№ 1/2005 (45)

Бизнес и безопасность

Бизнес и безопасность™

www.bsm.com.ua

ЭТИКА ВЕДЕНИЯ ДЕЛОВОЙ РАЗВЕДКИ

ДЕСЯТЬ ПРИЧИН КУПИТЬ СЕТЕВУЮ КАМЕРУ

«СКРЫТЫЙ» СЕРВИС ГОРОДСКИХ АТС

ПРАВОВЫЕ АСПЕКТЫ ЛЕГАЛИЗАЦИИ ЦИФРОВЫХ ЗАПИСЕЙ

КОМПЕТЕНТНЫЙ ПЕРСОНАЛ – УСПЕШНЫЙ БИЗНЕС

ЗАХИЩЕНА СВОБОДА ВАШОГО БІЗНЕСУ

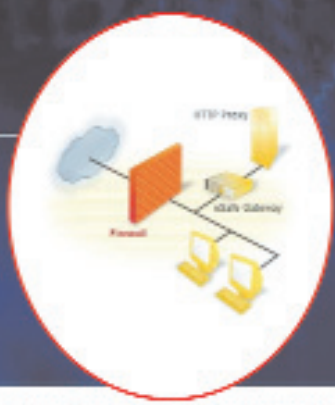
- **Аудит інформаційних мереж та комплексні рішення IT безпеки**

- **XSpider - єдиний сканер, який вже сьогодні визначає більш третини уразливостей, що принесе завтрашній день**
  - допомагає усувати уразливості, що виникають у комп'ютерній мережі через недосконалість програмного забезпечення
  - забезпечує ефективний процес моніторингу мережевої безпеки в комп'ютерній мережі будь-якого масштабу

- **eSafe - комплексний захист інформації в мережах будь-якого масштабу**
  - фільтрація й аналіз HTTP/FTP/SMTP трафіку (антивірус, антиспам)
  - URL-фільтрація, оптимізація використання інформаційних ресурсів
  - запобігання витоку та викраденню конфіденційної інформації

- **eToken - персональний засіб суворої аутентифікації і збереження даних**
  - підтримує роботу з цифровими сертифікатами і ЕЦП
  - виробляється в двох форм-факторах: USB-ключа і смарт-карти

- **Антивірусні системи**
  - Kaspersky Antivirus
  - Dr.Web
  - Symantec
  - UNA
  - Trend Micro



www.yug.com.ua

Об'єднання IGT

НАША АДРЕСА:

04070, Київ-70,
Контрактова пл., 4, "Гостинний Двір",
2-й поверх, оф. 38-41,
Тел./факс (+ 380 44) 417-03-76, 417-07-73.
E-mail: info@yug.com.ua

ТИЖДЕНЬ ЦИФРОВИХ ТЕХНОЛОГІЙ 2005

5-8 КВІТНЯ

EnterEX® 2005

Дванадцята міжнародна виставка корпоративних інформаційних систем

Виставковий центр
КИЇВ ЕКСПО ПЛАЗА
(м. "Нивки", вул. Салютна, 2-Б)

ЗАПРОШУЄМО ВІДВІДАТИ ВИСТАВКУ!

замовлення запрошень,
програма виставки на сайті

www.euroindex.ua

CIO
У рамках виставки — другий З'їзд IT-директорів України.
www.cio.org.ua

Інформаційний спонсор: Компьютерное обозрение
Інформаційний партнер: ЛІГА бізнесінформ

Організатор виставок: EUROINDEX, ufi
За підтримки: УСПП
Інформаційний спонсор: Компьютерное обозрение
Медіапартнер: CHIP
Онлайн-партнери Тижня цифрових технологій: ITC.ua, ITWARE.com.ua

IV МІЖНАРОДНИЙ ВИСТАВКОВИЙ ФОРУМ
ТЕХНОЛОГІЇ ЗАХИСТУ – 2005
МІЖНАРОДНІ СПЕЦІАЛІЗОВАНІ ВИСТАВКИ ТА КОНФЕРЕНЦІЇ
21-24 вересня 2005 р.
МІЖНАРОДНИЙ ВИСТАВКОВИЙ ЦЕНТР
Україна, Київ, Броварський пр-т, 15
"Лівобережна"
ЕКСТРЕМ ТЕХ
П О Ж ТЕХ
ОРГАНІЗАТОРИ:
Міністерство України
з питань надзвичайних ситуацій
ЗАТ "Міжнародний виставковий центр"
ЗАТ "Міжнародний виставковий центр"
Україна, 02660, Київ, Броварський пр-т, 15
тел./факс: (044) 201-11-65, 201-11-56, 201-11-58
e-mail: tatiana@iec-expo.com.ua
www.tech-expo.com.ua, www.iec-expo.com.ua
Генеральний інформаційний партнер
Генеральний медіа-партнер
Інформаційна підтримка:
ictv

НАЦІОНАЛЬНИЙ КОМПЛЕКС "ЕКСПОЦЕНТР УКРАЇНИ"
П'ята міжнародна спеціалізована виставка
25–28 квітня
ПОЖЕКСПО '2005
Пожежна техніка.
Засоби пожежогасіння та вогнезахисту.
Автоматичні системи пожежогасіння, сигналізації та оповіщення.
Забезпечення робіт в надзвичайних ситуаціях.
Індивідуальні та колективні засоби рятування людей на пожежах.
Спорядження пожежників.
Спеціалізований транспорт.
Науково-технічні розробки.
Дослідження пожеж.
Інвестиційні проекти.
Страхування.
Fifth International Specialized Exhibition
POZHEXPO '2005
25–28 April
Організатори:
МІНІСТЕРТВО УКРАЇНИ З ПИТАНЬ НАДЗВИЧАЙНИХ СИТУАЦІЙ,
ДЕРЖАВНИЙ КОМІТЕТ У СПРАВАХ ЗАХИСТУ НАСЕЛЕННЯ ВІД НАСЛІДКІВ ЧОРНОБИЛЬСЬКОЇ КАТАСТРОФИ,
НАЦІОНАЛЬНИЙ КОМПЛЕКС "ЕКСПОЦЕНТР УКРАЇНИ",
УКРАЇНСЬКИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПОЖЕЖНОЇ БЕЗПЕКИ МНС УКРАЇНИ
за сприяння АСОЦІАЦІЇ ПРОТИПОЖЕЖНОГО ЗАХИСТУ
В рамках виставки тематична експозиція "ЗАХИСТ І РЯТУВАННЯ"
Інформаційна підтримка:
Національний комплекс "Експоцентр України"
МСП 03680, м. Київ, пр-т Академіка Глушкова, 1
Тел./факс: (044) 251-92-80, 251-91-25
Факс: (044) 251-91-11 (12)
E-mail: pozhexpo@nvc.ukrsat.com
www.expocenter.kiev.ua

Бизнес и безопасность

№ 2005/1 (45)

Информационно-рекламный практический журнал для тех, кому есть что защищать.

Издается с 10 апреля 1996 года.

Рег. свид. КВ № 1347 от 27.03.95 г.
Учредитель: Беленький С. Я.
Гл. редактор: Беленький С. Я.
Корректор: Алещенко О. А.
Верстка: Мартыненко В. И.
Отдел рекламы: Козырева А. Я.
Беленькая С. В.
Кучмагра С. В.
Отдел подписки: Руссо В. О.
Малошук Н. Н.
Лихачева Л. А.

Адрес редакции:
ул. Ревуцкого, 44, г. Киев.
Для писем: 02140, а/я 100, г. Киев.
Телефон редакции: (044) 565-75-91,
факс (044) 565-96-37.
E-mail: post@bsm.com.ua
http://www.bsm.com.ua

☆ ☆ ☆

☆ ☆ ☆

Журнал отпечатан
ЧП «Коллегиум»
ул. Соломенская, 2
Заказ №
Печать офсетная.
Бумага офсетная. Формат 60x84 1/8.
Объем 6 усл.печ.стр.
Подписано в печать 14.02.2005 г.
Тираж 12 000 экз.
Индекс в каталоге периодических изданий ГП «Пресса» — 40226.
Периодичность: 6 номеров в год.
Цена договорная.

г. Киев — 2005

С О Д Е Р Ж А Н И Е

Охрана в предпринимательской деятельности

За годы независимости Украины охранная деятельность прочно вошла в наше сознание и стала практически неотъемлемой частью любого серьезного бизнеса. В тоже время в этом виде деятельности по-прежнему остается еще очень много недостатков, несовершенства, шаблона. И дело не только в том, что у нас нет специального законодательства по охранной деятельности. С точки зрения авторов, прежде всего, у нас нет научного подхода к охране: ни как к виду предпринимательства, ни как к виду деятельности, отсутствует научное обоснование и теоретические основы организации и тактики охраны при обеспечении деятельности предприятий негосударственной формы собственности.

Практика показывает, что без прочной теоретической базы многие вопросы в охране решаются методом проб и ошибок, отчего такая охрана становится слишком дорогой и не всегда эффективной. Исправляя одни ошибки мы наталкиваемся на другие и с каждым разом решаем новые проблемы, которые выстраиваются в череду трудно- и долгоразрешимых, перерастая при этом в постоянно существующие.

В этой связи, авторам хотелось бы высказать свою точку зрения, прежде всего, на теорию вопроса, которая, как известно, всегда была основой практики.

Прежде всего, что мы понимаем под охраной? Собрав все известные формулировки можем прийти к выводу, что под охраной понимается прежде всего определенные действия (комплекс действий) направленные на ограждение, защиту кого- или чего-либо от нападений, посягательств, враждебных действий. Исходя из данного определения охране должны быть свойственны, по крайней мере, четыре признака: действие (комплекс действий) - указывает на то, что охрана это, прежде всего процесс, который должен иметь определенные пространственные и временные характеристики; объект - как то, на что должны быть направлены действия охраны; субъект, то есть инструмент с помощью которого выполняются действия охраны; угроза - как возможность нападения, посягательства или враждебных действий по отношению к объекту. Другими словами охрана может существовать только при наличии указанных выше четырех признаков. Во всех других случаях действия по защите объектов нельзя квалифицировать как охрану.

Учитывая, что охрана представляет собой определенные действия, ее осуществление и развитие должно подчиняться определенным правилам, закономерностям, соответствовать выдвигаемым к ней требованиям. Основу таких правил, закономерностей и требований составляют принципы охраны.

Одним из основных принципов охраны является принцип законности. Данный принцип предусматривает, что все мероприятия охраны должны осуществляться в рамках действующего законодательства с соблюдением всех необходимых правовых норм, не допускать нарушения законных прав граждан и не препятствовать нормам, регулирующим свободу предпринимательской деятельности.

Другими принципами охраны являются: защита, активность, демонстративность, скрытность, экономическая целесообразность, непрерывность, конкретность, профессионализм.

Принцип защиты указывает на то, что система охраны должна базироваться на серьезной технической укрепленности объектов. Данный принцип раскрывает пассивную часть системы охраны.

В то же время принцип активности предусматривает, что система охраны должна не только препятствовать свободному доступу к охраняемым объектам, но и осуществлять противодействие различным их угрозам. Согласно этому принципу система охраны должна проводить мероприятия, направленные на поиск угроз объекту, их своевременную нейтрализацию еще на уровне потенциальной возможности. В таких условиях угрозы охраняемым объектам или вообще не смогут быть реализованы или действие их будет значительно снижено, а в случае их реализации охрана объекта будет способна эффективно противодействовать им.

Принцип демонстративности указывает на необходимость пропаганды сильного и активного режима охраны объекта. Реализация этого принципа на практике осуществляется различными способами, от обычного объявления «Во дворе злая собака», «Объект находится под охраной» и др. до выставления наружных постов физической охраны, демонстрации технических средств, используемых в охране объекта и т. д.

Практика показывает, что примерно в половине случаев злоумышленники узнав, что объект находится под охраной, отказываются от своих намерений, связанных с возможными посягательствами на него.

В то же время, в охране должна присутствовать и скрытая ее часть, действующая внезапно для лиц нарушающих режим охраны, злоумышленников осуществляющих посягательства на объекты. В этой связи в охране выделяют принцип скрытности. Согласно этому принципу часть сил и средств охраны выполняют свои задачи скрытно, находятся в резерве или маневрируют по сложно прогнозируемому графику. По определенному сигналу такие силы и средства концентрируют свои усилия на противодействии субъектам, которые совершают проникновение на объект или другим способом угрожают ему.

Принцип экономической целесообразности требует, чтобы расходы на охрану были адекватны роли и задачам, возложенным на нее. Низкое обеспечение охраны приведет к тому, что такая охрана будет не в состоянии обеспечивать надежную защиту объекта и противодействие его угрозам. В то же время чрезмерное обеспечение охраны приведет к неоправданным расходам и превышению ее возможностей над потребностями в ее услугах. В таких случаях придется загружать охрану дополнительными задачами.

Принцип непрерывности указывает на то, что объект должен находится под охраной в течение времени, когда реализация угрозы ему остается быть реальной. То есть охрана должна быть способна защищать объект, противодействовать его угрозам в пределах потребности объекта в этом.

Принцип конкретности предусматривает, что все мероприятия охраны должны осуществляться по конкретным объектам в отношении конкретных угроз посягательства на них. Не может быть охраны в резерв или впрок.

Принцип профессионализма предусматривает, что все мероприятия охраны должна проводиться грамотно на высоком профессиональном уровне, базироваться на объективных данных, не ограничивать права и не унижать достоинства граждан.

Система охраны, построенная с учетом указанных принципов, сможет обеспечить защиту объектов на необходимом уровне и эффективное противодействие их угрозам.

Акцентируя внимание на признаках охраны и выделяя, прежде всего, ее действия или комплекс действий, можно сказать, что в процессе этих действий применяются различные способы охраны.

Под способом охраны понимается порядок применения сил и средств охраны для защиты объекта и противодействия его угрозам. Учитывая специфику объектов, особенности их расположения, назначения, значимости в системе производства коммерческой структуры, условия функционирования, их охрана может осуществляться различными способами. К таким способам можно отнести: контроль доступа на территорию объекта или к отдельным его элементам, наблюдение за объектом или отдельными его элементами с использованием технических средств, контроль периметра территории объекта, нарядами (патрулями), караулами, отдельными постами, эскортное сопровождение объекта, наблюдение за подступами к объекту, радиоэлектронный контроль перемещения материальных ценностей.

Исходя из этого, охрана может быть организована контрольно-пропускными пунктами, постами видеонаблюдения, караулами, отдельными постами, нарядами (патрулями), эскортами, дозорами, секретами, радиоэлектронными системами сигнализации, системами сигнализации и оповещения и др.

Вторым среди признаков охраны является объект, в отношении которого направлены действия сил и средств охраны.

Под объектами охраны понимается зоны расположения средств производства, помещения или места хранения материальных ценностей, документов, офисы, другие учреждения, отдельные элементы зданий, производственных зон, грузы, транспортируемые различными видами транспорта, физические лица, существованию или деятельности которых угрожает определенная опасность.

В зависимости от размеров и характера расположения объекты могут быть точечные (квартиры, рабочие помещения офисов, отдельно стоящие торговые точки, физические лица), площадные (частные дома с усадьбой и хозяйственными постройками, офисы, банки, автостоянки, склады, базы хранения продукции, предприятия и др.), линейные (трубопроводы, линии электропередач, мосты через средние и крупные реки, линии связи).

По степени подвижности охраняемые объекты бывают стационарными (положение объектов не меняется в течении всего времени его существования), малоподвижными (место расположения может меняться не более чем 1 раз в месяц), подвижные (место расположения меняется каждый день).

По режиму работы объекты бывают с односменным, двусменным и круглосуточным режимом работы.

Такое деление объектов вызвано особенностями организации их охраны, что в последующем может влиять на расходы по их охране и стоимость охранных услуг.

Еще одним признаком охраны является угроза. Под угрозой понимается потенциально возможные или реальные действия злоумышленников, конкурентов или других лиц способные нанести материальный ущерб охраняемому объекту.

По своему происхождению угрозы бывают постоянные (от персонала объекта, населения, производственных систем и др.); периодические (обусловленные конъюнктурой рынка, социальными, политическими изменениями в стране или в отдельных ее регионах и т. д.); случайные, когда коммерческие структуры подпадают под действие негативных факторов определенных ситуаций напрямую их не касающихся; стихийные, которые вызываются силами природы.

Источниками формирования угроз безопасности предпринимательской деятельности является многообразие внутренних и внешних противоречий общественного развития в стране и на международной арене в разных сферах и областях человеческой деятельности как постоянно эволюционирующий процесс. То есть по своей природе причины угроз постоянны и последние с большей или меньшей вероятностью могут становиться реальностью для общества в целом, регионов страны или отдельных предприятий, организаций, а также их объектов. Это в свою очередь требует постоянной готовности предприятий к защите своей деятельности и собственности, в том числе и охраны их объектов.

Анализируя причины потерь охраняемых объектов можно заключить, что такие потери наступили вследствие:

★ недостаточного правового регулирования охранной деятельности;
★ недостаточной подготовки сил охраны и их обеспечения;
★ неэффективной оценки обстановки на объектах и вокруг них;
★ неэффективной кадровой политики сил охраны;
★ пассивности сил охраны;
★ недостаточности охраны, несбалансированности сил и средств охраны;
★ нарушений режима охраны персоналом объекта.

Среди случаев, приводящих к потерям на охраняемых объектах наиболее частыми были:

★ воровство работников охраняемых объектов;
★ воровство посторонних лиц;
★ воровство работников задействованных в охране объектов;
★незаконное использование (передача) материальных ценностей с охраняемых объектов их руководством;
★ разбойные нападения на охраняемые объекты;
★ потери, поломки, вывод из строя (сожжено, затоплено, другим образом приведено в негодность и др.).

Одной из серьезных причин потерь на охраняемых объектах является отсутствие их должного оборудования, то есть недостаточная техническая укрепленность объектов. Техническая укрепленность охраняемых объектов должна предусматривать:

★ наличие обособленного входа (въезда) на объекты. Специальное оборудование центрального и запасных входов на объекты;
★ оборудование всех элементов объектов и мест расположения сил охраны средствами связи;
★ внешние стены зданий охраняемых объектов должны исключать возможность их пролома и несанкционированного проникновения на объекты;
★ дополнительное укрепление оконных проемов первых, цокольных и подвальных этажей зданий охраняемых объектов;
★ оборудование помещений объектов средствами пожарной сигнализации;
★ наличие рабочего, дежурного и тревожного освещения объектов;
★ ограждение периметра объектов, выделение запретной зоны;
★специальное оборудование мест выполнения своих обязанностей силами охраны (наблюдательные вышки, постовые будки, укрытия для отражения нападения на объекты, скрытого наблюдения за подступами к ним;
★ наличие запорных устройств и замков на всех дверях помещений объектов;
★ аварийное питание потребителей электроэнергии задействованных в охране не менее чем из двух независимых источников с устройством автоматического переключения.

Техническая укрепленность объектов является основой их защиты и базовым элементом в системе охраны.

В охране различают физическую, техническую и комбинированную охраны. Под физической охраной понимается выполнение охранных действий силами охранников, то есть физическими лицами, задействованными на постах, в нарядах и т.д.

Под технической охраной понимается организация охраны объектов с помощью различных технических средств: радиоэлектронными системами сигнализации, системами сигнализации - оповещения, видеонаблюдения, автоматизированными системами доступа и т. д.

Комбинированная охрана осуществляется с использованием физических лиц и технических средств охраны.

Эффективность охраны достигается созданием системы многорубежной защиты объекта и установлением соответствующего охранного режима. Многорубежная защита объекта предусматривает организацию его охраны по определенным рубежам, которыми могут буть: территория объекта, здания объекта, помещения объекта. Каждый из этих рубежей должен иметь свои особенности охраны, которые предусматриваются системой охраны объекта.

Режим охраны объекта должен базироваться на внутреннем распорядке работы объекта и используемых предприятием технологиях производства. Он понимается как свод правил и мероприятий, регулирующих поведение работников и посетителей с точки зрения их безопасности, сохранности объекта, материальных ценностей и продукции.

По времени нахождения объекта под охраной режим охраны может быть круглосуточный, дневной (ночной) или временный. В зависимости от количества используемых сил и средств, платности контроля территории объекта, режим может быть простой и усиленный.

Выделяют три группы задач режима охраны: аналитические, предупредительные и процедурно-отражательные.

Аналитические задачи решаются путем сбора информации об угрозах объекту, их субъектах, возможных способах посягательств, состоянии и соблюдении режима охраны объекта.

Предупредительные задачи связаны, в первую очередь, с созданием имиджа сильного и надежного режима охраны объекта. В ходе их решения осуществляются мероприятия, направленные на своевременное обнаружение признаков готовящихся посягательств, заблаговременное сосредоточение сил и средств охраны на наиболее опасных участках, проведение мер маскировки и дезинформации злоумышленников.

Процедурно-отражательные задачи предусматривают проведение комплекса мер по созданию соответствующего режима охраны объекта, отражению и локализации посягательств на него, быстрой ликвидации последствий посягательств и восстановлению режима охраны.

Таким образом, все вышеизложенное может составлять основы охранной деятельности, которые являются одним из элементов ее теории.

Зубок Н. И.,
кандидат военных наук, профессор,
Яременко С. Н.

НОВОСТИ

Взломан почтовый сервер ФБР

Федеральное бюро расследований (ФБР) отключило свою действующую почтовую систему из-за опасений, что она была взломана хакерами, сообщает Associated Press.

По информации АР, пострадала только публичная почтовая система, которой ФБР пользовалась для связи с Джейн и Джоном Доу (общее обозначение мужчины и женщины в США), а внутренняя система не пострадала.

Как сообщает та же АР, ФБР в данный момент находится в поиске интернет сервис провайдера для хостинга своего нового публичного почтового сервиса.

http://itua.info

Компетенция персонала — залог прочности и безопасности бизнеса предприятия

Компетенцией персонала надо управлять как бизнесом. Компетентен персонал — успешно предприятие.

Сегодня бизнес функционирует в условиях информационной экономики, для которой характерны быстрая смена ситуаций как во внешней среде, так и на рынке, интенсивное обновление ассортимента представленной на рынке продукции, появление новых предпочтений потребителей. Активные знания – производные информации в сфере бизнеса предприятий и предпринимательства в целом, стали неотъемлемыми составляющими успеха. И успех этот напрямую зависит от уровня компетентности персонала предприятия (в первую очередь, разумеется, от компетенции его основных сотрудников). Кадры могут всё: они могут решить самую трудную задачу, добиться, казалось бы невозможного, но могут и лишить всего, доведя предприятие до краха. Компетентные и преданные фирме, работающие «как надо» люди – основной потенциал и ресурс предприятия и его бизнеса.

Компетенция – совокупное понятие, включающее знания, навыки, мотивы, поведенческие проявления и / или другие характеристики, которые необходимы для успешной работы сотрудников. **Суммарная компетенция персонала фирмы определяет её ценность, творческий и производственный потенциал, её корпоративную культуру.**

Сформированная (синтезированная) **модель компетенции персонала фирмы** помогает уловить (выявить) такие аспекты качества сотрудников, которые, не будь такой модели, остались бы вне поля зрения руководителей. Кроме того, основанная на модели компетенции система управления позволяет точнее определить, чему именно надо обучать перспективных сотрудников и какие качества следует развивать у них в первую очередь. Её применение позволяет значительно повысить эффективность кадровых решений и системы управления персоналом в целом и определить с достоверностью в 70–80 % в какой мере сотрудник соответствует требованиям фирмы. В этом смысле компетенция фирмы – вид её интеллектуального и производственного ресурса.

Чтобы оценить уровень компетентности фирма создаёт «банки», «словари» и «библиотеки», содержащие перечни ключевых компетенций персонала и критерии оценки выраженности каждой их них. Но в любом случае фирма должна определить, что она намерена проверять и оценить. **Основная задача: определить, соответствует ли поведение сотрудника и его отношение к работе требованиям фирмы,** выдвигаемым сегодня, установить степень выраженности компетенции у того или иного работника; потенциал развития нужных фирме компетенций; предрасположение сотрудника к определённой работе. Важно также определить, какую компетенцию у данного сотрудника следует развивать, т. к. компетенция – это исполнительный фактор, который непостоянен, а изменяется вместе с изменениями самой фирмы.

Основные аспекты использования компетентности персонала в бизнесе фирмы:

1. В области безопасности бизнеса:

1.1. Знание основ текущего законодательства, честного («прозрачного») бизнеса.

1.2. Соблюдение этики партнёрских отношений в бизнесе.

1.3. Минимизация рисков при принятии самостоятельных решений в области своей компетенции.

2. В области менеджмента:

2.1. Обмен (ротация) знаний по принципу «Даю»-«Получаю» или «Выиграл-Выиграл».

2.2. Способность осуществлять аудит и реинжиниринг бизнес-процессов.

2.3. Эффективная коммерциализа-ция нематериальных активов фирмы.

3. В области маркетинга:

3.1. Рыночное мышление и клиенториентация предпринимательства.

3.2. Знания и их использование в технологиях товаропроизводства, товародвижения (презентации, брэндировании, сервисном сопровождении и сбыте продукции предприятия).

3.3. Совершенствование связей с общественностью, рекламных и сервисных мероприятий.

4. В области управления:

4.1. Формирование и совершенствование здорового климата межличностных отношений.

4.2. Мотивация труда, общения, нацеленность работников на результат.

4.3. Совершенствование коммуникативных навыков, умения работать в коллективе, в команде.

Корме того, важными аспектами компетенции являются: системное мышление, видение перспективы развития бизнес процессов; принятие адекватных решений при нестандартных ситуациях (в рамках своей компетенции каждым ответственным сотрудником фирмы); минимизация рисков и оправданная гибкость.

К чему следует стремиться, формируя нужный уровень компенсации

Прежде всего – это стремление иметь «зрелых» сотрудников, которым возможно делегировать полномочия по принципу «поручил и забыл». Руководитель, который считает, что менее подготовленным и менее самостоятельным персоналом управлять легче, занимается ничем иным как самообманом. Это обязательно приведёт к истощению компетенции фирмы, и к утрате её рыночной позиции.

При формировании **модели компетенции фирмы** необходимо учитывать, что сотрудники фирмы подразделяются категориям и по типам.

Разделение сотрудников по категориям определяется уровнем их компетентности и надёжности.

Сотрудникам первой категории не делегируют никаких полномочий, а прививают присущие фирме ценности, развивают их профессиональные навыки и повышают уровень мотивации их труда.

Сотрудникам второй категории присуще большее развитие, как в мотивационном, так и в профессиональном плане. Им уже делегируют некоторые полномочия.

К третьей и четвёртой категориям относятся сотрудники, достигшие высокого уровня мотивационной и профессиональной зрелости. Им делегируют больше полномочий и предоставляют более обширную информацию.

Сотрудников четвёртой категории «слушают» и их мнение и видение решения проблем руководство фирмы использует при принятии важных решений.

Чем больше в фирме сотрудников третьей и четвёртой категорий – тем выше уровень корпоративной компетенции персонала и тем устойчивее она в штормовом океане бизнеса.

Самое сложное – понять, когда сотрудник уже готов перейти из второй категории в третью.

На «типы» сотрудники подразделяются по влиянию внутренних мотивов: стремлению к власти («человек-власть»); стремлению к достижению идеала («человек-достиженец») и по потребности к общению и контакту с людьми («человек-причастник»).

Эти типы людей наиболее эффективны в следующих видах деятельности:

«Человек-власть» – работа на новых рынках и с новой продукцией (менеджер, маркетолог).

«Человек-достиженец» – аналитическая работа (исследователь, юрист, аудитор).

«Человек-причастник» – PR-менеджер, сотрудник сервисной службы.

Способность фирмы генерировать новые идеи – показатель высокого уровня компетенции персонала. Но не следует забывать о том, что новаторские идеи интересны, но и опасны: могут нанести бизнесу серьёзный вред. Необходим здоровый консерватизм и **процедура выдвижения и оценки полезности идеи.** Такая процедура должна состоять, как минимум, из следующих этапов.

На первом этапе рассматривается, за-служивает ли данная идея внимания и стоит ли бороться за её реализацию. Далее проводится анализ наличия необходимой информации (знаний) и ресурсов для разработки бизнес-плана реализации идеи (этапы 2–3). На четвертом этапе принимается окончательное решение будет или не будет фирма реализовывать бизнес-проект на основе данной идеи в ближайшее время.

Для повышения компетентности персонала фирмы желательно предусмотреть в её подразделениях так называемый мотивационный бюджет и официально за-претить стиль общения на повышенных тонах. Вместо публичной критики лучше использовать беседу «один на один» и дать понять сотруднику причину его ошибки.

На, казалось бы, простой вопрос: «Все сотрудники стремятся развивать (повышать) компетентность?» дать положительный ответ нельзя. Оказывается, что в действительности значительное количество грамотных классных работников довольны тем, что у них уже есть. Они не стремятся к ответственности. Чтобы избежать разочарования, руководитель должен определить, какого уровня зрелости достиг тот или иной ис-

полнитель, и стараться ставить перед ним задачи, которые ему импонируют и по силам решать.

Факторы, над которыми следует задуматься

Большинство штатных сотрудников фирмы (порой до 80 %) могут быть вполне уверены в своей компетенции, хотя в действительности она гораздо ниже установленного работодателем уровня, покрывая реально этот уровень только на 45 %. В этом случае фирма должна задуматься над необходимостью сконцентрировать внимание на тех 55 % знаний, которыми сотрудники не владеют в полной мере.

Грош цена предприятию, которое имеет новые перспективные разработки, но не может их использовать из-за недостаточной компетенции персонала.

Яновский А.

НОВОСТИ

США: троян отключает противошпионское ПО от Microsoft

Троянская программа BankAsh-A, ворующая реквизиты с компьютеров, работающих на Windows, отключает и пытается удалить бета-версию антишпионского приложения Microsoft AntiSpyware.

Специалисты антивирусной компании Sophos утверждают, что это первая замеченная ими попытка борьбы с еще не вышедшим в коммерческом варианте приложением Microsoft AntiSpyware. Бета-версия приложения распространяется свободно с сайта Microsoft.

По мнению старшего технологического консультанта Sophos Грэхема Клули (Graham Cluley), "эта атака может быть первой из многочисленной серии в будущем". "Поскольку продукт Microsoft выходит из стадии бета-тестирования и приобретает популярность среди пользователей, мы можем ждать все новых и новых попыток его нейтрализации со стороны троянских коней, вирусов и червей", - добавил г-н Клули.

Жертвами BankAsh-A могут стать, в том числе, клиенты Barclays, Cahoot, Halifax, HSBC, Lloyds TSB, Nationwide, NatWest и Smile, говорят в Sophos. Эксперты по безопасности банковских транзакций уже предупредили пользователей о том, как не допустить кражи реквизитов через интернет, разместив информацию на сайте BankSafeOnline

CNews

ЭТИКА ВЕДЕНИЯ ДЕЛОВОЙ РАЗВЕДКИ: ВЗГЛЯД НА ПРОБЛЕМУ ФИНАНСИСТА В ШТАТСКОМ

Если трудности кажутся непреодолимыми,
значит, близок успех.
Анахарсис Клод, IV век до н. э.

Тема проблемы этики в деловой разведке, конечно, очень актуальна, особенно в Украине. По крайней мере, вряд ли кто-то может поручиться, что знает службу безопасности предприятия, которая ни разу не нарушила хотя бы одно из изложенных в предлагаемой статье правил.

Деловая разведка является составной частью корпоративной культуры ведения современного бизнеса [1]. Попытаемся определить основные цели и понятия деловой разведки. Для выживания предприятия в условиях современной конкурентной борьбы первоочередное значение начинает играть разведка намерений конкурентов, изучение основных тенденций бизнеса, анализ возможных рисков и т. д. Дисциплина, изучающая эти аспекты бизнеса, получила на Западе название «деловая разведка» (business intelligence). Поскольку этот термин еще не устоялся, в литературе можно встретить также термины «конкурентная разведка», «бизнес-разведка», которые эквивалентны деловой разведке [2-4,6].

Деловая разведка является мощным инструментом исследования рынка и конкурентной среды, и в настоящее время представляет собой бурно развивающуюся дисциплину, возникшую на стыке экономики, юриспруденции и специальных дисциплин. Деловая разведка занимается сбором и анализом информации о конкуренте (собственно разведкой), защитой своей информации (промышленная контрразведка), а также проведением специальных операций (на-пример, защитой имиджа предприятия и руководителя, противодействию «черному» пиару и т. д.).

Основное отличие деловой разведки от промышленного шпионажа – поиск и получение всей необходимой информации исключительно законными (с точки зрения норм существующего права) методами. Отличием деловой разведки от промышленного шпионажа является то, что деловая разведка проводится в рамках действующих правовых норм, и свои результаты получает благодаря аналитической обработке огромного количества разнообразных открытых информационных материалов. Появление новых информационных технологий (сетевых структур типа Internet, коммерческих баз данных, систем поиска информации и т. д.) и относительная дешевизна доступа к информационным ресурсам позволяют аналитикам деловой разведки готовить качественные материалы, пригодные для принятия решений руководством компаний [5].

Методы промышленного шпионажа ориентированы на использование всех доступных средств для получения искомой информации, включая как прямое нарушение законов (шантаж, подкуп, воровство, насилие и т. д.), так и неэтичные методы (обман, распространение компрометирующих сведений, выпытывание и т. д.). Методы деловой разведки исключают использование уголовно наказуемых средств, и в большей степени ориентированы на цивилизованные способы ведения бизнеса. Однако грань между этичными и неэтичными методами ведения деловой разведки (хотя и при соблюдении в обоих случаев действующих законов) остается очень размытой. По мере возрастания потребностей в получении ценной деловой информации возрастает роль этических норм. При возникновении проблем с получением информации в подразделении деловой разведки появляются стимулы «срезать углы» и нарушить этические ограничения. Иногда само руководство компании толкает на такие действия, так как для нее неважно, как получена информация, лишь бы была выполнена работа.

Рассмотрим этические проблемы, связанные с работой в сети Internet. Сетевое сообщество живет по своим законам, которые необходимо соблюдать. Хотя эти законы не регламентированы, «де-факто» они уже существуют. При ведении деловой разведки в сети и проведении PR-акций (т. е. выполнении функций деловой разведки) необходимо выполнять определенные правила, в частности:

★ при сборе деловой информации не выдавать себя за другое лицо или организацию (зарегистрировавшись под чужим, но известным именем);

★ не заниматься сбором сведений, составляющих коммерческую тайну конкурента (участвуя в электронных конференциях);

★ не переманивать ведущих специалистов конкурента;

★ не «подавлять» сайты конкурентов;

★ не публиковать компромат на конкурентов в любой форме.

Михаил Вертузаев

Остановимся на двух подходах в методах сбора необходимой информации: соблюдение законов, но пренебрежение нормами морали (подглядывание, обман при найме на работу, переманивание ведущих специалистов, получение информации из «мусорных ящиков» конкурентов) при ведении разведки (примеры - Microsoft против Oracle, осень 2000 г., Avon против Mary Kay Cosmetic, 1991 г.). В обоих примерах руководством фирм были наняты частные детективы, которые собирали деловую информацию из «мусорных ящиков» конкурентов. Этично ли это? На данный вопрос нет однозначного ответа у профессионалов деловой разведки. Если метод сбора информации легален, всегда ли он соответствует принятым этическим нормам? Все зависит от среды воспитания сотрудника деловой разведки. Люди, вышедшие из недр сило-

Колектив редакції журналу «Бизнес и безопасность» щиро вітає нашого постійного автора – завідувача відділу корпоративних систем управління фінансами Науково-дослідного фінансового інституту при Міністерстві фінансів України, професора кафедри технічних засобів попередження та розкриття злочинів Національної академії внутрішніх справ України, доктора технічних наук РФ та України, академіка Академії педагогічних і соціальних наук (м. Москва), дійсного члена Міжнародної слов'янської академії наук, члена Спеціалізованої вченої ради СРК 26.706.02 по захисту дисертацій, що містять державну таємницю зі спеціальності 21.07.02 «Розвідувальна діяльність органів державної безпеки» при Національної академії СБУ, полковника міліції Вертузаєва Михайла Сергійовича з обранням його Почесним професором Американського університету (American University, Washington DC) і висловлює надію на подальшу творчу співпрацю.

вых структур, например бывшие оперативники МВД или СБУ, часто думают и действуют только с точки зрения «буквы закона». Если их действия не выходят за рамки действующего законодательства, то они считают их нормальными, при этом считается, что соблюдены нормы морали присущие данному обществу при сборе деловой информации. Однако люди работающие в разведке, воспитанные в академической корпоративной среде, оценивают свои поступки исходя из других принципов, например, стремясь не попасть на страницы скандальной хроники. Большинство профессионалов, работающих в области деловой разведки, не будет восстанавливать и исследовать «мусор» других организаций и обманывать людей под видом приема на работу. Они считают такое поведение неэтичным и в их кругу не приемлемым.

В различных странах этические нормы поведения имеют свою национальную окраску. Этические соображения становятся также чрезвычайно важными по мере того, как компания расширяет свой бизнес и начинает деловые контакты с представителями зарубежных стран. Общепринятые стандарты делового поведения в разных странах различны. Например, в некоторых странах совершенно легальна дискриминация при приеме на работу по признакам пола. В других – гражданские служащие ожидают вознаграждения за представляемые вам официальные документы. Эта практика также отличается от развитых европейских и североамериканских норм ведения бизнеса. Например, автор этой статьи был, буквально, застигнут врасплох вопросом, с которым обратился ко мне директор ФБР (ныне бывший) Луис Фри. Это было в декабре 2000 года, сразу после моего пленарного доклада на Международной конференции в Вашингтоне «Транснациональная преступность, коррупция и информационные технологии» [7]. Его вопрос или точнее – реплика звучала приблизительно так: «Мои аналитики мониторят сообщения из России и Украины о многочисленных заказных убийствах, и я совершенно не понимаю смысла таких убийств в отношении бизнесменов. Естественно, и у нас были громкие политические заказные убийства (братья Кеннеди, Мартин Лютер Кинг и т. д.), убивали и убивают со времен Аль Капоне в криминальных разборках, заказывают агентов ФБР, копов, журналистов... Но у нас не заказывают бизнесменов. Как правило, основным мотивом заказного убийства, может быть либо необходимость возвращения долга, либо устранение конкурента. Но, ведь долг остается и после убийства кредитора и переходит к его приемнику, а устранить конкурентов раз и навсегда – мечта для наивных».

При этом мой оппонент не назвал еще одну главную причину – желание отомстить нечистоплотному партнеру по бизнесу, либо недобросовестному конкуренту, который «кинул» тебя в самое неподходящее время и, возможно, разрушил твой бизнес. При этом, со слов директора ФБР, американцы не прибегают к заказным убийствам, достаточно обратиться с иском в арбитражный суд и все ваши проблемы будут эффективно решены в установленном законом порядке.

Мне не хотелось вступать в долгую дискуссию со своим собеседником об особенностях украинского арбитражного и хозяйственного судоустройства и нерадостных перспективах «кинутых» бизнесменов. Поэтому я ограничился разъяснением нескольких наших национальных «понятий». В мире бизнеса принято считать, что если сегодня тебя безнаказанно «кинули» на один цент, то завтра у «кидалы» может появиться желание нагреть тебя на миллион, если он у тебя есть, конечно. И если твои партнеры узнают о твоем промахе и его безнаказанности, то вряд ли ты вызовешь у них уважение. Кто же захочет в дальнейшем иметь дело с «лохом»? А так, как говаривал отец народов «Нет человека (в данном случае – обидчика) – нет проблемы» и все довольны.

Хотя последний пример, как говорят официальные оппоненты на защите диссертаций, носит дискуссионный характер и отражает личную точку зрения автора. Однако, при этом, можно было бы привести множество кон-кретных фактов из нашей украинской действительности.

С понятием деловой разведки тесно связана коммерческая тайна. Важно понимать, что хотя и противозаконно пользоваться коммерческими тайнами чужих компаний, во многих случаях эти компании потеряли право называть что-либо коммерческой тайной из-за своих собственных необдуманных действий. На-пример, если компания выходит с новым продуктом на рынок, она должна предварительно его запатентовать и проконтролировать, не существует ли какой-то производитель, который может разобрать этот продукт на части и воспроизвести его под своим патентом.

В другом примере, один из отечественных заводов по производству некоторого класса железобетонных изделий потерял юридическое право, говорить о способе производства ЖБИ как о коммерческой тайне, потому что администрация завода не позаботилась об охране производственных помещений и не проинформировала служащих о необходимости соблюдения коммерческой тайны. Поэтому любой посетитель завода мог осмотреть производственную зону и собрать необходимую информацию.

Какое поведение соответствует принятым этическим нормам? Трудно дать определение, что такое этические нормы поведения. Толковый словарь Вебстера определяет этику как дисциплину, имеющую дело с добром и злом и с нравственным долгом. Для большинства из нас практическое ежедневное применение этических правил очень помогает в жизни. Например, как бы мы почувствовали себя, увидев заметку о своих действиях на первой странице бульварной газеты? Что бы мы чувствовали, если бы активность газетчиков была бы направлена на нас? Почувствовали бы мы заблуждение или обман?

Ответы на эти вопросы и образуют принципы, которым мы должны руководствоваться в нашем поведении при сборе информации. Хотя многие компании декларируют правила этического поведения для своих сотрудников, в действительности, в ежедневной гонке за прибылью этические правила могут не соблюдаться. Говоря о своем служении высокой морали, о миссии предприятия, многие менеджеры вместе с тем находятся под огромным давлением обстоятельств. Они не должны ограничивать возможности своих подразделений деловой разведки по сбору информации определенными рамками. Многие компании награждают свои подразделения деловой разведки за проделанную ими работу, но никогда не поощряют их за то, что эта работа выполнена при соблюдении этических норм.

Возможность несоблюдения этических норм поведения при сборе информации администрация аргументирует тем, что конкуренция по своей природе неэтична, поэтому зачем следовать каким-то правилам при проведении деловой разведки. Многие из менеджеров новой формации считают, что было бы неправильным совсем не заниматься мошенничеством, если этим занимаются конкуренты. Этот вопрос является одним из самых трудных, потому что этика изменяется так же, как изменяется и общество. Конечно, к сожалению, приходится согласиться, что мошенничество становится частью нашей культуры [8,9]. С другой стороны, следует ли поощрять падение нравов, глядя сквозь пальцы на мошенничество, и считать это нормой? Одним из самых трудных вопросов при изучении поведения менеджера является необходимость учитывать психологию человека. Например, хотя все соглашаются, что наем на работу служащих из конкурирующей фирмы лишь для того, чтобы получить их промышленные секреты, является неэтичным, всегда можно убедить себя, что вы нанимаете этого человека только из-за его высокой квалификации. В большинстве случаев люди переходят из компании в компанию в поисках новых возможностей внутри одной отрасли промышленности и почти невозможно доказать обратное.

Каковы же преимущества следования этическим нормам поведения? Следование этическим нормам является не только правильным с моральной точки зрения, но и экономически выгодно. Возможно, самая важная причина почему надо следовать этическим нормам поведения состоит в том, что такое поведение убережет вашу фирму от судебного разбирательства и связанных с ним затрат. Случаи с фирмами Microsoft и Oracle, Avon и Mary Kay служат хорошим примером. Другая причина, по которой целесообразно следовать этическим нормам поведения, состоит в том, что такое поведение делает жизнь служащих более спокойной и менее напряженной. Зная требования, предъявляемые к ним обществом, люди точно понимают, что им можно делать, а чего нельзя. С них снимается ответственность в выборе решений. Третья причина – доверие к компании и общественному мнению. Репутация одного из руководителей российской компании А, занимающейся гостиничным бизнесом была запятнана, когда он нанял консалтинговую фирму, которая помогала ему собирать информацию об организации гостиничного бизнеса в России. Нанятый им «охотник за головами» (The headhunter) получил несколько интервью у ряда менеджеров таких компаний. Хотя он не лгал, говоря, что сейчас для них есть работа, однако он обещал им ее в будущем. Действительно, некоторых из них впоследствии были наняты в компанию А. Однако, интервьюер в результате бесед получил много информации о гостиничном бизнесе, которую он бы не смог получить никаким другим способом. Ясно, что обещанием работы в будущем можно раскрыть многие секреты в настоящем. Еще раз отметим, что нельзя определить истинные мотивы интервьюера и его методы, но этот случай показался подозрительным для многих наблюдателей.

Несколько слов об этическом кодексе деловой разведки. Для правильной организации своей дея-

тельности компании нуждаются в собственном наборе этических правил – своеобразном кодексе поведения. Ниже перечислены основные стандарты поведения, связанные со сбором информации. Большинство из них ориентируется на минимальные требования, позволяющие не нарушать законы различного уровня. К ним относятся следующие нормы:

★ незаконны попытки обладания чужой коммерческой тайной;

★ незаконно получение какой-либо информации (составляющей коммерческую тайну или нет) от конкурента силой или обманом;

★ отказ от противоправных действий (например, нарушение чужого права владения или перехват телефонных сообщений) при сборе информации;

★ возврат владельцу конфиденциальной и частной информации, полученной случайно или непреднамеренно. В случае получения конфиденциальной правительственной информации, государственные органы должны быть уведомлены о нарушении государственной безопасности.

Важно отметить, что приобретение информации, о которой вы не знаете, что она «ворованная», или получение секретной информации, о конфиденциальности которой вы не знаете, не является нарушением закона. Однако, после того как вы узнали о ее противозаконном приобретении, невозвращение владельцу или использование ее в своих целях уже может рассматриваться как нарушение.

Поскольку многие менеджеры все еще полагают, что деловая разведка связана с чем-то непорядочным, абсолютно необходимо, чтобы руководитель подразделения деловой разведки представил директору компании «Этический кодекс деловой разведки», который был бы составной частью «Этического кодекса компании» (если он существует). В действительности, специфика кодекса деловой разведки должна заключаться в том, что в нем указываются виды информации, которые можно собирать и которые нельзя собирать, и приводятся дозволенные и недозволенные методы сбора информации. Кодекс также должен включать положения о поведении сотрудников деловой разведки при случайном получении запрещенной информации, например конфиденциальных заметок или личных писем.

В течение длительного времени приверженцы этического поведения утверждают, что нарушение норм морали и снижение этических стандартов общества приведет к огромным затратам на обеспечение его безопасности. В качестве аргумента выдвигается тезис, что если повсеместно этические стандарты ухудшаются, бизнесменам придется больше платить, чтобы защитить себя от агрессивной тактики поведения конкурента, которая может стать общепринятой нормой поведения в деловом мире, и тогда превентивные меры могут оказаться очень дорогими. Подходящей аналогией может служить та цена, которую общество платит из-за того, что не дает всем детям правильного воспитания с детства. Обществу приходится затрачивать огромные средства на содержание в тюрьме преступника и устранение последствий его преступлений, причем эти средства значительно больше, чем потребовались бы на воспитание законопослушного гражданина.

Можно сделать вывод, что если в деловом сообществе будет стремительно распространяться неэтичное поведение, то у высшего руководства не будет иного выхода, как ограничить информацию для своих сотрудников. Это может привести к недоверию среди служащих и к нежеланию работать с большей эффективностью – как утверждает адъюнкт-профессор Гарвардской школы бизнеса Лин Шарп Пейн (Lynn Sharp Paine), в журнале деловой этики Journal of Business Ethics. Ограничения пользованием служебным телефоном и ограниченный доступ к внутрифирменной информации для служащих компании, желающих расширить свои знания, налагают очевидные препятствия на внутренний обмен информацией, жизненно важной для фирмы. Когда исследователям отказывали в представлении информации о проектах, над которыми они сами работали, и в сведениях о том, как их работа связана с работой других людей, они тем самым отсекались от побудительной и творческой полезной информации. Для сбора требуемой информации нет необходимости нарушать Этический Кодекс. Даже для этой молодой дисциплины – деловой разведки – действуют старые истины. Одна из них гласит: «85 % информации, которая Вам необходима, находится в общественном пользовании. Другие 15 %, возможно, вам и не потребуются никогда». Некоторые аналитики говорят о 90 %. Используя экспертный анализ и соблюдая этические нормы, профессионалы деловой разведки в состоянии выполнять свою работу квалифицированно и эффективно. Ниже в качестве примера приводится Этический Кодекс, составленный американским «Обществом профессионалов конкурентной разведки» (Society of Competitive Intelligence Professionals) для своих членов.

★Постоянно старайся увеличить уважение и признание к этой профессии на всех государственных уровнях.

★ Выполняй свои служебные обязанности с рвением и прилежанием, поддерживай самый высокий уровень профессионального мастерства и избегай всех неэтичных поступков.

★ Оставайся верным политике компании, ее целям и общему курсу и выполняй обещания, данные своей компании.

★ Придерживайся всех действующих законов.

★ Во время делового свидания предоставляй всю относящуюся к делу информацию, включая принадлежность к организации.

★ Соблюдай правила работы с конфиденциальной информацией.

★ Действуй в полном соответствии с этими этическими стандартами при работе внутри компании, при ведении переговоров и во всех ситуациях, когда придется работать по специальности.

Частные службы и самостоятельные консультанты конкурентной разведки должны также объявить, какие виды деятельности им разрешены, а какие запрещены и осуждаются ими. Например, ведущая американская компания в области деловой разведки Fuld & Company, опубликовала свои собственные этические правила поведения, названные «Десять заповедей легального сбора разведывательной информации». По этим заповедям сотрудники компании не должны:

★ Лгать, когда представляетесь.

★ Нарушать официальную генеральную линию вашей компании.

★ Записывать на диктофон раз-говор с собеседником без его разрешения.

★ Предлагать взятки.

★ Устанавливать подслушивающие устройства.

★ Умышленно вводить собеседника в заблуждение при переговорах.

★ Получать от конкурента и передавать ему ценную конфиденциальную информацию.

★ Распространять дезинформацию.

★ Воровать промышленные секреты.

★ Осознанно давить на собеседника с целью получения требуемой информации, если это может подвергнуть опасности его жизнь или репутацию.

Наконец, высший управленческий персонал должен следить за тем, чтобы этические нормы соблюдались не только в конкурентной разведке, но и в в самой компании в целом.

Вертузаев М. С.,
заведующий отделом корпоративных систем управления финансами Научно-исследовательского финансового института при Министерстве финансов Украины,
доктор технических наук РФ и Украины,
профессор кафедры технических средств предупреждения и раскрытия преступлений Национальной академии внутренних дел Украины,
Академик академии педагогических и социальных наук

Література:

1. Задихайло Д. В., Кібенко О. В., Назарова Г. В. Корпоративне управління: Навчальний посібник. - Х.: Еспада, 2003. - 688 с.

2. Андрощук Г. А., Крайнев П. П. Экономическая безопасность предприятия: защита коммерческой тайны: Монография. - К.: Издательский Дом «Ин Юре», 2000. - 400 с.

3. Андрощук Г., Крайнев П., Кавасс И. Право интеллектуальной собственности: торговые аспекты. Науч.-практ. изд. - К.: Издательский Дом «Ин Юре», 2000. - 164 с.

4. Попович В. М. Економіко-кримінологічна теорія детінізації економіки: Монографія. - Ірпінь: Академія державної податкової служби України, 2001. - 524 с.

5. Вертузаев М. С., Вертузаев А. М., Юрченко А. М. Некоторые аспекты виртуальной разведки // Бизнес и безопасность.- 2002.- № 6.- С. 54-58.

6. Вертузаев М. С. Бенчмаркинг: особенности конкурентной разведки в бизнесе // Економіка та менеджмент: Матеріали V міжнародної науково-технічної конференції «АВІА-2003» 23-25 квітня 2003 року. - Т. 5-6. - К.: НАУ, 2003. - С. 6.17-6.20.

7. Vertuzaiev M. The View from the Former Soviet Union // Abstracts 2000 Annual International Conference «Transnational Crime, Corruption & Information Technology», Washington D.C., November 30 - December 1 2000, The Transnational Crime & Corruption Center American University Washington, D.C., 2000, p. 4.

8. Вертузаев М. С. Пластиковый бизнес в Украине или особенности национального мошенничества. - Ч.1. // Бизнес и безопасность. - 2001. - № 2. - С. 9-12.

9. Вертузаев М. С. Пластиковый бизнес в Украине или особенности национального мошенничества. - Ч.2. // Бизнес и безопасность. - 2001. - №3. - С. 5-7.

Захист від несанкціонованих та затяжних перевірок

Для кожного, хто тим чи іншим чином пов'язаний з веденням бізнесу, тема взаємовідносин із контролюючими органами здебільшого проблематична й гостра. Звичайно, хоча будь-яка діяльність пов'язана з певним ризиком, практика останніх років свідчить про те, що вже не одне підприємство стало банкрутом з вини безперервних візитів контролерів. Уміння правильно скористатися всіма існуючими засобами захисту від несанкціонованих та затяжних перевірок перш за все залежить від рівня знань. Особливо за сучасних умовне є винятком випадки, коли «ревізори» часто-густо плутають власну кишеню з державною.

Аналізуючи стан української економіки, більша частина зарубіжних економістів розвинених країн, вкрай обурена загальною некомпетентністю наших керівників. Український платник податків фактично більше стурбований – як би чого не порушити, «засвітиться», побоюючись потрапити в непосильні тиски чисельних перевірок. Фактично багатьом бізнесменам більше знайомі їх обов'язки, ніж існуючі права. Зрозуміло, що чисельну армію контролерів перш за все цікавлять обов'язки та відповідальність платників податків, а от про права найчастіше не знають.

Діючим законодавством надані наступні права, якими може скористатися кожен платник податків:

1. Подавати державним податковим органам документи, що підтверджують право платника податку на пільгове оподатковування в порядку, установленому Законами України. В Україні існує систематизований нормативний перелік усіх діючих пільг у сфері оподатковування, де вказуються конкретні умови та правила того чи іншого режиму оподатковування. Слід пам'ятати і те, що користування пільгами – це право, а не обов'язок.

2. Ті, кого перевіряють, мають право не тільки бути ознайомленим з висновками проведених контролюючими органами перевірок, але й у випадку незгоди з прийнятим рішенням, відмовлятися від підписання актів перевірки. Щоб засвідчити факт такої відмови, посадовими особами контролюючої служби повинен бути складений відповідний акт.

3. Після проведення ревізії (перевірки) існує право на звернення у контролюючий орган із пропозицією про перегляд рішення. Зауважимо, що бувають випадки, коли через відсутність можливості розрахуватися на даний момент по зобов'язаннях, іноді навіть вигідно розпочати процедуру адміністративного оскарження. Адже згідно пп. 5.2.3 ст. 5 Закону України № 2181-III, припиняється виконання платником податкових зобов'язань на строк від дня подачі скарги (заяви) контролюючому органу до дня закінчення процедури адміністративного оскарження. Оскаржена сума податкового зобов'язання вважається неузгодженою під час адміністративного оскарження, тільки після закінчення процедури адміністративного оскарження зобов'язання вважається узгодженим.

4. Кожен наділений правом оскаржувати у судовому порядку будь-які рішення державних контролюючих органів і дії їхніх посадових осіб.

Отже як ми вже зауважили, право оскаржити рішення або дію перевіряючих, закріплено за кожною зацікавленою особою.

Варто знати, що особа яке подала скаргу на рішення контролюючого органа, має право:

★ ознайомитися з усіма матеріалами перевірки;

★ особисто викладати існуючі докази та аргументи особі, що назначена перевірити скаргу;

★ надавати додаткові матеріали або наполягати на їхньому запиті;

★ бути присутнім при розгляді скарги;

★ користуватися послугами адвоката або вповноваженого представника;

★ одержати у письмовій формі відповідь про результати розгляду скарги;

★ пред'явити вимогу про дотримання таємниці розгляду скарги;

★ вимагати відшкодування збитків, якщо вони стали результатом неправомірних рішень;

★ відкликати або анулювати подану скаргу в будь-який час до ухвалення рішення про розгляд скарги.

Скарга подається в писемній формі й може супроводжуватися документами, розрахунками й доказами, які платник податків вважає за потрібне надати. Скарга повинна бути подана в контролюючий орган протягом 10 календарних днів, після дня одержання податкового повідомлення або іншого рішення контролюючого органа. При надходженні скарги, контролюючий орган зобов'язаний прийняти відповідне мотивоване рішення й направити його зміст протягом 20 календарних днів від дня одержання скарги. Надсилається рішення за поштовою адресою платника податків з повідомленням про вручення або віддається йому під розписку.

Якщо контролюючий орган направляє платникові податків рішення про повне або часткове незадоволення його скарги, такий платник податків має право звернутися протягом наступних 10 календарних днів, з повторною скаргою в контролюючий орган вищого рівня, а при повторному незадоволенні скарги – у контролюючий орган вищого рівня з дотриманням зазначеного 10-денного строку для кожного випадку оскарження й зазначеного 20-денного строку для відповіді на нього.

І все-таки, коли ще діло не дійшло до скарг і, коли ще й гадок немає про перевірку, перш за все треба неодмінно знати, хто взагалі уповноважений перевіряти. Так, згідно чинного законодавства, контроль за фінансовим станом підприємств покладений на:

★ органи державної податкової служби;

★ митні органи;

★ органи державного казначейства.

Здавалося б, небагато, але існуючу армію «ревізорів» цікавить не тільки фінансово-господарська діяль-ність підприємств, а й інші сторони його діяльності: санітарний стан приміщень, дотримання протипожежних норм, виконання інших норм діючого законодавства. Тож однойменна група органів контролю може нанести вам «дружній» візит із перевіркою.

В Україні правом проводити перевірку наділені:

1. Державна контрольно-ревізійна служба,
2. органи Державного казначейства
3. органи пожежного нагляду,
4. комітет з охороні прав споживачів,
5. санітарно-епідеміологічна служба та екологічна інспекція,
6. правоохоронні органи (міліція, СБУ, прокуратура),
7. Державний комітет зі справ по захисту прав споживачів;
8. Комітет по нагляду за охороною праці України;
9. Державний комітет будівництва, архітектури і житлової політики України та Державний комітет України по земельних ресурсах;
10. Державний департамент нагляду за дотриманням законодавства про працю;
11. Інспекція по контролю за цінами, по контролю за якістю лікарських засобів,
12. представники антимонопольного комітету,
13. комітет зі стандартизації, метрології й сертифікації,
14. Державна служба зайнятості,
15. Пенсійний фонд,
16. Фонди соціального страхування та ін.

Втім, навіть досвідчені юристи стверджують, що з'ясувати повний перелік контролюючих структур – завдання не з легких. Але не це головне, слід завжди діяти, виходячи з головного правила – будь-який контролюючий орган вправі діяти тільки у рамках своєї компетенції. Так, якщо Вас взявся перевіряти Державний комітет України по земельним ресурсах, а Ви ніякого відношення до землі не маєте, то таких ревізорів треба відправляти подалі.

Перше правило, ще до початку перевірки – намагатися максимально обмежувати доступ на Ваше підприємство «лже-ревізорів». Саме у ситуації, першого знайомства з «ревізором» наш головний ворог – поява паніки й розгубленості. Треба завчасно спланувати свої дії. Отже, ні в якому разі при одержанні вістки про перевірку не демонструйте свою стурбованість. Ніякого напруження не повинно бути, адже поява контролера, ще не доказ порушень. Перевіряючим треба знайти реальні факти порушення закону, що могли би підпадати під ознаку правопорушення.

Щоб бути впевненим, що ті, хто прийшов з перевіркою, є тими, за кого себе видають, пропоную наступну пораду – ще з порогу запропонуєте заповнити «Журнал реєстрації перевірок» і розписатися в ньому «ревізорам» у відповідній графі. Не зайвим буде переписати на окремому аркуші паперу всі відомості із пред'явленого вам посвідчення й направлення на перевірку, ще краще негайно зробити ксерокопії цих документів. Знайте, при виявленні неточностей у оформленні направлення на перевірку, у вас є право відмовити в перевірці.

Досконало вивчіть службові посвідчення контролерів. Інколи так трапляється, що контролер на секунду розкриває перед вами своє службове посвідчення, а потім ховає, а Ви навіть не встигли прочитати його особисті ініціали. Так не повинно бути! Уважно і ретельно перевірте все.

Порядок ведення Журналу реєстрації перевірок затверджено ще 10 серпня 1998 р. наказом Державного комітету України з питань розвитку підприємництва № 18. Втім він відкривається та ведеться за бажанням керівництва.

Ніколи не завадить перевірити, чи справді особи, які прийшли Вас перевіряти, представляють зазначену організацію. Дзвінок за вказаним телефоном допоможе уникнути багатьох складних ситуацій.

Уцілому наявність Журналу реєстрації перевірок – це прямий захист від несанкціонованих візитів. Бувають випадки відмови посадової особи, яка прийшла з перевіркою, підписуватися в журналі. А це вже підстава, щоб не допустити гостей до проведення перевірки. У разі відмови перевіряльника зареєструватися відповідно до існуючого Порядку ведення Журналу реєстрації перевірок суб'єкт підприємницької діяльності має право в триденний строк письмово повідомити контролюючий орган, у якому працює такий представник, про факт цієї відмови (ст. 10 Порядку). Крім того, ведення Журналу реєстрації перевірок дозволяє відстежити, як часто тим чи іншим контролюючим органом або відомством проводилися перевірки на Вашому підприємстві. Адже, планові перевірки можуть проводитися не частіше одного разу на рік.

Особливості перевірок

Останніми новинами нашого сьогодення є все масштабніша, характерна для всіх регіонів України, стурбованість пропонованої новим урядом реорганізацією контролюючих служб. Вирішується доля нині існуючої структури та повноважень контролюючих органів. Створення єдиного механізму фінансового контролю, підпорядкованого Міністерству фінансів досить сміливий крок. Можливими наслідками таких перетворень стануть, перш за все, повна ліквідація податкової міліції, що була створена з метою забезпечувати ефективність роботи податкової адміністрації та суттєве скорочення штату ревізорів.

Отже, 21 січня народні депутати внесли на розгляд парламенту законопроект № 6539 «Про внесення змін до деяких законів України про статус державних органів фіскального й бюджетного контролю». Цей Закон передбачає введення підпорядкованості Державної податкової адміністрації, Контрольно-ревізійного управління та Державної митної служби Міністерству фінансів України. Головна ідея цього документу досягнути в майбутньому чіткої координації між названими відомствами.

Найбільш значимим у новому Законі є те, що обов'язковою умовою для проведення позапланових перевірок стане рішення суду. І, якщо новий президент підпише Закон, всі позапланові перевірки будуть проводитися тільки за наявності судової санкції. Рішення суду буде необхідним також для будь-якого вилучення оригіналів фінансово-господарської й бухгалтерської документації, на призупинення операцій на банківських рахунках й інших фінансово-кредитних установах.

Новим законопроектом змінюється діючий Порядок координації проведення планових перевірок органами виконавчої влади, що відтепер буде визначатися Кабінетом Міністрів України. Забороняється проведення планових виїзних перевірок за окремими видами зобов'язань перед бюджетами, крім зобов'язань по бюджетних позиках і кредитам.

Важливий і той факт, що в новому Законі передбачене скорочення тривалості проведення планової перевірки, що не повинна перевищувати 20 днів, а щодо суб'єктів малого підприємництва – 10 (раніше було не більше 30). Максимальний строк проведення позапланових перевірок – 10 днів, а відносно суб'єктів малого бізнесу – 5. Що стосується періодичності планових перевірок, вони, як і раніше, будуть проводитися не частіше одного разу на рік.

Обов'язковим для контролюючого органа, що ініціює проведення позапланової виїзної перевірки, є подання в суд письмового обґрунтування підстав такої перевірки. У суді, при розгляді питання про надання дозволу на проведення позапланової виїзної перевірки, можуть брати участь представники суб'єкта господарської діяльності. Повідомлення про місце, дату й час розгляду в суді питання про надання дозволу на проведення позапланової виїзної перевірки повинне направлятися не пізніше, ніж за три робочі дні до дати такого розгляду. Тобто надається можливість усім зацікавленим особам доводити в суді необхідність проведення будь-яких позапланових перевірок.

Гордєєва Т.

НОВОСТИ

Щодо перекриття каналу незаконного ввезення в Україну валюти у великих розмірах

Служба безпеки України у взаємодії з митними та прикордонними органами перекрила канал контрабанди валюти. 9 лютого цього року було затримано групу військовослужбовців, які, використовуючи службове становище, налагодили канал нелегального ввезення в Україну валюти. Під час перетинання державного кордону України в них було вилучено понад 300 тисяч доларів США.

На даний час проводяться відповідні процесуальні дії.

Прес-центр СБ України

Блочные решения на базе технологии Инспектор+: DVI, VideoHUB, DVR Inspector

Основной тенденцией украинского рынка безопасности является постоянное повышение качества предлагаемых продуктов, в том числе и систем видеоконтроля, расширение их функциональности. Одним из направлений деятельности по повышению качества и функциональности систем видеоконтроля является создание блочных решений. Блочные решения значительно превосходят по надежности решения на базе обычных персональных компьютеров.

Тенденция развития рынка комплексов безопасности в направлении блочных, законченных решений иллюстрируется следующим фактом. В январе этого года был подписан долгосрочный договор между стратегическим партнером компании «Укр-Инвест-Консалтинг», компанией ISS (город Москва) и ведущим мировым лидером IT-индустрии, компанией IBM о создании решений для систем видеоконтроля на базе технологий «Инспектор» и серверов IBM.

Благодаря научно-техническому альянсу компаний ISS и IBM, в рамках которого осуществляется объединение технологий «Инспектор» с серверными решениями IBM, стало возможным создание уникальных систем Real-time Video Monitoring System, позволяющих вести многоканальное видеонаблюдение в формате «живое видео», использовать для обеспечения безопасности технологии распознавания образов и контроля транзакций.

Сотрудничество компаний в рамках подписанного договора позволит компании IBM в короткие сроки занять лидирующее положение на рынке средств безопасности, а продуктам технологии «Инспектор» – играть ключевую роль в формировании рынка самых современных средств безопасности.

Блочные решения создаются на базе специализированных компьютерных платформ. Оптимизированное программное обеспечение блочных решений обеспечивает многофункциональность, высокую надежность и повышенную сопротивляемость несанкционированным манипуляциям с оборудованием. Корпуса блочных решений разработаны таким образом, чтобы их удобно было монтировать в серверные стойки. Блочные решения поставляются проверенными и оттестированными на пиковых режимах работы. Заказчику, использующему блочное решение, достаточно только включить компьютерный блок в сеть бесперебойного питания, подключить видеокамеры и система готова к работе.

В категорию блочных решений от компании «Укр-Инвест-Консалтинг» входят: **DVI, VideoHUB,** а также ряд устройств **DVR Inspector,** специализированных под нужды предприятий малого и среднего бизнеса **DVR Inspector Standard,** крупных промышленных предприятий, DVR Inspector Industrial и банковских структур DVR Inspector Banking. Существуют устройства **DVR Inspector RealTime,** которые способны отображать видеоинформацию в формате «живое видео», причем один такой блок может обрабатывать от 4 до 16 видеоканалов. Блочные решения могут быть снабжены уникальной функциональностью на базе технологий SmartVideo, а именно технологии распознавания образов и контроля транзакций. Эти технологии являются уникальным инструментом для борьбы с мошенничеством, преступностью и терроризмом.

Все блочные решения от компании «Укр-Инвест-Консалтинг» имеют Сертификат соответствия требованиям Государственной системы сертификации УкрСЕПРО.

DVR Inspector

Компания «Укр-Инвест-Консалтинг» предлагает блочные решения DVR Inspector для партнеров и тех заказчиков, которым необходим исключительно надежный интегрированный комплекс безопасности.

Поставка систем безопасности именно в виде блочных решений DVR Inspector особенно актуальна в тех случаях, когда заказчику необходима система, которая удовлетворяла бы особенным требованиям, например:

★ в состав решения входит мощная видеоподсистема с большим количеством видеоканалов и высокой скоростью отображения видеоинформации (в этом случае к компьютерной платформе видеоподсистемы предъявляются особые требования);

★ необходимо обеспечить интеграцию с уникальным оборудованием (в этом случае не обойтись без дополнительного программирования и тестирования совместной работоспособности устройств);

★ используется сложное в настройке программное обеспечение класса SmartVideo, например, реализующие технологию распознавания образов.

Особенности построения блочных решений от компании «Укр-Инвест-Консалтинг» обеспечивают повышенную степень защищенности системы от несанкционированных изменений конфигурации системы, вызванных, например, некорректными действиями пользователя или вредительством.

Повышенная надежность таких решений обеспечивается оптимально подобранными техническими характеристиками оборудования и программного обеспечения. Так, при производстве блочных решений DVR Inspector используются специализированные компьютерные платформы, оптимизированные под весьма ресурсоемкие задачи видеонаблюдения. Это особенно актуально для профессиональных комплексов видеоконтроля, поскольку в таких системах в полной мере реализуется режим «триплекса» – подсистема видеоконтроля одновременно должна обеспечивать возможность вести видеонаблюдение, записывать видеоинформацию в архив и, не прерывая выполнение предыдущих задач, позволять просматривать информацию из видеоархива. Обращаем особое внимание на то, что при производстве DVR Inspector используется программное обеспечение, специально оптимизированное под специфику блочных решений. Таким образом, производство блочных решений поддерживается не только на аппаратном уровне, но и, начиная с версии 3.9 системы «Инспектор», на уровне программного обеспечения.

Таблица 1. Технические характеристики DVR Inspector

Версия продукта	DVR Inspector Standard	DVR Inspector Banking	DVR Inspector Industrial	DVR Inspector Real Time
Количество видеоканалов	до 16	до 32	до 64	до 16
Скорость отображения / записи (fps)	до 140	до 210	до 280	до 400
Количество аудиоканалов	до 16	до 16	до 64	до 16
Количество релейных входов / выходов	8/8	16/16	16/16	16/16
Глубина архива	500 Гб	750 Гб	до 1,2 Тб	до 1,2 Тб

Блочные решения DVR Inspector VideoServer проходят тщательную проверку качества их функционирования и многократное тестирование во всех возможных режимах эксплуатации. Производство блочных решений соответствуют международным стандартам качества ISO 9001.

Краткий перечень возможных конфигураций DVR Inspector VideoServer приведен в табл. 1.

Все классы блочных решений допускают удаленное администрирование и возможность дальнейшего наращивания системы безопасности путем увеличения количества отдельных блоков. При работе с DVR Inspector конечному пользователю доступен полный набор функциональности, присущий всем продуктам технологии «Инспектор». Кроме того, компанией «Укр-Инвест-Консалтинг» предлагаются блочные решения, обладающие функциональностью, необходимой для решения специфических задач, например, задач по распознаванию образов или контролю транзакций.

