получения отраженного светового излучения. Т.е. сначала световые волны падают на объект, потом от него отражаются и попадают на матрицу камеры, которая показывает «контраст картинки», т.е. чем лучше освещенность, тем выше контраст (четкость) картинки. Если освещенности нет (ночью) или нет контраста (камуфляж, маскировка), то нет и изображения. Если есть препятствие для видимой части света (дым, туман), изображение отсутствует. В условиях большой дальности и слабой освещенности не хватает мощности отраженного светового излучения и, как следствие, тоже нет изображения.

2. Тепловизор работает на прием ИК излучения объектов, т.е. тепловизор — это прибор, который способен выдавать картинку, зависящую только от ИК (теплового) излучения объекта вне зависимости от освещенности. Тепловизор способен работать круглые сутки, и для его работы не требуется привлечение дополнительных средств, обеспечивающих его работоспособность (прожекторов).

3. Чем больше длина волны, тем ей легче огибать препятствия, в нашем случае — ИК лучам диапазона 3-14 мкм легче проникать через атмосферу, которая состоит из молекул газов. Тепловизор видит намного дальше видеокамеры (при одинаковых углах зрения). Тепловизор на открытой местности может обнаружить объект типа автомобиль, катер, самолет (вертолет) с работающим двигателем на значительно большем расстоянии, чем видеокамера с объективом с таким же фокусным расстоянием и светосилой.

4. Тепловизор менее чувствителен к шумам (например, от листвы, неоднородностей атмосферы и т.д.), следовательно, лучше подходит для автоматического обнаружения (да и обнаружения оператором) движения в интеллектуальных системах охраны, для чего будет достаточно сигнала от всего двух-трех пикселей на тепловой картинке.

Таким образом, **применение тепловизионных камер**, учитывая все преимущества тепловидения, по сравнению с традиционными камерами видеонаблюдения **может значительно повысить эффективность охраны и снизить конечную стоимость** системы охранного наблюдения на объектах Заказчика, особенно:

- вдоль неосвещенного протяженного периметра, где затруднительна установка подсветки из-за проблем с обеспечением большого энергопотребления;
- для точного определения активности возможных нарушителей вблизи охраняемых объектов днем и ночью;
- в условиях частых атмосферных осадков (дождь, снег, туман);
- в местах с проблемным освещением (недостаточное освещение или освещение мешает обзору);
- для наблюдения за открытыми пространствами, в т.ч. за водной поверхностью (солнечные и лунные блики, низкая контрастность объектов на фоне воды в видимом диапазоне);
- для наблюдения за участками местности с густой растительностью (высокая трава, кустарник и т.п.);
- для объектов большой площади или протяженных периметров, так как требуется значительно меньше тепловизионных камер. ■

ОДО «Атомиум-Секьюрити»
220053, г. Минск, Долгиновский тракт, д.39, оф. 244
Тел.: (017) 289-02-69, 233-60-99, (044) 780-41-25
Сайт: www.atomium.by

Пожарная автоматика компании Siemens на многофункциональных объектах

Галиев Юрий Талгатович, заместитель директора ООО «Эскорт», официального представителя компании Siemens

Данный материал подготовлен на основе доклада и презентации, которые были представлены на прошедшей конференции «Безопасность многофункциональных и спортивных объектов».

Компания Siemens AG предлагает очень широкий перечень услуг для многофункциональных и спортивных объектов, где системы пожарной автоматики являются составной частью.

Если говорить о пожарной автоматике на многофункциональных объектах, то она имеет свою специфику, как имеют свою специфику и объекты нефтехимического комплекса, крупные объекты торговли или гостиницы. Попробуем эти специфические требования сформулировать.

1. Многофункциональный объект сам по себе подразумевает БОЛЬШОЕ здание, а для большого здания необходима БОЛЬШАЯ и развитая система пожарной автоматики. Что это под собой подразумевает?

- Система должна быть адресной.
- Система должна взаимодействовать не только с пожарными извещателями и звуковыми оповещателями, но также уметь взаимодействовать и с входными сигналами (закрытие-открытие задвижек, окон или дверей; наличие-отсутствие уровней или давлений в системе пожарной автоматики и т.п.) и с выходными сигналами (открытие-закрытие задвижек и клапанов, включение насосов, и т.п.). Причем инициализация выходных сигналов, т.е. сигналов управления, основана на анализе состояния пожарных детекторов и входных сигналов от системы пожаротушения, дымоудаления и иных систем автоматики здания.
- Система должна иметь «распределенный интеллект». Панели распределены по объекту, дабы снизить количество проводных коммуникаций и повысить надежность, но при этом они должны строго взаимодействовать друг с другом. Например: одна панель стоит в насосной пожаротушения, другая отвечает за арену или торговый зал, третья — за подсобные помещения, четвертая — за автостоянку и т.д. Но при этом каждая из них может отрабатывать функции управления пожарной автоматикой как своей зоны, так и общесистемных функций. Допустим, при возгорании на складе (зона подсобных помещений), оборудованном системой пожаротушения, запустится насосная пожаротушения под управлением своей панели, а панель, отвечающая за торговый зал, откроет какую-то проходную задвижку и т.п.
- Система должна иметь верхний уровень, т.е. возможность построения АРМ на базе ПЭВМ, что обеспечивает визуализацию, оперативное управление элементами системы, взаимодействие с иными подсистемами и т.п.

Теперь понятно, что такое БОЛЬШАЯ система пожарной автоматики и какими чертами она должна обладать. Это «голова» системы. Настало время поговорить о «зрении» и «обонянии» системы.

2. Многофункциональные торговые и спортивные сооружения имеют в своем составе хотя бы одно огромное помещение (торговый зал, арену, и т.п.), следовательно, рассматривать возможность применения той или иной системы следует начинать (помимо указанного в пункте 1) с решения вопроса защиты этого самого крупного помещения. Это, как правило, требует еще одного и, пожалуй, самого важного свойства. Система должна иметь в своем ассортименте весь перечень необходимых типов извещателей, а не только точечных дымовых и тепловых. Сюда входят и извещатели пламени, и линейные дымовые извещатели, и аспирационные извещатели.

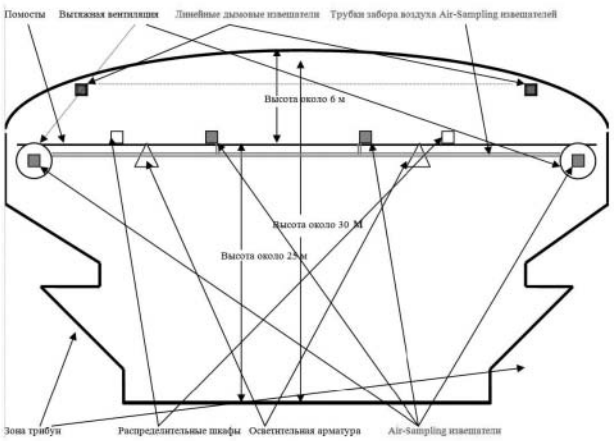
Чтобы не быть голословными, рассмотрим одну из типичных задач защиты больших помещений.

Как показывают исследования, в том числе выполняемые Siemens AG, дым распространяется по направлению снизу вверх до момента его остывания, что составляет около 12-18 метров. Затем дым остывает до температуры окружающего воздуха и равномерно смешивается с ним, при этом его концентрация опускается ниже пороговой для стандартных дымовых детекторов. Это свойство распространения дыма нашло свое отражение в нормативных документах РБ. В ТКП 45-2.02-190-2010 в п.п. 12.4-12.6 раздела 12 «Системы пожарной сигнализации» нормируется высота установки дымовых точечных и линейных извещателей, что составляет 10-12 м (Таблица 3) и 12-21 м (Таблица 4) соответственно.

Становится очевидным, что помещения с высотой более 21 м выходят за рамки действующих нормативов и требуют иного решения. Как быть в таких случаях?

Рассмотрим применяемые Siemens AG технические решения на примере Ледовой арены в Гамбурге. Ледовая арена в Гамбурге представляет собой здание размером 150*100*32 метра, размер площадки — 80*40 метров, размер ледяного поля — 60*30 метров, вместимость — 16000 человек.

Наибольший интерес представляют собой технические решения по пожарной автоматике непосредственно на арене, иные помещения (коридоры, служебные помещения и т.п.) оборудуются стандартно в соответствии с действующими нормами и правилами пожарной безопасности, действующими в стране.



Система пожарной сигнализации непосредственно арены состоит из трех типов защиты и основана на двух видах извещателей.

Первый вид — это линейные дымовые извещатели. Принцип действия основан на анализе интенсивности оптического луча между приемником и передатчиком, которые расположены друг от друга на расстоянии до 150 метров.

Другой вид детекторов — аспирационные системы. Принцип основан на применении детекторов дыма высокой чувствительности со свойством накопления значения параметра. Сам детектор с системой подпора воздуха устанавливается в доступном для обслуживания месте и соединяется с системой воздуховодов (пластиковые трубки диаметром около 30 мм с отверстиями), выведенных в необходимые зоны анализа дыма.

Возвращаемся к типам защит непосредственно арены.

Первая тип защиты — это аспирационные активные системы. Эти системы принудительно «прогоняют» воздух через воздуховоды, которые расположены на уровне помостов и распределены по всей арене на высоте около 25 метров. Предназначены для детектирования низких концентраций распределенного дыма непосредственно над ареной.

Второй тип защиты — линейные дымовые извещатели, установленные непосредственно около потолка арены. Данные извещатели анализируют наличие дыма, который возникает при пожаре в распределительных силовых шкафах и осветительной арматуре. Т.к. источник возможного возникновения дыма расположен приблизительно в 6 метрах от потолка, то это вполне нормативная ситуация в соответствии с ТКП 45-2.02-190-2010. Применение точечных извещателей в подобных помещениях в принципе недопустимо с точки зрения невозможности их дальнейшего обслуживания на таких высотах. Применение аспирационных и линейных дымовых извещателей позволяет разместить модули в зонах, доступных для обслуживания.

Третий тип защиты — это пассивные аспирационные системы, установленные в каналах вытяжной вентиляции. Пассивные аспирационные системы не «прокачивают» принудительно воздух через себя, а используют проток воздуха, обеспечиваемый самой вентиляцией. Этот тип защиты выявляет возникновение дыма в области трибун и в целом в помещении.

Следует отметить, что данный объект, а следовательно, и данные технические решения по пожарной сигнализации выходят за рамки, оговоренные нормативами. Поэтому технические решения по пожарной автоматике требуют согласования на стадии проектирования с Госпожнадзором МЧС РБ.

Мы отстаем в нормировании от развития техники. Считаю, что применение такого типа детекторов, как аспирационные, должно быть как-то нормировано соответствующими документами МЧС РБ. Здесь наблюдается полный нормативный вакуум. А объекты очень серьезные с точки зрения количества одновременно присутствующих на них людей.

Итак, мы определили специфику пожарной автоматики для многофункциональных объектов, а также требования к системе пожарной автоматики: как к «голове», так и к «зрению» и «обонянию». Теперь попытаемся поставленные задачи решить.

Начнем «снизу», т.е. с извещателей.

Для установки извещателей над ареной имеются активные аспирационные системы VESDA. В своем составе система имеет набор трубопроводов (по заказу), блок управления потоком воздуха (несколько типов, отличающихся по мощности и, следовательно, по защищаемой площади), непосредственно детектор дыма, обрабатывающее устройство (реализует различные алгоритмы самотестирования и анализирует состояние параметра во времени). Всасывающие трубки могут располагаться не только горизонтально, но и вертикально по любым строительным конструкциям и не требуют никакого обслуживания.

Также в номенклатуре Siemens AG имеются линейные дымовые извещатели типа DF. Извещатель состоит из приемно-передающего и отражающего модулей. Передающий элемент вырабатывает направленный световой сигнал на отражающий блок, установленный на расстоянии до 150 метров. Сигнал отражается от специального отражающего блока на приемный элемент, и по его интенсивности определяется наличие или отсутствие дыма в помещении.

Для установки в вентиляционные каналы предназначены детекторы серии FDBZ. Детектор состоит из пробоотборной камеры, устанавливаемой в вентканалы различных сечений, уплотнительных элементов и непосредственно детектора дыма.

В составе детекторов Siemens AG, помимо точечных тепловых, дымовых детекторов стандартного и взрывозащитного исполнения, имеются детекторы пламени, которые являются незаменимым средством для защиты помещений хранения ЛВЖ и помещений с опасностью утечки газа.

Как видим, арсенал детекторов достаточно богат, чтобы решить все специфические задачи многофункционального комплекса, и даже более.

Двигаясь снизу вверх, переходим к «голове», а именно к той ее части, которая называется «Приемно-контрольные приборы», куда и подключается весь этот арсенал детекторов.

Сегодня мы можем говорить о 2-х системах Siemens AG, пригодных для применения на многофункциональных и спортивных объектах с массовым пребыванием людей.

Это старая гвардия, уникальная в своем роде система AlgoRex и подрастающая молодь Cerberus Pro.

Итак, AlgoRex. Опыт применения на территории РБ — с 1999 года. Началось все с нефтехимического комплекса. Это 8 нефтеперекачивающих станций 2-х белорусских нефтепроводов «Дружба», Мозырский нефтеперерабатывающий завод, ЧПУП «Западтранснефтепродукт», объекты ОАО «Белоруснефть», включая Белорусский газоперерабатывающий завод и т.п. Далее объекты гражданского строительства: гостиница «МИНСК», гостиничный комплекс «ВИКТОРИЯ», 2 гипермаркета «ProStor», Дворец спорта, Офис «ТРАЙПЛ» (7 этажей) и т.п. Также объекты энергетического комплекса Мозырская ТЭЦ, Минская ТЭЦ 5.

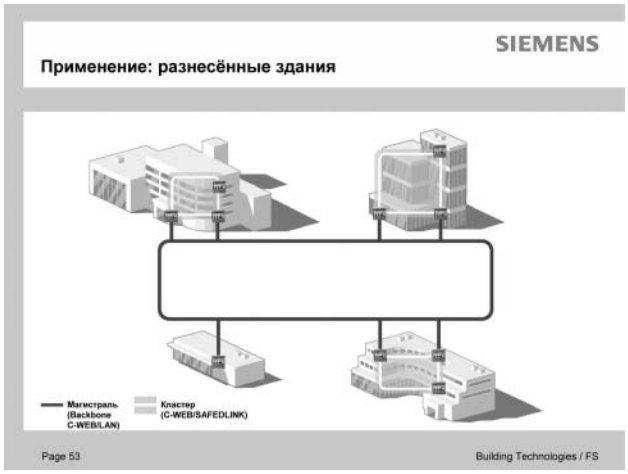
Этот перечень объектов приведен здесь для того, чтобы не утомлять вас сложными и достаточно сухими техническими описаниями, которые понятны и необходимы только узким специалистам. Перечень свидетельствует, что AlgoRex работает на крупных объектах и способен управлять сложными системами пожаротушения и дымоудаления. Теперь о самых крупных объектах.

Это Мозырский нефтеперерабатывающий завод. Система содержит 12 мощных пожарных станций СС1142, соединенных через оптоволоконные линии связи по протоколу CerLoop с АРМ-ом на верхнем уровне, реализованном на интегриро-

ванном программном пакете Siemens AG MM8000. Что такое нефтеперерабатывающий завод, количество зданий и сооружений на его территории и общая площадь объекта, думаю, представляют очень многие. И система AlgoRex решает все задачи.

ЛПДС «Мозырь» ОАО «Гомельтранснефть Дружба». Объект содержит 5 насосных нефтеперекачивающих станций, огромный резервуарный парк, 3 насосных пенного пожаротушения. Система состоит из 15 станций СС1142 и разбита на 4 подсистемы, объединенные через оптоволоконные линии связи по протоколу CerLoop с АРМ-ом на верхнем уровне, реализованном на интегрированном программном пакете Siemens AG MM8000.

Вторая система, представляемая Siemens AG в РБ, — это Cerberus Pro. Данная система впитала в себя все самые лучшие черты от AlgoRex, но выполнена на более современном технологическом уровне и имеет более развитые коммуникационные возможности. Из чего и вытекает, что при создании Cerberus Pro акцент сделан не на большие и мощные пожарные станции, а на более легкие и мобильные. Это позволяет еще более распределить интеллект системы, сделать ее более гибкой и снизить затраты инвестора. Одна из коммуникационных характеристик системы — это возможность использовать любые провода и кабели при инсталляции системы, даже старые, оставшиеся от ранее существовавших систем. Cerberus Pro анализирует параметры кабеля и определяет максимально допустимые скорости передачи данных, маршрутизирует потоки информации. Высокие коммуникационные характеристики Cerberus Pro позволяют создать единую систему пожарной автоматики не для одного крупного здания, а для комплекса зданий, либо размещенных в непосредственной близости друг от друга, либо находящихся в разных концах города, но принадлежащих одному собственнику. РИС 3.



И на самом верхнем уровне мы видим интегрированную систему MM8000, которая объединяет в себя все подсистемы безопасности, включая системы пожарной сигнализации, оповещения, охранной сигнализации, видеонаблюдения, контроля и управления доступом и обеспечивает взаимодействие с другими системами автоматизации здания, такими как управление лифтами, вентиляцией, энергетикой, пожаротушением, аварийным открытием дверей на путях эвакуации и т.п. Система состоит из мощного высоконадежного программного пакета MM8000, OPC сервера MK8000, дающего возможность интеграции в единое целое систем от других производителей, и Ehternet портов NK82xx. Помимо стандартных функций визуализации, управления подсистемами, обеспечения взаимных связей подсистем, ведения журналов событий в системе MM8000 сделан акцент на учет психологических особенностей человека. Интерфейс системы создан так, что оператор действует без напряжения, практически интуитивно. Особое внимание уделено обработке оператором тревожных ситуаций. Ведь «тревоги» случаются довольно редко, и даже опытный оператор испытывает стресс, что может повлиять на принятие решения: замедлить процесс или привести к принятию неверного решения. Алгоритмически MM8000 построен таким образом, что, учитывая психологические особенности человека, предлагает оператору варианты решений, визуально акцентирует его внимание на самых неотложных задачах и т.п., подталкивая оператора на максимально быстрое принятие правильного решения. Это система нового поколения, дружелюбная к человеку.

Вот очень коротко о том, что мы можем сегодня предложить в области пожарной безопасности многофункциональных объектов.

Вопросы, заданные в ходе доклада

О стоимости систем

– Не будем никого вводить в заблуждение, системы Siemens на крупных объектах — это недешево. Нас самих иногда удивляет цена (улыбается — прим. Ред.). Если мы говорим о коттедже в 3 этажа, то наша система будет стоить в 5 раз дороже, чем любая другая. Когда мы говорим о крупных объектах, то цена разглаживается, становится весьма приемлемой. Говоря о системах, необходимых, например, в нефтехимии, я не вижу на сегодняшний день сертифицированных в Беларуси систем-аналогов, которые обладают таким разнообразием детекторов и могут закрывать все вопросы отрасли.

– Где находится производство систем Siemens?

– Сборка и дизайн-разработка идет в Швейцарии. Программная часть разрабатывается только в офисе Siemens, на сторону такую разработку никому не дают, потому что именно на этом больше всего зарабатывают.

– Существуют ли вопросы интеграции отечественных систем с системами Siemens?

– Стыковка проходила на уровне сигналов, и она всегда вполне нормально решалась. Кроме того, наши инженеры ездят учиться в Швейцарию, поэтому отечественная компания обладает высококвалифицированными специалистами, способными решать и такие задачи.

– Насколько Siemens открывает свои протоколы для интеграции?

– Раньше Siemens никому никаких протоколов не давала. Сейчас компания стала более открытой, потому как ощущается необходимость в сотрудничестве. Возьмите хотя бы OPC сервер системы MM8000. Это стандартные, известные всем протоколы, позволяющие интегрировать системы различных производителей. ■

ООО «Эскорт»
220125, г.Минск, ул.Городецкая, 15
Тел./факс: (017) 286-45-13, 286-61-91
E-mail: escort@adsl.by
Сайт: www.escort-asf.com

SALTO
inspiredaccess

Инновационные беспроводные системы контроля доступа SALTO

Сушинский Александр, начальник технического отдела
ОДО Сфератрэйд

Чем же отличается система контроля доступа на спортивных сооружениях от рядовых систем, допустим, офисного здания? Есть несколько принципов построения СКД, как одного из элементов инженерной сети, на спортивном сооружении, которые отличают ее от систем на других объектах.

Во-первых, спортивно-оздоровительные комплексы являются многофункциональными и довольно сложными объектами, включающими в себя несколько самостоятельных зон: спортивную, технологическую, административную и торговые зоны, включающие в себя кафе, рестораны, автоматы по продаже напитков и т.д. Также вокруг комплекса присутствуют открытые спортивные площадки, бассейны под открытым небом. При этом все эти зоны связаны между собой единой системой энергоснабжения, связи, безопасности, диспетчеризации и прочими инженерно-техническими системами.

Во-вторых, эти инженерные системы должны быть масштабируемыми и адаптироваться к изменяющимся функциональным значениям помещений спорткомплекса. В комплексных спортивных сооружениях посетительская зона может трансформироваться, перемещаться в зависимости от меняющегося спроса на рынке услуг, предоставляемых комплексом. Т.е. сегодняшняя раздевалка через год может стать солярием, а зона отдыха превратиться в кафетерий.

И в-третьих, необходимо учитывать тот факт, что стадионы, арены, аквапарки, бассейны и прочие спорткомплексы имеют высокий уровень компьютеризации и автоматизации инженерных систем, который с каждым годом все повышается. Поэтому встроенный функционал систем должен обеспечить как минимум 5 лет работы без каких-либо серьезных доработок, и уж тем более без необходимости замены одной системы на другую, более усовершенствованную.

Этим принципам должны подчиняться все инженерные системы, в том числе и СКД. Однако у СКД имеются свои нюансы в данных комплексах.

Начнем с пользователей. Пользователи системы доступа очень разнообразны по правам доступа в различные зоны. К ним относятся постоянные работники, обслуживающий персонал из других организаций, обычные и VIP посетители комплекса. Каждая из групп пользователей может или не может находиться в той или иной зоне либо пользоваться какими-то услугами.

