МАРКЕТИНГОВОЕ ИССЛЕДОВАНИЕ
«РОССИЙСКИЙ РЫНОК СИСТЕМ БЕЗОПАСНОСТИ»
РЕЗЮМЕ
ПАРАМЕТРЫ ИССЛЕДОВАНИЯ

Параметр исследования	Описание параметра
Цель исследования	Анализ российского рынка систем безопасности.
Задачи исследования	1. Обзор мирового рынка систем безопасности (объем, сегментация, основные лидеры рынка по сегментам)
	2. Определение основных параметров российского рынка систем безопасностей (объем, структура, региональные особенности, тенденции развития)
	3. Исследование рынка информационной безопасности (объем, динамика, структура, сегментация потребителей, тенденции развития)
	4. Определение основных участников рынка и особенностей конкурентной среды
	5. Выявление основных потребителей и их предпочтений на рынке систем безопасности
	6. Анализ сбытовой политики и способов продвижения на рынке
	7. Анализ таможенной статистики в разрезе двух сегментов: индикаторных панелей и сигнализационных устройств
	8. Выявление нормативной базы рынка
	9. Прогноз развития рынка на 2009-2010 гг.
Методы исследования и источники информации	Экспертные оценки, кабинетное исследование, анализ вторичной информации, данные ФТС и игроков рынка
Дата проведения исследования	июнь 2009 года
География исследования	Россия

ОСНОВНЫЕ ВЫВОДЫ ПО ИССЛЕДОВАНИЮ

Объем мирового рынка составляет 215 млрд. долл. Темпы роста составили 7%в год

В структуре мирового рынка безопасности на долю рынка услуг приходится около 70%, на долю рынка средств безопасности - 30%.

Наибольшая доля рынка - 27% приходится на защиту от вторжения. 12% составляет доля сегмента по идентификации и обнаружению. Пожарная безопасность занимает 12%, видеонаблюдение - 20% и контроль доступа - по 17%.

В сегменте сетевой защиты самое распространенное средство защиты - межсетевой экран. Здесь лидирует компания Cisco (доля рынка - 41,7%), Juniper (18,1%) и Nokia (13,5%).

В сегменте систем обнаружения и предотвращения атак доля рынка компании Cisco составляет 29,4%, доля рынка ISS - 15,2%. В сегменте средств управления патчами доля рынка компании Patchlink составляет 14,4%, доля рынка Shavlink technologies - 11.6%.В сегменте средств расследования инцидентов лидером является компания Guidance, захватившая треть сегмента рынка (34,3%). За ней следует NIKSUN с 21,4%.

В сегменте средств управления сигналами тревоги наибольшую долю занимает компания HP -17%, на втором месте

SISCO - 12%.

В сегменте сетевых сканеров безопасности наибольшую долю занимает компания Internet security - 30%, на втором месте Qualys - 14%/

В сегменте хостовых IPS наибольшую долю занимает CISCO - 28%, на втором месте SYMANTEC - 22%

Российский рынок систем безопасности

Объем российского рынка систем безопасности и охранных услуг составляет около 6 млрд. долл.

Крупнейшим сегментом рынка является охранная и пожарная сигнализация, на долю которой приходится примерно 31%.

Наибольшая доля рынка приходится на два крупнейших мегаполиса - Москву и Санкт-Петербург. 23% потребителей проживают в Москве, этот показатель уменьшился с 28% в 2006 году до 23% в 2008 году. 21% проживает в Санкт-Петербурге

Доля центрального федерального округа составляет 35%,доля Северо-Западного - 25%,Приволжского федерального округа - 12%,Сибирского федерального округа - 11%, Уральского и Южного федеральных округов – по 7%, Дальневосточного-3%.

Рынок информационной безопасности

Объем рынка защиты информации составляет около 285 млн. долл.

Наибольшую долю занимает сегмент продаж продуктов - 58%, на втором месте - внедрение (31 %), на третьем месте - аудит (9%).

Наибольшую долю в структуре потребителей занимает крупный бизнес (40%),на втором месте - SMB (30%), на третьем месте - гос. органы (27%).

Примерно половина (50,6%) участников исследования считает, что защита корпоративных секретов всегда является первоочередной задачей, а 22,7%респондентовзаявили, что укрепление ИБ особенно важно в кризисные времена для повышения конкурентоспособности. Только 5,2% специалистов считают, что сэкономить можно и на безопасности.

Потребители систем безопасности

Среди покупателей различных систем безопасности преобладают технические специалисты фирмы по безопасности и проектировщики систем безопасности. На третьем месте - менеджеры по логистике и закупкам.

Что касается отраслей, то 33% потребителей работают в сфере безопасности,10% - в строительстве, 7% - в сфере информационных технологий

Спрос на системы безопасности также подвержен сезонным колебаниям.

На отношение потребителей сильно влияют популярность бренда, время его нахождения на отечественном рынке, а также статус дистрибуторов.

Импорт систем безопасности

Объем импорта индикаторных панелей составил 19 840 тыс. долл. В стоимостном выражении и 368 тонн в натуральном выражении. Темпы роста импорта индикаторных панелей в стоимостном выражении увеличились на 19%, а в натуральном выражении объем импорта сократился на 3%.

В структуре импорта индикаторных панелей в стоимостном выражении по странам-поставщикам большая часть приходится на Францию, которая ввозит в Россию 36% всех ввозимых индикаторных панелей, доля Китая в общем импорте составляет около 22%, на долю Германии приходится 9%.

Объем импорта сигнализационных устройств составил 60 931тыс. долл. в стоимостном выражении и 1 570 тонн в натуральном выражении. Темпы роста импорта сигнализационных устройств в стоимостном выражении увеличились на 15%, а в натуральном выражении объем импорта сократился на 22%.