Архитектура построения блочных решений является гибкой и позволяет рассматривать целесообразность применения той или иной их конфигурации в зависимости от уровня производительности системы и обеспечиваемой функциональности. Это является более понятным и приемлемым для потребителя, поскольку позволяет подобрать оптимальное, для данного охраняемого объекта решение, обладающее наиболее подходящими техническими характеристиками.

Цифровые видеорегистраторы (DVI)

Устройства типа DVI являются специализированными и недорогими устройствами для решения единственной задачи – обеспечение видеоконтроля.

DVI(tm) (Digital Video Inspector) представляет собой цифровой видеорегистратор (система видеонаблюдения и видеозаписи). DVI – это охранный блок промышленного дизайна, встраиваемый в 19-ти дюймовую компьютерную стойку, полностью готовый к работе, не нуждающийся в техническом сопровождении и сконфигурированный в соответствии с задачами пользователя. DVI по надежности многократно превосходит аналоговую технику. При этом система настолько проста в эксплуатации, что с ней может работать любой неподготовленный пользователь – все операции по настройке DVI сводятся к подключению к нему монитора и видеокамер, а управляется видеорегистратор клавиатурой, размером с небольшой калькулятор.

DVI предназначен для организации охраны офисных и жилых помещений, небольших предприятий «семейного» бизнеса, гаражей и автостоянок и обладает всеми функциональными возможности систем созданных на базе технологии «Инспектор» – многоканальной видеозаписью, встроенным программным детектором движений, видеоархивом большой емкости, поддержкой удаленного доступа.

При работе с видеорегистратором DVI пользователю доступны следующие возможности:

★ автоматическая цифровая запись видео от нескольких видеокамер одновременно;
★ четырехуровневая компрессия (сжатие) видеоизображения;
★ использование программного детектора движения;
★ неограниченное количество зон детекции движения;
★ настройка детектора по размеру объектов;
★ запись тревожной ситуации при срабатывании детектора;
★ работа с виртуальным пользовательским экраном;
★ просмотр изображений с нескольких камер одновременно («мультиэкран»);
★ вывод изображения от камеры на весь экран· цифровое увеличение изображения;
★ просмотр архивных записей (прямой, обратный, ускоренный и покадровый просмотр);
★ поиск видеозаписей по дате и времени;
★ возможность программного улучшения качества изображения – низкокачественное изображение контрастируется, осветляется, помехи отфильтровываются;
★ возможность просмотра информации реального времени и видеоархива удаленно, используя локальную сеть (или Internet), без специального программного обеспечения

Краткие технические характеристики DVI представлены в табл. 2.

За счет использования уникального алгоритма DeltaWavlet достигается минимальный размер видеокадров при сохранении VHS-качества видеоматериалов. Объем информации на диске равен объему видеозаписи 10–20 трехчасовых VHS-кассет. При этом пользователь получает возможность найти нужные материалы в видеоархиве по дате, времени, номеру камеры. Наблюдение и просмотр видеоархива осуществляется без остановки видеозаписи (триплексный режим).

Таблица 2. Технические характеристики DVI

Версия продукта	DVI 125	DVI 250	DVI 500
Количество видеокамер	8	16	16
Скорость отображения / записи по всем камерам	12.5 кадров/сек	25 кадров/сек	50 кадров/сек
Количество камер, одновременно отображаемых на мониторе пользователя	1/4/6/8	1/4/6/9/16	1/4/6/9/16
Удаленный доступ к системе по локальной сети	есть	есть	есть
Удаленный доступ к системе через Internet с помощью браузера	есть	есть	есть
Объем видеоархива при одновременной непрерывной записи по всем видеокамерам	4 дня		
Объем видеоархива при записи по детектору движения	1–4 недели		
Габариты	90 x 430 x 370		

DVI оснащен интеллектуальным детектором движений. Пользователь может задавать области обнаружения движений в кадре, настраивать чувствительность детектора по размерам объектов, движущихся в поле зрения видеокамер (люди, животные, автомобили и т. д.). Благодаря этому DVI может выборочно производить видеозапись только при появлении объектов с заданными параметрами, игнорируя любые фоновые изменения (колышущуюся траву и листву, падающий снег или дождь), фильтруя оптические помехи и не допуская ложных срабатываний.

DVI присуща высокая степень защиты информации от несанкционированного доступа и вирусов. Устойчивость системы можно объяснить основательной архитектурой системы, которая состоит из независимых слоев, имеющих специфические возможности и строгое разграничение прав доступа.

Архитектура DVI оптимизирована для использования в сетевой среде и приспособлена к дистанционному управлению. Продукт оснащен средствами конфигурирования и администрирования, развитым интерфейсом локального или дистанционного мониторинга.

Необходимое для работы DVI программное обеспечение могут размещаться на специальных Flash-модулях памяти.

VideoHub (PC-based / non-PC-based)

Для передачи видеоинформации по телекоммуникационным каналам (LAN / WAN), когда нет необходимости устанавливать на данном участке объекта видеосервер и строить, таким образом, территориально распределенную систему видеонаблюдения, применяются специализированные устройства VideoHub. Различаются две модификации таких устройств: VideoHub PC-based и VideoHub non-PC-based.

Перед передачей изображения устройства осуществляют оцифровку и сжатие видеоданных с помощью алгоритма DeltaWavelet. Просмотр изображения можно осуществлять на любом удаленном компьютере с помощью стандартного web-браузера или

Таблица 3. Технические характеристики VideoHub PC-based

Разрешение	PAL 352 x 288 NTSC 320 x 240
Суммарная скорость	16 к/с, ч/б 12,5 к/с, в цвете
Компрессия	5 уровней, Wavelet
Количество видеовходов	до 8
Входы / выходы для сигналов тревоги	до 8 реле / лучей
Количество клиентов на одно устройство	неограниченно
Детектор движения	программный
Подключение видеокамер	8 композитных BNC видеовхода, 75 Ом/Hi Z.
Интернет-протоколы	TCP/IP
Безопасность	защита паролем
Источник питания	Внешний, 12 В

программного обеспечения Инспектор+.

К данному устройству можно подключить до 8 видеокамер. Особенностью реализации является повышенная аппаратная надежность, за счет применения флэш-памяти вместо механического жесткого диска, а также системы аппаратной диагностики сбоя аппаратуры, обеспечивающей автоматическую перезагрузку процессора при сбое.

Технические характеристики устройства указаны в табл. 3.

К VideoHub PC-based может подключать устройства охранно-пожарной сигнализации. Это позволяет предоставлять пользователю системы более полную информацию об охраняемом объекте.

Более простым решением с точки зрения использования является решение VideoHub non-PC-based. Это устройство на основе специализированного image-процессора, с помощью которого осуществляется оцифровка и аппаратное сжатие видеоданных посредством инновационного алгоритма Motion Wavelet. К одному такому устройству может быть подключено до 4 видеокамер.

Таблица 4. Технические характеристики VideoHub non-PC-based

Разрешение	PAL 704 x 288 или 704 x 576 в цвете
Суммарная скорость	25 к/с в цвете
Компрессия	5 уровней, Motion Wavelet
Количество видеовходов	до 4
Входы / выходы для сигналов тревоги	до 4
Количество клиентов на одно устройство	неограниченно
Источник питания	Внешний, 12 В

Технические характеристики устройства указаны в табл. 4.

Устройства VideoHub работают только в составе программно-аппаратного комплекса Инспектор+.

Блочные решения от компании «Укр-Инвест-Консалтинг» являются профессиональными решениями, базирующимися на технологиях «Инспектор» и SmartVideo. Они уже находят своего потребителя. Компания «Укр-Инвест-Консалтинг» и её партнерская сеть обеспечивает поставку всего перечня оборудования и его техническую поддержку по всей территории Украины. Сервисные центры компании «Укр-Инвест-Консалтинг» расположены в городах: Винница, Днепропетровск, Донецк, Житомир, Запорожье, Ивано-Франковск, Кировоград, Кременчуг, Кривой Рог, Луганск, Луцк, Львов, Мариуполь, Николаев, Одесса, Полтава, Ровно, Севастополь, Северодонецк, Симферополь, Сумы, Тернополь, Харьков, Херсон, Черкассы, Чернигов, Черновцы, Феодосия, Ялта.

Литвиненко М. И.,
консультант по продажам
компания
«Укр-Инвест-Консалтинг»
Тел./факс 8(044) 538-00-12
http://www.security-systems.com.ua
Maxim.Litvinenko@ukr-invest.com.ua

НОВОСТИ

В США обсуждают возможность налога на интернет

Растущая зависимость человечества от Сети не могла пройти бесследно мимо фискальных органов. Недавние сообщения из объединенного комитета по налогообложению Конгресса США позволяют сделать вывод о том, что налог на телефонные переговоры, впервые введенный в качестве налога на «предметы роскоши» более 100 лет тому назад, может быть распространен на все телекоммуникационные услуги, включая интернет. По мнению обозревателя BBC Билла Томпсона (Bill Thompson), развитие Сети достигло той стадии зрелости, когда этот вопрос может быть поставлен со всей определенностью.

В настоящее время в США взимается 3-процентный налоговый сбор с телефонных звонков по фиксированным сетям, однако рост объема услуг связи, предоставляемых мобильными операторами и посредством протокола VoIP, ведет к прогрессирующему неравноправию операторов рынка связи. Одним из решений возникшей дилеммы могло бы стать точно такое же налогообложение мобильной и VoIP-связи, как и обычных телефонных звонков. Тем не менее, комитет по налогообложению Конгресса США решил подойти к проблеме максимально масштабно. Предлагается ввести единый налог на телекоммуникационные услуги вообще. Рвение американских законодателей у граждан страны понимания не встретило. В глазах многих из них сама мысль о необходимости щедрого финансирования государства ради общественного блага вообще воспринимается как опасный либерализм, граничащий с коммунизмом. Посыпались альтернативные предложения - отменить налог на связь вообще. Сторонники этой точки зрения указывают, что находчивые граждане всегда будут искать и успешно находить лазейки, позволяющие утереть нос власти.

Еще пять - десять лет назад прекрасным аргументом против «налога на Сеть» являлась сама новизна технологии, относительно небольшое число ее пользователей, а также тот факт, что любой, какой бы то ни было, фискальный режим привел бы к искажению изначальной идеи. Вместо максимального удобства Сети для пользователей ее развитие было бы подчинено требованиям и логике системы налогообложения. Однако сейчас, когда в ряде стран - например, в США и Великобритании - большая часть граждан уже «вышла в онлайн», данный аргумент утратил свою бесспорность.

Фактически, многие уже сейчас платят налог на Сеть - даже в либеральной Америке. Ряд штатов, в частности Алабама и Флорида, взимают налог с широкополосного доступа по технологии DSL, трактуя его как предоставление телекоммуникационных услуг. В Висконсине с 1991 года действует 5% налог на доступ к Сети. Тамошние законодатели проявили завидную расторопность - налог был введен еще до вступления в силу общеамериканского закона о запрете налогообложения интернета (так называемый Internet Tax Freedom Act), который стал барьером на пути обложения Сети новыми налогами.

В Великобритании, а также в европейских странах доступ в Сеть облагается налогом на добавленную стоимость. Тем же налогом облагаются и онлайновые покупки.

Тем не менее, на повестке дня стоит более спорный вопрос - о введении особого налогового режима, учитывающего специфический характер Сети. Речь идет об обложении налогом Сети как таковой - а не просто о приплюсовывании налогов к счетам за доступ в нее. В настоящее время пользовательская активность в Сети не учитывается вообще. Тем не менее, отсутствие платежной системы, которая позволила бы взимать налоги «за Сеть», отнюдь не означает, что такая система не появится в один прекрасный день.

Тема введения налога «на Сеть» - чрезвычайно болезненная, а сам такой гипотетический налог вряд ли будет воспринят обществом с пониманием и одобрением. Тем не менее, прогресс не стоит на месте, и по мере того, как интернет со своей инфраструктурой будет все глубже проникать в нашу жизнь, становясь важной частью ежедневной активности человека, вопрос о введении налога на него рано или поздно, но неизбежно будет поставлен властью.

CNews.ru

Надежная защита Ваших денег

В связи с обилием ценных бумаг и документов, требующих сохранности,увеличением колличества поддельных банкнот, перед самыми широкими слоями населения встала проблема обеспечения безопасности имущества. Ее можно осуществить с помощью целого ряда элементов, среди которых одно из основных мест занимают сейфы.

Сегодня на рынке предлагаются сотни модификаций данной продукции. Как же сделать правильный выбор и кому можно доверить свои деньги и ценные бумаги? НТО Олимпик имеет уже десятилетний опыт работы на отечественном рынке. Среди его постоянных клиентов ведущие банки Украины, многие финансовые структуры, посольства, частные фирмы.

Что же привлекает многочисленных клиентов к продукции, поставляемой НТО Олимпик? Это – качество, разнообразие продукции и индивидуальный подход к каждому клиенту.

НТО Олимпик предлагает множество моделей сейфов как отечественного, так и зарубежного производства. Кроме внешнего вида, целевого назначения, качества и цены сейфы отличаются друг от друга габаритами, конструкцией корпуса, дверей и запирающих устройств, технологией изготовления, использованными материалами, выполняемыми функциями, наличием торговой марки, хорошо зарекомендовавшей себя у покупателей, гарантийным сроком. Стоит отметить, что в последнее время многие специалисты отдают предпочтение сейфам украинского производства, отмечая их надежность по сравнению с зарубежными аналогами.

По желанию заказчика можно встроить сейф в стол, шкаф, тумбочку или иную офисную мебель. Это затруднит его поиск злоумышленником и, соответственно, увеличит безопасность хранения ценностей.

НТО Олимпик осуществляет сервисную поддержку поставляемой им продукции. В случае потери либо поломки ключа специалисты фирмы помогут решить эту проблему своим клиентам. Они прошли курсы обучения ремонту и техническому обслуживанию оборудования и имеют сертификаты от фирм-производителей.

Сотрудники НТО Олимпик помогут Вам правильно выбрать сейф, подобрать его исходя сугубо из Ваших условий и требований. Они заинтересованы в том, чтобы предложить покупателю наиболее подходящий сейф, потому что престиж НТО Олимпик и его доброе имя чрезвычайно важны и деньгами не оцениваются.

Но сейфами не ограничивается ассортимент продукции, поставляемой НТО Олимпик. Клиентам также предлагаются разнообразные и необходимые в наше время детекторы валют таких, зарекомендовавших себя на рынке фирм, как CashScan, SuperScan, DORS, D100, XD120.

Любой заказчик может подобрать себе модель детектора, полностью отвечающую его требованиям. Имеются в наличие портативные, универсальные, профессиональные и автоматические детекторы валют.

Как известно, для защиты банкнот используется несколько основных элементов. Например, бумага, различные специальные добавки к которой придают ей специфическую жесткость, а в отраженных УФ-лучах такая бумага не люминесцирует, в отличие от обычной. Также используется полиграфическая печать с эффектом орловской печати и ирисовым раскатом. Немаловажны и оптические эффекты, использование специфических красок, ультрафиолетовая и магнитная защита, клип-эффект, совмещенные рисунки, тактильный эффект и многие другие элементы защиты.

Кассир или другой служащий, работающий с деньгами, не всегда может определить подлинность купюры «на глаз», особенно это касается банкнот крупного номинала, которые подделываются чаще всего на достаточно хорошем оборудовании, что делает их почти неотличимыми от настоящих купюр для человеческого глаза.

Полностью решить эту проблему и помогают поставляемые НТО Олимпик детекторы валют. С помощью них можно проверять подлинность не только денег, а и ценных бумаг, водительских прав, кредитных карточек и аналогичных документов, что поможет Вам избежать подделок и мошенников. А это – немаловажный фактор в обеспечении безопасности финансовых операций.

И последнее, но не менее важное – защита информации. Надежным помощником в этом Вам также станет НТО Олимпик. С помощью шредеров (производства таких известных фирм, как Schieicher & Co International AG, Speed, HSM, GBC), которые предлагаются этой фирмой, Вы сможете уничтожить любой носитель информации - от бумажного листа, до дискет, дисков и других носителей информации.

Количество уничтожаемых за раз листов тоже может варьироваться в зависимости от моделей того или иного шредера. Оно составляет как пару, так и сотни листов. Клиент может подобрать модель, мощность которой будет полностью удовлетворять его потребности.

Уничтожители делятся на пять степеней секретности (General, Internal, Confidental, Secret, TOP secret) – это зависит от величины кусочков измельченной бумаги.

По производительности шредеры делятся на персональные (уничтожение информации как на рабочем месте, так и в домашних условиях), офисные (производительность, отвечающая высоким требованиям и бесшумность) и профессиональные (уничтожение любого носителя информации – бумаги, дисков и т. д.).

Основные преимущества уничтожителей, поставляемых НТО Олимпик:

★ Возможность перерабатывать документы вместе со скрепками, благодаря особым свойствам стальных ножей.

★ Низкий уровень шума.

★ Полное соответствие стандартам и другим регламентирующим документам.

★ Экономичность (низкое потребление электроэнергии).

★ Повышенная безопасность. Почти все аппараты автоматически включаются при попадании документов в загрузочное окно и останавливаются после окончания обработки, осуществляя световую индикацию режимов работы и блокировку двигателя при открытом или переполненном контейнере. Все аппараты имеют устройства, затрудняющие случайное попадание предметов в ножи (галстуки, волосы, манжеты...).

★ На ножи уничтожителей Taros всемирного лидера – торговой марки Martin Yale предоставляется пожизненная гарантия.

Многолетний опыт работы на рынке банковского оборудования, профессионализм сотрудников, качество поставляемой продукции удовлетворят любого клиента. А философия НТО Олимпик сделает наше сотрудничество продуктивным и приятным для обеих сторон. Наша продукция станет надежной гарантией безопасности Вашего бизнеса!

г. Киев,
ул. М. Коцюбинского, 4Б,
оф. 10
тел. (044) 255-16-00
(многоканальный)
http://www.olympic.kiev.ua

Пропонуємо нові можливості перевірених часом рішень!

Комплексна електронна система безпеки об'єктів
версії КСБО КМ-4_05 єднає в собі можливості контролю доступу з обліком робочого часу працюючих, відеоспостереження та охоронної сигналізації;
призначена для підприємств і організацій з кількістю робітників до 24 тисяч.

ФОРПОСТ - автономна комп'ютерна система безпеки для офісів і житла.

★ Наші системи забезпечують безпеку підприємств, організацій, офісів, житла на сучасному рівні.
★ Ми виконуємо всі необхідні роботи по введенню наших систем безпеки в експлуатацію.
★ Наші системи проектуються з урахуванням побажань Замовників.
★ Програмне забезпечення КСБО КМ і ФОРПОСТ функціонує в ОС WINDOWS - 98 SE; 2000; XP.
★ Гарантійний термін на встановлені нами системи безпеки - 3 (три) роки.

Детальна інформація про можливості систем знаходиться на сайті

www.km-cs.com

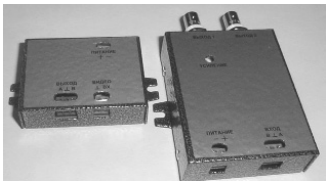
Нові пристрої для систем відеоспостереження

Комплект - передавач та приймач - типу ППВП-2_КМКС

забезпечує передачу та прийом електричних сигналів від телекамер.

Основні технічні характеристики комплекту:

★ Фіксована зміна АЧХ на кожні 100 м телефонного кабелю ТПП еп 5 х 2 х 0,5 на довжинах від 200 м до 1000 м.
★ Відсутність взаємного впливу сигналів при передачі їх по неекранованим парам одного кабелю.
★ Нелінійність АЧХ в діапазоні від 50 Гц до 5 МГц не перевищує 4 дБ.
★ Напруга живлення від 10 до 15 В.
★ Струм живлення не перевищує 50 мА.
★ Вмонтовані елементи грозозахисту.
★ Діапазон робочих температур від -40 до +85 °С.
★ Розмір корпусів: передавача – 50 х 65 х 20 мм; приймача - 85 х 65 х 20 мм.

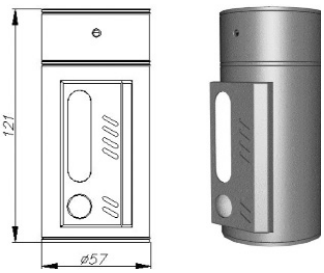


Для з'єднання однієї телекамери з монітором потрібна одна пара передавач-приймач.
Загальна ціна комплекту передавач-приймач типу ППВП-2_КМКС - 264 грн з ПДВ.

Вандалостійкий переговорний пристрій з телекамерою

Пристрій ГРАН_КМКС об'єднав у циліндричному стальному корпусі зовнішню вандалостійку частину домофону AVC-109 та телекамеру КРС-190SP4.
Пристрій призначений для зовнішніх пунктів переговорів з можливістю зовнішньої орієнтації телекамери і має необхідні елементи для різних варіантів установки.
Діапазон робочих температур від -50 до +75 °С.
Ціна 540 грн з урахуванням ПДВ:

- телекамера КРС-190SP4 – 330 грн,
- переговорний пристрій AVC-109 – 90 грн,
- корпус ГРАН – 120 грн.



Підприємство «Квазар-Мікро. Компоненти і системи»
Україна, 04136, м. Київ, вул. Північно-Сирецька,1
тел.: (044) 434-85-55; тел./факс: (044) 442-93-77
E-mail: office@km-cs.com; web: www.km-cs.com

КВАЗАР-Мікро®
КОМПОНЕНТИ І СИСТЕМИ

Комплексные системы санкционированного доступа компании IDTECK

Обеспечение различных уровней безопасности в системах санкционированного доступа достигается за счёт применения комплекса идентификаторов различных технологий с гибкой логикой их использования и принятия решения на доступ.

Современные системы санкционированного доступа (ССД) должны иметь возможность в зависимости от тех или иных условий применения обеспечение различных уровней безопасности (достоверности идентификации), пропускной способности, устойчивости к воздействию дестабилизирующих факторов и иных требований к системам доступа.

Решить эту важную практическую задачу в одной системе возможно за счёт комплексного применения идентификаторов, считывателей и контроллеров различных технологий с гибкой логикой их использования и принятия решения на доступ.

Указанные принципы реализуются в ССД компании IDTECK Co.(Южная Корея), использующей в своих разработках как широко применяемые технологии проксимити- и смарт-карт, так и перспективные биометрические считыватели (БС) по отпечаткам пальцев, лицу и голосу человека.

Распознавание лица, имеющего право на доступ по указанным технологиям, коротко сводится к следующему.

Идентификация предъявителя пассивной или активной проксимити-карты, контактной или бесконтактной смарт-карты осуществляется на основе считывания заложенного в картах персонального кода и сравнении его с соответствующим кодом, заложенным в блок памяти системы. Применение карт обеспечивает высокую пропускную способность ССД, реализует дистанционный способ считывания информации, что даёт возможность их использования в автоматических системах доступа, характеризуется низкими затратами на эксплуатацию. Кроме того, возможность многократной записи и перезаписи различной информации в смарт-карте делает её универсальным средством не только доступа в различные контролируемые зоны, но и средством платежа, учёта времени и. д. Вместе с тем, процесс считывания персонального кода по радиоканалу может привести к блокированию таких ССД помехами, перехвата кода карты. Кроме того, карта может быть утеряна или похищена.

Биометрические считыватели, снимая персональные физиологические характеристики человека, обеспечивают более высокую достоверность идентификации и степень защиты по сравнению с другими технологиями доступа благодаря большому объёму используемых данных о человеке как носителе уникальной информации, которую практически невозможно сымитировать, передать другому человеку, потерять и т. д.

Рис. 1. Считыватель - контроллер FINGER 007

Идентификация по отпечатку пальца

Это самая распространённая биометрическая технология, применяемая в системах доступа (52 % от всех биометрических систем). В её основе лежит использование индивидуального рисунка папиллярных линий на пальцах руки. В качестве признаков для идентификации могут быть взяты вершины отпечатка пальца, точки пересечения линий отпечатка с контуром определённого вида, тангенциальные характеристики линий и т. д. Обьём используемых параметров определяется задаваемым уровнем безопасности.

При использовании технологии распознавания по «картам контрольных точек», на папиллярных линиях определяются для каждого человека узловые точки, по которым формируется цифровой шаблон. Этот шаблон хранится в базе данных и используется при идентификации. Изображение отпечатка пальца по нему получить нельзя, что является дополнительной защитой ССД.

Для повышения достоверности распознавания, считывание отпечатка производится N(N = 2–3) раз. Если считать, что по каждому предъявленному отпечатку принимается частное решение, то результирующая вероятность правильного распознавания $P_{прN}$ определяется как

$$\mathbf{P}_{прN} = 1-[1-P_{пр1}]^N,$$

где $P_{пр1}$ - вероятность правильного распознавания при единичном считывании.

Таблица 1

	Считыватель +контроллер		Считыватель	
	FINGER 007	**FACE 007**	**Считыватель 007**	**FACE 007**
Тип биометрической системыи дентификации	По отпечаткам пальца	По лицу	По отпечаткам пальца	По лицу
Функции	Контроль доступа и учет времени	Контроль доступа и учет времени	Контроль доступа	Контроль доступа
Программируемый состав комплексов считывателей	1.Проксимити (смарт) – карта 2.Проксимити (смарт) – карта+ отпечаток пальца 3.Проксимити (смарт) – карта + PIN код (4разр.)+ отпечпток пальца 4.PIN код (4–8разр.)+ отпечпток пальца	1.Проксимити (смарт) – карта 2.Проксимити (смарт) – карта+ лицо 3.Проксимити (смарт) – карта + PIN код (4разр.)+ лицо 4.PIN код (4–8разр.)+ лицо	1.Проксимити – карта + (PIN код) 2.Проксимити (смарт) – карта+ отпечаток пальца 3.Проксимити (смарт) – карта + PIN код (4разр.)+ отпечпток пальца 4.PIN код(4–8разр.)+ отпечпток пальца	1.Проксимити – карта + (PIN код 2.Проксимити (смарт) – карта+ лицо 3.Проксимити (смарт) – карта + PIN код (4разр.)+ лицо 4.PIN код (4–8разр.)+ лицо
Время считывания (проверки) : карты отпечатка (лица) идентификации	30 мс < 1 сек 3 сек	03 мс < 0,5 сек	< 1 сек < 3 сек	< 0,5 сек
Частота работы проксимити–карты и дальность считывания, Д	125 кГц ~10 см	125 кГц ~10 см	125 кГц ~10 см	125 кГц ~10 см
Ошибка модуля распознавания по отпечатку пальца, FAR FRR	0,001 % 0,1 %		0,001 % 0,1 %	
Объем памяти по : отпечаткам пальца изображениям лица событиям в буфере	720 / 2.000 / 4.500 26.000	10.000 23.000	720 / 2.000 / 4.500	10.000
Диапазон рабочих температур	15 °С ...+ 40 °С	15 °С ...+ 40 °С	15 °С ...+ 40 °С	15 °С ...+ 40 °С
Питание	DC 12V I макс =300 мА	DC 12V I макс =1А	DC 12V I макс =300 мА	DC 12V I макс =1А
Вес	547 г	600 г	500 г	600 г

Помимо оценки эффективности ССД по вероятности правильного распознавания, используются вероятности ложного отказа в доступе (ложного несрабатывания) – ошибки первого рода FRR и вероятности ложного доступа (ложного срабатывания) – ошибки второго рода FAR.

Большой объём анализируемых вычислителем данных и образов, заложенных в память контроллера, требует значительного времени для принятия решения, что сказывается на пропускной способности системы. Для уменьшения

Рис. 2. Считыватель-контроллер FACE 007

времени идентификации до 0,1...1 сек. биометрический считыва тель имеет дополнительную клавиатуру для набора PIN-кода его владельца или считыватель карты.

Заметим, что для достоверного распознавания требуется четкая картина отпе-

Рис. 3. Сканирование лица в считывателе-контроллере FACE 007

чатков пальцев. При искажении этой картины ожогами, порезами, какими-либо наслоениями возрастают ошибки идентификации.

При распознавании по лицу

широко распространён антропометрический (геометрический) метод идентификации. Суть метода состоит в выборе на лицевой области человека «ключевых» точек с последующим выделением на базе этого набора характерных признаков. В качестве признаков выбирают расстояние между «ключевыми» точками,

Рис. 4а. 1 УБ - 4 - 6 разрядный PIN- код

отношение таких расстояний и другие параметры. Используемыми точками могут быть уголки глаз, губ, кончики ушей, носа, центры зрачков и т. д. При наличии в системе функции распознавания «живого» лица в процессе идентификации отбрасываются такие элементы на лице, как наличие очков, накладных бороды, носа и т. д.

Рис. 4б. 2 УБ - смарт (проксимити) - карта + набор PIN кода

Сканирование лица человека для последующего формирования его модели для записи, идентификации и проверки может осуществляться и в ИК-диапазоне. С этой целью специальное устройство осуществляет структурную ИК-подсветку лица, на основе которой методами триангуляции создаётся его трехмерная поверхность с точностью до миллиметра. В качестве обобщенного индивидуального признака человека используются особенности его черепа, которые не меняются с возрастом.

Эффективность метода распознавания

Рис. 4в. 3 УБ - считыватели карты, PIN кода и отпечатка пальца

по лицу требует надёжного механизма выделения черт лица и конструирования набора связей (биометрического шаблона), компенсации влияния изменения освещения, положения лица, его выражения и других факторов, возможности обработки двухмерных и трёхмерных изображений.

В системах доступа с **идентификацией по голосу** человека в качестве измеряемых характеристик используются :

-резонансные частоты рече-вого аппарата пользователя;

Рис. 4г. 4 УБ - считыватели карты, PIN кода, отпечатка пальца и лица

-период высоты тона ;

-огибающая формы сигнала и т. д.

Для компенсации незначительных отклонений в звучании человеческого голоса, вызванных влиянием эмоционального и физического состояния человека в момент речи, разработаны специальные программы. Уровень ошибки составляет 2–5 %.

Считыватели различных технологий, разработанные и используемые в ССД компании IDTECK Co., позволяют организовать пять различных уровней безопасности (**УБ**). Первый уровень обеспечивается за счёт набора на клавиатуре персонального 4–6 разрядного PIN-кода. Каждый последующий более высокий уровень безопасности, обеспечиваемый ССД, организуется за счёт добавления соответственно считывателей смарт (проксимити)- карты, отпечатка пальца, лица и голоса человека. Пятый уровень, включающий полный набор всех перечисленных типов считы-вателей, является самым высоким и используется при организации доступа на особо важные обьекты. Повышение уровня безопасности при комплексном применении идентификаторов различных технологий определяется тем , как используются данные распознавания по кажому из них.

Рис. 4д. 5 УБ-считыватели карты, PIN кода, отпечатка пальца, лица и голоса

При независимой работе каждого устройства идентификации и принятия в нем решения по распознаванию результирующая вероятность распознавания $P_{пр\Sigma}$ определяется как

$$P_{пр\Sigma} = 1-(1-P_{пр1})(1-P_{пр2})...(1-P_{прN}),$$

где $P_{пр1}$, $P_{пр2}$, ...$P_{прN}$ вероятность распознавания идентификаторов 1,2,...N. В случае, если результаты распознавания одного идентификатора (карты или PIN кода) используются для предварительного распознавания пользователя в одном из биометрических контроллёров, имеющего больший объём анализируемых вычислителем данных и образов, то результирующая вероятность правильного распознавания приблизительно может быть оценена следующим образом

$$P_{прр} = P_o\ [1-(1-P_o)\sqrt{1-r^2}\ ],$$

где $P_o = P_{пр1} = P_{пр2}$ - вероятности распознавания каждым из контроллёров;

r- коэффициент корреляции по распознаванию между первым и вторым устройством. Выигрыш во времени по идентификации за счет предварительного распознавания можно ориентировочно оценить коэффициентом

$$K_{вр} = \frac{M1}{M2},$$

где M - массивы используемых данных в памяти биометрического контроллера до (M_1) и после (M_2) предварительного опознавания.

Технология использования смарт-карт позволяет хранить биометрические признаки не в контроллере системы доступа, а в самой смарт- карте пользователя, чем обеспечивается существенное увеличение базы клиентов и скорости идентификации.

Технические характеристики считывателей и считывателей-контроллеров базовых моделей биометрических систем доступа компании IDTECK Co. приведены в табл. 1. Для организации системы контроля доступа автомобилей на открытые пло-

Рис. 5. Дистанционное считывание активной проксимити-карты

щадки, подземные и многоэтажные стоянки и т. д. компания IDTECK Co. предлагает радиочастотные считыватели большой дальности для пассивных и активных проксимити-карт. Активные карты IDA 150, IDA 200 (частота 125 кГц, считыватель RF-70) обеспечивают соответственно дальности 1,5 и 2,1 м, а карта IDA 500 (частота 311 мГц, считыватель RF-500) – до 5 м.

Предприятие СтилАрм является эксклюзивным дистрибьютером компании IDTECK Co. в Украине и обеспечивает полный комплекс услуг по продаже, монтажу и техническому сопровождению систем санкционированного доступа как выше указанной компании так и других производителей.

Родионов С. С.,
Косович О. М.

НОВОСТИ

США: программа-шпион фиксирует все действия оператора - от клавиш до буфера памяти

По нарастающей идет разработка программ-шпионов, где ни одно действие оператора невозможно скрыть.

Так, компании 3ami и BridgeHead Software создали систему Monitoring, Auditing & Security (MAS), которая позволяет сохранять информацию обо всех действиях, совершенных пользователем на компьютере: нажатие на клавиши, операции с мышью, с программами, с документами.

Также "шпион" может делать снимки открывавшихся приложений. Перехваченные данные можно сохранить на диск в реальном времени или, из буфера в памяти, на ежедневной основе. По сообщению разработчиков, в среднем потребности в хранении для одного ПК составят около 16,4 Мбайт в месяц. MAS позволяет производить поиск по сохраненным данным или вывести информацию за определенное время.

Internet.ru

НОВОСТИ

Мониторинг электронной почты сотрудников: мнения менеджеров разделились

Актуальность проблемы внутренних угроз для корпораций подтверждает статистика: по различным оценкам, от 70 до 80% потерь от преступлений в сфере ИТ приходится на атаки изнутри.

Независимый консультант по вопросам развития интеллектуального капитала Валерий Оськин в беседе с CNews отметил, что сегодня позиции не просматривать содержание переписки сотрудников придерживается более половины российских работодателей. «Существует еще 10-15% работодателей, которые считают слежку аморальной даже в том случае, если у них имеется возможность следить за подчиненными», - отмечает он. И львиная доля фирм, подвергающих своих сотрудников тотальному контролю, уже несет все большие потери в интеллектуальном капитале. Во-первых, сотрудники, чувствуя недоверие работодателя, придерживают «для себя» часть информации, которая могла бы пополнить интеллектуальный капитал организации. Во-вторых, работники снижают стремление творить для компании, ограничиваясь выполнением задания. При этом часть творческой энергии, которая могла быть направлена на работу, переключается на области деятельности, лежащие вне интересов работодателя. В-третьих, такие организации начинают покидать таланты, которые являются наиболее ценной составляющей человеческого капитала компаний. И, наконец, такие сотрудники, покидая недоверчивую компанию, чаще всего уходят к конкурентам. Моральное право на это им также дает проявленное недоверие. При этом, по мнению г-на Оськина, надо признать право компаний, в особенности - крупных финансовых структур - на определенную перлюстрацию информации. Но и каждая из фирм выбирает, реализовать это право или нет. «Думаю, что в дальнейшем компании будут все чаще отказываться от перлюстрации почты сотрудников, создавая корпоративную культуру, для которой разглашение закрытой информации будет неприемлемо, - считает он. - С другой стороны, если в компании работает «засланный казачок» или сотрудник, имеющий против нее злой умысел, то перлюстрация не станет препятствием для его реализации».

Большая часть опрошенных CNews респондентов - менеджеров крупных и средних компаний, - считают, что развивающаяся паранойя у руководителей - не самый удачный вариант обезопасить компанию. В то же время, в этом вопросе все зависит от корпоративных правил и политики информационной безопасности той или иной компании. «Перлюстрацию сообщений можно по-разному организовать, к примеру - сохранять все письма на сервере, независимо от того, удалили ее из личных ящиков или нет, и в случае чего - проверять, - рассказывает CNews менеджер одной из ИТ-компаний. - Но сидеть и читать всю почту всех сотрудников - это никому не нужно».

«Читать чужие письма безнравственно. Даже электронные, - уверен еще один респондент CNews. - Но для того чтобы придать процессу перлюстрации видимость приличия нужно, чтобы сотрудники были оповещены о ней заранее; необходимо также, чтобы личная переписка в теме письма была помечена как личная». По его мнению, еще один вариант - документально зафиксировать пользования IT-ресурсами компании (оговорить запрет использования e-mail в личных целях, обозначив при этом, какие именно цели являются личными). Ну, а если проверка осуществляется в целях предотвращения утечки коммерческой тайны - то в компании должен быть полностью оформлен и подписан сотрудниками соответствующий пакет нормативных документов.

Коммерческие компании во всем мире серьезно обеспокоены растущим количеством кибер-преступлений. Чтобы защитить себя от подобных нападений, они всерьез подумывают о том, чтобы внедрить систему мониторинга действий собственных сотрудников. А на днях в США было объявлено о создании программного обеспечения, позволяющего компаниям следить за каждым нажатием клавиши на клавиатурах компьютеров своих сотрудников. Данные программы можно будет использовать в качестве доказательства компьютерных преступлений в суде. Система, разработанная компаниями 3ami и BridgeHead Software, позволяет контролировать, записывать и сохранять все действия компьютера, не допуская при этом вмешательства извне в уже сохраненный файл. Разработчики уверены, что новая программа позволит компаниям отслеживать украденные файлы, устанавливать факт их отправки, копирования, записи на другие носители, распечатки или удаления.

Тем временем, многие американские правозащитники недовольны перспективой поголовного мониторинга действий сотрудников. Авторы программного обеспечения, отстаивая право на жизнь своего продукта, отмечают: «Люди должны уяснить, что они используют компьютер в качестве представителя компании, на которую они работают, а их работодатель имеет право хранить данные о действиях этого компьютера».

http://cnews.ru/

Решение проблем безопасности с помощью биометрической системы контроля доступа

Все мы уже привыкли к традиционным замкам, с обычными металлическими ключами, которые мы всегда носим с собой. У многих, особенно у руководителей и материальноответственных лиц на предприятиях, имеются целые связки ключей, для ношения которых продаются специальные футляры, а в сумках делают специальные отсеки. Иногда случается, что мы теряем ключи, из-за этого обычно происходит много неприятностей, и, как правило, в таких случаях обычно меняются замки. Особенно болезненна потеря ключей от помещений, в которых хранится дорогостоящее оборудование, деньги или другие ценные вещи, в результате возникает множество проблем, теряется время, нарушаются планы, графики, или вообще происходят ЧП.

Одним из основных недостатков традиционных замков является их примитивность, т. е. обычный ключ легко скопировать, подделать или открыть замок с помощью отмычек. Другим недостатком является то, что факт и время открытия, а тем более попытки открытия невозможно проконтролировать. Следствием этих недостатков является возникновение множества различных недоразумений: пропажи, недостачи, воровство и многое другое, и самый неприятный момент – это то, что доказать или зафиксировать факт проникновения невозможно.

На многих предприятиях, для исключения таких случаев устанавливаются камеры видеонаблюдения, которые частично решают эти проблемы. Но тут тоже есть свои недостатки, человек (сотрудник фирмы или преступник) может пройти так, что на видеозаписи трудно или вообще невозможно будет идентифицировать личность. Например, на записи, можно будет видеть только заднюю часть туловища или человек может надеть очки, головной убор и пройти так, что его никто не узнает, особенно при плохом освещении.

Такие ситуации бывают очень часто и, к сожалению, с этим ничего не поделаешь, опытные преступники, и

Пример с камеры видеонаблюдения: человека стоящего перед дверью идентифицировать невозможно

мошенники часто совершают свои дела, не взирая на то, что установлены камеры. Кроме того, сигнал обычной видеокамеры подделать или создать помехи еще проще, чем сделать копию ключа.

Существуют еще системы контроля доступа по пластиковым карточкам, т. е. чтобы пройти нужно приложить к считывающему устройству персональную карточку. Такие системы позволяют фиксировать время прохода, но к сожалению в плане идентификации личности ситуация ничем не отличается от той, что с обычными ключами, т. к. пластиковую карту можно также как и ключ передать другому лицу, потерять, а поломать еще проще чем ключ.

Все уже привыкли к такому положению вещей, и мало кто задумывается о безопасности и лояльности персонала, особенно над тем к каким последствиям может привести пренебрежение, или просто халатность сотрудников.

До недавних пор кроме усиленной службы безопасности, систем контроля доступа по пластиковым карточкам и видеонаблюдения, вариантов решения этой проблемы практически не было. Но время идет, появляются новые разработки и технологии. Одна из таких технологий, которая сейчас очень бурно развивается – это биометрическая идентификация личности. В этой области многие уже достигли очень хороших результатов, и некоторые компании начали предлагать коммерческие продукты.

Во многих странах уже начали применять биометрические технологии в масштабах государств, правительственные учреждения и коммерческие структуры. На-пример, в США уже сейчас нельзя въехать без снятия биометрических характеристик, с 2005 года в страны Евросоюза тоже нельзя будет въехать без отпечатков пальца. Украина собирается вводить новые паспорта с отпечатками пальцев, уже вышел ряд постановлений Кабинета Министров и для этого готовится законодательная база.

Совсем недавно в Украине появился новый продукт «БИО СКД» биометрическая система контроля доступа по отпечатку пальца, опредставленный на специализированной выставке в г. Одессе «Управление и автоматизация». Эта система позволяет не только решить проблему внутренней безопасности, контроля и управления доступом, она позволяет вести учет рабочего времени сотрудников, может быть интегрирована в бухгалтерскую систему, что позволяет автоматизировать процесс учета рабочего времени и начисление заработной платы. «БИО СКД» очень интересная разработка, имеющая много уникальных функций и возможностей, и что немаловажно для нашего рынка это ее цена от 2 500 у. е. и выше в зависимости от числа точек прохода и количества пользователей. Во многих случаях стоимость такой системы, особенно для большого числа пользователей, может оказаться даже дешевле карточной системы контроля доступа, например, на 1000 пользователей одни только карточки, не считая оборудования будут стоить около 3 000 у. е. (одна пластиковая карта стоит примерно 3 у. е.), и при работе такой системы, карточки нужно постоянно докупать как расходный материал.

Чтобы читатель имел полное представление о системе, которую мы будем дальше освещать более детально, скажем несколько слов о компании «SARBASH Lab.» (веб-сайт: http://www.sarbash.com/rus/). Это лаборатория компьютерных технологий и программного обеспечения. Компанией выполнены различные проекты для отечественных и зарубежных заказчиков, разработки установлены на разных объектах в США, Европе и странах СНГ, а готовые программные продукты пользуются спросом во всем мире. «SARBASH Lab.» является партнером и работает в тесном сотрудничестве с такими компаниями как Microsoft, BioLink и др. Основным направлением деятельности компании, является разработка программного обеспечения (ПО), для контроля, безопасности и видеонаблюдения. Клиентами компании являются различные заказчики, от частных лиц до корпораций.

Теперь более подробно о новейшей разработке «БИО СКД» (детальная информация доступна на сайте http://skd.com.ua). Компьютерная система управления доступом в помещения предназначена для контроля помещений в виде биометрической идентификации (по отпечатку пальца) и контроля электрозамков или турникетов, с дополнительной возможностью управления любыми исполнительными устройствами и механизмами, а также обработки сигналов, получаемых с различных датчиков.

Принцип работы:

Базовый вариант системы предназначен для открытия двери с помощью биометрического сканера отпечатка пальца. Для того, чтобы дверь открылась, необходимо только приложить большой палец любой руки к сканеру. Вся операция занимает не больше секунды! 100 % надежность! Обмануть систему невозможно, т. к. система запоминает не только сам отпечаток, но и другие характеристики.

При использовании «БИО СКД» не нужно носить с собой ключи, карточки, брелки, которые можно потерять, передать другому лицу, поломать и т. д., главное, чтобы один из двух пальцев не был сильно поврежден. Незначительные и многократные повреждения (порезы) допускаются, и не влияют на идентификацию!

Все данные и настройки параметров хранятся на компьютере, доступ к которому также может быть разрешен только биометрическим путем, т. е. только приложив палец.

Области применения

«БИО СКД» может быть установлена на любом объекте: от дома до больших промышленных предприятий. Система позволяет контролировать доступ, отслеживать движения людей по объектам, сохранять и просматривать все события, отпечатки и многое другое.

Кроме, непосредственно контроля доступа, с помощью этой системы можно автоматизировать процесс учета рабочего времени и начисления заработной платы на предприятиях. Сейчас реализована интеграция с системой «1С: Предприятие» и ведется работа над интеграцией с системой «Акцент».

Масштабируемость

«БИО СКД» может быть установлена в минимальном варианте: 2 сканера и 1–2 замка. При необходимости количество устройств можно увеличить до практически неограниченного числа. Возможно построение глобальной сети управления, территориально

удаленных объектов с единым центром управления, сбора и обработки статистики! Число пользователей от 1 до 10 000 на один сервер. Возможна интеграция видеонаблюдения и др., использование защищенных каналов связи через глобальную сеть Интернет и другие варианты.

Базовые компоненты

★ Сканеры отпечатков пальцев UMATCH.
★ USB-удлинители, кабели.
★ Контроллер управления.
★ Электромеханические замки.
★ Компьютер.
★ Программное обеспечение.

Принцип работы:

Приложив палец к сканеру, данные передаются на компьютер, на котором происходит идентификация и принимается решение о допуске (в зависимости от установленных прав доступа). При положительном результате подается сигнал на контроллер, который подает команду уже непосредственно на исполнительное устройство (электромеханический замок или турникет). При отрицательном результате, отпечаток сохраняется в графическом виде, а команда на контроллер не подается. Вся информация о любых событиях сохраняется в базе данных.

В продукте используются сканеры и технология биометрической идентификации компании BioLink, ведущего поставщика технологий биометрической идентификации в мире, основанные на принципе дактилоскопии. Компания «SARBASH Lab» является партнером BioLink и имеет лицензию на использование этих технологий.

При идентификации используется не только дактилоскопические характеристики, но и тепловой спектр. Это гарантирует высочайшую надежность и точность идентификации.

Специальные USB-удлинители состоят из двух приемо-передатчиков, которые соединяются между собой кабелем CAT5 (витая пара). Возможно использование имеющейся на предприятии инфраструктуры локальной компьютерной сети.

К компьютеру подключается контроллер управления.

Контроллер предназначен для управления замками или другими исполнительными устройствами, а также предусмотрено подключение различных датчиков и получение сигналов с других устройств, благодаря чему в базовом варианте возможно открытие всех дверей при срабатывании одного из подключенных, например пожарных датчиков. Возможны различные варианты интеллектуальной обработки событий получаемых с датчиков и включение определенных устройств.

Сканер отпечатков пальцев

На базе этого контроллера возможно создание систем называемых «Умный дом» (Smart House) или интеллектуальных зданий и комплексов!

Система работает на базе специального про-граммного обеспечения, с помощью которого управляется и контролируется каждое устройство.

После установки и запуска всего оборудования, специалисты проводят предварительное ознакомление и инструктаж ответственных лиц, по добавлению пользователей, конфигурированию прав доступа на объекте, ручному управлению. В случае экстренных событий, а также по работе с программой статистики, если это необходимо.

Сканер отпечатков пальцев. С креплением для монтажа в стене

В большинстве случаев программное обеспечение используется единоразово или периодически, для ввода новых пользователей и установки / изменения прав доступа на определенные двери.

Программное обеспечение может работать автономно и не требует постоянного взаимодействия с оператором или пользователями.

Основной модуль, в котором можно выполнять любые действия и просматривать оперативный статус и отпечатки, обычно используется, когда нужно вести наблюдение или внести изменения в конфигурацию системы.

Основные функции ПО:

★ просмотр оперативного статуса и вывод отпечатков;
★ ввод новых пользователей;
★ удаление пользователей;
★ поиск и изменение прав пользователей;
★ установка / изменение привязки сканеров к замкам;
★ ручное управление замками / устройствами;
★ включение / выключение групп замков / устройств;
★ ручное конфигурирование, включение / выключение сканеров;
★ включение / выключение автоматического запуска и перезапуска;
★ включение / выключение воспроизведения звуковых сигналов.

Каждая операция фиксируется в базе данных. Каждый отпечаток, включая отклоненные попытки проникновения, сохраняется в графическом виде, а информация записывается в базе данных с указанием даты, времени, объекта и двери (сканера). Т. е. в любое время можно просмотреть и найти информацию о любом событии. При установке дополнительного видеомодуля для работы с видеокамерой сохраняется также каждый снимок или или видеоряд с камеры.

По этим данным программа обработки статистики генерирует различные отчеты с возможностью сортировки по дням, месяцам и т. д.

Возможен просмотр оперативных данных и статистических отчетов в режиме ONLINE через Интернет или в локальной сети с помощью любого WEB-броузера.

Если заказчик захочет установить территориально удаленную систему или дополнительные компьютеры, то все данные от всех объектов и компьютеров будут передаваться на сервер и сохраняться в глобальной базе данных.

С этой базой данных работает программа обработки статистики. Все данные выводятся в реальном времени. Используются любые каналы связи, в том числе и Интернет, с возможностью работы по защищенным каналам, что обеспечивает конфиденциальность. При использовании Интернет или нестабильного канала связи, программное обеспечение автоматически определяет, что был сбой связи с сервером, и сохраняет все не переданные события локально. При появлении связи эти данные передаются на сервер, т. е. происходит автоматическая синхронизация.

В заключении хотелось бы сказать несколько слов еще об отличиях «БИО СКД» от других биометрических систем. В мире существует около десятка подобных биометрических систем, основное их отличие в том, что они работают полностью

автономно, т. е. каждый сканер, по сути, имеет свой встроенный НЕ стандартный компьютер и память. Периодически к ним можно подключать обычный компьютер для считывания данных. Как правило, в них существует ограничение по числу пользователей, и объему памяти для хранения информации о событиях. Кроме того, их размеры и стоимость пока очень велики. О глобальности, гибкости и масштабируемости, не говоря уже об автоматизации учета рабочего времени и начисления зарплаты, таких систем говорить очень сложно. Предприятиям очень тяжело подстраиваться под такие системы, а при возникновении каких-либо проблем, решить их будет

достаточно сложно и долго, т. к. необходимо будет обращаться к зарубежным фирмам производителям.

«БИО СКД» базируется на обычных компьютерах, что позволяет значительно сократить стоимость системы, и избавится от вышеперечисленных недостатков. При необходимости, производитель может не только быстро решить любую проблему, но и адаптировать систему под конкретное предприятие. Т. е. не предприятию нужно подстраиваться под систему, а система может быть адаптирована под предприятие, и это немаловажно. Фактически «БИО СКД» это система нового поколения, т. е. более высокого уровня по всем параметрам, и при этом менее дорогостоящая.

Сарбаш В.
Компания «SARBASH Lab.»
http://skd.com.ua
http://www.sarbash.com/rus
e-mail:info@skd.com.ua
тел./факс: (062)334-07-41

«НАУШНИКИ» ДЛЯ СКРЫТОЙ РАДИОСВЯЗИ

Одной из основных проблем в деятельности охранных структур и служб безопасности является незаметное для окружающих использование средств радиосвязи (обеспечение визуальной и акустической скрытности связи). Это достигается применением малогабаритных радиостанций, скрытным размещением радиостанций и микрофона на теле оператора, использованием миниатюрных выносных пультов управления радиостанцией (использование головных телефонов в таких ситуациях исключено).

Решение проблемы – в применении комплексов устройств индуктивной связи, состоящих из передающей антенны и миниатюрных беспроводных приемников-телефонов.

Передающая антенна (катушка индуктивности, индуктор) подключается к выходу усилителя низкой частоты (УНЧ) любой звуковоспроизводящей аппаратуры, в данном случае радиостанции, и создает вокруг себя переменное электромагнитное поле звуковой частоты. В антенной катушке приемника наводится ЭДС звуковой частоты, которая усиливается УНЧ приемника и преобразуется в звуковые колебания с помощью миниатюрного электромагнитного телефона.

Передающая антенна (индуктор) может быть помещена в малогабаритный корпус прямоугольной формы, крепиться к внутренней стороне пиджака либо выполняется в виде многовитковой петлевой антенны и размещается вокруг шеи. Существуют конструкции индуктора в виде погона, которые располагается под рубашкой или пиджаком. Приемник-телефон помещается в ушную раковину оператора так, что звуковоспроизводящий телефон входит в наружный слуховой канал уха. Кроме решения задачи скрытного от окружающих приема информации, такое размещение приемника-телефона улучшает качество воспроизведения речевого сигнала в условиях повышенных акустических шумов, т. к. акустический выход телефона максимально приближен к барабанной перепонке, а корпус изделия является звукоизолятором (звукоизолирующие свойства особенно четко проявляются в диапазоне частот от 1 000 до 4 000 Гц). При этом размещение приемника в ухе почти не сказывается на разборчивости принимаемой речевой информации от окружающих.

Как правило, питание приемников-телефонов осуществляется от миниатюрных элементов питания с напряжением 1,5 В.

Существует большое количество фирм, занимающихся производством аппаратуры данного класса, однако на рынке наиболее известны следующие модели подобных изделий:

★ акустический приемник ПА-1 (Россия),

★ приемник-телефон АМФ-У-С (Россия),

★ комплект аппаратуры, состоящий из приемника WR4 и индуктора CA19 фирмы «SONIC Communications» (США),

★ аналогичный комплект, изготавливаемый фирмой Dynatech Tactical Communication - DTC (Канада): индуктор - Z8, Z8L: приемники - R5, R8,

★ Phonak Inductor фирмы PHONAK Communication AG (Швейцария).

Сравнительные характеристики приемников-телефонов, составленные на основе рекламных материалов и паспортных данных на изделия, представлены в таблице.

Следует отметить, что приемники фирм SONIC и DTC имеют практически одинаковые характеристики и поэтому в таблице они сведены в один столбец. Ориентировочная стоимость изделий составляет от 500 до 4 000 грн.

Как видно из таблицы, лучшими акустическими свойствами (более высоким уровнем звукового давления и более широким диапазоном рабочих частот) обладают телефоны фирм SONIC, DTC и PHONAK. Вместе с тем, разница этих технических характеристик по сравнению с двумя российскими изделиями настолько незначительна, что может быть замечена только при проведении специальных артикуляционных испытаний, и обычным среднестатистическим пользователем практически не ощущается. Как правило, все приемники-телефоны рассчитаны на обеспечение разборчивости воспроизводимой речевой информации, соответствующей по классу ГОСТ 16600-72 в условиях повышенных внешних акустических шумов (в технических характеристиках фирмы указывают не средние, а наилучшие значения).

Обычно пользователя интересуют такие характеристики аппаратуры, как время работы приемника от одного источника питания, степень скрытности размещения, устойчивость звукового сигнала, удобство ношения антенны и самого приемника, надежность изделия, комплектность поставки (возможность поставки фирмой совместно с изделием других аксессуаров для организации скрытой радиосвязи), а также его стоимость. По времени работы источника питания российские образцы превосходят остальные изделия (не менее 100 часов для ПА-1 и не менее 120 часов для АМФ-У-С при 20 часах для Phonak Inductor и 72 часах для приемника SONIC и DTC). В ПА-1 это обеспечивается использованием воздушно-цинкового элемента питания большой емкости, а в изделии АМФ-У-С – экономичным режимом работы (ток потребления в 6 раз меньше, чем в ПА-1, и в 4 раза меньше, чем в Phonak Inductor).

Степень скрытности размещения определяется габаритами и конструкцией приемников-телефонов, а также их цветовым оформлением. Размеры приемников, устанавливаемых в ушную раковину, у различных фирм близки, однако наименьшие габариты из указанных изделий имеет АМФ-У-С. Следует также отметить, что конструкция приемников WR4 фирмы SONIC и АМФ-У-С выполнена с максимальным (по сравнению с другими изделиями) учетом анатомических особенностей наружного слухового прохода уха человека, поэтому при одинаковых размерах эти приемники устанавливаются глубже и более незаметны.

Разница в цветовом оформлении заключается в том, что приемники ПА-1, DTC, Phonak Inductor и SONIC

Параметр	ПА-1	АМФ-У-С	SONIC, DTC	PHONAK INDUCTOR
Рабочий диапазон частот (Гц)	300-3400	300-3400	400-7000	300-3400
Максимальный уровень звукового давления в диапазоне рабочих частот, не менее (дБ)	100	90	109	104
Коэффициент нелинейных искажений в диапазоне рабочих частот, не более (%)	10	10	10	5
Максимальное время работы без смены элемента питания (ч)	100	120	72	20
Емкость элемента питания (мА/ч)	110	18	-	20
Ток потребления (мА)	0,9	0,15	-	0.6

имеют телесный цвет и сочетаются с цветом уха человека, а изделие АМФ-У-С – темнее, его цвет подобран таким образом, чтобы он сочетался с цветом слухового канала уха. Поэтому приемник АМФ-У-С, установленный в ушную раковину, смотрится более естественно.

В целом можно говорить о большей степени скрытности размещения приемника-телефона АМФ-У-С по сравнению с другими изделиями. Важное требование к устройству индуктивной связи – устойчивость звукового сигнала приемника при движении и других активных действиях оператора. Устойчивость характеризуется зависимостью уровня звука от положения головы оператора и определяется, в основном, типом применяемой передающей антенны. Наименьшая зависимость проявляется при использовании петлевой антенны, формирующей равномерно распределенное электромагнитное поле звуковых частот, наибольшая – при индукторе, размещаемом в корпусе прямоугольной формы и имеющем узкую диаграмму направленности. При использовании антенны в виде погона и размещении приемника в ухе с той же стороны, что и погон, достигается устойчивость звукового сигнала, близкая к петлевой антенне.

В изделии ПА-1 передающая антенна (индуктор) размещается в малогабаритном прямоугольном корпусе, который крепится, как правило, к обратной стороне пиджака или пальто оператора связи. При таком конструктивном исполнении антенны и ее размещении громкость акустического сигнала существенно зависит от положения головы оператора. В изделии АМФ-У-С передающая антенна выполнена в виде петли и размещается на шее оператора, что позволяет свести к минимуму изменение громкости воспроизводимого приемником-телефоном сигнала при изменении положения головы.

Изделия фирм (DTC, SONIC и PHONAC) поставляются в комплектации с любым типом антенны. Удобство ношения в основном определяется надежностью закрепления изделия (отсутствием выпадения приемника при изменении положения головы) и комфортностью состояния человека при размещенном в его ушной раковине приемнике-телефоне и антенны на шее или внутренней стороне пиджака. Несимметричные конструкции приемников фирмы SONIC и DTC и изделия АМФ-У-С, наиболее приближенные к форме наружного слухового прохода уха человека, в данном случае обеспечивают максимальные удобства при ношении по сравнению с другими приемниками-телефонами.

В части конструктивного оформления индукторов определенное преимущество имеют фирмы дальнего зарубежья. Конструктивное исполнение передающих антенн обеспечивает большее удобство для оператора, к примеру, индуктор для изделий фирм DTC и SONIC поставляется совместно со специальным чехлом для размещения его на боку оператора (закрепляется на плече под одеждой). К сожалению, отсутствуют точные данные о надежности изделий фирм SONIC, DTC и PHONAK, а также ПА-1 (средняя наработка на отказ изделия АМФ-У-С составляет 40 000 часов), что не позволяет сравнить изделия по этому критерию.

С точки зрения комплексности поставки выгодно отличаются изделия фирм дальнего зарубежья, которые предлагают широкий выбор аксессуаров визуально скрытой радиосвязи (скрытноносимые радиоприемники, выносные пульты управления, микрофоны, аксессуары для ношения и т. д.), работающих в сочетании с приемником-телефоном индуктивной связи. Кроме того, имеется возможность согласования приемника с радиостанциями, имеющими различное выходное сопротивление (8, 15, 30, 60, 300, 600 Ом, 2 кОм), путем выбора соответствующей модификации индуктора.

Приемники изделий Phonak Inductor, ПА-1 и АМФ-У-С, как правило, поставляются в упаковке, содержащей также зеркало и комплект приспособлений для установки и изъятия приемника из ушной раковины. Изделия фирм DTC и SONIC поставляются без комплекта таких приспособлений.

Высокая стоимость американских и канадских изделий объясняется декларируемой высокой надежностью, широким диапазоном рабочих температур и соответствием военным стандартам. Однако приобрести аксессуары скрытой радиосвязи по цене 3–4 тыс. грн (правда, в стоимость включается целиком скрытноносимая гарнитура с микрофоном и пультом управления радиостанцией), в 2–3 раза превышающей среднюю стоимость аналоговых УКВ-радиостанций, может позволить только очень обеспеченный клиент. При этом преимущество в технических и эксплуатационных характеристиках по сравнению с другими изделиями представляется неоднозначным. Несколько меньшую стоимость имеет комплект устройства индуктивной связи фирмы PHONAK.

При этом по ряду важных эксплуатационных характеристик комплект АМФ-У-С превосходит изделие ПА-1 и имеет достаточно высокую надежность. Следует также отметить, что эксплуатационные расходы, связанные с приобретением сменных элементов питания, существенно ниже других у АМФ-У-С. В целом, проведенный анализ показывает наличие богатого выбора аппаратуры в классе устройств индуктивной связи, предназначенных для организации скрытой радиосвязи. На сегодняшний день пользователь может приобрести не только дорогостоящую технику производства дальнего зарубежья, отдав ей предпочтение по причине комплексности поставки, лучшего оформления, соответствия импортным стандартам и наличия различных аксессуаров для ношения, но и более дешевую аппаратуру российского производства, ничем не уступающую по техническим характеристикам, экономя при этом средства на закупку другой техники для организации скрытой радиосвязи.

При подготовке материалов были использованы рекламные материалы предприятий-изготовителей, материалы «Науково-технічного вісника МВС України», «Сучасної спеціальної техніки» и «Специальной техники» (Россия).

Яковенко А. В.

Правовые аспекты легализации цифровых записей

Актуализация принципа состязательности в судебном процессе и повсеместный переход на цифровые технологии записи речевых сообщений требует пересмотра некоторых устоявшихся взглядов на правовые аспекты легализации аудио записей. Практика показывает, что даже при наличии, касалось бы, «неопровержимых» объективных свидетельств: фонограмм с записями преступных переговоров, зачастую невозможно добиться соответствующих юридических последствий.Вне судебного рассмотрения могут оказаться фонограммы, полученные не только нелегитимным путем, но даже фонограммы, полученные из вполне легитимных источников. Проблема усугубляется тем, что практически неограниченные возможности цифровых технологий по компиляции цифровых фонограмм и почти полное отсутствие общепринятых методов подтверждения аутентичности цифровых записей, существенно ослабляют данный источник получения доказательств.

Законодатель четко не прописал все аспекты процедуры легализации записей в суде, поэтому попробуем провести анализ такого процесса с общих позиций.

Общеизвестно, что любая фонограмма, как материальный объект, находящийся в причинной связи с событием преступления является источником информации, но далеко не любую фонограмму можно считать вещественным доказательством.

Напомним, что установление обстоятельств преступления осуществляется в форме процессуального доказывания, основываясь на: показаниях свидетелей, потерпевших, подозреваемого, обвиняемого, заключением эксперта, вещественных доказательствах, протоколами следственных и судебных действий и иными документами (ст. 64 УПК Украины).

Если фонограмма отражает среду события, то потенциальная информация о преступлении должна быть еще кем-то декодирована, систематизирована и оценена для обоснования подлежащих установлению юридических фактов.

Кроме того, проблемы создает тот факт, что хотя звуковой след и материален, но он не отвечает принципу наглядности, поскольку не может быть представлен следователю либо суду для непосредственного восприятия, подобно отпечатку пальца, микроснимка, следа подчистки и т. д.[1].

При привлечении фонограммы в процесс дознания и затем и правосудия всегда будут стоять два основных вопроса: происхождение фонограммы и ее достоверность.

Происхождение фонограммы

По происхождению фонограммы можно подразделить на:

★ Фонограммы, полученные при допросе. Ст. 85-1 УПК Украины. Применение звукозаписи при производстве досудебного следствия.

★ Фонограммы, полученные в ходе судебного заседания. Конституция Украины ст. 129 п.7 и ст. 87-1 УПК Украины. Фиксирование судебного процесса техническими средствами.

★ Фонограммы, полученные в ходе следственных действий. Ст. 114 УПК Украины. Полномочия следователя.

★ Фонограммы, полученные в ходе ОРД по постановлению суда в соответствии с Законами Украины «О милиции», «Об оперативно-розыскной деятельности (ОРД)» и «Об организационно-правовых основах борьбы с организованной преступностью».

★ Остальные фонограммы, полученные представителями учреждений (диспетчерские записи), участниками (потерпевшим, обвиняемым) и случайными гражданами могут быть привлечены к протоколу следственного действия в соответствии со ст. 85 УПК Украины «...К протоколу могут быть приобщены фотоснимки, материалы звукозаписи, киносъемок, видеозаписи, планы, схемы, слепки и другие материалы, поясняющие его содержание».

С точки зрения здравого смысла не имеет доказательного значения факт, кто представляет фонограмму с записью звуковой среды на месте совершения преступления: орган дознания, потерпевший, свидетель или случайный гражданин. Во всех случаях для признания фонограммы в качестве источника доказательственной информации она должна быть подвергнута одной и той же процедуре - осмотру, описанию в протоколе, выяснению личности представляющего фонограмму, установлению содержания последней, технического средства фиксации и обстоятельств, при которых производилась данная запись [1].

По данным социологического опроса [2] более 92 % следователей и оперативных работников правоохранительных органов отметили, что фонограммы, приобщенные к материалам дела, явились одним из основных факторов, способствовавших расследованию и раскрытию преступлений.

Причем законность получения записи во всех случаях является одним из важнейших критериев, по которому запись относится либо к вещественным доказательствам, либо к материалам, поясняющим обстоятельства, подлежащие доказыванию.

Это означает, что запись, полученная незаконным путем, не может иметь прямых юридических последствий (например, не может быть положена в основу обвинительного заключения), но может способствовать установлению истины.

Напомним, что получение информации с нарушением действующего законодательства, есть действия, которые могут сами по себе повлечь уголовное преследование:

★ Ст. 163 УК Украины. Нарушение тайны переписки, телефонных разговоров, телеграфной или другой корреспонденции, которые передаются средствами связи или через компьютер.

★ Ст. 359 УК Украины. Незаконное использование специальных технических средств негласного получения информации.

Достоверность фонограммы

Согласно ГОСТ 13699-91 монтажом называется «преднамеренный подбор и соединение в определенном порядке фрагментов одной или нескольких фонограмм устной речи с целью умышленного изменения первоначального содержания или смысла высказываний одного или нескольких лиц, участвующих в записанном разговоре».

В [3] приводится более универсальное определения «Монтаж фонограммы – это процесс объединения при помощи технических средств отдельных частей фонограммы в единое целое с нарушением непрерывности и последовательности отражения окружающей среды».

В [4] на с. 695 (рис. 24, 25) представлена графическая иллюстрация монтажа во временной и спектральной областях.

К сожалению, данные определения не охватывают такого рода фальсификации как усечение начала и/или конца записи имеющей существенное значение. Причем, усечение может производиться как в реальном масштабе времени, так и вне него (например, при копировании на сменный носитель). То есть, достаточно оборвать запись в нужный момент и зачастую будет иметь место искажение смысла разговора или высказывания. В связи с этим частично теряет смысл изыскание универсальных экспертных методик по поиску следов цифрового монтажа.

В общем случае объектом фальсификации может быть не только перестановка или удаление отдельных фрагментов, но и целостность фонограммы, отражающей объективную последовательность и полноту событий, а также дата и время ее создания.

Таким образом, можно утверждать, что назревает необходимость введения в юридическую практику понятия речевой документ (РД).

Электронный документ

Прототипом этого нового для нас понятия «РД» может служить недавно вступивший в силу электронный документ (ЭД) [5].

ЭД по сути, является некой совокупностью текстовой (иногда графической) информации в виде электронных данных, защита целостности которых обеспечена механизмом электронной подписи (ЭП) автора.

Согласно Закону ЭД может иметь бесконечное множество виртуальных равноценных копий, а если так, то ЭД имея понятие визуальной (т. е. бумажной) формы представления, может также иметь бесконечное множество равноценных бумажных копий. В этом состоит основное отличие ЭД от традиционного бумажного документа, который может иметь только одно физическое воплощение каждого экземпляра. Данные соображения ни в коей мере не имеют целью покушаться на правомерность института ЭД и его документооборота, однако они позволяют увидеть основное отличие между цифровой и аналоговой фонограммой.

Аналоговая фонограмма, подобно бумажному документу может иметь только один экземпляр подлинника и множество копий. Бумажный документ, как и аналоговая фонограмма, на физическом уровне связывает информационную единицу (будь-то буква-символ или соответствующая плотности звуковой волны структура магнитных доменов) с материалом носителя (соответственно бумага или магнитная лента).

Коренное отличие цифровой фонограммы от аналоговой – кроется в ее виртуальности, т. е. оторванности от носителя информации. Последнее обстоятельство имеет самое существенное значение и объясняет методологические трудности судебно-криминалистической экспертизы относительно подлинности цифровых фонограмм.

Итак, основное свойство ЭД это его полное (визуальное и смысловое) соответствие своему бумажному аналогу и наоборот.

Речевой документ

РД, в общем случае, не может быть представлен в виде бумажной распечатки непосредственно, т. к. требуется его смысловая дешифровка.

В частном случае, при формальном ведении разговора, например при допросе, в суде, управлении воздушным движением и т. д. может иметь место полное и однозначное соответствие написанного и сказанного. Однако чаще всего, при свободном разговоре, некоторых диспетчерских переговорах, и пр. такой однозначности

может и не быть, т. к. вступает в силу профессиональный специфический сленг, неофициальная терминология, косноязычие и т. п.

Достаточно вспомнить знаменитое публичное высказывание экс-премьера: «Если за Януковича кто-то нарушил закон, я буду только благодарен...» – смысл которой, скорее всего, следовало понимать с точностью до наоборот.

Это обстоятельство, позволяет, в общем случае, рассматривать фонограмму с датой не как РД, а лишь как фономатериал для экспертизы.