И так как субъекты, относящиеся к группе «посетители», будут пользоваться системой контроля доступа впервые, не проходя никакого обучения, то она должна быть интуитивно понятной, а способ организации доступа в свою очередь — максимально дружественным.

Говоря об удобстве, безопасности и о комфорте для посетителей, стоит помнить и о необходимости интеграции данной системы со смежными, функционирующими на данном объекте. Это позволяет перевести платежи внутри комплекса в безналичную форму и предоставить доступ посетителей к услугам спорткомплекса.

А для сотрудников комплекса необходимо вести учет рабочего времени на базе системы контроля доступа, которой также пользуются и обычные посетители.

Стоит отметить, что головной болью для руководства спортивного сооружения является злоупотребление сотрудниками своим положением: использование оборудования в личных целях или предоставления доступа к нему третьим лицам. Эти злоупотребления может предотвратить система контроля доступа — как один из элементов системы безопасности.

Учитывая все вышеизложенные нюансы, становится понятно, что система контроля доступа не может ограничиваться базовыми для данных систем возможностями. Она должна удовлетворять требованиям сегодняшнего дня и быть готовой к тому, что в будущем появятся новые технологии и концепции, которые необходимо будет интегрировать в действующую систему.

Всем вышесказанным требованиям удовлетворяет СКУД SALTO. С принципом работы данной системы я и хочу Вас познакомить.

Думаю, правильнее будет для начала представить компанию-производителя и дать представление о том, что же собой представляет SALTO на сегодняшний день.

Как самостоятельная организация, SALTO существует на рынке уже 12 лет. Почему я употребил слово *самостоятельная*? Потому что основана она ведущими разработчиками и профессионалами с большим опытом работы по созданию систем контроля доступа из других компаний. На сегодняшний день штат сотрудников составляет более 170 человек. Деятельность компании SALTO включает в себя весь процесс создания продукта, начиная от исследования и разработки и заканчивая производством, сборкой, реализацией и поддержкой.

Причем все узлы разрабатываются внутри компании, будь то механика, электроника либо программное обеспечение.

Обращаясь к статистике, можно отметить, что за годы существования компании более 1 000 000 дверей оснащены замками и контроллерами SALTO.

SALTO предлагает новую концепцию построения системы контроля и управления доступом, используя технологию data-on-card (информация на карте) и создавая на ее основе SALTO Virtual Network — SVN (SALTO Виртуальная Сеть). Основная идея этой концепции заключается в комбинации офлайн и онлайн электронных замков, являющихся частью единой системы. Объединение замков в сеть обеспечивается благодаря использованию виртуальных каналов, т.е. путем передачи информации через ключи пользователей.

При таком подходе вы получаете 95% возможностей проводной онлайн-системы по цене автономной беспроводной системы.

Рассмотрим наглядно, как это работает. На входе в здание и ключевых точках устанавливается онлайн-считыватель, который по локальной сети (LAN или WAN) подключен к АРМ СКУД и может в реальном времени об-

мениваться с ним данными. Поднеся карту к онлайн-считывателю, система записывает на карту пользователя права доступа, а с карты — на считыватель, и далее в базу данных передается аудит событий пользователя и проводится верификация данных. Другими словами, на карту записывается информация о том, кто является владельцем карты, куда этот пользователь может ходить, по какому расписанию и прочие данные, необходимые для корректной работы системы. При входе в помещение, где установлен офлайн-замок, пользователь подносит карту к его считывателю, и между замком и картой происходит примерно следующий «диалог»:

Затем на выходе из здания при поднесении карты к онлайн-считывателю происходит перенос информации о совершенных пользователем проходах по офлайн-замкам, а также ряд служебной информации, необходимой для функционирования системы, например, об уровне заряда батарей офлайн-замков.

Т.к. идентификаторы имеют перезаписываемую память, то на карту можно записать не только информацию из системы SALTO, но и использовать разделы памяти карты в других системах, использующих технологию MiFare. Т.е. емкость памяти ключа делится на несколько секторов, и при этом каждый сектор защищается своим кодом доступа. Например, если у нас имеется карта с объемом памяти 4Кб, то система SALTO видит выделенные ей 2Кб, а две другие смежные системы видят по 1Кб выделенной памяти. На спортивных сооружениях таковыми смежными системами, работающими на одной карте, могут быть система проката спортивного инвентаря, расчет картой в кафетериях и ресторанах, POS-терминалы и прочее. «Карта» может быть представлена не только в привычном для большинства виде — «прямоугольный пластик», но и в исполнении «брелок», «браслет», «наклейка», «наручные часы». Это особенно важно при использовании системы в бассейнах, аквапарках, спортзалах, где далеко не всегда есть возможность положить карту в карман.

Как уже говорилось ранее, спортивный комплекс — это многофункциональный объект со множеством разнообразных зон. И в зданиях находится великое множество дверей, различных как по материалу изготовления, так и по функциональной нагрузке. Двери могут быть металлические, деревянные, стеклянные с рамой или даже полностью стеклянные стены, противодымные и огнеупорные, двери для эвакуационных выходов и прочие. Для всех типов дверей SALTO разработала модельные ряды электронных замков. Помимо до-

вольно обширного модельного ряда, замки поставляются в различной цветовой гамме и широком диапазоне дизайнерских решений, что позволяет вписать их в интерьер любого стиля.

Все типы замков можно условно разделить на две группы, в зависимости от идеи и возможности установки. Первый вариант включает в себя моторизованный замок SALTO, соединенные с ним считыватель и блок электроники с батареями. Этот вариант предпочтителен в том случае, когда двери еще только заказываются на производстве. И при изготовлении двери в нее сразу врезается замок SALTO.

Второй вариант — когда замки другого производителя уже стоят в дверях, заменить их не предоставляется возможным. В такой ситуации можно использовать электронные накладки SALTO на обычный механический замок. В этом случае дверная ручка замка в штатном режиме будет свободно нажиматься, при этом не оттягивая собачку замка и соответственно не открывая дверь. При чтении ликвидной карты, происходит сцепление ручки электронной накладки и механического замка, и вы свободно открываете дверь.

Однако бывают исключения из правил, когда замок или электронную накладку SALTO по каким-то причинам невозможно поставить на дверь с существующим механическим замком. В этом случае можно применить электронный цилиндр SALTO. Такой цилиндр устанавливается вместо обычного механического цилиндра замка и выполняет все те же функции, что и электронный офлайн-замок.

В спорткомплексах, помимо дверей для входа в помещения, существует еще один класс дверей, которые также могут оснащаться специализированными замками SALTO iLocker — это двери шкафчиков и кабинок в раздевалках.

Предугадываю появившийся у вас вопрос: «А если я хочу получать информацию с офф-лайн-замка в реальном времени, не дожидаясь, когда человек пройдет через онлайн-точку доступа?» Да, действительно, в некоторых случаях такая необходимость появляется. Это могут быть какие-то важные и ключевые помещения.

Для решения данного вопроса компанией SALTO был разработан электронный замок со встроенным радиомодулем, работающий по технологии ZigBee. Такой замок может обмениваться информацией со шлюзом по радиоканалу, а шлюз, будучи соединен по локальной сети с АРМ СКУД, обменивается информацией с базой данных в реальном времени.

Таким образом, применяя замки с радиомодулем, вы получаете беспроводную онлайн-СКУД. А несколько метров кабеля, что протянуты от блока питания до шлюза, и для подключения его к локальной сети объекта не лишают СКУД SALTO права называться беспроводной.

Функционал системы, заложенный на программном и аппаратном уровне, позволяет организовать многоуровневую разветвленную СКУД для любого типа объектов и без каких-либо ограничений. Система может обеспечивать контроль доступа от паркингов, открытых площадок, прилегающих к спорткомплексу, и бассейнов до технологических помещений и шкафчиков в раздевалке. А в стандартный функционал СКУД SALTO заложены значительные возможности по интеграции с любыми специализированными приложениями, такими как система учета проката оборудования и прочими.

ОДО «Сфератрэйд»
Беларусь 220118 г.Минск
ул. Машиностроителей 29-117
Тел./факс: +375 (17) 341 50 50
Velcom: +375 (29) 641 50 50
МТС: +375 (29) 541 50 50
info@secur.by www.secur.by

Единая система безопасности объектов

Повсеместное использование локальных компьютерных сетей подталкивает производителей различного рода оборудования к использованию их в качестве линии связи. В системах безопасности также используют данные технологии для построения систем.

Свидетельством тому новое направление — сетевое видеонаблюдение, активно набирающее обороты и занимающее все большую долю ранка систем видеонаблюдения. Аналогичная ситуация наблюдается и в системах контроля и управления доступом. Компания PERCo, предвидя такое развитие, разработала Единую систему безопасности PERCo S-20, которая основывается на Ethernet технологии.

В данном материале мы рассмотрим, что же все-таки представляет собой система S-20, какие предоставляет возможности и какие позволяет выполнять задачи.

Структуру выполняемых системой S-20 задач можно наглядно представить на следующем рисунке:

Как видно из иллюстрации, система S-20 выполняет одновременно 2 глобальные задачи. В первом случае она функционирует как система безопасности предприятия, выступающая в роли единой интегрированной системы, которая включает в себя СКД, охранную сигнализацию и систему видеонаблюдения. Такая система надежно защищает предприятие от краж, вандализма, проникновения посторонних и нежелательных лиц на территорию. В то же время она выполняет функцию повышения эффективности работы предприятия, что подразумевает увеличение трудовой дисциплины и автоматизацию ряда таких рутинных работ как, учет рабочего времени, расчет заработной платы, оформление и изъятие пропусков и т.д.

Эти две задачи выполняются параллельно, и их деятельность никоим образом не мешает работе друг друга. Однако, эти две задачи, в конечном итоге, преследуют одну цель — увеличение прибыли. Чтобы представить себе это схематично, обратимся к следующему рисунку.

Опираясь на реальные данные, экономия будет выглядеть следующим образом:

- сокращение потерь рабочего времени в 3-5 раз (опоздания, прогулы, отсутствие на рабочем месте);
- снижение в 2 раза трудозатрат, связанных с учетом рабочего времени, расчетом заработной платы, изъятием временных пропусков и приемом посетителей.

Единая система безопасности S-20 в прямом смысла слова — единая. Она работает как единый организм. Все ее основные компоненты — контроллеры, охранные приборы, видеокамеры работают в сети Ethernet по одним и тем же протоколам. Что закрывает вопрос о совместимости и уровне интегрированности различного рода оборудования. Контроллер прекрасно понимает команды от охранного прибора, так же как и камера от контроллера и т.п.

В чем же преимущество использования локальной сети при построении Единой системы безопасности S-20? Во-первых, сеть Ethernet применяется повсеместно, ее технология отточена многомиллионными инсталляциями. Все устройства функционируют в едином адресном пространстве по одному протоколу. При этом не используются различного рода преобразователи и конверторы интерфейсов. Использование стандартной шины передачи данных имеет еще одно достоинство — применение в линии связи многообразия организации сети: Wi-Fi, интернет, радиоканальные системы и иные возможности современной передачи данных.

При данном подходе достигается высокая скорость передачи данных, что позволяет без потерь выполнять одновременно множество операций. Система, построенная на основе Ethernet сети, не только отличается высокой скоростью, но может быть весьма распределенной и разнообразной топологии. Т.е. можно строить системы, оборудование которых расположено, допустим, в разных зданиях или даже в разных городах.

Не будем кривить душой, проблемы со связью могут возникнуть и в сетях Ethernet. Однако в S-20 постоянная связь контроллера с сервером не обязательна. При конфигурировании контроллера, в его энергонезависимую память заносится информация о его физическом местоположении, расписании групп пользователей, список разрешенных карт и прочая информация позволяющая контроллеру полноценно работать даже при отсутствии связи с сервером. При восстановлении связи, контроллер отправит на сервер всю информацию о проходах и других сохраненных событиях. Тут же может возникнуть вопрос: «С данными от контроллера все понятно, их объем невелик и проблем с хранением в контроллере не вызывает трудностей, но что делать в таких случаях при использовании в системе видеокамер?» Решением данного вопроса являются видеокамеры торговой марки Mobotix (Germany). Все камеры Mobotix оснащены слотом для flash-карт SD/microSD и, при соответствующих настройках, в случае отсутствия связи, либо задержках в сети, камера будет записывать информацию на внутренний носитель. При восстановлении связи, камера также автоматически отправит из внутреннего буфера недостающую на сервере информацию. Таким образом, в данном

тандеме оборудование становится менее критичным к аварийным ситуациям на линии связи.

Если система S-20 небольшая и ненагружена видеокамерами, то напрашивается использование уже существующей сети Ethernet. Это даст экономию на стоимости самой кабельной продукции и работах по ее прокладке.

При проектировании системы S-20 разработчики позаботились и об увеличении эффективности работы службы охраны. Для этой цели был создан программный модуль «Центральный пост». Его использование позволяет избежать весьма распространенной ошибки, когда видеокамеры используются в качестве инструмента обнаружения тревожных ситуаций. Такое решение требует от сотрудника службы охраны часами следить за десятком и более камер. В результате чего быстро наступает утомление и снижается работоспособность ответственного лица, а следовательно уменьшается и эффективность всей системы. Более практично отдать функцию обнаружения в «руки» техники, а для человека оставить только оценку ситуации и возможность принятия решений по реагированию на нее. Для этого можно использовать различные детекторы движения, охранные извещатели, и при срабатывании выводить изображение с видеокамеры на монитор сотрудника охраны. Далее, на основе полученной информации, охранник принимает решение, как действовать в конкретной ситуации, руководствуясь должностной инструкцией.

В системе S-20 нет каких-либо ограничений по количеству видеокамер. Однако на каждые 30 камер рекомендуется ставить выделенный сервер для обработки и хранения видеоинформации.

Теперь рассмотрим проходную предприятия. Как правило, на проходных используются электромеханические

турникеты или калитки, которые управляются контроллерами доступа. Для упрощения этого «конструктора» — турникет + контроллер + считыватели карт, была разработана электронная проходная PERCo-KT02, представляющая из себя турникет-трипод со встроенным контроллером и двумя считывателями. Она, так же как и прочее оборудование системы S-20, подключается непосредственно в сеть Ethernet. Это не только упрощает и ускоряет монтаж, но и снижает стоимость самой проходной.

Посетители наравне с сотрудниками могут пользоваться электронными пропусками. Получив карту доступа, они могут пройти только туда, где разрешен им доступ. Для ускорения сбора пропусков у посетителей, используется картоприемник IC02, либо законченное решение 2 в 1 — электронная проходная со встроенным картоприемником KTC01. Принцип картоприемника таков: сотрудники компании пользуются им как обычным считывателем, поднося карту к месту считывания, а посетители могут пройти только после помещения карты в бункер картоприемника.

Для организации усиленного контроля на проходной, либо помещениях где это необходимо, организуют видеоидентификацию — визуальное сравнение владельца карты с его фотографией, хранящейся в базе данных.

Вторая задача, которую решает Единая система безопасности S-20 — это повышение эффективности работы предприятия. Как мы и говорили выше, она преследует 2 цели. Во-первых — это уменьшение нарушений трудовой дисциплины, а во вторых автоматизация ряда трудоемких процессов (УРВ, расчет заработной платы, оформление и изъятие пропусков). Эти задачи выполняются с помощью того же оборудования, что используется при решении задач СКД. На практике чаще всего регистрация времени считается при проходе через электронную проходную / турникет на проходной предприятия. Однако если предприятие большое, то правильнее будет разместить регистрирующий контроллер рядом со входом в цех, офисное помещение, для регистрации времени прихода непосредственно на рабочее место.

Используя полученные данные, можно ежедневно получать дисциплинарные отчеты об опоздавших, ушедших ранее, либо отсутствующих на рабочем месте. Система автоматически формирует табели учета рабочего времени, используя стандартные формы Т-12 и Т-13, где учитывается только реальное время присутствия сотрудника на рабочем месте в соответствии с его рабочим графиком. Для различных подразделений, отделов могут быть определены различные графики работы: многосменные, недельные и скользящие.

При необходимости переноса данных из Системы S-20 в 1С: Предприятие, разработан специальный программный модуль «ФОРМУЛА: Модуль «Учет рабочего времени». Интеграция с 1С: Предприятие 8», осуществляющий передачу информации о реально отработанном времени, на основании которой формируется табель учета рабочего времени и рассчитывается заработная плата.

Для контроля сотрудников в течение рабочего дня существует функция «Прозрачное здание», которая использует видеоизображение, полученное от видеокамеры. Сотрудник будет ответственно подходить к соблюдению трудовой дисциплины, зная что его в любой момент может проконтролировать руководитель.

Отличие этой функции от модуля «Видеонаблюдение» состоит в том, что видеоизображение передается с малой частотой кадров и задержкой, не создавая нагрузок в компьютерной сети, тем самым, исключая задержки в работе системы безопасности.

При оснащении предприятия Единой системой безопасности S-20 стоит помнить о необходимости принятия соответствующих административных мер, позволяющих системе работать полноценно. Для этого необходимо назначить специалистов, соответствующей квалификации, ответственных за обслуживание и работу системы. При недостаточной квалификации — обеспечить обучение персонала. Также разработать нормативные акты, сопровождающие внедрение системы безопасности (должностные инструкции пользователей системы, положение о пропускном режиме, положение об учете рабочего времени и т.д.).

Напоследок следует отметить еще одно преимущество данной системы — соотношение функционал / стоимость. Решив поставить себе систему безопасности, вы одновременно приобретаете инструмент повышения эффективности работы предприятия. Затраты уменьшаются, и следовательно растет прибыль, т.е. система не просто работает, а зарабатывает Вам деньги.

Официальный дилер компании PERCo в Беларуси
ОДО «Сфератрэйд»
Беларусь 220118 г.Минск
ул. Машиностроителей 29-117
Тел./факс: +375 (17) 341 50 50
Velcom: +375 (29) 641 50 50
МТС: +375 (29) 541 50 50
info@secur.by www.secur.by

Организация билетно-пропускных систем многофункциональных спортивных объектов на базе оборудования компании SKIDATA

Компания SKIDATA основана в 1977 году. Изначально специализировалась на автоматизации платного доступа горнолыжных комплексов. Центральный офис находится в г.Зальцбург, Австрия. Штат — 500 сотрудников по всему миру и активность более, чем в 30 странах. Доля мирового рынка 86% (горнолыжные комплексы), это 6000 инсталляций, включая 1600 инсталляций парковочных систем. Сегодня SKIDATA предлагает клиентам высококачественные решения и сервисы для обеспечения доступа автомобилей и людей на стадионы и в спортивные комплексы и другие многофункциональные объекты с большим содержанием посетителей. Решения SKIDATA отличаются скоростью и надежностью управления доступом, а также, благодаря доступности и поддержки многочисленных платформ продаж билетов, обеспечивают высокий уровень сервисов.

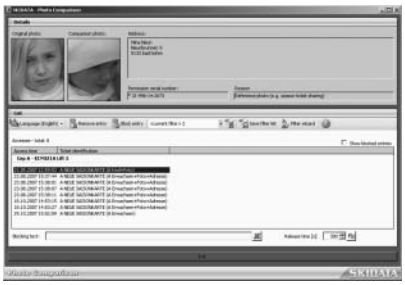
Билетно-пропускная система на основе оборудования SKIDATA состоит из нескольких основных подсистем и сервисов:

1. Турникеты Freemotion Full.Gate

Freemotion Full Gate — это максимальный контроль, удобство в использовании и безопасность. Благодаря наличию у турникетов таких важных функций, как определитель роста, идентификация по фотографии, вероятность мошенничества снижается практически до нуля. Наличие турникетов исключит случаи, когда гости используют детские скипассы (ski-pass) для подъема на склоны.

Датчик роста: предотвращение мошенничеств с использованием более дешевых детских билетов;

Миникамера:



- фотографирование непосредственно со считывающего устройства;
- возможность сравнительной идентификации фотографий в течение дня для билетов со сроком действия в один день;
- возможность индивидуальной проверки билетов, проданных в течение дня;
- сигнальные лампы (красная/желтая/зеленая) для обслуживающего персонала — расположены с тыльной стороны считывающего устройства;
- использование функции сравнения идентификационных фотографий:

фотографии, отснятые со считывающего устройства, могут использоваться для сравнения с фотографиями, отснятыми в точках продажи или на пропускном пункте, в соответствии с принятыми правилами. В случае если фотографии отличаются, обслуживающий персонал может заблокировать проход.

2. Рабочее место кассира (Point Off Sale).

Рабочее место кассира — является автоматизированным рабочим местом, в состав которого входят:

- персональный компьютер с монитором и специальной клавиатурой, оснащенной дополнительными функциональными клавишами;
- печатающее кодирующее устройство, предназначенное для кодирования билетов в памяти смарт-карт (записывание/перезаписывание) или в штрих-коде (печать), а также для печати на поверхности билетов персональной информации;
- дополнительно может быть установлена цифровая фотокамера для фотографирования клиентов с последующим сохранением фотографий в базе данных системы и нанесением термоспособом на лицевую сторону смарт-карт (дополнительно могут быть подключены периферийные устройства: фискальный регистратор, терминал для работы с банковскими картами).

3. Мини-центр управления турникетами (Minicentral).

Оборудован персональным компьютером с монитором и стандартной клавиатурой;

предназначен для управления работой турникетов и осуществления дополнительного визуального контроля (фотоконтроль владельцев билетов, при котором фотографии владельцев билетов отображаются на мониторе контролера при предъявлении билета турникету, а также контроль за соответствием возраста владельца билета типу этого билета, если такое различие определено тарифа-

ми) за проходящими через турникеты владельцами билетов, при этом существует возможность блокировать и разблокировать билеты;

4. Handheld.Gate — Ручной малогабаритный мобильный терминал

Предназначен для дополнительного контроля на местах посадки лыжников на подъёмник. Позволяет в режиме реального времени проверять билеты и отображает информацию о билете, а также имеет возможность отображать информацию о проходах через турникет с функцией показа фото проходящего, осуществлять блокировку билетов, помещать билет в стоп-лист.

5. Функционирование системы в режимах On-line и Off-line.