В структуре импорта сигнализационных устройств в стоимостном выражении по странам-поставщикам большая часть приходится на США, которые ввозят в Россию 29%всехввозимых сигнализационных устройств, доля Италии в общем импорте составляет около 16%. На долю Украины приходится 11 %.

Экспорт систем безопасности

Объем экспорта индикаторных панелей составил 7 362 тыс. долл. в стоимостном выражении и 17 тонн в натуральном выражении. Экспорт индикаторных панелей в стоимостном выражении увеличился на 96%, а в натуральном выражении рост экспорта составил 339%.

В структуре экспорта индикаторных панелей в стоимостном выражении по странам-получателям большая часть приходится на Узбекистан, в который вывозится из России24% всех вывозимых индикаторных панелей, доля Украины в общем экспорте составляет около 23%. Доля Казахстана составляет12%.

Объем экспорта сигнализационных устройств составил 17 201тыс. долл. В стоимостном выражении и183 тонны в натуральном выражении. Экспорт сигнализационных устройств в стоимостном выражении увеличился на 3%, а в натуральном выражении спад экспорта составил 9%.

В структуре экспорта сигнализационных устройств в стоимостном выражении по странам-получателям большая часть приходится на Казахстан, в который вывозится из России 35% всех вывозимых сигнализационных устройств, доля Украины в общем экспорте составляет около 16%. Доля Туркмении составляет14%.

КЛАССИФИКАЦИЯ СИСТЕМ БЕЗОПАСНОСТИ

К системам безопасности относят все технические средства охраны, а также противопожарные системы, антитеррористическое оборудование, системы связи и оповещения и средства личной безопасности.

Рынок можно классифицировать на следующие группы:

Системы безопасности

Охранное телевидение
Противокражное оборудование

Охранная и пожарная безопасность
Контроль и управление доступом

Средства и системы пожаротушения
Системы защиты компьютерных систем

Интеллектуальное здание
Переговорные и
видеопереговорные
системы
Средства
индивидуальной
защиты
Системы оповещения и управления эвакуацией
Интегрированные системы безопасности
Инженерно-технические
средства защиты
информации
Антитеррористическое и досмотровое оборудование
Системы связи

Современные системы безопасности - это высокотехнологичные программно-аппаратные комплексы, объединяющие в себе систему видеонаблюдения, охранно-пожарную сигнализацию, систему управления и контроля доступа, а также прочее специализированное оборудование.

К системам видеонаблюдения относят : телевизионные видеокамеры, сетевые видеоустройства, видеоквадраторы, коммутаторы видео -сигналов (свитчеры), переключатели, селекторы, видеодетекторы движения, мультиплексоры, видеомагнитофоны и видеорегистраторы, устройства для просмотра видеоизображения, многофункциональные цифровые системы видеонаблюдения, устройства видеозахвата, устройства передачи и коррекции видеосигналов, мониторы для систем видеонаблюдения, видеопринтеры, устройства наведения камер (поворотные устройства, сканеры), средства управления CCTV.

Устройства контроля доступа включают в себя: идентификаторы, считыватели, контроллеры, контроллеры считыватели, системы изготовления пропусков, карт, бэджей, программное обеспечение, замки и защелки, доводчики дверные и автоматика для дверей, кнопки выхода, автоматические двери, турникеты, автоматические проходные, калитки, ограждения, шлюзовые тамбуры и кабины, ворота и автоматика для ворот, шлагбаумы, системы парковки, средства принудительной остановки транспорта, металлодетекторы, блоки питания и аккумуляторы.

В состав охранно-пожарной системы безопасности входят: охранные извещатели (датчики), приемно-контрольные панели, пульты управления и индикации, релейные и переключающие модули, интерфейсные модули, интерфейс RS232, центральные станции, программное обеспечение, оповещатели, системы оповещения и управления эвакуацией (СОУЭ), радиосистемы передачи извещений, системы охранной сигнализации, радиолучевые системы, инфракрасные системы, емкостные системы, вибрационные системы, проводно-радиоволновые, сейсмические системы, армированная колючая проволока, магнитометрические (магнитные) системы, обрывные системы.

Антикражные системы представлены антеннами, деактиваторами, активаторами, аппликаторами, съемниками, жесткими ярлыками, датчиками и метками, этикетками, клеящимися метками, защитными сейферами.

В состав антитеррористического и досмотрового оборудования включают металлодетекторы, рентгеновское оборудование и комплексы, обнаружители паров взрывчатых веществ, обнаружители наркотических веществ, обнаружители часовых механизмов, устройства локализации и защиты от взрывов, приборы радиационного (дозиметрического) контроля, тепловизионные системы контроля, видеоскопы, эндоскопы технические, приборы ночного видения, досмотровые инструменты и приспособления.

В средства по защите информации входят: средства защиты информационных каналов, средства выявления каналов утечки информации, защита от несанкционированного доступа к информации (НСД), устройства уничтожения информации, средства восстановления и реконструкции информации, защита информации в компьютерных системах и сетях.

К числу переговорных и видеопереговорных систем относят: аудиодомофоны, видеодомофоны, квартирные многопользовательские аудио/видео системы, интеркомы, переговорные устройства селекторной связи, интерфоны, переговорные устройства внутренней телефонной связи, системы селекторной связи с трубочными подстанциями, системы оповещения, цифровые переговорные устройства, многофункциональные системы переговорных устройств.
Комплексные (интегрированные) системы безопасности - это ступень, предшествующая созданию «интеллектуального»

здания. Под ними понимается совокупность средств, обладающих технической, информационной и эксплуатационной совместимостью, которые связаны единой управляющей программой (системой сбора и обработки информации). «Интеллектуальное здание» представляет собой интеграцию всех инженерных систем и их объединение под управлением единого центра.