Существует еще один аспект РД отличающий его от ЭД, который связан с технологией создания фонограммы. Если ЭД от начала до конца (до закрепления ЭП) создает автор документа с помощью компьютера, то в случае с РД, «автор» только создает условия для документирования, т. е. подсоединяет, включает, обеспечивает. А сам процесс документирования, то есть фиксация объективной реальности, может осуществляться как бы без участия автора. Автор вообще может физически не присутствовать при процессе фиксации. Т .е. он может нести ответственность только за условия создания РД (достоверную фиксацию даты, времени и других реквизитов), а не за его содержание.

«Превентивная запись»

В связи с этим возникает еще одно соображение, возможно заслуживающее дополнительной юридической и законодательной проработки.

Законом предусмотрено, что в случае необходимости, сотрудник оперативно-розыскных органов, обращается в суд для получения разрешения на прослушивание разговоров.

Балансируя между двумя крайностями: с одной стороны опасностью сползания к государству полицейского типа, а с другой эффективной защиты прав личности законодатель вынужденно создает коллизию.

Абсурдность, ситуации состоит в том, что следователь вынужден, либо действовать в рамках закона и «бить по хвостам» в попытке получения доказательств, которых там уже нет (известны случаи, когда о разрешении на прослушивание субъект прослушивания узнает раньше, чем следователь), либо на свой страх и риск нарушать закон и самостоятельно проводить прослушивание.

Кроме прямого правового нарушения и морально – этического неодобрения, прагматический эффект таких незаконных действий может свестись к нулю т. к. добытые таким путем доказательства невозможно легализовать в суде.

В порядке дискуссии можно предложить компромиссный вариант. Запись телефонных переговоров в потенциально «криминогенных» местах (!) производить, а доступ к накопленным записям разрешать только по постановлению суда. Технически это вполне возможно, причем с высокой степенью гарантии защиты от несанкционированного прослушивания . При этом никакого нарушения тайны телефонных переговоров не происходит. Со временем, старые записи автоматически удалялись бы и уходили бы в лету.

Информация о переговорах, накопленная автоматическим регистратором оставалась бы недоступной для злоупотреблений. А при необходимости, в порядке, предусмотренном законом, субъекты ОРД могли бы получать к ней доступ и отматывать «время назад» для получения легальных вещественных доказательств на стадии подготовки и совершения преступления.

Достоверность фонограммы

Одно из официальных определений цифровой фонограммы приведено в [6]: фонограмма – звуковая информация (данные звукозаписи) судебного заседания, преобразованные в форму электронных данных, и включает обязательные реквизиты. Обязательными реквизитами являются дата, время, место создания записи и номер дела.

Это определение можно взять за основу для определения РД, однако необходимо увязать его с обстоятельствами его создания и применяемой при этом аппаратурой.

Как показано в [7], методы для выявления следов монтажа в фонограмме, изготовленной и представленной на экспертизу в цифровой форме, на сегодняшний день только разрабатываются.

Поэтому, единственным критерием подлинности цифровой фонограммы, может быть правильный выбор аппаратуры и надежное процессуальное исключение возможности подделки цифровой фонограммы.

Примером процессуального решения проблемы достоверности записей вообще и цифровых записей в частности может служить Инструкция о порядке документирования телефонных разговоров и переговоров по радиостанциям оперативных дежурных и их помощников дежурных частей, оперативных штабов органов внутренних дел Украины [8].

Суть которой сводиться к назначению ответственных лиц за документирование переговоров и ограничению доступа к средствам регистрации речевой информации.

Автору известно, что подобные процедуры для цифровых регистраторов речи разработаны и для многих других сфер деятельности: от банков до управления воздушным движением.

Таким образом, достоверность записей может подтверждаться не только путем фоноскопической экспертизы, а и путем проверки точности выполнения соответствующих инструкций. Причем, при использовании соответствующей аппаратуры, исполнители, эксплуатирующие средства документирования переговоров могут выступать в качестве, как свидетелей, так и экспертов.

Кроме того, очевидно, что «процедурная» проверка достоверности имеет значительно менее длительные сроки и может быть более категоричной, чем традиционная фоноскопическая экспертиза. Тогда как в случае криминалистического исследования цифровых записей однозначность заключения эксперта вовсе не гарантирована [7,10,11,12].

Как показано в [2] 86 % опрошенных сотрудников правоохранительных органов указали, на целесообразность назначения судебной фоноскопической экспертизы на этапе предварительного расследования и 99 % из них выразили неудовлетворенность длительными сроками производства фоноскопических экспертиз в государственных экспертных учреждениях и их высокой стоимостью в негосударственных.

Таким образом, с применением организационно-технических мер и «процедурной» проверки достоверности фонограмм, становится возможным избежать длительной и дорогостоящей экспертизы.

Заключение

Для легализации цифровых записей в суде необходимо обеспечить их достоверность и доказать легитимность их происхождения.

К мерам, которые, должны снизить вероятность монтажа специалисты [3] относят:

★ использование устройств, которые не имеют цифрового входа;

★ кодирование записей (в т.ч. и наложение сонограмм [8]);

★ криптографическая защита (ЭП).

Что касается легитимности, то это, скорее всего одна из организационных мер, которая заключается в уведомлении сторон, ведущих переговоры, о происходящей записи.

В некоторых случаях, как-то – шантаж, угрозы, незаконные указания и приказы и т. п., уведомление о записи абсурдно. Следует рассчитывать на то, что суд сможет признать действия по незаконному съему информации с каналов связи, как предпринятые в условиях крайней необходимости и тогда возможно будет применима норма «зло, предотвратившее большее зло». Но этот вопрос находится сугубо в компетенции суда.

Кривенко В.,
канд. тех. наук

Литература:

1. Салтевский М. В., Бегов Д. Д. Место звуковых следов в системе доказательств// Техника специального назначения – № 1, январь 2001.

2. Галяшина Е. Г., Теоретические и прикладные основы судебной фоноскопической экспертизы. Автореферат диссертации на соискание ученой степени доктора юридических наук. – Воронеж, 2002.

3. Богапов Г. Р. Цифровая регистрация речевых сообщений: технологические меры для легализации записей.

4. Вещественные доказательства: Информационные технологии процессуального доказывания/ Под общ. ред. док.юр.наук, проф. В. Я. Колдина.- М.: Издательство НОРМА, 2002.-768 с.

5. Закон Украины № 851-IV «Об электронных документах и электронном документообороте» и Закон Украины «Об электронной цифровой подписи» от 22 мая 2003 года.

6. Інструкція про порядок фіксування судового процесу технічними засобами (звукозапис) в судах загальної юрисдикції (крім господарських та апеляційних господарських судів). – Державна судова адмі-ністрація України, 2003 (Проект).

7. Рыбальский О. В., Жариков Ю. Ф., Струк И. А. Актуальные проблемы современной фоноскопической экспертизы//Техника специального назначения – № 1, январь 2001.

8. Евразийский патент № 002728. «Способ формирования фонограмм речевой информации». Женило М. В., 2002 г.

9. Приказ МВД Украины № 1343, (Додаток 2) от 10.11.2003 г.

10.Тимко Е. В., Усков К. Ю. Проблемы криминалистического исследования цифровых фонограмм – Киевский НИИ судебных экспертиз.

11. Желудков Р. Н., Тимко Е. В., Усков К. Ю. О влиянии сжатия речи на допустимость речевой фонограммы в уголовном судопроизводстве – Киевский НИИ судебных экспертиз

12. Желудков Р. Н., Тимко Е. В., Усков К. Ю. Выявление признаков цифровой обработки в аналоговых фонограммах – Киевский НИИ судебных экспертиз.

Система мониторинга подвижных объектов от «Smart Systems»

Автоматизированные системы мониторинга и управления транспортом и удаленными объектами получили широкое применение в различных сферах деятельности человека, т. к. они позволяют эффективно выполнять функцию удаленного контроля и управления объектами.

Компания «Smart Systems», г. Николаев, работающая на рынке интеллектуальной электроники с 2000 г., представляет систему мониторинга транспортных средств и других мобильных объектов. В её основе лежит модуль, производимый нашей компанией.

Модуль Smart-GPS, от компании Smart Systems, является устройством дистанционного контроля местоположения, скорости и маршрута подвижных объектов: автомобилей, прицепов, мотоциклов, сельскохозяйственных комбайнов, катеров, яхт, железнодорожных подвижных составов. Модуль имеет три логических входа для контроля систем объекта, на котором он установлен (например включение зажигания, открывание двери, капота двигателя или люка) и три выхода для управления (например, отключение бензонасоса, блокировка электрозамков дверей, включение сирены). Вся информация с подвижного объекта (географические координаты, высота, текущее время, получаемые с использованием информации от спутников, изменение сигналов контролируемых параметров) записывается в память прибора и по каналу GSM-связи поступает на диспетчерский пункт. Владелец объекта с диспетчерского пункта через Интернет получает данные на свой компьютер и наблюдает отображение маршрута объекта на загруженной карте и его скорость в каждый момент времени. С диспетчерского пункта, по решению владельца или в случае наступления заранее оговоренной с ним ситуации, могут быть поданы команды на три выхода управления модуля (например, для остановки двигателя, включения сирены, блокировки дверных замков). В случае изменения параметров (сигнал об открывании двери, капота двигателя, запуске двигателя), когда на объекте включена охранная сигнализация, информация немедленно поступает на диспетчерский пункт и сообщается владельцу объекта, оговоренным с ним лицам или в соответствующие службы. Модуль Smart-GPS подключается к бортовой сети подвижного объекта и имеет встроенный резервный источник питания.

Какие же блага сулит приобретение за 699 у. е. нашего устройства? Ответ может быть достаточно прост – наш модуль поможет сохранить ваше спокойствие и уменьшить ежемесячные расходы. Любой собственник искренне желает чувствовать себя спокойным в отношении обладаемого им движимого и недвижимого имущества. Канал Discovery часто рассказывает о том, как при помощи систем определения местоположения, специалисты наблюдают за изучаемыми животными. И применение устройства в подобных областях уже реально! Воспользовавшись нашей услугой, вы всегда будете точно проинформированы о том, где находится ваш автомобиль и в каком состоянии. В случае попытки угона или изменения каких-либо параметров транспортного средства, устройство немедленно сообщит, что позволит принять адекватные меры!

Владельцы парков транспортных средств смогут успешно решать вопросы логистики на своих предприятиях. Применение модуля позволит:

★ контролировать отклонения от рабочего графика,

★ находить ближайшую машину при поломке с минимальным холостым пробегом,

★ оптимизировать оперативные функции диспетчера,

★ исключить нецелевое использование автотранспорта, приписки пройденного пути и расход топлива,

★ принимать управленческие решения на основе достоверных статистических отчетных данных,

★ достигать экономии ГСМ и других ресурсов, связанных с эксплуатацией автотранспорта и максимизировать удельный доход с каждой машины,

★ минимизировать влияние человеческого фактора на систему контроля и управления в целом,

★ повышать качество транспортных услуг, за счёт:

а) ускорения и упорядочивания обработки заявок на перевозки,

б) планирования маршрутов и подготовки расписания выполнения заявок.

Применение устройства может повысить рентабельность вашего предприятия в сжатые сроки.

Однако, предлагая читателю серьёзный подход к нашему изделию, желаем обратить внимание на следующее. Очевидным является тот факт, что при рассмотрении экономического эффекта от внедрения подобных систем, в каждом конкретном случае необходимо рассматривать данный вопрос с учётом специфики парка оборудуемых машин и характера перевозимых грузов.

Итак, Вы заинтересовались!? Связаться с нами для получения подробной информации можно по нижеперечисленным телефонам и адресам. Мы с удовольствием сделаем шаг Вам навстречу!

+38044 201-75-99
+ 38 0512 44 -51- 52;
+38 068 201-75- 99;
+38 067 264 -19- 45;
Info@smartsys.com.ua
www.smartsys.com.ua

НОВОСТИ

Для борьбы с террористами и наркоторговцами в США будут использовать RFID технологию

Правительство США намерено начать тестовую эксплуатацию новой системы по контролю за пересекающими границы штатов. Об этом сообщает представитель Homeland Security Undersecretary, Аза Хатчинсон (Asa Hutchinson). В этом году планируется начать пилотную [тестовую] эксплуатацию метода радиочастотной идентификации на границах с целью пресечения попыток пересечь границы подозрительным лицам, уже занесенным в базы данных служб безопасности.

Границы часто пересекают дальнобойщики, туристы и другие люди, однако их нужно, по возможности, быстро пропускать не утомляя длительными вопросами и досмотром. Задерживать же террористов, наркоторговцев и прочих преступников должна помочь RFID технология.

Текущая система, именуемая «US-VISIT», работает по старинке - фотография и отпечатки пальцев, которые сверяются с данными баз данных федеральных агентств по безопасности. Использовании RFID технологии должно значительно увеличить скорость проверки людей, въезжающих на территорию страны и их груза [предметов]. Несмотря на то, что процесс проверки практически полностью автоматический, автомобилям и людям все же придется останавливаться на границах, и если данные, считанные из RFID чипа, не генерируют на терминале «красного света» , то пересекающий границу сможет продолжить свое путешествие, не будучи утомленным длительным досмотром и вопросами. RFID чип будет вмонтирован в документ, подобный тем что уже используются на мексиканской границе, и выдается тем людям, кто часто пересекает эту границу.

С технологической точки зрения все выглядит достаточно просто. RFID чип через антенну передает информацию в ручной сканер или стационарный терминал, который считывает биометрические данные и сравнивает их с уже имеющимися в базе данных. В отличие от штрих кодов, сканер не нужно вплотную подносить к идентифицируемому объекту под определенным углом, достаточно того, чтобы и сканер и источник находились на отдалении не более 5-9 метров.

У данного метода сразу же нашлись противники. Представитель American Civil Liberties Union, Джей Стенли (Jay Stanley), считает, что данная технология серьезно ущемляет права человека. «Такая система производит автоматическую скрытую проверку в интересах правительства», - заявил он.

Тем не менее, тесты новой системы идентификации должны начаться этой весной в разных частях страны и продлятся один год. Это позволит выявить слабые места у данного подхода, в том числе и выяснить работоспособность в разных климатических условиях.

ixbt.com

К вопросу о практическом применении индикаторов поля и частотомеров

Прекрасную статью написал Дмитрий Мусиенко (Радиоизлучающая подслушивающая аппаратура, Бизнес и безопасность № 6/2004) про наиболее простые средства выявления радиозакладок – индикаторы поля и частотомеры. Индикаторы поля несомненно имеют ряд преимуществ по отношению к другим средствам поиска радиозакладных устройств (РЗУ): простота, дешевизна, возможность поиска широкополосных РЗУ и РЗУ с «прыгающей» частотой. Однако, у приборов этого класса есть ряд недостатков и основной из них, как правильно заметил Д. Мусиенко, невозможность работать в сложной помеховой обстановке города где частотомеры и индикаторы поля для обнаружения РЗУ непригодны.

Продолжая эту тему, хотелось бы предложить выход из создавшегося положения.

Прежде всего, хотелось бы внести одно уточнение, касающееся индикаторов поля и частотомеров, а именно – на мой взгляд, индикаторы поля и частотомеры не должны иметь высокую чувствительность, как считают некоторые авторы. Прибор с высокой чувствительностью будет «ловить» все, даже удаленные маломощные радиостанции. Неслучайно основная регулировка на таких приемных устройствах – настройка порогового уровня, которой чувствительность приемного тракта искусственно «загрубляется».

Следует отметить, что в целом поиск РЗУ необходимо вести комплексно, т. е. выявлять демаскирующие признаки РЗУ, независимо используя разные приборы. Любой специалист в области защиты информации знает, что, осуществляя поиск РЗУ в радиодиапазоне одновременно несколькими устройствами, каждое из них фиксирует свой набор частот, в том числе необнаруженные другими. Так, для поиска РЗУ в радиодиапазоне, я и мои коллеги одновременно используют, как правило, не менее трех приборов.

Индикаторы поля и частотомеры – дополнение к другим, в том числе более функциональным приборам.

Итак, показания любого поискового прибора дают оператору некую информацию об источнике сигнала: индикатор поля – изменение уровня напряженности электромагнитного поля, частотомер – частоту и уровень «захваченного» сигнала, нелинейный локатор – наличие нелинейных элементов (содержащих p/n переходы), металлоискатели – наличие (а иногда и другие характеристики) металла и т. д. Наиболее информативна рентгенотелевизионная установка, которая позволяет (в определенных условиях) визуально идентифицировать источник электромагнитного излучения. Однако останавливаться на ней не будем поскольку в этой статье мы говорим только о простейших поисковых приборах.

Имея сведения о нескольких характеристиках источника (приблизительное или точное местоположение; наличие, распределение и приблизительную мощность излучения, частоту и вид модуляции сигнала, наличие корреляции с акустическими сигналами и т. д.), можно довольно точно выявить РЗУ. Однако, на практике, по тем или иным причинам, удается получать отрывочную, а иногда противоречивую информацию. Так, повышение напряженности электромагнитного поля может быть вызвано наличием пучностей электромагнитного поля одного источника в результате переотражения от металлических конструкций или наложения сигналов от нескольких источников, частотомер может «захватить» сигнал от мощного передатчика и «уверенно удерживать» его на протяжении всего поискового мероприятия, не давая возможности обнаружить РЗУ и т. д.

Получается, что чем большей информацией располагает оператор, тем больше вероятность выявления им РЗУ. Индикаторы поля и частотомеры могут, как правило, индицировать изменение напряженности электромагнитного поля, показать значение «захваченной» частоты, осуществить АМ (ЧМ) демодуляцию.

Дальность обнаружения РЗУ индикаторами поля в значительной степени зависит от мощности источника излучения и уровня помех. В обычных условиях дальность обнаружения РЗУ обычно не превышает 1 м. Расстояния в 5 и более метров таким приборам «не под силу».

Так, например, очень хороший прибор такого класса D-008 в сильных помехах (например, в центре Киева) не позволяет выставить уровень фона даже при полном «загрублении». Если подключить аттенюатор на 10 дБ (который входит в комплект устройства), то он «загрубляется» до такой степени, что способен «увидеть» РЗУ только при непосредственном контакте. При этом на окраине города Киева он свободно обнаруживает РЗУ на расстоянии 0,8–1 м. Про более простые – Protect 1203 или ROGER, я уже не говорю. Так что же делать?

Следующий случай – в сложной помеховой обстановке комплекс мониторинга радиоэфира выявляет «опасный» сигнал. Каким прибором его лучше локализовать?

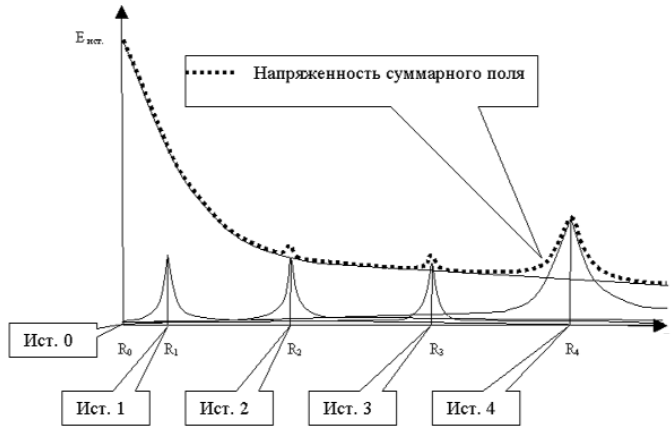
Прежде чем ответить на эти вопросы разберемся подробнее с принципом работы индикаторов поля и частотомеров.

Итак, уровень сигнала в заданной точке пространства зависит, прежде всего, от мощности источника и расстояния до него.

В, так называемом, «ближнем поле» напряженность электромагнитного поля уменьшается обратно пропорционально квадрату расстояния, в «дальнем поле» – обратно пропорционально расстоянию до источника. Поэтому, при внесении индикатора поля в «ближнее поле» РЗУ, уровень сигнала значительно возрастает, что способствует его выявлению. В то же время уровень напряженности электромагнитного поля от удаленного источника сигнала изменяется более плавно и часто «незаметна» для прибора.

Расстояние до границы «ближнего поля» связано с частотой и с некоторым приближением (при о = 3, т. е когда определяющая составляющая напряженности поля в 3 и более раз превосходит другие составляющие) определяется выражением $R_{бл.}$ = л/6р, для «дальнего поля» – $R_{дальн.}$ = 3л/2р. В таблице показаны значения $R_{бл.}$ и $R_{дальн.}$ для некоторых частот. Из таблицы видно, что чем меньше частота источника, тем дальше «простирается» его «ближнее поле» и тем больше дальность обнаружения РЗУ.

Схематично распределение амплитуд поля от нескольких разнесенных источников электромагнитного излучения разной мощности в зависимости от расстояния можно показать на графике. Здесь Ист. 0 – мощный источник электромагнитного поля, Ист. 1–4 – более слабые источники, отстоящие от нулевого на расстояния R_1, R_2, R_3, R_4 соответственно.



Как видно из графика, напряженность электромагнитного поля от более сильного источника (например, мощной вещательной станции) почти на всем промежутке между источниками превышает напряженность электромагнитного поля слабых источников (например, РЗУ). Но индикатор поля реагирует на суммарное поле.

Из теории известно, что, если разница в уровнях между максимальным и другими сигналами будет превышать 10 дБ, уровень напряженности суммарного поля в каждой точке приема будет определяться (с некоторым приближением) только уровнем максимального. Следовательно, если уровень поля от внешнего источника более чем на 10 дБ

Частота, МГц	100	200	300	500	1 000
Длинна волны, м	3,00	1,50	1,00	0,60	0,30
$R_{бл}$	0,16	0,08	0,05	0,03	0,02
$R_{дальн.}$	1,43	0,72	0,48	0,29	0,14

превышает уровень РЗУ, увеличения суммарного уровня не последует.

Это справедливо для широкополосного приема (индикаторы поля). Для узкополосного (частотомеры) – мощный сигнал также будет постоянно «захватываться» приемным устройством и препятствовать возможности «захватить» и точно определить частоту других источников. Поэтому, при поиске РЗУ в сложной помеховой обстановке, необходимо отстроиться от всех мешающих источников электромагнитного излучения.

Для решения данной задачи необходимо во-первых, обеспечить избирательность (что бы прибор реагировал на конкретный источник, а не на суммарное поле от всех источников), во-вторых, понизить порог срабатывания (что бы обеспечить возможность приема сигналов от маломощных источников), в-третьих, блокировать те источники, происхождение которых не вызывает сомнения (для удобства работы и увеличения скорости сканирования).

Для решения этих задач, как нельзя лучше, подходит приемник ближнего поля Xplorer (производство OPTOELECTRONICS).

Итак, приемник ближнего поля Xplorer – это многофункциональный тестовый и исследовательский приемник ближнего поля, представляющий из себя, высокоскоростной сканер, который, благодаря уникальной системе преобразования частоты, способен менее чем за одну секунду автоматически просканировать весь диапазон и выделить активные передатчики в ближней зоне. Он позволяет обнаруживать, демодулировать FM сигналы и воспроизводить звук через встроенный динамик. Xplorer как бы совмещает в себе индикатор поля, частотомер и сканер с памятью на 500 ячеек.

Основные режимы – сканирования, сохранения/пропуска частоты, блокирования частоты, настройки на определенную частоту, просмотр памяти. Он позволяет осуществлять настройку на заданную частоту (как обычный приемник) и обеспечивает демодуляцию ЧМ-сигналов, определить относительный уровень, FM-девиацию, идентифицировать DTMF, DCS, CTCSS, DTMF, LTR сигналов (из опыта скажу, что это вряд ли когда понадобиться), а также определяет параметры LTR транкинга, широту и долготу в координатах системы GPS.

Являясь по существу прибором такого же класса, что и частотомеры и индикаторы поля, Xplorer позволяет задавать диапазон сканирования, добавляя или исключая те или иные диапазоны (частоты). Возвращаясь к началу статьи, можно отметить высокую по сравнению с индикаторами поля и частотомерами информативность этого поискового прибора.

Нет смысла перечислять основные технические характеристики прибора – они подобны ТХ аналогичных устройств (например, частотомера CD-100, производства той же фирмы). Назову лишь некоторые:

★ Частотный диапазон: 30 МГц–2 ГГц.
★ Время сканирования диапазона: < 1 с.
★ Чувствительность: 350 mV на 450 МГц.

Время сканирования диапазона: Методика поиска РЗУ такова. Сначала необходимо озвучить помещение, затем, в течение нескольких минут просканировать эфир, при этом сигналы от мощных радиостанций занести в память и исключить из диапазона сканирования (блокировать). После чего как обычным частотомером (индикатором поля) совершить обход помещения, плавно проводя антенной прибора возле поверхностей стен и предметов, периодически исключая идентифицированные частоты. Признаком наличия РЗУ есть захват приемником его частоты и изменение напряженности электромагнитного поля при перемещении прибора.

Возможное местоположение радиозакладки грубо определяется по максимальному уровню сигнала. Точное обнаружение РЗУ осуществляется путем визуального осмотра.

Особо следует подчеркнуть, что Xplorer перемещается плавно. Объясняется это легко – при широкополосном приеме повышение уровня поля сразу же показывается прибором. А при узкополосном необходимо время для сканирования всего диапазона (в данном случае 1 с). Работать нужно, естественно, в наушниках.

На практике в сложной электромагнитной обстановке Xplorer «захватывает» РЗУ (мощностью около 5 мВт) на расстоянии нескольких метров при этом очень точно определяет частоту источника электромагнитного излучения. Наличие жидкокристаллической шкалы позволяет отслеживать изменение уровня поля при перемещении прибора. Во время тестирования в сложной электромагнитной обстановке (в центре Киева), приемник ближнего поля Xplorer – оказался единственным из трех аналогичных устройств, который позволил выявить и локализовать РЗУ.

Кроме указанных преимуществ, Xplorer имеет малый вес, габариты и может на протяжении 8 часов работать от встроенных аккумуляторов, что обеспечивает определенный комфорт при работе с ним. (Кто считает, что это неважно, пусть попробует подключить к частотомеру приемник и в течение нескольких часов поработать с этим «бутербродом».).

Особенностью работы с Xplorer в сложных электромагнитных условиях есть необходимость предварительной идентификации источников излучения. Хотя понятие «идентифицировать» будет не совсем точным. Ведь, проверяя зафиксированные частоты, нет необходимости определять все их характеристики и точное местоположение. Достаточно разделить их на «опасные» и «неопасные».

Действительно, во время работы с прибором, чаще всего мешают мощные радиовещательные станции, телевизионные сигналы, радиотелефоны, служебные радиостанции, которые легко идентифицировать и исключить.

Гораздо сложнее с цифровыми и кодированными сигналами, выяснить степень опасности которых не всегда просто. Однако и здесь можно определить примерное местонахождение источника (классифицировать на «внутренние» и «внешние»), например, настроившись на частоту излучения, измерить относительный уровень сигнала на некотором расстоянии от обследуемого объекта с разных направлений. Если уровень сигнала на объекте значительно выше чем за его пределами, то сигнал «опасный», если существенно не меняется – «неопасный». Однако идентификация частот это отдельная тема, поэтому останавливаться на этом не будем.

Конечно, приемник ближнего поля Xplorer не является универсальным поисковым прибором, так же как и другим приборам ему свойственны определенные недостатки (например, можно исключить вместе с мощной вещательной станцией частоту РЗУ), однако относительно невысокая стоимость и функциональность делают приемник ближнего поля Xplorer незаменимым при поиске РЗУ в сложной помеховой обстановке.

Изучая рынок аналогичных Xplorer приборов, я обнаружил еще некоторые. Правда пользоваться ими лично мне не приходилось поэтому приведу краткие описания их без комментариев.

R11

R11 – тестовый FM-приемник ближнего поля фирмы OPTOELECTRONICS.

Технические характеристики:

★ диапазон принимаемых частот – 20–3 000 МГц;
★ виды модуляции сигнала – AM, WFM, NFM, девиация < 100 кГц; чувствительность по входу для NFM при отношении сигнал-шум 12 дБ:
на частоте 100 МГц – не менее 15 мкВ;
на частоте 500 МГц – не менее 100 мкВ;
на частоте 1,0 ГГц – не менее 150 мкВ;
★ динамический диапазон измерителя уровня сигнала – не менее 70 дБ;
★ диапазон звуковых частот – 50–3 000 Гц;
★ время сканирования по всему диапазону – 1 сек;
★ дальность обнаружения радиопередатчиков с мощностью в антенне 5 мВт – не менее 5 м;
★ питание – внутренний Ni-Cd аккумулятор; 7,2 В, 600 мА/ч;
★ габаритные размеры – 106 x 68 x 32 мм.

Анализируя диапазон от 30 МГц до 2 ГГц, R11 менее чем за секунду может обнаружить 5-ваттный сигнал от UHF-радиостанции (450 МГц) на расстоянии до 130 м. Принимаемый сигнал демодулируется и может быть прослушан на встроенный громкоговоритель. Участок диапазона будет индицируется соответствующим светодиодом. R11 может быть использован для перехвата любых FM-сигналов, в том числе и от подслушивающих устройств.

R-11 имеет функцию удержания обнаруженной частоты, имеет возможность продолжить поиск пропустив ненужный сигнал. Имеется память блокированных частот, которая позволяет исключить нежелательные частоты из процесса поиска. Ее размер составляет 1 000 каналов. Отдельно управляется громкость и порог чувствительности.

R11 снабжен коммуникационным портом CI-5 для автоматической настройки от частотомера SCOUT. SCOUT захватывает и запоминает частоту, а R-11 настраивается и позволяет прослушивать ее.

СКОРПИОН-3

Приемник ближней зоны производства Лаборатории № 11 ОАО «Электрозавод», является продолжением линейки приемников «Скорпион» и «Скорпион-2».

«Скорпион-3» имеет более высокую чувствительность по сравнению с предшественниками по всему диапазону частот, увеличенный объем памяти, дополнительный внутренний атенюатор.

Технические характеристики:

★ диапазон принимаемых частот – 30–2 000 МГц;

★ чувствительность, мкВ:

в диапазоне 30–1 000 МГц – не более 30;

в диапазоне 1,0–2,0 ГГц – не более 100;

★ полоса пропускания на промежуточной частоте – 200 кГц;

★ время просмотра диапазона частот до 2 000 МГц при отсутствии сигнала – не более 10 с;

★ точность измерения и установки частоты – не более 10 кГц;

★ диапазон измерения уровня входного сигнала – до 70 дБ;

★ количество исключаемых каналов приема – 2 буфера по 9 850 шт.;

★ количество запоминаемых обнаруженных сигналов – 2 буфера по 256 шт.;

★ габаритные размеры прибора – не более 165 х 90 х 29 мм.

★ питание :

через адаптер 12 В от сети переменного тока 220 ± 22 В частотой 50 Гц;

от встроенной аккумуляторной батареи напряжением 9,6 В;

★ время непрерывной работы – не менее 6 час.

В качестве заключения хотелось бы сказать, что тема использования средств поиска закладных устройств данной статьей не исчерпывается. Более того, даже к ранее изложенному материалу об использовании простейших поисковых приборов есть что добавить (например, использование направленных антенн).

Романов И.

НОВОСТИ

Верховная Рада намерена легализировать частный сыск

Верховная Рада Украины в первом чтении приняла проект закона Украины «О частной детективной деятельности». За данный законопроект проголосовали 242 народных депутата.

Законопроектом предлагается легализовать частную детективную деятельность и установить нормативы ее осуществления.

Законопроектом также определены общие принципы государственной политики в сфере частной детективной деятельности. Субъектами частной детективной деятельности признаются частные детективы, детективные агентства, службы безопасности субъектов ведения хозяйства. Определены права, которыми могут пользоваться названные субъекты частной детективной деятельности для достижения своих целей. Законопроектом установлены требования, которым должны соответствовать претенденты - физические лица на получение лицензии на право занятия детективной деятельностью.

Проектом закона также регламентирован порядок получения лицензий и разрешений в сфере частной детективной деятельности, а также условия регистрации служб безопасности субъектов ведения хозяйства и выдачи соответствующих разрешений.

К основным видам услуг, которые субъекты частной детективной деятельности имеют право предоставлять заказчикам, в соответствии с законопроектом, может относится: поиск, сбор, фиксация и накопление сведений, необходимых для защиты прав и частных интересов заказчиков; поиск граждан пропавших без вести, установление их местонахождения, выяснение причин и обстоятельств исчезновения, возможностей и условий их возвращения; розыск исчезнувшего имущества клиента; восстановление для заказчика потерянной информации по вопросам его частных интересов; поиск и сбор данных о фактах, которые могут быть использованы как доказательства в гражданских, уголовных делах, или делах об административных правонарушениях; поиск и сбор биографических и других сведений о лицах - потенциальных или существующих клиентах и партнерах заказчика услуг; защита заказчиков (субъектов ведения хозяйства) от предпринимательского шпионажа.

http://for-ua.com/

PIMA – четвертое поколение технологий безопасности

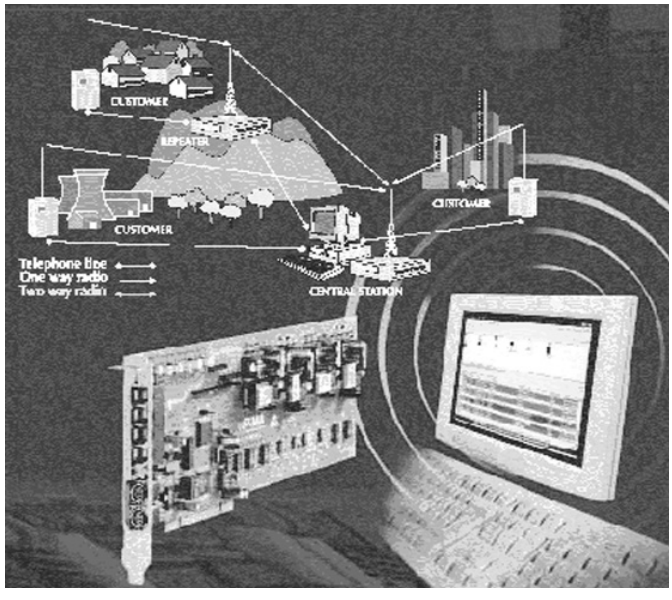
На прошедшей недавно выставке «БЕЗПЕКА-2004» украинский рынок безопасности познакомился с новым именем – одесской компанией «ЖЮСТАР». Представленный ею продукт – комплексная радиоканальная система централизованной охраны «PIMA-Alarms», – получила диплом «Лучший продукт выставки» в номинации «Охранно-пожарная сигнализация». PIMA – абсолютно новый бренд в Украине, поэтому за подробностями редакция обратилась с вопросами к эксперту компании «ЖЮСТАР» Михайлову Андрею Константиновичу.

Андрей Константинович, не секрет, что на рынке Украины уже присутствует большое число производителей и продавцов систем технической охраны, чем особенно интересна украинскому рынку представляемая Вашей компанией продукция?

– Компания «ЖЮСТАР» является эксклюзивным дистрибьютором в Украине израильской компании «PIMA Electronic Systems LTD» – одного из ведущих мировых производителей оборудования охранно-пожарной, тревожной и периметральной сигнализации, средств централизованного наблюдения и других средств охранного назначения. Специалисты знают, что компания PIMA основана в 1984 году и всю свою историю специализируется на производстве технических средств безопасности. PIMA выпускает широчайший спектр оборудования – от детекторов охранно-пожарной сигнализации до пультов централизованного наблюдения, от простых кодовых устройст управления доступом до интегрированных средств безопасности. Продукция компании PIMA соответствуем мировым стандартам качества ISO 9001:2000, IEC 60839, UL, I&F и CE. PIMA уделяет стратегическое внимание контролю качества продукции – каждая новая разработка попадает в серийное производство только после успешного прохождения «полевых испытаний» на реальных объектах, каждое изделие перед отправкой потребителю проходит трёхуровневый контроль работоспособности. В Украине сертифицирована комплексная радиоканальная система передачи извещений «PIMA-Alarms» (сертификат ДЦСЗОП № UA 1.018.0068244), являющаяся квинтэссенцией лучших технологий, разработанных и рекомендованных компанией PIMA.

– А почему выбор пал именно на израильского партнёра? В мире ведь много производителей, в том числе и в Украине...

– Все мы знаем историю и судьбу государства Израиль – с самого своего основания до сегодняшнего дня оно существует в состоянии войны и террора, ведя при этом и вполне нормальную мирную жизнь. Но для того, что бы жители страны могли спокойно жить и плодотворно трудиться государство и работодатели должны обеспечить им безопасность. Поэтому не удивительно, что Израиль давно уже прочно занял место мирового лидера в производстве средств охранного назначения. Достаточно отметить, что в Израиле расположено большинство известнейших мировых брендов охранной индустрии, больше, чем во всём остальном мире в целом. Многие израильские компании давно уже имеют филиалы и представительства за рубежом, их продукт высоко оценен и пользуется заслуженным уважением во всём мире.



Охранное, антитеррористическое и сопутствующее оборудование, производимое в Израиле, насыщенно самыми разнообразными сервисными функциями, высокоинтеллектуально (израильтяне шутят: «Интеллектуальный ресурс – это единственый природный ресурс Израиля» но в этой шутке «есть только доля шутки» – прекрасно известно сколько лучших умов одного только СССР уехало на ПМЖ в Израиль) и высокотехнологично – в виду низкой стоимости земли, сочетающейся с высоким профессионализмом жителей, многие мировые бренды электронной промышленности основали в Израиле свои производства (в окресностях Тель-Авива появилась вторая «силиконовая долина») – на их сверхсовременном высокотехнологичном оборудовании и собирается израильская охранная техника. В ценовой политике продукция Израиля также выгодно выделяется на общем фоне мировых производителей, особенно сейчас, когда Европа, где находятся многие бренды охранной индустрии, переходит в «зону евро», а Израиль по прежнему ориентируется на более дешёвый американский доллар.

– Я вижу, что в мировом масштабе PIMA - имя не новое. На сколько широко применяется её продукция?

– Системы сигнализации компании PIMA широко распространены в 60 странах мира: в Израиле (около 60 % всего охранного рынка страны), Латинской Америке, Японии, Западной Европе, Скандинавии, Прибалтике, Молдавии и в Российской Федерации (в ней на сегодняшний день успешно эксплуатируется более 800 пультов, произведённых компанией PIMA).

– На кого ориентирован ваш продукт?

– В основном – на компании, занимающиеся (или собирающиеся заниматься) централизованной охраной или монтажом охранно-пожарной сигнализации. Особенно нам интересны молодые, быстроразвивающиеся партнёры – им мы готовы предложить целый комплекс услуг: само оборудование и необходимые программные средства, обучение его использованию, технологии его эффективного применения, постоянную техническую поддержку.

– В чём основные преимущества системы «PIMA-Alarms»?

– Если быть кратким, то наша система перед другими радиоканальными пультами имеет следующие конкурентные преимущества:

★ Большой радиус действия

★ Три типа канала связи (радио, телефон и GSM), которые могут быть использованы независимо или параллельно в любых комбинациях. Едентичность информации, передаваемой по всем каналам связи.

★ Две частоты радиоканала существенно повышают надёжность прохождения сигнала.

★ Возможность работы в режима «on-line» и «off-line», причём режим работы выбирается индивидуально для каждого объекта. При работе в «off-line» режиме возможна обратная связь с объектом по телефонной линии.

★ Постоянный контроль каналов связи. Автоматический переход на резервный канал при появлении проблем на основном.

★ Самая высокая скорость передачи информации.

★ Большая информативность сообщений.

★ Гибкость конфигурирования, совмещённая с лёгкостью использования и настройки.

★ Возможность объединения в единую сеть и централизация нескольких пультов.

★ Возможность создания удалённых АРМ операторов.

★ Возможность посылки оповещений о событиях на мобильный телефон, пейджер и электронную почту хозяина объекта и материально-ответственных лиц.

★ Возможность определения статуса охраны и осуществления постановки на охрану с телефонного аппарата.

★ Автоматический контроль работоспособности объектового оборудования и своевременности постановки на охрану..

★ Дистанционное управление объектовой ОПС.

★Дистанционное прослушивание объекта.

★ Интеграция систем охранно-пожарной сигнализации, контроля доступа, видеонаблюдения и наблюдения за мобильными объектами в единый охранный комплекс.

– А нельзя ли раскрыть нашим читателям технический подробности?

– Конечно же можно. В Украине для использования оборудования PIMA выделены полосы частот в диапазоне УКВ: 150–168 МГц и 420–465 МГц (решение Государственного комитета связи и информации Украины № 5-02-988). Этот диапазон имеет следующие преимущества для охраны перед популярным в Украине диапазоном КВ:

1. Малая длина – антенны лёгки в монтаже (фактически, никакого монтажа нет и в помине – она просто устанавливается в BNC-разъём радиопередатчика), компактны, аккуратны, очень дёшевы.

2. Высокая частота улучшает прохождение сигнала сквозь плотные материалы (как, например, стены домов), что ликвидирует необходимость выноса антенны за пределы охраняемого помещения. Следовательно, возможность саботажа путём обрыва или экранирования антенны минимальна.

3. Меньшая длина волны уменьшает вероятность помех от близлежащих объектов.

4. Меньшая дальность распространения УКВ-радиоволн позволяет использовать одну и ту же частоту для работы в соседних населённых пунктах, не мешая друг другу.

5. Меньшая общая зашумлённость диапазона.

В состав системы «PIMA-Alarms» входят:

★ Объектовая ОПС, состоящая из приёмо-контрольного прибора, радиопередатчика, телефонного коммуникатора, опционально GSM-коммуникатора, модулей расширения (расширители зон, программируемых выходов, беспроводное расширение, модуль графического отображения информации, модуль подключения принтера) и детекторов охранно-пожарной сигнализации.

★ Система передачи информации (сеть интеллектуальных ретрансляторов и маршрутизаторов).

★ Пульт Централизованного Наблюдения (один или несколько), состоящий из одного или нескольких базовых декодеров сигнала SENTINEL, устанавливаемых в слот ISA или PCI персонального компьютера (каждый декодер обслуживает до двух радиоканалов и четырёх телефонных линий), стационарной радиостанции с антенно-фидерным трактом на каждый используемый радиоканал, GSM-модема (при использовании канала GSM-связи для сервисной маршрутизации) и программного обеспечения.

Хочу подробнее остановиться на объектовой ОПС. Она представлена двумя видами приёмно-контрольных приборов, различными средствами коммуникации и разнообразными детекторами.

ПКП CAPTAIN-i и HUNTER PRO – это профессиональные охранные системы, обладающие большим спектром функциональных возможностей и удобны в использовании благодаря русскоязычной жидкокристаллической клавиатуре. CAPTAIN-i представляет собой шестизонный ПКП, ориентированный на охрану квартир, котеджей и небольшого размера офисов и магазинов. Позволяет разделять охранную систему на два независимых раздела, сдавать под охрану только периметр, оставаясь внутри охраняемого помещения (режим «ДОМ»). В целях снижения стоимости возможна замена жидкокристаллической клавиатуры на светодиодную или даже считыватель TouchMemory, радио-брелок или ключевой контакт. HUNTER PRO – 32-х зонная охранная система, ориентированная на охрану средних и крупных объектов. Разделяется на 16 разделов, имеет два независимых режима «ДОМ», позволяет управлять различным внешним оборудованием (по событиям, по времени или вручную локально и удалённо – с телефонного аппарата и с ПЦН) в частности – системами видеонаблюдения и контроля доступа, эффективные средства борьбы с ложными срабатываниями (пересекающиеся зоны, интеллектуальные зоны и счётчик импульсов), позволяет подключать для отображения информации графические устройства, принтер и компьютер.

Радиоканал объектовой системы представлен несколькими типами взаимозаменимых радиопередатчиков: TRV-100 – однонаправленный двухчастотный радиопередатчик диапазона VHF, TRU-100 – однонаправленный двухчастотный радиопередатчик диапазона UHF и GSM-100 – гибридное устройство, включающее в себя двухсторонний приёмо-передатчик и GSM-коммуникатор (в зависимости от выбранного режима эти два передающих устройства могут быть задействованы либо по отдельности, либо вместе – в режиме подстраховки).

Есть интересные решения и среди детекторов охранно-пожарной сигнализа-

ции. В первую очередь хочется отметить комбинированный датчик LIGARD COMBY – уникальное устройство, совмещающее в себе три разных детектора – пассивный инфракрасный детектор движения с объёмной диаграммой направленности, акустический детектор разрушения стекла и вибрационный детектор разрушения строительных конструкций. Каждый детектор имеет независимую индикацию, регулировку и тревожное реле. Уникальной особенностью семейства LIGARD является температурный интервал работы – от -20 °С до +50 °С. Другой уникальный детектор – вибрационный датчик VIBRA SENS, предназначенный для блокировки труб и решёток с возможностью уличной установки. Так же хочется отметить детекторы движения 3D и DOUBLE TEC, в которых работают по два обнаружителя (2 пироэлемента с независимыми оптическими системами в первом случае и пироэлемент с активным микроволновым обнаружителем во втором), благодаря чему датчики максимально защищены от влияния факторов внешней среды, тепловых потоков и движения объектов неживой природы, детектор разрушения стекла MAX GLASS – благодаря двухчастотному сенсору и функции «антимаскинг» он минимально подвержен ложным срабатываниям, уличный объёмный датчик движения двойной технологии GUARD, периметральный инфракрасный четырёхлучевой барьер PROTECTOR и тревожную двухканальную радиокнопку ACS-102 с дальностью действия 250 м. Разумеется, в арсенале продукции компании PIMA представлены и другие датчики: магнитоконтактные, пассивные инфракрасные со всеми возможными диаграммами направленности, как аналоговые, так и цифровые, периметральные, стационарные тревожные кнопки, беспроводные устройства и др.

– А совместима ли ваша система с оборудованием других производителей?

– Вполне, и даже на нескольких уровнях. Совместно с нашими приёмо-контрольными приборами на равне с нашими детекторами могут быть использованы и детекторы других производителей, а наши – с чужими приёмно-контрольными приборами. Наши ПКП кроме фирменного протокола PAF могут общаться с ПЦН по телефонному и GSM-каналам связи по стандартизованным и широкопопулярным у разных производителей протоколам Ademco, Radionics, Silent Knight, Franklin, Surgard, DTMF 4x3, Contact ID и SIA FSK, по радиоканалу поддерживаются протоколы LARS, Scantronic, Electronics Line, Visonic. Соответственно, наши ПКП могут работать в любых охранных сетях, поддерживающих хотя бы один из этих протоколов. Все эти протоколы умеет «читать» и SENTINEL – следовательно, совместно с нашим ПЦН может работать чужое объектовое оборудование, поддерживающее один из вышеназванных протоколов связи. Недавно мы успешно реализовали связь декодера SENTINEL с популярной в Украине охранной системой СТРАЖ, сейчас заканчиваются работы по вводу ПЦН SENTINEL в комплексную систему ИНТЕГРАЛ. Компания PIMA открыта для сотрудничества и готова добавить в своё оборудование поддержку и других протоколов связи. Кроме того, для включения в охранную сеть «PIMA-Alarms» ПКП, не поддерживающих вышеназванные протоколы, мы предлагаем устройства SAT-8 – это интерфейс для связи релейных выходов ПКП с радиопередатчиками TRV-100 и TRU-100 и SAT-9 – интерфейс для подключения радиопередатчиков TRV-100 и TRU-100 к телефонному дозвонщику контрольных панелей.

– Спасибо, Андрей Константинович, теперь нам понятна техническая сторона вашего продукта, но учасников рынка, безусловно, интересует и вопрос цены...

– К сожалению, мы обратили внимание на то, что в Украине существует стереотипное мнение о, якобы, очень высокой стоимости радиоканального УКВ-оборудования. Вероятно, это связанно с не очень удачными попытками украинских производителей сделать свой подобный передатчик. Смею заверить Вас – это не так. Благодаря высокой технологичности применяемого в производстве оборудования, применению самых современных конструкторских идей и большому обороту компании PIMA удалось сделать радиопередатчики достаточно дешёвыми, а необязательность использования на объектах дорогостоящих антенн и фидеров делает наше оборудовании ещё более привлекательным в ценовом плане. Кроме того, компания ЖЮСТАР разработала гибкую ценовую и кредитную политику, которая, безусловно, понравится нашим клиентам.

PIMA
FOR BETTER PROTECTION

– Спасибо за плодотворную беседу. Надеюсь, она заинтересует наших читателей. А вашей компании желаю больших успехов в бизнесе.

В настоящий период фирма «Жюстар» формирует дилерскую сеть на территории Украины. Для заинтересованных фирм и физических лиц сообщаем реквизиты фирмы «Жюстар»:

65005, г. Одесса,
ул. Бугаевская, 21, оф. 601,
тел.: 8(0482)33-33-70,
факс: 8(0482)33-33-80,
e-mail: pima@eurocom.od.ua

НОВОСТИ

Возможность анонимной деятельности в глобальных сетях порождает ощущение безнаказанности

Большинство проблем технологической незащищенности глобальных сетей связано с тем, что Интернет строился как открытая среда коммуникации незначительного по сегодняшним меркам числа исследовательских и военных компьютерных центров. К настоящему времени достигнута такая стадия развития Интернета, когда заложенные при его создании принципы функционирования частично противоречат решаемым задачам.

Характерной особенностью современного этапа развития Интернета является практически полное отсутствие достоверных идентификаторов личности при работе в сети. Это позволяет лицам с определенными негативными наклонностями практически анонимно совершать свои действия, в том числе и противоправные.

Отсутствие официального общего списка пользователей сетей и их адресов, упрощенные процедуры регистрации пользователей провайдерами, постоянное совершенствование механизмов анонимного участия в сетевых процессах существенно усложняют выявление подобных лиц. Установление принадлежности конкретного сетевого адреса определенному субъекту возможно далеко не во всех случаях. Не требующая соблюдения особых юридических формальностей процедура регистрации новых пользователей сети и простота работы обеспечивают свободный доступ в глобальные компьютерные сети всем желающим, не исключая и потенциальных преступников. Такие лица могут использовать дополнительные возможности подключения к сети, еще более обезличивающие их участие в сетевых процессах (например, получать доступ к сетевым ресурсам в интернет-кафе или с применением интернет-карт).

Простота обеспечения анонимной активности в сети приводит к психологическому ощущению безнаказанности и, как следствие, созданию криминальных групп в сети, объединению вокруг них лиц, склонных к противоправной деятельности, возможности ведения пропаганды в целях привлечения новых участников.

Для изменения ситуации предлагаются различные способы, например, ввести в Интернете стандарт, требующий жесткой идентификации пользователя в момент вхождения в сеть. Однако все подобные предложения требуют для своей реализации колоссальных капиталовложений.

Существенное ослабление контроля над криптографией в большинстве государств стало причиной широкого распространения среди обычных пользователей сети Интернет программного обеспечения, реализующего шифрование данных с использованием стойких криптоалгоритмов. Обеспечивая право людей на сохранение конфиденциальности сеансов связи, данное обстоятельство создает большие проблемы для правоохранительных органов при идентификации участников противоправных действий и сборе доказательств в процессе расследования по соответствующим уголовным делам.

http://www.crime-research

ВАРИАНТЫ ОРГАНИЗАЦИИ ОПЕРАТИВНОЙ РАДИОСВЯЗИ СЛУЖБ БЕЗОПАСНОСТИ И ОХРАНЫ

Практически все службы безопасности и охраны в своей деятельности используют радиосвязь для организации взаимодействия и управления сотрудниками. Радиостанция в настоящее время является неотъемлемым атрибутом сотрудника охраны, как холодное и огнестрельное оружие или индивидуальные средства защиты. Вместе с тем, в отличие от них, радиостанция может обеспечить выполнение своих функций (обмен информацией) только при взаимодействии с другими подобными радиостанциями, то есть при работе в сети. Таким образом, наряду с параметрами и функциональными возможностями радиостанций важна правильная организация их взаимодействия, т. е. объединение в сети и системы связи.

Рассмотрим особенности построения сетей связи для служб безопасности. Такие сети предназначены для обслуживания абонентов, объединенных в группы до 20 человек. В составе группы могут быть мобильные (на автомашинах, пешие) и стационарные абоненты. Как правило, каждый абонент внутри группы должен слышать всех ее членов. В отдельных случаях необходима связь с абонентами телефонных сетей. Быстрое изменение оперативной обстановки требует минимального времени установления соединения при максимальной простоте управления радиостанцией. К аппаратуре таких сетей связи предъявляются дополнительные требования по защите передаваемой информации от прослушивания и по массо-габаритным характеристикам.

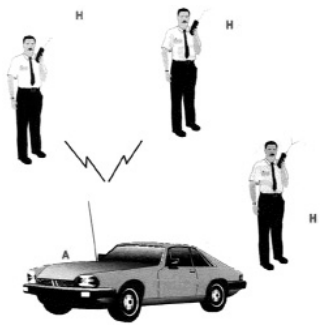


Рис. 1

В последнее время многие операторы радиосвязи предоставляют услуги на основе транкинговых систем типа SmarTrunk II, MPT 1327 и др. Во многих случаях, объем и качество услуг соответствуют требованиям служб безопасности и аренда ресурсов данных систем является единственно возможным решением, особенно где плотность абонентов достаточно высока, а радиочастотный ресурс практически исчерпан. В первую очередь, это касается крупных городов. Вместе с тем, во многих случаях предпочтительней иметь свою независимую (корпоративную) сеть радиосвязи. Например, при отсутствии оператора транкинговой связи (что наиболее вероятно в небольших городах), или недостаточности объема предоставляемых услуг, например, при отсутствии возможности обмена конфиденциальной информацией.

В техническом плане корпоративные оперативные системы связи строятся, в основном, на базе радиальной структуры с использованием фиксированного распределения каналов связи. В зависимости от решаемых задач, варианты организации радиосвязи в сети могут быть различны. Рассмотрим типовые варианты.

★ **Вариант 1.** Подвижная группа абонентов работает автономно, передвигаясь по территории. Связь осуществляется в локальной области сосредоточения абонентов радиусом 0,5–1 км. Чаще всего, такой вариант организации связи используется при охране VIP.

Структурная схема связи показана на рис. 1, где А – автомобильная радиостанция; Н – носимая радиостанция. В зависимости от выполняемой задачи в качестве носимых радиостанций могут использоваться открыто носимые или радиостанции скрытого ношения.

Для организации связи достаточно одного радиочастотного канала, т. е. все абоненты группы работают на одном канале и слышат друг друга. Радиосредства работают в симплексном режиме. В общем случае количество абонентов в группе определяется организационно-тактическими требованиями.

Поскольку средняя интенсивность работы абонента в сети невелика (обычно не более 1–2 связей в минуту при средней длительности сообщения 5–7 сек), то возможна независимая работа нескольких групп на общем частотном канале с раздельной доставкой сообщений. В этом случае, суммарное количество абонентов на одном радиочастотном канале не должно превышать 20–50 человек. Разделение групп осуществляется с помощью, так называемого, селективного вызова (CTCSS кодер-декодер). Для уменьшения помех в радиостанциях целесообразно запрограммировать запрет на передачу на занятом канале.

Можно отметить, что в данной задаче использование однозоновой транкинговой сети связи может оказаться хуже предложенного варианта, так как движение объекта охраны и группы территориально не ограничено. То есть, они могут покидать зону обслуживания транкинговой сети, что приведет к неустойчивости или потери связи. В предлагаемом варианте территория работы подвижной группы практически не ограничена, а благодаря компактности группы надежность связи достаточно высока.

В рамках рассматриваемой структуры сети связи возможно взаимодействие нескольких групп. Этот вариант показан на рис. 2.

Группа 1 (Гр. 1) работает на канале К 1, группа 2 (Гр. 2) – на канале К 2. При передаче сообщения из Гр. 1 в Гр. 2 абонент Гр. 1 переключает радиостанцию на канал К 2. И, наоборот, при инициативе передачи сообщения от Гр. 2 обмен информацией осуществляется на канале К 1. В качестве канала связи может использоваться виртуальный канал.

★ **Вариант 2.** Несколько независимых подвижных групп абонентов на ограниченной территории радиусом 1–2 км под управлением общего диспетчера выполняют каждая свое задание. Данный вариант хорошо описывает сеть радиосвязи для охраны большого промышленного объекта, когда независимыми группами являются подразделения пожарной безопасности, охраны, контроля сигнализации и др.

Структурная схема сети радиосвязи показана на рис. 3, где Н, Ст. – носимая и стационарная радиостанции. Группа 1 (Гр. 1) работает на канале К 1, группа 2 (Гр. 2) – на канале К 2. При большем количестве групп количество каналов должно пропорционально увеличиваться.

Работу стационарной радиостанции можно организовать двумя способами.

Первый заключается в том, что для связи с диспетчером выделяется отдельный канал связи – К 3, на который переключаются носимые радиостанции при связи с ним. Диспетчер связывается с соответствующей группой абонентов на канале этой группы. При такой организации диспетчер не слышит переговоры внутри групп, но может подключиться к переговорам в любой момент, переключив радиостанцию на соответствующий канал связи.

Второй способ организации связи с диспетчером предполагает использование стационарной радиостанции в режиме сканирования по каналам К 1 и К 2. В этом случае диспетчер постоянно контролирует переговоры внутри групп.

Очевидно, как и в предыдущем примере при соответствующем программировании носимых радиостанций возможно взаимодействие групп между собой. При передаче сообщения из Гр. 1 в Гр. 2 абонент Гр. 1 переключает радиостанцию на канал К 2, и, наоборот, при инициативе передачи сообщения от Гр. 2, обмен информацией осуществляется на канале К 1. Для разделения по каналам достаточно использовать сигналы CTCSS кодера, а для уменьшения помех запрет на передачу на занятом канале. Радиостанции в сети работают в симплексном режиме, поэтому для развертывания сети достаточно иметь один радиоканал.

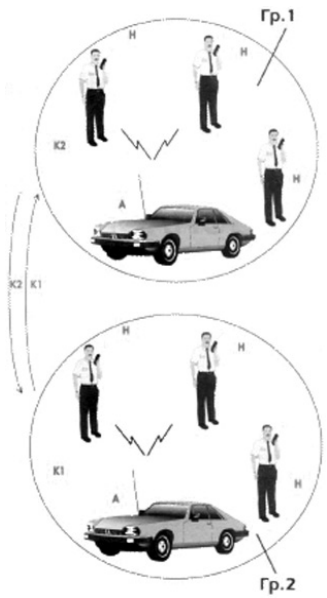


Рис. 2

Особенностью данной схемы организации связи является возможность увеличения дальности связи. Для этого стационарную радиостанцию используют как ретранслятор, ее антенну размещают на господствующей высоте, а в радиосредствах подвижных абонентов включают режим двухчастотного симплекса. В этом случае все сеансы связи между подвижными

абонентами осуществляются путем ретрансляции сигналов через стационарную радиостанцию. Вместе с тем данный режим имеет

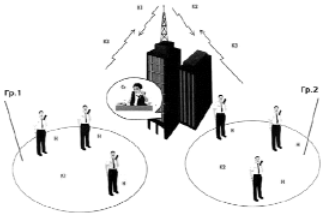


Рис. 3

и недостаток – на границе зоны обслуживания стационарной станции возможно отсутствие связи, даже если подвижные абоненты находятся в непосредственной близости друг от друга. Поэтому, как правило, предусматривают резервный канал, в котором радиостанции работают в симплексном режиме, как было рассмотрено в первом варианте. Кроме того, для реализации режима ретрансляции требуется выделение дуплексной пары радиочастот.

★ **Вариант 3.** Несколько подвижных групп работают на территории небольшого города радиусом 5–10 км, возможны выездные мероприятия в пригородных районах. Необходима связь со стационарным абонентом и выход на телефонные линии. Данный вариант может описывать работу частного сыскного или охранного бюро.

На рис. 4 показана структурная схема одного из вариантов построения такой сети связи. Ее новыми элементами являются: ретранслятор (РТ) и телефонный контроллер (ТК), соединенный с базовой станцией (БС). К телефонному контроллеру подключена абонентская линия телефонной сети (ТЛ).

Работа групп в городе не отличается от случая, рассмотренного во втором варианте. Абоненты группы работают на канале группы К 1. Связь с диспетчером осуществляется на канале К 3. По-прежнему, абонентские радиостанции работают на одном радиочастотном канале в симплексном режиме.

При выездных мероприятиях связь поддерживается через ретранслятор (РТ), размещаемый в направлении проведения выездных мероприятий, например, вблизи загородных дачных поселков. Это позволяет обеспечить связь между БС и автомобилем на расстояниях до 100 км. Ретранслятор работает в дуплексном режиме, поэтому для его работы должна быть выделена дуплексная пара радиочастот. Примем, что частота приема ретранслятора соответствует значению fp, а частота передачи совпадает с частотой работы сети связи в городе. Разделение каналов К 1 и К 3 осуществляется с помощью сигна-

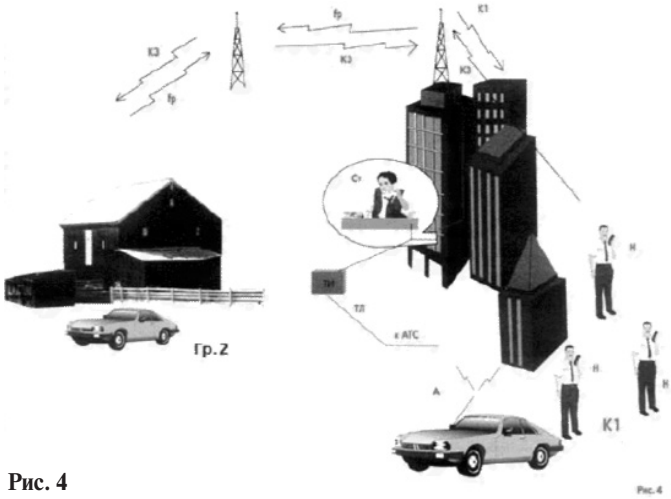


Рис. 4

лов CTCSS-кодера. Таким образом, для работы небольшой сети связи достаточно одной дуплексной пары радиочастот.

Связь выездной группы с диспетчером происходит следующим образом. В зоне работы ретранслятора выездная группа (Гр. 2) переводит радиостанцию на канал работы ретранслятора, при этом радио-станция должна функционировать в режиме двухчастотного симплекса с частотой передачи fp, и частотой приема на канале К 3. Диспетчер с помощью стационарной радиостанции, работающей на канале К 3, принимает сообщения от абонентов в городе, либо от ретранслятора. При ответе диспетчер переключает радиостанцию на канал связи с соответствующей группой. Очевидно, что на канале работы через ретранслятор стационарная радиостанция должна работать в режиме двухчастотного симплекса.

Использование в данном варианте дуплексной пары радиочастот позволяет связываться подвижным абонентам с абонентами телефонной сети.

В этом случае к стационарной радиостанции подключают телефонный интерфейс, например, CS-900 фирмы CSI, а абонентские – снабжают клавиатурой для набора номера и платой DTMF. На абонентских радиостанциях выделяют отдельный канал выхода в телефонную сеть. На данном канале радиостанция должна работать в режиме двухчастотного симплекса с частотой передачи, соответствующей каналу К 3, и частотой приема fp. Сигналы CTCSS-кодера для этого канала необходимо выбрать отдельно. Таким образом, для связи с абонентами телефонной сети используется общая с ретранслятором дуплексная пара радиочастот. Взаимодействие абонентов телефонной и радиосети происходит обычным образом.

Количество обслуживаемых абонентов данной сетью связи определяется как в первом варианте.

Приведенными вариантами не исчерпывается многообразие построения небольших корпоративных сетей радиосвязи. Очевидно, что отдельные элементы рассмотренных вариантов могут быть скомбинированы друг с другом для реализации новых возможностей.

Для построения описанных сетей связи имеется широкий ассортимент УКВ- радиостанций импортного и отечественного производства, с необходимым набором функциональных возможностей. Однако корпоративные сети связи целесообразно строить на базе комплектов профессиональных радиостанций. Отличительными особенностями профессиональных радиостанций

Таблица

Параметр	Вариант		
	1	2	3
Назначение сети	Охрана VIP	Охрана объекта	Охранное бюро
Минимальное количество радиочастот	1	1 (при необходимости +1 с дуплексным разносом)	1+1 с дуплексным разносом
Количество независимых направлений связи	> 1	> 1	> 2+1 при выходе в ТФСОП
Состав оборудования	1. Носимые радиостанции. 2. Автомобильные радиостанции.	1. Носимые радиостанции. 2. Автомобильные радиостанции. 3. Стационарные радиостанции*.	1. Носимые радиостанции. 2. Автомобильные радиостанции. 3. Стационарные радиостанции. 4. Ретрансляторы. 5. Телефонный интерфейс (при необходимости).
Обязательные функциональные возможности абонентских радиостанций	1. Симплексный режим. 2. Селективный вызов.	1. Симплексный режим (при необходимости - двухчастотный симплекс для радиостанций и дуплексный режим для стационарной радиостанции). 2. Селективный вызов. 3. Запрет на передачу на занятом канале. 4. Сканирование по каналам (при необходимости).	1. Симплексный режим, двухчастотный симплекс для радиостанций. 2. Дуплексный режим для ретранслятора. 3. Селективный вызов. 4. Запрет на передачу на занятом канале. 5. Сканирование по каналам (при необходимости).
Удельная стоимость оборудования на абонента	$ 800...1000	$ 1000...1200	$ 1000...1500

*Здесь под стационарными радиостанциями понимаются автомобильные радиостанции, укомплектованные для эксплуатации в стационарных условиях.

являются простота и удобство управления, надежность при эксплуатации в неблагоприятных условиях, защита от неквалифицированного перепрограммирования.В таблице приведены обобщенные оценочные технико-экономические параметры рассмотренных сетей связи. Данную таблицу не следует рассматривать как сравнительную, так как каждый из вариантов имеет свою нишу применения. Вместе с тем, она позволяет оценить требуемые ресурсы для развертывания системы

При выборе и заказе аппаратуры для развертывания сетей связи необходимо помнить о приобретении вспомогательного оборудования и аксессуаров, без которых немыслима надежная эксплуатация сети связи. К таким атрибутам относятся аккумуляторы, зарядные устройства, антенно-фидерные устройства, контрольно-тестовая аппаратура, техническая документация и т. д.

При подготовке материалов были использованы рекламные материалы предприятий-изготовителей, материалы «Науково-технічного вісника МВС України» «Сучасної спеціальної техніки» и «Специальнаой техники» (Россия).

Яковенко А. В.

НОВОСТИ

Как убедить руководство компании вкладывать средства в обеспечение информационной безопасности?

Типовой вопрос, с которым сталкиваются ИТ-менеджеры компаний, как обосновать руководству необходимость вложений в информационную безопасность. По статистике самым большим препятствием на пути принятия каких-либо мер по обеспечению информационной безопасности в компании являются две причины: ограничение бюджета и отсутствие поддержки со стороны руководства.

Если ИТ-менеджер четко представляет, сколько компания может потерять денег в случае реализации угроз, то решение задачи убедить руководство обратить внимание и выделить средства на обеспечение информационной безопасности становится значительно более реальным. В принципе, существуют два достаточно недорогих и наглядных способа решения задачи, как убедить руководство:

1. Провести комплексную оценку стоимости обрабатываемой информации (ущерба) и оценить существующие в системе риски (вероятный ущерб). Для этого лучше всего воспользоваться одной из автоматизированных систем анализа и контроля информационных рисков. Подобными системами являются западные CRAMM (www.cramm.com), RiskWatch (www.riskwatch.com) и российская разработка компании Digital Security - ГРИФ, с описанием и демо-версией которой можно ознакомиться по адресу: (http://www.security-lab.ru/tools/_services/download/redirect.asp?href=http://www.dsec.ru/soft/grif.php). Применение системы ГРИФ позволяет экономически обосновать необходимость вложений в информационную безопасность (ИБ), сравнив существующие в системе риски (вероятный ущерб) с ежегодными расходами на информационную безопасность.

2. Провести тесты на проникновение, успех которых наглядно продемонстрирует руководству необходимость повышенного внимания к вопросам обеспечения информационной безопасности. Тем более, что в случае применения современных технологий взлома вероятнее всего не устоит даже самая защищенная система, и успех проведения тестов на проникновение практически предрешен.

Данные способы (а эффективнее всего - их комбинация) позволят ИТ-менеджеру привлечь внимание руководства компании к животрепещущей теме информационной безопасности, обеспечив тем самым необходимый уровень инвестиций в обеспечение безопасности системы и повысив собственный вес и авторитет в глазах высшего руководства компании.

Обратим внимание, что других методов обосновать необходимость вложений в ИБ, кроме как, оценив существующие в системе риски и предоставив руководству данную финансовую информацию (риск - это ущерб, который понесет компания в случае атаки), не существует. А успешный тест на проникновение станет хорошей демонстрацией реальности атаки. Цепочка замкнулась! Уровни рисков оценены - возможность взлома доказана. Теперь нужно оценить необходимый уровень вложений в ИБ и сравнить при помощи той же системы анализа рисков насколько при этом уменьшатся риски. Решаемая задача сводится к следующему: минимизируя затраты на информационную безопасность, довести уровень риска до приемлемых значений (суммарные затраты на безопасность должны быть существенно меньше суммарного риска).

http://www.dsec.ru

НОВОСТИ

Дорогой безопасности

В июне компания MONT, совместно с Computer Associates, Symantec, IBM, «Лабораторией Касперского», Microsoft и Check Point, провела в семи городах России и Украины цикл семинаров Road Show MONT Security Day, посвященных программным решениям в области информационной безопасности. Компания TopS Systems Integrator, подразделением которой она являлась, в 2001 г. разделилась на самостоятельные структуры TopS и TopS Business Integrator, а год спустя TopS, один из крупнейших российских дистрибьюторов ПО, была переименована в MONT.

На семинарах рассматривались вопросы управления ИБ с помощью современных технологий, лицензионная политика ведущих поставщиков решений, программы обучения реселлеров, комплексные подходы к обеспечению безопасности, партнерские программы. Докладчики из IBM, Computer Associates, Symatec представили свое видение проблемы ИБ и линейки продуктов, например ПО IBM Tivoli, на базе которых можно построить современную, гибкую, мобильную, автономную, мощную и безопасную инфраструктуру.

В построении систем ИБ большую роль играет управление, и в последнее время CA активно инвестирует средства в разработку новых продуктов и технологий в области безопасности и в продвижение решений по управлению информационными системами. Ее технология Common Services объединяет различные решения в единую платформу и позволяет более гибко управлять ресурсами.

В Check Point безопасность рассматривают как один из основных факторов построения сетевой инфраструктуры, а ее решения охватывают три направления: безопасность периметра (VPN-1/Firewall-1), защиту приложений Web (линейка продуктов Connectra) и внутреннюю безопасность сетей (ПО InterSpect).