Все компоненты системы (турникеты, кассы, места контролеров, сервер) являются автономными и могут быть соединены между собой в локальную сеть по протоколу Ethernet. Все компоненты системы имеют возможность работы в режимах Online и Offline. При работе в режиме Online вся информация о транзакциях (вход, запрет доступа, выпуск билета и др.) поступает в базу данных системы (на сервер) немедленно или по расписанию в зависимости от важности информации и заданных параметров связи. При работе компонентов системы в режиме Offline (настраивается при отсутствии линий связи или автоматически активизируется при потере связи) информация сохраняется во внутренней памяти компонент (жесткий диск рабочего места или память контроллера), и передается в базу данных системы автоматически после восстановления связи или ручным способом при помощи носителей памяти flash.

6. Удаленная предварительная продажа билетов Offsite Point of Sale (OPOS)

Помимо продаж билетов непосредственно в кассах курорта, мы рекомендуем OPOS — модуль, который находится в управлении третьей стороны, например, отеля или спортивного магазина.

OPOS — технология удаленной предварительной продажи билетов.

Простой и экономичный способ организации предварительной продажи билетов на сторонних точках продажи, например, в отелях, пунктах аренды лыжного инвентаря, магазинах, турагентствах.

Удобство для гостей курорта: у них появляется возможность купить билет прямо в отеле и, минуя очередь в кассу, направиться к подъемнику.

7. Easy Ticket Cash — автомат по продаже скипассов

Этот удобный и красивый аппарат поможет Вам продавать билеты на подъемники в любое время суток, в любом месте. Автомат Easy Ticket Cash можно установить в точках дополнительных продаж: на ж/д вокзалах, в спортивных магазинах, и т.п.

Удобство для ваших клиентов:

• Безналичный платеж — быстро, легко, удобно

• Нет необходимости стоять в очереди, купить скипасс при помощи автомата и сразу начать кататься

• Меню на нескольких языках

Больше времени для Ваших клиентов:

• «стандартные билеты» продает автомат, а ваши кассиры смогут уделить больше внимания клиентам, которым требуется помощь.

Экономия:

• Нет необходимости работать с наличными, отсутствие сложных взаиморасчетов.

8. Программное Обеспечение SKIDATA для горнолыжных курортов

- Direct Connect.

Новый способ хранения данных и оперирования информацией внутри системы. Устройства системы (кассы, локальные серверы Minicentral, центральный сервер Datacentral) работают не только со своим локальным хранилищем данных, но дополнительно работают в режиме онлайн, в котором происходит перманентная синхронизация с единой центральной базой данных, охватывающей весь горнолыжный курорт.

- Generi Connector

Это «механизм», который конвертирует полученные от сервера данные в упрощенный вид, адаптируя структуру данных для экспорта в прочие системы. Таким образом, обработка данных при помощи прочих систем становится проще и понятнее.

- CRM -Connector

Это программа, позволяющая синхронизировать данные в системе SKIDATA™Ski-system с различными профессиональными инструментами CRM (Customer Relationship Management). Программное обеспечение SKIDATA™Ski-system создает и хранит данные о всех транзакциях, таких как выпуск билета, бронирование через Интернет, проход пользователя к подъемнику и т.п.

- Flexspace: новое поколение носителей данных

SKIDATA предлагает новый тип RFID билетов — билеты, отформатированные по принципу «Flexspace».

- DTA (Direct To Access)

DTA — Direct to Access, приложение, которое работает с последними версиями ПО, — откроет дверь в мир Интернета, что в наши дни открывает доступ в мир новых источников прибыли.

• DTA — совместимая платформа, позволяющая связать различные каналы сбыта с поставщиками услуг

• Модульная структура и прозрачность для комплексного направленного управления

• Возможности динамичного ценообразования и оплаты по факту пользования услугой

SKIDATA предоставляет платформу DTA и специализированную IT-инфраструктуру.

9. iSkipass — Используйте iPhone для связи с современной платформой бронирования

10. SDRDM — Статистические данные и отчётность.

Информация по продажам билетов является основной при анализе потока посетителей, что, к примеру, может служить инструментом оценки привлекательности товаров и услуг. Система отчетности (и ее программное обеспечение) в связи с этим является не только инструментом обработки информации; помимо простоты анализа информации и работы в режиме реального времени система отчетности должна также обеспечивать оптимальную поддержку для всего процесса принятия решений.

SD-RDM предоставляет возможность гибкой конфигурации отдельных отчетов для управляющего персонала, системных администраторов и менеджеров.

11.Pool Clearing —взаиморасчёты между курортами.

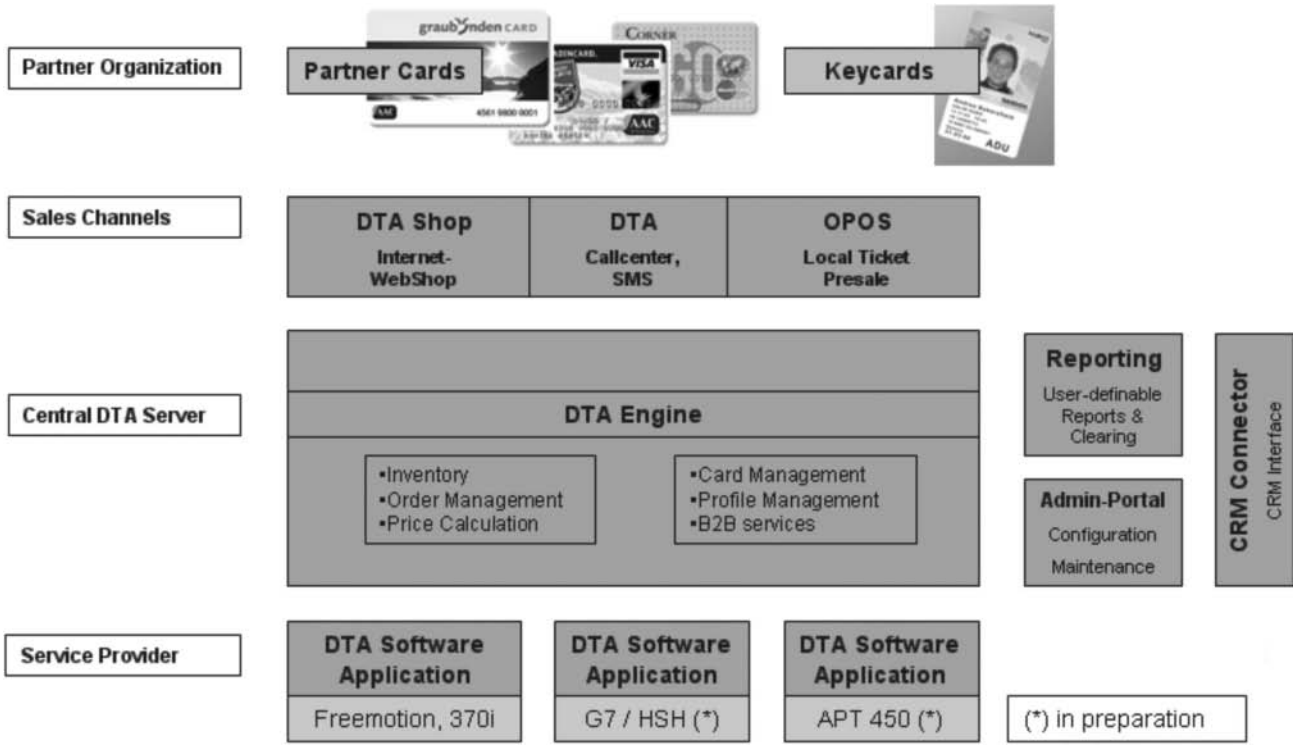
Эта функция позволит использовать один скипасс на несколько курортов, где уже установлена система Скидата и впоследствии производить грамотные и лёгкие взаиморасчёты между курортами.

12.Skiline — диаграмма альтиметра

Позволяет вам, просто используя свой скипасс, отображать метры, пройденные вами за день, следить за количеством подъемов, накапливать "вертикальные" метры и метры на склонах.

13.Sweb.Cockpit —удобный инструмент менеджмента и мониторинга.

Позволит сделать текущую информацию, практически в режиме реального времени — основой для вашего успеха. Вам нужен всего лишь браузер и доступ к важным данным — таким как продажи, количество проходов, состояние оборудования или количество гостей, гарантирован в любое время.



Веб-сайт SKIDATA

• SKIDATA предлагает технологию продажи через Интернет

• Дизайн веб-страницы разрабатывается для клиента, исходя из индивидуальных потребностей

• Возможна интеграция с платежными системами

• Динамичное ценообразование

• Оплата по факту: постоянным клиентам предоставляются выгодные пакеты предложений и возможность оплаты услуг после их фактического использования

Webshop.Cash: заказ билетов через Интернет

ООО «Корпоративные Информационные Системы»
220073, г.Минск, ул. Бирюзова, 10 а, офис 214
Тел./факс: (017) 204-87-41, (029) 610-70-97, (029) 650-19-76
E-mail: ciscompany@tut.by
Сайт: www.ciscompany.by

УНП: 191161232

АДАНИ

Рентгеновские инспекционные системы АДАНИ — новые возможности для обеспечения антитеррористической защищенности зданий и сооружений

Емельянов Юрий Леонидович, заведующий отделом технической физики УП «АДАНИ»

Справка ТБ

Компания АДАНИ создана в 1991 г. для реализации инновационных проектов по созданию современных образцов цифровой рентгеновской техники для таких отраслей, как экология, медицина и безопасность. В настоящее время компания АДАНИ является одним из ведущих разработчиков и производителей современных рентгеновских сканеров для медицины и безопасности.

Приоритетными направлениями разработок в области систем безопасности являются:

1. Сканеры для досмотра багажа, грузов и посылок.
2. Сканеры для досмотра людей.
3. Сканеры для досмотра большегрузных автомобилей, авиационных контейнеров и других крупногабаритных объектов.

Успешное развитие компании на международном рынке основано на достижениях высокопрофессионального коллектива специалистов в области физики, механики, электроники и программного обеспечения.

Стратегия АДАНИ — максимальное качество продукции при минимальной цене.

Компания АДАНИ ориентирована на учет специфических пожеланий своих клиентов при разработке новых образцов техники.

Качество продукции АДАНИ подтверждается сертификатами качества ISO 9001:2000, ISO 13485:2003.

1. Системы для досмотра багажа и грузов

Назначение

Сканеры предназначены для визуального контроля багажа, грузов, почтовых отправлений и т.п. без их вскрытия с целью выявления опасных и запрещенных предметов, материалов и веществ. Сканеры широко применяются в системе безопасности аэропортов, наземного транспорта, в исправительных учреждениях, на особоохраняемых объектах и т.д. Разработан ряд моделей, отличающихся размерами инспекционного тоннеля и грузоподъемностью конвейера.

Принцип действия

Сканирование осуществляется путем просвечивания объекта, движущегося по конвейерной ленте, веерообразным пучком рентгеновского излучения. Прошедшее через объект рентгеновское излучение регистрируется детектором, расположенным с обратной стороны инспекционного тоннеля. Детектор преобразует рентгеновское излучение в цифровые сигналы, которые передаются в компьютер для реконструкции двумерного теневого изображения на рабочем мониторе в целях последующего анализа оператором. Формирование рентгеновского изображения и его математическая обработка осуществляется в реальном режиме времени.

Двухэнергетическая технология

Все сканеры оснащены двухэнергетической технологией, позволяющей распознавать материалы по эффективному атомному номеру. Все материалы группируются в три класса и показываются на мониторе различным цветом:

- оранжевый — органические материалы с Z≤10;
- зеленый — смешанные и неорганические материалы со средним атомным номером от 10 до 18 (алюминий, кремний и другие);
- синий — металлоподобные материалы с высоким атомным номером > 18 (железо, медь и т.п.)

Дополнительно имеются функции отслаивания (визуализации) только органических или только неорганических материалов.

Рис. Конструкция и принцип действия

Основные технические характеристики

Технические возможности всех моделей сканеров отвечают самым современным требованиям к качеству изображения, надежности и безопасности и находятся на уровне лучших мировых образцов.

- Энергия фотонов — от 140 до 200 кэВ;
- Скорость движения конвейера — 0,22 м/с;
- Грузоподъемность конвейера — от 160 до 3000 кг;
- Размеры инспекционного тоннеля — от 640 до 1750 мм;
- Проникающая способность — до 35 мм стали;
- Обнаружительная способность — 0,1 мм (диаметр медной проволоки);
- Радиационные утечки не превышают 1 мкЗв/ч на расстоянии 5 см от внешних поверхностей сканера.

Функции программного обеспечения

Комплекс программ является оригинальным специализированным программным обеспечением для управления сканером и обработки рентгеновских изображений. Интерфейс оператора и сканера обеспечива-

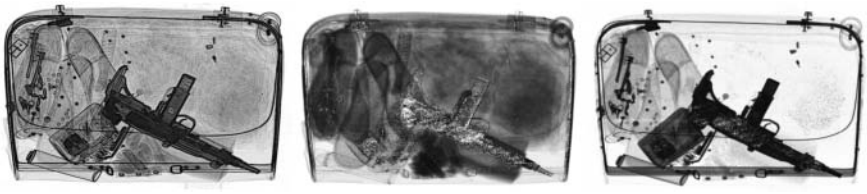


Рис. Слева направо: основное двухэнергетическое изображение, только органические материалы, только неорганические материалы.

ется с помощью специализированного пульта управления.

Функции управления процессом сканирования

- сканирование в прямом и обратном направлении;
- автоматическое включение/выключение излучения при наличии/отсутствии объекта на конвейере;
- движение конвейера без излучения;
- автоматическая калибровка детектора;
- отключения рентгеновского генератора в случае возникновения аварийной ситуации;
- автоматическая самодиагностика.

Функции обработки, хранения и передачи цифровых рентгеновских изображений

- автоматическая коррекция геометрических изображений;
- оптимизация общего контраста;
- усиление контраста сильно поглощающих объектов;
- инверсия изображения;
- варьируемая настройка контраста (гамма-коррекция);
- усиление границ;
- увеличение выбранного участка изображения;
- автоматическое сохранение изображений в базу данных;
- копирование выбранных изображений из архива на внешние носители информации.

Функции общего назначения

- парольный вход в систему;
- счет количества досмотренного багажа (циклов).

Дополнительные функции

- функция проецирования виртуальных изображений опасных и запрещенных объектов в изображение багажа (для тренировки операторов);
- автоматическое обнаружение подозрительных объектов.

2. Системы для персонального досмотра

Назначение

Сканеры предназначены для получения рентгеновского изображения человека с целью выявления опасных и запрещенных предметов, материалов и веществ, спрятанных под одеждой и внутри человеческого тела. Сканирование осуществляется путем перемещения человека на подвижной платформе через веерообразный пучок рентгеновского излучения.

Недостатки существующих технологий досмотра людей

Металлодетекторы

- Любые безопасные металлические объекты, включая распространенный сейчас пирсинг, а также детали медицинских устройств *(электронный стимулятор сердца)*, протезов и имплантатов, вызывают ложные сигналы тревоги. Наличие таких тревог приводит к необходимости применения дополнительных процедур досмотра *(ручной обыск, снятие пирсинга, сканирование отдельно обуви и одежды и т.п.)*, уменьшающих пропускную способность пунктов досмотра и приводящих к потере бдительности операторов.
- Неметаллические объекты, к которым относятся, например, пластиковая взрывчатка и оружие из дерева, пластика и подобных материалов, вообще не могут быть обнаружены с помощью металлодетектора. Как следствие, возникает необходимость в дополнительных процедурах досмотра *(например, отдельное сканирование обуви и одежды на багажных сканерах)*, которые лишь отчасти решают проблему.

Газоанализаторы

- Недостаточная избирательность приводит к росту числа ложных срабатываний.
- Некоторые химические соединения способны «маскировать» присутствие искомых химических компонентов, что приводит к снижению эффективности обнаружения.
- Системы предназначены для поиска ограниченного числа химических соединений (пластиковой взрывчатки, к примеру), т.е. не носят универсального характера (например, неметаллическое оружие не обнаруживается).
- Высокая стоимость технического обслуживания.

Поверхностно чувствительные технологии визуализации

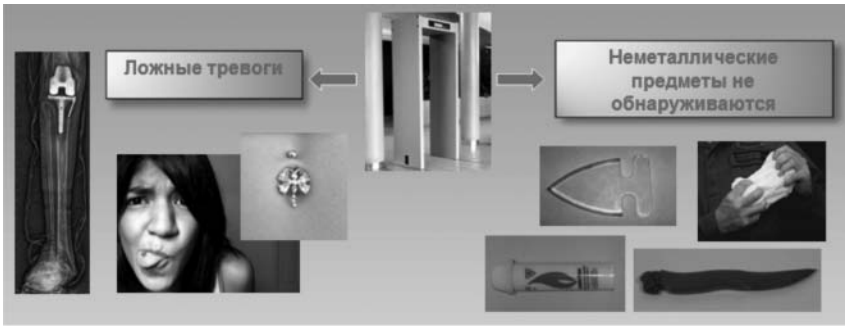
Действие таких систем основано на визуализации объектов, спрятанных под одеждой или на теле человека, с помощью ионизирующих и неионизирующих излучений. К данному классу относятся системы, основанные на использовании эффекта обратного рассеивания рентгеновских лучей, миллиметрового излучения *(микроволнового)* и терагерцового излучения *(переход между дальним инфракрасным и микроволновым излучением)*.

Общие недостатки таких систем:

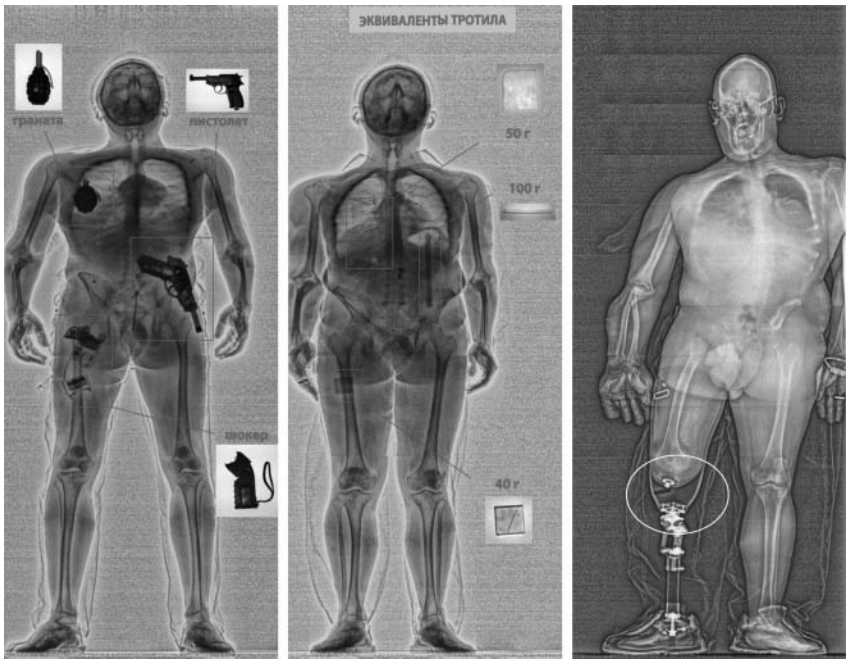
- Объекты в естественных полостях человека, спрятанные в протезах и гипсовых повязках, имплантированные в тело человека, не обнаруживаются.
- Низкая эффективность обнаружения объектов в проблемных зонах (под мышками, область паха, обувь, толстая одежда).
- Существует возможность маскировки объектов материалами, имитирующими человеческое тело (например, накладной живот для имитации беременности).
- Невысокое пространственное разрешение.

Просвечивающая рентгеновская технология

Рентгеновская просвечивающая технология — единственная технология, позволяющая обнаруживать любые объекты, как на поверхности тела человека, так и внутри него. Данная технология используется в системах АДАНИ.



Нижеприведенные изображения иллюстрируют возможности данной технологии.



Радиационная безопасность

Доза, которую получает инспектируемый человек, крайне мала и сравнима по величине с воздействием естественного радиационного фона в течение 1 часа. Как видно из данной диаграммы, доза на системе ConPass намного меньше дозы от медицинских рентгеновских обследований (в 400 раз) и дозы, получаемой пассажирами любых авиарейсов.

3. Системы для досмотра грузового транспорта и грузовых контейнеров

Назначение

Сканеры предназначены для визуального контроля содержимого грузовых контейнеров и грузовых автомобилей без их вскрытия с целью выявления в них опасных и запрещенных предметов, материалов и веществ, нелегальных мигрантов, а также в целях таможенного контроля перевозимых грузов.

Способ сканирования

Благодаря низкой интенсивности используемого рентгеновского излучения и наличию системы датчиков, обеспечивающих облучение только грузового отсека, сканирование реализуется путем движения транспортного средства через радиационный портал сканера своим ходом под управлением водителя («в потоке»).

Преимущества сканирования «в потоке»

- Высокая пропускная способность.
- Минимальная санитарно-защитная зона вокруг сканера.
- Улучшенное качество изображения из-за отсутствия вибраций в ходе сканирования (жесткая конструкция досмотрового портала).
- Стоимость системы значительно меньше аналогов из-за отсутствия движущихся механизмов, требующих повышенных расходов на техническое обслуживание и снижающих надежность системы в целом.

Технические характеристики

- Пропускная способность — до 50 объектов в час (длиной 30 м);
- Энергия излучения — 5 МэВ.
- Рекомендуемая скорость сканирования (скорость движения досматриваемого транспорта) — 5-10 км/ч.
- Время перебазирования: от нескольких часов для мобильной конфигурации до нескольких дней для перебазируемой конфигурации с подготовленной инфраструктурой.
- Доза на водителя (кабина не сканируется) — не более 0,02 мкЗв.
- Доза на персонал — не более 1 мкЗв/ч.
- Доза на нелегального мигранта — не более 1 мкЗв.
- Возможность интеграции в состав комплекса радиационного монитора портального типа для обнаружения

Качество изображения

- Проникающая способность — до 240 мм стали.
- Пространственное разрешение — 5 мм.
- Обнаружительная способность — стальная проволока диаметром 3 мм.

В настоящее время без рассмотренных выше рентгеновских сканеров, являющихся эффективными техническими средствами для контроля доступа в здания или отдельные помещения, а также на окружающую объект территорию, невозможно обеспечить комплексную безопасность многофункциональных и спортивных объектов с массовым пребыванием людей.