Работа систем электроснабжения, отопления, вентиляции и кондиционирования синхронизируется с определенным распорядком дня и заданными режимами. При этом появляется возможность экономии, которая достигается за счет выбора оптимальных режимов работы оборудования, принятия обоснованных оперативных решений по управлению технологическими процессами, применения ресурсосберегающих технологий в системах энергопотребления и жизнеобеспечения.

Автоматизированные системы управления позволяют повысить безопасность и улучшить условия находящихся внутри здания людей, поднять на новый уровень эффективность функционирования инженерных систем и оперативность принятия решений в чрезвычайных ситуациях, оптимизировать производственные процессы.

МИРОВОЙ РЫНОК СИСТЕМ БЕЗОПАСНОСТИ

ОСНОВНЫЕ ПАРАМЕТРЫ РЫНКА

Объем мирового рынка безопасности ежегодно растет на 7-12%, в 2008 году он составил примерно 215 млрд. долл. Темпы роста в 2008 году составили 7%, являются минимальными за рассматриваемый период.

Мировой рынок систем и услуг безопасности характеризуется:

- высокой фрагментарностью,
- преобладанием малых и средних компаний,
- большим удельным весом высокотехнологичной продукции,
- зависимостью от правительственных заказов,
- нестабильностью и слабой прогнозируемостью доходов;
- недостаточной открытостью информации;
- процессом консолидации рынка.

СТРУКТУРА РЫНКА

В структуре мирового рынка безопасности на долю рынка услуг приходится около 70%, на долю рынка средств безопасности - 30%.

Наибольшая доля рынка - 27%приходитсяна защиту от вторжения. 12%
составляет доля сегмента по идентификации обнаружению. Пожарная безопасность занимает 12%, видеонаблюдение - 20% и контроль доступа -17%.

РЫНОК СЕТЕВОЙ БЕЗОПАСНОСТИ

Рынок межсетевых экранов и VPN

Самое распространенное средство защиты - межсетевой экран (он же firewall, он же брандмауэр, он же файрвол). Учитывая современную тенденцию использовать в сетевой безопасности аппаратные решения, рассмотрим сегмент программно-аппаратных межсетевых экранов (firewall appliance). Здесь, по данным ЮС, с существенным отрывом лидирует компания Cisco (доля рынка - 41,7%). Далеко позади Juniper (18,1%) и Nokia (13,5%). Доли рынка остальных компаний не превышают 27%.

Однако если посмотреть на долю рынка, определяемую исходя из объемов продаж (с точки зрения количества инсталляций, что лучше показывает интерес со стороны потребителя), то разрыв между Cisco и Juniper будет не двукратным, а восьмикратным.

Компания Check Point доминирует на рынке программных межсетевых экранов с долей в 57,1%. С большим отрывом за ней следует Microsoft (14,2%) и Symantec (5,5%).

Рынок систем предотвращения атак

За межсетевыми экранами идут системы обнаружения и предотвращения атак. Здесь лидер тот же - Cisco. А дальше уже совсем другие игроки. И отрыв от лидера не такой значительный как на рынке межсетевых экранов.

Игроки	Доля рынка, %	Число инсталляций	Средняя цена, долл.
Cisco	29,4%	13 853	12 397
ISS	15,2%	6 047	17 353
McAfee	9,3%	2 045	31 415
3Com / Tipping Point	8,5%	1 561	37 572
Juniper	5,7%	2 022	19 568

Таблица Характеристика крупнейших игроков в сегменте систем предотвращения атак

Рынок средств управления патчами

В корпоративной сети существует не только "периметровая" защита. Одна из важнейших задач, правильная реализация которой позволила бы практически исключить необходимость использования антивирусов и IPS, -

управление патчами, которые затыкают дыры в операционных системах, приложениях и сетевых сервисах. Явного лидера на этом новом сегменте рынка пока нет - три первых компании (PatchLink, Shavlik и Microsoft) вместе "держат" только треть всех продаж, а остальное распределено среди более мелких компаний.

На рынке средств управления патчами доля рынка компании Patchlink составляет 14,4%, доля рынка Shavlink technologies - 11.6%

Рынок средств расследования инцидентов

Расследование инцидентов необходимо в случае, если патч не был установлен, а атака произошла. В этом случае необходимо расследовать инцидент. Для этих целей на рынке достаточно давно появились системы автоматизации рутинных действий по анализу файлов и диска, журналов регистрации и т.п. Признанным лидером в этой области является компания Guidance, захватившая треть сегмента рынка. За ней следует NIKSUN с 21,4%. Оставшиеся 45% делятся между другими игроками.

Рынок средств управления сигналами тревоги

Обилие средств защиты не только повышает уровень защищенности оператора связи, но и увеличивает нагрузку на администраторов безопасности, которым приходится оперировать поистине огромными объемами данных, сигнализирующих о несанкционированной активности.

Анализ сигналов тревоги осложняется тем, что среди них не все события представляют реальную опасность для инфраструктуры, а часть сигналов являются следствием ложного срабатывания системы защиты. Поэтому одна из первых задач администратора безопасности - определить, какие атаки требуют немедленной реакции, какие подождут своего часа, а какие можно спокойно проигнорировать. И эта задача не была бы столь сложна, если бы все сообщения, сгенерированные средствами защиты, соответствовали реальным атакам. Однако действительность такова, что атак, которые и впрямь могут нанести ущерб ресурсам сети, несоизмеримо меньше, чем событий, фиксируемых защитными механизмами.

Мнение о том, что ложное сообщение лучше, чем его отсутствие, далеко не всегда оправдано. Найти реальную атаку в сотнях мегабайт фиксируемых событий - все равно, что искать иголку в стоге сена. Но даже если вы совершили невозможное и обнаружили угрозу вашей сети, то необходимо оповестить об этом и других заинтересованных лиц - владельцев атакуемой системы или ее администратора, группу реагирования на инциденты и т.п.