Докладчики Microsoft, как и на других подобных форумах, рассказали о концепции Trustworthy Computing, элементы которой реализованы в таких продуктах, как Windows Server 2003, Exchange Server 2003 и Office 2003. Новая партнерская программа MSPP призвана помочь клиентам в выборе партнеров.

Участники семинаров отметили быстрый рост отечественного рынка ИБ, а MONT планирует продолжить цикл региональных семинаров по этой актуальной теме.

http://www.osp.ru

Новые возможности для банков

Темпы современной жизни вынуждают людей ценить и беречь свое время. Множество функциональных нововведений помогают им в этом. Среди них привлекают внимание модульные безбалансовые банковские отделения. Про эту новинку на отечественном рынке журналу «Бизнес и безопасность» рассказал директор НИЦ испытаний изделий и материалов защиты Андрей Вячеславович САБЛИН.

- Каково преимущество модульных безбалансовых отделений по сравнению с обыкновенными банковскими филиалами?

- В отличии от стандартных банковских отделений, которые занимают здание либо его часть, так называемые «модули» – это малые архитектурные формы. То есть их можно располагать в местах, удобных как для банка, так и для клиентов (станции метро, рынки и другие людные места). Также, что немаловажно, на их строительство значительно легче получить разрешение, чем на сооружение (или даже переоборудование) уже существующих зданий. Нацбанк ратифицировал использование таких конструкций и любой банк может легко получить разрешение на их установку. Это нововведение способствует значительному расширению банковской сети, что, в свою очередь, делает ее более доступной для клиентов.

- А возможна ли их транспортировка?

- Да, конечно, так как их вес составляет не более трех тонн, то их свободно можно перемещать по городу или за его пределы. Поэтому такие модули можно будет установить в любом населенном пункте, чтобы облегчить его жителям доступ к банковской системе. Установить такой модуль не составит особого труда – достаточно будет подключить его к электросети.

- Насколько надежен такой модуль?

- Для банка, открывающего такое отделение, очень важна его безопасность. Рабочие места кассира и оператора защищены пулене-пробиваемым и взломостойким остеклением. Модуль обязательно оснащается охранно-пожарной сигнализацией. Все это в комплексе дает гарантию надежности.

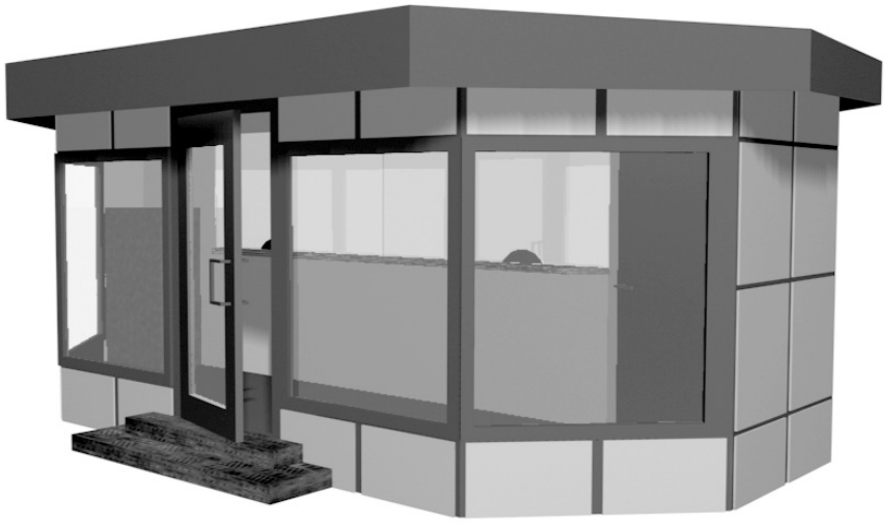
- Сколько рабочих мест в нем предусмотрено?

- Данный модуль рассчитан на два рабочих места. Он также может быть оборудован биотуалетом и кондиционером. Это способствует созданию комфортных условий труда. Тут предусмотрено место для клиентов, что немаловажно в случае неблагоприятных погодных условий (дождя, снега). Встроенный банкомат пятого поколения позволяет как снимать, так и вносить наличность на свой расчетный счет. В таких модулях можно оплачивать коммунальные услуги, осуществлять вклады и совершать другие банковские операции.

- Пользуется ли спросом данная продукция среди своих основных потребителей – банков?

- В связи с тем, что производство таких модулей ново для нашего рынка, такую продукцию изготовляют единицы. Поэтому большинство потенциальных потребителей просто не знают о ней. Я думаю, что если будет предложение, то обязательно будет и спрос. Так как данная продукция выгодна не только для банков, но и для их клиентов.

Беседовала Алещенко О.



НОВОСТИ

Украинский антивирусный центр

В целом, январь 2005 года, как и предполагалось, прошел без заметных эпидемий, и праздники удалось отметить по достоинству: спокойно и стабильно, однако в конце минувшего месяца, специалистами антивирусной лаборатории был выявлен ряд новых модификаций почтовых червей: I-Worm.Bagle.ax, I-Worm.Bagle.ay, I-Worm.Bagle.ba, которые распространяются в составе спам-рассылок.

Благодаря использованию спамерских технологий вредоносным программам буквально за считанные часы удалось войти в число наиболее часто встречающихся в почтовом трафике вирусов.

TOP 10 наиболее опасных вирусов почтового трафика в январе выглядит следующим образом:

1. I-Worm.Bagle.ay
2. I-Worm.Bagle.ba
3. I-Worm.Bagle.at
4. I-Worm.Nodoom.q
5. I-Worm.NoDoom.aa
6. I-Worm.Bagle.au
7. I-Worm.Mydoom.m
8. I-Worm.Bagle.ah
9. I-Worm.Nodoom.g
10. PSW.Bagle.based

У конечного пользователя TOP 10 вирусных инцидентов выглядит соответственно:

1. Trojan.Win32.Dialer
2. I-Worm.Bagle.ay
3. Trojan.Win32.StartPage
4. TrojanDownloader.Win32.Small
5. Backdoor.RBot
6. Worm.Win32.Padobot
7. Backdoor.Agent
8. I-Worm.Bagle.at
9. Worm.Win32.Opasoft.s
10. Backdoor.Dumator

В завершении, хотелось упомянуть о немаловажном событии для «Украинского Антивирусного Центра», которое ознаменовалось преодолением очередного рубежа вирусной базы: 96 000 вирусных записей.

UNA

Комплексний засіб захисту інформаційно-комп'ютерних мереж на рівні Інтернет-шлюзів

У наш час необхідність вирішення питань захисту інформації в комп'ютерних мережах не потребує великих і довгих обгрунтувань. Причина – зростання обсягу дій різних зловмисників, що зараз переростає у проблему «кібертероризму». Це стосується як державних інформаційних ресурсів, фінансових закладів, так і підприємств малого та середнього бізнесу. Проникнення зловмисників в інформаційно-комп'ютерні мережі підприємств може призвести до самих непередбачуваних наслідків. А основним шляхом проникнення сьогодні є Інтернет.

Технологія eSafe від компанії «Aladdin Knowledge Systems» забезпечує комплексний захист корпоративної інформації на рівні Інтернет-шлюзів, забезпечує захист від вірусів і будь-якого іншого шкідливого впливу, контролює доступ користувачів до Інтернет-ресурсів, блокує роботу різних мережевих програм. Технологія eSafe органічно поєднує в собі функції антивірусу, антиспаму, URL-фільтра і деякі функції IDS-систем.

Архітектура eSafe надає оптимальний рівень захисту з якнайменшими витратами на адміністрування. З багатьох причин цей унікальний продукт у різних країнах став стандартом де-факто для шлюзів, що вимагають підвищеної безпеки. Він прозорий для користувачів, не вимагає установки клієнтського програмного забезпечення на кожній робочій станції, не вимагає змін у конфігурації комп'ютерних мереж.

eSafe має такі можливості:

Н завдяки наявності в дистрибутиві операційної системи Linux RedHat та використанню технології Virtual Applience продукт інсталюється за лічені хвилини;

★ могутній антивірусний та антимодульний шлюз з функцією контентної фільтрації, що забезпечують комплексний захист інформації, перевіряючи **SMTP, HTTP, FTP, POP3** протоколи;

★ перевірка електронної пошти – технологія включає функції антирелей, антибомбінг, перевірку автентичності відправників, наявність додаткового модуля для боротьби зі спамом, що містить 17 видів перевірок, що дозволяють розпізнати спам, використовуючи технології від найпростіших перевірок по RBL до аналізу зображень;

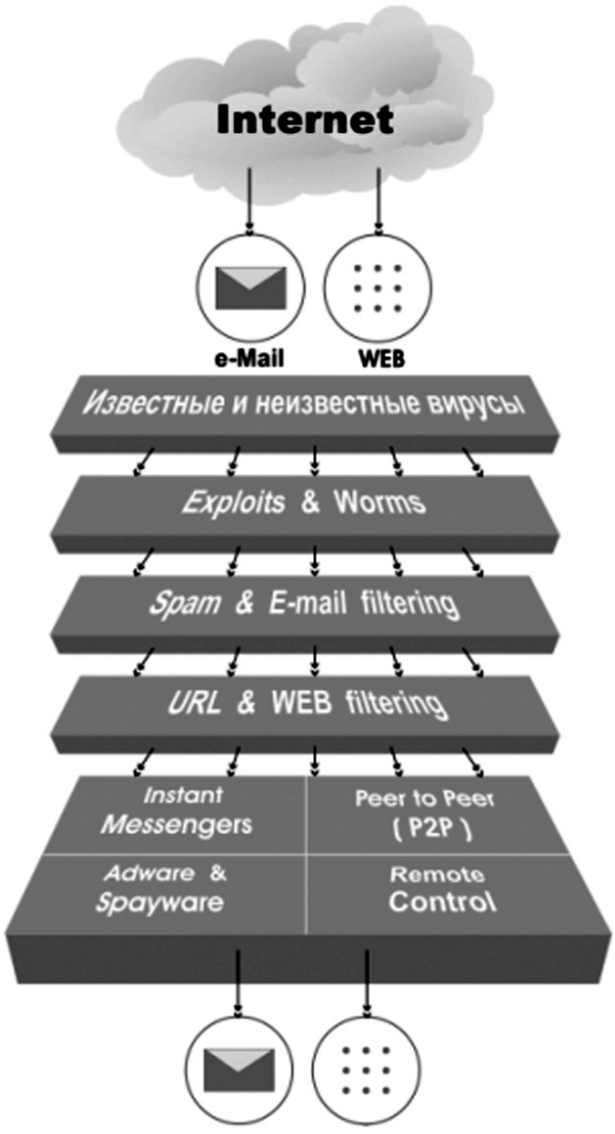
★ повний контроль користувачів комп'ютерної мережі, що попереджує витік інформації;

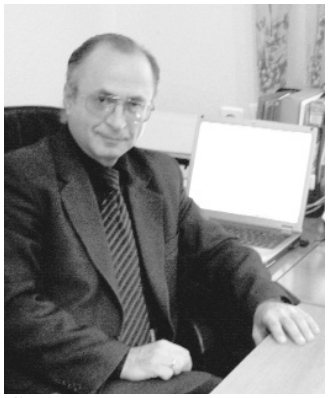
★ оновлення списку Web-сайтів небажаного або шкідливого вмісту. База даних містить більше 20 мільйонів сайтів. Такі можливості дають гарантію, що Інтернет буде використаний за призначенням. Наприклад, адміністратор може включити в перевірку категорію «Web-пошта» і використання співробітниками поштових Web-серверів особистого користування стане неможливим;

★ блокування роботи мережевих програм: системи обміну повідомленнями (ICQ, MSN), троянські програми, системи віддаленого адміністрування, Adware&Spyware і т. д.;

★ забезпечення високої продуктивності функ-ціонування комп'ютерної мережі. Один комп'ютер з eSafe здатен забезпечити пропускну спроможність мережі до 40 Мбіт/с при більш ніж 1 000 одночасних підключень або обробляти до 50 000 листів електронної пошти на годину;

★ одноосібного і єдиного комплексного інструменту інформаційної безпеки, що об'єднує в собі найефективніші технології для захисту при роботі в мережі Інтернет.





Ситник В. Н.

На завершення додамо, що компанія ЗАТ «Об'єднання ЮГ» є ексклюзивним бізнес-партнером компанії Aladdin з питань розповсюдження та супроводження продуктів сімейства eSafe в Україні.

ЗАТ «Об'єднання ЮГ»,
м. Київ 04070, Контрактова пл., 4,
тел. /факс: +380 44 417-07-73,
417-03-76
info@yug.com.ua

НОВОСТИ

Расходы на безопасность в мире в 2005 составят $48 млрд.

Затраты США и остального мира на безопасность будут быстро и стабильно увеличиваться. По оценкам Homeland Security Research Corporation, в 2005 году мировые затраты на безопасность (товары и услуги, предназначенные для борьбы с террором и криминалом) составят примерно $48 млрд., причем около половины этих расходов придется на долю США.

Как сообщает Washington ProFile, в 2007 году мировые вложения в эту сферу достигнут $57 млрд., в 2009 году - примерно $90 млрд. В 2015 году затраты на безопасность превысят $170 млрд. При этом, доля США постепенно будет снижаться и к 2015 году расходы Соединенных Штатов на безопасность составят примерно 30% от общемировых.

REGNUM. WP

Классификация угроз для компьютерных данных и систем по рекомендациям Конвенции о киберпреступности Совета Европы

Тенденция к расширению международного сотрудничества в борьбе с преступностью в сфере высоких технологий отмечается в деятельности многих международных организаций. Одной из них является Совет Европы, по мнению которого без государственного контроля компьютерных сетей обойтись нельзя, а законодательное регулирование киберпространства в одной отдельно взятой стране вряд ли возможно. Поэтому рост компьютерной преступности требует согласованного подхода государств к выработке стратегии борьбы с ней. Очевидно, что данное противоречие можно устранить только в рамках международного права. Этой проблеме посвящен ряд принятых Советом Европы рекомендаций, в которых сделана попытка определить понятие и очертить круг «преступлений, связанных с использованием компьютерных технологий». Однако рекомендательный характер этих документов не способствует разрешению возникающих на практике коллизий, для чего необходимы полноценные международно-правовые документы.

Осознание этого повлекло за собой формирование Комитетом министров Совета Европы в феврале 1997 г. Комитета экспертов по преступности в киберпространстве, перед которым была поставлена задача изучить юридические проблемы, возникающие при расследовании компьютерных преступлений. По результатам изучения им был разработан проект Конвенции о киберпреступности, вариант которой представлен Советом Европы для публичного обсуждения в апреле 2000 г. Реакция правозащитных организаций разных стран на проект Конвенции оказалась вполне ожидаемой.

В открытом письме правозащитных групп к Совету Европы утверждается, что проект «противоречит известным нормам защиты личности, неоправданно усиливает полномочия национальных правительств, подрывает развитие методов обеспечения безопасности информации, что уменьшает ответственность государств перед законом».

После открытого обсуждения проект доработан с учетом требований усиления гарантий неприкосновенности частной жизни и подготовлен к обсуждению исполнительными органами Совета Европы. В 2001 г. он был обсужден на заседании Европейского комитета по проблемам преступности, которым в него были внесены некоторые изменения и принято решение о вынесении проекта Конвенции для принятия и подписания Комитету Министров Совета Европы, затем предстояло подписание Конвенции странами-членами Совета Европы, ее ратификация и исполнение. Конвенция о киберпреступности Совета Европы вступила в действие с 7.01.2001 г. Украина подписала Конвенцию 23.11.2001 г. В связи с этим настало время внимательно ознакомиться и уяснить основные положения этого международно-правового документа, а также выработать меры, обеспечивающие его исполнение в нашей стране и гармонизацию его с законодательными актами Украины.

Конвенция о киберпреступности представляет собой комплексный документ, содержащий нормы, призванные оказать существенное влияние на различные отрасли права: уголовное, уголовно-процессуальное, авторское, гражданское, информационное. Она базируется на основных принципах международного права: уважения прав человека, сотрудничества и добросовестного выполнения обязательств.

Нормы Конвенции направлены на регулирование трех основных блоков вопросов:

★ сближение уголовно-правовой оценки преступлений в сфере компьютерной информации;

★сближение национальных уголовно-процессуальных мер, направленных на обеспечение сбора доказательств при расследовании таких преступлений;

★ международное сотрудничество в уголовно-процессуальной деятельности, направленное на собирание доказательств совершения таких преступлений за рубежом.

Уголовно-правовые вопросы.

Нормами права Конвенции предлагается включить в законодательство стран-участниц единые нормы об уголовной ответственности за «киберпреступления», перечень которых включает:

★ деяния, направленные против компьютерной информации (как предмета преступного посягательства) и использующими ее в качестве уникального орудия совершения преступления;

★ деяния, предметом посягательства которых являются иные охраняемые законом блага, а информация, компьютеры и т. д. являются лишь одним из элементов объективной стороны преступления в качестве, к примеру, орудия его совершения, составной части способа совершения или сокрытия.

Объектом киберпреступлений, согласно Конвенции, является широкий спектр охраняемых нормами права общественных отношений, возникающих при осуществлении информационных процессов по поводу производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления компьютерной информации, а также в иных областях, где используются компьютеры, компьютерные системы и сети.

Среди них, **учитывая повышенную общественную значимость, нормами права Конвенции выделяются правоотношения, возникающие в сфере обеспечения конфиденциальности, целостности и доступности компьютерных данных и систем, законного использования компьютеров и компьютерной информации (данных), авторского и смежных прав на интеллектуальную собственность.**

Объективная сторона киберпреступлений характеризуется выделением четырех групп общественно опасных деяний, успешное противодействие которым возможно только при широком международном сотрудничестве стран-членов, подписавшим Конвенцию Совета Европы. Для выработки соответствующей политики безопасности и ее гармонизации с достигнутым международным опытом в таблице предлагается для сравнительного анализа и использования модель потенциальных угроз компьютерным данным и системам, регламентированных по нормам права Конвенции о киберпреступности Совета Европы. Рассмотрим предложенную в модели классификацию и содержание четырех групп преступлений.

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем.

★ **Противозаконный доступ** – получение доступа к компьютерной системе в целом или к любой ее части без права на это, который может рассматриваться как преступление, если совершен в обход мер безопасности и с намерением завладеть компьютерными данными или иным бесчестным намерением, или в отношении компьютерной системы, соединенной с другой компьютерной системой.

★ **Противозаконный перехват компьютерных данных** – если он осуществлен с использованием технических средств перехвата без права на это и для непубличных передач компьютерных данных в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные, а также если он совершен в обход мер безопасности и с намерением завладеть компьютерными данными или иным бесчестным намерением, или в отношении компьютерной системы, соединенной с другой компьютерной системой.

★ **Нарушение целостности данных** – повреждение, стирание, порча, изменение или блокирование компьютерных данных без права на это, в том чис-

ле исключительно в случаях, повлекших за собой серьезные последствия.

★ **Вмешательство в работу (функционирование) системы** – создание без права на это серьезных помех работе компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или блокирования компьютерных данных.

★ **Противоправное использование устройств** – производство, продажа, приобретение для использования, импорт, оптовую продажу или иные формы предоставления в пользование: (1) устройств, включая компьютерные программы, разработанные или адаптированные, прежде всего для целей совершения преступлений; (2) компьютерных паролей, кодов доступа или иных подобных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или к любой ее части, с намерением использовать их с целью совершения преступлений.

Владение одним из предметов, упоминаемых выше, с намерением использовать его с целью совершения преступлений.

2. Преступления, связанные с использованием компьютеров.

★ **Подлог с использованием компьютеров** – ввод, изменение, стирание или блокирование компьютерных данных, приводящие к нарушению аутентичности данных с намерением, чтобы они рассматривались или использовались в юридических целях, как будто они остаются подлинными, независимо от того, являются ли эти данные непосредственно читаемыми и понятными.

★ **Мошенничество с использованием компьютеров** – лишение другого лица его собственности путем ввода, изменения, стирания или сокрытия компьютерных данных или вмешательства в функционирование компьютера или системы с целью неправомерного получения экономической выгоды для себя или для иного лица.

3. Преступления, связанные с содержанием данных.

★ **Правонарушения, связанные с детской порнографией** (порнографическими материалами, визуально отображающими участие несовершеннолетнего или кажущегося совершеннолетним лица в сексуально откровенных действиях, а также реалистические изображения, представляющие несовершеннолетних, участвующих в сексуально откровенных действиях), а именно:

- производство с целью распространения через компьютерные системы;
- предложение или предоставление через компьютерные системы;
- распространение или передача через компьютерные системы;
- приобретение через компьютерную систему для себя или для другого лица;
- владение детской порнографией, находящейся в компьютерной системе или в среде для хранения компьютерных данных.

4. Преступления, связанные с нарушением авторского и смежных прав.

★**Нарушения авторского права,** предусмотренного нормами внутригосударственного законодательства, с учетом требований Парижского акта от 24 июля 1971 г. к Бернской Конвенции о защите произведений литературы и искусства, Соглашения о связанных с торговлей аспектах прав на интеллектуальную собственность и Договора об авторском праве Всемирной организации интеллектуальной соб-ственности (ВОИС), за исключением любых моральных прав, предоставляемых этими Конвенциями, когда такие действия умышленно совершаются в коммерческом масштабе и с помощью компьютерной системы.

★ **Нарушение смежных прав, связанных с авторским правом:**

- предусмотренных нормами внутригосударственного законодательства, с учетом требований Международной конвенции о защите прав исполнителей, производителей звукозаписей и радиовещательных организаций (Римская конвенция);
- соглашений о связанных с торговлей аспектах прав интеллектуальной соб-ственности и Договора ВОИС об исполнителях и звукозаписях, за исключением любых предоставляемых этими Конвенциями моральных прав, когда такие действия совершаются умышленно в коммерческом масштабе и с помощью компьютерной системы.

В качестве вредных последствий перечисленных деяний Конвенцией признается нарушение прав законных пользователей компьютерной информации, компьютеров, их систем или сетей. Установление в качестве обязательного признака более тяжелых последствий (материального ущерба, противоправного использования полученной компьютерной информации и т. д.) проектом оставлено на усмотрение государств. В целом нормы Конвенции не предусматривают обязательность наступления вредных последствий.

Субъектом киберпреступлений может быть физическое лицо, совершившее указанные выше действия.

Исходя из складывающейся в различных странах практики, нормы Конвенции требуют установления ответственности юридических лиц за правонарушения, предусмотренные ею. Условиями наступления ответственности юридического лица являются: совершение действия с целью получения выгоды в пользу юридического лица его должностным лицом, занимающим руководящий пост, с использованием его полномочий по представлению юридического лица, принятию решений или осуществлению контроля за его деятельностью.

Кроме того, Конвенция предписывает устанавливать ответственность юридических лиц и в случаях совершения противоправных действий иным работником под руководством должностного лица, занимающего руководящий пост, с целью получения выгоды в пользу юридического лица.

Субъективная сторона киберпреступлений

Все преступления, упомянутые в нормах Конвенции, влекут наступление ответственности только в случае их совершения умышленно. В некоторых статьях проекта, устанавливающих преступность «традиционных» преступлений, совершенных с использованием компьютера или компьютерной информации, предусмотрено, что умышленная форма вины должна характеризовать не только само деяние, но и противоправное их использование, хотя это и является квалифицирующим признаком таких преступлений (к примеру, статья 8 – мошенничество с использованием компьютера).

Наряду с оконченными преступлениями в Конвенции предусматривается необходимость установления ответственности за покушение, соучастие или подстрекательство к его совершению.

Согласно нормам Конвенции установление конкретных санкций за совершение указанных деяний отнесено к ведению государств стран-членов, подписавшим Конвенцию. По их усмотрению может устанавливаться уголовная ответственность для физических лиц, а также уголовная, гражданско-правовая либо административная ответственность юридических лиц. Предусмотренные внутригосударственным законодательством санкции должны быть эффективны, пропорциональны и убедительны.

Уголовно-процессуальные аспекты

Одной из главных особенностей Конвенции является то, что в ней предложено исходить из того положения, что главенствующая роль в регулировании уголовного процесса расследования преступлений в сфере компьютерной преступности принадлежит национальному законодательству. В силу этого Конвенция включает главу 2 – «Меры, которые надлежит принять на национальном уровне», в которой предусмотрено включение в национальный уголовный процесс норм о процессуальных действиях, специфических для расследования и судебного разбирательства по делам о компьютерных преступлениях.

В круг процессуальных норм, предлагаемых в Конвенции для включения в национальное законодательство, входят, прежде всего, известные следственные действия, дополненные рядом особенностей, связанных со спецификой, присущей доказательственной информации в форме компьютерных данных.

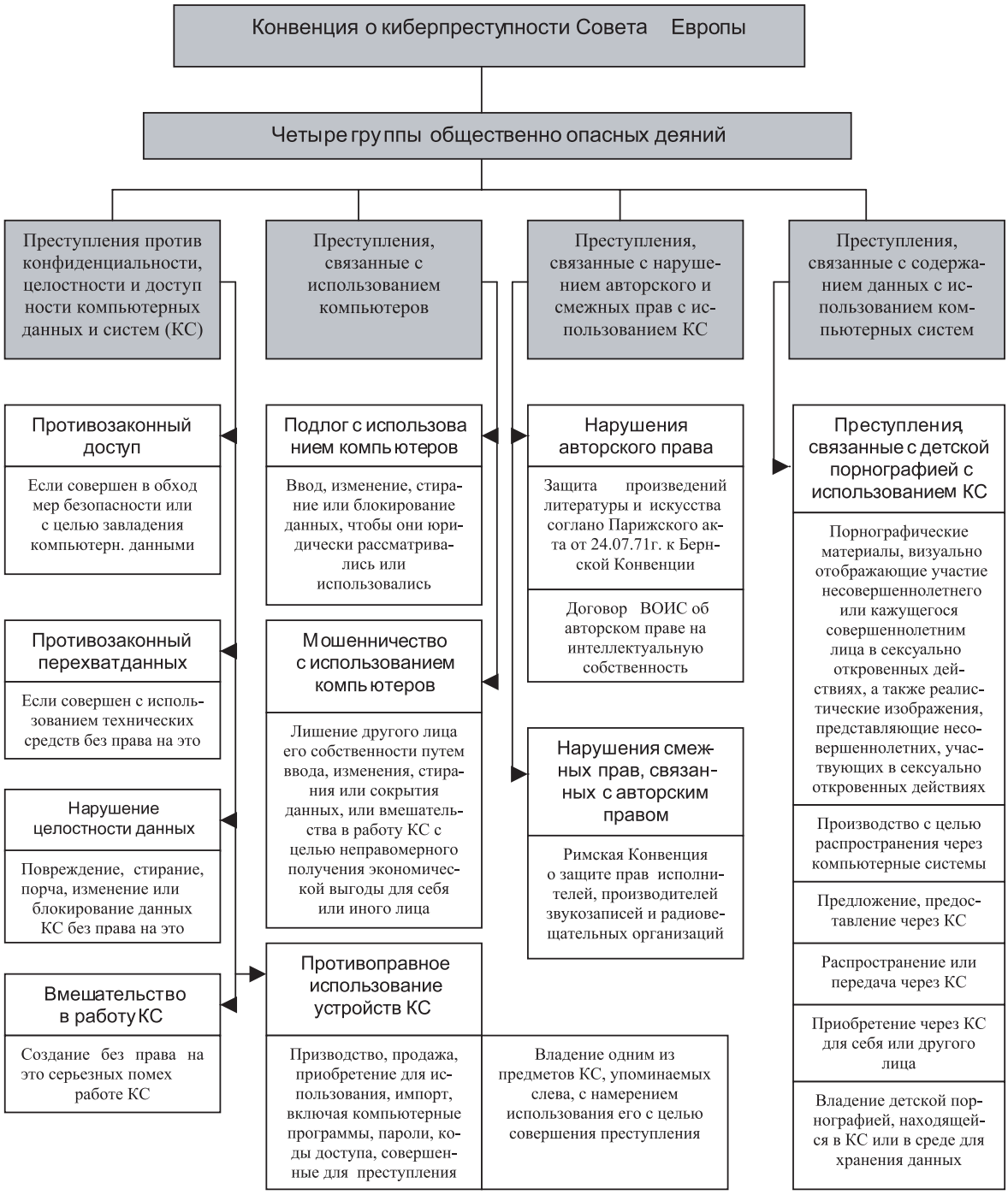
В силу этого, прежде всего, круг процессуальных институтов предлагается дополнить новым видом обыска и выемки – обыск и выемка хранимых компьютерных данных. Конвенция содержит предписания о том, что:

★ обыску или иному подобному следственному действию, обеспечивающему непосредственное получение доказательственной информации, могут быть подвергнуты компьютерные системы или их части, а также хранящиеся там компьютерные данные, и среда для хранения компьютерных данных, в которой могут храниться искомые компьютерные данные;

★ если в ходе обыска имеются основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части и когда такие данные доступны из первой системы или могут быть получены с ее помощью, компетентные органы должны быть вправе незамедлительно «распространить» производимый обыск на эту другую систему;

★ при обнаружении искомых компьютерных данных компетентные органы должны быть вправе: произвести выемку вычислительной системы, ее части или среды для хранения компьютерных данных либо иным подобным образом наложить арест на них; изготовить и сохранить копии соответствующих компьютерных данных; обеспечить сохранение целостности относящихся к делу хранимых компьютерных данных; сделать эти компьютерные данные в компьютерной системе, доступ в которую был получен, недоступными или удалить их из нее.

Термин «данные о потоках информации», согласно пункту «d» ст. 1 Кон-



Примечание: ВОИС – всемирная организация интеллектуальной собственности
КС – компьютерные данные и системы

Рис. 1 Модель потенциальных угроз компьютеоным данным и системам по нормам права Конвенции о киберпреступности Совета Европы

венции, означает любые компьютерные данные, относящиеся к передаче информации через посредство вычислительной системы, которые генерируются вычислительной системой, являющейся составной частью соответствующей коммуникационной цепочки, и указывают на источник, назначение, путь или маршрут, время, дату, размер, продолжительность или тип соответствующего сетевого сервиса.

Для обеспечения выемки требуемых компьютерных данных компетентные органы вправе обязать любое лицо, обладающее знаниями о функционировании соответствующей компьютерной системы или применяемых мерах защиты, оказать соответствующую помощь.

Наряду с этим в Конвенции предусматривается необходимость формирования на внутригосударственном уровне **правовых основ новых процессуальных действий.** К ним отнесены:

Во-первых, незамедлительное обеспечение сохранности хранимых компьютерных данных, включая данные о потоках информации, которые были генерированы и сохранены с помощью компьютерной системы, когда имеются основания полагать, что эти данные особенно подвержены риску потери или модификации. Оно должно осуществляться на основе распоряжения компетентных органов, отданного любому лицу, во владении или под контролем которого находятся компьютерные данные. Конкретный срок сохранения Конвенцией не установлен, но обозначен как «адекватный период времени, который позволит компетентным органам добиться раскрытия этих компьютерных данных». Это означает, что предлагаемый процессуальный институт не дает правовых оснований для прямого доступа органов власти к компьютерной информации, а лишь создает условия для него, являясь мерой предварительного характера. При этом под сохранностью данных следует понимать оставление их в том виде, в каком они уже имеются в ЭВМ, защитив от любых внешних воздействий.

Во-вторых, незамедлительное обеспечение сохранности и частичное раскрытие данных о потоках информации. Оно отличается от предыдущего тем, что подлежит применению в случаях, когда речь идет о необходимости сохранения сведений о сообщениях электросвязи, передаваемых по компьютерным сетям. Это должно позволить незамедлительно сохранять данные о потоках информации «независимо от того, один или большее число поставщиков услуг были вовлечены в передачу соответствующего сообщения», а с другой – незамедлительно раскрывать эти данные компетентным органам в объемах, достаточных, чтобы «идентифицировать поставщиков услуг и путь, которым передавалось сообщение», то есть фактически для того, чтобы оперативно отследить прохождение компьютерной информации в сетях от точки ввода до конечного адресата.

В-третьих, отдача распоряжения о предъявлении. Такое распоряжение может быть отдано лицу - о предъявлении компьютерных данных, находящихся под контролем этого лица, хранящихся в компьютерной системе или в иной среде для хранения компьютерных данных, поставщику услуг - сведений о его абонентах. К последним отнесена любая имеющаяся у поставщика услуг информация о пользователях, выраженная как в форме компьютерных данных, так и в любой другой форме (за исключением данных о потоках или содержании информации), с помощью которой можно установить: тип использованной связи, ее технические условия и время осуществления; личность пользователя, его адрес, номера телефонов и иных средств доступа, сведения о выставленных ему счетах и произведенных им платежах; любые другие сведения о месте установки коммуникационного оборудования. Следует отметить, что нормы Конвенции допускают применение данного вида новых полномочий строго на индивидуальной основе для решения задач расследования конкретных уголовных дел. В связи с этим нужно понимать, что эти новые полномочия не должны использоваться для того, чтобы заставить всех поставщиков услуг постоянно накапливать и хранить сведения о всех своих абонентах, всю передаваемую ими компьютерную информацию и т. д.

В-четвертых, сбор и запись с применением технических средств в режиме реального масштаба времени данных о потоках информации, передаваемых через компьютерные системы.

Нормами Конвенции предусмотрено наделение полномочиями осуществлять эту деятельность как компетентных органов государства, так и по их указанию поставщиков услуг. Данный вид деятельности рассчитан на применение в отношении сведений о сообщениях, передаваемых по сетям электросвязи, которые формируются (создаются) непосредственно в момент реализации таких полномочий. При этом осуществляется передача нематериальных объектов (например, в форме электромагнитных импульсов), а их сбор и запись не мешают прохождению самого сообщения по сетям электросвязи до адресата.

В-пятых, перехват (сбор и запись) данных о содержании сообщений, передаваемых с помощью компьютерных систем, осуществляемый как компетентными органами государства, так и поставщиками услуг по их указанию. Данный институт аналогичен предыдущему, но касается непосредственно содержательной части сообщений, передаваемых по сетям электросвязи.

Хотя в нормах Конвенции детально и не прописан механизм правового регулирования реализации двух последних способов собирания компьютерной информации, имеющийся опыт и соотнесение с нормами законодательства других стран позволяют утверждать, что они, вероятнее всего, в настоящее время подлежат использованию путем проведения оперативно-розыскных мероприятий.

Таким образом, предложенная модель потенциальных угроз для компьютерных данных и систем с учетом рекомендаций Конвенции о киберпреступности Совета Европы может быть полезна для специалистов при создании защищенных компьютерных систем, а также для гармонизации внутригосударственных законодательных актов Украины как страны-участницы по выполнению этой Конвенции.

Статья подготовлена по результатам проведенных исследований, а также по материалам журнала «Защита информации. Конфидент» и документов Совета Европы.

Шорошев В. В.,
Близнюк И. Л.,
Балина С. Н.

НОВОСТИ

Бывший сотрудник AOL продал спамерам 92 млн адресов

24-летний инженер, некогда работавший в American Online, обвиняется в краже 92 миллионов ников (screen name) и e-mail адресов и продаже этой информации спамерам, после чего на пользователей обрушились почти 7 миллиардов почтовых сообщений.

Jason Smathers обвиняется в нарушении правил конфиденциальности. Ему грозит от полутора до двух лет тюремного заключения, а также от $200,000 до $400,000 обязательного возмещения убытков.

Jason Smathers сообщил на суде, что получил $28,000 от кого-то, кто хотел распространить информацию о сайте азартных игр среди пользователей AOL.

Smathers был уволен из AOL в июле прошлого года. Говорят в 2003 он воспользовался кодом доступа другого сотрудника для кражи списка пользователей AOL в представительстве компании в Далласе. Как утверждает обвиняемый, он продал список Шону Данавею (Sean Dunaway), который использовал его для рассылки нежелательной рекламы.

Украденный список из 92 миллионов адресов содержал множественные адреса 30 миллионов пользователей AOL. Он по-прежнему циркулирует в спамерских кругах.

itua.info

XSpider 7 – професійна система моніторингу і аудиту безпеки комп'ютерної мережі

Навіщо потрібен сканер безпеки?

Забезпечити високий рівень безпеки мережевих ресурсів з найменшими зусиллями і витратами.

Подвійний захист

1 При роботі в Інтернет, завдяки XSpider всі зовнішні атаки приречені на поразку.

2 Внутрішні користувачі локальної мережі не зможуть спричинити небезпеку своїми діями.

Що необхідно для зовнішнього захисту?

Найпростішим рішенням для захисту зовнішнього периметра мережі (шлюзів) вважається:

★ Встановлення і розташування міжмережевих екранів (firewall).

★ Постійна перевірка нових уразливостей та впровадження адекватних заходів.

Перевірка уразливостей – це найбільш важливий і в одночас складний і трудомісткий процес, полегшення здійснення якого забезпечує сканер.

Що потрібно для внутрішнього захисту мережі?

Звернути увагу на те, що:

★ Всі комп'ютери мережі розглядаються як потенційно уразливі.

★ Створення грамотної архітектури внутрішньої мережі, розробка і дотримання політики безпеки – важлива умова забезпечення інформаційної безпеки.

Архітектура системи – річ відносно стала, в той час, як контролем за виконанням політики безпеки треба займатися постійно, і саме це виявляється найважчим.

Саме тому, найголовнішим завданням виявляється постійний моніторинг уразливостей окремих об'єктів та полегшення цього процесу шляхом автоматизації.

Уразливості

Термін «уразливості» означає власне уразливості (vulnerabilities) і дефекти (exposures).

«Класичні» уразливості – це помилки в програмному забезпеченні. «Дефект» – це порушення безпеки, викликане неправильним налаштуванням або конфігурацією програми, тобто помилками адміністраторів.

Збільшення кількості уразливостей має цілком конкретні причини. По-перше, – це встановлення нового програмного забезпечення із своїми власними недоробками і змінами налаштувань, які не завжди проводяться кваліфіковано. По-друге, – виявлення нових «дірок» в існуючому програмному забезпеченні. Існує ціла інформаційна індустрія, що займається збиранням, публікацією і аналізом уразливостей. Регулярні бюлетені (bugtrack) про нові уразливості одержують інформацію як від розробників ПЗ, так і від незалежних експертів, фахівців і навіть іноді від хакерів, які прагнуть уваги.

Особливості XSpider 7

1. Логічний і структурований процес моніторингу безпеки завдяки багатовіконному інтерфейсу і засобам автоматизації.

2. Зручність використання :

★ вибір завдань, встановлення розкладу їх виконання,

★ можливість вибору профілю сканування,

Поляков В. А.

★ перегляд історії сканування,

★ наочність та простота виведення результатів,

★ одночасне виконання багатьох завдань,

★ моментальна генерація звітів,

★ зручна доставка звітів до користувача.

3. Висока якість :

★ проведення повного аналізу уразливостей, як через базу даних, так і евристичними методами,

★ мінімальна кількість помилкових діагностик,

★ стовідсоткова достовірність результатів сканування,

★ висока надійність моніторингу,

★ підвищена безпека мережі шляхом щоденного оновлення бази даних уразливостей,

★ економія часу та підвищення ефективності роботи фахівців.

На закінчення

Відомо, що сканери безпеки відносяться до числа інструментів, якими користуються хакери. XSpider 7 створювався не для нападу, а для захисту ресурсів. Даний продукт, розроблений компанією Positive Technologies (Москва) і користується великою популярністю завдяки своїм широким можливостям і невисокій вартості володіння. ЗАТ «Об'єднання ЮГ» є ексклюзивним партнером компанії Positive Technologies і займається впровадженням і технічним супроводженням XSpider в Україні.

Отримати пробну версію і придбати XSpider 7 можна в компанії «Об'єднання ЮГ»
Тел. / факс: (044) 417-07-73, 417-03-76
e-mail : info@yug.com.ua

НОВОСТИ

США: ремни безопасности снижают смертность на 7%

Обязательное использование ремней безопасности снижает число смертей у водителей на 7%.

По данным Национальной Администрации Безопасности Дорожного Движения США\National Highway Traffic Safety Administration, в 21 штатах и Федеральном Округе Колумбия (город Вашингтон) приняты «первичные законы» об обязательном использовании ремней безопасности. В таких штатах в 2004 году ремни безопасности постоянно использовали 84% водителей. В 28-ти штатах полицейский в случае, если автомобиль совершил иное нарушение, то неиспользование ремня будет считаться отягчающим обстоятельством или будет караться отдельно (как правило, с помощью штрафа). В таких штатах в 2004 году пристегивались 73% водителей.

WP

НОВОСТИ

Microsoft «переводит стрелки» на ФБР

Корпорация Microsoft отказывается блокировать недавно найденную «дыру» в проигрывателе Windows Media Player, заявляя, что уязвимость эта - искусственная и изначально задумывалась для борьбы с пиратским копированием цифровых материалов. Пострадавшим же от троянцев, использующих эту лазейку, Microsoft рекомендует направлять свои претензии ФБР.

Пять лет тому назад в Microsoft произошло событие первостепенной важности - Билл Гейтс уступил высший пост в компании Стиву Баллмеру. В специальном заявлении Билл Гейтс отметил, что произведенные кадровые перестановки позволят ему «делать то, что я люблю больше всего, и сосредоточиться на технологиях будущего». Это событие, тем не менее, так и не привело к эпохальным переменам: «ахиллесовой пятой» продуктов компании как были, так и остаются вопросы обеспечения безопасности ее продуктов.

Ушедший год предельно остро поставил проблему уязвимости продуктов Microsoft. Широко разрекламированное обновление Windows XP SP2, вышедшее в 2004 году, не стало панацей, но лишь добавило пользователям новые проблемы. Количество «дыр» в продуктах компании достигло такого уровня, что американская организация CERT (Computer Emergency Rresponse Team - группа быстрого реагирования по вопросам информационной безопасности) рекомендовала пользователям переходить на браузеры, альтернативные Internet Explorer. Как следствие, впервые за долгое время доля Microsoft на рынке браузеров начала заметно сокращаться. Выход долгожданной операционной системы нового поколения Longhorn, на разработку которой уже затрачено более $1 млрд., откладывается на все менее определенное будущее - пока что на 2006 год.

Пятилетняя годовщина ухода Билла Гейтса «в тень» ознаменовалась еще одним знаковым событием, переводящим вопрос компьютерной безопасности в качественно иную плоскость. Компания отказалась блокировать уязвимость, выявленную испанской компанией Panda Software, на том основании, что уязвимость эта - искусственная и изначально задумывалась для борьбы с пиратским копированием цифровых материалов, а, следовательно, «дырой» в прямом смысле слова не является. Несмотря на то, что хакеры так не считают и вовсю используют новую технологию для заражения компьютеров своих жертв целыми «букетами» хакерских программ, Microsoft порекомендовала пострадавшим обращаться напрямую ... в ФБР.

CNews

Мобильный телефон, Интернет, вирусы...

С развитием технологий беспроводной передачи данных и мобильного доступа в Интернет современные сотовые телефоны приобретают свойства персональных компьютеров. Скоро в каждом мобильном телефоне будут своя операционная система, текстовые редакторы, базы данных. Все это даст возможность создавать файлы и обмениваться ими. С помощью сотовых телефонов станут возможными ведение банковских операций, совершение интерактивных покупок, обмен электронными данными. Поэтому все чаще можно слышать разговоры об опасности появления «сотовых вирусов». Ведь вирусы чаще всего передаются через электронную почту, доступ к которой становится доступной владельцам сотовых телефонов. Таким образом, создаются все заражения вирусами мобильных телефонов.

Специалисты считают, что в настоящее время реальной серьезной угрозы появления вирусов в мобильных системах не существует. Сотовые телефоны пока что недостаточно мощные и сложные, и у них отсутствуют аппаратные возможности для существования вирусов. К тому же операционные системы мобильных телефонов закрыты. Для того, чтобы в какую-то среду проникли вирусы, необходима информация о том, как эта среда работает, а компании, производящие мобильные телефоны, не раскрывают своих технологий в целях безопасности.

Компания Sun Microsystems и ряд ее партнеров завершила разработку стандарта MID (Mobile Information Device) на базе языка программирования Java для использования в мобильных телефонах, а компания Motorola выпустила интерфейс прикладного программирования (API), позволяющий разрабатывать для этих устройств дополнительные программы. Интеграция языка Java даст возможность запускать на телефонах программы третьих компаний и в дальнейшем позволит пользователям создавать собственные программы и обмениваться ими. Такие функциональные возможности мобильных телефонов открывают путь для создания как полезных, так и вредоносных программ. Однако технология Java доказала свою надежность и защищенность. За годы ее существования на персональных компьютерах были обнаружены всего лишь несколько Java-вирусов.

И тем не менее, еще 6 июня 2000 года в Испании был обнаружен «Timofonika». Он отсылал SMS-сообщения стандарта GSM через испанского оператора сотовой связи MoviStar. Это обстоятельство обусловило распространение слуха о появлении первого вируса, способного заражать непосредственно мобильные телефоны. На самом деле, кроме посылки SMS-сообщений, «Timofonica» более никакого отношения к телефонам не имел.

В начале августа далекого 2000 года была обнаружена утилита под названием HSE, которая имела способность рассылать SMS-сообщения любого содержания на мобильные телефоны ряда немецких сотовых сетей. Автор утилиты назвал свое детище SMS-Flooder (flood- наводнение, потоп). Эту программу нельзя отнести ни к разряду вирусов, ни к разряду Интернет-червей. Это просто вредоносная программа, которая может использоваться для совершения несанкционированных действий в отношении владельцев мобильных телефонов. И все же появление настоящих «мобильных» вирусов – это вопрос ближайшего будущего. Уже сейчас возможно появление вирусов в телефонах, поддерживающих стандарт WAP-протокол, посредством которого владельцы мобильных телефонов могут посещать в Интернете WAP-сайты, получая там примерно ту же информацию, которую содержат привычные www-ресурсы. Распространение вирусов сдерживает только недоступность средств разработки и плохая документированность стандарта.

Как считают специалисты аналитического агентства Gartner, появления «мобильных» вирусов стоит ожидать не ранее середины 2004 года. Пользователи мобильных телефонов будут бороться с вирусами аналогично тому, как это делается в компьютерах. На центральные станции операторы сотовой связи будут устанавливать аналоги серверных антивирусов.

Над разработкой антивирусных программ для мобильных систем активно работают многие фирмы. Например, финская антивирусная компания F-Secure разработала антивирусное программное обеспечение (ПО) для мобильных телефонов, работающих на основе операционной системы EPOC фирмы Symbian. F-Secure утверждает, что создание антивирусов – это подготовка Software к борьбе с надвигающейся угрозой.

Компания McAfee добавила в свою антивирусную программу VirusScan Wireless, предназначенную для беспроводных компьютерных устройств, выполненных на базе платформ PalmOS, Windows CE и Symbian EPOC, поддержку мобильных телефонов. Новая версия этого ПО называется VirusScan Wireless for Mobile. Эта программа производит сканирование приложений, имеющихся на так называемых смартфонах (smartphones), для их защиты от вирусов, червей и троянских коней.

Компания Brightmail анонсировала программное обеспечение Brightmail Solution Suite 2.1, которое, по ее заявлению, обеспечит пользователям мобильных телефонов и карманных компьютерных устройств защиту от спама и вирусов. Эта программа предназначена для операторов сетей мобильной связи.

Яковенко А. В.

НОВОСТИ

Самые необычные мобильники - в Японии!

Владельцы сотового телефона теперь по праву могут считать себя спортсменами: в Японии появился мобильник, позволяющий играть в активные игры - например, отрабатывать удар клюшкой для гольфа или же "расстреливать" воображаемых монстров из фотонного пистолета.

Мобильный телефон V603SH массой 142 г и размерами 50 x 99 x 25 мм разработан японскими компаниями Sharp и Aichi Steel Corporation. Новый аппарат первым в Японии начал реагировать на команды, подаваемые посредством его перемещения в пространстве.

Телефон можно использовать в качестве воображаемой клюшки для гольфа - бросив взгляд на экран, можно определить силу удара. Это - не единственное "побочное" предназначение телефона.

V603SH позволит также своим владельцам просматривать телевизионные передачи на жидкокристаллическом дисплее (2,4 дюйма, 240 x 320 пикселей, отображает до 260 тыс), который может поворачиваться на 180 градусов, и слушать радио. Полной зарядки аккумулятора хватает на час просмотра или проигрывания, 130 минут непрерывного разговора или 450 часов в режиме ожидания. Встроенная камера с разрешением 2,02 мегапикселя и CCD-матрицей позволяет делать снимки размером 1224 x 1632 пикселей. Камера поддерживает 2-кратное оптическое увеличение и 40-кратное - цифровое. Объем встроенной памяти телефона - 12 МБ, имеется слот для карт памяти формата SD.

Британское отделение сотового оператора Vodafone представило новинку 31 января. Правда, с ценой компания пока что не определилась. Ожидается, что продажи V603SH в Японии начнутся уже с середины февраля.

Вчера Vodafone представил в Японии еще один телефон - V603T от Toshiba со встроенным аналоговым ТВ-тюнером и системой караоке. Новинка позволяет смотреть телевизор и слушать радио в FM-диапазоне: полной зарядки батареи хватает на час просмотра или проигрывания, или же два часа непрерывного разговора. В режиме ожидания заряда аккумулятора хватит на 380 часов.

"Мобильный телевизор" оснащен также кредлом. Размеры нового V603T 50 x 103 x 25 мм, вес - 142 г. Основной ЖК-дисплей устройства размером 2,4 дюйма (240 x 320 пикселей) отображает до 260 тыс. цветов. Для удобства ЖК-дисплей можно вращать на все 360 градусов. Встроенная камера с разрешением 1,31 мегапикселя, CMOS-матрицей и 8-кратным цифровым увеличением (10-кратным для видео) позволяет делать снимки размером 960 x 1280 пикселей. Встроенной памяти телефона хватает на 10 МБ фотографий или видео, имеется также и разъем для карт памяти miniSD. Продажи V603T начнутся в Японии также уже в этом месяце.

В разработке чувствительных к движениям мобильников Японию обогнала Южная Корея. Еще в середине января компания Pantech начала продажи первого в мире такого телефона. В рекламе утверждалось, что с его помощью можно имитировать рыбную ловлю или управлять гоночным автомобилем. Кроме того, корейский телефон PH-S6500, позиционируемый как "телефон для активного отдыха", позволяет, к примеру, бегуну определить скорость бега, расход калорий и длину дистанции.

Cnews

Сотовый радиотелефон и безопасность

Время от времени в средствах массовой информации поднимается вопрос о вредном воздействии на человека систем сотовой связи, в частности, в связи с последствиями облучения головного мозга при пользовании сотовым радиотелефоном. В последнее время страх перед сотовыми аппаратами превратился в некое подобие городского мифа. Они и для здоровья вредные, и самолет могут с курса сбить, и пожар на заправке вызвать. И все это никак не подтверждается документально. Даже в США, где сотовая связь гораздо раньше стала неотъемлемым атрибутом жизнедеятельности человека, не известны какие-либо статистически обоснованные закономерности распространения тех или иных заболеваний среди абонентов систем сотовой связи. Да и в других странах проводимые по данному вопросу исследования не дали каких-либо определенных подтверждений подобным страхам.

Никто не может категорически утверждать, что нет вреда от радиотелефонов, равно как никто не может утверждать, что вред есть. Исследования в этой области ведутся с начала 1990-х годов. Все ученые единодушно сходятся на том, что электромагнитное излучение сотовых радиотелефонов, конечно же, воздействует на ткани головного мозга. Опыты над мышами, проведенные в Австралии и Финляндии, показали, что у животных нарушалась ориентация и развивались опухоли, хотя это и не является строгим доказательством того, что сотовые телефоны вредны и для здоровья людей. Сейчас появляется все больше свидетельств того, что радио- и микроволновые излучения видоизменяют основы клеточных биохимических процессов. Это вызывает изменение тканей и функций мозга. Но, как всегда, речь идет не об абсолютном исключении вредного фактора, а лишь о допустимой степени его воздействия.

Международное и Европейское агентства выработали стандарты безопасности, касающиеся мобильных телефонов. В выработке этих стандартов принимали участие группы врачей, ученых, инженеров, государственные медицинские учреждения и промышленные группы. Все мобильные телефоны, легально продаваемые на сегодняшний день, соответствуют этим стандартам, а следовательно, – безвредны. Но только в том случае, если соблюдать правила пользования и необходимые предосторожности.

Как показывают исследования, ткани мозга могут поглощать до 60 % энергии излучения передатчика сотового радиотелефона. И хотя многие исследователи говорят, что уровень излучений сотовых телефонов далек от зоны риска, он все же лежит близко к предельному уровню, рекомендованному международными нормами безопасности. Единицей влияния микроволнового излучения на организм человека является «специфическая норма поглощения» SAR (Specific Absorption Rates), численно равная энергии поглощенного излучения, приходящейся на 1 г (иногда 1 кг) биоткани. При поглощении единицы излучения в течение 20 минут ткани мозга нагреваются на 1 °С. Этот нагрев адекватно (либо неадекватно) компенсируется обменными процессами организма. Европейские организации считают, что для сотовых телефонов SAR не должна превышать 2 мВт/г.

Таблица 1. Коэффициенты излучения некоторых моделей сотовых телефонов.

Модель телефона	Коэффициент излучения
MOTOROLA T2288	0,54
SONY ERICSSON T100	0,61
NOKIA 65 10	0,71
NOKIA 8210	0,72
NOKIA 3310	0,75
NOKIA 7210	0,76
NOKIA 3510	0,81
SIEMENS C60 (A52, A55)	0,99
BENEFON Twin Dual	1,01
SONY J70	1,06
MOTOROLA V66	1,13
SIEMENS C45	1,14
SAMSUNG C100	1,17
SIEMENS C35i	1,19
NOKIA 6210	1,19
ERICSSON T200	1,27

Исследования Федерального технологического института г. Цюриха, проведенные с 16-тью различными моделями сотовых радиотелефонов, показали пятикратную разницу их SAR. Максимальный уровень SAR у самой безопасной модели составил 0,28 мВт/г, у самой опасной – 1,33 мВт/г.

Ученые Бристольского университета и Бристольского королевского госпиталя провели эксперимент под руководством доктора Алана Приса, в котором приняли участие добровольцы, с целью определить кратковременные эффекты от излучения при работе мобильных телефонов. Участникам эксперимента предлагалось выполнить определенный набор заданий на сообразительность, находясь в разных условиях: под воздействием микроволнового излучения от цифровых радиотелефонов, аналоговых радиотелефонов и без какого бы то ни было воздействия. Никаких значительных изменений в кратковременной памяти или неустойчивости внимания после 30-минутного воздействия излучения отмечено не было. Между тем исследования позволили установить, что время реакции мозга при визуальных тестах даже сокращается – для этого 36 добровольцев подверглись излучению, характерному для работающих мобильных телефонов. Этот эффект, по-видимому, связан с увеличением кровотока в мозгу под воздействием излучений. Увеличение кровотока, по мнению ученых, может быть вызвано незначительным нагреванием. Рост температуры можно объяснить двумя причинами: либо само по себе микроволновое излучение вызывает нагревание, либо это следствие выработки в крови определенных веществ, которая происходит в том случае, когда срабатывает защитный механизм организма в ответ на угрозу болезни или травмы.

Швейцарский институт технологии совместно с австралийской компанией EMC измерили уровень излучаемого поля некоторых моделей сотовых телефонов. Результаты этих измерений приведены в табл. 1.

И тем не менее, сотовый телефон может быть опасен не только для здоровья, но и для жизни некоторых людей. Источник этой опасности, как оказалось, давно и хорошо известен специалистам в области радиосвязи. Речь идет об электромагнитной совместимости радиоэлектронных устройств, во взаимных помехах, создаваемых этими устройствами. Радиопередающие устройства современных сотовых телефонов имеют выходную мощность в единицы ватт, а малые размеры самих радиотелефонов делают возможным их появление в местах повышенной опасности, например, в больнице или на борту авиалайнера.

Приведем пример. В современных больницах для проведения сложных операций, наблюдения за состоянием тяжелобольных или диагностики заболеваний используется большое количество весьма сложного и чувствительного электронного медицинского оборудования, которое является особенно уязвимым для радиопомех.

О степени названной опасности говорит тот факт, что за рубежом выпущено устройство, специально предназначенное для использования в медицинских учреждениях. Оно обнаруживает работающие поблизости сотовые радиотелефоны и радиостанции и подает сигнал тревоги, а также выдает специальное звуковое сообщение, предписывающее немедленно прекратить пользование сотовым телефоном. Такими приборами оснащаются, в первую очередь, хирургические, кардиологические и родильные отделения, отделения интенсивной терапии, диагностические и реабилитационные центры, лаборатории.

Практически все современное оборудование защищено от воздействия радиочастотного излучения. Тем не менее, излучение сотовых телефонов может оказывать воздействие на некоторые электронные приборы, особенно неисправные или плохо экранированные.

Сотовые телефоны могут быть опасны для тех людей, которые пользуются электронными кардиостимуляторами и другими приборами, функционирование которых связано с их жизнеобеспечением. В мире более миллиона человек живет с имплантированными кардиостимуляторами. В случаях, когда собственный ритм сердца прерывист или слишком слаб, этот прибор посылает электрические импульсы, необходимые для нормальной работы сердца. Кроме того, кардиостимулятор следит за работой сердца и, почувствовав нормальное биение, перестает его стимулировать. Может ли сотовый телефон вызвать сбой в работе сердечного стимулятора?

Да! Это подтверждают исследования. Вот мнение петербургского специалиста Евгения Долгих: «Опыты показывают, что электромагнитное поле сотового телефона способно «ослепить» стимулятор, сделать его нечувстви-

тельным к ритму сердца пациента, заставить его посылать стимулирующие импульсы, когда это не требуется сердцу, и даже отключить прибор».

Немецкие ученые тоже провели исследования с целью получить ответ на вопрос: может ли сотовый телефон вызвать сбой в работе кардиостимулятора? Исследовались три стандарта сотовой связи: NMT-450, GSM-900 и GSM-1800. Была проверена работа 231-го кардиостимулятора от различных фирм-производителей. Результаты исследования таковы: 30,7 % стимуляторов испытывали помехи от излучения телефонов стандарта NMT-450, 34,2 % – от GSM-900; при использовании телефонов, работающих в стандарте GSM-1800, сбоев в работе кардиостимуляторов не было.

Больным с кардиостимуляторами не следует держать телефон слишком близко к стимулятору, так как это может нарушить его работу. Согласно рекомендации Ассоциации производителей медицинского оборудования, включенный сотовый телефон должен находиться не ближе чем 15 см от кардиостимулятора, чтобы исключить сбои в его работе.

Проблема электромагнитного воздействия на кардиостимуляторы не ограничивается влиянием сотовых телефонов. Главная опасность – базовые станции, расположенные по всему городу и обладающие большой мощностью. Если от воздействия сотового телефона пациент может уберечься, держа его на достаточном удалении от стимулятора, то от мощного излучения базовой станции он совершенно не защищен. Больной может и не знать, что проезжает мимо такой станции на автобусе или что она находится на крыше его собственного дома.

В городе антенны базовых станций устанавливаются на высоте 15–100 м от поверхности земли на уже существующих постройках (общественных, производственных зданиях, жилых домах, дымовых трубах). А за городом базовую станцию легко увидеть даже издалека, это – высокие красные мачты за решетчатыми заборами.

Базовые станции работают в режиме приема и передачи сигнала. В зависимости от стандарта, станции излучают электромагнитную энергию в диапазоне частот от 463 до 1880 МГц. А такие излучения, как известно, могут неблагоприятно сказываться на здоровье. Поэтому влияние базовых станций постоянно изучается.

В последнее время специалистами разных стран, в том числе из Швеции, Венгрии и России, были проведены специальные исследования электромагнитной обстановки на территориях, прилегающих к базовым станциям. По результатам измерений специалисты констатировали, что во всех 100 % случаев электромагнитная обстановка в помещениях зданий, на которых установлены антенны, не отличалась от фоновой, характерной для данного района в данном диапазоне частот.

На прилегающей территории в 91 % случаев зафиксированный уровень электромагнитного излучения был в 50 раз меньше допустимого. Даже максимальный уровень излучений был в 10 раз меньше допустимого, и он был зафиксирован у здания, на котором были установлены сразу три базовые станции разных стандартов.

Имеющиеся научные данные и действующая система контроля при вводе в эксплуатацию станций сотовой связи позволяют отнести эти станции к наиболее безопасным системам связи (как с экологической, так и с санитарно-гигиенической точки зрения). Так что наличие антенны на вашем доме или мачты вблизи дачного участка никакого вреда вашему здоровью не причинит.

Вопрос о влиянии электромагнитного излучения на сердце не исчерпывается только проблемой устойчивой работы кардиостимуляторов. О других опасностях, которые таит в себе сотовый телефон, можно судить по результатам экспериментов, проведенных в Московском институте биофизики над подопытными животными. При облучении сердца лягушки высокочастотным модулированным электромагнитным сигналом в течение 5–10 минут, даже при очень низкой интенсивности сигнала, удавалось остановить каждое второе сердце, а у оставшихся – снижалась частота биения. Для крыс и кроликов то же излучение оказалось не столь губительным, однако в 30 % случаев отмечались достоверные изменения сердечной деятельности.

Немецкие исследователи обнаружили еще один изъян сотовых телефонов – во время работы они повышают артериальное давление человека. Исследование было проведено корректно. У десяти добровольцев на правой стороне головы были закреплены сотовые телефоны GSM-900. Располагали аппараты примерно так же, как они находятся во время разговора. Телефоны включали в рабочий режим так, чтобы испытуемые об этом не знали. Это позволило исключить субъективные факторы, которые могли повлиять на давление. С помощью специальных мониторов у больных постоянно измеряли артериальное давление. Разговор в течение 35 мин приводил к повышению давления на 5–10 мм рт. ст. Предполагается, что поле вызывало спазм сосудов, снабжающих кровью правое полушарие, а уже это приводило к повышению давления.

Электромагнитное излучение сотовых телефонов может повлиять не только на ваше здоровье (в прямом смысле), но и на неисправное или плохо экранированное электронное оборудование автомобилей и другой техники, что также может подвергнуть вас опасности.

Мобильный телефон может влиять на работу некоторых моделей слуховых аппаратов. В этом случае следует обратиться в центр обслуживания для выяснения возможных вариантов решения проблемы или к производителю слухового аппарата и приобрести другую модель.

Чтобы избежать неприятностей, владельцу автомобиля нужно проконсультироваться у его производителя, достаточно ли хорошо экранирована электроника. Следует задать этот вопрос и изготовителям любого другого оборудования, установленного в автомобиле. Необходимо также проследить, чтобы сотовый телефон и его принадлежности были правильно установлены и не мешали раскрытию подушек безопасности.

Одно из последних исследований, проведенных Отделом торговли и промышленности, показало, что использовать устройства для мобильных телефонов hands free более безопасно для здоровья людей, чем держать сами телефоны непосредственно около головы. Тесты показали, что эти устройства значительно уменьшают воздействие электромагнитного излучения. Позиция телефона, включая угол, под которым клавиатура направлена к лицу, также влияет на уровень поглощения этого излучения. Поэтому, даже при использовании устройства hands free, телефон лучше держать не в руке, а, например, в кармане.

Австралийская ассоциация потребителей тоже провела исследования, которые показали, что использование наушников с микрофоном в сотовых телефонах уменьшает эффект воздействия электромагнитного излучения на 92 %. Однако это исследование в корне противоречит британскому, которое показало, что такие устройства действуют как своеобразные антенны и поэтому уровень электромагнитного излучения, действующего на мозг абонента, в три раза превышает уровень обычного сотового телефона. В любом случае, уровень излучения от сотового телефона не превышает допустимых в Австралии норм. Главный аргумент в пользу приобретения устройств hands free – желание обезопасить себя в дороге. Однако данных, подтверждающих, что системы hands free – это своего рода панацея, не хватает. Анализ, на который ссылается один медицинский журнал, показал, что главным фактором, приводящим к ДТП, является не держание мобильного телефона в руке, а, скорее, отвлечение водителя на разговоры. Отвлечение водителя на набор номера абонента не намного опаснее отвлечения на настройку автомагнитолы или на разговоры с пассажирами. Очевидно, есть определенные ситуации, когда hands free может выручать водителя. Например, иногда водитель старается крепче держать телефон, чем рулевое колесо, потому что он часто выпадает из рук в ответственный момент телефонного разговора.

Не меньшую опасность представляют сотовые телефоны и для авиаторов. Нет необходимости объяснять, что может произойти с самолетом при сбое в работе навигационной системы или при внезапном отказе системы автопилотирования из-за работы сотового телефона.

Однако, согласно исследованиям, проведенным производителями самолетов Boeing и Airbus, а также Американской (American Federal Aviation Authority) и Британской (Britain's Civil Aviation Authority) службами гражданской авиации, запрет на использование мобильных телефонов в самолетах не имеет под собой никаких научных обоснований. Исследования, приведенные компанией Boeing еще в 1995 году, показали, что 20 мобильных телефонов, работавших в салоне самолета Боинг-737, не создали каких-либо радиопомех. Аналогичные исследования проводила и компания Airbus. Проведенные в 1996–2000 годах исследования 70 000 отчетов экипажей воздушных судов о возникавших в полете проблемах, не выявило ни одного случая, связанного с использованием мобильных телефонов.

И все же, несмотря на эти исследования, занимающиеся расследованием крушения пассажирского самолета в Швейцарии в январе 2000 года специалисты утверждают, что наиболее вероятной причиной катастрофы был мобильный телефон. К тому же пилоты жалуются на внезапные изменения работы электронной системы самолета, если кто-либо из пассажиров звонит по такому телефону. Уже несколько раз мобильный телефон становился причиной чрезвычайных ситуаций, приводивших к аварийным посадкам. Поэтому ни одна авиакомпания мира не разрешает пользоваться сотовым

телефоном на борту своих самолетов. Впрочем, некоторые изменения все же происходят. В частности, компания American Airlines разрешила пассажирам использовать портативные электронные устройства, включая сотовые телефоны и двухсторонние пейджеры, пока самолет находится на парковке во время посадки и высадки пассажиров, а также во время задержек, когда самолет стоит на взлетном поле без движения. Всякий раз командир воздушного корабля объявляет, когда можно и когда нельзя использовать радиооборудование. Во время полета пассажиры могут использовать телефоны AT&T, которыми оборудованы самолеты этой компании.

Итак, относительно опасности влияния мобильных телефонов на здоровье человека существуют разные мнения. Одни доказывают, что при использовании таких телефонов повышается риск онкологических заболеваний, другие – что «мобильники» безвредны и, даже наоборот, способствуют сокращению времени реакции человека на внешние события. Не исключено, что и те и другие заявления имеют под собой некоторую экономическую заинтересованность. Те, кто опасается за свое здоровье, могут воспользоваться одним из средств защиты от электромагнитных излучений наиболее уязвимого органа – головного мозга. На рынке аксессуаров сотовой связи представлены в настоящее время различные защитные покрытия, составы и электронные приборы, которые, судя по их рекламным описаниям, позволяют уменьшать или рассеивать электромагнитное излучение радиотелефона, не влияя на качество связи. Многие из них вызывают у специалистов только улыбку, другие – сомнения. Пока нет ни одного защитного устройства, признанного производителями мобильных телефонов. Если бы появилось такое устройство, которое, не влияя на качество связи и электрическую емкость батареи, действительно сводило бы к минимуму вредное излучение, то компании-производители мобильных телефонов, скорее всего, приобрели бы право на использование этой технологии и сделали бы такое устройство частью телефона.

Поскольку единого мнения, вреден или нет мобильный телефон нет, а также неизвестно, эффективны ли предлагаемые средства защиты от электромагнитных излучений, то вопросы о том, защищаться или нет, решать только Вам самим. Воспользуйтесь такими рекомендациями:

★ аналоговым стандартам и телефонам предпочитайте цифровые, их излучение в 4–8 раз меньше;

★ чем меньше мощность сотового телефона, тем он безопаснее;

★ более глубоко проникает в человеческие ткани низкочастотное излучение;

★ при покупке сотового телефона требуйте копию его гигиенического сертификата;

★ не покупайте сотовый телефон детям, у них еще не окрепли нервная и иммунная системы;

★ старайтесь не пользоваться сотовым телефоном во время беременности.

Яковенко А. В.

Защита и безопасность информации в сетях мобильной связи

В рассматриваемом стандарте под безопасностью понимается исключение несанкционированного использования системы и обеспечение секретности переговоров абонентов. Для выполнения этих требований в стандарте GSM предусмотрены:

★ аутентификация,

★ секретность передачи данных,

★ секретность абонента,

★ секретность направления вызова.

Защита сигналов управления и данных пользователя осуществляется только при передаче по радиоканалу. В стандарте используется алгоритм шифрования с открытым ключом RSA (первые буквы фамилий авторов Rivest, Shamir, Adleman), который обеспечивает высокую степень безопасности передачи речевых сообщений.

Для исключения несанкционированного использования ресурсов системы связи в стандарт введены и определены механизмы аутентификации – удостоверения личности абонента. Как уже отмечалось, каждый абонент на время пользования системой получает стандартный модуль подлинности абонента – SIM-карту, которая содержит:

★ международный идентификационный номер подвижного абонента IMSI,

★ свой индивидуальный ключ аутентификации Ki,

★ алгоритм аутентификации A3.

Для обеспечения секретности передаваемой по радиоканалу информации ее зашифровывают. Алгоритм формирования ключей шифрования A8 хранится в SIM-карте. Одновременно с вычислением отклика SRES, аппаратура подвижной станции определяет и ключ шифрования Kc. Этот ключ не передается по радиоканалу, а вычисляется сетью и абонентским терминалом одновременно.

Вместе со случайным числом, подвижной станции посылается числовая последовательность, содержащая ключ шифрования. Это число связано с действительным значением Kc и позволяет избежать формирования неправильного ключа. Число хранится в подвижной станции и содержится в каждом первом сообщении, передаваемом в сеть.

Для установки режима шифрования сеть передает подвижной станции команд CMC (Ciphering Mode Command), после принятия которой станция, используя имеющийся у нее ключ, приступает к шифрованию и дешифрованию сообщений. Поток передаваемых данных шифруют бит за битом поточным шифром, используя алгоритм шифрования A5 и ключ Kc.