УП «АДАНИ»
220075, г. Минск, ул. Селицкого, д.7, пом.2/1
Тел: (017) 346-29-03, факс: (017) 346-29-02
E-mail: info@adani.by
Сайт: www.adani.by

Рис. Пример изображения грузового отсека автомобиля

Regula forensic science systems

Возможности построения систем идентификации в системах контроля доступа на критически важных объектах

Скворчевский Юрий, начальник отдела маркетинга компании «Регула»

Контроль доступа на КВО является основой безопасности такого рода объектов. Компания «Регула» на основе собственных приборов-индетификаторов разработала и внедрила специализированный комплекс, позволяющий проводить идентификацию посетителей по документам, удостоверяющим личность.

Комплекс предлагается к использованию в местах, где требуется не только корректное считывание данных из документа, но и проверка как самих данных, внесённых в документ различными способами (в том числе, с помощью бесконтактных идентификационных микросхем (чипов), так и проверка подлинности самого документа.

Такими местами могут являться (при доминирующей задаче контроля подлинности документа и проверки находящейся в нём информации):

1) банковские пункты выдачи кредитов («быстрых» кредитов) населению;

2) пункты прохода в «режимные» зоны — банковские хранилища, территории производств и другие помещения, где требуется идентификация личности по паспорту;

3) в аэропортах, при регистрации пассажиров на рейс;

4) пункты продажи телефонных карт мобильной связи.

Также комплекс может использоваться (при доминирующей задаче — автоматизация ввода данных из документа):

1) в авиа и железнодорожных кассах;
2) в паспортно — визовых службах;
3) в страховых компаниях;
4) в нотариальных конторах.

Рис.1. Считыватель документов «Регула» 70X4.XXX

Назначение комплекса

Использование считывателя документов в системах контроля доступа, осуществляющих автоматизированный ввод данных (сейфовое хранилище, проходная/пункт пропуска в банк).

В процессе работы комплекса происходит:

Получение изображений:

1) получение цветного изображения документа;

2) получение ультрафиолетового изображения документа;

3) получение инфракрасного изображения документа.

Считывание данных:

1) считывание данных из машиносчитываемой зоны (MRZ) документа;

Рис.2. Получение цветного изображения документа.

Рис. 3. Получение ультрафиолетового изображения документа.

Рис.4. Получение инфракрасного изображения документа.

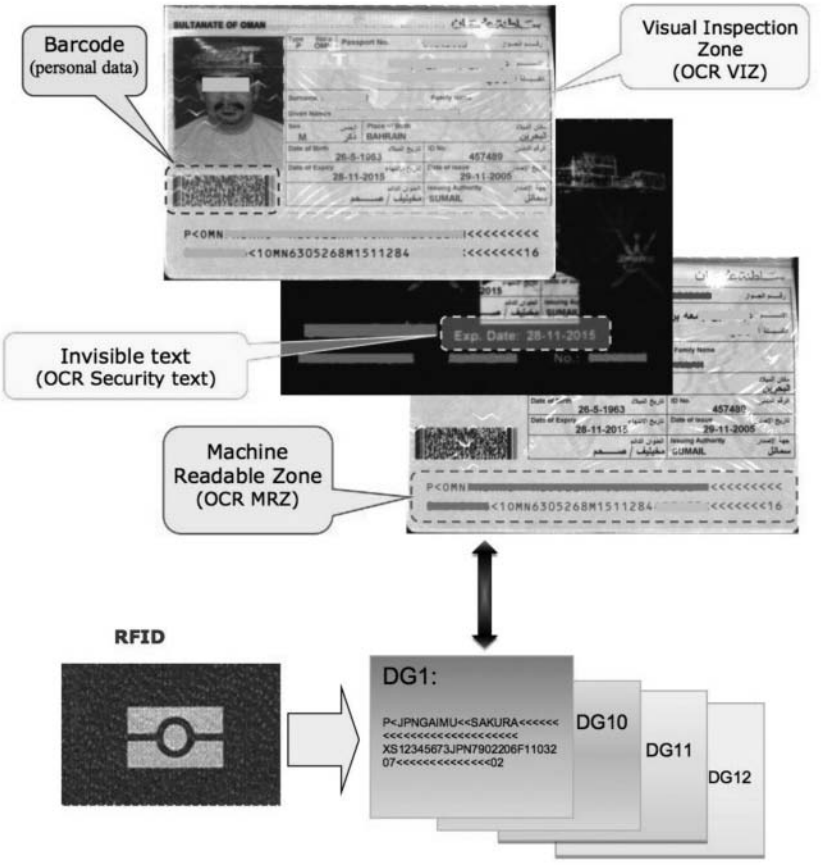


Рис. 5. Считывание текстовых данных

2) чтение текстовых данных (OCR);

3) определение государственной принадлежности и типа документа;

4) получение изображения фотографии владельца документа.

Проверка подлинности:

1) проверка подлинности и оценка качества печати машиносчитываемой зоны (MRZ) документа;

2) наличие ультрафиолетовой защиты;

3) наличие инфракрасной защиты.

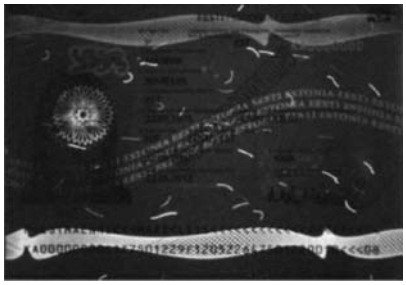


Рис. 6. Проверка подлинности в УФ-свете.

Дополнительно:

1) сканирование отпечатка пальца;

2) фиксация изображения владельца документа;

3) ввод персонального кода клиента.

Рис. 7. Сканирование отпечатка пальца.

Контроль:

1) сравнение полученных данных из машиносчитываемой зоны (MRZ) документа и текстовых данных (OCR). При их несовпадении — уведомление (сигнал);

2) проверка контрольной суммы машиносчитываемой зоны;

3) контроль срока действия документа;

4) сравнение изображений владельца документа с полученными ранее изображениями (визуально);

В состав комплекса входит:

1. Считыватель документов Регула мод.70X4.XXX

(Считывание документов, получение изображения. Считывание машиночитаемой зоны документа, считывание информации из визуальной зоны контроля паспорта. АРМ регистрации посещений хранилища ценностей клиентов.

2. Устройство сканирования отпечатка пальца.*

3. Устройство ввода персонального кода клиента.*

4. Видеокамера.*

5. Устройство ввода подписи.*

* – п.п.2,3,4 — поставляются по желанию заказчика при технологической необходимости.

АРМ регистрации посещений хранилища ценностей клиентов

На основе комплекса реализована СКУД для банковских хранилищ, позволяющая проводить идентификацию посетителей по документам, удостоверяющим личность — АРМ регистрации посещений хранилища ценностей клиентов, состоящий из двух программных частей:

- АРМ Администратора;
- АРМ Оператора.

АРМ Администратора предна-

значен для администрирования системы (создание, изменение, удаление учетных записей пользователей; сервисные операции с базой данных; настройка параметров функционирования системы; подключение и настройка работы с внешним оборудованием; просмотр и обслуживание журналов работы системы; администрирование справочников системы).

АРМ Оператора предназначен непосредственно для регистрации посещений клиентами хранилища.

Алгоритм работы программы следующий:

Оператор авторизуется при входе в программу, указывая имя и пароль, выданные администратором системы.

При обращении клиента:

Оператор создает новое посещение, указывает его параметры (дата и время посещения; цель посещения; в хранилище или к ячейке; указывает дополнительную информацию при необходимости; устанавливает статус посещения; указывает ответственного работника и авторизует свой выбор паролем).

Оператор добавляет в посещение нового посетителя. Затем оператор вставляет документ, удостоверяющий личность клиента, в считыватель и происходит сканирование и распознавание документа.

Если распознанные данные позволяют идентифицировать клиента как уже известного системе, то из базы данных поднимается информация о нем и оператору предоставляется возможность дополнительной идентификации клиента (путем получения визуального изображения клиента и сравнения с сохраненным в базе данных; путем визуального сравнения отсканированного изображения документа с сохраненным в базе данных; путем сканирования отпечатка пальца и автоматического сравнения с отпечатком, сохраненным в базе данных; путем запроса на введение ПИН-кода клиентом и автоматического сравнения с сохраненным в базе данных при регистрации). Если идентификация прошла успешно, то операция повторяется для каждого посетителя (если их несколько), после чего клиенты могут пройти в хранилище.

Если по распознанным данным отсканированного и обработанного документа невозможно идентифицировать клиента как зарегистрированного (новый клиент), то система предлагает зарегистрировать клиента как нового, с получением и заполнением всех необходимых данных для идентификации (изображение, отпечаток пальца, ПИН-код). Если регистрация состоялась успешно, система позволяет добавить клиента в посещение.

После того как посещение состоялось, оператор имеет возможность открыть посещение в журнале и изменить его статус с «в процессе» на «состоялось» или «не состоялось» (с указанием причины).

Система позволяет просматривать и печатать журнал посещений за определенный период с фильтром по посетителю, по посещаемой ячейке, по статусу посещения или без фильтра.

Все действия, совершаемые оператором или администратором в АРМ, регистрируются в системном журнале с указанием даты, времени, пользователя и совершенного действия.

Пример схемы использования считывателя документов при выдаче «быстрого» кредита.

На этапе сканирования происходит:

Получение изображений:

1) получение цветного изображения документа;

2) получение ультрафиолетового изображения документа;

3) получение изображения документа при коаксиальном освещении;

4) получение инфракрасного изображения документа.

Считывание данных:

1) считывание данных из машиносчитываемой зоны (MRZ) документа;

2) чтение текстовых данных (OCR);

3) чтение штрих-кодов с изображения документа;

4) считывание информации с бесконтактных идентификационных микросхем (чипов);

5) определение государственной принадлежности и типа документа;

6) получение изображения фотографии владельца документа.

Проверка подлинности:

1) проверка подлинности и оценка качества печати машиносчитываемой зоны (MRZ) документа;

2) наличие ультрафиолетовой защиты;

3) наличие инфракрасной защиты;

4) проверка скрытых текстов;

5) проверка ретрорефлективной защиты;

6) визуализация скрытых изображений.

Дополнительно:

1) получение образцов изображений и описания документа из базы данных справочно-информационной системы FDS для выполнения сравнительного анализа (сравнения с отсканированным документом);

2) сканирование отпечатка пальца;

3) получение образца подписи.

Автоматизированный контроль:

1) сравнение полученных данных из машиносчитываемой зоны (MRZ) документа, текстовых данных (OCR) и информации с бесконтактных идентификационных микросхем (чипов). При их несовпадении — уведомление (сигнал);

2) проверка контрольной суммы машиносчитываемой зоны;

3) контроль срока действия документа.

ООО «Регула»
220036, г. Минск, ул. Волоха, 1, комн. 314
Тел.: (017) 286-28-25, факс: (017) 210-23-97
E-mail: mail@regula.by
Сайт: www.regula.by

Комплексный подход в практике обеспечения безопасности VIP — резиденций, многофункциональных и спортивных объектов с массовым пребыванием людей

УП «Дизайн-студия СЭНС», Трофименко В.П. Иванов В.Г.

Комплексный подход в решении сложных проблем является залогом успеха. История создания сложных технических комплексов и технологий является хорошим примером и доказательством, достаточно вспомнить историю развития современных направлений техники и передовых технологий, таких как, развитие систем радиосвязи, развитие химической промышленности, атомной энергетики и развитие других отраслей народного хозяйства.

В настоящее время комплексный подход при создании систем антитеррора (АТ) с целью безопасных условий проведения многофункциональных и спортивных мероприятий с массовым пребыванием людей является важнейшим фактором предупреждения террористических намерений.

Тенденции развития средств АТ

Специалисты нашего предприятия постоянно и очень тщательно отслеживают совершенствование законодательства в нашей стране и анализируют мировые тенденции развития этого направления.

Наиболее интересные материалы мы стараемся анализировать и наблюдать за их перспективным развитием. Так на проведенной конференции мы прокомментировали две темы, которые наиболее полно характеризуют тенденции развития поисковых направлений борьбы с террором:

1. Задача обнаружения стрессов водителей во время реального движения с помощью физиологических датчиков;
2. Пограничная оценка безопасности через анализ гетерогенных областей.

В приведенных темах рассматривается анализ эмоционального состояния водителей или наблюдаемых людей для определения их состояния — стрессовых ситуаций, незаконных намерений, от простого наблюдения до анализа гетерогенных областей.

Это новое поколение антитеррористического оборудования, которое значительно повысит эффективность борьбы и, самое главное, нацелено на предупреждение террористических намерений. При этом предлагается создание совершенно новых рабочих мест эффективного контроля.

Контроль эмоционального, стрессового состояния водителя

Вариант организации рабочего места контроля эмоционального, стрессового состояния водителя с помощью системы физиологических датчиков: электрокардиограммы, электромиографии, датчиков руля и датчиков педалей.

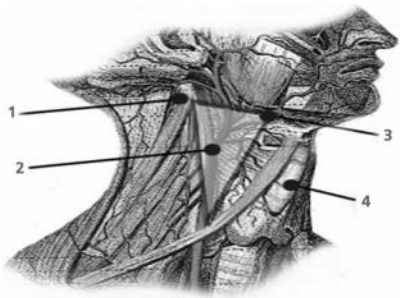


Рис. 2. Анатомия гетерогенных зон лицевой области человека.

человека. Контроль эмоционального, стрессового состояния водителя демонстрирует наибольшую точность, однако сопряжён с размещением датчиков в не-

Рис. 1. Структурная схема системы контроля психо-физиологического состояния водителя транспортного средства.

Анализ гетерогенных зон человека

Гетерогенные зоны человека:

1. Грудинно-ключично-сосцевидная мышца.
2. Сонная артерия.
3. Сонный треугольник.
4. Трахея.

Установлено, что анализ этих зон лица может характеризовать эмоциональное состояние человека. Исследованию этого явления посвящено много работ и созданы методики анализа. Задача инженерная — применить разработанные методики и создать приборы для оперативного применения.

Примеры иллюстрируют различные подходы к автоматическому контролю психо-эмоционального состояния посредственном контакте с телом человека. Анализ гетерогенных зон человека нацелен на минимизацию инвазивности самой процедуры контроля. Собеседник при работе такой системы не испытывает физического и эмоционального дискомфорта.

Однако в обоих случаях применение автоматики позволяет утверждать, что таким образом достигаются следующие желательные свойства контролирующей системы:

1. Возможность и экономическая эффективность массового применения системы контроля;
2. Универсальная объективность решающего алгоритма, который свободен от влияния межличностных аспектов на принятие конкретного решения;

Рис. 3. Система компьютерного зрения, анализирующая портрет лицевой области человека в диапазоне инфракрасного излучения.

3. Неразглашение приватной информации о сознательных или бессознательных аспектах поведения конкретной личности без исключительной на то необходимости.

Комплексный подход и классификация при решении задач АТ

При подготовке материала, после проведенного анализа, на основе опыта полученного при внедрении и организации производства сложных научно-технических проектов, мы пришли к выводу, что работа по обеспечению безопасности многофункциональных и спортивных мероприятий с массовым пребыванием людей, может быть успешной только при условии реализации комплексного подхода.

Проведенные исследования показывают, что для того, чтобы система автоматического контроля психо-эмоционального состояния давала надёжные оценки, она должна получать широкий спектр входных сигналов, а также должна содержать в себе достаточно подробную модель классифицируемого объекта во времени. Такая система сможет стать надёжной именно **при сочетании целого комплекса отдельных задач классификации**. Архитектура такой системы должна обеспечивать многостадийный механизм принятия решений. На первой стадии определяются отдельные признаки, которые могут соответствовать множеству возможных причин, в дальнейшем возможные причины, приведшие к одновременному возникновению таких признаков, ранжируются по величине оценки условной вероятности возникновения данной комбинации признаков. Каждая последующая стадия принятия решения позволяет характеризовать классифицируемый объект на всё более абстрактном уровне, так как причины предыдущей стадии становятся признаками при переходе к последующей. Синтез таких многостадийных решающих систем в настоящий момент является предметом активных исследований в области методик машинного обучения.

Очень правильным, считаем, предложенную работой Ушакова Игоря из Сан-Диего, США, структуру сил антитеррора и предложение разделять решение задач: для **государственного**, **регионального**, а также **локального** уровней. Он также вывел формулы определения и оптимизации затрат по мероприятиям антитерроризма, что позволило создать **компьютерные модели**, позволяющие рассмотреть более реалистические постановки задач, учесть большее число различных факторов. Ввести векторные характеристики затрат (людские ресурсы, денежные средства, а так же проводить сценарий анализа различных ситуаций). Именно компьютерная модель позволит быстро определять направления «главного удара», основные недостатки технических средств и оперативно принимать организационные меры антитеррора.

В рамках развитой математической модели можно определять роль и основные требования ко всем техническим средствам (в т.ч. отечественного производства), обеспечивающим безопасность граждан во время проведения спортивных мероприятий с массовым пребыванием людей. Например, новые возможности ИСО-«777» в связи с переходом на поддержку новых баз данных (My SQL) — ИСБ «777 Комплекс», нашли подтверждение наших намерений по созданию **Компьютерной модели системы безопасности**.

Необходимо определить комплекс технических средств, для каждого уровня обеспечения антитеррористической защиты:

1. Государственного уровня с его техническими характеристиками.
2. Регионального уровня, учитывая особенности региона.
3. Локального уровня, или объектовые комплексы, которые позволят оперативно и полно выявить задуманное террористами на ранних стадиях.

Работа компании «Сэнс»

В нашей лаборатории «Цифровой рентгенографии» имеется программа научно-технического развития по четырём направлениям:

1. Рентгенографические исследования.
2. Совершенствование детекторной системы.
3. Отработка сканирующей системы.
4. Постоянный поиск новых решений и перспективных направлений.

Все наши поисковые работы мы сосредоточиваем на достижении поставленных задач с целью совершенствования изготавливаемых изделий для достижения максимального эффекта.

При создании антитеррористических комплексов специалисты нашего предприятия уделяют особое внимание снижению дозовой нагрузки на обслуживающий персонал. Сегодня мы разработали и оснастили антитеррористический комплекс КОНСИС защитной кабиной, которая полностью снимает все вопросы. Дозовая нагрузка на оператора КОНСИС соответствует естественному фону и этот факт даёт основание заявлять, что система КОНСИС полностью безопасна для широкого применения в сфере антитеррористической деятельности (См. фото).

Вывод

В настоящее время крайне необходимо перейти к решению более перспективных задач и проектов, повысить актуальность внедряемой техники, провести техническое перевооружение систем антитеррора на республиканских объектах с массовым пребыванием людей. Создать в Республике Беларусь систему, которая обеспечила надёжную защиту населения от террористических актов. Для этого наше предприятие инициирует комплексный подход к решению этой задачи и предлагает следующие первоочередные шаги:

1. Создание компьютерной модели республиканской системы безопасности.
2. Регулярный мониторинг республиканской системы безопасности по трём уровням.
3. Проводить периодические встречи всех участников проектных и поисковых работ этого направления.
4. Создать программу обучения специалистов антитеррористических подразделений современным методам противодействия терроризму.
5. Создать современный учебно-тренировочный комплекс на базе Военной Академии с привлечением специалистов СНГ для совершенствования навыков противодействия терроризму.

УП «Дизайн-студия СЭНС»
220026, г. Минск, пер. Бехтерева, 8, к.365, 366
Тел.: (017) 346-88-90, 346-84-54,
Факс: (017) 346-88-91
E-mail: sens@mail.bn.by
Сайт: www.belsens.com

Обеспечение комплексной безопасности критически важных объектов информатизации

Маликов Владимир Викторович, начальник цикла технических и специальных дисциплин УО «Учебный центр Департамента охраны» МВД Республики Беларусь, майор милиции, кандидат технических наук.

В настоящее время обеспечение комплексной защиты критически важных объектов информатизации (КВОИ) является одной из приоритетных задач современного общества.

Данная проблема приобретает сегодня особую значимость и для Республики Беларусь в связи с необходимостью разработки и внедрения современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Согласно п. 14 Концепции национальной безопасности Республики Беларусь: обеспечение надежности и устойчивости функционирования КВОИ является одним из основных национальных интересов в информационной сфере Республики Беларусь.

Следует отметить то, что публикуемые в открытых источниках информации материалы по методикам создания и функционирования КВОИ имеют общий характер, а почти все статистические данные по безопасности данных объектов являются закрытыми. Однако, учитывая то, что функционирование КВОИ осуществляется в рамках единого административно-территориального и экономического пространства государства, то можно предположить для указанных объектов в той или иной мере будут применимы общие подходы по выделению данных, связанных с построением их информационной и инженерно-технической защиты.

Основу современных систем обеспечения информационной и инженерно-технической защиты КВОИ от несанкционированного доступа составляют нормативно-правовые и организационно-технические методы защиты информации, позволяющие сформировать необходимое нормативное и организационное обеспечение для организации инфраструктуры таких систем, а также реализовать поддержку принятия соответствующих управленческих решений в вопросах безопасности объектов.

В настоящее время на территории стран СНГ идет активный процесс по формированию национального нормативно-правового обеспечения в области защиты КВОИ от несанкционированного доступа. Однако, принятые (разрабатываемые) нормативно-правовые акты в большинстве случаев носят ведомственный характер, что приводит к снижению эффективности взаимодействия между различными органами управления и ведомствами, так как при наличии их большого количества уровень и качество связей остается низким. Также следует отметить, что в области информационного права остро стоят вопросы о развитии и применении международного законодательства, международного частного права, гармонизации правовых норм. Данные проблемы также особенно актуальны для национального законодательства стран СНГ.

Одним из основных принципов противодействия угрозам безопасности КВОИ будем считать превентивность принимаемых мер защиты, так как устранение последствий проявления угроз требует значительных финансовых, временных и материальных затрат.

С учетом того, что в системах защиты КВОИ используются аппаратно-программные средства охраны, существуют угрозы, связанные с возможным внедрением в изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия, а также программного обеспечения, нарушающего функционирование системы защиты. Анализ организационно-технического обеспечения при построении систем защиты КВОИ позволяет определить комплекс мероприятий по их защите на стадии проектирования системы, обеспечив оптимальное сочетание организационных и технических мер защиты информации.