Решить все эти проблемы одиночными средствами защиты невозможно. У одной системы не хватает механизма сопоставления разнородных событий безопасности, у другой отсутствует эффективный механизм хранения гигабайт собранных данных, третья не обладает системой генерации высокоуровневых отчетов, понятных руководству... Чтобы избежать описанных неприятностей, необходима эффективная система управления информационной безопасности, которая позволяет связать все используемые в сети защитные средства в единый управляемый комплекс. Такие системы известны под общим названием Security Information Management Systems (SIMS).

На рынке средств управления сигналами тревоги наибольшую долю занимает компания HP -17%, на втором месте SISCO - 12%.

Рынок сетевых сканеров безопасности

Чтобы узнать про уязвимости, которые затем будут устраняться патчами, необходимы сканеры безопасности, которые дистанционно сканируют сотни и тысячи узлов в поисках различных уязвимостей, потенциально доступных злоумышленникам. Российский рынок мало что знает об этом сегменте, кроме одного имени - компании 1SS, которая была куплена IBM. Зато на российском рынке хорошо известна X-Spider - российская разработка, которая пока не попала в международные "чарты".

На рынке сетевых сканеров безопасности наибольшую долю занимает компания Internet security - 30%, на втором месте Qualys - 14%/

Рынок хостовых IPS

В отдельную категорию средств защиты входят решения для отражения широкого спектра угроз на персональные компьютеры и лэптопы. Если раньше большой популярностью пользовались персональные межсетевые экраны, то сейчас этот интерес спадает. Это связано с тем, что очень сложно бывает заранее описать, с какими IP-адресами можно общаться, а с какими нет. Системы предотвращения атак (особенно те, которые используют поведенческий, а не сигнатурный контроль) позволяют уйти от этой проблемы и сконцентрироваться на задаче отражения широкого спектра угроз, включая утечку информации через USB и другие носители, контроль загрузки с посторонних носителей и т.д.
На рынке хостовых IPS наибольшую долю занимает CISCO - 28%, на втором месте SYMANTEC - 22%/

Были рассмотрены далеко не все сегменты рынка информационной безопасности, но уже можно делать определенные выводы. Рынок постепенно консолидируется, все чаще в разных сегментах повторяются одни и те же имена. Небольшие компании - стартапы выводят на рынок новые технологии. И, возможно, со временем на этом рынке останется всего несколько крупных игроков, как это происходит на рынке браузеров, СУБД или ERP-систем.

РОССИЙСКИЙ РЫНОК СИСТЕМ БЕЗОПАСНОСТИ
ОСНОВНЫЕ ПАРАМЕТРЫ РЫНКА

В 2008 г. общий объем российского рынка систем безопасности и охранных услуг составил около 6 млрд. долл. По отношению к предыдущему году рынок в стоимостном выражении (долл. США) остался на прежнем уровне.

До финансово-экономического кризиса, рынок систем безопасности являлся быстрорастущим рынком, каждый год объем оборотов на нем увеличивается от 10 до 35% в зависимости от сектора. Однако в связи с изменением экономической ситуации, темпы роста резко сократились.

Крупнейшим сегментом рынка является охранная и пожарная сигнализация, на долю которой приходится примерно 31%. Это легко объясняется тем, что государством установлена уголовная и административная ответственность за правонарушения, в области обеспечения пожарной безопасности, и любое построенное здание обязательно должно соответствовать требованиям пожарной безопасности. Второй по величине сегмент — охранное телевидение - занимает 25% рынка, а замыкает тройку СКУД с 15%. На сегменты системы охраны периметра и систем пожаротушения приходится 8% и 11% соответственно. На прочие системы безопасности приходится 10% рынка.

Таким образом, в 2008 году объем на рынке технических систем безопасности составил в каждом сегменте:
Охранная и пожарная сигнализация - 1,86 млрд. долл.
Охранное телевидение - 1,5 млрд. долл.
СКУД - 0,9 млрд. долл.;
Системы пожаротушения - 0,66 млрд. долл.
Системы охраны периметра - 0,48 млрд. долл.
Остальное - 0,6 млрд. долл.

РЕГИОНАЛЬНОЕ РАСПРЕДЕЛЕНИЕ РЫНКА

Наибольшая доля рынка приходится на два крупнейших мегаполиса - Москву и Санкт-Петербург. 23% потребителей проживают в Москве, этот показатель уменьшился с 28% в 2006 году до 23% в 2008 году. 21% проживает в Санкт-Петербурге - (это объясняется высокой покупательной способностью предприятий и большим числом банков).

Доля центрального федерального округа составляет 35%, доля Северо-Западного -25%, Приволжского федерального округа - 12%, Сибирского федерального округа - 11%, Уральского и Южного федеральных округов - по 7%, Дальневосточного - 3%.

Распределение клиентов по городам

Доля центрального федерального округа составляет 35%, доля Северо-Западного -25%, Приволжского федерального округа - 12%, Сибирского федерального округа - 11%, Уральского и Южного федеральных округов - по 7%, Дальневосточного - 3%.

В целом спрос на системы безопасности определяется размещением промышленных групп, уровнем развития финансовой системы, а также имеющимися доходами населения.

Региональный рынок информационной безопасности не отстает по своему развитию от столичного рынка, это связано с тем, что: развитие информационных технологий позволяет регионам быть в одном информационном поле со столицей. Многие предприятия в регионах за последние 10 лет тем или иным образом стали частью крупных холдингов, которые уделяют большое внимание вопросам развития ИТ-систем в общем и информационной безопасности в частности. Современные требования бизнеса диктуют одинаковые условия развития абсолютно всем компаниям, независимо от их географического местоположения, направления деятельности и размера.

Крупнейшие компании осознают перспективы регионального развития и открывают в городах - миллионниках филиалы.