Для исключения выявления абонента путем перехвата сообщений, передаваемых по радиоканалу, каждому абоненту системы сотовой связи присваивается временный международный идентификационный номер пользователя – TMSI (Time Mobile Subscriber Identity), который действителен только в пределах зоны обслуживания с идентификационным номером LAI (Location Area Identification). В другой зоне обслуживания абоненту присваивается новый TMSI. Если подвижная станция переходит в новую зону обслуживания, то ее TMSI должен передаваться вместе с LAI той зоны, в которой TMSI был присвоен абоненту.

При выполнении процедуры корректировки местоположения по каналам управления осуществляется двухсторонний обмен между подвижной станцией MS и базовой станцией BTS служебными сообщениями, содержащими временные номера пользователей TMSI. В этом случае, в радиоканале необходимо обеспечить секретность смены TMSI и их принадлежность конкретному абоненту.

Рассмотрим случай корректировки местоположения в момент эстафетной передачи. В этом случае, подвижная станция уже зарегистрирована в регистре перемещения VLR с временным номером TMSI, соответствующим TMSI прежней зоны обслуживания. При входе абонента в новую зону осуществляется процедура опознавания, которая проводится по старому, зашифрованному в радиоканале TMS1, передаваемому одновременно с номером LAI зоны обслуживания. Последний дает информацию центру коммутации и центру управления о направлении перемещения подвижной станции и позволяет запросить прежнюю зону расположения о статусе абонента и его данные, исключив обмен этими служебными сообщениями по радиоканалам управления. При этом по каналу связи сообщение передается как зашифрованный информационный текст с прерыванием сообщения в процессе эстафетной передачи на 100–150 мс.

Яковенко А. В.

«Скрытый» сервис городских АТС

Современные городские телефонные станции (ГТС) обладают широким спектром дополнительных видов обслуживания (ДВО), о которых абонентам обычно не известно. В данной статье я попытаюсь кратко осветить эти возможности и те преимущества, которые абонент приобретает с их использованием.

Краткое описание ДВО

1. Безусловная переадресация.

Данная услуга позволяет абоненту автоматически переадресовывать все его входящие вызовы на другой номер, который он запрограммировал при включении услуги. Исходящие вызовы осуществляются в обычном порядке, при этом перед непрерывным тональным сигналом приглашения к набору номера абонент слышит специальный уведомляющий тон.

2. Переадресация входящего вызова в случае занятости абонента.

Данная услуга позволяет абоненту автоматически переадресовывать входящие вызовы с его номера, если он в данный момент занят, на другой номер, который абонент запрограммировал при включении услуги. Исходящие вызовы осуществляются в обычном порядке, при этом перед непрерывным тональным сигналом приглашения к набору номера абонент слышит специальный уведомляющий тон.

3. Переадресация входящего вызова при не отвечающем абоненте.

Данная услуга позволяет абоненту автоматически переадресовывать входящие вызовы с его номера, если он не отвечает на вызов, на другой номер, который он запрограммировал при включении услуги. Количество посылок вызова до переадресации согласовывается с оператором АТС при регистрации услуги и может быть от 2 до 10. Исходящие вызовы осуществляются в обычном порядке, при этом перед непрерывным тональным сигналом приглашения к набору номера абонент слышит специальный уведомляющий тон.

4. Передача вызова на автоинформатор.

Данная услуга позволяет абоненту, который не может отвечать на входящие вызовы в связи с отсутствием, переадресовывать такие вызовы на автоинформатор АТС, дающий соответствующую голосовую информацию («Вызываемый Вами абонент временно отсутствует»). Исходящие вызовы осуществляются в обычном порядке, при этом перед непрерывным тональным сигналом приглашения к набору номера абонент слышит специальный уведомляющий тон.

5. Переадресация входящих вызовов.

Данная услуга позволяет перенаправить вызовы, адресованные на занятую линию одного из членов бизнес-группы (линии с серийным исканием), на одну из свободных линий других членов той же бизнес-группы. Обычно многолинейной бизнес-группе присваивается так называемый «пилотный» абонентский номер. Присвоение абонентских номеров другим линиям группы не требуется, но допускается. В этом случае звонить можно как на «пилотный» номер, так и на личные абонентские номера отдельных членов группы. Существует две разновидности данной услуги: «с проскальзыванием» и «без проскальзывания». Услуга «с проскальзыванием» позволяет осуществлять перенаправление при вызове занятого личного номера отдельного члена группы на свободные номера других членов группы. Услуга «без проскальзывания» такого перенаправления не позволяет.

6. Удержание вызова.

Данная услуга позволяет абоненту повторить набор ранее набиравшегося занятого номера путем простого снятия трубки. Услуга включается только при получении сигнала «Занято» от вызываемого абонента после кратковременного нажатия на рычаг отбоя (или клавишу «Flash»). При поднятии трубки через 4 секунды вызываемому абоненту поступает вызов. Если услугу не отменять, то каждый раз после поднятия трубки абоненту будет поступать вызывной сигнал.

7. Временный запрет входящей связи.

Данная услуга позволяет абоненту, который не хочет, чтобы его беспокоили, переадресовывать свои входящие вызовы на автоинформатор АТС, дающий соответствующую голосовую информацию («Вызываемый Вами абонент просил не беспокоить»). Исходящие вызовы осуществляются в обычном порядке, при этом перед непрерывным тональным сигналом приглашения к набору номера абонент слышит специальный уведомляющий тон.

8. Уведомление о поступлении нового вызова.

Данная услуга позволяет абоненту принять новый вызов в процессе уже ведущегося разговора. Переключение между вызовами производится абонентом путем кратковременного нажатия на рычаг отбоя (клавишу «Flash»). Абонент, с которым разговор в данный момент не ведется, находится в режиме удержания («Hold») и слышит специальный тональный сигнал ожидания вызова.

9. Конференц-связь.

Данная услуга позволяет абоненту организовать трехстороннюю связь без помощи оператора. Порядок установления конференц-связи (услуга зарегистрирована для абонента А):

★ абонент А набирает номер абонента В, абоненты А и В разговаривают; абонент А кратковременно нажимает на рычаг отбоя (клавишу «Flash»);

★ абонент А слышит непрерывный тональный сигнал приглашения к набору номера; абонент В слышит тональный сигнал ожидания;

★ абонент А набирает номер абонента С; абоненты А и С разговаривают;

★ абонент А кратковременно нажимает на рычаг отбоя (клавишу «Flash») и затем на клавишу «3»;

★ абоненты А, В и С разговаривают между собой;

★ абонент А кратковременно нажимает на рычаг отбоя (клавишу «Flash») и затем на клавишу «2»; абоненты А и В разговаривают между собой, абонент С слышит тональный сигнал ожидания;

★ абонент А кратковременно нажимает на рычаг отбоя (клавишу «Flash») и затем на клавишу «1»;

★ абоненты А и В разговаривают между собой, абонент С слышит тональный сигнал «Занято».

10. Сокращенный набор номера.

Данная услуга позволяет абоненту делать вызовы путем набора коротких кодовых комбинаций вместо полных телефонных номеров. Абонент может хранить в памяти АТС определенные телефонные номера, каждому из которых соответствует сокращенный номер (номер ячейки памяти). Количество ячеек памяти для хранения номеров согласовывается с оператором АТС при регистрации услуги и может быть 8 или 20. Нумерация для 8 ячеек памяти – 10:17, для 20 ячеек памяти – 10:29.

11. Соединение без набора номера.

Данная услуга позволяет абоненту делать телефонный вызов без набора номера. Когда абонент снимает трубку и не делает попытки нормального набора номера в течение 4 секунд, АТС автоматически набирает номер, запрограмированный абонентом при включении услуги.

12. Будильник.

Данная услуга позволяет абоненту заказать автоматический оповещающий вызов АТС на свой номер в то время, которое он запрограммировал при включении услуги. Когда наступает заданное время, абоненту поступает автоматический вызов с голосовым уведомлением от автоинформатора АТС («Вы просили напомнить о времени»). Если абонент не отвечает на этот вызов, через 4 минуты вызов будет повторен. Если абонент снова не отвечает на вызов, оператору АТС будет выдано сообщение «Абонент не отвечает». Если

ДВО для телефонов с тональным набором номера

Наименование услуги	Код включения	Код проверки	Код выключения
Безусловная переадресация	*21*XXXXX#	*#21*XXXXX# или *#21#	#21#
Переадресация входящего вызова в случае занятости абонента	*22*XXXXX#	*#22*XXXXX# или*#22#	#22#
Переадресация входящего вызова при не-отвечающем абоненте	*61*XXXXX#	*#61*XXXXX# или*#61#	#61#
Передача вызова на автоинформатор	*23#	*#23#	#23#
Переадресация входящих вызовов	Не нужен	Проверка не предусмотрена	Не нужен
Удержание вызова	*27#	*#27*XXXXX# или*#27#	#27#
Временный запрет входящей связи	*35*	*#35#	#35#
Уведомление о поступлении нового вызова	*43#	*#43#	#43#
Конференц-связь	Не нужен	Проверка не предусмотрена	Не нужен
Сокращенный набор номера	*51*NN*XXXXX#	Использование услуги: набрать:**NN	#51*NN#
Соединение без набора номера	*52*XXXXX#	*#52*XXXXX#	#52#
Будильник	*55*HHMM#	*#52*XXXXX# или *#55#	#55*HHMM или #55#
Временный запрет исходящей связи	*31*AAAA*RC#	*#31#	#31*AAAA#
Установка вызова на ожидание	*26#	Проверка не предусмотрена	#26#

линия абонента занята, автоматический вызов будет повторен через 4 минуты. Если линия абонента снова занята, оператору АТС будет выдано сообщение «Линия абонента занята». Время задается в формате ЧАСЫ (00:23) + МИНУТЫ (00:55) с дискретностью 5 минут. Допускается одновременная установка до 3 оповещающих вызовов.

13. Временный запрет исходящей связи.

Данная услуга позволяет абоненту запретить все или определенные виды исходящих вызовов со своего телефонного аппарата (в зависимости от вводимого двузначного кода вида запрета RC). Для инициализации и отмены услуги требуется личный 4-значный код абонента, который назначается по согласованию с оператором АТС и обязательно должен быть зарегистрирован. При попытке осуществления запрещенного исходящего вызова абонент будет постоянно слышать сигнал «Занято». Входящие вызовы осуществляются в обычном порядке. Типовые значения двузначного кода вида запрета RC:

★ 01 – запрещены все исходящие вызовы;

★ 03 – запрещены исходящие междугородние и международные вызовы.

14. Установка вызова на ожидание.

Данная услуга позволяет вызывающему абоненту автоматически получить обратный вызов от вызываемого им занятого абонента после того, как линия вызываемого абонента освобождается. Услуга включается только при получении сигнала «Занято» от вызываемого абонента после кратковременного нажатия на рычаг отбоя (или клавишу «Flash»). После того, как услуга будет активизирована, необходимо положить трубку. Когда вызываемый абонент освобождается, вызов от АТС поступает вызывающему абоненту. После того, как он снимает трубку, вызов от АТС поступает на аппарат вызываемого абонента.

15. Обратный вызов.

Автоматическое установление соединения к занятому вызываемому абоненту после его освобождения.

16. Наведение справки во время разговора.

Установление соединения с другим (справочным) абонентом без разрушения первоначального соединения.

17. Уведомляющий исходящий вызов.

Посылка специального сигнала уведомления занятому абоненту о поступлении к нему входящего вызова.

ДВО для телефонов с импульсным набором номера

Наимено вание услуги	Код включения	Код выключения
Безусловная переадресация	172XXXXX	173
Переадресация входящего вызова в случае занятости абонента	184XXXXX	185
Переадресация входящего вызова при неотвечающем абоненте	186XXXXX	187
Передача вызова на автоинформатор	176	177
Переадресация входящих вызовов	Не нужен	
Удержание вызова	188	189
Временный запрет входящей связи	178	179
Уведомление о поступлении нового вызова	174	175
Конференц-связь	Не нужен	
Сокращенный набор номера	Для абонентов с DP услуга не предоставляется	
Соединение без набора номера	170XXXXX	171
Будильник	180HHMM	181HHMM
Временный запрет исходящей связи	Для абонентов с DP услуга не предоставляется	
Установка вызова на ожидание	182	183

В таблицах приведены некоторые коды включения услуг (на каждой конкретной АТС коды могут отличаться).

Примечания:

1. Каждый вид ДВО для конкретного абонента должен быть предварительно зарегистрирован (введен оператором в базу данных АТС).

2. Успешные включения, подтверждение и выключение каждой из перечисленных услуг сопровождаются специальным уведомляющим тональным сигналом АТС.

3. XXXXX – номер, на который производится переадресация или номер, заносимый в ячейку памяти АТС.

4. NN – двузначный номер ячейки памяти номера в АТС (от 10 до 17 (запоминается 8 номеров) или от 10 до 29 (запоминается 20 номеров)).

5. AAAA – личный 4-значный код абонента (назначается по согласованию с оператором АТС, обязательно должен быть зарегистрирован).

6. RC – двузначный код вида запрета исходящего вызова.

7. HHMM – время побудки в часах и минутах (HH 00...23, MM 00...59, например, 0600).

Яковенко А. В.

НОВОСТИ

Германия: многофункциональный «офисный» мобильник стандарта 3G - уже летом!

Компания T-Mobile на пресс-конференции в Бонне представила новую совместную с Microsoft разработку - телефон MDA IV, первый телефон для сетей стандарта 3G, способный читать и редактировать документы, созданные офисными приложениями MS Excell, Word и т.п.

Среди прочих возможностей новинки - возможность синхронизировать почтовую программу с Outlook на настольном ПК. Примечательно также, что операционная система, под управлением которой работает MDA IV, не Windows Smartphone, как можно было ожидать, а Windows Mobile PC. Обладая стандартным расположением букв на клавиатуре, устройство способно составить серьезную конкуренцию КПК и смартфонам, к числу последних, кстати, его и можно отнести. Тем более что «сердцем» системы является 520 МГц процессор Intel.

Располагая двумя видеокамерами, устройство позволяет как проводить конференц-связь, так и работать в режиме видеотелефона! Новинка, как ожидается, будет доступна в свободной продаже уже этим летом, цена пока не разглашается.

Proext

Система записи Quadra

DVR (digital video recorder) Quadra - это революционная система записи и контроля изображения пришедшая на смену аналоговым системам.

Quadra не использует системный блок компьютера, а является самостоятельным устройством с функциями контроля и управления. Она позволяет проводить мониторинг и автоматическую запись изображения как каждого экрана так и мультиэкрана с разрешением 320 x 240 и 640 x 480. Для управления используются кнопки на лицевой панели. Функционально управление аналогично бытовому видеомагнитофону.
Система поддерживает передачу данных по сетям 10BaseT, RS-232.
Новая модель этой серии поддерживает запись в реальном масштабе времени четырёх изображений с видеокамер и четырёх звуковых дорожек. Записанную информацию можно оперативно записать на CD-RW находящийся на борту системы. Алгоритм записи MPEG4.

Сводные функции системы

★ Монитор системы – одна или четыре камеры.
★ Вход камеры – BNC.
★ Выход – 1 BNC, 1 SVHS.
★ Скорость просмотра – 100 кадров / сек.
★ Скорость записи – 100 кадров / сек.
★ Разрешение – 320 x 240, 640 x 480.
★ Метод компрессии – MPEG4, JPEG.
★ Размер кадра – 0,1–30 кВ.
★ Режим записи – непрерывный, детектор движения,сенсор, таймер.
★ Звук – 1, 4.
★ Жёсткий диск – max 200 Gb.
★ Сеть – да

Коммерческое предложение на поставку систем наблюдения. Поставщик – официальный представитель фирмы Vixell на Украины.

Децентрализованная цифровая система видеонаблюдения

За счет децентрализации всей системы видеонаблюдения служба охраны может избежать бесполезного использования сетевых ресурсов и неудобств, возникающих из-за ограниченной пропускной способности сети. Главным интеллектуальным узлом представляемой цифровой системы видеонаблюдения на объекте является сетевой цифровой видео регистратор Quadra II. К нему можно подключить 1–4 аналоговые видеокамеры, установленные в банкомате. Информация с видеокамер сжимается MPEG компрессором видеорегистратора и записывается на его жесткий диск. Запись может осуществляться в нескольких режимах: непрерывно, по детектору движения, запись событий / тревожных ситуаций, ручная или по графику, со скоростью до 25 кадр / секунду на каждую видеокамеру.
Видеорегистратор имеет все необходимые компоненты для записи и просмотра видео по сети: центральный процессор, Ethernet интерфейс, контроллеры памяти, интерфейсы устройств, MPEG компрессор, место для установки жесткого диска.
За счёт использования конструкции со съёмным диском и наличия программы DVR_reader, можно просматривать записанные события на любом PC использующем ОС Windows.
Архив событий записанных видео регистратором составляет 1–3 месяца в зависимости от настроек. Все изменения настроек защищены двойным паролем.

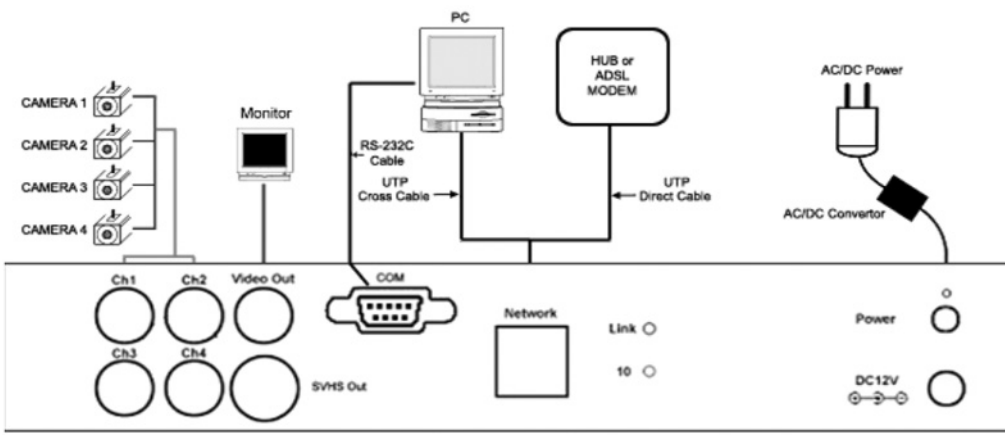
Цифровая видео система DVR Quadra

Система выполняет следующие операции:
★ Оперативный контроль за объектом четырьмя видеокамерами с последующей записью на HDD (до 200 Gb).

★ Использовать сменный HDD и просматривать его на любом другом компьютере с помощью программы просмотра входящей в комплект поставки.
★ Удалённый просмотр видеоизображений, записанных в архив через сеть.
★ Выполнять активацию системы за 5 секунд.

Система не использует операционные системы Windows и др., поэтому нет необходимости покупать лицензионный продукт.
Алгоритм компрессии изображения позволяет записывать фрагмент (кадр) размером от 5 Кб до 30 Кб.
Наличие встроенного детектора движения позволяет настроить, отдельно по каждой камере, запись и сжатия картинки, что позволит вести оперативную запись событий на HDD 40 Гб – 5(пять) суток, при этом скорость отображения информации на дисплее 100 кад / с, скорость записи 100 кад / 4 канала.
Система позволяет использовать цветные и черно-белые SVHS видеокамеры.

Работа с системой проста, так же как с бытовым видеомагнитофоном.
Управлять системой можно дистанционно используя радиоканал (Включение / выключении записи).
Каждое действие и событие, происходящие с системой протоколируются. Вход в систему защищён паролем.



ООО «ТАЛ» Украина
г. Донецк 83122
ул. Артёма ,142
Тел. (062) 345-93-92
E-mail tal@telenet.dn.ua
Тарасевич
Андрей Леонидович

Улучшение качества видеоизображения при неблагоприятных погодных условиях

Компания Dmist Technologies Ltd выпустила новый видеопродукт: устройство ClearVue способно восстанавливать качество видеоизображений, ухудшенное неблагоприятными погодными условиями.

Система ClearVue автоматически корректирует видеопотоки, которые подверглись влиянию таких факторов окружающей среды, как дымка, туман или водяные брызги, восстанавливая исходную четкость, чистоту и точность цветопередачи. ClearVue использует подобный процесс для восстановления полной чистоты цветопередачи видео, съемки которого производились в условиях низкой освещенности. Данную патентованную технологию можно применять как в реальном времени по мере захвата видеокадров, так и при работе с видеопленкой или DVD с уже имеющейся на них записью.

Способность захватывать качественное видео в условиях, при которых обычные системы были бы бесполезными, предлагает реальные преимущества практически всем операторам видеонаблюдения и также демонстрирует значительные преимущества с точки зрения экономии по сравнению с более дорогими вариантами.

Сферы применения данной системы включают:

★ Системы безопасности и защиты аэропортов и морских портов.
★ Контроль дорожного движения.
★ Внестудийная видеосъемка и репортажи с места события.
★ Системы охранного видеонаблюдения.
★ Подводные исследования.
★ Поисковые и спасательные работы.
★ Оборонные объекты.
★ В составе авиационных навигационных систем.

Купольная телекамера UltraView с новой технологией широкого динамического диапазона Xposure

Компания GE Infrastructure Security объявила о начале выпуска новой купольной телекамеры UltraView с широким динамическим диапазоном, в которой применяется новая передовая технология компании GE – Xposure, с помощью которой производится независимая обработка каждого отдельного пикселя каждого кадра.

Телекамера UltraView от GE использует новую технологию широкого динамического диапазона Xposure. Помещенная в компактный 5-дюймовый алюминиевый корпус с ударопрочным куполом из поликарбоната, эта новая телекамера позволяет производить захват четких, детальных изображений в самых неблагоприятных условиях.

Купольная телекамера Ultra View обеспечивает наивысшее качество картинки

даже в условиях низкой освещенности. Технология Xposure увеличивает экспозицию при съемке на затененных участках и уменьшает экспозицию на участках с ярким освещением, что позволяет получать изображения с коррекцией света, где четко различаются все важные детали. Даже в рамках одного и того же изображения производится настройка с учетом различных условий освещенности.

В связи с тем, что пользователи ожидают появления телекамер, изготовленных на основе все более сложных технологий, позволяющих получить еще лучшее качество изображения и повышенные функциональные возможности, компания продолжает вкладывать значительные инвестиции в усовершенствование телекамер, отметил Даррен Николсон (Darren Nicholson), вице-президент по маркетингу. К примеру, данный продукт совмещает в себе надежность линии телекамер с широким динамическим диапазоном UltraView с популярным купольным корпусом – прочным и одновременно элегантным и неброским.

Когда данные телекамеры устанавливаются в вестибюлях учреждений, пользователи могут видеть четкие изображения лиц людей, входящих в здание, даже если полуденное солнце или яркие отражения светят прямо в камеру. Кроме того, пользователи могут дополнительно вести наблюдение за автомобилями и объектами, находящимися на парковке. Телекамеры UltraView с широким динамическим диапазоном особенно подходят также для захвата изображений лиц у уличных банкоматов.

Новая купольная телекамера GE UltraView Dome будет доступна широкому кругу пользователей с января 2005 г.

Новые телекамеры LX300 для нуждающихся в высокой степени безопасности

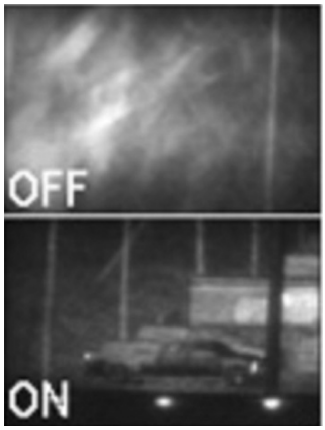
Компания Extreme CCTV Inc объявила о подписании соглашения с Obzerv Technologies о совместной разработке телекамеры нового поколения для целей видеонаблюдения, которая способна будет эффективно функционировать при тумане, дымке, дожде, снеге, обеспечивая при этом разрешающую способность, превышающую разрешение обычных приборов ночного видения.

Новая телекамера марки LX300 разрабатывается для государственных и коммерческих объектов, нуждающихся в высокой степени безопасности. Появление телекамеры LX300 создает новую категорию продуктов на рынке оборудования систем безопасности. LX300 включает лицензионные

технологии селекции цели по дальности компании Obzerv, а также защищенную патентом систему микроколлимированного лазерного диода, которая называется DALIS. Используя DALIS для ночного освещения, телекамера LX300 применяет световые импульсы ближней инфракрасной части спектра для освещения целей, расположенных в отдалении до 300 метров, при ненастных погодных условиях, таких как дождь, снег, туман и дымка. Усиленная ПЗС-телекамера захватывает видео-изображения с высоким разрешением в условиях, которые для обычных телекамер являются невозможными для ведения съемки. Телекамера LX300 эффективно интегрируется со стандартными устройствами дистанционного управления, а также современным радиолокационным оборудованием для отслеживания цели и операций дистанционного управления.

В индустрии безопасности чаще всего используются камеры тепловидения для целей ночного видения дальнего действия. Однако, ввиду того, что функционирование телекамер тепловидения полностью основано на разнице температур, с их помощью нельзя получить ни изображения с идентифицирующей разметкой и символами, ни изображения, которые могут приняты в качестве доказательства в суде. В противоположность этому, активное инфракрасное ночное видение, используе-

мой телекамерой LX300 обеспечивает видеонаблюдение с высокой степенью разрешения, и позволяет получать эффективные изображения с идентифицирующей разметкой и символами. Способность данной те-



лекамеры, применяющей импульсы ближней инфракрасной части спектра, показывать буквы и отметки на больших расстояниях, уже привлекла внимание специалистов отрасли обеспечения безопасности.

Она была специально разработана так, чтобы специалисты-системотехники смогли эффективно интегрировать LX300 в составе систем, обеспечивающих высокий уровень безопасности в портах, гаванях, водных объектах и критически важных объектах жизнеобеспечения и инфраструктуры, расположенных в стратегических зонах.

Коммерческие образцы телекамеры LX300 будут выпущены к концу 2005 года.

Безпроводное мобильное видеонаблюдение

Компания Aegison Corporation, находящаяся в г. Санта-Клара, является ведущим мировым поставщиком мобильных систем видеонаблюдения с возмож-

ностью подключения к широкополосным IP-сетям. Недавно она представила новейшие цифровые радиопередатчики – аппараты серии DWT100.

Аппарат DWT100, работающий совместно с мобильным цифровым видеорегистратором серии DV6010, позволяет пользователям в режиме реального времени передавать информацию на тысячи километров. Таким образом, компания Aegison стала единственной фирмой, которая предоставила цифровой видеорегистратор с полноценной частотой смены кадров и возможностью полноценного безпроводного видеонаблюдения.

Аппарат DWT100-G оснащен встроенным модулем GPS и GPRS-модемом, который позволяет обнаруживать и поддерживать трехдиапазонную сеть GSM по всему миру. Он имеет также встроенный коммутатор Ethernet, обеспечивающий скоростную передачу данных из мобильного цифрового видеорегистратора Aegison. В транспортном средстве с цифровым видеорегистратором Aegison DV6010 аппарат DWT100-G просто подключается к порту Ethernet и в режиме реального времени отправляет видеоизображение по сети GPRS к конечному пользователю. Просмотр отправленного видеоизображения возможен с помощью подключенного к сети компьютера и даже с помощью мобильного телефона. При автономной работе аппарата DWT100-G конечным пользователям периодически доставляется информация GPS, что позво-

ляет пользователям определять местоположение своих передвижных аппаратов.

Новый аппарат позволяет без проводной связи наблюдать за происходящим за много километров, немедленно, в режиме реального времени принимая решения. Можно предполагать эффективность и управляемость, которой можно достичь везде, где используется централизованная схема управления: перевозка денег, тушение пожаров, полицейское преследование, реагирование на дорожно-транспортные происшествия, и др. Аппарат DWT100-G фирмы Aegison имеет две уникальные функции, которых нет ни в одном другом аналогичном продукте. Во-первых, он имеет собственный центральный процессор и операционную систему реального времени и работает как автономный веб-сервер. Это позволяет ему поддерживать двустороннюю связь в качестве маршрутизатора и обеспечивает возможность удаленной настройки через локальную сеть. Другая функция – так называемая «адаптивная полоса пропускания», которая позволяет пользователям непрерывно получать видеоизображение от удаленного цифрового видеорегистратора даже при плохом соединении GPRS.

Скоро компания Aegison планирует выпустить особый продукт для сервера базы данных, предназначенный для резервного сохранения видеоизображений реального времени и данных GPS, переданных с DWT100-G.

Яковенко А. В.

НОВОСТИ

Начальник управления Харьковской госадминистрации пойман при получении взятки

Милиция и пресс-служба областной администрации сообщили, что при получении взятки задержан начальник одного из управлений обладминистрации и трое сотрудников этого управления.

Уникальность ситуации в том, что о взятке, сумма которой не указывается, почти сразу сообщили госструктуры, которые обычно не торопятся обнародовать информацию, тем более, если речь идет о высокопоставленных чиновниках.

Начальника управления и троих его замов задержали с поличным сотрудники городского отдела по борьбе с экономической преступностью.

По словам правоохранителей, вымогательство взяток в этом управлении - каком именно, правда, тоже не сообщается - носило систематический характер. Сейчас сотрудники отдела по борьбе с экономическими преступлениями собирают доказательства, чтобы подтвердить это.

Медиа-группа "Объектив"

Политика безопасности против перехвата информации около хот-спотов Wi-Fi?

Фальшивые точки доступа, расположенные рядом с настоящими хот-спотами, могут ввести пользователя в заблуждение и перехватить важные конфиденциальные данные.

Исследователи Королевского военного колледжа при университете Крэнфильд сообщили о практической возможности использования подставных базовых станций для перехвата конфиденциальной информации.

Специально сконфигурированные станции-двойники, расположенные рядом с настоящей станцией и передающие более сильный сигнал на ее частоте, могут установить соединение с мобильным клиентом от имени оригинального хот-спота, а ничего не подозревающий пользователь передаст ей свои идентификационные данные для входа в сеть или для совершения онлайновой транзакции.

Профессор университета Крэнфильд Брайан Коллинз (Brian Collins) утверждает, что пользователь может обезопасить себя от подобной уязвимости, если настроит функции защищенного соединения и передачи данных на своем Wi-Fi-устройстве. Однако, по его словам, большинство людей не обременяет себя подобными заботами, предпочитая использовать настройки по умолчанию, которые обычно сконфигурированы в режиме минимальной безопасности. Г-н Коллинз предостерегает бизнесменов от использования Wi-Fi-ноутбуков или других устройств для передачи финансовой информации.

По мере распространения устройств с поддержкой Wi-Fi, растет и количество общественных точек доступа. Ожидается, что к 2008 году количество хот-спотов по всему миру достигнет 200 тыс. В России и странах СНГ насчитывается около 250 хот-спотов. Несмотря на очевидные удобства Wi-Fi для развертывания корпоративных сетей, многие компании не спешат их использовать из-за опасений по поводу безопасности конфиденциальной информации.

CNews

Сторож, который не спит

Официальный представитель компании Pelco (США) в Украине фирма ВАТЕК предлагает продукцию не имеющую аналогов, которую оценили по достоинству во всем мире.

Многолетний опыт ООО «ВАТЕК» в области внедрения и установки систем видеонаблюдения позволяет предложить клиенту продукт, способный удовлетворить все требования по эффективному и длительному контролю за охраняемыми объектами благодаря возможности управлении сложным оборудованием с помощью простого и интуитивно-понятного пользовательского интерфейса. Сегодня рынок предлагает большее количество систем видеонаблюдения, многие из которых вполне адекватно справляются с решением вопросов безопасности объектов. Интеллектуальные системы видеонаблюдения позволяют задействовать именно те функции, которые требуются для каждой конкретной ситуации, обеспечивая необходимую в процессе видеонаблюдения гибкость, избирательность и надежность.

Быстрее, меньше, интеллектуальнее

Системы позиционирования Esprit

Esprit – это высокоэффективная система дистанционного позиционирования со встроенным кожухом и полностью интегрированным приемником, она обеспечивает быструю работу привода и работу с переменной скоростью. Система Esprit устанавливается проще, чем любая другая система дистанционного позиционирования. Разнообразные возможности монтажа значительно упрощенны и сокращены до одного пакета. Имеется широкий выбор комплектов с высокоэффективными телекамерами, оптикой и объективами.

★ Внутренняя проводка кабеля.

★ Система работает при скорости ветра 145 км/ч; она способна выдержать скорость ветра до 209 км/ч.

★ Встроенный многопротокольный приемник-драйвер с кожухом, допускающим панорамирование и наклон.

★ Предустановленное позиционирование, предустановки, несколько режимов сканирования.

★ Встроенный источник питания с креплением.

★ Угол обзора от +33° до -83°;

★ Непрерывный поворот на 360° при панорамировании и многое др.;

★ Возможность установки трансфокаторнных объективов с большим фокусным расстоянием.

Esprit

Серия Spectra III

Малозаметные купольные системы видеонаблюдения

Spectra внутрипотолочная модель

Повсюду – от неблагоприятной среды до лучших офисных зданий, система Spectra прекрасно отвечает вашим потребностям в видеонаблюдении. Эту серию отличает самый широкий спектр возможностей монтажа и типов купольных видеокамер в отрасли. Таким образом, кожухи серии Spectra III можно использовать практически для любого известного приложения высокоскоростных купольных систем, включая:

★ Внутрипотолочные системы для установки в помещении.

★ Системы, устанавливаемые на поверхности в помещении.

★ Подвесные системы для установки в помещении.

★ Внутрипотолочные системы для наружной установки.

★ Подвесные системы для наружной установки.

★ Системы с кожухом из нержавеющей стали для наружной установки в жесткой среде.

★ Прочные антивандальные варианты.

Каждая из четырех пакетов камеры и оптики включает возможности технологии LowLight для обеспечения высокой чувствительности в условиях слабой освещенности. Например, высококлассная модель имеет объектив с 23-кратным оптическим увеличением, формирователь изображения с широким динамическим диапазоном 80X, программируемое обнаружение движения и отключаемый инфрокрастный режекторный фильтр для работы в дневном и ночном режимах.

Полнофункциональный видеорегистратор

На рынке потребители постоянно требуют повышения качества видеоизображений, используемых для защиты людей и имущества, поэтому способность DX8000 записывать изображение в формате 4CIF (720 x 480) означает повышение четкости изображения, что жизненно важно для успеха любой системы охранного телевизионного наблюдения. Более того, все 16 телекамер могут работать в режиме максимальной скорости записи (30 кадров/с) в CIF (320 x 240), что дает в

общей сложности 480 кадров/с. DX8000 также дает возможность выбирать различное качество изображения для каждой телекамеры в отдельности.

Возможности Pelco DX8000:

★ Возможна запись в формате 4CIF (720 x 480).

★ Запись до 480 (NTSC) или 400 (PAL) кадров/с в формате CIF (320 x 240).

★ Несколько дисплеев для прямого просмотра или для воспроизведения в процессе записи.

★ Запись в постоянном режиме, при обнаружении движения, по тревожному сигналу или по заданному графику.

★ Цифровое увеличение изображения при воспроизведении.

★ Запись периодов до обнаружения движения и поступления тревожного сигнала.

★ Экранное управление функциями PTZ (панорамирование, наклона и трансфокации) с возможностью программируемой настройки купольной системы и др.

8 (044)536-08-75, 492-76-00
e-mail: info@vatec.com.ua
www.vatec.com.ua

Досмотровая система RAPISCAN

RAPISCAN 3D20

Досмотр на контрольно-пропускных пунктах является напряженной работой, и требования к персоналу по безопасности определять объекты угрозы также

Rapiscan 3D20

являются суровыми. Учитывая внимание к деталям и бдительность, требуемую на протяжении всего рабочего дня, легко понять удар, который сенсорная усталость может нанести на эффективность работы по безопасности. Данные исследований показывают, что уменьшение требований к оператору по обработке информации поможет увеличить вероятность определения и уменьшить сигналы ложной тревоги. Трехмерное изображение предметов уменьшает сенсорные требования к операторам и улучшает работу по надежности досмотра.

3D20 – это единственная система досмотра багажа на контрольно-пропускных пунктах, которая дает возможность операторам в режиме реального времени осматривать в трехмерном пространстве сканируемый багаж с минимальным количеством сигналов ложной тревоги.

Этот новый подход дает более тщательный обзор при досмотре багажа, это больше похоже на обычное видение человека. 3D20 включает в себя современную технологию с запатентованным устройством камеры AXIS-3D R, для обеспечения высокого качества и высокой разрешающей способности рентгеновского изображения. Система оснащена широким спектром увеличения, отбора органических / неорганических материалов и функцией глубокофокусной обработки изображения, которые могут сделать объекты угроз более видимыми. Система также дополняется рядом возможностей, которых нет в обычных рентгеновских платформах, включая способность «подбрасывать» предметы (двигая их с переднего плана на задний и наоборот), и переключать между 3D и 2D изображениями в режиме реального времени.

Когда операторы осматривают багаж в трехмерном пространстве, они могут определить предметы, содержащие угрозу, которые иным способом не могут быть обнаружены.

Опция Threat Image Projection / демонстрация объекта угрозы (TIP) – программа тренировки, которая может быть включена в обычное управление 3D20. TIP позволяет внести объекты угрозы, созданные компьютером, в сканируемый участок и следить за ответом оператора, тем самым позволяя контролировать его действия. TIP был представлен как самый эффективный способ улучшения уровня знаний для персонала, занимающегося досмотром, и он является наиболее предпочтительным методом, используемым контролирующими органами во всем мире.

Rapiscan 620XR

RAPISCAN 620XR

Rapiscan – это Ваш партнер в технологии досмотра багажа на контрольно-пропускных пунктах, а модель 620XR является решением с высоким коэффициентом обнаружения угрозы при самой низкой стоимости.

Модель 620XR является новым образцом досмотровой технике и предназначена для использования в аэропортах, таможнях, зданиях суда, почты и других охраняемых помещениях.

Эргономический дизайн модели 620XR и интеллектуальный пользовательский интерфейс обеспечивают легкость в использовании, здоровье и безопасность операторов. Модульная сборка системы и открывающиеся поворотные панели с легким доступом к ним обеспечивают непревзойденную надежность и удобство в эксплуатации. Новые рентгеновские детекторы и программно-реализованные алгоритмы предоставляют наивысшую степень обнаружения угрозы и классификации материалов по сравнению с обычной рентгеновской системой.

Система также содержит в себе новый алгоритм TARGET(tm), который автоматически опознает объекты потенциальной угрозы – характерные признаки материалов сопоставляются с теми признаками материалов, которые содержат взрывчатку или наркотики.

Компания «ВАТЕК» предлагает свои услуги в сфере обеспечения обьектов комплексами технических средств безопасности разного уровня сложности на базе новейших мировых технологий.

8 (044)536-08-75,
492-76-00
e-mail: info@vatec.com.ua
www.vatec.com.ua

Подбор оборудования для видеообнаружения движения

Техника видеообнаружения движения (VMD) быстро меняет те методы, при помощи которых специалисты в области безопасности используют видео для решения своих профессиональных задач. Термин «обнаружение движения» («motion detection») в той мере, в какой он применим к цифровому видео, не является однозначным и допускает двоякое толкование. Он может относиться к целому диапазону возможностей, начиная с простого обнаружения активности и до ведения поиска в больших базах данных в целях предотвращения серьезных происшествий. Таким образом, если вы намереваетесь применить систему видеообнаружения движения, вам следует принять во внимание множество различных аспектов.

Когда видеоизображение превращается в данные в цифровом формате, информация об изображении становится сохраненной цифровой величиной. Такое цифровое значение меняется по мере того, как меняются видеоизображение и источник информации. Сложные алгоритмы (серия аналитических действий) анализируют меняющиеся цифровые величины для распознавания образов. Некоторые изготовители оборудования называют это анализом видеоконтента. Так как действие этих алгоритмов является функцией программного обеспечения, они программируются в чипы и платы, которые могут быть встроены в телекамеры, автономные модули, цифровые видеорегистраторы и специализированные компьютерные процессоры. Технология видеообнаружения движения доступна также в качестве программного обеспечения для установки на серийно выпускаемых компьютерах.

По сложности данные продукты значительно отличаются друг от друга. В сетевых телекамерах предусматривается отдельный выход для первоначального обнаружения движения, в то время как компьютерное программное обеспечение и модули обеспечивают графическую идентификацию опознанного движения. Пользователем могут выбираться необходимые участки контроля, производится компенсация фонового движения в окружающей среде, а также имеется целый ряд других функциональных возможностей.

Технические возможности систем видеообнаружения движения

Поскольку терминология по видеообнаружению движения не стандартизирована, информация, предоставляемая изготовителем оборудования, иногда бывает более чем краткой. Выбор соответствующего подхода к видеообнаружению движения требует от пользователя понимания имеющихся технических характеристик и возможностей, а понимание, в свою очередь, требует изучения.

Простое обнаружение движения обычно распознает любой тип движения на видеополе. Через выходное устройство затем активируется автоматический вызов к экранам видеомониторов персонала, осуществляющего видеонаблюдение, или же запускается автоматическая запись цифровым видеорегистратором. В настоящее время, видеовызов уже не ограничивается кабельными системами видеонаблюдения, он может быть также передан по сети Интернет или линиям беспроводной связи. Многие стандартные цифровые видеорегистраторы могут производить поиск записей движения или активности, хранящихся на их жестких дисках. Такими функциями часто снабжено серийно выпускаемое оборудование, которое является экономичным и применяется в ограниченных областях. В передовых продуктах видеообнаружения движения концепции стандартного обнаружения усовершенствуются далее и могут, при правильном применении, обеспечивать новые, эффективные решения проблем безопасности. Большинство из этих возможностей появилось благодаря сложным алгоритмам, которые производят поиск детальных схем движения и активируют срабатывание системы только при конкретных условиях. Такие возможности включают:

★ Идентификацию проникновения: распознавание людей, не имеющих права доступа к определенным участкам, расположенным в поле обзора.

★ Коррекцию с учетом фонового движения в окружающей среде: распознавание и игнорирование переносимого ветром мусора, животных, фонового движения транспорта и т. д.

★ Подсчет: распознавание количества движущихся предметов, а также частоты выполненных действий.

★ Идентификацию направления: игнорирование объектов, движущихся в одном направлении, и одновременная подача сигнала относительно объектов, движущихся в направлении участков, доступ к которым запрещен.

★ Распознавание конкретных предметов: активация, когда определенные, указанные пользователем предметы пропадают, или наоборот помещаются в несанкционированном месте, или проносятся через поле обзора.

★ Отслеживание объекта: выделение и сопровождение конкретного человека или предмета по мере того, как они передвигаются в поле обзора, или из поля обзора одной телекамеры в поле обзора другой.

★ Отслеживание нескольких объектов: выделение и сопровождение нескольких людей или объектов, по мере их движения в поле обзора, или из поля обзора одной телекамеры к другой.

Программирование «распознавания конкретных действий» только начинает появляться по результатам экспериментальных разработок. Эта техника обнаружения движения распознает уникальные или сложные движения, связанные с нежелательными действиями или явлениями. Распознаваемые действия могут включать типичное движение магазинных воров, акты физического насилия или такие явления как пожар. Программы видеообнаружения дыма в настоящее время уже имеются на рынке. Также появляются системы, объединяющие в себе обнаружение движения с распознаванием символов и биометрической идентификацией. В недалеком будущем ожидается появление систем, которые будут распознавать номерные знаки или надписи на движущихся автомобилях, дистанционно обрабатывать номера или знаки и активировать соответствующий сигнал в отношении разыскиваемого автомобиля. Кроме этого, найдут свое место на рынке и системы, распознающие лица людей, движущихся в толпе.

Универсальность таких систем продолжает повышаться. Некоторые системы могут теперь быть «обучены» новым функциям посредством настройки на повторяющиеся действия и обычные виды активности. Другие продукты часто обладают способностью адаптации к условиям окружающей обстановки с тем, чтобы не зависеть от воздействия меняющегося освещения или погодных условий.

Практически все оборудование, предоставляющее функции обнаружения движения, может быть настроено в той или иной степени в соответствии со специфическими потребностями конечного пользователя. Посредством программирования можно настроить изменение операционных требований в соответствии со временем дня, полем обзора и изменениями в фоновом движении. Многие многокамерные системы, программируемые пользователем, позволяют производить индивидуальные настройки визуального реагирования или автоматического реагирования на любую распознанную схему движения. Экраны и устройства операторского интерфейса могут обычно модифицироваться с использованием стандартного меню инструментальных средств, имеющегося в каждой операционной системе.

Какие функции системы видеообнаружения движения наиболее подойдут для вашего объекта?

Применение наиболее правильно подобранного оборудования и характеристик обнаружения движения может решить множество сложнейших проблем обеспечения безопасности. Однако прежде чем выбирать оборудование, необходимо сначала тщательно изучить данный вопрос и определиться с тем, ка-

ковы операционные потребности вашего объекта в данном оборудовании.

Руководитель службы безопасности, имеющий хорошее представление об охраняемом объекте, и профессионал-системотехник, хорошо знающий возможности и сферы приложения оборудования, должны начать с того, чтобы задать себе такие важные вопросы: Что и кто может двигаться в пределах объекта? И что мы хотели бы узнать об этом движении? Несмотря на кажущуюся простоту данных вопросов, ответы на них должны быть детальными, точными и полными.

Первоначальной целью является установление того, кто и что может двигаться в пределах охраняемого объекта. Это определит участки наблюдения, которые должны захватывать телекамеры, и позволит начать процесс подбора требующегося оборудования по обнаружению движения. Ответ на вопрос «кто и что может двигаться?» включает как предметы и людей, представляющих непосредственный интерес, так и любые движущиеся фоновые объекты, которые могут отвлекать систему.

Предметами, представляющими особый интерес, могут быть предметы, которые обычно находятся в движении и, вследствие этого, либо проходят через поле обзора, останавливаются в поле обзора, требуют идентификации, либо должны отслеживаться аппаратурой видеонаблюдения. Сюда можно включить следующее:

★ Автомобили, движущиеся через въездные ворота или по предписанным направлениям движения.
★ Обычный приход и уход персонала, имеющего право доступа.
★ Оставленный без присмотра багаж.
★ Личные вещи, переносимые людьми.
★ Подозрительные личности.
★ Методы работы персонала по обработке материальных активов.

И наоборот, причиной беспокойства могут стать предметы, которые обычно неподвижны и не должны никуда передвигаться. Это применяется обычно для защиты особо важного и ценного имущества, или же предметов, которые очень легко сбыть после кражи. Предметом интереса могут быть также необычные обстоятельства или явления, которые характеризуются определенным видом движения. Перечень включает, но не ограничивается следующим:

★ Лица, незаконно проникшие на охраняемый участок или в границы периметра, или же персонал, не имеющий права доступа на такие участки.
★ Утечки и механические повреждения.
★ Дым, пожар или отдельные возгорания.
★ Агрессивное или странное поведение.
★ Движение в направлении, противоположном основному потоку.

Как только руководитель службы безопасности и профессионал-системотехник определили предметы, которые будут представлять особый интерес, они должны определить участки наилучшего захвата изображения и предложить схему расположения оборудования. Чаще всего расположение уже имеющихся телекамер видеонаблюдения представляет удобную исходную позицию, и поэтому модификации расположения могут быть минимальными. В других случаях должна быть предусмотрена совершенно новая схема расположения. Наличие фонового движения и условия окружающей обстановки должны быть главным соображением при подготовке схемы расположения. Как упоминалось ранее, на рынке уже существуют системы, способные отделять фоновое движение и приспосабливаться к изменениям в окружающей обстановке. Однако эти функции не являются стандартными для многих систем обнаружения движения и должны указываться специалистами-системотехниками, если схема расположения требует их наличия.

И наконец, когда сформировалось четкое понимание типов движения, следующим критерием, влияющим на выбор оборудования и проектирование системы, должен быть ответ на вопрос, что следует предпринять, когда регистрируется одно из вышеупомянутых видов движения. Если интересующий объект требует немедленной реакции, то дежурный персонал, ведущий видеонаблюдение, должен получить соответствующее видеоизображение и понять то, что он на нем видит. В большинстве систем видеообнаружения движения предусмотрены такие состояния тревожного сигнала, которые способны захватывать активный монитор. Многие обладают расширенными графическими возможностями, при помощи которых можно выделять интересующее движение. Это представляет огромную ценность при взаимодействии диспетчеров с персоналом, осуществляющим реагирование. Если требуется отслеживание субъекта или объекта, то могут быть задействованы телекамеры на цифровом или механическом поворотном устройстве, или панорамные телекамеры, функционирующие на основе дистанционного управления с процессора обнаружения движения.

Если основной целью видеоматериала является документальное подтверждение для судебного процесса, то изменения поля обзора для вмещения движения должны быть минимальными, и должно быть применено большее количество телекамер для подтверждения событий. Кроме этого, графическое усиление видеообнаружения движения, методы хранения видеоматериала, а также методы сжатия видеосигнала должны быть тщательно продуманы при выборе системы в целях минимизации расхождений. Если распознанное движение требует идентификации или авторизации, то процессор системы обнаружения движения должен иметь возможности взаимодействия со скорректированной базой данных. Иногда это требует интеграции видео с серверами контроля доступа или другими файловыми процессорами. От системы обнаружения движения также может потребоваться быть способной переводить требуемую видеоинформацию в информацию базы данных для сравнения.

Рекомендации

Обширный ассортимент продуктов и множество их возможностей вносят неопределенность при выборе и установке систем обнаружения движения. Единственное, что является несомненным, это то, что данные системы будут продолжать наращивать новые технические возможности применительно к решению проблем обеспечения безопасности. Таким образом, для любой системы видеонаблюдения, которая в данный момент имеет или может иметь в будущем потребность в самом простом оборудовании по обнаружению движения, целесообразно принимать во внимание следующее:

★ Используйте свое воображение. Если вы считаете, что это возможно сделать, вполне вероятно, что это действительно так.
★ Составьте план постоянной модернизации системы и функций, которые она выполняет. Наиболее выгодным может быть постепенное внедрение оборудования систем обнаружения движения.
★ Не следует быть излишне экономным. Серийные продукты хорошо подходят для общих потребностей, в то время как комплексные решения требуют изучения, проектирования и соответствующих денежных вложений.

Хотя сложные решения могут вносить неопределенность, новшества, предлагаемые системами обнаружения движения, создают новый потенциал, обеспечивающий более безопасную и лучше управляемую среду. Поэтому наилучшим средством в работе с данными системами является постоянное пополнение знаний и техническая осведомленность.

При написании статьи использованы материалы сайта www.secnews.ru

Десять причин купить сетевую камеру (о чем не станет говорить поставщик аналоговой телекамеры)

Сетевые камеры существуют уже несколько лет – первая из них была выпущена в 1996 году. Сначала технологии сетевых камер не могли тягаться с аналоговыми телекамерами профессионального уровня. Считалось, что это тип веб-камер для наблюдения за объектами и событиями по сети Интернет или локальной сети. Эти камеры, первоначальным назначением которых была цифровая передача изображений, связь через сеть и Интернет в новых сферах применения, не использовались для видеонаблюдения. Но теперь ситуация сильно изменилась. В течение последнего года сетевые камеры потеснили аналоговые и отвечают теперь тем же требованиям и характеристикам. В некоторых важных областях сетевые телекамеры превосходят по параметрам аналоговые.

Вообще говоря, рассматривая вопрос о переходе к сетям на базе IP-технологий, кроме сравнения двух типов телекамер с точки зрения пользователя, следует иметь в виду еще ряд факторов. К ним относятся как характеристики, так и взаимодействие открытых систем, гибкость, перспективность и связность узлов сети. Однако в этой статье будут рассмотрены десять важнейших функциональных различий между современными сетевыми телекамерами и их аналоговыми сородичами.

★ С проблемами чередования покончено. Аналоговая телекамера при высоком разрешении (4CIF) имеет значительные проблемы с чередованием. Это происходит из-за того, что при аналоговом видеосигнале, даже если он подключен к цифровому видеорегистратору, все изображения состоят из линий, а каждое изображение состоит из двух перекрывающихся полей. Если изображение содержит много движущихся элементов, оно становится размытым. Размытость возникает вследствие смещения предметов между зафиксированными изображениями двух перекрывающихся полей. В сетевых камерах используется технология «последовательной развертки», которая способна более четко фиксировать изображения движущихся предметов. Эта улучшенная технология регистрации изображения означает, что все изображение регистрируется одновременно, благодаря чему кристально четкие изображения получаются даже при высокой степени подвижности.

★ Технология питания по кабелю Ethernet увеличивает экономию и надежность. Подать питание на аналоговую телекамеру всегда было очень трудно и дорого. Благодаря значительной экономии затрат, которую предоставляет стандарт IEEE 802.3af Power over Ethernet (PoE), он оказался довольно удачным. Для аналоговых телекамер такой стандарт не предусмотрен – он предполагает, что сетевые устройства получают питание от коммутатора с функцией PoE или промежуточного усилителя по тому же стандартному кабелю 5-й категории, по которому передаются данные и видеоизображения. Поскольку принят стандарт, все оборудование является совместимым, что максимизирует выгоду для конечного пользователя. В сфере видеонаблюдения стандарт PoE предоставляет еще одно преимущество: возможность оборудования централизованного резервного источника питания для камер в аппаратной. В случае сбоя питания их работа прервана не будет.

★ Разрешающая способность в мегапикселах. Аналоговые телекамеры изготовляются в стандартах NTSC/PAL, и разрешающая способность 4CIF соответствует 0,4 мегапиксела. Современным конечным пользователям, которые располагают новыми компьютерными мониторами и цифровыми телекамерами, нужны большие значения емкости в мегапикселах, это требование они выдвигают и к системам видеонаблюдения. Благодаря высокому разрешению сетевые камеры дают более подробное изображение и покрывают более обширные области. Таким образом, вложение в систему безопасности не пропадет зря – ведь на таком изображении можно разглядеть лицо грабителя и что он выносит. Кроме того, увеличенная разрешающая способность сетевых камер позволяет осуществлять такие функции, как цифровой поворот, наклон и увеличение.

★ Интеллектуализация на уровне камеры. Сейчас в мире осуществляется очень много видеозаписей с целью наблюдения или поиска. Появилось новое течение – интеллектуальное видео. Для выполнения таких требований новейшие сетевые камеры оснащаются функцией обнаружения движения и обработки тревог. Телекамера сама принимает решение, когда посылать видеоизображение, с какой частотой смены кадров и разрешающей способностью, когда выдать сигнал конкретному оператору с целью наблюдения и/или реакции. Кроме того, сетевые камеры оснащаются и интеллектуальными алгоритмами: распознавание номерных знаков, подсчет количества людей и т. п. Наличие интеллектуальных функций на уровне камеры предоставляет намного больше плодотворных и эффективных средств, чем можно было достичь с помощью цифрового видеорегистратора или другой централизованной системы. Сетевая камера решает также другую возникающую проблему: не-хватки вычислительных мощностей для анализа в режиме реального времени большого количества каналов. Сетевые камеры создаются на основе целевого аппаратного обеспечения высокой степени интеграции, которое прекрасно выполняет задачи анализа изображения и тем самым позволяет устанавливать крупные интеллектуальные видеосистемы.

★ Интегрированное управление функциями поворота, наклона и увеличения и ввода/вывода. Для аналоговой телекамеры с функциями поворота, наклона и увеличения (PTZ), кроме видеокабеля, необходим отдельный кабель для последовательного канала управления движением PTZ. Это дорогое и громоздкое решение. Технология, используемая для сетевых камер, позволяет управлять функциями PTZ по той же сети, которая передает видеосигнал. Команды PTZ для сетевой купольной камеры посылаются по IP-сети, что позволяет значительно сократить затраты и достичь повышенной гибкости. Более того, в сетевые камеры могут входить входные и выходные сигналы, например, сигнализация и управление замками. Это позволяет сократить расходы кабеля, средств, и повысить функциональность и возможности интеграции.

★ Интегрированный аудиосигнал. В некоторых применениях повышается значение звукового сигнала. В аналоговой системе передача звука невозможна, разве что в случае прокладки соответствующего кабеля к цифровому видеорегистратору. Сетевая камера решает эту проблему путем регистрации звука самой камерой, синхронизации его с видеосигналом или даже интеграции его в тот же видеопоток и отправить его для наблюдения и/или записи по той же сети. Аудиосвязь может быть полностью двунаправленной, что позволяет собеседникам вести разговор через переговорные устройства. Такие звуковые устройства дешевы и легки в установке – но только при наличии сетевой камеры.

★ Безопасная связь. При использовании аналоговой телекамеры видеосигнал передается по коаксиальному кабелю безо всякого шифрования или аутентификации. Таким образом, кто угодно может подключиться к видеосигналу, или даже хуже – заместить видеосигнал телекамеры другим видеосигналом. Но сетевая камера способна перед отправкой по сети шифровать видеосигнал, что предотвращает просмотр или подмену его посторонними лицами. Систему можно также настроить на аутентификацию соединения с помощью за-

шифрованных сертификатов, воспринимаемых конкретной сетевой камерой, устраняя таким образом возможность, что кто-нибудь вклинится в линию. Сетевая камера способна и добавлять зашифрованные «водяные знаки» в поток видеоданных с информацией об изображении, времени, расположении, пользователях, тревогах и т. д., чтобы обеспечить свидетельство. Предоставляет ли аналоговая телекамера такой высокий уровень функциональности? Ни в коем случае.

★ Гибкий, дешевый выбор инфраструктуры. Аналоговый видеосигнал обычно передается по дорогому коаксиальному или волоконно-оптическому кабелю или же беспроводным способом. Во всех этих способах расстояние влияет на качество изображения. Положение усложняется подводом питания, подачей входных и выходных сигналов и звука. Стандартные системы на базе IP-технологий преодолевают эти препятствия, имея намного меньшую цену и предоставляя намного больше возможностей. Точно так же, как просмотр веб-сайтов возможен из любой точки мира, качество изображения сетевой камеры не ухудшается из-за расстояния. Сетевое IP-соединение является общепринятой, стандартизированной технологией, а это означает сравнительно низкие затраты. В отличие от аналоговых систем, видеопотоки в сети IP можно маршрутизировать по всему миру, используя широкий ряд взаимодействующих вспомогательных устройств. По одному каналу можно передавать множество разнотипных потоков, поскольку он работает по принципу пакетной коммутации. Новые модели подключаются дешевым кабелем 5-й категории, и при использовании 1 ГБ Ethernet по одному каналу могут одновременно передаваться сотни полнокадровых видеопотоков.

★ Истинно цифровое решение. Датчик ПЗС аналоговой телекамеры выдает аналоговый сигнал, который затем оцифровывается на АЦП, что дает возможность улучшения изображения с помощью цифровой обработки сигнала. После этого сигнал снова преобразуется в аналоговую форму и передается по коаксиальному кабелю. И наконец, цифровой видеорегистратор снова оцифровывает сигнал, чтобы записать его. Итого, осуществляется три преобразования, каждое из которых приводит к потере качества изображения. В сетевой камере оцифровка изображения осуществляется один раз, и оно остается цифровым все время – ненужные преобразования, приводящие к ухудшению изображения, отсутствуют.

★ Более низкие эксплуатационные затраты. Логично, что все описанные выше расширенные функции стоят денег. Первоначальная цена сетевой камеры, действительно, может быть выше – для того, кто сравнивает только цены камер. Но сравните затраты на канал – и сетевая камера с ее превосходной гибкостью и характеристиками сразу станет сравнимой с аналоговыми системами, подключенными с видеорегистраторами. Во множестве конфигураций систем авансовые затраты на систему видеонаблюдения на основе сетевых камер даже ниже, чем в аналоговом варианте. Снижение общих затрат на систему на основе сетевых камер в основном происходит за счет серверных приложений и хранения, которые работают на серверах промышленного стандарта на основе открытых систем, а не на фирменном оборудовании, например, на цифровых видеорегистраторах. Это значительно сокращает затраты на обеспечение и оборудование, особенно в больших системах, в которых значительную долю полной стоимости системы занимают емкости записи и серверы. Дополнительная экономия затрат основана на используемой инфраструктуре. IP-сети, такие как Internet или локальные сети, и различные способы соединения, например, беспроводный, можно использовать для других приложений в организации. Они намного дешевле обычных коаксиальных и волоконно-оптических кабелей. Итак, покончено с последним возражением против использования сетевых камер. Чего же еще ждать?

Заключение: Будущее – за сетевыми камерами

Уважаемое аналитическое агентство J.P. Freeman and Co. Inc., прогнозирует, что рынок сетевых камер является наиболее быстро растущим сегментом видеонаблюдения, и в 2008 он превысит объем продаж аналоговых камер. Поскольку управление системами безопасности по IP-сетям приобретает все большую популярность и применение, можно сказать о наступлении новой эпохи в передовом управлении безопасностью. С другой стороны, аналоговым камерам характерна недостаточная гибкость и функциональность, что не соответствует требованиям новой эпохи. Поскольку сетевые камеры берут на себя сбор кадров и интеллектуальные функции цифровых видеорегистраторов, облегчается расширение систем, и заказчики смогут использовать для записи и архивирования изображений выгодные стандартные серверы. Они получат широкий выбор программного обеспечения управления видеозаписью и анализа изображений. Этот переход от фирменных цифровых видеорегистраторов к открытым системам, а также преимущества сети, цифрового изображения и интеллектуальных функций камер станет сильным мотивом для быстрого освоения сетевых камер с их преимуществами.

Яковенко А. В.

НОВОСТИ

«Простая схема» мошенников стоила сотовому оператору Грузии $0,5 млн

Финансовая полиция министерства финансов Грузии возбудила уголовное дело по факту мошенничества в отношении двух граждан Азербайджана, которые, по данным следствия, в результате аферы нанесли грузинской компании мобильной связи «Джеосел» ущерб в размере более 1 миллиона лари (около 555,5 тысяч долларов). Как сообщили в пресс-службе финансовой полиции, по данным следствия, в ноябре 2004 года в Тбилиси двое азербайджанцев вошли в доверие к двум местным жителям - Церетели и Никибишвили - представились бизнесменами и пообещали трудоустроить их в коммерческую фирму.

Затем подозреваемые попросили новых знакомых приобрести для них на свои имена сим-карты «Джеосел» с включенным роумингом. Таким образом, на фамилии Церетели и Никибишвили были приобретены 17 сим-карт, которые через некоторое время через Азербайджан были переправлены, соответственно, в Англию и в Грецию. В период 26-29 ноября 2004 года посредством этих сим-карт были произведены звонки на общую сумму 1 миллион 29 тысяч 930 лари. Поскольку сим-карты были оформлены на подставных лиц, то сумму пришлось полностью покрыть компании «Джеосел».

По данным финансовой полиции Грузии, МВД Азербайджана уже задержало этих мошенников, которые, как выясняется, осуществили подобную аферу и в Азербайджане, а также в ряде европейских стран.

REGNUM

США: «солдаты-роботы» за $200 тыс. в Ираке все равно дешевле, чем живые

США направляют для борьбы с повстанцами в Ираке вооруженных роботов. Первая партия из 18 "механических солдат" направится в Ирак уже нынешней весной. Разработанные американской компанией роботы-солдаты представляют собой модернизацию робота "Талон", который уже используется военными для обезвреживания взрывных устройств.

Новый робот Sword может быть вооружен автоматической винтовкой M249 или M240, при этом обладает повышенной точностью стрельбы. Для наводки на цель и ориентировки на местности он оснащен четырьмя видеокамерами, прибором ночного видения и телеобъективами. Дистанционное управление обеспечивается двумя ручками управления типа "джойстик" и экраном. Как утверждают конструкторы, робот, высота которого составляет около метра, способен преодолевать такие препятствия как камни и колючая проволока

Newsru, BBC

Интеграция СКД «Золотые ворота» с системой безопасности «Интеллект»

Для некоторых фирм январь ознаменовался не только яркими праздничными днями, но для киевских компаний «Габитус» и «Integrated Technical Vision LTD» и успешным сотрудничеством. Ими вначале 2005 года была осуществлена интеграция системы безопасности «Интеллект» с новой отечественной системой контроля доступа «Золотые ворота». Такое объединение имеет очень важное преимущество: каждому событию системы соответствует свое видео. Как распорядится таким мощным оружием решать потребителю, подчеркнем лишь, что особенно эффективна система для предприятий с большим количеством сотрудников (сотни, тысячи людей) и большим количеством помещений с ограниченным доступом.

Система позволяет

★ одновременно контролировать сотни помещений,
★ запоминать информацию обо всех входящих и выходящих,
★ ограничивать доступ в помещения (выходные дни, в определенное время, определенным лицам),
★ контролировать одновременно несколько категорий пользователей,
★ получать сообщения о попытках повреждения считывающего устройства, и при этом блокировать дверь,
★ получать сообщения об открытой двери длительное время,
★ следить за состоянием охранной сигнализации, и при срабатывании датчиков блокировать, или разблокировать (при пожаре) двери.

Эффективным средством обеспечения безопасности предприятий и организаций в рабочие часы является система контроля доступа (СКД). Она создает комфортные условия для работы персонала и позволяет надежно преградить путь лицам, которые не имеют права входить в здание или посещать отдельные его помещения. СКД «Золотые ворота» позволяет выделять отдельные категории персонала, а также учитывать их график работы. Для принятия решения о допуске в помещение система использует идентификаторы в виде проксимити карточек – «бесконтактный ключ» от дверей. Этот ключ несет информацию о своем владельце (Ф.И.О., фото, должность, отдел, смена и др.). База данных СКД позволяет хранить данные карточки (персональные данные о владельце) и о контролируемых помещениях. Примечательно то, что при просмотре архива, например, событий по выбранной двери на мониторе оператора отображаются данные карточки-ключа совместно с соответствующим видеоизображением. Это позволяет получить истинную картину происходящего, и стало доступным лишь благодаря выполненной интеграции перечисленных систем. При этом из системы «Интеллект» наиболее полно задействована видеоподсистема.

Работу с архивом можно вести по следующим факторам:

★ сотрудник (Ф.И.О., должность);
★ помещение (номер или наименование двери);
★ время (промежуток времени).

Также, любая организация может создать себе определенное количество гостевых карточек. Гости обычно имеют право ограниченного прохода, и, если гость воспользуется этой карточкой для входа в другое помещение, система немедленно отреагирует. Это распространяется не только на посетителей предприятия, но и на сотрудников. Реагирует СКД следующим образом: на мониторе оператора немедленно появляется изображение этой двери (или коридора с этой дверью), и сотрудник охраны имеет возможность молниеносно отреагировать. Также, система позволяет выводить сообщения на экран, не только при попытке несанкционированного входа (с заблокированной или утраченной карточкой), но и при др. обстоятельствах, например, повреждение коммуникаций, незакрытая дверь и т. д. Это позволяет оператору, с одной стороны, не тратить время на проверку помещения лично (в случае несущественных событий), и оперативно реагировать в случае крайней необходимости – с другой. Эта функция стала возможной только благодаря задействованной видеоподсистеме комплекса «Интеллект» при интеграции.

Интеграция в систему безопасности «Интеллект» СКД «Золотые ворота» привела к созданию комплекса, который в состоянии решать целый ряд задач по организации системы безопасности объекта охраны, и вместе с этим быть мощной подсистемой комплекса «Интеллект».

ООО «Габитус»
тел./факс: 8(044) 269-35-15,
e-mail: habitus@svitonline.com
http://www.habitus.com.ua

Новости от компании «Габитус»

В продажу поступила новая система видеонаблюдения эконом-класса «SMARTvideo».
Предназначена для обеспечения видеоконтроля небольших организаций, которые не требуют высокой производительности и мощности (такие как небольшие магазины, квартиры, офисы). В состав системы входит 2-х канальная аудиорегистрация, клиентское сетевое рабочее место просмотра и управления телеметрией. Отличается высокой надежностью, простотой в эксплуатации и внедрении, и, самое главное, – доступной ценой.

Телекамера ближнего инфракрасного диапазона с частотой смены кадров 10 тыс. и выше

Компания Sensors Unlimited, Inc. (SUI), которая занимается средствами обработки изображений в ближнем инфракрасном диапазоне на основе арсенида галлия-арсенида индия (InGaAs), объявила о выпуске новейшей миникамеры с кадрированием, достигающей высокой частоты смены кадров.

Новая миникамера с кадрированием моментальных снимков (Windowed Snapshot MiniCamera SU320MSW-1.7RT) – первая миниатюрная телекамера ближнего инфракрасного диапазона с возможностью создания района интереса. Кроме окон, выбираемых пользователем, можно создать до четырех окон районов интереса. Размер предварительного окна может составлять от 16 x 16 до 200 x 200 пикселов. Окна размещаются по центру устройства формирователя изображений и работают с максимально возможной частотой, в зависимости от размера окна района интереса. При размере 16 x 16 пикселов, максимальная частота смены кадров телекамеры превышает 10 000 кадров в секунду. Кроме предварительно заданных окон, управление телекамерой осуществляется посредством последовательных команд, с помощью которых можно полностью управлять размером, расположением и временем интеграции окна района интереса.

Улучшенная коротковолновая инфракрасная миникамера с кадрированием моментальных снимков Sensors Unlimited имеет разрешающую способность 320 x 256 с размером зерна 25 мкм и может работать при дневном, солнечном или комнатном освещении. Полнокадровое изображение одновременно передается через совмещенный видеовыход и 12-разрядный интерфейс RS-422. Твердотельная телекамера ближнего инфракрасного диапазона с высокой чувствительностью (в пределах от 900 до 1700 нм) имеет коэффициент заполнения 100 % и квантовой эффективностью 100 % в пределах от 1 000 нм до 1 600 нм. Миникамера SUI, обладающая встроенной коррекцией неоднородностей и защитой от выцветания, которые обеспечивают прекрасное качество изображений, работает при комнатной температуре и потребляет менее 1,6 Вт.

Она предназначена для таких применений, как профилирование лазерного луча, машинное наблюдение быстродвижущихся объектов в коротковолновом инфракрасном диапазоне, анализ движения и тепловидение факелов горелок и ракетных двигателей.

Яковенко А. В.

ПОДВІЙНІЙ ЗАГРОЗІ – ПОДВІЙНА ПРОТИДІЯ

Імпульси перенапруги

ФІЛЬТР ЗАХИСНИЙ ПРОТИЗАВАДНИЙ

Uном = 220V, 50 Гц Iном = 3А, 10А або 25А
Діапазон робочих частот від 10 кГц до 18 ГГц
Подавлення імпульсів перенапруги з амплітудою до 4 кВ

Витік інформації

У Вашій організації працюють з файлами під грифом «для службового користування» або вищим рівнем секретності? Якщо так, то не забудьте обладнати свої комп'ютери електромережними фільтрами ЕМСБІ. Компактні та легкі, фільтри ЕМСБІ захистять Вашу техніку від витоку інформації та неприємних сюрпризів електромережі – імпульсів перенапруги, що загрожують як програмній, так і апаратній її частині.