Обеспечение комплексной безопасности КВОИ неразрывно связано с инженерно-техническими средствами и системами защиты, позволяющими обеспечить защиту от несанкционированного физического доступа к объекту / ресурсам объекта. Причинами возникновения угроз инженерно-технической защите КВОИ могут быть действия человека, форс-мажорные обстоятельства, отказ оборудования и внутренних систем жизнеобеспечения. Однако, основной причиной таких угроз является, как правило, преднамеренное или случайное действие человека (нарушителя). Потенциальный нарушитель для реализации своих замыслов руководствуется определенной мотивацией и намерениями, владеет совокупностью знаний, умений и навыков (способов) совершения противоправных действий.

Продолжение см. стр. 60

Сеть — это платформа

Клименок Илья, инженер-системотехник.
Представительство Cisco Systems Holding BV в Республике Беларусь

Cisco Connected Stadium

Современный стадион — это не просто трибуны, на которых болельщики собираются, чтобы посмотреть на игру любимой команды. Арена, как место проведения различных массовых мероприятий, состоит из множества разнородных инженерных, охранных и коммерческих систем, призванных сделать ее посещение максимально комфотным и безопасным для зрителей, а также максимально прибыльным для организаторов мероприятия.

Неудивительно, что порой за фальшпотолком прячутся километры кабелей — прямо настоящие джунгли коммуникаций. А действительно ли требуется такое количество отдельных линий связи? Есть ли возможность уменьшить их количество, упростить обслуживание и эксплуатацию, снизить капитальные затраты на проектирование и строительство?

Именно над этим и задумалась наша компания. Компания Cisco, являясь одним из пионеров компьютерных сетей и имея огромный опыт в их проектировании и эксплуатации, увидела потенциал локальной вычислительной сети как платформы для коммуникаций систем Арены.

Сеть — это платформа

Так родилась концепция Cisco Connected Stadium. Это набор согласованных технических решений для передачи по единой мультисервисной сети разнородных видов информации — безопасно и надежно. Сеть становится своего рода коммуникационной «платформой» комплекса.

Сеть Арены может использоваться как для организации продажи билетов и сувениров, так и для видеоизображений с камер наблюдения и команд для системы контроля доступа. При этом гарантируется безопасность данных от несанкционированного доступа, а также для каждого вида информации будет применяться свой тип качества обслуживания. Например, информация платежной системы может пройти с небольшой задержкой, но гарантированно не будет утеряна, в то время как данные IP-телефонии допускают утерю небольшого количества пакетов, но должны проходить без задержки. Только интеллектуальная мультисервисная сеть в состоянии правильно распределить свои ресурсы между различными потребителями.

Мультисервисная сеть Cisco Connected WiFi

Мультисервисная сеть состоит из нескольких функциональных блоков. Сюда входят и высокопроизводительное ядро сети, и коммутаторы доступа с высокой плотностью инерфейсов, и выделенный центр обработки данных — мозг системы. Сегодня неотъемлемым компонентом также стала беспроводная технология доступа к сети — WiFi.

Единая сеть Wi-Fi

Назначение и необходимость беспроводной сети на Арене не столь очевидна, ведь посетители приходят в первую очередь посмотреть матч, а не листать странички в Интернете.

В качестве конкретного практического примера посмотрим на эту технологию с другой стороны: давайте представим себя на месте рекламодателя Арены. Лучшая реклама — индивидуальная реклама, а единственным на сегодняшний день индивидуальным устройством, имеющимся у каждого из посетителей, является телефон или смартфон. Иметь возможность показывать рекламу, продавать сувениры online или просто оказывать справочные услуги — это серьезный дополнительный шаг Арены к самоокупаемости. Однако такая «массовость» вызывает и некоторые проблемы. В связи с этим в обозримом будущем распространение Интернета и смартфонов будет создавать все большую нагрузку на мобильные сети. Когда 10-15 тысяч болельщиков со смартфонами придут на стадион, их смартфоны будут создавать настолько большую нагрузку на мобильную сеть, что ухудшение доступа в Интернет будет более чем заметно. Это делает невозможным использование интерактивных сервисов на Арене через мобильную сеть.

Именно поэтому была разработана специальная технология Wi-Fi для «подключенного стадиона» (Cisco Connected Stadium Wi-Fi). Эта высокоскоростная, хорошо масштабируемая безопасная сеть оптимизирована для работы в среде с высокой плотностью абонентов. Она создает новые возможности для бесперебойных мобильных подключений на стадионах и в других местах проведения массовых мероприятий, выводя взаимодействие абонентов на

Сеть это платформа

Единая сеть Wi-Fi

Объединение нескольких отдельных специализированны беспроводных сетей в единую с сохранением виртуального раздедения и соблюдением правил информ-безопасности.

качественно иной уровень и создавая новые возможности для операторов связи и владельцев спортивных сооружений, зачастую используемых и для развлекательных мероприятий.

Cisco Connected Stadium Wi-Fi

Традиционно каждый из беспроводных сервисов использует выделенные точки доступа WiFi, систему управления и т.д., т.е. строится несколько отдельных сетей. Решение Cisco Connected Stadium WiFi сводит отдельные беспроводные сети в одну общую сеть, сохраняя при этом их виртуальное разделение. Логическое разделение сервисов в рамках единой беспроводной сети настолько эффективно и надежно с точки зрения информационной безопасности, что даже удовлетворяет требованиям для платежных систем в торговых точках (PCI for Point of Sale).

Традиционная беспроводная сеть на Аренах и стадионах строилась в первую очередь в технологических целях: для обслуживающего персонала, службы безопасности, торговых точек. В некоторых случаях оставались свободные ресурсы для предоставления сервиса WiFi в VIP-ложах. Для этих задач подходит традиционный метод организации радиопокрытия с небольшим количеством точек доступа, покрывающих обширные площади. Централизованная система управления не является абсолютной необходимостью, могут использоваться всенаправленные антенны.

Такая сеть не может справиться с большим количеством абонентов, предоставлять услугу WiFi всем желающим посетителям в традиционной сети невозможно.

В противоположность традиционной модели WiFi, Cisco Connected Stadium WiFi использует большое количество точек доступа и централизованную систему управления ими. Для исключения интерференции радиосигналов с соседними точками доступа используются направленные антенны и точная автоматизированная настройка мощности излучения.

Использование централизованной модели позволяет реализовать функциональность, абсолютно недостижимую при использовании автономных точек доступа. Например, безопасный роуминг между точками доступа: когда WiFi-клиент перемещается по Арене и переходит из одной зоны радиопокрытия в другую, происходит автоматическая перенастройка точек доступа и проводной мультисервисной сети так, чтобы пользователь в новой зоне радиопокрытия продолжал работать в своей виртуальной сети и его данные не попадали в другие сети.

Централизованный контроллер WiFi принимает информацию о состоянии радиосети от точек доступа и может определить и изолировать радиопомехи — естественные и искусственно созданные злоумышленником. При этом контроллер либо меняет частотный канал, либо увеличивает мощность точек доступа. В случае отказа одной или нескольких точек доступа контроллер может восстановить покрытие сети, увеличив мощность соседних точек доступа.

Для того чтобы упростить управление единой беспроводной сетью, дать возможность управлять ею не только высококвалифицированным инженерам, но и сотрудникам Арены, мы разработали специальное программное обеспечение с интуитивно понятным интерфейсом — Cisco WCS. Оно позволяет не только контролировать состояние сети, но и вносить незначительные корректировки в настройки, а также дает возможность в реальном масштабе времени отслеживать физическое положение всех WiFi-клиентов.

Система управления

Таким образом, высоконадежная беспроводная сеть, построенная по технологии Cisco Connected WiFi, может стать непосредственным продолжением проводной мультисервисной сети и обеспечить платформу мобильным устройствам и системам. ■

Представительство Cisco Systems Holding BV в Республике Беларусь
220034, г.Минск, ул. Платонова, 1Б, Бизнес-центр «Виктория Плаза»
E-mail: pburba@cisco.com
Сайт: www.cisco.com

Внедрение DLP-решений для КВО

Барановский Александр, директор ООО «НПТ»

Справка ТБ

Барановский Александр Валерьевич, окончил БГУИР, ФИТУ в 2000 г. После службы в пограничных войсках РБ занимал руководящие должности в ряде коммерческих организаций. С 2009 г. — директор компании «НПТ», эксперт по информационной безопасности. Автор ряда публикаций и исследований.

Сегодня мы поговорим о DLP-системах. Это класс программного обеспечения, имеющий наибольшую важность для обеспечения информационной безопасности. Сегодня многие компании и государственные организации приобретают DLP-системы для защиты своих данных. К сожалению, далеко не все специалисты по безопасности знакомы с DLP-системами, поэтому необходимо рассказать о них вкратце, прежде чем переходить к практике.

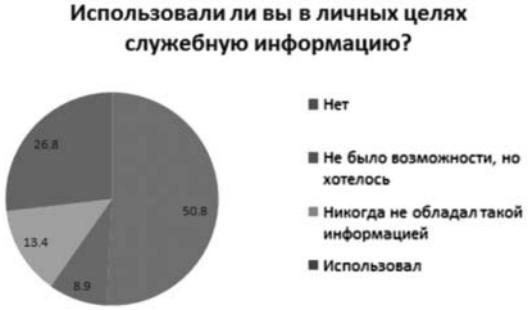
Согласно нашему исследованию, около 9-10% рабочего времени в коммерческих организациях и банках сотрудники тратят на занятия, не связанные с работой (социальные сети, «аська», просмотр фильмов и т.п.). В государственных предприятиях — уже около 19%. Лидером являются проектные организации — там такой вид активности занимает 36% рабочего времени.

Еще одна проблема заключается в том, что сотрудники используют ресурсы предприятия, дорогой лицензионный софт, плоттеры и т.п., делают «левые» проекты, что несет за собой финансовый ущерб для организации. Понятно, что мириться с этим нельзя, однако и на этом сложности не заканчиваются. Следует отметить также проблему передачи сотрудниками конфиденциальной информации за пределы организации (утечка информации). На сегодня существует много каналов потери информации. В первую очередь, это:

1) электронная почта;

2) клиенты для мгновенного обмена сообщениями (ICQ, MSN Messenger, QIP, Jabber);

3) Skype, который считается наиболее защищенным, и в основном все непубличные беседы происходят именно в нем;



Опрос пользователей

4) информация в виде файлов может быть передана по FTP-протоколу;

5) запись на съемный носитель (USB-флешку или CD/DVD диски);

6) распечатка на принтере.

Зачастую компании выбирают методологию запрета каких-то определенных способов, минимизируют количество каналов потенциальной утечки информации. Например, запрещают использовать флэшки, ICQ и т.д. Создается иллюзия безопасности, на самом же деле это недостаточно эффективное решение. Дело в том, что при подобных запретах сотрудник теряет мобильность. Чтобы передать необходимые документы на USB-носителе, сотруднику необходимо обратиться в службу безопасности, которая откроет порт и даст добро на запись документов. Это потеря рабочего времени, и в масштабах организации потери будут достаточно заметными.

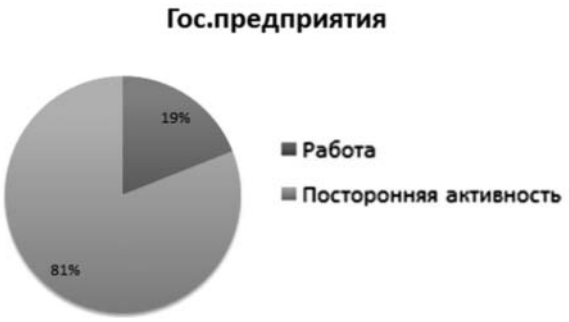
Использование рабочего времени сотрудниками в банках

Гораздо эффективнее позволить сотруднику пользоваться привычными и удобными для него способами передачи информации, при этом контролировать данный процесс. Перехват информации никакой сложности сегодня не представляет, для этого существует ряд бесплатных программ. Но производить поиск в больших объемах весьма проблематично, для этого нужен качественный аналитический модуль. Причем из-за необходимости обработки неструктурированной информации простой «поиск по словам» не подходит, иногда нужен поиск похожего, возможность поменять слова местами. В таком случае необходимо обратиться в компании, хорошо зарекомендовавшие себя на рынке корпоративного поиска.

Очень важным аспектом анализа перехваченных данных являются *синонимические ряды*. Можно по общению двух людей понять, о чем идет речь, даже если говорят они иносказательно. Например, с силовыми структурами мы разработали синонимический ряд по получению взятки.

DLP-системы как раз и отличаются от обычных перехватчиков данных (снифферов) тем, что позволяют не только перехватывать, но и анализировать перехваченную информацию. Впрочем, этим их возможности не ограничиваются. Рассмотрим подробнее. Все они в полной мере реализованы в предлагаемом нашей компанией решении — «Контуре информационной безопасности SearchInform».

Интеграция с доменной структурой Windows. С ее помощью достаточно легко определить пользователя, который отправил почту, сообщение, можно определить, какой пользователь и в какое время, с какой рабочей станции, какие ресурсы использовал для отправки любого рода информации. Часто сотрудники пытаются обойти подобные системы. Архивируя почту, ставят на нее пароль, передают информацию в графическом виде. Однако **полноценная DLP-система позволяет отследить этот процесс** и выявить злоумышленника. **DLP-системы дают возможность определить группу риска.** Например, из 10 тысяч сотрудников выбрать 500, которые уже были замечены в нарушениях инфор-



Использование рабочего времени сотрудниками в гос.предприятиях

мационной безопасности. В случае проведения внутреннего расследования легко получить информацию по конкретному сотруднику, посмотреть его активность за заданный промежуток времени.

Модуль электронной почты позволяет происходить перехвату всех протоколов электронной почты, в том числе через Web-интерфейс. Все блоги, форумы, куда сотрудник может написать информацию, также легко контролируются и перехватываются.

FTP-протокол предназначен для передачи данных больших объемов (чертежи, финансовая информация и т.д.). По нему могут происходить наиболее опасные для организации утечки информации, поэтому данный канал необходимо контролировать не менее тщательно, чем ту же электронную почту.

Мы являемся первой компанией на территории СНГ, которая начала перехватывать **Skype**: текстовые сообщения, пересылаемые файлы и голосовые сообщения.

Также поддерживается и стандартный для современных DLP-систем **перехват Интернет-месенджеров и печати**. Есть возможность перевода графической информации в текстовый вид с последующим полнотекстовым поиском. Все, что пишется на съемные устройства, перехватывается, складывается и хранится определенное время.

Модуль **MonitorSniffer** позволяет в режиме реального времени отслеживать одновременно до 16 рабочих столов пользователей. Кроме того, позволяет делать снимки с определенным интервалом времени, своеобразный скриншот. Параллельно безопасник может отслеживать загруженные процессы.

FileSniffer обеспечивает эффективный и оперативный контроль того, кто и каким образом использует хранящуюся на файл-серверах конфиденциальную информацию.

Индексация рабочих станций позволяет отследить появление конфиденциальной информации на компьютерах пользователей, а также любые действия над ней.

ReportCenter позволяет отследить связи между сотрудниками как внутри организации, так и вне ее. Кроме того, позволяет собирать статистику по активности пользователей и инцидентам, связанным с нарушениями политики безопасности, представляя ее в виде отчетов.

В организациях есть сотрудники, которые часто ездят в командировки и берут с собой ноутбук. Опасности подвергается информация, которая в нем находится. **EndpointSniffer** позволяет отследить все те же информационные потоки, которые я перечислял, но уже локально, на отключенной от сети рабочей станции. При подключении обратно в сеть этой рабочей станции происходит пересылка информации в общую базу данных. Также данный модуль позволяет контролировать внешние устройства, перехватывать шифрованные протоколы и Skype.

«Контур информационной безопасности SearchInform» позволяет предупреждать не только заранее спланированные, но и случаные утечки. Например, в банковской сфере часто существует такая проблема. Сотрудник имеет какой-то план работы за день, скажем, оформление 20 заявок на получение кредита. За день он успевает сделать 15, премия же выплачивается при норме 20. Пять оставшихся заявок сотрудник скидывает на свой электронный ящик, без какого-либо злого умысла, дома спокойно завершает работу, утром приносит отчет за предыдущий день. Он не думает о том, что эти заявки могут пройти через несколько бесплатных ресурсов и быть кем угодно перехвачены, либо же утечка может произойти при взломе бесплатного ящика сотрудника. С нашим решением можно отследить такие действия и сотрудников, подобным образом нарушающих должностные инструкции.

Преимущества Контура информационной безопасности:

1. **Простота и скорость внедрения.** Среднее время развертывания системы — около 2-х часов.
2. **Возможность контроля всех каналов передачи информации**, которые существуют на предприятии.
3. **Функция «поиск похожих».** Уникальная функция, которая позволяет искать текст, похожий по смыслу на задаваемый в параметрах. Также отслеживаются случаи перестановки слов или целых абзацев в тексте.
4. **Полная идентификация пользователя.**

Использование рабочего времени сотрудниками в проектных организациях

Вопросы:

– Сейчас развиваются корпоративные сети на основе ноутбуков, нетбуков, беспроводных сетей. Каким образом адаптируются DLP-системы в таких корпоративных сетях?

– На самом деле, для нас нет разницы, по какому принципу построена сеть. Существует как вариант установки через контроль зеркалируемого трафика, так и вариант, когда устанавливается программа-агент на рабочую станцию.

– Как ваша DLP-система будет согласовываться с системой обнаружения/вторжения?

– В случае установки агента необходимо в большинстве случаев наш «Контур» добавлять в доверительные приложения антивирусов, после чего никаких уведомлений появляться не будет.

– Контроль передачи голосовых сообщений Skype и контроль монитора предполагает наличие клиентской части. В случае использования клиентом технологии «Tor» ваш шлюз зафиксирует, какие ресурсы пользователь посещает?

– В этом случае будет зафиксирована передаваемая информация и указано, кем реализовано действие. Какие ресурсы посещались, мы не отслеживаем, нам важна информация, которая передается, в том числе и по технологии TOP. Кстати, наше решение является единственным из DLP, которое позволяет полноценно контролировать информационные потоки при использовании терминальных решений.

– Авторизация в Skype происходит…

– По имени. Есть привязка — какой пользователь, с какого компьютера и в какое время авторизировался.

– Под какой платформой вы работаете?

– Под Windows.

– Какова стоимость системы?

– Весь комплект модулей — из расчета 4 млн за 1 рабочее место. Но ненужные для организации модули можно убрать, что значительно сократит стоимость.

ООО «НПТ»
220012, г. Минск, ул. К.Чорного, 5А, пом.5а
Тел.: (029) 649-77-79
E-mail: ab@searchinform.ru
Сайт: www.searchinform.ru

ВирусБлокАда

Анализ вирусной активности за 2011 год

Александр Изотов,
вирусный аналитик
ООО «ВирусБлокАда»

Справка ТБ

Александр Изотов, выпускник Белорусского государственного университета (факультет Радиофизики и компьютерных технологий), вирусный аналитик компании «ВирусБлокАда» с 2010 года.

Антивирусная лаборатория компании «ВирусБлокАда» проанализировала вирусную активность за 2011 год на основе обращений в службу технической поддержки компании.

На основе полученной информации можно выделить следующие тенденции 2011 года:

1) использование социальной инженерии;
2) отклик на мировые события;
3) использование уязвимостей;
4) появление специализированных угроз;
5) развитие технологий сокрытия.

Наиболее популярной тенденцией является использование социальной инженерии, которая базируется на незнании основ информационной безопасности. Это явление широко распространено в Интернете для получения конфиденциальной информации или информации, которая представляет большую ценность. Для злоумышленника становится гораздо проще хитростью выудить информацию из системы, чем взломать ее. В связи с этим в 2011 году появилось большое количество вредоносных программ, которые реализуют принципы социальной инженерии.

• В очередной раз заставил обратить на себя внимание **Trojan.Winlock**, блокирующий работу ОС Windows. Следует заметить, что семейство Trojan.Winlock существует еще с 2007 года. Лето 2011 года ознаменовалось появлением «национального» экземпляра Trojan.Winlock, ориентированного на белорусских пользователей Windows и требующего у них перечислить злоумышленникам некоторую сумму в белорусских рублях на электронный кошелек WebMoney. Главные причины широкого распространения этой угрозы — невнимательность либо некомпетентность пользователей, оказывающихся жертвами вымогателей.

• Наблюдалась и активность **ArchSMS** (фальшивого самораспаковывающегося архива). Как правило, вредоносная программа загружается пользователем из сети Интернет под видом самораспаковывающегося архива (исполняемого файла), содержащего требуемый пользователю файл. Пользователь, запустив исполняемый файл, наблюдает на мониторе процесс, похожий на распаковку. Но в определенный момент «распаковка» останавливается, появляется сообщение о том, что для окончания распаковки архива необходимо отправить с мобильного телефона платное SMS-сообщение. При этом размер самого файла близок к «оригиналу» запрашиваемой информации.

• С середины 2011 года наблюдалось значительное уменьшение количества фальшивых антивирусов (**FakeAV**), программ, которые находят на компьютере пользователя множество несуществующих вирусов и для «чистки» машины предлагают активировать себя через SMS на определенный номер. Количество фальшивых антивирусов постепенно начало переходить в качество. Отдельные вирусописатели организуют кибергруппы и пишут уже меньшее количество фальшивых антивирусов, но пытаются сделать их более совершенными — более подобными на настоящие, чтобы пользователь, который незнаком с особенностями работы реальных антивирусов, попадался на данные уловки.

Следующей значимой тенденцией является отклик на мировые события. Спамеры традиционно используют интерес пользователей к событиям, имеющим широкий общественный резонанс, в своих корыстных целях. И последние месяцы 2011 года также не стали исключением. Так, после смерти 5 октября основателя компании Apple Стива Джобса мошенники распространяли информацию о бесплатных устройствах iPad «в память о Стиве Джобсе». Пройдя по ссылке, предложенной злоумышленниками, пользователей перенаправлялись на вредоносные сайты.

Использование уязвимостей является одной из самых динамичных тенденций. Новым направлением стало активное использование злоумышленниками уязвимостей платформы Java, являющейся самым слабым элементом в защите операционных систем, на которых она установлена. В этом году хакеры, как и в предыдущие годы, активно использовали уязвимости в веб-приложениях, в IIS, MS SQL, а также системах обработки файлов и сервисах сообщений операционной системы.