РЫНОК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные параметры рынка

Информационная безопасность (ИБ) организации - задача, решение которой сочетает в себе административные, технические и программные средства.

Объем рынка защиты информации в 2008 году составил около 285 млн. долл.

Этот рынок достаточно четко сегментирован. Всего можно выделить 5 классов технологий, используемых на рынке:
защита от утечек (Anti-Leakage Software),
средства внутреннего контроля (Internal Controls),
системы сильной аутентификации (ЗА:аутентификация,авторизация,администрирование),
предотвращение нецелевого использования почтовых ресурсов и интернета,
архивирование корпоративной корреспонденции.

Структура рынка по сегментам

Рассматривая более подробно структуру рынка, можно выделить четыре основных сегмента, рост которых будет продолжаться и далее:

- продажа решений по защите информации,
- аудит безопасности,
- внедрение
- аутсорсинг.

Наибольшую долю в 2008 году занимал сегмент продаж продуктов - 58%, на втором месте - внедрение (31%), на третьем месте - аудит (9%).

Такое преобладание продаж продуктов объясняется высокой степенью консерватизма рынка ИБ. Многие коммерческие и государственные организации стараются не допускать к своим внутренним ресурсам сторонних специалистов и пытаются решать возникающие задачи собственными силами. Но с усложнением бизнеса этих организаций и, соответственно, IT-проблем (включая подготовку и проведение аудита, сертификацию по стандартам и многое другое) обращение к внешним консультантам будет неизбежно и в количественном отношении только возрастет.

Сегментация потребителей на рынке

В большинстве отраслей уровень затрат на ИБ и развитие рынка ИБ напрямую зависит от наличия в них крупных холдингов, имеющих единую и предпочтительно территориально-распределенную инфраструктуру. Подобные холдинги, как правило, обладают достаточно большими массивами конфиденциальной информации. Стабильность работы телекоммуникационной и сетевой инфраструктуры имеет для них большое значение, поэтому они вынуждены выделять значительные средства для комплексного обеспечения информационной безопасности. Компании среднего и малого бизнеса именно сейчас начинают активно использовать те средства защиты, которые отраслевые лидеры и госструктуры используют в обязательном порядке уже несколько лет— межсетевые экраны, сетевое антивирусное ПО и т. д.
Условно рынок потребителей ИБ можно разделить на четыре основные группы:
гос. органы,
крупный бизнес,
SMB
частные клиенты.

Наибольшую долю в структуре потребителей ИБ в 2008 году занимал крупный бизнес (40%), на втором месте - SMB (30%), на третьем месте - гос. органы (27%).

По мнению экспертов, с развитием рынка структура потребителей будет постепенно меняться.
Для нее станет характерно:
снижение доли гос. органов;
снижение доли крупного бизнеса;
рост сегмента SMB;
рост частных потребителей.

Снижение доли гос. органов. Обусловлено постепенным общим снижением их затрат на автоматизацию. В 1990-е и начале 2000-х годов именно гос. органы были основными потребителями IT, но с развитием рынка и постепенным насыщением этого сектора современными IT средства, выделяемые на закупку IT (в том числе и безопасность), будут сокращаться. Это приведет к постепенному сокращению их доли. Увеличение доли гос. органов возможно, если на IT будут выделяться деньги в рамках национальных проектов.

Снижение доли крупного бизнеса. Причины сокращения доли крупного бизнеса аналогичны. В основном эти компании уже прошли этап большой автоматизации, и соответственно, их доля будет постепенно сокращаться. Однако именно в среде крупного бизнеса происходят основные изменения структуры потребления. В этом сегменте наиболее востребованы услуги, связанные с аудитом IT, а также с защитой ранее незащищенных областей.
Рост сегмента SMB. В связи с тем, что именно в сегменте SMB наблюдается основной рост потребления IT, в этом сегменте будет наблюдаться и наибольший рост средств IT-защиты. Особенностью данного сегмента в ближайшее время будет то, что в нем будут потребляться самые простые средства, без использования которых нормальное бесперебойное функционирование IT невозможно. Это прежде всего средства защиты периметра.

Рост сегмента частных потребителей. Частные клиенты начинают «обелять» свое ПО, закупка ими оригинальных средств защиты будет постепенно возрастать. Также росту данного сегмента способствуют OEM-программы, когда частный покупатель вместе с компьютерной техникой приобретает уже инсталлированные средства защиты.

В целом, именно рынок средств защиты наименее «пиратский». По мнению опрошенных экспертов, это связано с тем, что как для корпоративных, так и для частных пользователей защита данных — одна из первостепенных задач, а использование «пиратских» средств само по себе несет риск потери или утечки информации. Поэтому данный рынок первым стал выходить из «тени».

Тенденции на рынке

Ожидается, что в ближайшие годы рост рынка ИБ будет и дальше плавно снижаться от уровня прироста в 40% в год до темпов роста рынка IT — 5%. При этом корпоративный и государственный сектор, а также наиболее прогрессивные компании рынка SMB уже видят недостатки существующего спектра предложений на рынке ИБ и готовы перейти на новую модель потребления услуг И Б.

Сегодня рынок ИБ не сбалансирован, структура предложения формируется не потреблением, а предложением. На рынок выводятся все новые продукты, для которых разработчики и интеграторы находят «нужные» ниши и предлагают «правильные» рекомендации. Пользуясь подобными рекомендациями, можно купить приличный комплект ПО только для защиты от, например, вирусов: три обычных антивируса для эшелонированной защиты, antispyware, специальный антивирус от макровирусов или полиморфных вирусов (когда продукт не может найти свое место на рынке, он«специализируется»). Таким же образом можно «защитить» свою компанию от любой угрозы, при этом оставшись незащищенным — средства будут защищать сами себя, а информация будет утекать или пропадать по причинам, не описанным на сайтах выбранных поставщиков.