Припинення витоку інформації в електромережу на частотах до 18 ГГц.

Вищі гармоніки центрального процесора комп'ютера, виробленого сьогодні, сягають частот 10 ГГц і вище – отже, інформація витікає з комп'ютера по проводах мережі електроживлення на частотах до 10 ГГц і вище.

Електромережні фільтри ЕМСБІ на номінальні струми від 3 А до 25 А ефективно протидіють витоку інформації в діапазоні від 10 кГц до 18 ГГц, зменшуючи витік в мережу сигналів до рівнів, на яких їх неможливо прочитати та розшифрувати.

Захист від високовольтних імпульсів перенапруги

Електромережні фільтри ЕМСБІ на номінальні струми від 3 А до 25 А захистять Ваші комп'ютери та під'єднані до них джерела безперервного живлення від виведення з ладу внаслідок:

– ударів блискавки поблизу підстанцій;

– роботи потужних промислових установок, зварювального обладнання, аварійних замикань;

– електромагнітного тероризму – розрядів штучного походження, що надходять на об'єкт захисту зовні.

Фільтри ЕМСБІ – електробезпечні при монтажі, обриві або відсутності заземлення

Струм витоку є мірилом безпеки фільтра для людей, які працюють з комп'ютером або монтують на ньому захисне обладнання.

Вітчизняні стандарти вимагають, щоб струм витоку електромережного фільтра не перевищував 10 % від робочого струму. Це означає, що струм витоку фільтра на 3 А не може бути вище 30 мА, фільтра на 10 А – вище 100 мА, фільтра на 25 А – вище 250 мА.

Показники струмів витоку фільтрів ЕМСБІ у п'ять–вісім разів кращі: 3,5 мА для фільтра на 3 А, 17 мА та 35 мА для фільтрів з робочим струмом 10 А та 25 А відповідно.

Монтаж та під'єднання – без зайвого головного болю для клієнта!

Назавжди забудьте про копітку процедуру монтажу, розпайки кабелів та інші неприємні етапи під'єднання фільтра до електромережі та комп'ютера. Кожен фільтр ЕМСБІ, на бажання замовника, оснащується системою «РКП» – спеціальним набором екранованих кабелів, кріплень та комп'ютерних роз'ємів. Фільтр вмикається в мережу, комп'ютер та периферія – в гнізда системи «РКП», і можна починати роботу. Окрім спрощення процедури під'єднання, система «РКП» забезпечує безперервність електромагнітного екранування на всьому шляху проходження струму – від споживача-комп'ютера до електромережі.

Наші ціни не ростуть

3 А: від 210 у.о. з ПДВ (ФЗП–103).
10 А: від 270 у.о. з ПДВ (ФЗП–110).
25 А: від 299 у.о. з ПДВ (ФЗП–125).

ТМ ЕМСБІ ТМ

Виробник: ТОВ ЕМСБІ. Електромагнітна сумісність та безпека інформації.
03057, м. Київ,
пр. Перемоги, 56, оф. 478.
Тел.: (044) 458 15 80
E-mail: info@emsbi.net.ua
www.emsbi.net.ua
Ліцензія ДСТСЗІ
№ 604461від 16.01.2004.

DigiScan EX Monitor и DigiScan EX Professional – новые редакции программного обеспечения для сканирующих приемников

Программное обеспечение DigiScan EX давно знакомо профессионалам в области техники защиты информации. Оно позволяет расширить возможности сканирующих приемников AOR/ICOM (AR8200, AR5000A, AR3000A, IC-R10, IC-R8500, IC-PCR1000), ускорить и автоматизировать процесс поиска закладных устройств. Поиск «закладок» ведется путем обнаружения активных частот и выполнения различных тестов с измерением акустической корреляции, что позволяет классифицировать данные частоты по уровню опасности. Программа DigiScan EX Lite включает базовые поисковые функции, а DigiScan EX Standard является расширенной версией с возможностями по созданию расписания работы, таймером на включение, дополнительным тестом и печатью сигналов и спектра.

В январе 2005 г. выпущены две новые редакции программы – DigiScan EX Monitor и DigiScan EX Professional (версия 1.6).

DigiScan EX Monitor

Данная версия предназначена для выполнения задач мониторингового характера – выявление активных частот, регистрация, звукозапись, накопление статистики по сигналам. В расписании DigiScan EX Monitor есть 3 задачи (см. Рис 2):

★ **«Сканирование диапазона»**

Сканирование диапазона частот с произвольным шагом и модуляцией, построение панорамы, регистрация активных сигналов, прослушивание или автоматическая звукозапись сигналов в базу звуковых файлов, распознавание DTMF.

★ **«Сканирование базы данных»**

Сканирование сигналов из БД на предмет их активности, прослушивание или автоматическая звукозапись сигналов в базу звуковых файлов, распознавание DTMF.

★ **«Контроль частоты»**

Контроль частоты на предмет активности, прослушивание или автоматическая звукозапись сигнала в базу звуковых файлов, распознавание DTMF.

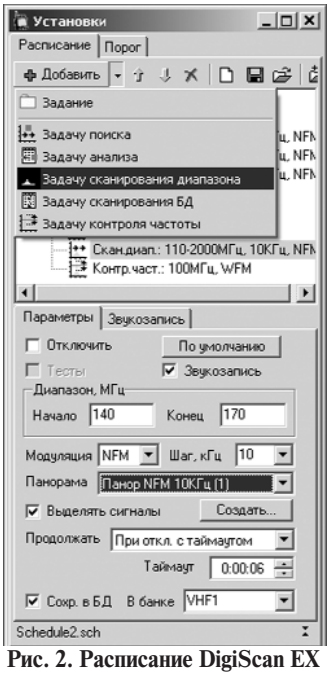


Рис. 2. Расписание DigiScan EX – параметры задачи сканирования диапазона

Программа обеспечивает обработку звуковых файлов аналогично многоканальным системам регистрации:

★ Выполняется компрессия звука с использованием кодеков типа MP3, ADPCM, GSM и т. д. Емкость часа записи – от 5.7 Мб, т.е. на диск 40 ГГб помещается 6 000 часов записи

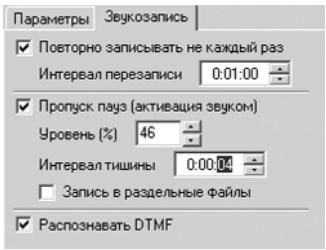


Рис. 3. Параметры звукозаписи

★ В базе звуковых файлов хранится дата/время записи, длительность, частота, модуляция, определенный номер DTMF.

★ Имеется функция активации голосом (VOX) для сокращения пауз в записи (см. Рис. 3).

★ Выполняется автоматическая очистка жесткого диска по мере его заполнения.

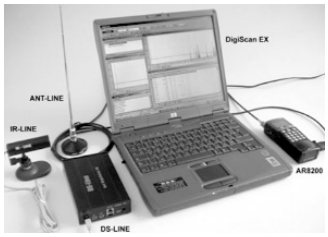


Рис. 1. Внешний вид поискового комплекса на базе DigiScan EX

★ Есть возможность экспорта звуковых файлов на другие диски или носители.

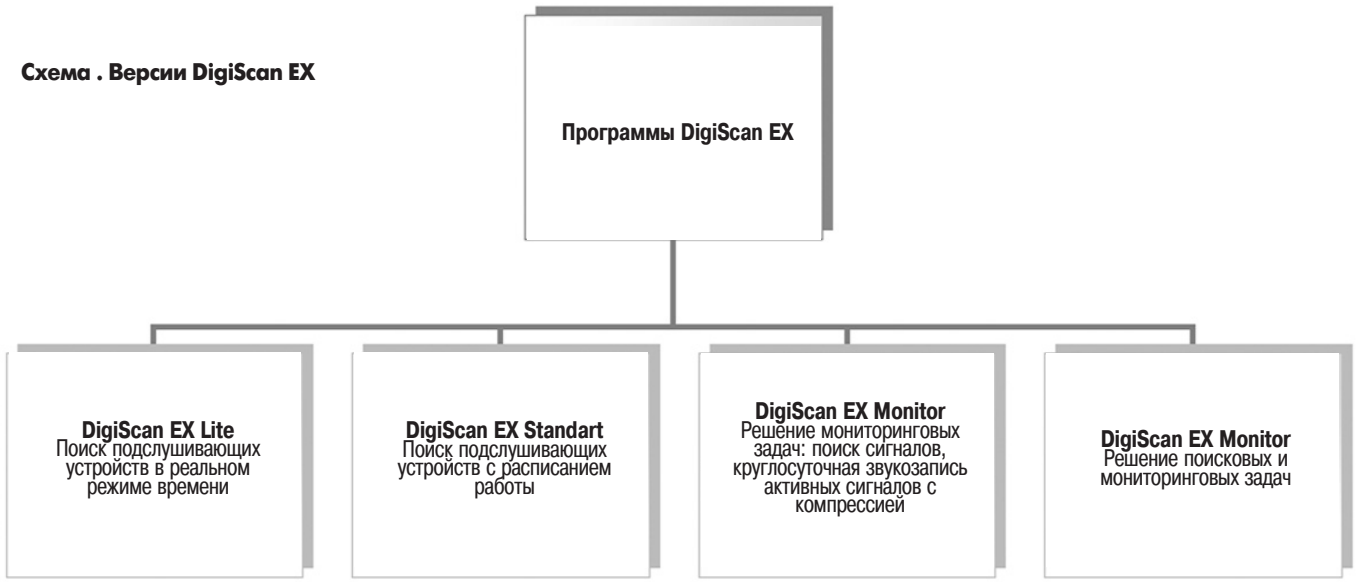
DigiScan EX Professional

Данная версия включает возможности DigiScan EX Standard и DigiScan EX Monitor, и предназначена для профессионалов, решающих различные задачи (см. Табл.).

Оповещение оператора об обнаружении закладки.

Информация предоставлена D.A.S.
www.das.kiev.ua
(044) 235-57-17,
490-67-34,
216-93-28

Схема . Версии DigiScan EX



	DigiScan EXLite	DigiScan EX Standart	DigiScan EX Monitor	DigiScan EX Professional
Расписание работы		+	+	+
Таймер на автоматическое выполнение задач		+	+	+
Виды выполняемых задач				
Задача «Поиск»: поиск подслушивающих устройств в заданном диапазоне, выполнение тестов для проверки «опасности» сигнала, сохранение сигналов в базе и автоматическая звукозапись на частоте опасных сигналов	+	+		+
Задача «Анализ»: тестирование сигналов в базе данных (БД) на их «опасность» и автоматическая звукозапись на частоте опасных сигналов		+		+
Задача «Сканирования диапазона»: сканирование заданного диапазона с заданным шагом и модуляцией, сохранение сигналов в БД, програмируемое условие продолжения и автоматической звукозаписи			+	+
Задача «Сканирование базы данных»: сканирование сигналов БД на предмет активности, программируемое условие продолжения и автоматическая звукозапись			+	+
Задача «Контроль частоты»: контроль частоты на предмет активности, программируемое условие продолжения и автоматическая звукозапись			+	+
Поисковые функции				
Пассивная амплитудная корреляция	+	+		+
Пассивная корреляция	+	+		+
Активная амплитудная корреляция	+	+		+
Активная параметрическая корреляция		+		+
Проверка налячая гармоник	+	+		+
Классификация сигналов по уровню опасности	+	+		+
Автоматическая запись звука от опасных сигналов	+	+		+
Автоматическая печать опасных сигналов		+		+
Оповещение оператора об обнаружении закладки	+	+		+
Пассивные режимы поиска	+	+		+
Локализация закладки и печать результатов		+		+
Автоматическое озвучивание помещения	+	+	+	+
База данных дружественных сигналов	+	+		+
Режим поиска дружественных сигналов		+		+
Настройка чувствительности распознавания сигналов	+	+	+	+
Настройка громкости спектральной и параметрической корреляции	+	+		+
Режим проверки НЧ-диапазона (проводных линий)	+	+		+
Звукозапись				
База звуковых файлов (частота, модуляция, дата / время, длительность, DTMF) с возможностью автоматической очистки и экспорта звуковых файлов	+	+	+	+
Выбор частоты оцифровки	+	+	+	+
Использование компрессии звука (MP3, ADPCM, GSM и т. д.). Объем занимаемого дискового пространства – от 5,7 Мб/час			+	+
Распознование тонального набора DTMF			+	+
Активация голосом и настройка уровня сработки			+	+
База данных				
Формат базы данных Microsoft Access (.mdb)	+	+	+	+
Хранение произвольного количества сигналов. Работа с сигналами через Clipboard	+	+	+	+
Хранение произвольного количества панорам, в т. ч. панорам максимумов, минимумов и усредненной. Настройка способа отображения и цвета панорам	+	+	+	+
Импорт-экспорт панорам, в т. ч. для их визуального сравнения	+	+	+	+
Экспорт сигналов в Excel и текстовый файл	+	+	+	+
Защита сигнала в базе данных от изменения	+	+	+	+
Печать сигналов и их спектров		+	+	+
Поддержка банков и отбор сигналов по банку			+	+
Выбор стиля работы («Поиск», «Мониторинг», «Эксперт»)				+
Прочее				
Режим предварительного сканирования (для оценки загрузки диапазона перед настройкой порога)	+	+	+	+
Режим отображения сигнала с обновлением	+	+	+	+
Возможность работы на Notebook с микрофонным входом (с ограниченными возможностями)	+	+	+	+
Настройка порога на панораме	+	+	+	+
Осциллограф, спектрограф	+	+	+	+

Мошенники становятся все более изощренными в фишинге

Эксперты предупреждают, что характер преступлений связанных с использованием фишинга изменился.

По словам Серджио Пинона (Sergio Pinon), старшего вице-президента по безопасности компании MasterCard International, за последние два месяца было зафиксировано, по крайней мере, 10 попыток фишинга с использованием фальшивых сайтов www.mastercard.com.

Если раньше мошенники бесхитростно действовали от лица известных банков и компаний, посылая миллионы писем, например, с темой «необходимо обновление учетной записи», которые заманивали наивных пользователей на подставные веб-сайты. Теперь увеличивается количество случаев использования вирусов-червей и шпионских программ для незаметного перенаправления пользователей на фальшивые сайты.

За последний год 57 млн. человек подверглись фишинговым атакам, в которых использовались торговые марки 122 известных компаний. По словам г-на Трудо, около половины атак проводилось с использованием шпионских программ или другого вредоносного кода. Так, например, одна из подобных атак, зафиксированная датской консалтинговой фирмой Secunia, вводила пользователя в заблуждение путем модификации файлов операционной системы Windows, после чего, во время набора пользователем адреса веб-сайта, браузер жертвы перенаправлялся на подставной сервер.

Более «амбициозные» атаки ставят своей целью уже серверы доменных имен, которые служат виртуальными адресными книгами, сопоставляющими имена сайтов с IP-адресом, имеющимся у каждого устройства, подключенного к интернету. Контролируя такой сервер, можно перенаправлять пользователей, запрашивающих, к примеру, www.bankofamerica.com, на подставной сайт с идентичным дизайном.

Если раньше мошенники пользовались ссылками с адресом, похожим на адрес сайта известной компании, то теперь ссылки на фальшивые сервера прячут внутрь кода письма, показывая пользователю ссылку в виде настоящего адреса.

В декабре 2004 года количество активных подставных сайтов, используемых фишерами, составило 1,7 тыс.

CNews

Обеспечение безопасности удаленного доступа

Увеличение мобильности пользователей, количества филиалов компании, желания предоставлять информацию только избранным заказчикам и клиентам приводит к пропорциональному увеличению необходимости в использовании технологий удаленного доступа и, естественно, к увеличению популярности последних. Области применения технологий удаленного доступа весьма разнообразны: соединение филиалов компаний друг с другом и с центральным офисом; предоставление сотрудникам, находящимся за пределами компании, средств связи с корпоративной сетью компании; предоставление доступа к корпоративным сетевым ресурсам партнерам или клиентам компании.

Как Вы уже успели заметить, средства удаленного доступа дают возможность расширить вашу сеть практически на весь мир. И при этом Вам необходимо лишь сервер удаленного доступа, который будет выполнять функцию приема и обслуживания запросов, и клиента удаленного доступа, представляющим собой компьютер с соответствующим программным обеспечением. Также Вам будет необходимо оснастить сервер и клиента удаленного доступа модемами и подключить их к телефонной линии. Обратите внимание, что на сервере и клиенте удаленного доступа должен быть установлен один и тот же протокол.

Итак, удаленный доступ к ресурсам корпоративной сети компании – это любой вид доступа, который осуществляемый по внешним каналам доступа и при этом устройства доступа, которые Вы используете, размещены за пределами охраняемой зоны и не контролируются вашей организацией.

Предоставляя удаленным пользователям доступ к сети, Вы должны четко осознавать приоритетность проблемы обеспечения повышенной безопасности сети. Сочетание мер безопасности с управлением правами доступа к разделяемым файлам и ресурсам позволит достичь высокого уровня безопасности и при этом не лишив пользователей возможностей удаленного доступа. Основными мерами безопасности являются метод обратного вызова, службы TACACS и RADIUS, стратегия удаленного доступа, политика удаленного доступа, блокировка учетных записей, хосты безопасности. Рассмотрим каждую из перечисленных мер в отдельности.

Метод обратного вызова.

Принцип его работы достаточно прост и в тоже время эффективен. Изначально использованием этого метода, Вы автоматически ограничиваете себя списком телефонных номеров абонентов, с которыми сервер удаленного доступа будет иметь возможность установить соединение. Включенный режим обратного вызова приводит к тому, что сервер удаленного доступа не верит регистрационной информации, то есть имени пользователю и паролю, введенными пользователем.

Принцип действия метода обратного вызова следующий:

★ конфигурируя сервер удаленного доступа, Вы, в качестве параметра, вводите определенный список телефонных номеров с учетными записями пользователей;

★ пользователь, набирая номер сервера удаленного доступа, вводит имя пользователя и пароль, по которым сервер удаленного доступа произведет идентификацию данного пользователя и проверит его учетную запись;

★ сервер разрывает соединение с целью набрать телефонный номер пользователя, находящийся в определенном Вами же списке;

★ пользователь, ответив серверу удаленного доступа, получает доступ к сети.

Обойти этот метод защиты злоумышленник может путем подключения к телефонной линии пользователя, или же если будет непосредственно звонить из дома или с рабочего места пользователя.

TACACS и RADIUS.

Управлять удаленными соединениями маленькой, во всяком случае небольшой, локальной сети Вы сможете с помощью одного сервера удаленного доступа. Однако если в состав локальной сети входят большие сегменты, а количество удаленных пользователей постоянно возрастает, то одного такого сервера будет явно недостаточно. В таких случаях возникает потребность централизованного контроля удаленного доступа. Осуществляют его протоколы централизованного контроля доступа к сети удаленных пользователей. Наиболее популярными считаются: TACACS (Terminal Access Controller Access Control System) и RADIUS (Remote Authentication Dial-In User Service).

Протоколам TACACS и RADIUS необходим отдельный сервер аутентификации, как для проверки подлинности пользователей, так и для определения их полномочий. Причем, осуществляя эти функции, он может использовать не только собственную базу данных, но и взаимодействовать с современными службами каталогов такими, как NDS и Microsoft Windows NT Directory Service. Серверы TACACS и RADIUS могут выступать в роли посредников как между серверами удаленного доступа и сетевыми ресурсными серверами, так и между внешними системами аутентификации.

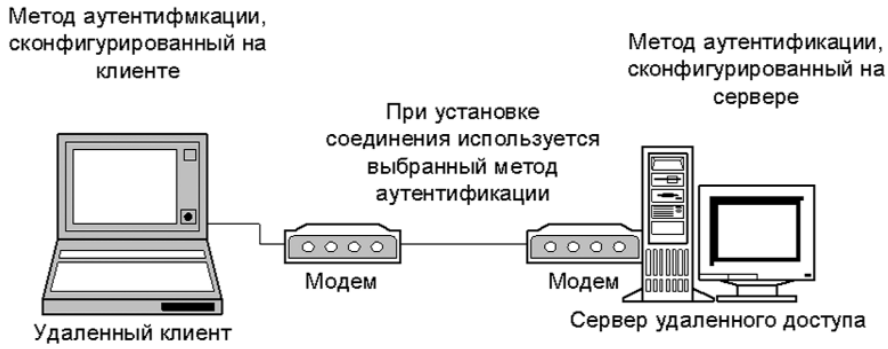
На примере протокола TACACS попробуем разобраться в особенностях централизованного контроля удаленного доступа.

Изначально мы имеем компьютерную сеть, в которую подключаем несколько серверов удаленного доступа и устанавливаем один сервер аутентификации TACACS. На сервере TACACS у Вас будет формироваться центральная база учетной информации о удаленных пользователях, включая их имена, пароли и полномочия; вестись база данных аудита, хранящая регистрационную информацию о логическом входе, продолжительности сессии и использовании ресурсов сети. Запросы удаленных пользователей на доступ к ресурсам сети принимают сервера удаленного доступа, которые и являются, непосредственно, клиентами сервера TACACS. Протокол TACACS, реализованный встроенным программным обеспечением, позволяет серверам удаленного доступа осуществлять взаимодействие с ним, на основе задания возможных типов запросов, ответов и соединений.

Клиенты, обращаясь к серверу TACACS, с определенным запросов, получают от него ответ сообщением, соответствующим этому запросу. Последовательности пар «запрос-ответ», которые соответственно ориентируются на решение отдельной задачи, под-

разумевают под собой соединения, задаваемые протоколом. Рассмотрим следующие типы соединений и операций, выполняемых при установке подключения:

★ AUTH – аутентификация;



★ LOGIN – аутентификация и фиксация логического соединения с пользователем;

★ SLIP – аутентификация, фиксация логического соединения с пользователем и подтверждение IP-адреса клиента.

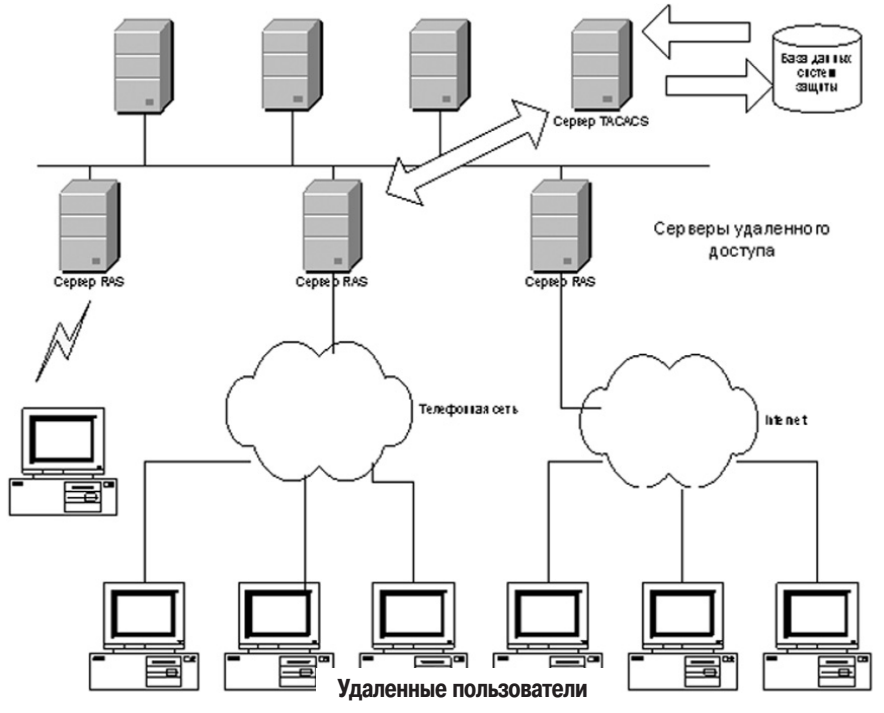
Перенаправление серверами удаленного доступа серверу TACACS потока запросов на логическое подключение пользователей к сети осуществляется с помощью соединения AUTH. А перенаправление серверами удаленного доступа серверу TACACS запросов на логическое подключение пользователей к отдельным компьютерам локальной сети осуществляется с помощью соединения LOGIN.

При установке соединения AUTH сервер TACACS получает от сервера удаленного доступа одно сообщение – пакет AUTH формата: username – имя пользователя; password – пароль пользователя (открытый текст); line – номер порта сервера удаленного доступа, по которому установил соединение пользователь; style – способ аутентификации. Сервер TACACS, проверив пароль, посылает ответ – пакет REPLY, сообщающем о удачной или неудачной аутентификации. Выполнять аутентификацию сервер TACACS может сам, и может также обращаться к другим системам аутентификации, например, NDS ОС NetWare и т. д.

С учетом того, что, при передаче пароля между сервером удаленного доступа и сервером аутентификации, пароль находится в открытом виде, то рекомендуется применять протокол TACACS совместно с проколом аутентификации по одноразовым паролям, к примеру, совместно с протоколом S/Key.

При установке соединения LOGIN происходит следующий обмен пакетами:

★ сервер посылает пакет REPLY в ответ на отправленный клиентом пакет LOGIN в случае установки логического соединения;



★ сервер посылает пакет REPLY в ответ на, отправленный клиентом, пакет CONNECT в случае подключения к конкретному компьютеру;

★ сервер посылает пакет REPLY в ответ на, отправленный клиентом, пакет LOGOUT в случае завершения сессии.

Запросу LOGIN соответствует такой формат, как (username, password, line), а ответу сервера – REPLY – (result1, result2, result3), где все эти три поля являются целыми числами, интерпретация которых зависит от соглашения, принятого конкретным типом сервера удаленного доступа и сервера TACACS. Запрос CONNECT имеет такой формат, как (username, password, line, destination IP, destination Port). Два последних поля предназначены для идентификации IP-адреса компьютера назначения и TCP-порта приложения, с которым устанавливается связь, соответственно.

Пути выполнения сервером TACACS аутентификации и авторизации удаленных пользователей различны: использования встроенного механизма аутентификации ОС сервера; использование централизованных справочных систем ОС (NIS, NIS+, NDS, Directory Services и др.); использование систем аутентификации на основе одноразовых паролей; передача запросов другим системам аутентификации (например, Kerberos).

Уязвимость протокола TACACS, связанная с открытой передачей пароля по сети, устранена в протоколе TACACS+, где пароль для передачи по сети шифруется с помощью алгоритма MD5. Также необходимо отметить, что TACACS+ обеспечивает разделенное хранение баз данных аутентификационной, авторизационной и учетной информации.

Централизованная аутентификация сервером RADIUS выполняется с помощью одного из протоколов: PAP (Password Authentication Protocol – Протокол аутентификации пароля), CHAP (Challenge Handshake Authentication Protocol – Протокол аутентификации с предварительным согласованием вызова) или MS-CHAP (Microsoft Challenge / Reply Handshake Authentication Protocol – Протокол Microsoft аутентификации с предварительным согласованием вызова), EAP (Extensible Authentication Protocol – Расширенный протокол аутентификации), DNIS (Dialed Number Identification Service – Служба идентификации набранного номера), ANI (Automatic Number Identification – Автоматическая идентификация номера).

Инициализация процесса аутентификации на базе протокола PAP происходит следующим образом. Сервер удаленного доступа устанавливает сеанс связи, после чего отправляет удаленному компьютеру пакет LCP (Link Control Protocol – Протокол управления каналом). Данный пакет указывает, что необходимо применить протокол PAP. Удаленный пользователь у себя на компьютере вводит идентификатор и пароль, которые отправляются по каналу связи проверяющей стороне. На основе вышеупомяну-

того идентификатора сервер удаленного доступа выбирает эталонный пароль из базы данных системы защиты с целью сравнения его с полученным паролем пользователя. При их совпадении удаленному пользователю сообщается о успешной аутентификации. Учтите, что идентификаторы и пароли передаются по линии связи в открытом виде. Это приводит к необходимости применять протокол PAP совместно с каким-либо протоколом аутентификации по одноразовым паролям. В противном случае существует вероятность перехвата пароля злоумышленником с целью его несанкционированного использования.

Инициализация процесса аутентификации на базе протокола CHAP происходит следующим образом. Сервер удаленного доступа устанавливает сеанс связи, после чего отправляет удаленному компьютеру пакет LCP, который указывает на необходимость применения протокола CHAP и определенного алгоритма хэширования. При поддержании алгоритма хэширования удаленным компьютером, последний отсылает серверу удаленного доступа пакет LCP, свидетельствующий о согласии с предложенными ему параметрами. Далее начинается аутентификация на основе обмена пакетами протокола CHAP. Формат любого пакета протокола CHAP следующий: (код, указывающий на тип пакета; идентификатор, являющийся уникальным числом для определения, какому запросу соответствует ответ; длина пакета в байтах; длина и формат поля данные в зависимости от типа пакета CHAP).

Зашифрованное с помощью уникального секрета, владельцами которого являются как проверяемая сторона, так и проверяющая сторона, произвольное слово-вызов является основой для аутентификации удаленного пользователя в протоколе CHAP. Изначально сервер удаленного доступа отправляет пакет Challenge (Вызов), поле данных которого содержит произвольную числовую уникальную для каждого пакета этого вида последовательность, ее длину в байтах и идентификатор проверяющей стороны. Данный пакет зашифровывается с применением односторонней функции и секрета удаленным компьютером. Полученный дайджест в виде пакета Response (Отклик), поле данных которого содержит дайджест и идентификатор проверяемой стороны, отсылается серверу удаленного доступа. Сервер удаленного доступа извлекает секретный эталонный пароль пользователя из базы данных системы защиты по идентификатору проверяемой стороны, взятому из полученного пакета Отклик. Далее сервер удаленного доступа зашифровывает идентификатор проверяющей стороны и числовую последовательность из пакета Вызов с помощью алгоритма хэширования и секретного эталонного пароля. Содержимое результата проделанной процедуры сравнивается с содержимым результата из пакета Отклик. Совпадение означает успешную аутентификацию. Теперь сервер удаленного доступа отсылает удаленному компьютеру либо пакет Success (Подтверждение), либо пакет Failure (Отказ) в зависимости от успешно или неуспешно пройденной аутентификации соответственно.

Обратите внимание, пакет Вызов может отправляться повторно в течении сеанса удаленной связи, что позволяет Вам проводить динамическую аутентификацию для проверки подлинности противоположной стороны. Защита от перехвата ответа сервера удаленного доступа зависит от уникальности числовой последовательности в пакете Вызов. Эта уникальность обеспечивается способом ее формирования, который заключается в конкатенации двух элементов: текущего времени и сгенерированного случайного числа. С целью защиты пароля от хищения и повторного использования злоумышленником перехваченных пакетов с зашифрованным паролем, пароль пользователя для передачи по линиям связи шифруется с применением случайного числа, присланного сервером.

Также не стоит забывать о возможном возникновении проблем несовместимости узлов сети из-за используемых функций вычисления дайджеста. Именно, по этой причине компания Microsoft реализовала собственный вариант протокола, получивший название MS-CHAP.

Мы рассмотрели процессы прохождения аутентификации в наиболее часто применяемых в компьютерных сетях протоколах аутентификации. О следующих трех скажем лишь то, что в EAP используются MD5, интеллектуальные карты или сертификаты; DNIS основан на номере, который набран пользователем; ANI основан на номере, с которого звонит пользователь.

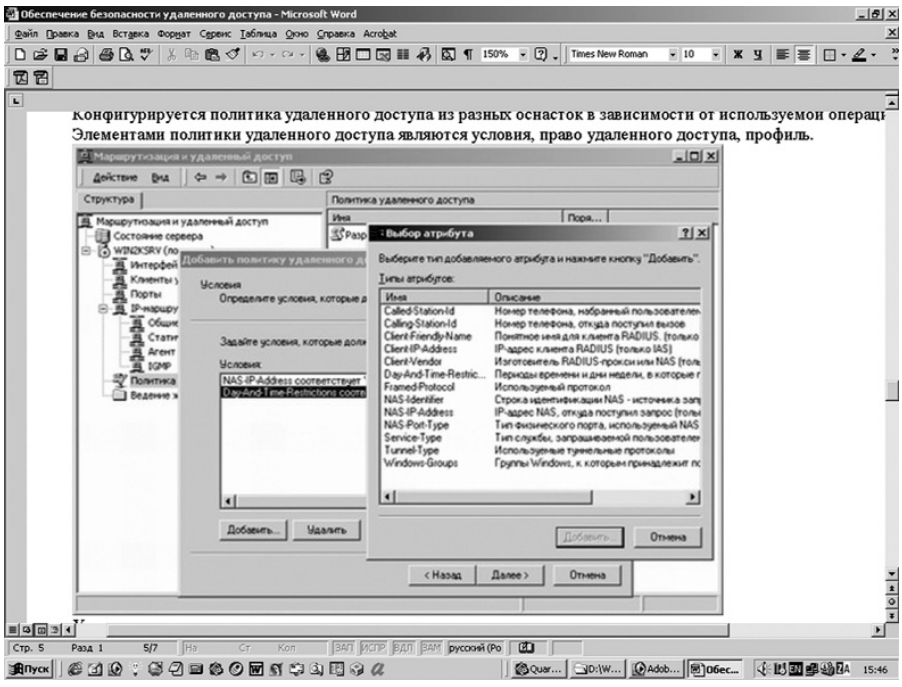
Протоколы TACACS и RADIUS по функциональным возможностям практически одинаковы. Однако протокол RADIUS более популярный среди производителей систем централизованного контроля удаленного доступа за счет бесплатно распространяющегося серверного программного обеспечения. Также в протоколе TACACS используется протокол TCP для взаимодействия между сервером удаленного доступа и сервером аутентификации, а в протоколе RADIUS – UDP, являющимся более простым, но менее надежным.

Стратегия удаленного доступа

С целью централизованного управления доступом Вам необходимо будет создать и в последующем применять стратегию удаленного доступа. Ведь пользователи Вашей корпоративной сети могут пользоваться незащищенными, нешифруемыми соединениями, а любой неконтролируемый вход в систему сам по себе уже является потенциальной «дырой» в защите. Стратегия удаленного доступа должна позволять выполнять пользователям свою роботу при поддержании соответствующего принятого уровня защиты корпоративной сети.

Временный вариант стратегии удаленного доступа может включать в себя правила предоставления доступа или отказа в доступе, ограничения времени существования соединения и определять используемые методы аутентификации. Причем правила предоставления доступа и отказа в доступе основываются на таких критериях, как время дня, день недели, членство в группе, тип удаленного соединения. Если же Вы решили разработать более серьезную стратегию удаленного доступа, то пойдем дальше.

Изначально, Вам будет необходимо определить к каким ресурсам необходим доступ с учетом особенностей деятельности Вашего предприятия. А вот при определении того, каким об-



разом Вы предоставите нужное соединение с сетью, воспользуйтесь следующими рекомендациями:

★ используйте аналоговые модемы при отсутствии потребности в высокой пропускной способности;

★ ISDN (Integrated Services Digital Network) или Frame relay на 56 Кбит/с – при наличии потребности в более высокой пропускной способности;

★ скоростные соединения посредствам реализации беспроводной локальной сети, ADSL (Asymmetric Digital Subscriber Line) или выделенные линии – при необходимости высокой пропускной способности.

Применяйте идентификацию и шифрование так как Интернет не является защищенной сетью. В случае использования идентификации на основе пароля, создайте и утвердите четкие правила по парольной защите, определяющие безопасность генерации пароля, его максимальный и минимальный сроки действия, минимальную длину паролей, требования сложности и неповторяемости паролей. Желательно применение идентификации с помощью обратного вызова, идентификации по PAP, CHAP. Также Вам необходимо будет обеспечить передачу паролей по сети не в открытом виде. Например, используя закрытые схемы идентификации с однократно генерируемыми паролями. Также можете внедрить такие схемы защиты, как Kerberos, RADIUS, TACACS. Итак, мы можем сделать вывод, что:

★ PAP / CHAP – базовая идентификация для соединений по PPP. Рекомендовано использовать с Kerberos или RADIUS;

★ S / Key – генератор одноразовых паролей для серверов терминалов;

★ Kerberos – набор средств идентификации общего назначения;

★ RADIUS – идентификация в масштабах предприятия;

★ TACACS – схема идентификации, являющаяся стандартом Интернет.

В любом случае, спроектированная Вами архитектура будет являться своеобразным согласованным набором различных схем, включая целый комплект низкоуровневых сетевых протоколов, надежно обслуживающих разнообразные методы и приложения удаленного доступа. С учетом того, что такие протоколы, как NetBIOS, NetBEUI, AppleTalk не разрабатывались для использования в корпоративных сетях, их применение не рекомендовано. Если же это неизбежно, то, во-первых, изолируйте их в пределах подсети, во-вторых, разработайте план их последующего исключения из использования. Данные аспекты находят свое применении не только на транспортном и нижележащих уровнях, но и на прикладном уровне.

Стандартными протоколами для нижеперечисленных приложений являются следующие протоколы: базовый протокол – TCP / IP; модемное соединение –PPP, SLIP; электронная почта – SMTP, POP3, IMAP; терминальный доступ – telnet; передача файлов – ftp; разделение файлов – NFS; WWW (World Wide Web) – HTTP; доступ к мэйнфрейму – TN3270; удаленная печать – LPR / LPD.

Стратегия удаленного доступа должна гарантировать безопасность корпоративной сети. При организации защиты сети обратите внимание на такие аспекты, как:

★ единственная точка входа в сеть для узла;

★ протоколирование доступа по средствам соответствующего программного обеспечения;

★ квоты на время доступа пользователя;

★ система аутентификации;

★ брандмауэры;

★ шифрование каждого байта перед его передачей через сеть;

★ избегайте нестандартных решений;

★ систему отчетности.

С целью дальнейшего внедрения стратегии удаленного доступа и ее последующего исполнения Вам будет необходимо обучить пользователей Вашей корпоративной сети. Наилучшим вариантом выхода из сложившейся ситуации будет организация обучающих классов для потенциальных удаленных пользователей. Программа занятий должна включать правила настройки, защиты и доступа. Естественно, и Ваша корпоративная сеть, и рассмотренная нами, стратегия удаленного доступа будут совершенствоваться, но исходная точка будет играть решающую роль.

Политика удаленного доступа

Добиться гибкости в настройке разрешений удаленного доступа и атрибутов соединения Вам позволит применение политики удаленного доступа. Политика удаленного доступа представляет собой набор правил и параметров соединения, хранящихся на локальном компьютере. Применение политики удаленного доступа Вам позволит как предоставлять разрешения удаленного доступа в соответствии с временем дня, днем недели, группой Windows, членом которой является дозвонившийся пользователь, типом требуемого соединения (коммутируемое или VPN-соединение), так и определять параметры настройки, накладывающие ограничения на максимальное время сеанса связи, тип аутентификации и шифрования, фильтрацию IP-пакетов.

Важным моментом является осознание того, что применении политик удаленного доступа соединения устанавливаются успешно только в том случае, когда параметры настройки соединения соответствуют, хотя бы, одной из политик удаленного доступа.

Конфигурируется политика удаленного доступа из разных оснасток в зависимости от используемой операционной системы.

Элементами политики удаленного доступа являются условия, право удаленного доступа, профиль.

Условия:

★ NAS-IP-Address (Network Access Server – IP-Address) – IP-адрес сервера сетевого доступа;

★ Service-Type – тип службы;

★Framed-protocol – протокол кадрирования;

★ Called-Station-ID – идентификатор вызванной системы;

★ Calling-Station-ID – идентификатор вызывающей системы;

★ NAS-Port-Type – тип порта NAS;

★Day-and-time-restrictions – ограничения по дню и времени;

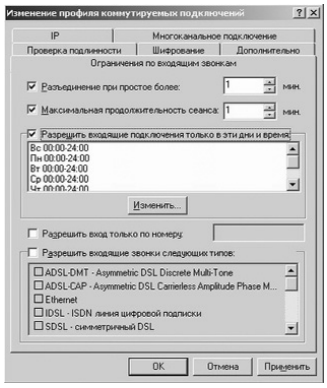
★ Client-IP-address – клиентский IP-адрес;

★ Client-Vendor – изготовитель клиента;

★ Client-friendly name – имя клиента, дружественное название;

★ Windows-Groups – группы Windows.

Право удаленного доступа может как предоставляться, так и нет в зависимости от выполнения всех условий политики удаленного доступа или их не выполнения соответственно. Вы должны будете поставить выключатель либо в положение «Предоставлять право удаленного доступа» (Grant remote access permission), либо в положение «Запретить разрешение удаленного доступа» (Deny remote access permission).



Для получения разрешения удаленного доступа параметры соединения должны соответствовать параметрам учетной записи пользователя или профиля. В противном случае разрешение удаленного доступа будет отклонено. По умолчанию для политики удаленного доступа установлено значение «Запретить разрешение удаленного доступа» (Deny remote access permission).

После успешного получения разрешения удаленного доступа к соединению применяется ряд параметров, вместе образующих профиль политики удаленного доступа.

Параметры профиля политики удаленного доступа:

★ Idle Disconnect Time – разъединение при простое;

★ Maximum Session length – максимальная продолжительность сеанса;

★ Day and time limits – разрешить входящие подключения только в эти дни и время;

★ Dial-in Number – разрешить вход только по номеру;

★ Dial-in media – разрешить входящие звонки следующих типов;

★ IP – свойства IP;
★ Multilink – многоканальное подключение;
★ Authentication – проверка подлинности;
★ Encryption – шифрование;
★ Advanced – дополнительно.

Блокировка учетных записей

Настоятельно рекомендуется использовать такую возможность безопасности как блокировка учетной записи (Account Lockout). Блокировка учетной записи подразумевает под собой отмену разрешения удаленного доступа для учетной записи пользователя после определенного числа не принятых попыток проверки подлинности. Обратите внимание на то, что регистрация под заблокированной учетной записью невозможна. Давайте четко разберемся, какие характеристики блокировки мы можем задать с помощью параметров блокировки учетных записей в ОС Windows. Итак,

★ Lockout After определяет число не принятых попыток, после которого учетная запись пользователя будет заблокирована;
★ Reset Count After определяет интервал в минутах обнуления счетчика не принятых попыток;
★ Lockout Duration: Forever – учетная запись пользователя блокируется до разблокировки администратором; Duration - время в минутах, на которое блокируется учетная запись пользователя, и, по истечению которого учетная запись будет автоматически разблокирована (диапазон: от 1 до 99 999);
★ Forcibly disconnect remote users from server when logon hours expire (Принудительно отключать удаленных пользователей по истечению разрешенного для работы времени) (ОС Windows NT Server): при таком установленном флажке пользователь принудительно отключается от всех серверов домена по истечению разрешенного времени работы; при таком сброшенном флажке пользователь не будет принудительно отключен от всех серверов домена по истечению разрешенного времени работы, но новые подключения для него будут запрещены.

В последних версиях Windows с целью разрешения возможности блокировки учетной записи Вам потребуется изменить некоторые параметры в системном реестре:

1.HKEY_LOCAL_MACHINE / SYSTEM / CurremControlSet / Services / RemoteAccess / Parameters / AccountLockout / MaxDenials. Значение параметра MaxDenials - максимальное число не принятых попыток (от 1 до 999). По умолчанию MaxDenials = 0, что означает блокировка учетной записи запрещена.

2.HKEY_LOCAL_MACHINE \SYSTEM\CurremControlSet / RemoteAccess / Parameters / AccountLockout / ResetTime. Значение параметра ResetTime – временный интервал в минутах до сброса счетчика не принятых попыток (от 1 до 99 999). По умолчанию ResetTime = Oxb40, что означает 2 880 мин. или 48 ч.

Рассмотрим пример определения стратегии учетных записей для всех учетных записей пользователей домена сети ОС Windows:

1. Войдите в систему под учетной записью Администратора.
2. В меню Policies (Политика) утилиты User Manager for Domains (Диспетчер пользователей домена) выберите пункт Account (Учетные записи).
3. В отобразившемся диалоговом окне Account Policy (Политика учетных записей) установите значения в зависимости от требований к защите следующих ограничений: Maximum Password Age (Максимальный срок действия), Minimum Password Age (Минимальный срок действия), Minimum Password Length (Минимальная длина пароля), Password Uniqueness (Уникальность пароля), Account Lockout (Блокировка учетной записи), Lockout After (Блокировка после X не принятых попыток входа), Reset Count After (Сброс счетчик через X минут), Lockout Duration (Длительность блокировки).
4. Щелкните на кнопке OK.

Также Вам необходимо знать, как разблокировать учетную запись в компьютере под управлением ОС Windows:

1. Войдите в систему под учетной записью Администратора.
2. В списке Username (Пользователь) утилиты User Manager for Domains (Диспетчер пользователей домена) дважды щелкните на заблокированной учетной записи.
3. Сбросьте флажок Account Locked Out (Заблокировать учетную запись).
4. Щелкните кнопку OK и закройте окно утилиты User Manager for Domains.

Хосты безопасности

Дополнением к системе безопасности являются хосты безопасности. Функцию проверки наличия разрешения на соединение с сервером удаленного доступа у вызывающего клиента удаленного доступа выполняют устройства, называемые хостами безопасности. Исходя из поставленной перед ним задачи, делаем вывод, что хосты безопасности необходимо располагать между клиентом и сервером удаленного доступа. С целью реализации этого дополнительного уровня безопасности Вам потребуется некий аппаратный ключ для проверки подлинности. Проверка клиента удаленного доступа, с целью выявления является ли он владельцем вышеоговоренного ключа или нет, выполняется до подключения к серверу удаленного доступа. Это позволяет использовать хосты безопасности сторонних производителей, что в свою очередь, повышает безопасность удаленного доступа.

Хосты безопасности могут быть различных типов. Например, пользователь должен ввести имя и пароль, основным требованием к которым является отличие и отсутствие зависимости от имени пользователя и пароля для регистрации на сервере удаленного доступа. А модемы PC Card компании Security Dynamics позволяют выполнять автоматическую аутентификацию мобильных пользователей, то есть если введенный пользователем PIN правильный, то модем автоматически передают регистрационную информацию на хост безопасности с целью ее проверки.

Статистика показывает, что большинства компаний становятся жертвами атак, направленных на получение несанкционированного доступа к информации компании, лишь по причине не осознания важности обеспечения безопасности удаленного доступа.

Исходя из того, что большинство специалистов в области компьютерной безопасности считают, что существующие методы защиты удаленного доступа являются недостаточно эффективными, рекомендуем Вам использовать комплексный подход к обеспечению безопасности.

Канд. тех. наук
Сорокопуд С. А.,
Мудрова Л. В.

Dynacord ProMatrix – идеальная система оповещения и трансляции для торговых предприятий

Продолжая разговор о системах оповещения и трансляции (Public Address) мы остановимся на описании работы системы Dynacord ProMatrix на торговых предприятиях.Какую функцию выполняют эти системы и зачем они необходимы? В наше неспокойное время система оповещения и трансляции, прежде всего, является составной частью системы безопасности большого здания – в экстренных случаях (пожар, природный катаклизм или техногенная катастрофа) она обеспечивает передачу информации о происшествии и инструкции по эвакуации посетителям и персоналу. В обычном режиме посредством этой системы передаются различные рекламно-информационные объявления и транслируется фоновая музыка для обеспечения комфортной атмосферы для покупок.

Для правильной работы система оповещения и трансляции должна отвечать следующим требованиям:

★ Наличие, как минимум, одного или нескольких микрофонных терминалов для передачи рекламно-информационных сообщений посетителям и персоналу;

★ автоматическое отключение трансляции фоновой музыки при подаче сообщений;

★ оптимальная разборчивость речи, высокое качество сигнала и транслируемой музыки;

★ возможность свободного выбора зон для передачи сообщений и оповещения о тревоге и трансляции фоновой музыки;

★ возможность передачи сообщений с внутренних телефонных линий в любую зону объекта;

★ простая запись сообщений, автоматическое воспроизведение рекламы и других объявлений;

★ передача сообщений о рабочем состоянии системы и неполадках в ее отдельных компонентах на диспетчерский пункт;

★ высокая надежность и безопасность эксплуатации и быстрое устранение неполадок.

Система Dynacord ProMatrix, установленная в торговом центре в базовой конфигурации, полностью отвечает вышеприведенным требованиям. Она является простым и экономически оправданным решением проблемы озвучивания, так как она включает в себя все необходимые компоненты: несколько микрофонных терминалов с кнопками выбора зон и кнопками подачи аварийных сигналов и экстренных сообщений, центральный процессор системы со встроенными модулями обработки сигналов и системными часами, устройство для записи рекламных объявлений и других повторяющихся сообщений, усилители мощности и источники фоновой музыки. Кроме того, система позволяет делать объявления из внутренней телефонной сети.

Микрофонные терминалы позволяют выбирать зону подачи сообщения и источник фоновой музыки (CD-проигрыватель или тюнер). Предупреждающие сообщения, рекламные и сообщения о закрытии магазина воспроизводятся

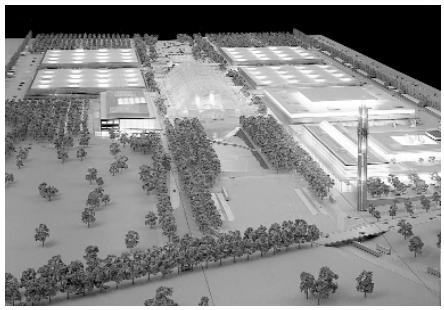
автоматически в установленное время или могут быть запущены нажатием кнопок микрофонного терминала, на которые назначены соответствующие сообщения. Все передаваемые сообщения имеют разный приоритет, например, рекламное сообщение может прервать трансляцию фоновой музыки, но при поступлении сообщения с микрофонного терминала оно будет выключено. На всех микрофонных терминалах имеются закрытые кнопки для подачи экстренных сообщений и сигналов тревоги.

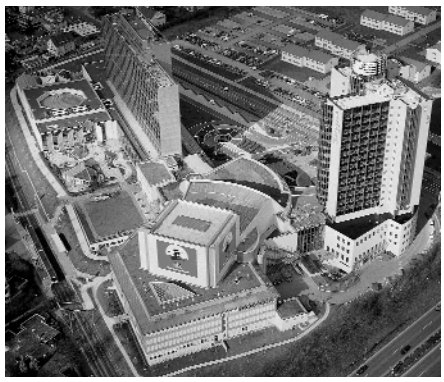
Текстовые сообщения, которые повторяются ежедневно, хранятся в менеджере сообщений DMM 4650, который записывает, хранит и воспроизводит до 100 различных текстовых сообщений. Рекламные сообщения, сообщения о специальных ценовых предложениях и о закрытии магазина записываются с высоким качеством и благодаря системным часам воспроизводятся в определенное время.

Фоновая музыка назначается на каждую зону отдельно при помощи микрофонного терминала. Проигрыватель компакт дисков и тюнер подключаются на вход центрального процессора системы, который регулирует уровень громкости сигнала, например, при подаче какого-либо сообщения он плавно снижает уровень фоновой музыки, а после завершения сообщения также плавно его увеличивает. При передаче аварийных сообщений фоновая музыка отключается полностью для обеспечения максимальной разборчивости сообщения.

В экстренной ситуации, например, при пожаре, система используется для передачи инструкций посетителям и персоналу по действиям в данной ситуации. Для работы системы в экстренной ситуации даже при отключении питания, есть источник резервного питания, который позволяет транслировать сигналы тревоги и инструкции на протяжении не менее 30 минут. Сигнал пожарной тревоги и инструкции по эвакуации заранее записываются и программируются в менеджер сообщений и запускаются нажатием закрытых кнопок на микрофонных терминалах. Дополнительный микрофон или микрофонный терминал позволяет командиру пожарной бригады давать объявления во всех зонах на самом высоком уровне громкости.

Надежность работы системы ProMatrix обеспечивает система мониторинга, которая выводит отчет о текущем состоянии всей системы и неполадках ее отдельных компонентов на дисплей главного микрофонного терминала. Посредством модема авторизованные специалисты могут получить доступ к системе, получить отчет о состоянии системы и, при необходимости, внести изменения в установки. Система настраивается при помощи специального программного обеспечения ProMatrix Designer.





Работу системы уже можно оценить в супермаркетах торговой сети «АМСТОР» в г. Донецке.

Напомним, что система Dynacord ProMatrix прошла сертификацию Государственным центром сертификации МЧС Украины (Сертификат соответствия системы оповещения о пожаре Dynacord ProMatrix UA 1.016.0074381-04 от 04.10.04).

Лицензия Госкомитета Украины по строительству и архитектуре АА № 486032 от 26.12.2002
Лицензия Государственного департамента пожарной безопасности МЧС Украины АА № 776795 от 14.09.2004
Сертификат соответствия для систем оповещения о пожаре Dynacord ProMatrix UA 1.06.00 74381-04 от 04.10.04 г.

ООО «КОРТМИ»
83086, г. Донецк, ул. Артема, 51А,
тел.: 038 /062 382-64-65,
345-08-12
факс: 038 /062 335-22-86
e-mail: cortmi@cortmi.com.ua
www.cortmi.com.ua

ОЦІНКА ЕФЕКТИВНОСТІ ЛІХТАРІВ ДИМОВИДАЛЕННЯ

Основним заходом протидимного захисту будинків та споруд під час пожежі є застосування ефективних систем димовидалення зі штучним або природним спонуканням. Підходи до визначення ефективності (вогнестійкості) елементів систем вентиляції зі штучним спонуканням (вогнезатримуючі клапани, димові клапани, вогнестійкі повітроводи, вентилятори димовидалення) вже розглядалися на сторінках журналу (№ 3 / 2003). Останнім часом при будівництві широкого поширення набувають системи димовидалення з природним (гравітаційним) спонуканням із застосуванням різноманітних зенітних ліхтарів димовидалення, тому оцінка їх ефективності (функціональної здатності під час пожежі) є досить актуальна.

Для видалення диму під час пожеж в будівлях та спорудах передбачається протидимний захист, який поєднує комплекс технічних засобів та організаційних рішень, що передбачають застосування систем димовидалення, димонепроникних огороджувальних конструкцій та інше.

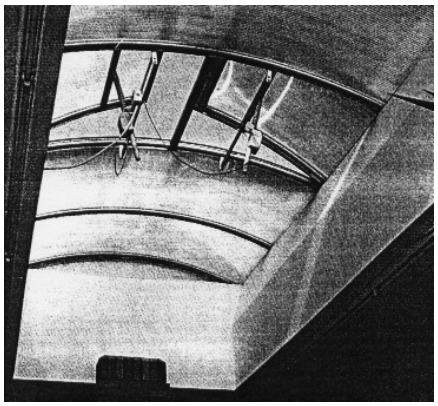
Одним з основних заходів протидимного захисту є застосування ефективних систем димовидалення з штучним або природним спонуканням.

Так, згідно з п. 5.10 СНиП 2.04.05-91 «Отопление, вентиляция й кондиционирование», у **багатоповерхових будинках,** як правило, потрібно передбачати системи димовидалення зі **штучним спонуканням,** які містять різноманітні вогнезатримуючі клапани, димові клапани, вогнестійкі повітроводи та вентилятори димовидалення. Видалення диму під час пожежі безпосередньо із приміщень **одноповерхових будинків та споруд,** як правило, потрібно передбачати системами з **природним (гравітаційним) спонуканням.**

Останнім часом, у зв'язку з будівництвом великих торгівельних, спортивних, виставкових, промислових одноповерхових об'єктів та будинків з атріумами (пасажами), почали застосовуватись системи димовидалення із природною (гравітаційною) тягою, основним елементом яких є зенітні ліхтарі (люки) димовидалення, що встановлюються на покритті. Відповідно до ДБН В.2.2-9-99 «Будинки та споруди. Громадські будинки та споруди. Основні положення», відкриття клапанів (люків, ліхтарів) димовидалення повинно здійснюватися автоматично від системи пожежної сигналізації, дистанційно та вручну. Відкриванню димових клапанів (ліхтарів) у покритті не повинні перешкоджати атмосферні опади. Клапани (ліхтарі) повинні відповідати вимогам по енергозбереженню будинків, а саме – мати теплозахисні властивості, та бажано сприяти природному освітленню приміщень.

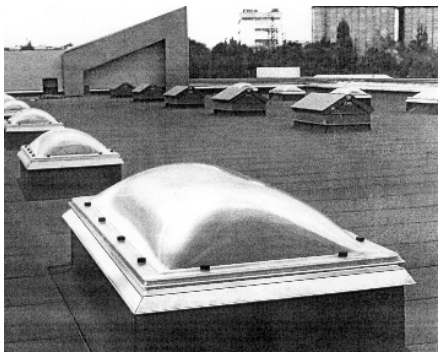
Абрамов О. О., Ткачук І. А.

Тому, ліхтарі димовидалення можуть мати, як прозоре так і непрозоре заповнення. Прозоре – багатошарове, як правило зі скла, акрилу або полікарбонату.



Привід відкривання ліхтаря може бути електричним, від електродвигуна з передачею гвинт-гайка, пневматичним – від джерела підвищеного тиску (пневмоциліндри з газовим балоном або піротехнічним зарядом) та електромеханічним (пружини з пусковим електромагнитом). Приводи оснащуються пристроями автоматичного спрацювання від системи пожежної сигналізації та від плавкого елементу, дистанційного спрацювання (від електрокнопки) та ручного спрацювання.

До переваг електричного приводу відноситься те, що він може бути застосований для провітрювання



приміщень та не потребує змінних елементів. Недолік – неможливість відкриття ліхтаря в разі відсутності напруги. Наявність пневматичного приводу ліхтаря передбачає необхідність заміни джерела тиску через певний термін та після кожного спрацювання (перевірка, помилкове спрацювання системи сигналізації тощо).

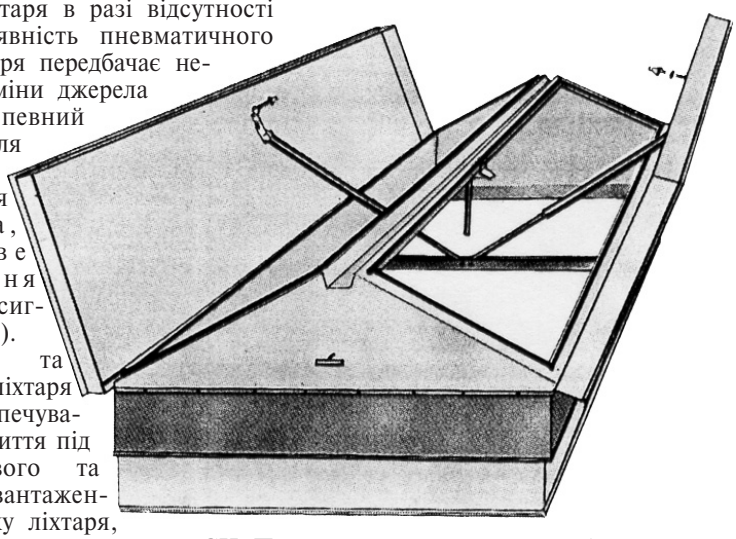
Привід та конструкція ліхтаря повинні забезпечувати його відкриття під дією снігового та вітрового навантаження на кришку ліхтаря, значення яких регламентується СНиП 2.01.07-85 «Нагрузки и воздействия».

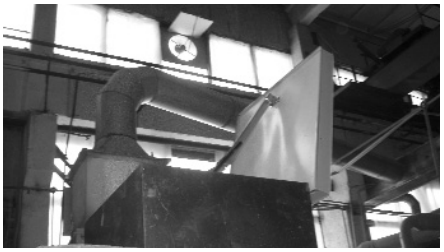
Під час пожежі (теплового впливу диму) прохідний переріз ліхтаря не повинен зменшуватись. Згідно до СНиП 2.04.05-91 температура диму під час його видалення з коридорів та холів приймається 300 °С, а під час горіння нафтопродуктів – за 600 °С.

Оцінка ефективності ліхтарів (люків) димовидалення в Україні здійснюється за методикою, яка відповідає європейському стандарту EN 12101-2:2003 «Smoke and heat control system – Part 2: Specification for natural smoke and heat exhaust ventilators ».

Сутність методу випробування полягає у **визначенні інерційності спрацювання** ліхтаря під дією зовнішніх атмосферних факторів (вітрових та снігових навантажень), а також **функціональної здатності** в умовах теплового (вогневого) впливу, який імітує температурний вплив продуктів горіння (диму) на ліхтар у разі виникнення пожежі у приміщенні.

Під час проведення випробувань на **інерційність спрацювання,** зовнішнє механічне навантаження на ліхтар повинне бути еквівалентне сніговому навантаженню з повним нормативним значенням згідно СНиП 2.01.07-85, з урахуванням особливостей конструктивного виконання та умов розташування ліхтаря на покритті. Снігове навантаження встановлюється з ряду 0, 125, 250, 500, 1 000 Па.





Вітрове навантаження виникає внаслідок повітряного потоку зі швидкістю 10±1 м/с або механічним навантаженням виходячи зі створення розподіленого по контуру кришки ліхтаря навантаження, яке повинне відповідати нормативному значенню вітрового тиску згідно зі СНиП 2.01.07-85.

Ліхтар, що встановлений на опорній конструкції, піддають 10 циклам відкривання без навантаження від дистанційного відкриваючого пристрою. Фіксують час повного відкривання ліхтаря під час кожного циклу.

Навантажують ліхтар (вітрові та снігові навантаження) та піддають його 3 циклам відкривання від дистанційного пристрою. Фіксують час повного відкривання ліхтаря під час кожного циклу. Реєструють будь-яку ознаку пошкодження або те, що ліхтар працює неправильно.

Граничним станом ліхтаря за ознакою **інерційності спрацювання** є стан, коли час повного відкривання ліхтаря (проміжок часу від подачі сигналу на відкривання ліхтаря до повного відкриття кришки) під дією зовнішніх атмосферних факторів (вітрових та снігових навантажень) перевищує 60 с.

Випробування на **функціональну здатність** в умовах теплового впливу здійснюється на вогневій печі.

Зразок ліхтаря встановлюють, закріплюють та герметизують на горизонтальній опорній конструкції, що імітує покриття, на печі згідно з технічною документацією підприємства-виробника. Вимірюють площу прохідного перерізу ліхтаря. Ліхтар, який встановлюється на світлових стрічках покриттів, повинен

спиратися на опорну конструкцію через фрагмент світлової стрічки, розмір якої по периметру корпуса ліхтаря до опорної конструкції повинен бути не менше 250 мм.

До ліхтаря з плавкими елементами автоматичного спрацювання приєд-нують дистанційне пристосування, що імітує спрацювання плавкого елементу, а ліхтар з електричним приводом до системи дистанційного управління.

Під час випробувань приріст температури у печі повинен бути 60 °С / хв ± 6 °С / хв. На п'ятій хвилині від початку випробувань температура в печі повинна відповідати значенню 300^{+60} °С та підтримуватись у подальшому на цьому рівні протягом часу випробувань, який становить 30 хв. У разі застосування ліхтаря на покритті приміщення, призначеного для зберігання паливно-мастильних матеріалів (склади нафтопродуктів тощо), на 10-й хвилині від початку випробувань температура в печі повинна відповідати значенню 600^{+120} °С та підтриму-ватись у подальшому на цьому рівні протягом часу випробувань (30 хв.).

На 5-й хв від початку випробувань подають сигнал від дистанційного пристою на відкриття ліхтаря та фіксують час його повного відкриття. Після проведення випробувань фіксують площу поперечного перерізу ліхтаря.

Граничним станом ліхтаря за ознакою **втрати функціональної здатності** в умовах теплового (вогневого) впливу є стан, коли: час повного відкривання ліхтаря на п'ятій хвилині від початку температурного впливу перевищує 60 с; площа поперечного перерізу ліхтаря після випробувань зменшилася більше ніж на 10 мм від площі поперечного перерізу ліхтаря зафіксованої до початку випробувань.

Абрамов О. О.,
Ткачук І. А.,
випробувальний» центр ТОВ «ТЕСТ»,
тел./факс: 8(044)946-66-05

Введено в дію оновлені правила пожежної безпеки

У серпні минулого року відділом нормативно-правового забезпечення діяльності пожежної охорони НДІ пожежної безпеки МНС України розпочалася робота з приведення у відповідність до чинного законодавства попередньої редакції «Правил пожежної безпеки в Україні», затверджених ще у 1995 році. Напередодні Нового року, зі змінами й доповненнями до ряду пунктів і положень, оновлені Правила введено в дію. Про характер цих змін розповідає головний спеціаліст зазначеного відділу Надія Довгошеєва.

За останні два роки переглянуто та прийнято велику кількість документів, що регулюють питання пожежної безпеки в державі та діяльності державного пожежного нагляду, а саме: «Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України», «Перелік посад, при призначенні на які особи зобов'язані проходити навчання і перевірку знань з питань пожежної безпеки, та порядок їх організації», «Положення про добровільні пожежні дружини (команди)», «Типове положення про службу пожежної безпеки» тощо. Таким чином, уся нормативно-правова база, що регулює діяльність Державного пожежного нагляду та питання пожежної безпеки зазнала суттєвих змін.

Сьогодні здійснено перегляд «Правил пожежної безпеки в Україні» та внесено до них відповідні зміни, які, в основному, стосуються приведення у відповідність із чинним законодавством України посилань на нормативно-правові акти. Крім того, зміни стосувалися розділів, в яких викладені вимоги щодо утримання засобів протипожежного захисту, а також вимоги щодо оснащення об'єктів та автотранспорту первинними засобами пожежогасіння у зв'язку з введенням в дію таких нормативно-правових актів, як: «Типові норми належності вогнегасників», «Правила експлуатації вогнегасників» тощо. Зазначимо, що у старих Правилах були викладені рекомендовані вимоги щодо оснащення об'єктів різного призначення первинними засобами пожежогасіння, які не враховували сучасного технічного рівня вогнегасників та мали необґрунтований вибір їх кількості для оснащення об'єкта. Водночас ситуація ускладнювалася відсутністю нормативного документа з питань експлуатації вогнегасників.

Оновлені Правила узгоджені з Федерацією профспілок України, Держнаглядохоронраці України, Держспоживстандартом України, Держпід-приємництвом України, Держбудом України, затверджені наказом МНС України від 19.10.2004 № 126 та зареєстровані в Мін'юсті України 04.11.2004 за № 1410/10009.

Правила увібрали в себе значний обсяг вимог пожежної безпеки, але вони можуть і потребують постійного вдосконалення, для чого слід проводити їх моніторинг та обговорювати питання, які виникають у працівників різних галузей, форм власності та рівнів під час виконання вимог цього документа.

Розмову вела Сердюк Т.,
інженер відділу
НТІМтмЗЗМІ УкрНДІПБ МНС України

НОВОСТИ

На Сумщині перекрито ряд контрабандних каналів

Протягом 2004 року за матеріалами управління СБ України в Сумській області порушено 9 кримінальних справ стосовно осіб, причетних до вчинення контрабанди в особливо великих розмірах. Співробітники регіонального управління спецслужби у взаємодії з працівниками інших правоохоронних органів не допустили контрабандного переміщення через кордон України комп'ютерної техніки та інших товарів загальною вартістю понад 1 млн. 750 тисяч гривень.

За рішенням судів протягом року у прибуток держави було конфісковано предметів контрабанди, затриманої співробітниками спецслужби, на суму близько 1 млн. 800 тисяч гривень та накладено штрафних санкцій на правопорушників на суму понад 79 тисяч гривень.

Прес-група управління СБУ в Сумській області

НОВОЕ ПРЕДЛОЖЕНИЕ НА РЫНКЕ УКРАИНЫ

СЕРТИФИЦИРОВАННЫЕ ОГНЕЗАЩИТНЫЕ И ТЕХНИЧЕСКИЕ ДВЕРИ

При строительстве сооружений промышленного, общественного и жилого назначения возникает необходимость оборудования их специализированными техническими дверями, обладающими огнезащитными свойствами. Эта необходимость обусловлена требованиями государственных строительных норм в области пожарной безопасности.

Приказом Госстроя Украины с 01.05.2003 введены в действие ДБН В.1.1-7-2002 «Пожарная безопасность объектов строительства». Данные нормы заменяют ранее действовавшие СНиП 2.01.02-85 и призваны поднять отечественные требования и стандарты пожарной безопасности до мирового уровня. Наша компания с 2003 года представляет на украинском рынке продукцию полностью соответствующую требованиям Евросоюза и новым строительным нормам Украины. Данные двери могут быть выполнены в стандартном и специальном огнезащитном варианте и обладают следующей конструкцией:

- прямоугольная дверная рама из оцинкованной стали толщиной 1,5 мм с углублением для дымозащитного уплотнителя, окрашенная порошковой краской серого цвета RAL 7038;
- полотно двери изготовлено из металлического листа толщиной 0,8 мм, толщина полотна 54 мм, покрытие из PCV серого цвета RAL 7035;
- наполнение: минеральное волокно, плотность 180 кг/м^3 (для одностворчатых дверей), 150 кг/м^3 (для двустворчатых дверей);
- регулируемые петли NORMA DIN с автоматической закрывающейся пружиной (встроенный доводчик закрывания);
- нажимная дверная ручка из огнестойкого полиамида со стальным стержнем;
- цилиндровый замок в комплекте с евроцилиндром (в комплекте 2 ключа);
- вес полотна 34,5 кг/м^2 (для одностворчатых дверей), 27 кг/м^2 для двустворчатых дверей.

Это сертифицированные в соответствии с ДСТУ БВ.1.1-4-98 «Строительные конструкции. Методы испытания на огнестойкость» огнезащитные и технические двери, предназначенные для использования в жилых и служебных помещениях с высокой интенсивностью эксплуатации. Представляемые нами двери соответствуют п.п. 2.14, 4.28 ДБН В.1.1-7-2002, обладают пределом огнестойкости EI60/EI72 (1,0–1,2 часа по признакам потери целостности и теплоизолирующей способности).