Еще одной тенденцией являются специализированные угрозы, цель которых — проведение шпионажа. В конце 2011 года отмечено много ярких примеров данного направления.

• В октябре появились сообщения о повышенной активности червя **Duqu**, который имеет сходство с компьютерным червем **Stuxnet** (впервые обнаруженным компанией «ВирусБлокАда» летом прошлого года). Главная задача Duqu — сбор конфиденциальных данных об имеющемся на предприятии оборудовании и системах, используемых для управления производственным циклом. Это может быть любая информация, которая пригодится при организации нападения: снимки с экрана, журналы нажатых клавиш, список запущенных процессов, данные учетных записей пользователей, названия открытых окон, сетевая информация, сведения о домене, имена дисков, файлов и пр.

• Также в октябре была обнаружена программа **Bundestrojaner**, которая по своей природе аналогична вирусу, следит за Интернет-браузером и такими программами, как Skype, электронная почта и чаты. Немецкие госслужбы использовали эту шпионскую программу около 100 раз, заявил представитель фракции ХДС-ХСС в парламенте Германии Ганс-Петер Уль в интервью Neue Osnabruecker Zeitung. Программа может делать снимки с экрана, которые в немецких судах рассматриваются в качестве доказательств. Помимо прослушки телефонных разговоров и слежки за пе-

Продолжение см. стр. 57

Защищаем сайты

Виктор Кобзарев,
системный администратор
УП «Надежные программы»

Утечка информации, некорректное функционирование сайта, испорченная репутация… История насчитывает миллионы печальных примеров проникновения на веб-ресурсы. Подбор паролей или расщепление HTTP-запроса — да мало ли какой способ атаки изберет злоумышленник.

Справка ТБ

Виктор Кобзарев. В 2005 году окончил Белорусский государственный университет информатики и радиоэлектроники, специальность — инженер по автоматическому управлению в технических системах. Опыт работы: 2005-2006 гг. — ОАО «Пеленг», инженер по автоматическому управлению; 2006-2009 гг. — Белтелерадиокомпания, ведущий инженер-программист; с 2009 по настоящее время — УП «Надежные программы», системный администратор.

Способов много, а причина уязвимости одна — недостаточная защищенность. Путь к минимизации рисков — защищенный хостинг. Все вы прекрасно знаете, что для функционирования сайта, кроме доменного имени (названия сайта), необходима услуга хостинга. Виртуальный хостинг (shared), VPS (Virtual Private Server), Colocation — каждый заказчик может выбрать приемлемый по цене и производительности вид услуги.

Время от времени веб-ресурсы клиентов подвергаются атакам. Сегодня одним из самых популярных сайтов, предоставляющих информацию о том, какие веб-приложения уже подверглись атаке, является www.stopbadware.org. Сайт бесплатный, его поддерживают такие крупные компании, как Google и Firefox.

Начало см. стр. 56

перепиской, на зараженном компьютере можно дистанционно включить микрофон или веб-камеру. Таким образом, полиция способна прослушать и увидеть, что происходит в помещении, где стоит ПК. Данные события представляют собой примеры промышленного и правительственного шпионажа.

За 2011 год соотношение вредоносного ПО выглядит следующим образом:

Наибольший объем (44%) занимает Trojan. BackDoor/Downloader/Dropper, Trojan.Injector и т.д. Они имеют различные технологии внедрения и существования в ОС. Следующей крупной группой, составляющих 38 %, являются FraudTool (мошеннические программы). Это те виды вредоносных программ, к которым относятся фальшивые антивирусы, трояны, блокирующие работу систем (FakeAV, ArchSMS, Winlock , Ransom Encoder, Trojan.Cidox). Крупной группой, занимающей 9 % от общего количества вредоносных программ, является **Adware**. Adware — это программное обеспечение, содержащее рекламу или же предназначенное для показа рекламных сообщений. В большинстве случаев Adware скрытно инсталлируется в систему с какой-нибудь бесплатной или условно бесплатной программой, после чего удалить его, как правило, не представляется возможным, так как Adware-модуль маскируется в системе, используя технологии, близкие к вредоносному ПО. Базовое назначение Adware — это неявный метод оплаты использования бесплатного программного обеспечения, рекламодатели платят за показ их рекламы рекламному агентству, рекламное агентство — разработчикам Adware-программ. Доля сетевых червей составляет около 5 %. В 2011 г. мошеннические программы, трояны и Adware имели положительную динамику. Соответственно, из-за их роста объем всех остальных вредоносных программ в этот период сокращался.

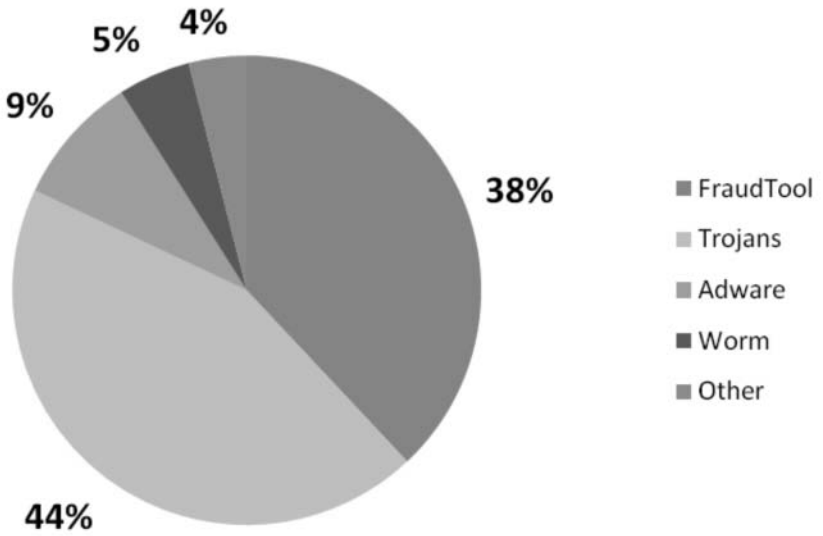


Рисунок 1. Распределение вредоносных программ по типам

Таким образом, на основе анализа вирусной активности в 2011 году можно сделать некоторые выводы. Динамика роста вредоносных программ остается постоянной, можно наблюдать устойчивость тенденций еще с 2010 г. Вирусы и трояны усложняются, увеличивается масштаб их распространения, а также скорость, с которой они поражают компьютеры пользователей. В 2011 году, как и прогнозировалось, увеличилось число угроз, работающих на 64-битных платформах. Люди, как и прежде, остаются самым уязвимым звеном в обеспечении информационной безопасности. ■

Белорусская антивирусная компания «ВирусБлокАда»
220088, г.Минск, ул. Смоленская, 15 - 803б
Тел.: (+375 17) 294-84-29 (коммерческий отдел),
290-59-29 (технический отдел)
E-mail: info@anti-virus.by
Сайт: www.anti-virus.by

Сейчас в базе данных stopbadware находится около миллиона зараженных ссылок, и это число постоянно увеличивается. Именно поэтому клиенты, желающие свести к минимуму нежелательные последствия вторжения злоумышленников, выбирают защищенный хостинг.

Атаки на сайты

Различают следующие виды атак:

1. **Аутентификация**. Данный вид атак направлен на используемые Web-приложением методы проверки идентификатора пользователя, службы или приложения. Аутентификация использует как минимум один из трех механизмов (факторов): «что-то, что мы имеем», «что-то, что мы знаем» или «что-то, что мы есть». Эти атаки направлены на обход или эксплуатацию уязвимостей в механизмах реализации аутентификации Web-серверов.

2. **Авторизация**. Данный вид атак направлен на методы, которые используются Web-сервером для определения, имеет ли пользователь, служба или приложение необходимые для совершения действия разрешения. Многие Web-сайты разрешают доступ к некоторому содержимому или функциям приложения только определенным пользователям. Доступ другим пользователям должен быть ограничен. Используя различные техники, злоумышленник может повысить свои привилегии и получить доступ к защищенным ресурсам.

3. **Атаки на клиентов**. Открыв сайт, вы хотите получить доступ к какому-то сервису или информации. Во время посещения сайта между пользователем и сервером устанавливаются доверительные отношения — как в технологическом, так и в психологическом аспектах. Пользователь ожидает, что сайт предоставит ему легитимное содержимое. Кроме того, пользователь не ожидает атак со стороны сайта. Пользуясь этим доверием, злоумышленник может прибегать к различным методам проведения атак на клиентов сервера.

4. **Выполнение кода**. Этот вид атак направлен на выполнение кода на Web-сервере. Все серверы используют данные, переданные пользователем при обработке запросов. Часто эти данные используются при составлении команд, применяемых для генерации динамического содержимого. Если при разработке не учитываются требования безопасности, злоумышленник получает возможность модифицировать исполняемые команды. Внедрение серверных сценариев — это внедрение какого-либо вредоносного кода, который выполнится на сервере в запущенном веб-приложении. Так как оно запускается с правами и привилегиями полноценного пользователя, вы можете столкнуться с очень большими проблемами.

5. **Разглашение информации**. Данный вид атак подразумевает, что злоумышленник любыми способами будет пытаться получить информацию о ваших сервисах. В частности, это идентификация приложений: мы получаем версию ПО веб-сервера, язык и, соответственно, можем узнать текущие уязвимости сайта. Еще одна из угроз — утечка информации. Например, в Беларуси в комментарии java-скрипта, т.е. кода, который выполняется на стороне клиента, находилась информация о том, как программист писал данный код. Это дополнительная информация и ею можно воспользоваться.

6. **Логические атаки**. Данный вид атак подразумевает следующее: злоумышленник представляет себе логику вашего приложения и будет стараться использовать ее в своих корыстных целях. Самый простой пример — отказ в обслуживании, когда вы нагружаете сервер запросами.

Защищенный хостинг: для кого-то он обязателен?

Этот тип хостинга необходим, прежде всего, государственным органам и организациям, которые используют в своей деятельности сведения, составляющие государственные секреты.

Для решения проблемы конфиденциальности достаточно давно была предложена идея размещения сайтов таким образом, чтобы вероятность атак была минимальной. В 2010 г. ОАЦ при Президенте РБ от слов перешел к конкретным действиям: была создана документация, описывающая требования к защищенному хостингу. Одно из положений Указа № 60, направленного на улучшение работоспособности нашего Интернета в целом, говорит: если вы являетесь государственной организацией и ваша работа связана с использованием государственных секретов, вы обязаны размещать сайт на защищенном хостинге. Таким образом, чтобы минимизировать угрозы безопасности данных, все серьезные организации (банки, крупные коммерческие организации) должны перейти на защищенный хостинг.

Переход на защищенный хостинг

Во-первых, для перехода на защищенный хостинг необходимо определиться с типом размещения. Выделяют три типа размещения: виртуально-защищенный сервер, виртуальный (shared) хостинг и выделенный сервер, который находится на защищенной площадке.

На виртуальном хостинге разрешено размещать только сертифицированные системы управления сайтом. На данный момент их также три:

1. СУС «CMS DEW POWER» (ОАО «Гипросвязь»);

2. SectorCMS 1.4. (РУП «Белтелеком»);

3. Программные средства управления сайтом (разработка Центра информационных ресурсов и коммуникаций БГУ).

Если сайт использует любые другие программные решения (в т.ч. собственной разработки), либо проект имеет повышенные требования к ресурсам сервера — необходимо размещать его исключительно на выделенном сервере.

На данный момент существуют 7 организаций, которые уполномочены представлять услуги защищенного хостинга:

1. Научно-производственное частное унитарное предприятие «Надежные программы».

2. Государственное учреждение «Главное хозяйственное управление» Управления делами Президента Республики Беларусь.

3. Государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси».

4. Белорусско-английское совместное предприятие общество с ограниченной ответственностью «Деловая сеть».

5. Республиканское унитарное предприятие электросвязи «Белтелеком».

6. Закрытое акционерное общество «ГЛОБАЛВАНБЕЛ».

7. Общество с ограниченной ответственностью «АйПи ТелКом».

Эти организации полностью прошли процедуру регистрации и включены в реестр ОАЦ при Президенте Республики Беларусь для предоставления такого типа услуг.

Обязанности заказчика:

- Сайт должен принадлежать национальной доменной зоне Республики Беларусь — .by. Исключение составляют 2 зоны, которыми занимается ОАЦ при Президенте Республики Беларусь, — .gov.by и .mil.by (использовать домен в этой зоне можно только с разрешения ОАЦ).
- Сообщить поставщику услуг данные администратора ресурса.

• Сообщить IP-адреса, откуда будет администрироваться ресурс.

• Выбрать протоколы транспортного уровня, по которым будет осуществляться доступ к ресурсу, и сообщить их поставщику услуг.

• Предоставить данные для регистрации ресурса в БелГИЭ.

• Незамедлительно устранять выявленные нарушения безопасности сайта, если хостинг-провайдер не может их устранить собственными силами.

Обязанности поставщика услуг:

• Фильтровать трафик от вредоносного программного обеспечения.

• Обеспечивать бесперебойное электропитание используемого оборудования.

• Размещать сайт заказчика на оборудовании, находящемся на территории Республики Беларусь.

• Осуществлять мониторинг работоспособности Интернет-сайта, серверов, средств защиты информации с постоянным оповещением администратора безопасности о нарушениях функционирования системы защиты информации.

• Незамедлительно устранять выявленные нарушения безопасности Интернет-сайтов. При невозможности их устранения собственными силами в течение одного дня информировать ОАЦ и администраторов соответствующих Интернет-сайтов.

• Применять сертифицированные средства защиты информации.

• Обеспечивать ежедневное обновление используемого для оказания Интернет-услуг программного обеспечения.

• Предоставлять доступ государственным органам и организациям к сетям общего пользования только по портам протоколов транспортного уровня, определенным договором на оказание Интернет-услуг.

• Обеспечивать синхронизацию системного времени на серверном оборудовании от службы единого времени белорусского государственного института метрологии.

Защищенный хостинг: как он работает?

На защищенном хостинге реализована защита от угроз и атак, о которых мы говорили в начале статьи. Она достигается следующими средствами:

• Межсетевое экранирование аппаратными средствами.

• Защита целостности ресурса (дефейс, фишинг, взлом).

• Ограничение административного доступа.

• Анализ поступающих запросов на уровне http-протокола.

• Защита от DDoS-атак.

• Использование оборудования премиум-класса.

• Сертифицированные ОАЦ средства защиты информации.

• Система аудита и протоколирования событий безопасности ресурса.

• Постоянное резервное копирование.

• Круглосуточный мониторинг.

• Защищенная почта (шифрование SSL и ограничение по IP-адресу).

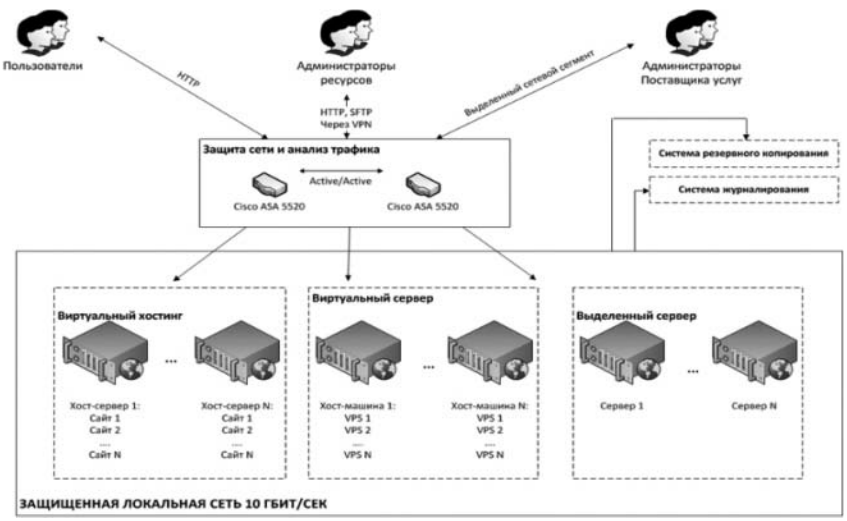
• Тестирование защищенности ресурса (компания BelSoft).

Для предоставления услуг используется оборудование премиум-класса — HP BladeSystems C7000. Это очень качественное аппаратное решение на сегодняшний день.

Фильтрация трафика осуществляется оборудованием Cisco ASA5520. Это оборудование сертифицировано в ОАЦ. Оно осуществляет глубокий анализ поступающего трафика и обнаруживает вредоносный код, защищает от DDoS-атак, обеспечивает функционирование защищенной зоны с доступом по протоколу L2TP over IPSec с поддержкой шифрования AES. Кроме того, происходит полное резервирование оборудования.

Наша компания (hoster.by) предлагает 3 типа услуг защищенного хостинга: виртуально-защищенный сервер, виртуальный (shared) хостинг и выделенный сервер. Существует три типа доступа к серверам, каждый из которых осуществляется по защищенному протоколу для административной части ресурса. Обычные пользователи не видят внутреннюю сеть этих ресурсов, получается, что серверы полностью разграничены логически. Внутри работают серверы, и эта сеть изолирована с помощью Cisco ASA5520 от внешнего мира. У нас есть свой сегмент сети, и мы осуществляем администрирование ресурсов только из него. Администраторы ресурсов имеют доступ к своей административной части только с определенных IP-адресов, поэтому, чтобы взломать такую систему, злоумышленнику необходимо знать IP-адрес владельца ресурса. По-другому не получится.

Наша компания заинтересована в оказании клиентам действительно качественных услуг хостинга. Мы всегда идем навстречу своим пользователям, оказываем помощь в переносе сайта на защищенную площадку при отсутствии у клиента собственных специалистов. ■



УП «Надежные программы» (hoster.by)
220005, г. Минск, ул. В.Хоружей, 1А, 6 этаж
Тел.: +375 17 239-57-02,
velcom: +375 29 3-4444-83,
МТС: +375 29 776-44-83,
life: +375 25 720-52-66,
факс +375 17 239-57-20
info@hoster.by

Начало см. стр. 51

Следует отметить, что факты практической реализации угроз инженерно-технической защите КВОИ, связанные с несанкционированным физическим доступом к объекту / ресурсам объекта, как правило, направлены на нарушение свойств целостности, доступности и конфиденциальности средств и систем обработки информации, каналов телекоммуникации таких объектов.

На основании изложенного выше, современные системы обеспечения безопасности КВОИ, как правило, представляют собой многоуровневые, территориально распределенные, автоматизированные информационные системы, осуществляющие мониторинг состояния безопасности, как отдельных объектов, так и их территориально-административных объединений. Основу построения таких систем составляют аппаратно-программные средства и методы обеспечения комплексной безопасности КВОИ, задачей которых является практическая реализация информационной и инженерно-технической защиты с учетом специфики возникающих угроз. В свою очередь основой аппаратно-программных средств и методов обеспечения информационной и инженерно-технической безопасности являются:

1. Технологии передачи данных.
2. Программное обеспечение средств и систем защиты.
3. Аппаратно-программные средства и системы защиты информации.
4. Интегрированные системы технических средств охраны.
5. Автоматизированные системы передачи извещений.
6. Системы управления рисками.

Очевидно, что системы обеспечения комплексной безопасности КВОИ должны проектироваться с учетом принципов равнопрочности средств защиты, согласованности критериев безопасности и информационного единства.

Основные направления исследований по совершенствованию комплексной безопасности КВОИ.

1. Разработанные системы защиты и управления рисками для КВОИ по нормативно-правовым, организационно-техническим и физическим факторам имеют множество недостатков и уязвимостей, а также значительную (во многих случаях избыточную) стоимость и низкую функциональность. Необходимо формирование нового системообразующего документа для реализации комплексного подхода в области безопасности КВОИ для решения проблем согласованного взаимодействия заинтересованных структур, централизации управления при обеспечении защиты КВОИ.

2. Имеющаяся классификация КВОИ не имеет категорирования по признакам информационной и инженерно-технической безопасности с учетом особенностей доступа. Существующие критерии не учитывают в полном объеме вопросы организационной структуры управления объектом, функционально-экономического организацию процесса деятельности объекта, оценки риска. Необходимо проведение классификации угроз безопасности не только для защищаемого КВОИ, но и для системы защиты с учетом жизненного цикла последней.

3. При использовании технологий передачи данных в системах защиты необходимо учитывать как категорию защищаемого объекта, так и пропускную способность каналов связи, параметры их надежности и помехоустойчивости. Существующие в настоящее время аппаратно-программные системы защиты информации и инженерно-технической безопасности КВОИ имеют низкий уровень унификации, проблему совместимости используемых средств безопасности при работе с различными системами защиты объектов.

4. Существующие методы оценки эффективности систем защиты КВОИ не позволяют проводить полный анализ и динамическую коррекцию результатов оценки.

5. Эксплуатируемые в рамках СПИ средства и системы охраны обеспечивают отражение только части программно-технических и физических угроз КВОИ и, в целом, не всегда отвечает современным требованиям к комплексным системам защиты объектов. ■

Президент Республики Беларусь Александр Лукашенко 25 октября 2011 года подписал Указ № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»

Согласно Указу создается Государственный реестр критически важных объектов информатизации (далее — КВОИ).

Указом также утверждено Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации, согласно которому отнесение объекта информатизации к критически важным объектам информатизации осуществляется на основании отраслевых критериев и с учетом уровня ущерба национальным интересам в политической, экономической, социальной, информационной, экологической и иных сферах, причинение которого возможно в случае возникновения угроз различного характера в отношении объекта информатизации (его составляющих элементов).

Обеспечение безопасности КВОИ включает комплекс мероприятий по созданию системы безопасности КВОИ правового, организационного и технического характера, в том числе по мониторингу угроз безопасности КВОИ и принятию мер реагирования на угрозы безопасности КВОИ. ■

http://oac.gov.by/news/26.html

Интервью с регуляторами, комментарии специалистов планируются в следующих номерах журнала «Технологии безопасности»

Система комплексной безопасности административно-торгового центра по ул. Машиностроителей в г. Минске

Место реализации проекта: г. Минск, ул. Машиностроителей 29.

Время осуществления: 2011 г.

Задача: Система комплексной безопасности административно-торгового центра по ул. Машиностроителей — это совокупность программно-аппаратных средств систем сетевого видеонаблюдения и контроля доступа.