Пик потерь компаний приходится не только на информационные риски. Еще дороже, как оказывается, обходится компаниям невнимательность сотрудников, даже самых профессиональных. Сложно представить, что службы

безопасности подобных компаний не профессиональны или не используют солидный набор инструментов для защиты. И дело здесь не столько в постоянно эволюционирующих угрозах. Компаниям необходима экспертиза ИБ, независимая от определенных продуктов в области ИБ или определенного набора услуг компании эксперта. Риски привлечения сторонней компании к изучению своей IT-инфраструктуры несоизмеримо меньше рисков проектирования ненадежной системы ИБ.

Особенно, если сторонняя компания гарантирует качество и конфиденциальность оказания услуг.

Проведенное исследование российского рынка ИБ дает ясную картину состояния рынка и тенденций. Потребители услуг и продуктов в области ИБ все больше влияют на структуру и качественный состав участников рынка, что говорит о переходе к более зрелому этапу.

Влияние производителей продуктов и решений, равно как и системных интеграторов, имеет тенденцию к снижению. На смену им придут не зависимые от разработчиков и особенностей собственной ресурсной базы компании эксперты, которые будут работать по модели «компания — адвокат потребителя». Также на рынке будет популярна модель аренды персонала под выполнение конкретных задач и реализации спроектированных систем ИБ.

Тенденция роста доли услуг на рынке продолжится. Структура рынка услуг также претерпит существенные изменения в силу появления новых игроков, компаний с принципиально новым подходом к оказанию услуг, доступных гораздо большему числу потребителей. Рынок SMB тоже станет заметным потребителем услуг и продуктов в области ИБ за счет структурных изменений и роста числа угроз и ценности информации. Совокупно рынок ИБ продолжит расти опережающими темпами относительно рынка IT, но при этом появится тенденция к насыщению, то есть темпы роста постепенно будут снижаться.

Развитие рынка в период кризиса

Как показало исследование на рынке информационной безопасности в период финансово-экономического кризиса, даже в столь неблагоприятном климате на рынке важность ИБ не вызывает сомнений. Примерно половина(50,6%) участников исследования считает, что защита корпоративных секретов всегда является первоочередной задачей, а 22,7% респондентов заявили, что укрепление ИБ особенно важно в кризисные времена для повышения конкурентоспособности. Только 5,2% специалистов считают, что сэкономить можно и на безопасности.

Как оказалось, участники исследования видят в кризисе не только отрицательные, но и положительные моменты. Так, компании получают мотивацию к сокращению лишних расходов (47,6%). Финансирование будет выделяться, прежде всего, на ИБ -проекты с быстрой и очевидной отдачей. Особую роль будет играть профессионализм и оперативность внедренцев ИБ - решений.

Как показал опрос, только несколько процентов наиболее дальновидных компаний увеличивают расходы на безопасность. Остальные вынуждены сокращать расходы, прежде всего на оборудование (42,1% организаций) и программное обеспечение (37%). Приостанавливаются проекты без гарантированного результата, прекращается пора масштабных закупок. В этой ситуации возрастает роль консультантов и внедренцев, которые будут доводить проекты до конца и обеспечивать эффективность вложений в безопасность.

При отсутствии денег на приобретение новых средств ИБ компании будут более полно использовать существующие. К тому же, многие крупные организации и госструктуры располагают арсеналом не доведенных до эксплуатации систем. В условиях, когда крупные интеграторы уже выбрали все ресурсы по данным проектам, на помощь придут команды профессиональных консультантов и внедренцев. "В условиях "финансового благополучия" контракты на ИБ -проекты часто получали крупные системные интеграторы благодаря устоявшейся репутации либо личным связям. Сегодня же, когда компании как никогда озабочены эффективностью вложений в ИТ и ИБ, преимущество будет уже на стороне небольших компаний профессионалов, готовых предложить действительно лучшие условия.

Эффективным способом сокращения финансирования без ущерба для безопасности является перераспределение средств между статьями расходов. Более всего в сложившейся ситуации востребованы будут продукты для защиты информации от разворовывания, а также услуги профессиональных консультантов по ИБ. Кроме того, компании переориентируются с интеграторов широкого профиля на профессиональных консультантов по ИБ, предлагающих более качественные услуги за меньшие деньги.

В то же время, несмотря на тотальное сокращение расходов, отдать ИБ на аутсорсинг готовы только в 5,5% компаний. Вместе с тем, организации не имеют противопоказаний для привлечения внешних ИБ -консультантов на конкретные проекты. Это позволит получить услуги высокого качества по разумной цене и сохранить независимость службы ИБ. Несмотря на непростую для некоторых компаний ситуацию, перспективы развития отрасли ИБ в России достаточно оптимистичны. Скорее всего, отдельные компании, в том числе и работающие в сфере ИБ, вынуждены будут уйти с рынка. Однако их сотрудники не останутся на улице и перейдут к конкурентам. Те, в свою очередь, пройдя через кризис, станут только сильнее, и смогут продолжить экспансию, в том числе и на иностранные рынки.

УТЕЧКА ИНФОРМАЦИИ

Именно бизнес больше всего страдает от утечек конфиденциальной информации.

В исследовании8 проводился анализ инцидентов внутренней информационной безопасности. Целью исследования было проанализировать все утечки конфиденциальной информации (в том числе, персональных данных), упоминавшиеся в СМИ. Анализировались инциденты во всех странах мира и во всех отраслях.

Всего за отчётный период (9 месяцев 2008 года) зафиксировано 249 инцидентов, то есть, более чем по одному инциденту в день. Если просуммировать общее число записей персональных данных (почти всегда сообщается о том, сколько человек затрагивает утечка), то получится 106 996 883 записей или 390 500 записей в день (строго говоря, прямое суммирование не совсем корректно, поскольку два разных инцидента могут касаться одного и того же лица, но вероятность этого совпадения мала). То есть, можно сказать, что утечки затронули интересы более 100 миллионов

человек.