	№ сертификата	тип двери	макс. размеры	огнестойкость
1	UA 1.016.102364-03	двустворчатая	**2233 x 2395 мм H**	**EI60 (1,0 час)**
2	UA 1.016.102365-03	одностворчатая	**1150 x 2393 мм H**	**EI72 (1,2 часа)**
3	UA 1.016.102366-03	одностворчатая	**1141 x 2357 мм H**	**EI60 (1,0 час)**

Двери (как в стандартном, так и огнезащитном вариантах) могут быть снабжены ручкой «антипаника» — данная система препятствует образованию больших скоплений людей у дверей. Полотно двери распахивается при нажатии на ручку (расположенную по всей ширине полотна) туловищем. Для всех моделей дверей (поставляемых как в одностворчатом, так и двустворчатом вариантах) предлагаются также и досылатели двери и координаторы закрывания дверных полотен. Важной особенностью конструкции дверей являются регулируемые петли — позволяющие с максимальной плотностью соединить дверную коробку и полотно двери — как при монтаже — так и в процессе длительной эксплуатации. Как официальный поставщик данной продукции в Украину мы готовы предоставить Вам выгодные условия поставки и отличные ценовые предложения. Обладая профессиональными навыками работы, мы рады предложить Вам квалифицированное информационное обслуживание, а также консультационные и монтажные услуги. (***Лицензия на монтаж*** *№ АА 6329636 от 11.03.2004 г. выдана Государственным Департаментом Пожарной Охраны в г. Киеве).*

Дверями поставленными нашей компанией оборудованы следующие объекты:
- универмаг «Украина», г. Киев
- Управление Одесской железной дороги
- Торговый центр «Европа», г. Одесса, ул. Дерибасовская
- Одесский Припортовый завод
- больница «Интосана», г. Одесса
- отель «Отрада****»
- жилой комплекс, г. Одесса, ул. Уютная 11-13
- бизнес-центр «Форум», г. Киев и другие.
- гипермаркет «Метро», г. Харьков
- выставочный центр «Среднефонтанский», г. Одесса

студия 58

www.padilla.com.ua

«Студия 58»
тел.:+38(048)777-08-58
факс: +38(0482)34-52-93
e–mail: contract@studio58.com.ua

ОБЕСПЕЧЕНИЕ ПОЖАРНОЙ БЕЗОПАСНОСТИ НА СУДАХ – ЗАЛОГ БЕЗОПАСНОГО МОРЕПЛАВАНИЯ

В марте 2003 года исполнилось 55 лет со дня подписания Конвенции о создании ведущими морскими государствами Межправительственной морской консультативной организации ИМКО, переименованной с 1982 года в Международную морскую организацию – ИМО. За четверть века ИМО из консультативного органа превратилось в авторитетное агентство ООН, с помощью которого вырабатываются и своевременно совершенствуются международная нормативно-правовая база и технические рекомендации, регулирующие в мировом сообществе безопасность мореплавания, включая выживание людей при пожарах на море и противопожарную защиту судов.

Новым, 152-м членом ИМО, Украина стала 28 марта 1994 года. Интересы государства в ИМО представляет Государственный департамент морского и речного транспорта Министерства транспорта Украины. К этому есть все основания, ведь история украинского судоходства насчитывает большое количество пожаров на судах как в открытом море, так и в портах и на судостроительных и судоремонтных предприятиях.

Более полувека назад, 3 сентября 1948 года, на одном из судов Черноморского морского пароходства произошел пожар с катастрофическими последствиями. В Чёрном море на траверзе крымского порта Феодосия загорелось пассажирское судно германской довоенной постройки «Победа». Оно шло уже третий рейс по маршруту «Нью-Йорк - Гибралтар - Александрия - Батуми - Одесса» с отечественными и иностранными пассажирами, когда в тот день в специальном служебном помещении для перемотки катушек с кинолентами загорелась легковоспламеняющаяся нитроцеллюлозная кинопленка. При неудачном тушении вспыхнули все складированные в помещении катушки с плёнками, горевшие как рассыпанный порох. К сожалению, при невнимании экипажа пассажиры не по назначению использовали судовую противопожарную технику, пряча и провозя в ней за «железный занавес» предметы мелкой контрабанды. Пожару удалось не только развиться, но и выйти из-под контроля экипажа. Судно выгорело, большинство пассажиров удалось спасти подошедшими судами, но десятки людей на борту всё-таки погибли, спасаясь от морского пожара.

После этого трагического события у украинских моряков и пожарных портов и предприятий судоремонта были случаи успешной борьбы с пожарами на судах в портах и в рейсах («Тарас Шевченко», «Украина», «Шота Руставели», «Максим Горький»), а также случаи неудачных действий («Советская Украина», «Виталий Бонивур», «Валериан Зорин», «Анатолий Халин»). Несколько случаев борьбы с пожарами произошло уже на судах независимой Украины, включая выгорание жилой надстройки на сухогрузе «XI пятилетка» Укрречфлота с ущербом свыше 250 000 гривен. Весной 1998 года случился пожар на плавучем доке Ильичевского СРЗ с гибелью старшего матроса, а 6 октября того же года серьёзный пожар в порту Керчь на заводе «Залив» был потушен в доке на греческом судне в ремонте. По сообщению национальных украинских телеканалов 17 августа 2003 года на СРЗ имени Коминтерна г. Херсона на сухогрузном теплоходе «Алексей Фёдоров» водоизмещением 5 000 тонн, принадлежащем АСК «Укрречфлот», произошёл взрыв. Судно ремонтировалось у стенки причала судоремонтного завода. Ремонтные работы, огневые и огнеопасные, то есть газосварочные и малярные, в трюмах судна выполняли два предприятия, привлеченные СРЗ. В результате неправильного технологического режима в трюме теплохода образовалась взрывоопасная концентрация газа. При взрыве огромной силы, выбившей стекла окон домов и зданий в радиусе более 500 м, в стальной обшивке трюма образовалась огромная пробоина в борту площадью около 180 м^2, в которую хлынула вода и судно затонуло на глазах судоремонтников и экипажа тут же у причальной стенки СРЗ. При взрыве погибло четыре человека и один получил тяжёлые ранения.

Согласно международной статистике Регистра судоходства Английского Ллойда, ведущейся с 1824 года, пожары и взрывы на судах мирового флота, казалось бы, всего лишь одна из девяти учитываемых причин аварий в международной практике судоходства. Действительно, на долю пожаров и взрывов среди всех видов аварий судов выпадает только 5–8 %. Однако, примерно 20 % из всех случившихся в году аварий от пожаров и взрывов развивались до катастрофических последствий. Более того, около 30 % всех потерь мирового торгового и рыболовного флота ежегодно обусловлено именно по причине пожаров и взрывов, что во второй половине XX века постоянно делает ее первостепенной значимости.

Известно древнее суждение: человеческая жизнь не имеет цены. Следует учесть, что сегодня в мире есть немало экономически развитых стран, где пострадавшим в авариях семьям погибших выплачивается, по нашим меркам, огромная компенсация. Например, при урегулировании последствий пожара на датском пароме «Скандинавиан Стар» в 1990 г., состоявшегося в рейсе из Норвегии, жена и ребёнок за потерю кормильца получили единовременно 1,3 млн. крон, а ребёнку, потерявшему при пожаре родителей, устанавливалась ежегодная пенсия в 60 тыс. крон до совершеннолетия и единовременная компенсация в 570 тыс. крон.

Однако, даже эти отдельные страны-члены ИМО, как и все другие, несмотря на теоретическую бесценность человеческих жизней на море, не спешат требовать полностью пожаробезопасных судов. Мировое сообщество на данном этапе

не готово экономически, по затратам, к созданию и эксплуатации абсолютно пожаробезопасного морского торгового или рыболовного судна, а потому вынуждено соизмерять мораль и экономику. Отражение этого мы видим в непрерывном совершенствовании содержания даже такой наиболее основательно разработанной за 6 000-летнюю историю мирового мореплавания Международной конвенции по охране человеческой жизни на море СОЛАС, прошедшей в XX веке этапы эволюционного развития от оставшейся в проекте СОЛАС-14 через действовавшие в мировом судоходстве СОЛАС-29, СОЛАС-48, СОЛАС-60 к СОЛАС-74 и уже с поправками в виде трёх комплектов.

Подписанная в ноябре 1974 года, дополненная Протоколом 1978 года, СОЛАС-74 вступала в права с трудом и состоялась лишь 25 мая 1980 года под впечатлением, произведенным на судовладельцев и правительства стран-членов ИМО последствиями аварийности на мировом флоте за 1979 года и, в особенности, от взрывов и пожаров на судах. В специальном «Отчете об аварийности мирового торгового флота» за 1979 год, выпущенном Регистром судоходства Ллойда, год, предшествовавший году массового официального признания СОЛАС-74 правительствами стран-членов ИМО, был назван «годом мрачного рекорда мирного времени». Тогда более 1/3 потерь флота пришлось на сгоревшие и взорвавшиеся суда, т. е. на 83 судна общей валовой вместимостью 752 499 рег. т., из которых 33 судна пострадали от пожаров и взрывов в портах. В числе погибших судов по этой причине были и девять

танкеров, причем крупных, таких как «Энерджи детерминейшн» дедвейтом 321 186 т., сгоревший в Ормузском проливе, или «Атлантик эмпресс» дедвейтом 292 686 т. и «Эгеен кэптен» дедвейтом 210 257 т., погибшие от пожаров при столкновении в Карибском море.

ИМО значительно усовершенствовала тремя комплектами поправок СОЛАС-74 в части конструктивной (КПЗ) и активной (АПЗ) противопожарной защиты судов к моменту возникновения торговых и рыболовных флотов новых морских государств в бассейнах Черноморья (Россия, Украина, Грузия, Молдова), Балтики (Латвия, Литва, Эстония), Каспия (Азербайджан, Казахстан, Туркменистан). Новые нормы для КПЗ и АПЗ новых судов действуют с 1 февраля 1992 года С 1995 г. усовершенствована международная система квалификации плавсостава в деле борьбы с пожарами на судах разных назначений в виде Конвенции ПДНВ-78/95. Наконец, с июля 1998 г. действует разработанная ИМО IX глава СОЛАС-74, то есть Международный кодекс управления безопасной эксплуатацией судов (МКУБ).

По информации Главной государственной инспекции Госдепартамента морского и речного транспорта Украины еще с 1 июля 1997 года суда под украинским флагом включены в список подлежащих первоочередному инспектированию в целях проверки соответствия конвенционным требованиям по безопасности мореплавания, включая пожаробезопасность. Это означает, что комсостав и члены экипажей украинских судов должны пройти обязательную подготовку и аттестацию плавсостава в специализированных центрах обучения. Противопожарное оборудование, находящееся на судах, а также средства индивидуальной защиты личного состава и пассажиров и спасательные средства должны быть своевременно и качественно проверены, при необходимости подвергнуты ремонту и техническому обслуживанию и, в дальнейшем, освидетельствованы. Право проведения подобных мероприятий имеют исключительно специализированные организации, получившие признание и полномочия классификационных мировых обществ по надзору за состоянием судов (Регистры судоходства России, Украины, Регистры Ллойда Германии и Англии, Норвежский Веритас и др.). Подобные организации и предприятия есть во всех странах мира, имеющих выход в море. В их штате должны быть квалифицированные специалисты со стажем работы, достаточное количество необходимого оборудования, нормативно-техническая документация, а также разработана Система качества – свод требований к выполняемым услугам. Ведь требования к оборудованию, обеспечивающему защиту пассажиров судна и самого судна от пожаров жестче и конкретнее требований, предъявляемых к наземному подобному оборудованию. После постройки или ремонта судно не выйдет в рейс, если хоть один огнетушитель на его борту не будет соответствовать необходимым требованиям и освидетельствован. Регистры и надзорные службы портов требуют этого в неукоснительном порядке, доверяя при этом результатам услуг, выполненных признанными ими организациями.

Автор этих строк имеет непосредственное отношение к выполнению мероприятий, обеспечивающих контроль за состоянием пожарной безопасности на судах, так как является руководителем Исследовательско-испытательной лаборатории Главного управления МЧС Украины в Николаевской области. Лаборатория аккредитована в Российском Морском Регистре судоходства и в Регистре судоходства Украины на право проведения огневых испытаний неметаллических судостроительных материалов, по результатам которых Регистр вправе выдать сертификат о типовом одобрении. Также лаборатория производит проверку и освидетельствование средств пожаротушения на судах, занимается информационной деятельностью в этом направлении, активно сотрудничает с отделениями Регистров, а также судостроительными заводами, судоходными компаниями и предприятиями, занимающимися продажей и обслуживанием средств пожаротушения. При непосредственном участии сотрудников лаборатории было издано учебное пособие «Технические средства борьбы с пожарами на судах», созданное николаевскими специалистами в этой области – начальником Главного управления МЧС области генерал-майором службы гражданской защиты Поступальским Николаем Ивановичем и кандидатом технических наук, профессором Мартыненко Владиславом Ивановичем, к сожалению, ушедшим из жизни в прошлом году. Книга актуальна на сегодняшний день и не имеет аналогов в Украине как учебник для подготовки специалистов водного транспорта в области обеспечения пожарной безопасности.

По вопросам приобретения книги обращаться по телефонам: (0512) 49-06-68, 49-06-56.

Голубев Л.,
начальник Исследовательско-испытательной лаборатории ГУ МЧС Украины в Николаевской области

НОВОСТИ

США: последние версии Microsoft Word как находка для шпиона

Около 75 процентов электронных документов, находящихся в документообороте различных коммерческих компаний Запада, содержат информацию, которую сами компании считают не подлежащей разглашению, однако в 90 процентах этих компаний не знают, что такую информацию легко перехватить. Такие выводы, содержатся в исследовании фирмы Workshare, которая занимается вопросами компьютерной безопасности в корпоративных офисах.

Одна из проблем ненадежности хранения, по мнению экспертов фирмы, связана с широким применением последних модификаций формата Microsoft Word, который способен сохранять различные версии фрагментов документа при его изменении. Часто при создании документов используются фрагменты не подлежащего распространению текста, который потом убирается, но может оставаться в скрытом виде. Квалифицированный специалист по безопасности или хакер может очень легко прочесть такую скрытую информацию, что может использоваться при промышленном шпионаже и в других неблаговидных целях, отмечают в Workshare.

Отмечается, что сама Microsoft признает наличие проблемы и предлагает специальную программу «Remove Hidden Data» (rhdtool.exe), которая убирает из документов всю лишнюю информацию. Microsoft рекомендует обрабатывать этой программой каждый документ перед опубликованием его в публичных источниках.

BBC, Lenta

Огнетушители: применение, обслуживание, новости нормирования

Едва ли можно представить себе производство, организацию или учреждение, в котором нет ни одного огнетушителя. К сожалению, мало кто умеет пользоваться этими средствами. А жаль: вопреки расхожему мнению, изготовленный на совесть огнетушитель – весьма эффективное средство пожаротушения. Недаром в развитых странах при помощи огнетушителей на начальных стадиях ликвидируется более 30 % от общего количества пожаров, тогда как в Украине, согласно статистическим данным, эта цифра близка к 8 %. Буквально в течение полугода в Украине введено в действие три новых нормативных документа, регламентирующих оснащение объектов различного назначения огнетушителями, сроки их технического обслуживания, а также стандарт, устанавливающий общие требования к процессам технического обслуживания огнетушителей. Данная статья содержит информацию, которая может быть полезна владельцам и руководителям предприятий, лицам, ответственным за пожарную безопасность на объектах, частным лицам, организациям, занимающимся производством и техническим обслуживанием огнетушителей или желающих заняться такой деятельностью.

Огнетушители наряду с пожарным инвентарем (покрывала, ящики с песком, пожарные ведра, совковые лопаты и др.) и пожарным инструментом (багры, ломы, топоры и т. п.) относят к первичным средствам пожаротушения, с помощью которых ликвидируется загорание на начальных стадиях. К причинам неэффективности применения огнетушителей можно отнести низкую эффективность огнетушителей некоторых марок, которые серийно выпускались до недавнего времени, частые отказы таких огнетушителей, нарушение сроков перезарядки, использование огнетушителей не по назначению, неумение ими пользоваться, а также ошибки, совершаемые человеком в стрессовой ситуации.

Грамотное оснащение объекта первичными средствами пожаротушения и, в первую очередь, огнетушителями, дает возможность существенно повысить уровень его пожарной безопасности. Согласно п. 6.4.8 «Правил пожарной безопасности в Украине», «здания, сооружения, помещения, технологические установки должны быть обеспечены первичными средствами пожаротушения», причем «это требование касается также зданий, сооружений и помещений, оборудованных любыми типами установок пожаротушения, пожарной сигнализации или внутренними пожарными кранами». Кроме того, «впервые построенные, после реконструкции, расширения, капитального ремонта объекты (здания, сооружения, помещения, технологические установки) должны быть обеспечены первичными средствами пожаротушения (согласно нормам положенности) до начала их эксплуатации».

Количество и номенклатура основных видов пожарной техники (в т. ч. огнетушителей) для защиты объектов определяется в соответствии с требованиями общегосударственных и отраслевых нормативных документов и правил пожарной безопасности. Иногда допускается использование на одном и том же объекте (или в одном и том же помещении) различных типов огнетушителей, что ввиду разницы в их стоимости позволяет сэкономить немало денег. Но не исключено, что один огнетушитель не сработает, и тогда наличие второго может спасти положение.

Классификация пожаров

Классификация пожаров устанавливается ГОСТ 27331-87 Пожарная техника. Классификация пожаров. Эта классификация представлена в табл. 1, а условные обозначения классов пожаров согласно ему же – на рисунке. В странах СНГ, помимо указанных классов, пользуются обозначением горения оборудования, находящегося под напряжением, пожарами класса Е. Категория зданий и помещений производственного и складского назначения по взрывопожарной или пожарной опасности определяется в соответствии с НАПБ Б.07.005-86 (ОНТП 24-86 Определение категорий помещений и зданий по взрывопожарной и пожарной опасности).

Таблица 1. Классификация пожаров согласно ГОСТ 27331-87

Обозначение класса пожара	Характеристика класса пожара	Обозначение подкласса пожара	Характеристика подкласса пожара
A	Горение твердых веществ	A 1	Горение твердых веществ, сопровождающееся тлением (например, древесины, бумаги, соломы, угля, текстильных изделий)
		A 2	Горение твердых веществ, не сопровождающееся тлением (например, пластмассы)
B	Горение жидких веществ	B 1	Горенее жидких веществ, не растворимых в воде (например, бензина, эфира, нефтяного топлива), а также твердых веществ, переходящих при нагревании в жидкое состояние (например, парафина)
		B 2	Горенее жидких веществ, растворимых в воде (например, спиртов, металлов, глицерина)
C	Горение газообразных веществ	–	Горенее газообразных веществ (например, бытового газа, водорода, пропана)
D	Горенте металлов	D 1	Горенее легких металлов, за исключением щелочных (например, аллюминия, магния, и их сплавов)
		D 2	Горение щелочных и других подобных металлов (например, натрия, калия)
		D 3	Горение металлосодержащих соединений (например, металлоорганических соединений, гидридов металлов)

Виды и возможности огнетушителей

Огнетушители можно заряжать различными огнетушащими веществами. В зависимости от этого различают водные (огнетушители, содержащие в качестве зарядов воду или воду со специальными добавками), воздушно-пенные (огнетушители, содержащие в качестве зарядов пенообразующие растворы), порошковые (содержат в качестве зарядов огнетушащие порошки) и углекислотные огнетушители (огнетушители, содержащие в качестве заряда углекислоту). За рубежом производятся также хладоновые огнетушители. В последнее время на рынке Украины появились водопенные аэрозольные огнетушители (внешне они похожи на баллончики, в которые заправляют, скажем, дезодоранты, но имеют соответствующую назначению окраску). Говорят, существуют еще и комбинированные огнетушители, т. е. огнетушители, заряд которых состоит из двух и более типов огнетушащих веществ.

Водные огнетушители применимы для тушения твердых веществ, воздушно-пенные – для тушения твердых веществ и горючих (легковоспламеняющихся) жидкостей (как правило, неполярных). Для тушения спирта, эфира, ацетона и других полярных растворителей (включая смесевые) обычные воздушно-пенные огнетушители неприменимы. Столь популярные химические пенные огнетушители в принципе можно применять для тушения тех же веществ и материалов, что и воздушно-пенные огнетушители, однако эффективность химической пены на порядок ниже эффективности пены воздушно-механической. По имеющимся данным, химические пенные огнетушители наконец-то сняли с производства в Украине, прежде всего по причине несоответствия их огнетушащей эффективности требованиям нормативных документов. Однако на различных объектах таких огнетушителей хранится еще очень много. Как утверждают специалисты, ни одно сколько-нибудь серьезное возгорание огнетушителем типа «ОХП-10» потушить нельзя.

Порошковым и углекислотным огнетушителям по силам тушить твердые и жидкие вещества (в т. ч. полярные жидкости), электроустановки под напряжением до 1 000 В и горючие газы. Хотелось бы обратить внимание на то, что до недавнего времени на корпусах углекислотных огнетушителей писали «10 000 В». Надо полагать, причины, по которым эту цифру уменьшили в 10 раз, достаточно серьезны, так что будьте осторожны. Анало-

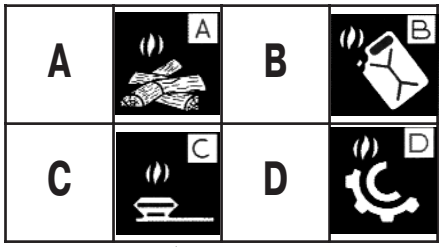


Рис. Условные обозначения классов пожаров различных классов согласно ГОСТ 27331-87

гичны возможности хладоновых огнетушителей, которые, насколько нам известно, в Украине не производятся и даже не упоминаются в нормативных документах.

Различают переносные и передвижные огнетушители. К первым относятся те из них, которые обычный человек может переносить вручную и пользоваться огнетушителем, держа его в руках (масса не превышает 20 кг). Передвижные огнетушители оснащаются колесами. Буква «з» в маркировке огнетушителя говорит о том, что он является закачным, т. е. что в его корпусе содержится не баллончик со сжатым воздухом, который перед применением огнетушителя нужно пробивать при помощи специального приспособления, а сжатый газ.

Чтобы понять, для тушения пожаров каких классов можно применить данный огнетушитель, нужно посмотреть на маркировочную надпись, нанесенную на его корпус. Из нее же можно почерпнуть некоторые сведения о том, как этим огнетушителем пользоваться. Применимость огнетушителей разных типов для тушения пожаров различных классов можно проиллюстрировать в виде сводной табл. 2.

Хотелось бы отдельно отметить особый случай – горение металлов (пожары класса D, которые обычными огнетушителями не тушат). Если загорелся, к примеру, кусок натрия, магниевая стружка или еще что-то в этом роде (по счастью, такие загорания случаются достаточно редко), то традиционное используемые огнетушащие вещества вряд ли помогут.Так как при взаимодействии ряда металлов с водой выделяется водород, а его смеси с кислородом (гремучий газ) весьма взрывоопасны. Если горит металлический натрий, магний, литий или еще что-то в этом роде, то лучше всего засыпать его песком.

Категорирование помещений

Очень часто в нормативных документах можно встретить такое понятие как категория помещения по взрывопожарной опасности. В зависимости от категории помещения, его площади, обращающихся в помещении веществ и материалов подбирают виды, емкость корпуса и количество огнетушителей. Чем «опаснее» категория помещения, тем более жесткие требования предъявляются к его оснащению огнетушителями. Это категорирование согласно НАПБ Б.07.005-86 (ОНТП 24-86) Определение категорий помещений и зданий по взрывопожарной и пожарной опасности представлено в табл. 3. Расчетное избыточное давление взрыва, равно как и категории помещений, определяются на стадии проектирования и указываются на специальных табличках, вывешиваемых около входов в них.

Какие огнетушители можно покупать

Специалисты считают, что большая часть изделий противопожарного назначения (в т. ч. огнетушителей) украинского производства имеет примерно один уровень качества и надежности с аналогами зарубежного производства. Существенная разница в стоимости не всегда означает существенную разницу в эффективности.

Многие продавцы, равно как и производители, занимаются, кроме продажи, также их перезарядкой, ремонтом и техническим обслуживанием. Хотелось бы предостеречь потенциальных клиентов от возможных ошибок: заведомо заниженная цена огнетушителя говорит о том, что это кустарное или полукустарное изделие. А для того, чтобы осуществлять перезарядку, ремонт или техническое обслуживание огнетушителей, равно как и

Таблица 2. Применимость огнетушителей для тушения пожаров различных классов

Тип огнетушителя	Применимость для тушения пожаров классов			
	A	B	C	E (ДО 1 000 В)
Водный	+	–	–	–*
Воздушно-пенный	+	+	+	–*
Порошковый	+	+	+	+
Угле-кислотный	–	+		+

Примечание. Знак «+» означает применимость, знак «-» – неприменимость, знак «-*» – опасность применения для жизни.

других средств пожаротушения, нужно иметь соответствующую лицензию.

Ст. 11 Закона Украины «О пожарной безопасности» гласит: «Все виды пожарной техники и противопожарного оборудования, применяемые для предупреждения пожаров и для их тушения, должны иметь государственный сертификат качества». 30.08.2002 подписан приказ бывшего Госстандарта Украины № 498 «Об утверждении Перечня продукции, подлежащей обязательной сертификации в Украине», который Минюст зарегистрировал 25.09.2002 под № 782/7070. В этот перечень, кроме всего прочего, попали «огнетушители, смеси и заряды к ним». В настоящее время сертификацию огнетушителей проводят на соответствие одному из двух государственных стандартов: ДСТУ 3675-98 Пожарная техника. Огнетушители переносные. Общие технические требования и методы испытаний или ДСТУ 3734-98 (ГОСТ 30612-99) Пожарная техника. Огнетушители передвижные. Общие технические требования.

Покупая огнетушитель, убедитесь, что он сертифицирован в Украине и пригоден для тушения веществ и материалов, обращающихся в производстве либо служащих конструкционными. Проверьте, имеется ли в наличии паспорт огнетушителя, на месте ли пломбы, нет ли видимых повреждений. Если огнетушитель является закачным, то стрелка индикатора давления должна находиться в зеленом секторе шкалы (рабочий диапазон). На маркировочной надписи огнетушителя и в его паспорте должны быть указаны производитель, дата изготовления (продажи) и дата проведения технического обслуживания огнетушителя.

Как применять огнетушители

Чтобы огнетушитель не оказался в нужный момент бесполезным куском железа, нужно заранее ознакомиться с тактикой его применения. Обычно переносные огнетушители рассчитаны всего на 8...12 с непрерывной подачи огнетушащего вещества, и любая ошибка при пользовании ими может оказаться непоправимой. Характерная ошибка состоит в том, что огнетушители перед применением переворачивают или бьют о землю (все это производили с рядом огнетушителей устаревших конструкций, подобные действия не только «вредны» для огнетушителя, но и опасны для человека, пытающегося воспользоваться им, ибо внутри корпуса находится газ под высоким давлением). Другая характерная ошибка состоит в неправильном выборе расстояния или направления подачи огнетушащего вещества. Если в процессе тушения корпус огнетушителя наклонить, то значительная часть заряда остается в нем. Если забыть пробить баллончик со сжатым воздухом либо сорвать предохранительную чеку (такое тоже бывает часто), то огнетушитель просто невозможно привести в действие.

Нужно помнить, что в большинстве случаев для тушения пожаров класса А лучше всего подходят водные и порошковые огнетушители, а также огнетушители, предназначенные для тушения пожаров пеной низкой кратности. Худший эффект обеспечивает применение воздушно-пенных огнетушителей, предназначенных для подачи пены средней кратности, совсем мало толку от углекислотных огнетушителей. Если материал склонен к тлению, то более эффективны огнетушители с зарядом на водной основе. Тушение горящего материала нужно производить с наветренной стороны, последовательно обрабатывая горящую поверхность. Струю огнетушащего вещества следует подавать в основание пламени, а после того, как удастся его сбить, необходимо произвести дотушивание отдельных очагов горения (или тления). После ликвидации горения желательно разгрести горевшие предметы, чтобы при необходимости дотушить их уже без помощи огнетушителя.

Для тушения пожаров класса В применимы порошковые, воздушно-пенные и углекислотные огнетушители. Порошок или пену нужно начинать подавать с наветренной стороны с максимально возможного расстояния, на которое «достает» струя, а затем стараться покрыть ими всю поверхность горения. Особенно быстро приходится перемещать из стороны в сторону раструб порошкового огнетушителя. Не следует подавать порошок или пену с излишне малого расстояния, чтобы не допустить разбрызгивания горящей жидкости. Если для ее тушения применяется углекислотный огнетушитель, то его раструб вначале следует направлять в основание пламени со стороны, ближайшей к оператору, а затем можно продвигаться вперед, ближе к очагу горения, выполняя движения из стороны в сторону. Если происходит вытекание горящей жидкости из емкости или технологического оборудования, то тушение нужно начинать именно с места вытекания.

Тушение газов – наиболее сложная операция. Как правило, речь идет о тушении газовых

струй, вытекающих из технологического оборудования, и пригодны для этого разве что порошковые огнетушители.Тушение может быть достигнуто при подаче струи порошка в основание пламени, т. е. в то место, откуда вытекает газ. Наиболее эффективно тушение средней частью струи, поскольку при этом уже достигается хороший распыл частиц огнетушащего порошка, а их кинетическая энергия еще достаточно высока для того, чтобы можно было сбить пламя.

Электрооборудование, находящееся под напряжением до 1 000 В, можно тушить с расстояния не менее 1 м при помощи порошковых и углекислотных огнетушителей. Огнетушащее вещество подается непосредственно в очаг горения. После завершения тушения оборудование желательно обесточить, для предотвращения повторного возгорания (как и в случае тушения любых других веществ и материалов, не вступающих в химическое взаимодействие с водой) потушенную поверхность полезно полить водой (для этого можно использовать любые водоисточники, а также водные огнетушители). Если есть только водные или пенные огнетушители, то оборудование перед тушением нужно обесточить.

Особенность тушения пожаров в закрытых помещениях состоит в том, что обычно существует сильное задымление, ухудшается видимость, затрудняется дыхание либо атмосфера становится непригодной для него. Поэтому особенно важно постараться воспользоваться огнетушителем как можно скорее. Для тушения пожаров внутри помещений, где нет людей, обычно наиболее приемлемы порошковые огнетушители. Разумеется, нужно тушить так, чтобы самому не пострадать от порошкового облака. Если в помещении находятся люди, то лучше воспользоваться водными или воздушно-пенными огнетушителями (кроме случаев, когда горят электроприборы, включенные в сеть). Не стоит пользоваться внутри таких помещений и углекислотными огнетушителями: значительное снижение концентрации кислорода в воздухе опасно для жизни. Еще одна опасность, подстерегающая пользователя углекислотного огнетушителя, заключается в том, что при переходе в газообразное состояние углекислота поглощает значительное количество теплоты и, держась незащищенной рукой за раструб огнетушителя, ее можно обморозить.

Принимая во внимание достаточно высокий уровень автомобилизации граждан и организаций, а также большой интерес к данному вопросу, заметим, что еще 8 октября 1997 г. Кабинет Министров Украины издал Постановление №1128 «Об обеспечении транспортных средств первичными средствами пожаротушения». Этим Постановлением утвержден «Перечень транспортных средств и нормы их оснащения огнетушителями». В соответствии с ним, к примеру, легковые автомобили и пассажирские транспортные средства для перевозки не более 8 человек должны оснащаться одним огнетушителем типа «ОП-2», а двухосные грузовые автомобили – одним огнетушителем «ОП-2» или «ОУ-5». О том, как эти огнетушители называются в соответствии с новыми нормативами, рассказано ниже.

Если загорелся двигатель, то для тушения лучше всего подойдет порошковый огнетушитель. Струю огнетушащего порошка нужно направлять непосредственно в очаг горения. Если часть горючего пролита на землю, то нужно вначале потушить сам пролив, а уже потом тушить жидкость в месте ее вытекания. Если имеет место горение в салоне (кабине) автомобиля, то тушение лучше всего осуществлять при помощи водного или порошкового огнетушителя, находясь при этом вне салона (кабины) и держась подальше от топливного бака.

Неэффективность применения огнетушителя может быть обусловлена также слишком большими размерами очага пожара. Если есть сомнение в возможности подавления горения одним огнетушителем, можно попробовать потушить его при помощи 2–3 и более изделий. Порошковые и углекислотные огнетушители следует приводить в действие одновременно (особенно при тушении пожаров классов В и С), а водные и воздушно-пенные можно применять и последовательно.

Таблица 3 . Категорирование помещений по взрывопожарной опасности согласно ОНТП 24-86

Категория помещения	Характеристика веществ и материалов, обращающихся в помещении
А	Горючие газы, легковоспламеняющиеся жидкости с температурой вспышки не выше 28 °С в таком количестве, при котором они способны образовывать взрывоопасные паро-газовые смеси, при воспламенении которых развивается расчетное избыточное давление взрыва в помещении, превышающее 5 кПа. Вещества и материалы, способные взрываться и гореть при взаимодействии с водой, кислородом воздуха или друг с другом в таком количестве, что расчетное избыточное давление взрыва в помещении превышает 5 кПа.
Б	Горючая пыль или волокна, легковоспламеняющиеся жидкости с температурой вспышки выше 28 °С, горючие жидкости в таком количестве, при котором они могут образовывать взрывоопасные пылевоздушные смеси, при воспламенении которых развивается расчетное избыточное давление взрыва в помещении, превышающее 5 кПа.
В	Горючие и трудногорючие жидкости, твердые горючие и трудногорючие вещества и материалы (в том числе пыль и волокна), вещества и материалы, способные при взаимодействии с водой, кислородом воздуха или друг с другом только гореть, при условии, в которых они находятся или пребывают в обращении, не относятся к категориям А и Б.
Г	Негорючие вещества и материалы в горячем, нагретом или расплавленном состоянии, процесс обработки которых сопровождается выделением лучистого тепла, искр и пламени; горючие газы, жидкости и твердые вещества, сжигаемые или утилизируемые в качестве топлива.
Д	Негорючие вещества и материалы в холодном состоянии. Допускается относить к категории Д помещения, в которых находятся горючие жидкости в системах смазки, охлаждения и гидропривода оборудования при количестве не более 60 кг в единице оборудования при давлении не выше 0,2 МПа, кабельные электропроводки к оборудованию, отдельные предметы мебели на местах.

Новые документы

2 апреля прошлого года Министерством Украины по вопросам чрезвычайных ситуаций и по делам защиты населения от последствий Чернобыльской катастрофы издан приказ под № 151 «Об утверждении типовых норм положенности огнетушителей», зарегистрированный в Министерстве юстиции Украины 29 апреля под № 554/9153. В тот же день подписан приказ МЧС № 152 «Об утверждении правил эксплуатации огнетушителей», который тогда же зарегистрирован Минюстом под № 555/9154. Кроме того, 1 октября введен в действие национальный стандарт Украины ДСТУ 4297:2004 Пожарная техника. Техническое обслуживание огнетушителей. Общие технические условия. Этим документам присвоены шифры нормативных актов по пожарной безопасности –НАПБ Б.03.001-2004 и НАПБ Б.01.008-2004 соответственно.

«Типовые нормы положенности огнетушителей»

В Украине действует множество отраслевых норм, в которых изложены требования к оснащению различных объектов огнетушителями, причем многие из этих документов были разработаны не один десяток лет назад и содержат устаревшие требования. Например, требуют устанавливать морально устаревшие и снятые с производства огнетушители химические пенные («ОХП-10»). Если отраслевые нормы были неприменимы в данном конкретном случае, то «Правилами пожарной безопасности в Украине» предписывалось оснащать объекты в соответствии с требованиями приложения № 3 к этому документу. Разработанные «Типовые нормы положенности огнетушителей» распространяются на «производственные, складские, лабораторные, административные и бытовые здания, помещения объектов различного назначения, общественные здания и сооружения и предназначены для выбора типа огнетушителей и определения их необходимого количества для оснащения указанных объектов».

Они не распространяются на «здания, сооружения и помещения, в которых хранятся, производятся или обращаются взрывчатые вещества и средства подрыва, сильнодействующие ядовитые вещества, радиационные и бактериологические средства», «подземные сооружения предприятий горнодобывающей промышленности», «электроподвижной состав и подземные сооружения метрополитенов», а также «дорожные транспортные средства и транспортные средства железнодорожного, воздушного, речного и морского транспорта».

Министерствам и другим центральным органам исполнительной власти, не возбраняется разрабатывать отраслевые нормы положенности огнетушителей с учетом «специфических условий и особенностей пожарной опасности производств». Такие нормы должны «утверждаться в установленном порядке после согласования с Государственным департаментом пожарной безопасности МЧС Украины». При этом их требования должны быть не ниже требований, установленных цитируемыми нормами, а также не должны противоречить им. Таким образом, учитывая наличие «Типовых норм положенности огнетушителей» в перечне документов, зарегистрированных Минюстом, великое множество объектов придется переоснастить огнетушителями, чтобы они соответствовали требованиям «Типовых норм».

«Правила эксплуатации огнетушителей»

Этот документ обязателен для исполнения предприятиями, учреждениями и организациями независимо от вида их деятельности и формы собственности, а также должностными лицами, гражданами Украины, иностранными гражданами и лицами без гражданства, пребывающими на территории Украины. «Правила эксплуатации огнетушителей» устанавливают «общие требования к эксплуатации огнетушителей общего назначения на объектах защиты огнетушителями».

Документ не распространяется на «объекты, в которых хранятся, перерабатываются или обращаются взрывчатые вещества и средства подрыва», «объекты военного назначения», «защитные сооружения гражданской обороны», «подземные сооружения предприятий горнодобывающей промышленности», «электроподвижной состав и подземные сооружения метрополитенов», равно как и «дорожные транспортные средства и транспортные средства железнодорожного, воздушного, речного и морского транспорта».

Как и в случае «Типовых норм положенности огнетушителей», разрешается при необходимости разрабатывать отраслевые правила эксплуатации огнетушителей, которые не должны противоречить цитируемым «Правилам эксплуатации огнетушителей» и содержать «заниженные» по сравнению с ними требования.

ДСТУ 4297:2004

ДСТУ 4297:2004 интересует в первую очередь тех, кто занимается производством и (или) техническим обслуживанием огнетушителей общего назначения, сертифицированных в Украине и соответствующих требованиям ДСТУ 3675-98 Пожарная техника. Огнетушители переносные. Общие технические требования и методы испытаний или ДСТУ 3734-98 (ГОСТ 30612-99) Пожарная техника. Огнетушители передвижные. Общие технические требования и ГОСТ 12.2.037-78 ССБТ. Техника пожарная. Требования безопасности. Стандарт распространяется на огнетушители, находящиеся в эксплуатации, и устанавливает общие технические требования к проведению их технического обслуживания. Не распространяется он на «огнетушители специального назначения (лесные, авиационные, шахтные, ранцевые, а также огнетушители, пригодные для тушения металлов и веществ, горение которых может происходить без доступа воздуха) и огнетушители разового использования». Стандарт велено применять «всем субъектам хозяйствования независимо от форм собственности и подчиненности, осуществляющим техническое обслуживание огнетушителей».

Терминология

Поскольку в названных выше вновь изданных нормативных документах упоминается ряд специфических понятий (в том числе таких, которые не использовались ранее), позволим себе привести ряд содержащихся в них терминов и определений.

★ **Огнетушитель** – техническое средство, предназначенное для прекращения горения подачей огнетушащего вещества, содержащегося в его корпусе, под действием избыточного давления, по массе и конструктивным особенностям пригодное для транспортировки и применения человеком.

★ **Огнетушитель общего назначения** – огнетушитель, предназначенный для обеспечения противопожарной защиты объекта.

★ **Огнетушитель специального назначения** – огнетушитель, предназначенный для обеспечения противопожарной защиты объекта со специфическими условиями эксплуатации и (или) особенностями пожарной опасности производства и (или) по конструктивному исполнению отличающийся от огнетушителя общего назначения.

★ **Объект защиты огнетушителем** (огнетушителями) – движимое или недвижимое имущество юридического и физического лица, относительно которого установлены требования пожарной безопасности и которое требует наличия огнетушителя (огнетушителей) как элемента его защиты от пожарной опасности.

★ **Эксплуатация огнетушителя** – стадия жизненного цикла огнетушителя, на которой реализуется и обеспечивается его работоспособность. К стадиям эксплуатации огнетушителя относятся начало его эксплуатации, хранение, транспортировка, ожидание применения по назначению, применение по назначению, техническое обслуживание, а также завершение эксплуатации.

★ **Жизненный цикл огнетушителя** – промежуток времени от изготовления до завершения эксплуатации огнетушителя.

★ **Начало эксплуатации огнетушителя** – календарная дата, проставленная отделом технического контроля производителя в паспорте и маркировке огнетушителя.

★ **Хранение огнетушителя при эксплуатации** – содержание огнетушителя в снаряженном состоянии в отведенном для его хранения месте в течение заданного срока.

★ **Транспортировка огнетушителя при эксплуатации** – перемещение огнетушителя в снаряженном состоянии с применением, при необходимости, транспортных и грузоподъемных средств.

★ **Ожидание применения по назначению** – наличие огнетушителя на объекте (защиты огнетушителем) в состоянии, пригодном для применении по назначению, в отведенном для его размещения месте.

★ **Техническое обслуживание огнетушителя** – комплекс операций, направленных на проверку огнетушителя и обеспечение его работоспособности в режимах ожидания применения по назначению, транспортировки и хранения, или на принятие решений по ремонту или снятию его с эксплуатации.

★ **Техническая диагностика огнетушителя** – стадия технического обслуживания, целью которой является определение технического состояния огнетушителя, поиск неисправности и принятие решения относительно его ремонта, технического освидетельствования, перезарядки или завершения его эксплуатации.

★ **Техническое освидетельствование огнетушителя** – стадия технического обслуживания, цель которой – установить отсутствие повреждений, исправность корпуса и (или) баллона с газом-вытеснителем, проверить их прочность проведением гидравлического испытания и принять решение о возможности его дальнейшей эксплуатации.

★ **Перезарядка огнетушителя** – стадия технического обслуживания, цель которой – заменить заряд огнетушащего вещества и (или) газ-вытеснитель в его корпусе.

★ **Завершение эксплуатации огнетушителя** –календарная дата в документе, свидетельствующем о невозможности восстановления работоспособности огнетушителя с показателями качества, предусмотренными техническими требованиями к нему.

★ **Условия эксплуатации огнетушителя** – совокупность факторов, действующих на огнетушитель при его эксплуатации.

★ **Ввод огнетушителя в эксплуатацию** – событие, фиксирующее готовность огнетушителя к ожиданию применения по назначению на объекте защиты огнетушителем и документально оформленное в установленном порядке.

★ **Гарантийный срок эксплуатации** – промежуток времени, установленный производителем или пунктом технического обслуживания огнетушителей и указанный в паспорте и на маркировке огнетушителя, в течение которого гарантируется его работоспособное состояние при условии соблюдения потребителем требований инструкции по эксплуатации.

★ **Работоспособное состояние огнетушителя** – состояние огнетушителя, при котором значения параметров, характеризующих его способность выполнять заданные функции, соответствуют требованиям нормативных и эксплуатационных документов.

★ **Осмотр огнетушителя** – первичная, а также периодическая проверка, проводящаяся визуально лицом, ответственным за пожарную безопасность объекта, с целью установления соответствия внешнего вида огнетушителя требованиям паспорта, правильности его размещения, наличия неповрежденной пломбы и устройства блокировки, отсутствия механических повреждений и следов коррозии, наличия рабочего давления (для закачного огнетушителя), а также принятия решения о необходимости его технического обслуживания или возможности дальнейшего ожидания применения по назначению в соответствии с эксплуатационными документами.

★ **Ремонт огнетушителя** – стадия технического обслуживания, направленная на замену поврежденных и (или) изношенных деталей и составных единиц огнетушителя, ставших непригодными.

★ **Снятие огнетушителя с эксплуатации** – событие, фиксирующее невозможность или нецелесообразность дальнейшего ожидания применения огнетушителя по назначению или его технического обслуживания и документально оформленное в установленном порядке.

★ **Огнетушащее вещество** – химическое вещество или смесь, по своим физико-химическим свойствам пригодная к применению в технических средствах с целью прекращения горения.

★ **Заряд огнетушащего вещества** – количество огнетушащего вещества, содержащегося в корпусе огнетушителя, которое выражают в единицах массы (килограммах).

★ **Номинальный заряд огнетушащего вещества** – заряд огнетушащего вещества, относительно которого устанавливают его предельные значения.

★ **Фактический заряд огнетушащего вещества** – заряд огнетушащего вещества, определенный измерением с допустимой погрешностью.

★ **Коэффициент наполнения огнетушителя** – отношение массы огнетушащего вещества (в килограммах) к обьему (в литрах) корпуса огнетушителя.

★ **Регенерация огнетушащего вещества** – технологический процесс восстановления физико-химических свойств огнетушащего вещества с целью его дальнейшего использования по назначению.

★ **Утилизация огнетушащего вещества** – технологический процесс переработки огнетушащего вещества, не подлежащего регенерации, с целью использования его в других сферах хозяйственной деятельности, не связанных с процессами прекращения горения.

★ **Лицо, ответственное за пожарную безопасность объекта** – лицо, назначенное приказом администрации объекта и имеющее полномочия для размещения и осуществления осмотра огнетушителей на объекте, организации их технического обслуживания, ведения эксплуатационных документов и обучение работников объекта правилам применения огнетушителей.

★ **Пункт технического обслуживания огнетушителей (ПТОО)** – субъект хозяйствования, осуществляющий техническое обслуживание огнетушителей, удостоверяющий их исправность и имеющий на это право в соответствии с действующим законодательством.

★ **Наставление по техническому обслуживанию огнетушителей** – нормативный документ, содержащий сведения о практических приемах и методах технического обслуживания огнетушителя.

★ **Каталог деталей и составляющих единиц огнетушителя** – документ, содержащий перечень деталей и составляющих единиц огнетушителя с иллюстрациями и сведения об их количестве, размещении, взаимозаменяемости, конструктивных особенностях и материалах.

★ **Специальное обучение** – подготовка, переподготовка, повышение квалификации по учебным планам и программам, утвержденным в установленном порядке.

Обозначение огнетушителей

Хотелось бы обратить внимание на обозначение огнетушителей, используемое при их маркировке и в «Типовых нормах положенности огнетушителей». «ВВ» (по-русски маркируется «ОВ») означает «вогнегасник водяний», «ВВП» («ОВП») – «вогнегасник водопінний», «ВВПА» («ОВПА») – «вогнегасник водопінний аерозольний», «ВВК» («ОУ») – «вогнегасник вуглекислотний», «ВП» («ОП») – «вогнегасник порошковий».

После обозначения типа огнетушителя ставится цифра, означающая массу содержащегося в нем огнетушащего вещества, выраженную в килограммах. Цифра после обозначения аэрозольного водопенного огнетушителя означает массу его заряда, выраженную в граммах.

Георгий Минин

Аерозольне пожежогасіння

Основні вимоги проекту ДСТУ

«Пожежна техніка. Установки аероМзольного пожежогасіння. Генератори вогнегасного аерозолю. Загальні технічні вимоги та методи випробувань».

Аерозольне пожежогасіння виникло як альтернатива застосування озоноруйнівних речовин в установках газового пожежогасіння. Спосіб пожежогасіння заснований на використанні процесу згорання деяких видів твердих палив, в результаті якого утворюється суміш газів та конденсованих твердих часток мікронних розмірів. Це дозволяє усунути основні недоліки, які мають традиційні порошки, і тим самим підвищити ефективність і надійність протипожежного захисту об'єктів, що захищаються установками аерозольного пожежогасіння.

Генератором вогнегасного аерозолю (ГВА) в загальному вигляді прийнято вважати технічний засіб, що включає в себе аерозолеутворювальну сполуку (АУС), корпус та вузол запуску.

ГВА застосовується для гасіння пожеж підкласу А2 і класу В, а також локалізації пожеж підкласу А1 за ГОСТ 27331-87 (СТ СЕВ5637-86).

До явних переваг ГВА слід віднести: малу елементну базу, високу надійність експлуатації систем, можливість використання в широкому діапазоні температур та агресивних середовищах. Порівняно з газовими системами пожежогасіння системи аерозольного пожежогасіння мають невелику вартість та нескладні в технічному обслуговуванні.

Основні фактори, завдяки яким аерозоль здійснює локалізацію та гасіння пожеж:

★ хімічне гальмування ланцюгової реакції горіння, що здійснюється під дією каталітично-активних твердих частинок аерозолю;

★ поглинання тепла пожежі та охолодження палаючого середовища завдяки термічному розпаду й випаровуванню твердих частинок аерозолю;

★ утворення над поверхнею горіння локальних поверхневих тонкошарових низькокисневих зон завдяки продукуванню з твердих частинок аерозолю (в разі їх термічного розпаду) інертних газів (азоту та діоксиду вуглецю).

Установки аерозольного пожежогасіння найбільш придатні для захисту таких об`єктів: окремо розташовані гаражі, паркінги, суднові трюми, закриті гартівні ванни, автосалони, котельні та дизельні, тимчасові будівельні споруди, кабельні тунелі та приміщення, що знаходяться на цокольних поверхах. Малогабаритні генератори «Допінг-2», МАГ-2М використовують для гасіння пожеж в підкапотному просторі автомобілів та електрощитах.

Доцільність застосування ГВА для захисту серверних і банківських сховищ є сумнівною. Оскільки, у разі попадання аерозолеутворювальної сполуки (АУС) всередину системного блоку виходить з ладу вентилятор, що, в свою чергу, приводить до перегріву та пошкодження плат. Крім того в разі несвоєчасного прибирання аерозолю з поверхні обладнання (доба і більше) за рахунок вологості відбувається спікання аерозолю в важкодоступних місцях.

До недоліків ГВА слід віднести:

★ наявність високотемпературної зони безпосередньо біля ГВА, в результаті чого можуть постраждати обладнання, ланцюги управління систем гасіння, персонал (якщо ГВА встановлені з порушенням вимог експлуатації);

★ під час роботи ГВА видимість знижується практично до нуля, що ускладнює евакуацію персоналу;

★ ГВА не рекомендують застосовувати в місцях масового перебування людей (більше 50 чоловік);

★ ГВА неефективні під час гасіння лужноземельних металів; твердих речовин, горіння яких супроводжується тлінням (деревина, сіно, солома, борошно, зернові, папір, тканини та ін.); речовин, що горять без доступу повітря; газових трубопроводів під тиском; електрообладнання під напругою більше 1000 В; порошкових металів і хімічно активних металів (магній, титан, цирконій та ін.); хімічних речовин, схильних до термічного розпаду;

★ можливість хибного спрацювання димових сповіщувачів в суміжних приміщеннях. Для виключення хибних спрацювань потрібно забезпечити надійність приладів контролю та управління, номінальні значення струму контролю, що встановлені в технічній документації (як правило, 50 мА).

Найбільш широко в Україні застосовуються генератри типу АГС-6 і «ОСА», які мають низьку температуру згорання АУС.

Сьогодні на ринку України з`явилися нові генератори вогнегасного аерозолю типу «АГС» одинадцятої та дванадцятої серії.

Перевагами нових ГВА є низька вихідна температура аерозолю (50 °С на відстані 0,5 м від вихідного отвору ГВА), збільшення інтенсивності аерозолеутворення, компактність.

АГС-11 з успіхом застосовуються в широкому інтервалі температур (від мінус 50 до 50 °С) для захисту електрошаф систем автоматики й можуть гасити їх без від'єднання від мережі живлення напругою до 40 кВ. Також застосовуються в автомобільній та авто-

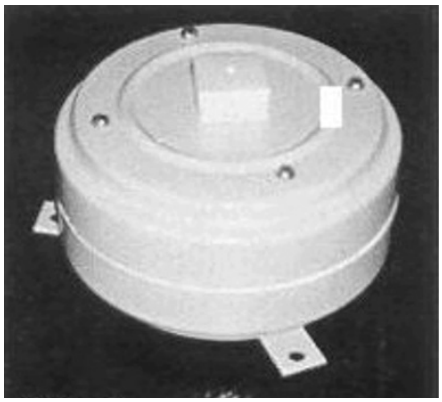


Рис. 1. Зовнішній вигляд генератора вогнегасного аерозолю АГС-11

транспортній техніці, для гасіння тягових електродвигунів тощо.

АГС-12 призначаються для захисту приміщень будь-якого об'єму, з умовним коефіцієнтом негерметичності менше 0,1 %. У подальшому передбачається, що один генератор дванадцятої серії буде здатний захистити приміщення об'ємом до 200 м^3. Подібні АГС призначаються для захисту машинних залів, приміщень, насичених високотехнологічним обладнанням,

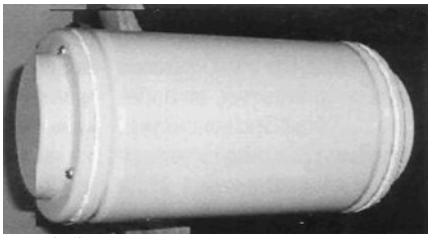


Рис. 2. Зовнішній вигляд генератора вогнегасного аерозолю АГС-12

кабельних поверхів і тунелів, складів, у тому числі для зберігання ЛЗР та ПММ, автопаркінгів.

УкрНДІПБ МНС України розроблений проект ДСТУ «Пожежна техніка. Установки автоматичного пожежогасіння. Генератори вогнегасного аерозолю. Загальні технічні вимоги та методи випробувань» (далі – стандарт), який зараз знаходиться на затвердженні в Держспоживстандарті України.

Цей стандарт поширюється на генератори вогнегасного аерозолю з використанням твердопаливних аерозолеутворювальних сполук, які призначені для отримання вогнегасного аерозолю та подачі його в приміщення, що захищається, з метою локалізації або ліквідації пожежі.

Стандарт не поширюється на генератори вогнегасного аерозолю, які призначені для захисту транспортних засобів та об'єктів, що проектуються за спеціальними нормативними документами.

Обов'язкові вимоги до показників якості генераторів викладені у розділі 5, а обов'язкові вимоги до методів випробувань генераторів за цими показниками – у розділі 6 цього стандарту.

Стандарт придатний для цілей сертифікації

За цим стандартом:

Генератор вогнегасного аерозолю – це пристрій для одержання вогнегасного аерозолю з заданими параметрами та подавання його у захищуване приміщення.

Аерозолеутворювальна сполука – це композиція спеціального складу, яка здатна до самостійного горіння без доступу повітря з утворенням вогнегасного аерозолю.

Вогнегасний аерозоль (ВА) – це продукти горіння АУС, які забезпечують вогнегасну дію під час гасіння пожежі.

Генератори поділяються:

★ за температурою ВА на зрізі випускного отвору на типи:

I – температура перевищує 500 °С ;

II – температура складає від 130 °С до 500 °С ;

III – температура складає менше 130 °С.

★ за конструктивним виконанням на типи:

Р – з роз'ємним від корпуса ГВА пусковим пристроєм;

Н – не роз'ємним від корпуса ГВА пусковим пристроєм.

★ за способом приведення в дію на типи:

Е – спрацьовуючи від електричного сигналу ;

Т – спрацьовуючи від теплового сигналу ;

К – з комбінованим пуском.

Генератори повинні відповідати вимогам цього стандарту, технічній документації на конкретний вид генератора та виготовлятися за конструкторською документацією, яка затверджена у встановленому порядку.

Характеристики

Основні параметри ГВА повинні відповідати значенням, наведеним в табл. 1.

Таблиця 1. Основні параметри ГВА

Параметри ГВА	Значення параметрів ГВА
Маса спорядженого ГВА, кг	згідно технічній документації на ГВА
Маса АУС в спорядженому генераторі, кг, не більше	15,0
Вогнегасна концентрація ВА, що утворюється при роботі ГВА, кг/м^3: - для ГВА типу I (за температурою), не більше - для ГВА типу II та III (за температурою), не більше	 0,2 0,7
Тривалість подавання вогнегасного аерозолю, с, не більше	200
Інерційність (для ГВА з приведенням в дію від електричного сигналу), с, не більше	5

При цьому встановленні виробником та вказані у документації відхилення значень параметрів ГВА: для маси спорядженого ГВА та маси АУС не повинні перевищувати ±20 %; для тривалості подавання вогнегасного аерозолю ±15 %; для інерційності ±10 %.

Габаритні розміри ГВА та вогнегасна здатність ГВА, що відповідає максимальному об'єму приміщення, з відповідним ступенем негерметичності, в якому генератор забезпечує утворення вогнегасної концентрації для гасіння модельних вогнищ пожежі класу А та В, повинні відповідати значенням, встановленим виробником і вказаним в технічній документації на ГВА.

Радіус або довжина температурних зон, що утворюються безпосередньо біля ГВА під час його роботи, відносно зрізу випускного отвору ГВА повинні бути не більше:

0,6 м – для температурної зони з температурою 400 °С ;

1,1 м – для температурної зони з температурою 200 °С ;

2,5 м – для температурної зони з температурою 75 °С .

Параметри електросигналу для запуску ГВА та контролю стану працездатності ланцюга пускового пристрою ГВА повинні відповідати значенням, наведеним в технічній документації. Напруга електросигналу для запуску ГВА не повинна перевищувати 36 В. Електричний пуск ГВА не повинен здійснюватись електросигналом для контролю стану працездатності ланцюга вузла пуску.

Електричній опір між корпусом ГВА та клемами, які служать для подачі електричного сигналу для пуску ГВА, за нормальних кліматичних умов згідно з ГОСТ 15150 повинен становити не менше 1 МОм.

Наскрізні тріщини, прогари і горіння зовнішньої поверхні корпусу ГВА після закінчення його роботи не допускаються. Допускається пошкодження лакофарбового покриття корпусу ГВА.

ГВА повинні бути стійкими до дії вібрації з амплітудою та частотою, встановленими виробником і вказаними в технічній документації на ГВА.

Захист від корозії металевих поверхонь ГВА слід здійснювати нанесенням лакофарбових, металевих або неметалевих неорганічних покриттів відповідно до ГОСТ 9.032, ГОСТ 9.303.

Лакофарбові покриття, нанесені на ГВА, повинні відповідати вимогам ГОСТ 12.4.026.

Вимоги надійності

Імовірність безвідмовної роботи згідно з ГОСТ 27.410 та ДСТУ 2860 після одного року експлуатації ГВА повинна бути не менше 0,94 (бракувальний рівень) при приймальному рівні, який дорівнює 0,98.

Відмовою слід вважати:

★ неможливість приведення ГВА до дії пусковим сигналом з параметрами згідно з технічною документацією на ГВА;

★ інерційність спрацювання ГВА більша за регламентовану технічною документацією на ГВА;

★спрацювання ГВА під дією контрольного сигналу.

Термін служби ГВА регламентований технічною документацією на нього, але строк експлуатації не може бути нижчим 5 років. Гарантований строк зберігання ГВА – 5 років.

Вимоги стійкості до зовнішніх впливів

ГВА за кліматичним виконанням та категорією розміщення в частині впливу кліматичних факторів зовнішнього середовища повинні відповідати вимогам ГОСТ 15150, умовам експлуатації та зберігати свою працездатність.

Діапазон температур зберігання та експлуатації ГВА для кліматичного виконання У, згідно з ГОСТ 15150, повинен складати від мінус 20 до 50 °С, для кліматичного виконання УХЛ, згідно з ГОСТ 15150, повинен складати від мінус 50 до 50 °С.

Працездатність ГВА повинна зберігатися після перевезення будь-яким видом транспорту за умови дотримання правил перевезення вантажу на транспорті цього виду. Працездатність ГВА повинна зберігатись після дії транспортного трясіння з прискоренням 30 м/с^2 і частотою ударів від 80 до 120 за хвилину протягом 3 год. Умови транспортування ГВА у частині дії кліматичних чинників повинні відповідати умовам зберігання – група 4 (Ж2) згідно з ГОСТ 15150, але для нижнього значення температури мінус 40 °С.

Вимоги до сировини та матеріалу

Деталі, комплектувальні вироби і матеріали, що використовуються для виготовлення ГВА, повинні відповідати технічній документації на них.

ГВА повинні мати гігієнічний сертифікат Міністерства охорони здоров'я України на відповідність ВА санітарно-гігієнічним нормам України.

Матеріали, що використовуються в ГВА, повинні відповідати вимогам чинних нормативних документів щодо відповідних матеріалів.

Комплектність

До комплекту поставки ГВА, спорядженого вузлом запуску повинні входити:

★ керівництво з експлуатації;

★ паспорт;

★ кріплення для ГВА.

Примітка – Для генератора, не спорядженого вузлом запуску, в комплект поставки повинен входити вузол запуску.

У технічній та експлуатаційній документації на ГВА, повинні бути вказані:

★ Маса спорядженого генератора, кг;

★ Маса АУС в спорядженому генераторі, кг;

★ Інтервал температур експлуатації і зберігання.

★ Максимальний умовно герметичний об'єм приміщення з ступенем негерметичності, в якому генератор забезпечує гасіння модельних вогнищ пожежі, м^3.

★ Вогнегасна концентрація аерозолю, що утворюється під час роботи ГВА, кг/м^3.

★ Тривалість подавання вогнегасного аерозолю, с.

★ Інерційність ГВА (час спрацьовування), с.

Параметри електричного сигналу (величина напруги, сила струму, його тип і тривалість дії), що необхідні для запуску ГВА.

Параметри електричного сигналу (напруга, сила струму, його тип і тривалість дії), що необхідні для контролю стану ланцюга електричного запуску під час експлуатації ГВА у складі установки аерозольного пожежогасіння.

Габаритні розміри генератора.

Дані про показники надійності роботи генератора відповідно до ДСТУ 3004 або ГОСТ 27.410.

Параметри відповідно до вимог п. 1.3 ГОСТ 12.4.009, що визначають галузь застосування генератора на об'єктах і стійкість його до впливу зовнішніх впливів.

Умови транспортування і зберігання

Розміри температурних зон з температурою, що перевищує 75, 200 і 400 °С, що утворюються під час роботи ГВА.

Клас небезпеки генератора відповідно до ГОСТ 19433, ГОСТ 26319-84 .

Температура продуктів горіння АУС, що утворюється на зрізі випускного отвору ГВА.

Рівень вибухозахисту генератора (у разі застосування ГВА у вибухонебезпечних зонах).

Маркування

Кожний ГВА маркують у будь-який спосіб, що забезпечує чіткість та зберігання маркування протягом усього терміну служби, із зазначенням:

★ товарного знаку підприємства-виробника;

★ позначення ГВА;

★ об'єму приміщення, у якому ГВА забезпечує вогнегасну здатність;

★ дати виготовлення;

★ номера партії;

★ номера ТУ, відповідно якого виготовлено ГВА;

★ знаку відповідності згідно з ДСТУ 2296 про підтвердження факту сертифікації продукції.

Транспортне маркування – згідно з ГОСТ 14192.

Пакування

Пакування повинне захищати ГВА від механічних пошкоджень і забруднення.

Вид і спосіб пакування встановлюють за узгодженням між споживачем та виробником і зазначають у нормативному документі на конкретний тип ГВА.

До кожної пакувальної одиниці прикріплюють ярлик із зазначенням:

★ назви підприємства-виробника або його товарного знака та його юридичної адреси;

★ позначення нормативного документа на конкретний тип ГВА;

★ номера пакувальної одиниці;

★ умовного позначення ГВА;

★ номера партії;

★ дати виготовлення;

★ номера пакувальника;

★ номера сертифіката відповідності, терміну його дії та назви органу, що його видав.

Ярлик повинен бути прикріплений до пакувальної одиниці способом, що забезпечує його неушкодженість.

Стандартом передбачені обов'язкові випробування ГВА з визначення таких показників якості:

1. Контроль зовнішнього вигляду.
2. Контроль розмірів.
3. Випробування з визначення маси ГВА та маси АУС.
4. Випробування з визначення вогнегасної здатності ГВА, вогнегасної концентрації ВА, інерційності спрацювання ГВА, тривалості подавання ВА, параметрів електричного сигналу при спрацювання ГВА.
5. Випробування з визначення розмірів температурних зон ГВА, температури ВА на зрізі випускного отвору ГВА під час роботи та перевірка стану корпусу ГВА після закінчення роботи.
6. Випробування на відсутність спрацювання ГВА від електросигналу контролю стану працездатності ланцюга пускового пристрою.
7. Випробування на стійкість до дії кліматичних факторів зовнішнього середовища.
8. Випробування на стійкість ГВА до дії вібрації.
9. Випробування з визначення електричного опору між корпусом ГВА та клемами для подачі електричного сигналу на за пуск ГВА (для ГВА з запуском від електричного сигналу).
10. Випробування з оцінки імовірності безвідмовної роботи ГВА.
11. Контроль середнього терміну служби.
12. Контроль відповідності вихідної сировини.
13. Випробування на стійкість до дії транспортного трясіння.

Криницький Я.,
головний спеціаліст НДЦ-1
УкрНДІПБ МНС України
Полозук Р,
науковий співробітник НДЦ-1
УкрНДІПБ МНС України

Системи пожежезахисту: сучасні, надійні, ефективні

Традиційно, і це приємно відзначати, що коли замовники говорять: «ТОВ «Алтосан», мають на увазі професіоналізм і якість виконаних робіт. Це дійсно так, за 16 років роботи на ринку надання протипожежних послуг «Алтосан», потужна виробничо-комерційна фірма, може по праву пишатися своїми здобутками та постійно прагнучи нового, розширюючи сферу послуг, підвищувати їх якість. ТОВ «Алтосан» розробив і виробляє прилади пожежні приймально-контрольні типу «АЛТО 2000», проводить розробку, доопрацювання нормативних документів, щодо систем пожежегасіння, впроваджує нові технології пожежегасіння та пасивного пожежезахисту, розробляє нові концепції застосування традиційних та передових засобів пожежезахисту.

ТОВ «Алтосан» активно співпрацює з Державними закладами та громадськими організаціями, є співзасновником міжнародної асоціації «Пожежна безпека України», «Українського Союзу виробників протипожежної продукції та послуг».

Коротко про продукцію, що виробляє та постачає на ринок України ТОВ «Алтосан»

1. Прилади керування пожежні типу «АЛТО 2000» (ППКП).

ТУ У 16307479.001-99, сертифікат UA1.016.97654-03. Співвідношення, надійність, якість, ціна – порівняно з приладами подібними до «АЛТО 2000», які присутні на ринку України, по багатьом функціональним параметрам свідчить на користь «АЛТО 2000». Можливість створювати за допомогою

Фото 1
Пульсар 1-01

«АЛТО 2000», оптимальну конфігурацію установки пожежегасіння для будь-якого типу об'єкту – від малого автономного, до великого комплексу.

До основного комплекту «АЛТО 2000» входить:

★ Блок «АЛТО 2000 ЦП» (централь пожежна). ППКП на 32 шлейфи. Забезпечує управління пожежегасінням (керуючи блоками «АЛТО 2000 БКП» до 16 напрямків по контрольованій інформаційній лінії. Наявна розвинута світлова та рідкокристалічна індикація, зручні механізми керування, енергонезалежна пям'ять подій, ручне тестування та самотестування.

★ Блок «АЛТО БКП» (блок контрольно пусковий). Виконує в повному об'ємі функції ППКП на 2 шлейфи, забезпечує керування пожежегасінням по 4 пусковим лініям (до 10 А кожна), забезпечує всі обумовлені нормативною базою функції, що є обов'язковими для автоматичних систем пожежегасіння. Наявна зручна світлова індикація та механізми керування, можливість підключення до інформаційної лінії для комплексної роботи з блоком «АЛТО 2000 ЦП» – приладами, що входять до складу системи пожежегасіння.

★ Блок «АЛТО ИБП» (джерело постійного живлення струмом з напругою на 12 В і 24 В).

Номінальний стум навантаження при напрузі 12 В до 1,0 А, при напрузі 24 В до 0,7А; максимальний струм навантаження при напрузі 24 В короткостроково, до 60 с – 10 А. Резервні акумулятори 12 В, 7,5 А/год (3 шт.).

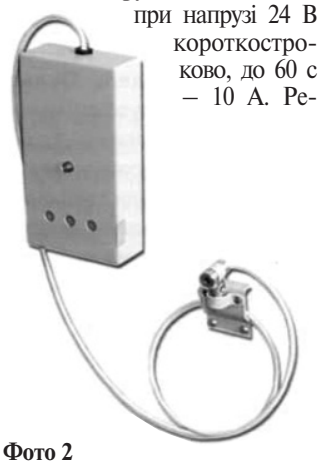


Фото 2
Пульсар1-011

★ Блок «АЛТО ОСЗ» (сповіщувач світлозвуковий) Забезпечує світлове і звукове (голосове) сповіщення людей про пожежу та спрацьовування установки пожежегасіння. Сила звуку сирени не менш 110 дБ. Наявне пульсуюче підсвічене табло з маркуванням попередження події. Напруга живлення становить від 11,8 до 26 В. Струм споживання становить до 0,25 А (звуковий) та до 0,4 А (голосовий).

2. Пожежні оповіщувачі полум'я серій «Пульсар®1» «Пульсар®2»

Фото 3
Пульсар 1-011

Стислі технічні характеристики наведені в табл. 1. та табл. 2.

Струм споживання до 10 мА дозволяє при умові навантажувальної здатності шлейфу та при коефіцієнті запасу 1,5, підключити до одного шлейфу 19 оповіщувачів.

Базова модель **Пульсар®1-01** (фото 1). Чутливий елемент вбудований в корпус. Розетка оповіщувача кріпиться на стіну, стелю, або спеціальний кронштейн, стійку. Оповіщувач кріпиться на розетку трьома гвинтами через монтажні отвори в передній панелі. Після монтажу отвори закриваються засувкою.

Пульсар®1-010, подібний до Пульсар1-01, але чутливий елемент встановлено на лицьовій панелі на поворотному кронштейні, за допомогою якого оптичну вісь чутливого елементу можна скеровувати під кутом до

Фото 4
Пульсар 2-012

площини встановлення оповіщувача. Кут повороту становить: у вертикальній площині ±15, у горизонтальній ±30 кутових градусів.

Пульсар®1-011 (фото 2). Чутливий елемент розташований у малогабаритному корпусі та винесений на

Таблиця 1

Параметр	Діапазон значень	Типове значення
Час спрацьовування (на замовлення)	3,0 –15,0 сек.	4,5 сек.
Стійкість до фонової освітленості: Лампи розжарювання Розсіяне сонячне світло Люмінесцентні лампи, не гірше	 750 лк. 15000 лк. 2500 лк.	 300 лк. 6000 лк.
Напруга живлення	9,0–28,0 В	24,0 В
Струм в режимі чергування	0,28–0,35 мА	0,30 мА
Струм в режимі «Пожежа»	16,0–24,0 мА	20,0 мА
Відстань визначення модельного вогнища ТП5 (нафтопродукти)*	30,0–35,0 м.	32,0 м.
Відстань визначення модельного вогнища ТП6 (спирти)*	12,0–14,0 м.	13,0 м.
Кут зору для Пульсар1 (на замовлення)**	30–120 кутових градуси	120 кутових градуси
Кут зору для Пульсар2 (на замовлення)**	30–90 кутових градуси	90 кутових градуси

*Модельні вогнища ТП5 та ТП6 являють собою кювету з площею палаючої рідини 0,1 м^2.