Система видеонаблюдения обеспечивает контроль въезда/выезда автотранспорта с распознаванием номеров, оперативный визуальный контроль входов в здание, лестничного и лифтового пространства, служебных и гостевых парковок. Система осуществляет круглосуточную запись видеоизображений в архив.

Автоматические шлагбаумы служат для разграничения доступа автотранспорта к служебной парковке и складским помещениям.

Поставленное оборудование: Сетевые камеры Mobotix, сетевой видеорегистратор NUUO, шлагбаумы QUIKO, устройство радиоуправления, радиобрелки, специализированное программное обеспечение.

Возможности системы:

- Установлены видеокамеры Mobotix высокого разрешения 3,1 Мп (2048x1536) со скоростью записи 30 кадров/сек.
- Съемка всего помещения без мертвых зон (угол обзора 180С), что позволило уменьшить количество камер и снизить затраты. Новая функция панорамирования дает возможность получить обзор в 180С в виде широкоформатного изображения высокого разрешения.
- Диапазон рабочих температур камер от -30 до +60С, что позволяет обходиться без систем нагрева или охлаждения.
- Сетевой видеорегистратор (16 видео/аудиоканалов) дает возможность создавать архив видео до 8 ТБайт(RAID 0), поддерживает RAID 0, 1, 5, 10.
- В комплект входит программное обеспечение с пожизненной поддержкой.

Название предприятия, предоставившего описание: ОДО «Сфератрэйд» ■

Система видеонаблюдения ОАО «Белтрансгаз»

Место реализации проекта: ОАО «Белтрансгаз», г. Минск

Время осуществления: 2010–2011 гг.

Задачи: круглосуточное видеонаблюдение за прилегающей территорией; контроль безопасности объекта и оповещение о ситуациях; визуальное отслеживание событий на объекте; управление PTZ-камерами; запись и хранения архива; возможность управления системой по локальной сети.

Выполненные работы:

поставка оборудования, монтажные и пусконаладочные работы системы видеонаблюдения.

Поставленное оборудование:

видеорегистраторы, поворотные и стационарные камеры, специализированное программное обеспечение, мониторы, производства компании EverFocus Electronics (Тайвань).

Возможности (структура) системы:

Камеры с режимом работы День/Ночь; PTZ-камеры с 36-кратным оптическим зумом. Цифровая запись видеоизображения со скоростью 25 кадров в секунду; управление PTZ-камерами; детектирование движения; удаленный просмотр и управление по сети Ethernet.

Название предприятия, предоставившего описание:

СООО «Сатурн-Инфо». ■

Новинки рынка

Цифровой видеорегистратор AM-DVR2032

Торговая марка: Axiom
Поставщик: ОДО «Сфератрэйд»
Назначение:
Видеорегистратор предназначен для работы в составе цифровой системы видеонаблюдения для сбора, записи, хранения с последующим просмотром в различных режимах видеоизображения.
Особенности:
Конструктивно цифровой видеорегистратор выполнен в виде моноблока, который может быть установлен самостоятельно. На фронтальной панели прибора расположены кнопки управления, разъем USB для резервного копирования. Мониторинг в реальном времени. Пентаплексный режим работы. Работа по сети с помощью ПО удаленного клиентского места. Управление посредством USB мыши, с передней панели или ИК-пульта дистанционного управления (в комплекте).
Технические характеристики: видеовход, 1В/75 Ом BNC 32; пентаплекс; 1xBNC, 1xVGA, 1xHDMI; NTSC, PAL; H-264; 704x576, 704x288, 352x288; 400 (720x576) / 400 (720x288) / 400 (360x288); режимы записи: постоянный / по тревоге / детекции движения/ по расписанию; аудио входы/выходы RCA 16/2; блокировка клавиш; тревожный вход/выход 16/4; запись тревожных событий до 1000; управление PTZ (интерфейс RS-485); 220 В; рабочая температура 5~40ºС; температура хранения 0~40ºС; влажность менее 90%; 422x438x92 мм; 5 кг (без жесткого диска).
Время появления на рынке: 3 квартал 2011 г.

Извещатель охранный оптико-электронный радиоканальный ИО40910-2/1«Фотон-12-РК»

Производитель: Риэлта, РФ

Поставщик: ОДО «Сфератрэйд»
Назначение:
Извещатель охранный оптико-электронный радиоканальный ИО40910-2/1 «Фотон -12-РК» предназначен для обнаружения проникновения в охраняемое пространство закрытого помещения с последующей выдачей извещения путем дистанционной беспроводной передачи закодированных идентифицируемых сигналов (сообщений) по двунаправленному каналу связи в диапазоне частот от 433,05 до 434,79 МГц.
Особенности:
Чувствительный элемент — двухплощадный пироприемник; защита от проникновения насекомых к пироприемнику; индикатор для визуального контроля работы извещателя; температурная компенсация обнаружительной способности.
Технические характеристики:
Диапазон рабочих температур, от -20 до +50°С; относительная влажность воздуха при 25°С до 95%; период контроля канала от 12 с до 1,5 ч; масса 0,13 кг; габаритные размеры 92x57x48 мм; срок службы батареи питания (при нормальных условиях) не менее 5 лет; тип зон обнаружения — объемная; максимальная дальность действия 12 м; угол обзора в горизонтальной плоскости 90°; высота установки 2,3 м; диапазон обнаруживаемых скоростей 0,3-3 м/с. Работает с 16-ти канальным приемным блоком Ладога БРШС-РК-Р.
Время появления на рынке: 3 квартал 2011 г.

Извещатель охранный магнитоконтактный радиоканальный «Ладога МК-РК»

Производитель: Риэлта, РФ
Поставщик: ОДО «Сфератрэйд»
Назначение:

Извещатели охранные магнитоконтактные радиоканальные «Ладога МК-РК» (далее–МК-РК), предназначены для блокировки на открывание (смещение) дверей, окон, витрин и других конструктивных элементов закрытых помещений, а также организации устройств типа «ловушка» с последующей выдачей извещения о тревоге путем дистанционной беспроводной передачи закодированных идентифицируемых сигналов (сообщений) по двунаправленному каналу связи в диапазоне частот от 433,05 до 434,79 МГц.
Технические характеристики:
период контроля канала от 10 с до 10 мин; диапазон рабочих температур -20 ... +50°С; масса 0,1 кг; габаритные размеры 112x42x32 мм; срок службы батареи электропитания (при нормальных климатических условиях, отключенной индикации и периоде выхода в эфир не менее 30 с) не менее 5 лет; электропитание извещателей осуществляется от двух литиевых батарей — основного типа С R123A (типоразмер 1/2R6 (1/2AA) напряжение 3В и резервного типа CR2032. Работает с 16-ти канальным приемным блоком Ладога БРШС-РК-Р.
Время появления на рынке: 3 квартал 2011 г.

Видеокамера AMC-B920HD

Торговая марка: Axiom
Поставщик: ОДО «Сфератрэйд»
Назначение:

Профессиональная цветная корпусная видеокамера разрешения HD и высокой чувствительности благодаря своим техническим характеристикам и удобству в использовании, успешно применяется как в простых системах видеонаблюдения, так и в сложных конфигурациях в интегрированных охранных комплексах.
Особенности:
Применение новой 1.3 CMOS матрицы 1.3 Megapixel Sony Progressive формирует сверхвысокое разрешение и наиболее четкое изображение с разрешением 720ТВЛ при минимальной освещенности на объекте 0,06лк.
Благодаря широким возможностям настройки, а также большому количеству режимов автоматической регулировки уровня видеосигнала (выкл./низкий/средний/высокий), баланса белого (авто/отслеживание/пользователь), а также различным эффектам изображения (антиблик, зеркальное отображение, негатив/позитив, «заморозка») камера прекрасно работает в самых сложных условиях. Отображаемые на экране сообщения позволяют оперативно отслеживать состояние камеры.
Видеокамеры предназначены как для внутренней установки, так и для монтажа в термокожухах вне помещений.
Технические характеристики: PAL, NTSC, 1.3 Megapixel Sony Progressive, HD-SDI 720p/30fps, 720 ТВЛ, 0.1лк/F1.4, HD-SDI (BNC), отношение сигн./шум более 48 dB, PAL: 1/50 ~ 1/100000 сек., ме-

ханический ИК фильтр, баланс белого — авто, авторегулировка усиления — вкл./выкл., экранное меню, цифровой зум X8, управление автодиафрагмой DD, DC12V, C/CS, — 10°C..+50°C, регулировка резкости, установка секретных зон, 126(Д)x67(Ш)x60(В) мм, 350г.

Время появления на рынке: 3 квартал 2011 г.

Цифровой гибридный видеорегистратор AM-DVR3009HD1

Торговая марка: Axiom

Поставщик: ОДО «Сфератрэйд»

Назначение:

Видеорегистратор гибридный предназначен для работы в составе цифровой системы видеонаблюдения для сбора, записи, хранения с последующим просмотром в различных режимах видеоизображения.

Особенности:

Конструктивно цифровой видеорегистратор выполнен в виде моноблока, который может быть установлен самостоятельно. На фронтальной панели прибора расположены кнопки управления, разъем USB для резервного копирования. Мониторинг в реальном времени. Возможность подключения одной камеры HD–качества. Пентаплексный режим работы. Работа по сети с помощью ПО удаленного клиентского места. Управление посредством USB мыши, с передней панели или ИК-пульта дистанционного управления (в комплекте).

Технические характеристики: видеовход, 1В/75 Ом BNC 9;, видеовход, SDI 1; пентаплекс; 1xBNC, 1xVGA, 1xHDMI; NTSC, PAL; H-264; 1280x720 (HD); 704x576, 704x288, 352x288; 20 (HD) / (720x576) / 200 (720x288) / 400 (360x288); режимы записи: постоянный / по тревоге / детекции движения/ по расписанию; аудио входы/выходы RCA 8/2; блокировка клавиш; тревожный вход/выход 9/2; запись тревожных событий до 10000; управление PTZ (интерфейс RS-485); 12 В (блок питания в комплекте); рабочая температура 5~40ºC; температура хранения 0~40ºC; влажность менее 90%; 430x293x55 мм; 1,85 кг (без жесткого диска).

Время появления на рынке: 3 квартал 2011 г.

ВИДЕОКАМЕРА EQ610e

Производитель: EverFocus Electronics Corp. (Тайвань)

Поставщик: СООО «Сатурн-Инфо»

Сертификат: не подлежит обязательной сертификации

Особенности:

- 700ТВЛ
- 1/3" Sony 960H EXview HAD CCD II
- Платформа Sony Effio-E
- Чувствительность 0,03Люкс/F=1.2
- Функция День/Ночь с IRC модулем
- OSD меню
- Функция D-WDR, BLC, AES, AGS, AWB
- Встроенный детектор движения

Характеристики: питание DC12B/AC24B, потребление 1.5Вт/2.5Вт, размеры 68 x 56 x 120 мм, вес 290 г, рабочая температура -10˚C~50˚C.

Время появления на рынке: декабрь 2011 г.

ВИДЕОКАМЕРА EXD300

Производитель: EverFocus Electronics Corp. (Тайвань)

Поставщик: СООО «Сатурн-Инфо»

Сертификат: не подлежит обязательной сертификации

Особенности:

- 700ТВЛ
- 1/3" Sony 960H EXview HAD CCD II
- Платформа Sony Effio-E
- Чувствительность 0,03Люкс/F=1.2
- Варифокальный объектив 2.8~10.5мм
- OSD меню
- Функция D-WDR, BLC, AES, AGS, AWB
- Встроенный детектор движения

Характеристики: питание DC12B, потребление 1.5Вт, Размеры 111.4 x 83мм, вес 440г, рабочая температура -10˚C~40˚C.

Время появления на рынке: декабрь 2011 г.

ВИДЕОКАМЕРА EHD610e

Производитель: EverFocus Electronics Corp. (Тайвань)

Поставщик: СООО «Сатурн-Инфо»

Сертификат: не подлежит обязательной сертификации

Особенности:

- 700ТВЛ
- 1/3" Sony 960H EXview HAD CCD II
- Платформа Sony Effio-E
- Чувствительность 0,03Люкс/F=1.2
- Функция День/Ночь с IRC модулем
- OSD меню
- Функция D-WDR, BLC, AES, AGS, AWB
- Встроенный детектор движения
- 3-Axis для установки на стену и потолок
- Класс защиты IP66

Характеристики: питание DC12B/AC24B, потребление 1.5Вт/2.5Вт, размеры 110 x 112мм, вес 290г, рабочая температура -40˚C~40˚C.

Время появления на рынке: декабрь 2011 г.

ВИДЕОРЕГИСТРАТОР ECOR264 D3

Производитель: EverFocus Electronics Corp. (Тайвань)

Поставщик: СООО «Сатурн-Инфо»

Сертификат: не подлежит обязательной сертификации

Особенности:

- Запись и Воспроизведение 50кадр/с D1 (модели 4кан и 8кан)
- Формат Сжатия H.264
- VGA и BNC выход
- Один внутренний HDD
- DVD привод
- Бесплатный EverFocus DDNS сервис
- Мобильный мониторинг на экране КПК или Смартфона
- Встроенный калькулятор расчета время записи
- Умный Поиск: Поиск движения в заданной зоне
- Поддержка PTZ протоколов EverFocus, Pelco D, Pelco P, Samsung, Transparent
- USB Мышь и ИК пульт управления в комплекте

Характеристики: 10/100Mbps Ethernet; TCP-IP/DHCP/PPPoE/DDN; питание DC12B; рабочая температура 0˚C~40˚C.

Время появления на рынке: 1 квартал 2012 г.

Cisco Systems Holding BV,
Представительство в Республике Беларусь

220034, г.Минск, ул. Платонова, 1Б,
Бизнес-центр «Виктория Плаза»
E-mail: pburba@cisco.com
Сайт: www.cisco.com
Год основания: 2008
УНП: 102341971
Контактные лица: Глава Представительства Павел Бурба.
Сертификат: ОАО «Гипросвязь».

A

АВАНТ-ТЕХНО, ОДО

220004, г. Минск, ул. Короля , 45- 16в
Тел./факс: (017) 200-01-09, 226-43-52
E-mail: contact@avant.by
Сайт: www.avant.by
Год основания: 2003
УНП: 190423783
Контактные лица:
директор Козодаев Руслан Валерьевич,
начальник отдела продаж Новик Владимир Павлович,
начальник отдела систем видеонаблюдения Красногоров Александр Михайлович.
Лицензии:
№ 02300/0343681 на право осуществления деятельности по обеспечению пожарной безопасности выдана МЧС РБ, действительна до 02.06.2013.
Производство: охранные, пожарные извещатели и оповещатели.
Сертификаты: производство (перечень товаров с номером сертификата и датой выдачи):

Наименование	Дата выдачи	Действителен до:	Сертификат №
Извещатель «АВАНТ-DG55»	07.05 2010	03.05.2015	BY/112 03.03.023 00243
Извещатель «АВАНТ-Glasstrek»	07.05 2010	03.05.2015	BY/112 03.03.023 00244
Извещатель «АВАНТ-Pro»	07.05 2010	03.05.2015	BY/112 03.03.023 00239
Извещатель «АВАНТ-Digigard»	07.05 2010	03.05.2015	BY/112 03.03.023 00242
Извещатель «АВАНТ-211»	07.05 2010	03.05.2015	BY/112 03.03.023 00245
Извещатель «АВАНТ-Pro PET»	07.05 2010	03.05.2015	BY/112 03.03.023 00238
Извещатель «АВАНТ-Pro CU1»	07.05 2010	03.05.2015	BY/112 03.03.023 00241

Услуги:
консультации по подбору и применению охранно-пожарного оборудования и систем видеонаблюдения. Гарантийное и послегарантийное сервисное обслуживание на базе собственного авторизованного сервисного центра.
Поставка:
- технические средства охранно-пожарной сигнализации;
- системы видеонаблюдения и контроля доступа;
- IP видеосистемы;
- сопутствующие материалы для монтажа систем.

Дистрибьютор компаний:
PARADOX (Канада) — ведущий мировой производитель охранной техники, выпускающий обширный спектр охранного оборудования и продающий свою продукцию более чем в 60 стран мира.
HIKVISION — международная компания с производством в Китае, разработка и производство IP видеосистем, видеокамер, видеорегистраторов и плат видеоввода. Первое место в мире по производству видеорегистраторов. Hikvision представляет самые передовые решения со сжатием в формате H.264 для индустрии цифрового видеонаблюдения на основе своих собственных запатентованных алгоритмов. Продукция Hikvision обеспечивает безопасность различных сфер деятельности во всем мире, включая розничную торговлю, аэродромы, железные дороги, банки, промышленные предприятия, стадионы и т.д.
Бастион — широкий ассортимент источников питания.
НВП **Болид** — производитель интегрированных охранных систем.
Avicam Electronics — видеокамеры, видеорегистраторы, объективы и сопутствующее оборудование.

АДАНИ, УП

220075, г. Минск, ул. Селицкого, д.7, пом.2/1
Тел: (017) 346-29-03, **факс:** (017) 346-29-02
E-mail: info@adani.by
Сайт: www.adani.by
Год основания: 1991
УНП: 100054851
Контактное лицо: генеральный директор Линев Владимир Николаевич.
Лицензии:
№ 02300/108-4 выдана Госпромнадзором МЧС РБ, действительна до 15.07.2014.
Производство:
КОНПАСС Сканер рентгенографический цифровой для персонального досмотра;
BAGVISION Сканер рентгенографический цифровой для досмотра багажа и грузов различных модификаций;
КАРГОСКАН Комплекс инспекционно-досмотровый ускорительный в перебазируемом и мобильном исполнениях.
Услуги:
Проектирование, монтаж, наладка, ремонт, обслуживание цифровых рентгенографических аппаратов.

АкссонСофт, ООО

220100, г. Минск, ул. Куйбышева, 40, офис 3.
Тел.: (017) 292-66-11, 292-66-99
E-mail: minsk@axxonsoft.com
Сайт: www.axxonsoft.by
УНП: 191217449
Контактное лицо: директор Лисовский Дмитрий Васильевич.
Производство: программное обеспечение.
Поставка:
- интегрируемая платформа безопасности с распределенной архитектурой «Интеллект».
- цифровые системы видеонаблюдения:
  - Интеллект Лайт;
  - SmartВидео;
  - Axxon Smart IP.

Дистрибьютор компаний: официальное представительство компании ITV | AxxonSoft.

АльфаСистемы, ООО

220090, г. Минск, Логойский тракт, д. 22а, оф. 207
Тел.: (017) 262-84-64,
факс: 265-12-59, (029) 652-21-32
E-mail: info@cctv.by
Сайт: www.samsungcctv.by
Год основания: 2005
УНП: 190598104
Контактные лица: директор Гаврютиков Александр Анатольевич, заместитель директора Комачков Ренат Инсатулович.
Услуги:
технические консультации, поставка оборудования, гарантийное и послегарантийное обслуживание систем видеонаблюдения, систем контроля и управления доступом.
Дистрибьютор компаний:
- Samsung (Корея),
- AXIS Communications (Швеция),
- Computar (Япония),
- GE Security (США),

- IFS (США),
- LevelOne (Германия),
- TORCAM (Китай),
- SC&T (Тайвань),
- Widearea Times Technology Co. (Китай),
- ITV (РФ).

Атомиум-Секьюрити, ОДО

220053, г. Минск, Долгиновский тракт, д.39, оф. 244
Тел.: (017) 289-02-69, 233-60-99,
(044) 780-41-25
Сайт: www.atomium.by
Год основания: 1997
Контактные лица: директор Крохин Андрей Владимирович, заместитель директора Дашкевич Людмила Анатольевна.
Лицензии:
№ 02010/614326 на право осуществления деятельности по обеспечению безопасности юридических и физических лиц выдана МВД РБ, действительна до 09.10.2014.
Производство: тепловизионные камеры.
Услуги:
1) разработка и проектирование систем безопасности:
- видеонаблюдение,
- охранная сигнализация,
- контроль доступа.
2) строительно-монтажные и пусконаладочные работы;
3) гарантийное и техническое обслуживание.

Дистрибьютор компаний:
Siemens (Швейцария), PeakBeamSystems,Inc (США), Охранная техника (РФ), ПолюсСТ (РФ), ООО «Фракталь-СБ» (РФ), НПП ООО «Лазерные системы» (РФ), ЗАО «Старт-7» (РФ), ООО «фирма АКА» (РФ), ООО «Этис».
Выполненные проекты:
- Государственный комитет пограничных войск РБ;
- Министерство внутренних дел РБ;
- государственная фельдъегерская служба РБ;
- Министерство иностранных дел РБ;
- Посольство РБ в Германии; Италии; Польше;
- Посольство Государства Израиль в РБ;
- ГП «Белтрансгаз»;
- ОАО «Белвнешэкономбанк».

Б

БЕЛНЭТЭКСПЕРТ, ЗАО

220036, г. Минск, ул. Волоха, 1, ком. 407
Тел./факс: (017) 286-20-03, 286-20-04
E-mail: info@netexpert.by
Сайт: www.netexpert.by
Год основания: 1997
УНП: 190512711
Контактное лицо: начальник отдела маркетинга Козак Андрей.
Поставка: оборудование для систем телекоммуникации, локальных компьютерных сетей, материалы для построения структурированных кабельных систем, электротехническая продукция.
Дистрибьютор компаний: AMP Netconnect, APC, Belconn, DELL, HELUKABEL, Hirschmann, Phoenix Contact, Planet, Rittal, Schneider Electric.

В

ВирусБлокАда, ОДО

220088, г. Минск, ул. Смоленская, 15 — 803б
Тел./факс: (017) 294-84-29
E-mail: info@anti-virus.by
Сайт: www.anti-virus.by
Год основания: 1997
УНП: 101294617
Контактное лицо: коммерческий директор Резников Геннадий Константинович.
Лицензии:
№01019/50 на право осуществления деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи, выдана ОАЦ при Президенте РБ, действительна до 14.12.2014.
Сертификаты:
21 декабря 2006 г. компании получила сертификат соответствия системы менеджмента качества проектирования, производства и технической поддержки программного продукта требованиям белорусского стандарта СТБ ИСО 9001-2001 и немецкого DIN EN ISO 9001: 2000 (ежегодно компания проходит подтверждение соответствия).
Услуги:
в Республике Беларусь — разработка, внедрение и эксплуатация программного обеспечения, предназначенного для защиты от воздействия вредоносных программ в промышленных и иных организациях республики для замещения аналогичных импортных продуктов;
в мире — экспорт разработанного ОДО «ВирусБлокАда» национального программного обеспечения, предназначенного для защиты от воздействия вредоносных программ, способного конкурировать с лучшими мировыми аналогами.
Проекты и разработки:
- комплекс антивирусных программ Vba32;
- автоматизированное рабочее место администратора «Комплекса VBA32»;
- система фильтрации нежелательной электронной почтовой корреспонденции в Национальном банке Республики Беларусь, функционирующей совместно с компонентами комплекса Vba32 программных средств защиты от воздействия вредоносных программ и др.