Причины утечки информации

Все причины утечки поделены на умышленные и неумышленные (случайные).

Достаточно распространены кражи компьютерной техники; в таком случае утечка считается случайной, если есть достаточные основания полагать, что целью вора была материальная часть похищенной техники, а не информация на ней.

Как и в прошлые периоды, количество случайных утечек существенно больше. Но их процент несколько снизился. Снижение это можно отнести на изменение политики учёта. Часто невозможно чётко установить, была ли утечка действительно случайная (обусловленная небрежностью, беспечностью, неблагоприятным стечением обстоятельств), или такое заявление призвано покрыть злой умысел. Если раньше подобные сомнительные случаи учитывались в разделе «случайные утечки», то ныне они помечаются как «причина не установлена».

Несмотря на изменение статистики, по-прежнему можно уверенно утверждать, что приоритетной задачей является борьба с ненамеренными утечками информации. Поскольку противодействовать таким утечкам проще, дешевле, а в результате покрывается большая часть инцидентов.

Борьба с намеренными утечками - задача более сложная. Эффективность такой борьбы будет заведомо ниже, поскольку предстоит столкнуться с противодействием злонамеренных инсайдеров. А доля соответствующих утечек намного меньше половины.

Структура утечек по типу организаций

Источники утечек, разделены на три категории:
государственные,
коммерческие
прочие.

В последнюю категорию включены все учебные заведения. Хотя формально школы и вузы могут числиться «коммерческими» или государственными. Традиционно учебные заведения довольно сильно отличаются по принятым в них порядкам как от производственных предприятий, так и от государственных органов. Причем доля умышленных утечек больше в коммерческих, образовательных и общественных организациях - 49% и 33% соответственно. Случайные утечки чаще по отношению к среднему встречаются в коммерческих и государственных организациях - 49% и 19% соответственно.

Распределение мало изменилось по сравнению с первым полугодием 2008 и даже по сравнению с 2007 годом. Меры по предотвращению утечек конфиденциальной информации предпринимаются как в государственных, так и в коммерческих информационных системах. В вузах эти меры также вводятся, правда, за неимением денег там упор делается не на технические средства, а на организационные. Как видим (сравнивая данные 2007 года и первого полугодия 2008), доля образовательных учреждений растёт, но медленно. Это означает, что с утечками можно бороться при различном уровне финансирования.

Латентность утечек

Следующая таблица иллюстрирует латентность утечек персональных данных.

Страна	Число утечек	Доля	Утечек на млн. населения
AU	1	0.40%	0.050
CA	5	2.01%	0.154
CL	1	0.40%	0.064
CN	3	1.20%	0.002
DE	2	0.80%	0.024
FR	1	0.40%	0.017
GB	23	9.24%	0.382

Страна	Число утечек	Доля	Утечек на млн. населения
IE	3	1.20%	0.500
IN	1	0.40%	0.001
IT	2	0.80%	0.034
KR	3	1.20%	0.062
RU	4	1.61%	0.028
US	192	77.11%	0.655
Другие	7	2.81%	

Таблица . Латентность утечек персональных данных

Число утечек в расчёте на 1 миллион населения для стран, где учёт поставлен нормально, изменилось мало. По-прежнему можно сказать, что приблизительно происходит 1 утечка в год на каждый миллион. Естественно, в этой цифре учтены лишь те утечки, которые стали достоянием гласности. По оценкам, латентных утечек происходит примерно ещё столько же. А в тех странах, где учёт поставлен не так строго, как можно заключить из сравнения показателей, латентность значительно выше. Там большинство утечек конфиденциальной информации скрывается от публики.

Структура утечек по типу конфиденциальной информации

Ниже представлено распределение утечек по типу разглашённой информации. Наверное, следует ещё раз подчеркнуть, что все факты собираются из сообщений прессы, которая пишет в основном о персональных данных. Поэтому существенной статистики по иным видам конфиденциальной информации нет. Факт утечки государственной тайны сам вполне может являться государственной тайной. Аналогично и с тайной коммерческой. Зато утечка персональных данных обычно оглашается при первой возможности.

Структура каналов утечки информации

Ниже показано распределение утечек по носителю. То есть, при помощи какого носителя (канала) конфиденциальная информация пересекла охраняемый периметр. Ниже, после общего распределения показано тоже распределение по носителям отдельно для умышленных и для случайных утечек. Больше всего данных утекает через сеть, а на втором месте - переносные компьютеры. Их теряют и крадут. Данная категория почти сравнялась с утечками через сеть (25 против 29%).

Для случайных утечек «мобильные носители» не только догоняют, но и уверенно опережают утечки через сеть (15 против 12%).

Трафик в частности и услуги связи в целом за последнее время подешевели, но не сильно. Зато мобильные носители информации - очень сильно. Гигабайтные флэшки продаются в газетных киосках как карандаши. В метро читающих книги стало меньше, чем читающих наладонники. Именно удешевление портативных компьютеров и иных носителей информации привело к росту доли «мобильных» утечек.

Наибольшая разница между умышленными и случайными утечками наблюдается (помимо мобильных носителей, что обсуждалось выше) для электронной почты и бумажных документов. Умышленных краж конфиденциальной информации с использованием электронной почты не зафиксировано вообще.