**За замовленням передбачено зменшення кута зору до 30 кутових градуса

електричному кабелі довжиною до 25 м. Чутливий елемент може закріплятися на кронштейні, його оптична вісь може бути скерована

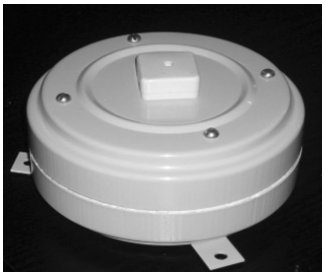


Фото 5
АГС-11/4

відносно площини кронштейна у вертикальній площині ±15, у горизонтальній ±45 кутових градуси. Чутливий елемент можливо встановити в стіновій декоративній панелі, або в панелі підвісної стелі. Таке технічне рішення дозволяє контро-

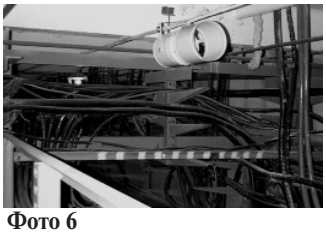


Фото 6
АГС-7/2 в кабельному каналі

лювати зони де необхідно мати невеликі розміри оповіщувача.

Пулсар®1-011П (фото 3). Оповіщувач виконаний у промисловому виконанні. Ступінь захисту оболонки –

Фото 7
АГС-5 після спрацювання

IP55. Чутливий елемент винесений на електричному кабелі, що знаходиться в металорукаві, довжина кабелю до 25 м.

Чутливий елемент встановлюється на поворотному кронштейні. Ущільнення металорукава, що проходить через бокову стінку оповіщувача виконано спеціальним сальником.

Оповіщувач Пульсар®2 (фото 4).

Оповіщувач Пульсар2 випускається в одній модифікації: Пульсар2-012.

Модель Пульсар2-012 виготовляється у промисловому виконанні. Чутливий елемент встановлено всередині електронного блоку. Оптичний сигнал на нього потрапляє по оптоволоконому кабелю, який знаходиться в металорукаві і на вільному кінці якого встановлена приймальна оптична система. Довжина кабелю може сягати до 25 м.

Приймальна оптична система та оптоволоконий кабель мають інтервал робочих температур в межах мінус 50° до плюс 200° за шкалою Цельсія, їх функціювання не пов'язане з використанням електричної енергії, що виключає виділення тепла, та можливість виникнення іскри.

Завдяки такому технічному рішенню стає можливим контролювати зони з широким діапазоном температури, наявністю агресивних компонент, з вибухонебезпечним середовищем.

За правилами «ПУЕ» приймальну оптичну систему та оптоволоконий кабель дозволяється встановлювати у вибухонебезпечних зонах класів (В-1; В-1 а, б, г; ВІІ). Електронний блок дозволено встановлювати в зонах класу В-1 а, б, г.

Пульсари відповідають високим вимогам надійності – так, середній час роботи на відмову становить не менш ніж 60 тис. годин.

Строк працездатності не менш 10 років. Серія Пульсарів1 відповідає вимогам ТУ 4371 - 010 - 26289848 - 01; Пульсарів2
ТУ 4371 - 011 - 26289848 - 01.

3. Генератори вогнегасного аерозолю АГС

Читачі журналу, наші шановні клієнти, прекрасно знають і мали змогу особисто переконатися в перевагах вогнегасних систем, створених на базі генераторів вогнегасного аерозолю типу АГС. Порівняно з традиційними методами гасіння – переваги суттєві.

Компактність, невисока температура потоку аерозолю, простота обслуговування, відсутність впливу на навколишнє середовище, екологічна безпечність продуктів термодеструкції. За оцінкою ступеня токсичності та небезпечності вогнегасний аерозоль представлений продуктами 4 і 3 класу небезпечності. Значний строк придатності (10 років), можливість зручного розташування – все це надає можливість макси-

Фото 8
Робота оперативно-рятувального загону під час гасіння вагону потягу

мально ефективно використати вогнегасні властивості аерозолю, який генерує АГС.

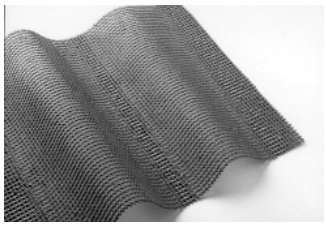


Фото 9

Для читачів, хто вперше знайомиться з АГС, дозволю привести три основних фактори, завдяки яким аерозоль здійснює локалізацію, гасіння пожеж класів: «А»; «В»; «С»; «Е» і їх підкласів.

1. Хімічне гальмування ланцюгової реакції, що здійснюється за рахунок каталітичної комбінації твердих частинок аерозолю.

2. Поглинання тепла пожежі та охолодження вогнища завдяки термічного розпаду та випаровування твердих частинок аерозолю.

3. Утворення локальних поверхневих тонкошарових (до двох міліметрів) низькокісневих зон над поверхнею пожежі завдяки продукуванню з твердих частинок аерозолю, при їх термічному розпаді, інертних газів (N_2; CO_2).

Стислі характеристики АГС зведені в табл. 3.

Генератори нового типу АГС-11 (фото 5) мають вигляд невисокого циліндра у якого є пристрої для кріплення та клеми для підключення вузла запуску, що знаходиться безпосередньо в корпусі АГС. Серія генераторів АГС-11 з успіхом застосовується в електрошафах систем електроавтоматики. АГС-11 з успіхом застосовують в автомобільній та автотракторній техніці, для гасіння тягових електродвигунів та ін. Генератори типу АГС-7; АГС-8; АГС-3; АГС-4, генератори одинадцятої серії можливо встановити в любому положенні корпусу. АГС допускають можливість гасити об'єкти, що знаходяться під напругою живлення до 40 кВ без відключення (фото 6). Всі типи АГС сертифіковані в Україні.

4. Генератори вогнегасного аерозолю оперативного застосування АГС-5

АГС-5 – генератор, який можливо застосувати для гасіння виробничих, торгових, житлових приміщень, транспортних засобів. Таким генератором необхідно споряджати: пости по-

Таблиця 2.

Параметр	Звичайне виконання	Промислове виконання
Габаритні розміри електронного блоку (мм)	150 x 80 x 45	280 x 155 x 70
Габаритні розміри виносного датчика (мм)	12 x 12 x 20	35 x 35 x 78
Вага (кг)	0,6	3,5
Ступінь захисту оболонки електронного блоку	IP41	IP55
Ступінь захисту оболонки виносного датчика	IP50	IP66
Виконання	Нормальне (Н)	Спеціальне (С)
Робочий температурний діапазон в градусах за шкалою Цельсія	Мінус 10, 55	Мінус 50, 55

жежної безпеки, оперативний черговий персонал або охорону, оперативні бойові підрозділи пожежної охорони МНС з метою щонайскорішого застосування в разі винекнення ймовірної пожежі. Доставка АГС-5 на місце в разі виникнення пожежі – займає лічені секунди. Гасіння вогнища починається відразу після запуску АГС-5. Запуск здійснюється вручну за допомогою теркового вузлу запуску.

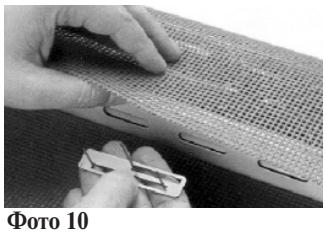


Фото 10

5. Засіб пасивного пожежозахисту – тканина «Hapuflam»

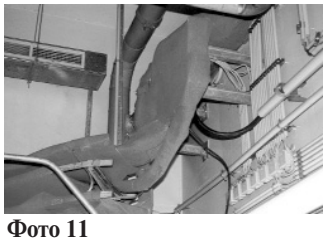


Фото 11

Донедавна, забезпечення вогнестійкості кабельних каналів, тобто можливість їх працездатності в умовах розвинутої пожежі, було складним завданням для проектувальників виробничих, спеціальних, житлових об'єктів, військової техніки. Вогнезахистна тканина «Hapuflam» з успіхом вирішує такі задачі. Один шар тканини яким обгорнутий кабель, кабельний лоток, або пучок дозволяє працювати кабелям при наявності на струмопроводах кабелів напруги 250 В. та навколишній температурі 750° за шкалою Цельсія впродовж 180 хвилин. Випробування проводились у Німеччині під керівництвом доктора технічних наук пана Веше. Методика випробувань відповідала вимогам DIN 4102-12 : 1998-11.

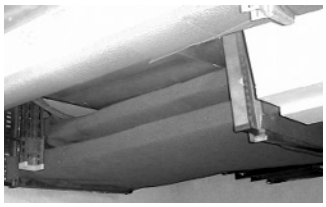


Фото 12

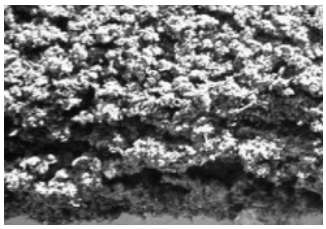


Фото 13

В Україні вперше фахівцям вогнезахистна тканина «Hapuflam» була продемонстрована під час показових випробувань на міжнародній виставці «ПОЖЕКСПО 2004»; Хмельницькій та Рівненській АЕС. Проведені випробування викликали легкий шок у фахівців – кабелі, що раніше не підлягали захисту, лишалися абсолютно неушкодженими, причому впродовж усього випробування на Рівненській АЕС по струмопровідним жилам кабелів протікав електричний струм зі значенням напруги 220 В.

Простота виконання захисного покриття, 100 % контроль якості виконання покриття, незначне навантаження до 1,1 кг. на м^2 площі покриття, можливість не зменшувати струменеві навантаження на кабелі, здійснення в любий час огляду кабельних пучків, можливість легко додати, або вилучити кабель, змінювати конфігурацію лотка, нанесення при мінусовій та плюсовій температурі, гарантована працездатність впродовж 10 років. Ось далеко не всі переваги, які роблять вогнезахистну тканину «Hapuflam» недосяжною для конкурентів (фото 9; 10; 11; 12; 13).

Безперечно ця стаття не може бути повною і відображати всі нюанси п'яти запропонованих Вам, шановний читачу, систем. Надалі ми будемо розкривати якомога повніше кожну з них. Нам цікаво, про яку Ви хотіли б прочитати вже в наступному номері. Чекаємо Ваших пропозицій в редакції журналу та за телефонами і адресою:

ТОВ «Алтосан»
вул. Північна, 5,
м. Київ, 04214.
Тел./факс: (044) 412-00-29.
Тел: (044) 411-97-61;
411-08-33; 411-05-84;
411-49-88.
http://www.altosan.kiev.ua
e-mail: altosan@i.kiev.ua

Пропонуємо нашим читачам комплект:
ДСТУ EN54-1–54-5 : 2003;
ДСТУ EN54-7–54-13: 2004;
ДСТУ 4240 : 2003;
ДСТУ 4312 : 2004.

Євмєньєв Л. О.,
головний фахівець
ТОВ «Алтосан»

Таблиця 3.

Тип АГС	Маса аерозолеобразуючого заряду (кг)	Час роботи (сек.)	Температура струменя аерозолю на відстані 0,5 м від генератора не більше, (^{0}C)	Діаметр х довжина (мм)	Об'єм, що захищає АГС (м^3)	Маса АГС (кг)	Інтервал температур за яких може працювати АГС (^{0}C)
АГС-3	0,32	19	30	122 х 65	3,2	1,2	Мінус 50 до 50
АГС-4/2	1,6	40	120	167 х 179	21,0	5,3	Мінус 50 до 50
АГС-5	2,7	24	170	210 х 112	60,0	4,6	Мінус 50 до 50
АГС-6	3,4	35	75	167 х 420	52,0	14,3	Мінус 50 до 50
АГС-7/1	3,25	80	270	172 х 360	65	5,8	Мінус 50 до 50
АГС-7/2	6,7	160	270	172 х 500	134,0	10,5	Мінус 50 до 50
АГС-8/1	3,25	80	120	220 х 220	65,0	10,0	Мінус 50 до 50
АГС-8/2	6,7	160	120	220 х 350	134,0	19,0	Мінус 50 до 50
АГС-11/1	0,1	7	75	122 х 25	2,0	0,5	Мінус 50 до 50
АГС-11/2	0,16	10	75	124 х 32	3,2	0,7	Мінус 50 до 50
АГС-11/3	0,3	20	75	124 х 52	6,0	1,2	Мінус 50 до 50
АГС-11/4	0,9	25	75	165 х 72	18,0	2,5	Мінус 50 до 50
АГС-11/5	1,5	36	90	187 х 94	30,0	4,5	Мінус 50 до 50
АГС-11/6	2,0	36	90	187 х 94	50,0	4,5	Мінус 50 до 50

НОВОСТИ

Україна та Швейцарія інтенсифікують співпрацю у боротьбі з „брудними" грошима

Україна та Швейцарія шукатимуть додаткові законодавчі можливості для співпраці двох країн у боротьбі з відмиванням коштів, зокрема, щодо конфіскації активів, здобутих злочинним шляхом. Про це йшлося під час робочої зустрічі заступника Міністра юстиції Василя Мармазова з заступником Федерального прокурора Швейцарської Конфедерації по міжнародній і континентальній співпраці Марією Шнеблі.

Як повідомив заступник Міністра юстиції Василь Мармазов, у ході зустрічі було обговорено можливі шляхи інтенсифікації двостороннього міжнародно-правового співробітництва України та Швейцарії у сфері кримінального судочинства. Представники української та швейцарської юстиції дійшли згоди, що така співпраця може бути поглиблена на основі застосування багатосторонніх міжнародних договорів, зокрема, через спеціальні спільні заходи в рамках цих угод.

Прес-служба Міністерства юстиції України

Надежность безопасности

Давно канули в лету те времена, когда предприниматели для обеспечения безопасности своего бизнеса, а так же личной безопасности обращались за помощью к «браткам» или организовывали собственные службы безопасности. В настоящее время рынок охранных услуг Украины достаточно широк. Кроме Государственной службы охраны при МВД (созданной вместо вневедомственной охраны входившей ранее в состав МВД), имущество, покой, и сон граждан берегут негосударственные предприятия безопасности (далее НПБ), которые возникли чуть более десяти лет назад и характеризуются неизменной востребованностью. Как известно, спрос рождает предложения, что в свою очередь рано или поздно приводит к конкуренции. В таких условиях повышаются требования к уровню профессионализма сотрудников охранных структур. Успех или неудача практической деятельности частного охранного предприятия зависят от многих объективных и субъективных факторов. К ним относится наличие четкой иерархической структуры организации, профессионально грамотное руководство, хорошая материально-техническая база.

Однако деятельность любой организации обеспечивается, прежде всего, людьми, квалифицированный кадровый состав – половина успеха в любом бизнесе. Клиент, пользуясь услугами охранного предприятия, хочет быть уверен в надежности защиты. А это напрямую зависит от профессиональной подготовки и надежности сотрудников, качественного подбора и расстановки кадров. Просчеты приводят к нежелательным последствиям. Так, например, в одном одесском филиале киевского банка нес службу сотрудник частной охранной фирмы. Внешне – парень в отличной физической форме, аккуратен, услужлив и предупредителен по отношению к своему и банковскому руководству. Но в резюме психолога присутствуют и другие характеристики: примитивен, соображает медленно, коммуникативные навыки и общий культурный уровень – низкие, склонен к агрессивному поведению. В одно прекрасное утро филиал посещает незнакомый охраннику киевский соучредитель банка и видит стража порядка, читающего газету. В ответ на замечание, он откровенно нахамил киевлянину. Естественно, банкир высказал руководству охранной фирмы весьма недвусмысленные пожелания. Результат: охранник уволен, престиж фирмы подорван. Узнав про инцидент, несколько потенциальных клиентов воспользовались услугами другого охранного предприятия. В то же время, сотрудник мог быть успешно задействован на другом объекте, например, в составе ночного караула на стройке и неплохо справлялся бы со своими обязанностями.

Директору НПБ приходится решать множество задач: предоставлять клиенту качественные услуги, обеспечивать рентабельность в условиях конкуренции, организовывать работу персонала и другие. Совмещать обязанности высококлассного специалиста в сфере охранной деятельности и успешного бизнесмена нелегко. Подготовка менеджеров охранного бизнеса – перспектива светлого будущего. В основном, в настоящее время НПБ возглавляют офицеры запаса Вооруженных сил, СБУ и органов внутренних дел. Им приходится искать ответы на коммерческие вопросы, осваивая новую профессию «без отрыва от производства». Вопросы подготовки и расстановки кадров во многих фирмах – открыты. Сотрудники кадровых органов, отбирая кандидатов на должности, в основном опираются на изучение различного рода документов и справок, характеристик и рекомендаций. Это немаловажно, но существуют более достоверные способы определения ведущих черт характера и способностей человека к тому или иному виду деятельности. Современные методы психодиагностического исследования позволяют определить профессионально важные качества для специалистов конкретной профессии, раскрыть индивидуальные качества человека, его способности, преобладающий стиль поведения, совместимость с другими людьми.

Сегодня руководители частных охранных фирм все чаще привлекают к работе психологов, так как по результатам психологического профотбора можно составить предварительный прогноз профессиональной успешности кандидата на ту или иную должность, а также эффективно решать многие вопросы: комплектовать экипажи, команды, регулировать межличностные отношения в коллективе и др.

Кроме того, некоторые руководители, ратуя за развитие отечественной психологии и скорейшее воссоединение ее с практикой, предоставили психологам возможность провести научное исследование на базе своих охранных предприятий. Исследование проводилось в группе из 130 сотрудников младшего и среднего звена, работающих в различных НПБ г. Одессы.

Вначале был проведен психологический анализ деятельности сотрудников охраны и экспертная оценка требований профессии. Экспертами выступили специалисты, имеющие опыт руководящей работы не менее пяти лет в охранных структурах. Определив профессионально важные качества личности, необходимые для успешной работы в системе негосударственной охраны, подобрали соответствующие тесты. Затем разработали методику психодиагностического профотбора, которая включала: изучение автобиографии и характеристик с последнего места работы, службы или учебы; неструктурированное интервью; психологическое тестирование; наблюдение в процессе собеседования и тестирования; составление психологического заключения.

Автобиография и характеристики дают определенные сведения об образовании, профессиональном опыте, мотивациях и т. д. Анализируя же ответы сотрудника на специальные вопросы, заданные в ходе интервью и наблюдая за его реакциями в процессе беседы, мы получали много косвенной, непроизвольно предоставленной информации. Рассказ о прошлом положительном и отрицательном опыте помогает определить ведущие жизненные установки и закрепившиеся схемы поведения, выяснить, какие ситуации являются для человека конфликтогенными или стрессовыми, способствует выявлению позитивных и негативных, в профессиональном отношении, качеств. Достаточно информативны такие показатели как тембр, тон голоса, скорость речи, словарный запас, речевые ошибки, мимика, жестикуляция, почерк и др. Сведения, полученные во время интервью, и результаты тестирования дают возможность составить психологический портрет кандидата в охранники и прогноз его профессиональной успешности.

Психологическое тестирование проводилось с помощью специально подобранных тестов. **В качестве основных использовались следующие методики:**

1. Тест, который определяет психотип личности, то есть характеризует позитивные и негативные особенности человека, профессиональные и личностные склонности, предпочтения, наиболее распространенный тип поведения, принятия решений. Кроме того, тест дает возможность отделить норму от патологии, позволяя выявлять психически нездоровых кандидатов или находящихся в пограничном, относительно болезни, состоянии. Время тестирования около 40 минут.

2. Методика, с помощью которой можно выявить эмоциональное состояние человека, способность к адекватному анализу собственного поведения, способность к самоконтролю, критичность и другие качества личности. Тест так же выявляет индивидуально-психологические особенности в рамках психической нормы. Время тестирования – 20–25 минут.

3. Тест на склонность человека к открытому агрессивному поведению, то есть поведению, противоречащему соци-

альным и законодательным нормам. Понятие «агрессивность» в данном контексте включает три взаимосвязанных компонента: намеренность (в отличие от случайности), силовые приемы решения конфликта, стремление к телесным повреждениям. Люди, склонные к такому поведению, не пригодны для работы в охранных структурах. Исследование длится 15–20 минут.

4. Методика, определяющая остроту восприятия, способность логически мыслить, находить существенные связи между предметами и явлениями, умение концентрировать внимание, адекватность реакции, т. е. качества, необходимые в деятельности охранника. Время тестирования – 3–5 минут.

В качестве дополнительных методик использовались экспресс-тесты характеризующие внимание, память, реакцию. После составления психологических портретов мы в течение шести месяцев наблюдали за поведением сотрудников на рабочих местах, во время учебных занятий, изучали должностные характеристики, ежедневные оперативные отчеты о несении службы. Затем, руководители охранных предприятий и преподаватели оценили работу каждого из сотрудников. С помощью методов математической статистики был проведен анализ результатов психологического профотбора и результатов практической деятельности охранников, проведено сравнение тестовых показателей с показателями экспертной оценки. По уровню профессиональной пригодности 130 сотрудников были разделены на три группы. В первую группу вошли 32 человека полностью соответствующие требованиям специальности. Вторая группа численностью 51 человек – средний уровень профессиональной пригодности, 47 человек были признаны профессионально непригодными, из них впоследствии были уволены по служебному несоответствию 43 человека.

Эффективность работы охранников зависит от конкретных условий труда на охраняемом объекте и индивидуально-личностных особенностей конкретного человека, которые могут быть выявлены в процессе психологического профотбора. Психологическое здоровье сотрудника – один из основных критериев его профессиональной успешности. Профессия охранника связана с постоянной возможностью возникновения критических ситуаций, требующих немедленного реагирования. Работа, требующая повышенной на-блюдательности, напряжения внимания, сосредоточенности может являться причиной развития стресса и негативно влиять на работоспособность. Монотонность труда, причиной которой является выполнение простых действий, не вызывающих позитивных эмоций, так же может повлиять на состояние сотрудника: теряется интерес к выполняемой работе, снижается внимание, наблюдательность.

Для сотрудников НПБ Украины сложность заключается еще и в том, что они должны обеспечить безопасность, не имея возможности в критической ситуации применить оружие. Правовые полномочия подразделений охраны при МВД допускают применение огнестрельного оружия и специальных средств защиты. Отсутствие надежных средств защиты, кроме разрешенных сегодня некоторых спецсредств, является одним из стрессогенных факторов, усиливающих нервно-психологическое напряжение. Психологический и физический риск является обязательной характеристикой труда охранника и требует определенных качеств личности.

Существует ряд противопоказаний для работы в охранных структурах: повышенная тревожность, эмоциональная неуравновешенность, импульсивность, низкая стрессоустойчивость; низкие показатели распределения и концентрации внимания; недостаточно развитые память и мышление; доминирование установок на применение физической и вербальной агрессии и другие. В повседневной деятельности такие люди могут довольно хорошо справляться со своими обязанностями, но в сложных ситуациях для них с большей вероятностью характерна либо паника, либо сильно заторможенное поведение, что в любом варианте ведет к неадекватным действиям.

Многие из тех, кто работает сегодня в системе охраны – бывшие военнослужащие, сотрудники МВД, которым приходилось бывать в экстремальных ситуациях, принимать участие в боевых действиях. У людей после пребывания в «зоне напряженности» формируется определенный тип личности со своей психологией и системой ценностей. По статистике, до 70 % лиц, принимавших участие в боевых действиях, по возвращении имеют проблемы во взаимоотношениях с окружающими, из них 30–35 % – имеют нервно-психические расстройства. Так, ветеран боевых действий по документам и характеристикам полностью соответствовал должности охранника. По результатам же психологического отбора был отнесен к группе профнепригодных. После принятия на работу в охранное предприятие в течение первых двух-трех недель работы все было в порядке. Затем начались необоснованные с точки зрения служебной дисциплины (но сверхзначимые для самого охранника) опоздания на службу, уходы с поста, прогулы, причина которых – религиозный фанатизм как следствие тяжелой психической травмы, полученной во время военных действий в Афганистане. При всем уважении к жизненным ценностям и вероисповеданию человека, строгое соблюдение обрядов, включая обязательное ежедневное посещение храма, никак не сочетается с работой охранника.

Кроме того, у человека в погонах и сотрудника НПБ в основном разный подход к выполнению поставленной задачи, да и задачи перед ними стоят разные. За спиной военнослужащего и милиционера – государственная система правовой защиты, которая в свою очередь обеспечивает и относительную психологическую защиту. Поэтому он, долго не раздумывая, применит оружие в экстремальной обстановке, ведь его долг – любым способом выполнить приказ, как говорится «если враг не сдается – его уничтожают». Сотрудник НПБ в критической ситуации, даже при наличии оружия, прежде всего, должен семь раз подумать, дабы «не превысить пределы допустимой обороны». Его основная задача – постараться не допустить форс-мажора.

Во время обучения и работы по конкретной специальности у человека, как правило, формируются определенные черты характера и профессиональные качества. Процесс адаптации к новому виду деятельности зависит от многих факторов, в том числе от индивидуальных особенностей человека. К сожалению, не всем удается перестроиться.

Анализ результатов психологического обследования, включенного в систему профотбора, позволяет оценивать широкий спектр личностных характеристик, особенностей состояния и поведения кандидатов в сотрудники, определять способности того или иного лица к охранной деятельности. Это, в свою очередь, является одним из условий разрешения проблем, связанных с эффективностью использования кадрового потенциала и управления персоналом; подготовкой и переподготовкой кадров, что также способствует повышению эффективности работы охранного предприятия и надежности предоставляемых услуг. Психологический профотбор – это только одно из направлений деятельности психолога. Формирование корпоративной культуры, психологическое сопровождение переговоров с клиентами, комплектование команд и коллективов, участие в рекламных компаниях предприятия, психологическая подготовка охранников, психопрофилактическая и психокоррекционная работа – далеко не полный перечень возможностей использования психологических знаний в сфере охранного бизнеса.

Белова М.

ЗАКОНЫ МЕРФИ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Законы Мерфи для информационной безопасности Мерфология - область человеческих знаний, которая не только забавна и интересна, но и которая реально отражает многие аспекты человеческой деятельности. Всего из одного шутливо/правдивого закона Мерфи «если какая-нибудь неприятность может произойти, она обязательно случается», родилось целое направление, которое позволяет понять многие процессы в человеческом обществе. Существуют различные направления мерфологии - военная, медицинская, писательская, рекламная, бытовая и т.п. Но мне ни разу не приходилось видеть законов Мерфи для информационной безопасности. Кроме давно опубликованной статьи «Murphy's law and computer security» (http://www.insecure.org/stf/wietse_murphy.html) автора сканера безопасности SATAN Витса Венема, эта деятельность, которая становится все более и более важной, не нашла отражение в мерфологии. И я решил исправить это упущение и попытался собрать разрозненные наблюдения и замечания в одном документе. Какие-то из нижеприведенных тезисов являются следствием уже известных законов Мерфи, какие-то наблюдения и аксиомы не вошли в этот документ, т.к. полностью совпадают с законами из других направлений мерфологии. Однако некоторые наблюдения достаточно интересны и присущи только информационной безопасности. Что из этого получилось - решать вам.

Основные законы

★ Если вас можно атаковать, вас атакуют (следствие основного закона Мерфи).

★ Если 4 дыры устранены, то всегда найдется пятая.

★ Не заявляй о своей неуязвимости и невзламываемости - всегда найдется кто-то, кто докажет обратное.

★ Следствие - Если вы считаете свою сеть неуязвимой, то вы ошибаетесь.

★ Любая программа содержит дыры.

★ Следствие: даже системы защиты содержат дыры.

★ Обнаружить все дыры невозможно.

★ Если вы уверены, что написанная вами инструкция по правилам выбора паролей не может быть понята неправильно, всегда найдется сотрудник, который поймет ее именно так.

Наблюдения за пользователями

★ Экспертом по безопасности, как и знатоком футбола, считает себя каждый второй пользователь (не считая каждого первого).

★ Каждый программист считает себя специалистом по криптографии и умению разрабатывать невзламываемые алгоритмы шифрования.

★ Не усматривайте злого умысла в том, что вполне объяснимо обычной пользовательской ошибкой (следствие из бритвы Хеллона).

Законы построения системы обеспечения информационной безопасности

★ Система информационной безопасности никогда не строится в срок и в пределах сметы (следствие из закона Хеопса).

★ Как бы хорошо не была написана политика безопасности всегда найдется используемая у вас технология, которая не нашла в ней отражение.

★ Как только политика безопасности окончательно утверждена, она уже окончательно устарела.

★ Любые издержки на построение системы информационной безопасности больше, чем вы ожидаете (следствие пятого закона Фостера).

Наблюдения о руководстве

★ Руководство всегда озадачивается безопасностью своей компании только после того, как ее уже взломали.

★ Руководителем отдела защиты информации назначают либо отставного военного, либо бывшего милиционера, либо бывшего сотрудника 1-го отдела.

★ Человек, знающий как и куда правильно потратить деньги на информационную безопасность, и человек, их выделяющий - это всегда разные люди.

★ Исключение: исключений не бывает.

Наблюдения об атаках

★ Из всех атак произойдет именно та, ущерб от которой больше всего.

★ Если вас атаковали один раз, не ждите, что на этом все и кончится.

★ Атаки происходят тогда, когда администратор безопасности отсутствует на работе.

★ Следствие - Стоит вам отлучиться на 5 минут, как именно в этот момент ваш босс не сможет закачать себе новую MP3-композицию из-за настроек МСЭ.

★ Целью атаки будет именно тот сервер, падение которого нанесет наибольший ущерб (следствие закона избирательного тяготения).

★ Если атака все-таки нанесла вам ущерб всегда найдется администратор, который скажет «я так и знал» (следствие закона Эванса и Бьерна).

★ Если в вашей сети всего один непропатченный сервер, именно через него и начнется эпидемия очередного червя.

★ Эпидемия червя начинается именно тогда, когда вы забыли продлить подписку на антивирусные базы или базы сигнатур атак.

★ Если атака проходит незамеченной для администратора безопасности, значит вас ждет ловушка (основной закон для хакеров).

★ Именно тот незначительный скан, который вы проигнорируете, будет предвестником массированной атаки.

★ Об атаках всегда сообщается в прошедшем времени (следствие уотергейтского принципа).

★ Из всех атак произойдет именно та, от который вы забыли защититься.

Наблюдения о хакерах

★ Сотрудники отдела защиты информации приходят и уходят, а хакеры остаются (следствие девиза Джоунза)

★ Действия профессиональных хакеров можно предсказать, но Интернет полон любителей.

Наблюдения о консультантах по безопасности

★ Консультанты по безопасности - загадочные люди; сначала они выспрашивают все о вашей сети и ее безопасности, а потом приводят эту информацию в своем отчете, выдавая ее за титанический плод своих усилий (следствие второго закона Макдональда).

★ Приглашенные эксперты по безопасности всегда кажутся лучше своих собственных.

★ Если эксперт по безопасности знает, как называется атака, которой вы подверглись, это еще не значит, что он знает, как от нее защититься.

★ Каждый способен сказать, что в вашей сети есть дыра, но не каждый способен найти ее.

★ Виновным в неудачном внедрении системы защиты всегда оказывается внешний эксперт, приглашенный для консультаций.

★ Приглашенный эксперт, обвиненный в неудачном внедрении системы защиты, обвинит вас в непредоставлении всей необходимой информации (закон противоположного обвинения).

★ Стоимость услуг по обследованию корпоративной сети - величина, никак не зависящая от числа и квалификации экспертов, участвующих в обследовании.

Замечания по аутсорсингу

★ Передать свою безопасность на аутсорсинг - значит потерять контроль над сетью. Не передать - потерять контроль еще быстрее.

★ Доступность аутсорсинга еще не показатель, что им надо воспользоваться.

Наблюдения о средствах защиты

★ Расходы на средства защиты информации стремятся сравняться с доходами от их внедрения (следствие из второго закона Паркинсона).

★ Стоимость системы защиты информации всегда больше, чем вы запланировали (следствие пятого закона Фостера).

★ Установив систему защиты, не ждите благоприятных отзывов от сотрудников.

★ Ни одно средство защиты, введенное в эксплуатацию, не прошло тестирования.

★ Ни одно средство защиты, прошедшее тестирование, не готово к вводу в эксплуатацию (закон противоположности).

★ Чем больше функций в системе защиты, тем больше вероятность, что одна из них не работает так как надо.

★ Если вы не уверены, работает ли ваша системы защиты, значит она не работает.

★ Если ваша система защиты работает по расписанию, то вы обязательно забудете запустить ее в нужное время.

★ Система, защищающая от самых современных атак, будет неспособна защитить вас от давно устаревших.

★ Надежность системы защиты обратно пропорциональна числу и положению лиц, управляющих ею (следствие закона Уатсона).

★ Если вы хотите создать централизованную систему управления средствами защиты информации, окажется, что все ваши средства выпущены разными производителями и не интегрируются между собой.

★ Наличие сертификата соответствия на систему защиты еще не означает, что продукт соответствует классу защищенности, указанному в сертификате.

★ Следствие - Это также не значит, что продукт вообще работает.

★ Вывод - Это вообще ничего не значит.

★ Система защиты блокирует доступ вашего босса в Интернет именно в тот момент, когда он думает об увеличении вашей зарплаты.

★ Если вы приобрели большую партию электронных брелоков или смарт-карт, то обязательно окажется, что более 50% ваших сотрудников являются женщинами, которым негде носить эти средства аутентификации (наблюдение Левашова).

Разные наблюдения

★ Когда администратор безопасности испытывает затруднения при обнаружении дыр, это значит, что он ищет не там, где следует.

★ Нет ничего более приятного, чем отбитая атака хакеров.

★ Если вы уверены, что в вашей сети нет бесконтрольно установленных и используемых модемов, то вы ошибаетесь.

★ В отделе защиты информации всегда не хватает людей.

★ Если после отпуска вы забыли свой пароль, отдых удался на славу.

★ Именно в тот момент, когда вам нужно собрать доказательства несанкционированной деятельности, окажется, что регистрация событий не включена.

★ Если вашу статью кто-то украл, то скорее всего это преподаватель какого-либо ВУЗа (пессимистическое наблюдение Лукацкого)

http://www.securitylab.ru

ПЛАН МЕРОПРИЯТИЙ ИНДУСТРИИ БЕЗОПАСНОСТИ – 2005,

В КОТОРЫХ ПРИНИМАЕТ УЧАСТИЕ ЖУРНАЛ «БИЗНЕС И БЕЗОПАСНОСТЬ»

Наименование мероприятия, краткое содержание, тематические разделы	**Дата проведения** Место проведения	**Организатор**
Связь, системы безопасности Ситемы связи. Защита информации. Безопасность бизнеса. Услуги охраны. Системы пожарной безопасности	**22.02.-24.02** г. Днепропетровск ул. Комсомольская, 58 Деловой центр	Компания «СМТ» (056) 371-3412, 771-4495 771-4498 Бизнес центр
«Инфоком» Специализированные выставки: компьютеры, связь и коммуникации, современный офис, банк	**23.03-26.03** г. Днепропетровск ДС «Метеор»	**«Коминфо»** (056) 370-14-14 www.cominfo.ua
Пожежна та техногенна безпека України Системи пожежної та техногенної безпеки; Пожежна, аварійно - рятувальна техніка й устаткування; Спорядження і засоби індивідуального захисту; Нові технології попередження та боротьби з надзвичайними ситуаціями техногенного і природного характеру	**04.04-06.04** м. Київ вул.Салютна, 2-б КиївЕкспоПлаза	Міністерство України з питань надзвичайних ситуацій, Добровільне пожежне товариство України, Міністерство палива та енергетики, Міністерство промислової політики України (044)244-20-54
«EnterEx-2005»»ExpoTEL 2005» Решение для управления предприятием 2005 Неделя цифровых технологий	**5.04–8.04** г. Киев ВЦ Киев Экспо Плаза	Компания «Евроиндекс» (044)461-93-01 www.enterex.ua
Корпоративні та банківські системи 2005 X Міжнародна виставка - конференція «Сучасні інформаційні системи, технології, обладнання для банків, корпорацій та підприємств»	**12.04 -14.04** м. Київ Броварський проспект, 15 Міжнародний виставковий центр,	Прем'єр Експо (044) 451-41-60 E-mail: cdse@.pe.com.ua www.pe.com.ua
Пожежна безпека Друга спеціалізована виставка техніки, обладнання і технологій для захисту від пожеж	**13.04 -15.04** м. Одеса , Виставковий комплекс Одеського порту	Центр виставкових технологій (048) 777-57-90 (0482) 22-30-15 E-mail: nm@.expo-odessa.com
«Пожэкспо 2005» Пожарная техника и средства пожаротушения, сигнализации, средства огнезащиты; средства связи, информационные системы и технологи, исследования пожаров	**25. 04 -28.04** г. Киев Експоцентр Украины	Експоцентр Украины (044) 251-92-80 (044) 251-91-25
Связь и телекоммуникации Телекоммуникационные технологи и услуги.Системы связи.	**05.05-07.05** г. Одесса Одесский морской торговый порт	Экспо - Юг -Сервис (048) 777-60-68 (048) 728-60-68 www.expodessa.od.ua
Hi -Tech 2005 Информационные технологии, системы связи и телекоммуникации; Компьютерные системы и програмное обеспечение; Оборудование для дома и офиса; Интелектуальные технологии	**05.05-07.05** г. Одесса, Одесский морской торговый порт	Выставочный центр»Одесский дом» (0482) 37-17-37 (048)728-64-94 E-mail: org@hi-tech.com.ua
«ISPEK 2005» V міжнародна спеціалізована виставка засобів захисту, озброєння та спецтехніки	**24.05-27.05** м. Київ ВК «ЗовнішЕкспоБізнес»	«ЗовнішЕкспоБізнес» (044)272-31-72 (044)216-76-04 E-mail: ispek@vneshexpo.kiev.ua www.vneshexpo.kiev.ua

НОВОСТИ

4 февраля 2005 года, в Московском Театре «Школа драматического искусства» в 16 часов состоялась церемония вручения Национальной отраслевой Премии по безопасности «ЗУБР». Корпорация «ПЕНТАКОН» уже во второй раз стала Лауреатом Премии.

Цифровая система VideoNet была признана лучшим продуктом для обеспечения безопасности банков. Присвоенный профессиональным сообществом статус «лучшей из лучших систем» является неоспоримым свидетельством лидерства VideoNet, не подлежащим каким либо сомнениям. Президенту корпорации «ПЕНТАКОН» Виктору Михайловичу Крылову была вручена награда - почётный диплом и статуэтка зубра.

Вячеслав Владимирович Шабайкин - И.О. Председателя Восточносибирского банка Сбербанка России, также отмеченный Премией в номинации «За выдающиеся достижения в области укрепления безопасности банков», поблагодарил корпорацию «ПЕНТАКОН» за непосредственное участие в обеспечении совершенно нового уровня безопасности крупнейшего банка России и создание уникальной системы VideoNet, которая действительно позволяет из одного центра проводить наблюдения во всех отделениях и филиалах банка, а также даёт серьёзный экономический эффект.

http://www.cctv.ru

НОВОСТИ

Работа в милиции требует чистых рук и высоких моральных качеств

Одним из самых важных вопросов для органов внутренних дел на сегодняшний день остается профилактика дисциплины и законности среди личного состава.

В 2004 году судами области осуждено 5 бывших работников милиции - все за должностные преступления.

К примеру, в августе прошлого года Центрально-Городским судом г. Макеевки по двум "должностным" статьям осужден оперативный работник Харцызского ГО, который скрыл место нахождения разыскиваемой гражданки, получив от нее взятку. Виновного подвергли наказанию в виде штрафа в 13,5 тысяч гривен с лишением права заниматься организационно-распорядительной деятельностью сроком на один год.

Из ОВД Донетчины по отрицательным мотивам таким образом было уволено 78 сотрудников - в основном из служб, которые непосредственно контактируют с населением: административная служба милиции, угрозыск, ГАИ ... И это понятно, ведь в общении с гражданами необходимо иметь не только определенный багаж знаний и практический опыт, но и желание помочь человеку, оказавшемуся в непростой ситуации. При этом соблюдение закона должно стоять во главе угла.

Александр Костин,
ЦСО УМВД Украины
в Донецкой области

Банківське обладнання

товар, послуга	*ціна*	*телефон*
Rexel HS-80+сервіс	**260,00**	044 255-16-00 255-16-00
Rexel V125+ сервіс, ремонт, гарантія	**1130,00**	044 255-16-00 255-16-00
Rexel V25+ сервіс, ремонт, гарантія	**450,00**	044 255-16-00 255-16-00
Детектори валют «Спектр» всі типи, ремонт	**40,00**	044 255-16-00 255-16-00
Знищувач документів, асорт. Ремонт	**150,00**	044 255-16-00 255-16-00
Лічильник банк. «MAGNER-35»+сервіс	**1900,00**	044 255-16-00 255-16-00
Лічильник банк. «Банкнота-1»+сервіс	**2800,00**	044 255-16-00 255-16-00
Лічильник банк. SPEED LD50+сервіс	**1620,00**	044 255-16-00 255-16-00
Лічильник банк. SPEED LD-60A+сервіс	**2600,00**	044 255-16-00 255-16-00
Ремонт, модернізація грошерахувальних машин, знищувачів документів, детекторів валют, від	**16,00**	044 255-16-00 255-16-00

Захист інформації

товар, послуга	*ціна*	*телефон*
Атестація об'єкта ЕОТ	**1200,00**	044 201-45-84 201-45-84
Багатофункціональний пошуковий прилад PROTECT 2800	**$0,00**	044 490-67-34 235-57-17
Блок захисту телефонного апарату	**$150,00**	(067)702-76-84
Блокування витоку мовної інформації, поставка та монтаж захисних пристроїв, від	**5240,00**	044 201-45-84 201-45-84
Виготовлення нормативно-методичної документації в галузі захисту інформації	**0,00**	044 201-45-84 201-45-84
Вимірювання ефективності екранування приміщення серверної, від	**4600,00**	044 201-45-84 201-45-84
Вимірювання рівня екранування приміщення серверної, від	**4800,00**	057 744-83-65 336-25-29
Вимірювач частоти ROGER RFM-31	**$247,00**	044 490-67-34 235-57-17
Вимірювач частоти ROGER RFM-32	**$275,00**	044 490-67-34 235-57-17
Вимірювач частоти цифрових сигналів SC-1	**$240,00**	044 490-67-34 235-57-17
Виявлення активних закладних пристроїв по радіоефіру та в провідних лініях	**1200,00**	044 201-45-84 201-45-84
Виявлення закладних пристроїв в активному режимі по радіоканалу та провідних лініях	**1200,00**	057 744-83-65 336-25-29
Виявлення закладних пристроїв в пасивному режимі, за 1м^2	**20,00**	057 744-83-65 336-25-29
Виявлення пасивних закладних пристроїв в інженерних комунікаціях та в предметах інтер'єру, грн/м^3	**20,00**	044 201-45-84 201-45-84
Вібраційний випромінювач TRN-2000 для генератора білого шуму	**$75,00**	044 490-67-34 235-57-17
Генератор білого шуму DNG-2000	**$625,00**	044 490-67-34 235-57-17
Генератор шуму мережевий	**$150,00**	(067)702-76-84
Захист від прослуховування через GSM	**$250,00**	044 490-67-34 235-57-17
Індикатор поля PROTECT 1203	**$180,00**	044 490-67-34 235-57-17
Індикатор поля-ручка PROTECT 1205	**$245,00**	044 490-67-34 235-57-17
Локатор нелінійностей «Катран»	**$0,00**	044 490-67-34 235-57-17
Мобільний пригнічувач GSM-900, 1800, DCC	**$300,00**	(067)702-76-84
Пошукове программне забезпечення для приймачів AOR/ICOM DigiScan EX Lite/Standard/Monitor/Professional	**$0,00**	044 490-67-34 235-57-17
Пошуковий комплекс СРМ-700 «Акула» з розширювачем до 10 кГц–12 ГГц	**$0,00**	044 490-67-34 235-57-17
Пригнічувач GPS-терміналів	**$250,00**	(067)702-76-84
Приймач широкодіапазонний AOR AR5000A	**$0,00**	044 490-67-34 235-57-17
Приймач широкодіапазонний AOR AR8200 Mk3	**$0,00**	044 490-67-34 235-57-17
Приймач широкодіапазонний ICOM IC-R5	**$0,00**	044 490-67-34 235-57-17
Приймач широкодіапазонний з вбудованим диктофоном ICOM IC-R20	**$0,00**	044 490-67-34 235-57-17
Прилад для забезпечення конфіденційності переговорів	**$0,00**	044 490-67-34 235-57-17
Прилад пошуку прихованих відеокамер «Алмаз»	**$0,00**	044 490-67-34 235-57-17
Прилад пошуку прихованих відеокамер «Алмаз»	**$0,00**	044 490-67-34 235-57-17
Система ПАВУК (акустичного контролю приміщень)	**$0,00**	(067)702-76-84
Сотова сигналізація для квартири, дачі, будинку, офісу, авто	**$0,00**	(067)702-76-84
Спеціальне обстеження комп'ютера по каналу ПЕМВН, захист комп'ютера засобів на наявність акусто-електричних перетворювань, від	**2700,00** **350,00**	044 201-45-84 201-45-84 044 201-45-84 201-45-84
Спецобстеження і атестація виділених приміщень, від	**1800,00**	057 744-83-65 336-25-29
Спецобстеження і атестація комп'ютера по каналу ПЕМВН	**4200,00**	057 744-83-65 336-25-29
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80
Фільтри електромережні протизавадні, діапазон захисту 10 кГц–10 ГГц.	**$183,00**	044 458-15-80

Звукозапис

товар, послуга	*ціна*	*телефон*
Багатоканальна система реєстрації телефонних розмов DigiVoice-24	**$0,00**	044 490-67-34 235-57-17
Диктофон професійний EDIC MINI B-1120	**$308,00**	044 490-67-34 235-57-17
Диктофон професійний EDIC MINI B-2240	**$412,00**	044 490-67-34 235-57-17
Касетний телефонний реєстратор GT-TR800B2	**$160,00**	044 490-67-34 235-57-17

Зв'язок

товар, послуга	*ціна*	*телефон*
Акумулятори для р/ст. в асортименті	**$0,00**	044 442-33-44 442-33-06
Антени для р/ст. в асортименті	**$0,00**	044 442-33-44 442-33-06
Р/ст. ALINCO в асортименті	**$0,00**	044 442-33-44 442-33-06
Р/ст. ICOM в асортименті	**$0,00**	044 442-33-44 442-33-06
Р/ст. KENWOOD в асортименті	**$0,00**	044 442-33-44 442-33-06
Р/ст. MOTOROLA в асортименті	**$0,00**	044 442-33-44 442-33-06
Р/ст. VERTEX в асортименті	**$0,00**	044 442-33-44 442-33-06
Р/ст. YAESU в асортименті	**$0,00**	044 442-33-44 442-33-06
Р/ст. для охорони в асортименті	**$0,00**	044 442-33-44 442-33-06
Радіостанції без реєстрації	**$0,00**	044 442-33-44 442-33-06

Контроль доступу, огляд

товар, послуга	*ціна*	*телефон*
Грунтовий металодетектор GARRETT GTI-2500	**$0,00**	044 490-67-34 235-57-17
Грунтовий металодетектор MINELAB Explorer II	**$0,00**	044 490-67-34 235-57-17
Електромеханічні/магнітні замки, від	**$20,00**	044 205-36-46 205-36-87
Кодовий доступ, Touch Memory, від	**$24,00**	044 205-36-46 205-36-87
Металодетектор арочного типу в асорт.	**$1,00**	044 442-33-44 442-33-06
Металодетектор колонного типу в асорт.	**$1,00**	044 442-33-44 442-33-06
Металодетектор ручного типу в асорт.	**$1,00**	044 442-33-44 442-33-06
Металошукачі в асортименті	**$1,00**	044 442-33-44 442-33-06
Металошукачі ручні асорт.	**$1,00**	044 442-33-44 442-33-06
Програмно-апаратний комплекс «Відео для офісу», від	**$199,00**	044 205-36-46 205-36-87
Ручний металодетектор GARRETT SUPERSCANNER	**$247,00**	044 490-67-34 235-57-17
Ручний металодетектор GARRETT SUPERWAND	**$284,00**	044 490-67-34 235-57-17
Ручний металодетектор GARRETT THD	**$247,00**	044 490-67-34 235-57-17
Системи контролю доступу, охоронні системи	**$0,00**	044 234-95-34 235-02-70

Охорона периметра, загородження

товар, послуга	*ціна*	*телефон*
Дріт колючий оцинкований	**$0,00**	04469 521-23 511-60
Експертиза інженерних охоронних систем	**$0,00**	04469 521-23 511-60
Загорожі «Єгоза» – монтаж	**$0,00**	04469 521-23 511-60
Загорожі колючо-стрічкові оцинковані «Єгоза» в асортименті	**$0,00**	04469 521-23 511-60
Інженерні загорожі моделі «НАТО» в асортименті	**$0,00**	04469 521-23 511-60
Інженерні системи захисту периметра	**$0,00**	04469 521-23 511-60
ІЧ-бар'єри «Optex», від	**$85,00**	044 205-36-46 205-36-87
Прилад нічного бачення 2-го покоління DEAL-45	**$0,00**	044 490-67-34 235-57-17

Охоронна і пожежна сигналізація

товар, послуга	*ціна*	*телефон*
16-зонний (базових 10 зон) концентратор, 4 групи, пам'ять 256 подій, 6 програм. транзисторн. вих.	**900,00**	0322 722-955 970-316
BXB WS - 100 T - стельовий гучномовець, 100 В, 6 Вт, 6,5 , 100 дБ, 80 Гц - 15 кГц	**114,00**	(062) 382-64-63 382-64-64
BXB WS - 650 T - стельовий гучномовець, 2-смуговий,100 В, 6 Вт, 6,5 , 97 дБ, 60 Гц - 20 кГц	**158,00**	(062) 382-64-63 382-64-65
BXB WS - 801 T - стельовий гучномовець, 100 В, 6 Вт, 8 , 101 дБ, 80 Гц - 15 кГц	**133,00**	(062) 382-64-63 382-64-66
BXB WS - 802 T - стельовий гучномовець, 2-смуговий, 100 В, 6 Вт, 8 , 100 дБ, 60 Гц - 20 кГц	**179,00**	(062) 382-64-63 382-64-67
BXB WS - 651 T - підвісний гучномовець, 100 В, 6 Вт, 104 дБ, 80 Гц - 15 кГц	**185,00**	(062) 382-64-63 382-64-68
BXB WS - 652 - підвісний 2-смуговий гучномовець,35 Вт, 8 Ом, 104 дБ, 60 Гц - 20 кГц	**214,00**	(062) 382-64-63 382-64-69
BXB WS - 652 T- підвісний гучномовець, 100 В, 6 Вт, 6,5 , 101 дБ, 60 Гц - 20 кГц	**236,00**	(062) 382-64-63 382-64-70
Dynacord DL 800/30 - рупорний гучномовець, 100 В, 30 Вт, 115 дБ, 400 Гц - 8 кГц, алюмінійовий, світло-сірий	**543,00**	(062) 382-64-63 382-64-71
Dynacord DL 800/25 - рупорний гучномовець, 100 В, 25 Вт, 115 дБ, 400 Гц - 8 кГц, алюмінійовий, світло-сірий	**502,00**	(062) 382-64-63 382-64-72
Dynacord DL 800/15 - рупорний гучномовець, 100 В, 15 Вт, 115 дБ, 400 Гц - 8 кГц, алюмінійовий, світло-сірий	**435,00**	(062) 382-64-63 382-64-73
Dynacord DL 800/10 - рупорний гучномовець, 100 В, 10 Вт, 115 дБ, 400 Гц - 8 кГц, алюмінійовий, світло-сірий	**368,00**	(062) 382-64-63 382-64-74
Dynacord MV 512 - мікшер-підсилювач, 100 /70/25 В, 120 Вт, 50 Гц - 15 кГц, 2 мікрофонних + 2 мікрофон/лінія + 1 лінійний входи	**3 177,00**	(062) 382-64-63 382-64-75
Dynacord MV 506 - мікшер-підсилювач, 100 /70/25 В, 60 Вт, 50 Гц - 15 кГц, 2 мікрофонних + 2 мікрофон/лінія + 1 лінійний входи	**2 926,00**	(062) 382-64-63 382-64-76
GSM автодозвон для Siemens C 35–S45, 4 входи, 4 виходи керованих SMS	**$50,00**	044 493-47-46
LCD клавіатура (українізована), додаткові 2 зони	**420,00**	0322 722-955 970-316
LED клавіатура для управління групою та ел. замком	**210,00**	0322 722-955 970-316
LED клавіатура з релейним виходом для управління ел. замком	**210,00**	0322 722-955 970-316
Адресний блок (для ST-764ADR), відстань до розширювача до 1 000 м	**72,00**	0322 722-955 970-316
Аксесуари до пультів-концентраторів ST-708...ST-716, розширення 6 зон	**108,00**	0322 722-955 970-316
Безпровідні ППК Jablotron, від	**$150,00**	044 205-36-46 205-36-87
Блок розширення на 16 двопровідних пожежних зон, в складі ST-764	**1194,00**	0322 722-955 970-316
Голосовий синтезатор для ST-708, ST-716, ST-764, енергонезалежн.	**120,00**	0322 722-955 970-316
Голосовий синтезатор для ST-764, 16 повідомлень по 15 сек.	**306,00**	0322 722-955 970-316
Графічна панель 290 х 220 мм, 32 світлодіоди в комплекті	**1770,00**	0322 722-955 970-316
Датчик диму СПД - 3.2, від	**$8,00**	044 205-36-46 205-36-87
Датчик розбиття скла GBD-2 (Crow), від	**$13,50**	044 205-36-46 205-36-87
Зчитувач Proximity карт (для ST-764-SR), акуст. та оптич. сигнал, відстань дії до 14 см	**138,00**	0322 722-955 970-316
ІЧ - датчик руху SRP-100 (Crow), від	**$11,00**	044 205-36-46 205-36-87
Клавіатура до ST-704 (додаткова)	**132,00**	0322 722-955 970-316
Клавіатура до ST-708 (додаткова)	**138,00**	0322 722-955 970-316
Клавіатура до ST-708 (додаткова), компактна	**138,00**	0322 722-955 970-316
Клавіатура мініатюрна рідиннокристалічна до ST-716 (додатк, українізов)	**390,00**	0322 722-955 970-316
Клавіатура світлодіодна до ST-716 (додатк), індикація 12 зон	**138,00**	0322 722-955 970-316
Клавіатура світлодіодна до ST-716 (додатк), індикація 16 зон, 4 групи	**138,00**	0322 722-955 970-316
Комунікатор «Атлас-3/6», «Каштан», «Дунай», для централей ST і DSC з фільтром	**150,00**	0322 722-955 970-316

Модель СА-5, 5-зонний концентратор	**468,00**	0322 722-955 970-316
Модель ST-7088-зонний концентратор	**534,00**	0322 722-955 970-316
Модель ST-71616-зонний (базових 10 зон) концентратор	**672,00**	0322 722-955 970-316
Модуль для індикації світлодіодами стану 64 зони і 32 групи, RS-232, блок живл. на 2,2 А	**1062,00**	0322 722-955 970-316
Модуль керування по тел. лінії (набір DTMF) для ST-708, ST-716	**120,00**	0322 722-955 970-316
Модуль розшир. 8 зон, 4 вих. О. С. , 4 рел. вих. , тампер, блок живл. на 2,2 А	**420,00**	0322 722-955 970-316
Модуль розшир. д/під'єдн. 2 зчитувачі Dallas, 1 реле, блок живл. на 2,2 А	**420,00**	0322 722-955 970-316
Модуль розшир. д/під'єдн. 2 зчитувачі Proximity карт, 1 реле, блок живл. на 2,2 А	**420,00**	0322 722-955 970-316
Модуль розшир. для під'єдн. до 48 адресн. блоків, блок живл. на 2,2 А	**420,00**	0322 722-955 970-316
Модуль розширення - 4 релейні вих., тампер, блок живл. на 2,2 А	**384,00**	0322 722-955 970-316
Модуль розширення - 4 релейні виходи, 4 виходи О. С. , тампер	**270,00**	0322 722-955 970-316
Модуль розширення - 8 виходів О. С., тампер	**210,00**	0322 722-955 970-316
Модуль розширення - 8 виходів О. С. , тампер, блок живлення на 2, 2 А	**324,00**	0322 722-955 970-316
Модуль розширення - 8 зон, тампер	**210,00**	0322 722-955 970-316
Модуль розширення - 8 зон, тампер, блок живлення на 2, 2А	**324,00**	0322 722-955 970-316
Модуль розширення - 8 релейних виходів, тампер	**324,00**	0322 722-955 970-316
Модуль розширення - 8 релейних виходів, тампер, блок живл. на 2, 2 А	**420,00**	0322 722-955 970-316
Модуль розширення на 8 транзисторних виходів для ST-7XX	**138,00**	0322 722-955 970-316
ППК «DSC», від	**$55,00**	044 205-36-46 205-36-87
ППК «Satel», від	**$58,00**	044 205-36-46 205-36-87
Пульт-концентратор SteelArm для пож. сигналізації, 16-зонний пульт	**1848,00**	0322 722-955 970-316
Пульти-концентратори Satel, ST-7044-зонний концентратор	**396,00**	0322 722-955 970-316
Пульт-концентратор 16 зон (розшир. до 64-х зон), 32 групи, 16 вих.	**1380,00**	0322 722-955 970-316
Релейний модуль для ST-708, ST-716, ST-764	**120,00**	0322 722-955 970-316
Рідиннокристалічна клавіатура до ST-716 (додатк, українізов)	**408,00**	0322 722-955 970-316
Світлодіоди до графічної панелі AS10 (упаковка 16 шт.)	**210,00**	0322 722-955 970-316
Сотова сигналізація для квартири, дачі, будинку, офісу, авто	**$0,00**	(067)702-76-84

Снарядження, галантерея

товар, послуга	*ціна*	*телефон*
Жезли ДАІ, від	**30,00**	044 568-59-41 234-40-49
Жилет ДАІ-ДПС світлоповертаючий	**45,00**	044 568-59-41 234-40-49
Жилет розгрузочний	**240,00**	044 568-59-41 234-40-49
Кобури поясні і оперативні, від	**21,00**	044 568-59-41 234-40-49
Обкладинки шкіряні для всіх видів документів, від	**9,00**	044 568-59-41 234-40-49
Плащ ДАІ світлоповертаючий	**99,00**	044 568-59-41 234-40-49
Ремінь охоронника з чохлами для спецзасобів і кобурою	**96,00**	044 568-59-41 234-40-49
Ремні брючні 25, 30, 35, 40 мм	**18,00**	044 568-59-41 234-40-49
Ремні офіцерські, солдатські, білі парадні, від	**15,00**	044 568-59-41 234-40-49
Спорядження ДАІ біле світлоповертаюче	**111,00**	044 568-59-41 234-40-49
Сумки-барсетки для зброї, від	**69,00**	044 568-59-41 234-40-49
Чохли для газбалончиків, наручників, кийків, від	**8,00**	044 568-59-41 234-40-49

ТВ спостереження

товар, послуга	*ціна*	*телефон*
CCTV варіооб'єктиви, від	**$33,00**	044 205-36-46 205-36-87
Аудіодомофони в асорт., від	**$13,00**	044 205-36-46 205-36-87
Багатоквартирні домофони, від	**$66,00**	044 205-36-46 205-36-87
Блоки живлення для систем відеоспостереження, від	**$7,00**	044 205-36-46 205-36-87
Відеодомофони в асорт., від	**$70,00**	044 205-36-46 205-36-87
Відеодомофони, приховані камери, монтаж	**$0,00**	044 234-95-34 235-02-70
Відеокамери безкорпусні, від	**$22,00**	044 205-36-46 205-36-87
Відеокамери зовнішні, від	**$45,00**	044 205-36-46 205-36-87
Відеокамери кольорові, від	**$47,00**	044 205-36-46 205-36-87
Відеокамери корпусні, від	**$28,00**	044 205-36-46 205-36-87
Відеопередавач на S36 ТВ-канал	**$20,00**	044 493-47-46
Інфрачервоні прожектори, пластини, від	**$14,00**	044 205-36-46 205-36-87
Квадратори, від	**$68,00**	044 205-36-46 205-36-87
Кольорові, TFT монітори, від	**$135,00**	044 205-36-46 205-36-87
Монітор 4"–21", від	**$60,00**	044 205-36-46 205-36-87
Мультиплексори, від	**$240,00**	044 205-36-46 205-36-87
Панелі антивандальні для домофонів, від	**$12,00**	044 205-36-46 205-36-87
Системи в/спостереження, установка, монтаж, від	**$1,00**	044 205-36-46 205-36-87
Системи комп'ют. в/спостереження,	**$140,00**	044 205-36-46 205-36-87
Системи ТВ спостереження для казино, банків та офісів	**$0,00**	044 234-95-34 235-02-70
Спец. в/магнітофон тривалого запису, від	**$280,00**	044 205-36-46 205-36-87
ТВ-модулятор, 21–69 канали	**$20,00**	044 493-47-46
Термокожухи, кронштейни, від	**$28,00**	044 205-36-46 205-36-87
Цифрові відеорегістратори, від	**$430,00**	044 205-36-46 205-36-87

Здійснюють передплату на журнал «Бизнес и безопасность»:

м. Біла Церква	ПП Болобан Е.В.	3-67-84
м. Вінниця	ЗАТ "Бліц-Інформ"	(0432) 27-66-58, 27-83-20
м. Вінниця	ТОВ ТПК "Преса"	35-45-70, 32-67-59
м. Дніпропетровськ	ТОВ "ПресЦентр"	32-08-56
м. Дніпропетровськ	ЗАТ "Бліц-Інформ"	(0562) 32-17-18
м. Дніпропетровськ	ПФ "Бібліотека Прес Інформ"	778-00-93, 778-00-47
м. Дніпропетровськ	ТОВ"Меркурій"	778-52-86, 744-72-87
м. Донецьк	ТОВ "ПресЦентр"	305-01-60
м. Донецьк	ЗАТ "Бліц-Інформ"	(062) 381-19-32, 381-19-33
м. Донецьк	ТОВ "Донбасс-Де-Юре"	345-00-50, 335-03-95
м. Донецьк	ТОВ "Донбасс-Информ"	93-82-72, 93-49-42
м. Донецьк	ТОВ "НВП Ідея"	381-09-32, 92-20-22
м. Донецьк	ТОВ "НПП "Дон ЕО Консалтинг Проект"	335-96-41, 335-98-60
м. Житомир	ЗАТ "Бліц-Інформ"	(0412) 36-04-00, т/ф 41-84-03
м. Запоріжжя	ККК "ПРЕС-СЕРВІС"	62-52-43, 62-51-51
м. Запоріжжя	ТОВ "ПресЦентр"	62-45-39
м. Запоріжжя	ТОВ "Преса"	62-52-43, 62-51-51
м. Запоріжжя	ТОВ "Светла"	64-22-29, 64-29-92
м. Запоріжжя	ЗАТ "Бліц-Інформ"	(0612) 63-91-82, (061) 220-92-23
м. Івано-Франківськ	ЗАТ "Бліц-Інформ"	(0342) 52-28-70, 55-96-02
м. Київ	"БукМаркет"	237-82-73, 295-48-88
м. Київ	"Офіс-сервіс"	490-90-87, 490-55-04
м. Київ	"Фінансова консультація"	296-97-96, 296-97-40
м. Київ	АТЗТ "Самміт"	290-77-45, 573-96-49
м. Київ	ДП "CN-Столичні новини"	234-33-27, 234-51-19
м. Київ	ЗАТ "Бліц-Інформ"	(044) 205-51-50
м. Київ	МІЦ "Сільвер-Поліграф"	274-12-91, 059
м. Київ	ТОВ "Альянс"	244-60-20
м. Київ	ТОВ "Баланс Інформ"	516-66-85
м. Київ	ТОВ "Періодика"	228-00-24
м. Київ	ТОВ "ПресЦентр"	536-11-75, 536-11-80
м. Кіровоград	ЗАТ "Бліц-Інформ"	(0522) 32-03-06, 32-03-00
м. Кременчук	ЗАТ "Бліц-Інформ"	(0536) 7-97-050, (05366)3-72-36
м. Кременчук	ПП "ОР-Прес" ул. Шевченко, 50А	79-71-48
м. Кривий Ріг	ЗАТ "Бліц-Інформ"	(0564) 66-24-36, 66-82-18
м. Кривий Ріг	СПД "Бондаренко"	74-35-70
м. Луганськ	ЗАТ "Бліц-Інформ"	(0642) 53-11-56, 53-81-07
м. Луганськ	ПП Ребрик И.В.	55-82-35, 53-40-73
м. Луцьк	ЗАТ "Бліц-Інформ"	(0332) 72-05-48,
м. Львів	ТОВ "ПресЦентр"	52-85-86
м. Львів	ЗАТ "Бліц-Інформ"	(0322) 39-28-69, 41-90-88
м. Львів	ПП "Компанія "Регіон"	763-786, 781792
м. Львів	ПП "Львівські оголошення-кур'єр"	21-37-46
м. Львів	ПП "Система Прес-Експрес"	62-52-81, 62-93-50
м. Львів	ППКС "Львівський кур'єр"	21-21-01, 23-04-10
м. Львів	ТОВ НВП "Фактор"	76-57-56
м. Львів	ТОВ"Офіс-Сервіс"	97-86-81, 98-00-80
м. Маріуполь	ЗАТ "Бліц-Інформ"	(0629) 33-54-98, 53-24-61
м. Миколаїв	ЗАТ "Бліц-Інформ"	(0512) 47-10-82, 47-49-55
м. Миколаїв	ПП "Інформ-Центр"	35-11-65, 35-63-18
м. Миколаїв	ТОВ "Ноу-Хау"	36-20-03, 47-25-47
м. Одеса	ЗАТ "Бліц-Інформ"	(048) 711-70-79, 714-48-82
м. Одеса	СПД "Пугачьова І.Ю."	760-17-21, 760-17-81
м. Одеса	ТОВ "Ласка"	711-66-16, 63-44-00
м. Одеса	Центр підписки "МіМ"	777-45-38
м. Полтава	ЗАТ "Бліц-Інформ"	(0532) 56-26-17, 50-92-61
м. Рівне	ЗАТ "Бліц-Інформ"	(0362) 62-33-06, 62-56-26
м. Рівне	Чимшит Олег Валерійович	22-31-06, 29-04-69
м. Севастополь	ЗАТ "Бліц-Інформ"	(0692) 55-44-51, 54-53-71
м. Севастополь	ПП "Істар"	71-62-19, 71-63-19
м. Сімферополь	ЗАТ "Бліц-Інформ"	(0652) 249-300
м. Сімферополь	ПП "Фактор"	27-44-31
м. Сімферополь	РКА "ЛБ-Сервіс" ЛТД	26-08-45
м. Сімферополь	ТОВ "Флора"	27-00-92, 27-95-10
м. Суми	ЗАТ "Бліц-Інформ"	(0542) 27-52-09, 21-36-99
м. Тернопіль	ЗАТ "Бліц-Інформ"	(0352) 25-88-59
м. Тернопіль	ТОВ "Айсберг" 46001, ул Грушевского, 23	
м. Ужгород	"Афіша Закарпаття"	3-55-12
м. Ужгород	ЗАТ "Бліц-Інформ"	(0312) 61-42-88, (03122) 2-38-63
м. Харків	ДП "Агенство підписки та реклами"	43-11-89
м. Харків	ТОВ "Всеукраїнська служба підписки"	14-11-27, 40-96-14
м. Харків	ТОВ "Інститут електродинаміки"	712-55-20, 19-15-76
м. Харків	ТОВ ИА "Лавина"	18-50-00
м. Харків	ДП "Фактор-Преса"	32-11-71, 32-23-11
м. Харків	ЗАТ "Бліц-Інформ"	(0572) 17-03-23, (057) 702-04-10
м. Херсон	ЗАТ "Бліц-Інформ"	(0552) 32-57-37
м. Херсон	ХФ "Ноу-Хау"	26-50-83
м. Хмельницький	ЗАТ "Бліц-Інформ"	(0382) 79-24-23, 79-55-12
м. Хмельницький	ПФ "Європроф"	76-59-20
м. Черкаси	ЗАТ "Бліц-Інформ"	(0472) 47-05-51, 32-13-89
м. Чернівці	ЗАТ "Бліц-Інформ"	(03722) 2-00-72, 2-55-70
м. Чернігів	ЗАТ "Бліц-Інформ"	(0462) 10-18-82

Предплатна Агенція «KSS» (КСС) передплата і доставка видань

тел. (044) 464-02-20
багатоканальний
інтернет-передплата:
www.kss.kiev.ua

Пункти прийому передплати по Україні та Молдові:
Алчевськ (06442) 2-2244, 2-9294
Бердянськ (06153) 6-3415
Вінниця (0432) 32-3000
Дніпропетровськ (0562) 32-2257
Донецьк (062) 345-0359,90-5899
Запоріжжя (0612) 13-4950, 49-9600
Івано-Франківськ (03422) 7-0440
Ілліївськ (0482) 370-555, (048) 714-34-34
Ізмаїл (04841) 2-0335
Київ (044) 464-0220
Кривий Ріг (0564) 74-6642, 65-7334
Кіровоград (0522) 29-9650, 56-5103
Кишенеу (103732) 27-7027
Львів (0322) 41-9165, 41-9166
Маріуполь (0629) 34-8428
Одеса (048) 777-03-55
Рівне (0362) 28-0994
Сімферополь (0652) 24-8579
Суми (0542) 21-9550
Тернопіль (0352) 43-0427
Ужгород (03122) 3-4220
Харків (0572) 38-2150
Херсон (0552) 26-4232, 28-2169
Хмельницький (03822) 3-2931
Черкаси (0472) 65-5238

Кур'єрське обслуговування відкрито в містах:
Алчевськ, Бердянськ, Вінниця, Вознесенськ, Донецьк, Дніпропетровськ, Дніпродзержинськ, Запоріжжя, Івано-Франківськ, Ізмаїл, Іллічівськ, Київ, Кіровоград, Ковель, Кременчук, Кривий Ріг, Лисичанськ, Львів, Луганськ, Луцьк, Маріуполь, Мелітополь, Миколаїв, Одеса, Полтава, Павлоград, Рівне, Сімферополь, Севастополь, Сєвєродонецьк, Суми, Тернопіль, Харків, Херсон, Хмельницький, Чернігів, Черкаси