К

Корпоративные Информационные Системы, ООО

220073, г.Минск, ул. Бирюзова, 10 а, офис 214
Тел./факс: (017) 204-87-41, (029) 610-70-97,
(029) 650-19-76
E-mail: ciscompany@tut.by
Сайт: www.ciscompany.by
Год основания: 2008
УНП: 191161232
Контактные лица: директор Голев Алексей Михайлович, финансовый директор Церлюкевич Валерий Валерьевич
Сертификаты: Perco, «SKIDATA», «Wintersteiger», «SERVIO».
Услуги:
разработка, проектирование, поставка, внедрение и сервисное обслуживание программно-аппаратных комплексов и систем.
Поставка:
- оборудование «SKIDATA» Австрия;
- оборудование «Wintersteiger» Австрия;
- оборудование GEOVISION;
- оборудование Perco;
- продукция Onity;
- продукция Vingcard;
- ПО «SKIDATA», «Wintersteiger», GEOVISION, «SERVIO», MICROS-FIDELIO.

Проекты и разработки:
- платежно-пропускные системы «SKIDATA» Австрия;
- оборудование и ПО для пунктов проката «Wintersteiger» Австрия;
- комплексные системы автоматизации отелей и общественного питания «SERVIO»;
- системы управления для гостиниц и ресторанов MICROS-FIDELIO;
- системы доступа, безопасности и их компоненты;
- системы видеонаблюдения GEOVISION.

Л

Легион безопасности, ООО

220118, г. Минск, ул. Машиностроителей, 29-117, офис 7
Тел./факс: (017) 340-42-17
E-mail: info@mobotix.by
Сайт: www.mobotix.by
Год основания: 2004
УНП: 190539684
Контактное лицо: директор Пеганов Владимир Николаевич.
Лицензия:
№ 02300/0565670 по обеспечению пожарной безопасности выдана МЧС РБ, действительна до 15.07.2015.
Услуги:
специализируется в предоставлении услуг в области обеспечения безопасности. Основные направления деятельности — поставка широкой номенклатуры технических средств охраны и оказание инжиниринговых услуг в области систем безопасности.
Поставка:
MOBOTIX — IP-системы видеонаблюдения высокого разрешения. Интеллектуальные цифровые сетевые видеокамеры высокого разрешения с уникальными возможностями от немецкой компании MOBOTIX.
AXIOM — оборудование CCTV видеонаблюдения. Видеокамеры (миниатюрные, корпусные, купольные, уличные, поворотные Speed Dome и т. д.); видеорегистраторы от экономкласса до профессиональных; вариофокальные объективы с ручной и автоматической диафрагмой; профессиональные LCD и CRT-мониторы; термокожухи и блоки питания; устройства передачи видеосигнала по витой паре; пульты управления и многое другое.
ITV — цифровые системы видеонаблюдения, интегрированные комплексы безопасности.
NUUO — платы видеоввода, гибридные системы видеонаблюдения, сетевые видеорегистраторы для IP-систем видеонаблюдения.
Дистрибьютор компаний:
MOBOTIX AG (Германия);
AXIOM (PRC);
ITV (Россия);
NUUO (Тайвань).

Н

Надежные программы, УП (hoster.by)

220005, г. Минск, ул. В. Хоружей, 1а, 6 этаж
Тел./факс: (017) 239-57-02, 239-57-20
E-mail: info@hoster.by
Сайт: www.hoster.by
Год основания: 2000
УНП: 100160363
Лицензии: № 01019/78 на право осуществления деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи, выдана 06.04.2011 ОАЦ при Президенте РБ, действительна до 06.04.2016.
Услуги: хостинг и электронная почта, регистрация международных доменных имен и доменов .BY.

Научно-исследовательский институт технической защиты информации (НИИ ТЗИ), НП РУП

220088, г. Минск, ул. Первомайская, 26/2
Тел./факс: (017) 294-01-71, 285-31-86
E-mail: info@niitzi.by
Сайт: www.niitzi.by
Год основания: 1986
УНП: 100036784
Контактное лицо: директор Картель Владимир Федорович.
Лицензии:
- № 01019/0531779 на право осуществления деятельности по технической защите информации, в том числе криптографическими, включая применение электронной цифровой подписи методами выдана ОАЦ при Президенте РБ, действительна до 20.03.2012;
- № 02010/9833 на право осуществления охранной деятельности выдана МВД РБ, действительна до 12.06.2013;
- № 03070/0336515 на право осуществления деятельности, связанной с криптографической защитой информации и средствами негласного получения информации выдана КГБ РБ, действительна до 13.04.2013.

Сертификаты:
- сертификат соответствия Государственного комитета по стандартизации Республики Беларусь, система менеджмента качества.

Услуги:
– аудит систем защиты информации, информационных ресурсов и систем на информационную безопасность;
– разработка политик безопасности, заданий по безопасности, сопутствующих нормативно-методических документов;
– подбор, сертификация, поставка и установка средств защиты информации;
– сертификационные испытания программных и аппаратно-программных продуктов информационных технологий (ИТ), технических средств защиты информации на соответствие требованиям безопасности информации, оценка заданий по безопасности;
– создание систем защиты информации информационных систем и автоматизированных систем в защищенном исполнении, их аттестация.
– специальная проверка защищаемых помещений и технических средств на наличие возможно внедренных специальных технических средств негласного съема информации;
– подготовка, аттестация объектов информатизации на соответствие требованиям руководящих и нормативных документов по безопасности информации, сопровождение и периодический инструментальный контроль аттестованных объектов информатизации;
– проектирование и монтаж вычислительных сетей, защищенных от утечки информации по техническим каналам.
Дистрибьютор ЗАО «Конструкторское бюро «ПРИБОР».
Дилер ЗАО «Научно-производственный центр Фирма «НЕЛК».

НПТ, ООО

220012, г. Минск, ул. К.Чорного, 5А, пом.5а
Тел.: (029) 649-77-79
E-mail: ab@searchinform.ru
Сайт: www.searchinform.ru
Год основания: 2009
УНП: 191117428
Контактное лицо: директор Барановский Александр Валерьевич.
Поставка: КИБ SearchInform (DLP решение, позволяющее контролировать Skype, почту, внешние устройства, интернет-мессенжеры, устройства печати, HTTP трафик, шифрованные каналы, учёт рабочего времени).

Р

Регула, ООО

220036, г. Минск, ул. Волоха, 1, комн. 314
Почтовый адрес: 220036, г. Минск, а/я 39
Тел.: (017) 286-28-25, **факс:** (017) 210-23-97
E-mail: mail@regula.by
Сайт: www.regula.by
Год основания: 1992
УНП: 100069352
Контактное лицо:
начальник отдела маркетинга Скворчевский Юрий Антонович.
Производство:
оборудование, программно-аппаратные комплексы контроля подлинности документов, денежных знаков, ценных бумаг, а также специаль-

ное досмотровое оборудование и приборы для считывания информации с документов.
Дополнительная информация:
ООО «Регула» специализируется в области проектирования, разработки, производства и обслуживания оборудования, программно-аппаратных комплексов контроля подлинности документов, денежных знаков, ценных бумаг, а также специального досмотрового оборудования и приборов для считывания информации с документов.
Производит программное обеспечение: система криминалистического исследования, редактирования и документирования исследуемых документов «Видеоскоп», информационно-поисковые системы «Паспорт» и «Автодокументы».

РОВАЛЭНТСПЕЦСЕРВИС, ООО

220007, г. Минск, ул. Вододько, 22
Тел.: (017) 228-17-73, 228-16-80
Отдел продаж: 228-17-75, 228-17-72, 228-16-95
Факс: 228-16-96
E-mail: sales@rovalant.com
Сайт: www.rovalant.com
Год основания: 1994
УНП: 190285495
Контактные лица:
директор Карпович Владимир Викторович,
заместитель директора Куприянов Александр Семенович.
Лицензия:
№ 02300 /0344206 на право осуществления деятельности по обеспечению пожарной безопасности выдана МЧС РБ, действительна до 21.02.2012.
Производство:
- адресно-аналоговая система пожарной сигнализации АСПС БИРЮЗА;
- пожарный прибор управления ОБЕРЕГ;
- импульсные источники бесперебойного питания ББП;
- система мониторинга НЕМАН;
- интегрированная система безопасности ИСБ 777;
- извещатели пожарные дымовые оптико-электронные: ИПДО-212-1, ИПДО-212-С, ИПДО-212-А;
- приемно-контрольные охранно-пожарные приборы серии «А»;
- автоматизированные системы контроля и учета энергоресурсов (АСКУЭ).

Продажа: системы видеонаблюдения компании Samsung Techwin.
Услуги:
- разработка, производство и торговля оборудованием систем безопасности и мониторинга; системы контроля доступа; аксессуары;
- проектирование, монтаж и техническая поддержка;
- весь спектр продукции для организации технического противодействия угрозам — от систем объектовой защиты и каналов передачи информации до систем мониторинга.

С

САТУРН-ИНФО, СООО

220015, г. Минск, ул. Пономаренко, 35а, офис 616
Тел./факс: (017) 251-62-06; 256-25-23,
(029) 656-17-50, (029) 756-17-18
E-mail: saturn@saturn-info.com
Сайт: www.saturn-info.com
Год основания: 1994
УНП: 100063951
Контактные лица:
директор Худалеев Сергей Романович, заместитель директора Гилеп Михаил Ярославович.
Лицензии:
№ 02300/728 на право осуществления деятельности по обеспечению пожарной безопасности выдана МЧС РБ, действительна по 21.04.2016;
№ 02010/0444875 на право осуществления деятельности по обеспечению безопасности юридических и физических лиц выдана МВД РБ, действительна по 21.05.2014.
Производство:
аналоговый акустический извещатель «ШКЛО-730»; цифровой акустический извещатель «ШКЛО-У»; источник бесперебойного питания «ИБП Сатурн».
Услуги:
проектирование, монтаж, наладка и сервисное обслуживание систем безопасности.
Дистрибьютор компаний:
Bosch Security Systems (Нидерланды), Honeywell Security (Нидерланды), Everfocus Electronics (Тайвань), SC&T (Тайвань), AverMedia (Тайвань), AVTech (Тайвань), Anvox (Китай).
Выполненные проекты:
Белорусская железная дорога (станция «Минск-Пассажирский»); бизнес-центр «Инфо»; ОАО «Беларуськалий»; сеть магазинов «Соседи»; сеть магазинов «Связной»; фабрика «Ареола»; ОАО «Белгазпромбанк»; ЗАО «Трастбанк»; ЗАО «Минский транзитный банк»; ОАО «Технобанк»; ЗАО «РРБ-Банк»; ОАО «Банковский Процессинговый Центр»; ОАО «Белтрансгаз»; РУП «Белавиа»; сеть АЗС «Юнайтед Компани»; ООО «Софтклуб», ОАО «Горизонт»; Минский электромеханический завод имени Козлова; ООО «Франдеса»; Минское областное управление Департамента охраны МВД РБ.

Сименс, ООО
Представительство (РФ) в Республике Беларусь

220004, г. Минск, ул. Немига 40, пом.43
Тел./факс: (017) 217-34-84, факс: (017) 210-03-95
E-mail: minsk-office.cd@siemens.com
Сайт: www.siemens.by
Год основания: 2003
УНП: 102295743
Контактное лицо: Новокрещенная Екатерина Владимировна
Проекты и разработки: в областях — Энергетика, Индустрия, Инфраструктура и города, Здравоохранение.

Синезис, ООО

220043, г. Минск, пр-т Независимости, дом 95, пом. 12, офис 316
Тел./факс: (017) 281-77-85, 281-77-91
E-mail: s@synesis.ru
Сайт: www.synesis.ru
Год основания: 2007
УНП: 190950894
Контактные лица: Шведко Дмитрий, Михолап Михаил.
Сертификаты:
1) i-LIDS® approved primary detection system for operational alert use in sterile zone monitoring applications (одобрено i-LIDS как система первичного обнаружения для формирования оперативных тревог в приложениях видеонаблюдения стерильной зоны);
2) 2) i-LIDS® approved event based recording system for sterile zone monitoring applications (одобрено i-LIDS как система регистрации событий в приложениях видеонаблюдения стерильной зоны).
"i-LIDS" (Imagery library for intelligent detection systems) — лаборатория в научном подразделении МВД Великобритании.
Оборудование ООО «Синезис» входит в каталог охранного оборудования, сертифицированного МВД Великобритании.
Услуги: разработка оборудования и программного обеспечения для охранного видеонаблюдения и цифрового телевидения.
Поставка: технологии и оборудование для охранного видеонаблюдения и цифрового телевидения.
Разработки:
- видеоаналитическое устройство «MagicBox»;
- встроенная видеоаналитика для охраны периметра, одобренную i-LIDS;
- менеджер устройств ONVIF (бесплатное ПО с открытым кодом);
- система 3D-моделирования для оценки эффективности системы безопасности;
- линейка ресиверов цифрового ТВ высокой четкости с функциями медиацентра;
- высокоточный детектор лиц, выбранный поисковой системой Яндекс;
- система стереоскопической видеорегистрации и сопоставления лиц;

- дактилоскопические алгоритмы идентификации по отпечаткам ладоней и пальцев.

Дополнительная информация:
Устройство «MagicBox» удостоено высшей награды форума «Технологии Безопасности 2010» (Москва) в номинации «Технические средства предупреждения и борьбы с терроризмом». Устройство было отмечено Дипломом 1-ой степени и Золотой медалью «Лучшее инновационное решение 2010».

Сфератрэйд, ОДО

220118, г. Минск, ул. Машиностроителей, 29-502
Тел: +375 17 341 50 50,
+375 29 641 50 50 (Velcom),
+375 29 541 50 50 (МТС).
E-mail: info@secur.by
Сайт: www.secur.by
Год основания: 1995
УНП: 100972915
Контактное лицо: директор Малаховский Денис Святославович.
Лицензии:
- № 02010/209 на право осуществления охранной деятельности, в том числе проектирование, монтаж, наладка и техническое обслуживание средств и систем охраны выдана МВД РБ, действительна до 15.08.2021.
- № 02300/50 на право осуществления деятельности по обеспечению пожарной безопасности выдана МЧС РБ, действительна до 10.02.2016.

Услуги:
- технические консультации по вопросам обеспечения безопасности любого уровня сложности;
- обследование и экспертная оценка состояния технических средств безопасности на объектах административного, производственного и других назначений;
- составление технического задания и проекта;
- поставка оборудования;
- гарантийное и послегарантийное обслуживание поставляемого оборудования.

Поставка:
- IP и CCTV-системы видеонаблюдения;
- системы контроля и управления доступом;
- системы охранно-пожарной сигнализации;
- системы защиты товаров от краж;
- системы аварийного оповещения и звуковой трансляции;
- сопутствующие материалы для монтажа и др.

Проекты:
Хозяйственный суд (г. Минск), Представительство ООН в РБ, «Тойота-Центр» (г. Минск), автоцентр «Пежо», летний амфитеатр (г. Витебск), РУП БМЗ, СП «Санта Бремор», РУП «Белтелеком», ИООО «БелЕвросеть», Минский метрополитен, сеть АЗС ОАО «Беларуснефть», РУП «Белпочта», ГП «Белаэронавигация», аэропорт «Минск-1», ЗСАО «Бролли», ВЦ ЗАО «Аквабел», ИООО «Атлант-М Холпи», ТС «КВАРТАЛ ЗЕЛЕНЫЙ БОР», ОАО БПЦ, Казино ZEUS, паркинг бизнес-центра «ТИТАН», ЗАО «ВТБ-банк», ЗАО «БТА-банк» и др.

Дистрибутор компаний:
ОДО «Сфератрэйд» — дистрибутор оборудования безопасности известных торговых марок и производителей: AXIOM, KT&C (South Korea), MOBOTIX AG (Germany), ZAVIO (Taiwan), NUUO (Taiwan), ACTi (Taiwan), Fujinon (Japan), Pinetron (South Korea), SALTO (Spain), GSN Electronic (Israel), LOB (Poland), Elmes (Poland), Roger (Poland), QUIKO (Italy), JIS (Spain), Kenwei (PRC), Seoul Commtech Co. (South Korea), PERCo (Russia), ITV (Russia), JSB Systems (Russia), Elesta (Russia) и др.

СЭНС Дизайн-студия, УП

220026, г. Минск, пер.Бехтерева, 8, к.365, 366
Тел.: (017) 346-88-90, 346-84-54,
Факс: (017) 346-88-91
E-mail: sens@mail.bn.by
Сайт: www.belsens.com
Год основания: 1989
Контактное лицо: директор Трофименко Владимир Павлович.
УНП: 100050950

Лицензии:
№02300/159-4 выдана МЧС Республики Беларусь, действительна до 09.10.2016.

Производство:
рентгеновские сканирующие системы антитеррористического и дефектоскопического назначения.

Услуги: проектирование, монтаж и сервисное обслуживание поставляемого оборудования.

Поставка:
модификации рентгеновской сканирующей системы КОНСИС.

Выполненные проекты:
ОАО «Белшина» (дефектоскопическая система контроля качества сверхкрупногабаритных шин), ГХУ Управления делами Президента Республики Беларусь (кабинет комплексного досмотра посетителей), ОАО «Норильский никель» (система контроля КОНСИС), аэропорт «Домодедово» (система контроля КОНСИС), золотодобывающее предприятие в Республике Казахстан (система контроля КОНСИС).

У

УНИБЕЛУС, СП ООО

220033, г. Минск, ул. Нахимова, 10
Тел.: (017) 291-15-05, **факс:** (017) 230-72-40
E-mail: info@unibelus.com
Сайт: www.unibelus.by
Год основания: 1994
УНП: 100834637
Контактное лицо: генеральный директор Забабуха Юлия Аркадьевна.
Производство:
Система трансляции и оповещения о пожаре «АРИЯ».
Услуги: от консультации и проектирования до пусконаладочных работ и последующего сервисного обслуживания всех слаботочных сетей.
Поставка: систем пожарной сигнализации; трансляции и оповещения; конференц-связи и синхроперевода; видеонаблюдения; контроля доступа; пожаротушения; мультимедийной; локально-вычислительные сети; охранной сигнализации; периметральной системы охраны; противокражной; диспетчеризации; телефония; часофикация; радиофикация; система автоматизации.
Дистрибьютор:
Aiphone (Япония), OPTEX (Япония), «Риэлта» (Россия), «Артон» (Украина), «Технос-М» (Россия), «ТПД Паритет» (Россия), CEM Systems (Великобритания), LG Iris (США), Openers&Closers (Испания), Amtel Security (США), Green (Чехия), FEIG Electronic (Германия), Kocom (Корея), Samsung Techwin (Корея), JVC Professional Europe (Германия), CBC (Ganz, Computar), AVerMedia Information (Тайвань), Win4net (Корея), Daiwon optical (Корея), «Тахион» (Россия), Panasonic (Япония), TOA (Япония), Tasker (Италия), JTS (Тайвань), DNH (Норвегия).

Ф

ФИМА БР, ООО

220073, г. Минск, ул. Бирюзова, 10а, офис 201
Тел.: (017) 200-59-99, **факс:** (017) 200-96-66
E-mail: info@fima.by
Сайт: www.fima.by
Год основания: 2010
УНП: 191297443
Контактное лицо: директор Криворотов Герман Петрович.
Лицензии:
№02010/0615983 на право осуществления деятельности по обеспечению безопасности юридических и физических лиц выдана МВД РБ, действительна до 13.08.2015.
Услуги: проектирование, монтаж, наладка и техническое обслуживание средств и систем охраны (за исключением средств охраны индивидуального пользования).
Поставка: CCTV, СКУД, ОПС и т.д.

SAMSUNG TECHWIN

Разрешение Full HD в Ваших системах видеонаблюдения

с телекамерами и видеорегистраторами **HD-SDI Samsung**

Лучшее решение для создания и модернизации систем видеонаблюдения объектов с массовым скоплением людей

- разрешение 1920x1080 пикселей при отображении и записи (одна телекамера HD-SDI заменяет более 5 телекамер с разрешением D1);
- скорость отображения/записи - 30 кадров/сек на канал;
- отсутствие задержек, характерных для IP систем;
- возможность поэтапной модернизации существующей аналоговой системы видеонаблюдения;
- возможность использования существующей кабельной инфраструктуры аналоговой системы видеонаблюдения;

HD-SDI телекамера	HD-SDI телекамера	4-х канальный HD-SDI видеорегистратор
SCB-6000	SCD-6080	SRD-480D

Официальный дистрибьютор в Республике Беларусь - компания «АльфаСистемы»
г. Минск, Логойский тракт 22а, офис 207
Тел./факс: (+375 17) 262 84 64, 265 12 59
info@cctv.by www.cctv.by

УНП 190598104

UNEX
системы видеонаблюдения

www.unexpro.ru

ДВЕ ФУНКЦИИ В ОДНОЙ КАМЕРЕ

Универсальный дизайн

UNP632-DV1

КОМПАКТНЫЙ РАЗМЕР

Вандало защищенный купол ø57 мм
Класс герметичности IP68
Высокое разрешение (600 ТВЛ)
Высокая чувствительность
Легкий монтаж

UNP634FV-DV5

НАКЛАДНОЙ+ВРЕЗНОЙ монтаж

Вандало защищенный купол ø100 мм
Класс герметичности IP68
Высокое разрешение (600 ТВЛ)
Высокая чувствительность
Легкий монтаж, 3 оси вращения

УНП: 100834637

UNEX
системы видеонаблюдения

СП «Унибелус» 000, г. Минск, ул. Нахимова, 17, Тел.: +375 (17) 291 15 05
info@unibelus.com www.unibelus.by