В предыдущем отчёте мы упоминали, что отправить электронное сообщение (да ещё и с приложением «тяжёлого» документа) не тому адресату - довольно затруднительно. Но, оказывается, возможно. Особенно учитывая современную моду, введённую известной софтверной корпорацией, не показывать пользователю адрес электронной почты, когда вполне «To:» или «From:» видно только имя. Оказалось, что ни один из злоумышленников этого года (во всяком случае, ни один из выявленных злоумышленников) не пожелал воспользоваться таким способом, как электронная почта. Таким, казалось бы, простейшим, очевидным, напрашивающимся способом. Инсайдеры предпочитали иные каналы: HTTP, флэшки, переносные диски, даже бумагу.Когдаслужбабезопасностизамышляетучинитьперлюстрациютрафика предприятия, начинают, как правило, именно с электронной почты. Зачастую ей и заканчивают.

ТЕНДЕНЦИИ В ОСНОВНЫХ СЕГМЕНТАХ РЫНКА

Среди основных тенденций рынка можно отметить:
интеллектуализация рынка;
развитие IP-видео технологий.

Заметной тенденцией на рынке CCTV (охранного телевидения) является рост спроса на интеллектуальные PC-based системы. На Западе камеры, например, уже давно и повсеместно в автоматическом режиме фиксируют нарушения правил дорожного движения. У нас подобная практика еще не получила столь широкого распространения, но решений отечественной разработки, функциональность которых значительно шире, нежели просто распознавание номеров, предостаточно. Использование интеллектуальных систем позволяет нескольким операторам отслеживать информацию с сотен камер наблюдения, а также уже сегодня реализовать довольно специфические возможности как распознавание лиц или оставленных предметов, цвета и марки автомобиля.

В сегменте СКУД необходимо отметить несколько важных тенденций:
интеграция с другими системами безопасное охранно-пожарной сигнализации, видеонаблюдения и др.
СКУД стали заметно чаще использоваться и для контроля рабочего времени, в частности именно это направление дало толчок к более активному использованию биометрических технологий. «интеллектуализация» СКУД, за счет использования специализированного программного обеспечения, которое стало сегодня залогом эффективного управления контролем доступа.

В системах видеонаблюдения эксперты определяютбудущее за IP-технологиями.

Преимуществами таких систем можно назвать: избавление от дорогостоящих и неудобных коаксиальных кабелей, быстрое развертывание системы, легкая масштабируемость в рамках распределенных объектов, возможность использования беспроводных технологий, централизованное управление.

Как следствие распространения IP-технологий отмечается повышенный интерес заказчиков к применению оптических методов передачи видеоинформации. Стоит отметить, что оптоволоконные сети легко модернизируются при необходимости передачи большего объёма видеоинформации, это свойство важно иметь в виду, при необходимости построения крупной сети, масштабы которой нельзя спрогнозировать заранее. Многие современные офисные здания уже при строительстве оснащаются сетевой инфраструктурой, и в этом случае очень часто выбор сразу падает на сетевые

камеры - это еще один фактор роста спроса на IP-решения. Если еще учесть, что цены на камеры быстро падают, а сейчас цена является едва ли не главной причиной выбора не в пользу IP, то вскоре можно ожидать настоящий бум на цифровые системы.

Одним из наиболее перспективных направлений в охранном бизнесе является пультовая охрана. В настоящее время, помимо вневедомственной охраны, системы пультовой охраны существуют также у частных компаний и количество их увеличивается. Компании производители систем безопасности способствуют этому, производя системы, способные интегрироваться и объединяться в единый центр - пульт охраны. Развитие технических средств охраны ранее сдерживалось необходимостью сравнительно высоких финансовых затрат для закупки и установки современного оборудования.

Сейчас вложения в ПЦО имеет хорошую отдачу, и большинство предприятий стремятся приобрести собственные пульты. В настоящее время с появлением GSM сигнализаций данная тенденция прослеживается как в области охраны недвижимости, так и в области охраны транспорта.

По мере развития уровня технологии на рынке систем безопасности наблюдается устойчивая тенденция к постоянному уменьшению формата, поскольку при этом падает цена изготовленной камеры видеонаблюдения. В настоящее время практически исчезли видеоматрицы форматов Г и 2/3", а наиболее распространены 1/2, 1/3" и 1/4". Эксперты прогнозируют бурный рост российского рынка ПО для систем безопасности: ИТ -директоры компаний все чаще ставят вопросы обеспечения информационной безопасности в один ряд с другими жизненно важными задачами.

УЧАСТНИКИ РЫНКА

КЛАССИФИКАЦИЯ ОСНОВНЫХ УЧАСТНИКОВ РЫНКА

Структура рынка технических систем безопасности включает игроков четырех уровней:
Российский рынок систем безопасности значительно фрагментирован.

Крупнейшие компании имеют годовые обороты несколько десятков миллионов долларов, что позволяет лидерам владеть долей рынка не превышающей 5-8%. По оценкам РБК к лидирующим компаниям можно отнести не более 10 компаний в каждом сегменте рынка. Надо отметить, что на мировом и российском рынках информационной безопасности наблюдается, совершено иная картина - доли лидеров в некоторых сегментах могут превышать 50%. Стоит отметить, что, оставаясь фрагментированным, российский рынок обнаруживает признаки начинающейся консолидации.

Мониторинг сайта www.brandcenter.ru (Центр брендов безопасности и связи) показал, что наиболее популярными российскими компаниями, работающими в сфере систем безопасности, в июне 2009 года стали:
Системные интеграторы

Системный интегратор - это компания, обеспечивающая создание, внедрение, развитие и сопровождение определенной инфраструктуры Заказчика, и ее интеграцию в основной бизнес Заказчика. Поэтому системные интеграторы — это большие компании, состоящие более чем из 100 человек, осуществляющие глубочайшую экспертизу по основным продуктам и основным технологиям на рынке. В их составе есть производственные и торговые подразделения, отделы разработок, поставок и монтажа, проектные отделы.
Сегодня системные интеграторы, помимо процесса проектирования и внедрения, все больше внимания обращают на последующее обслуживание внедряемых ими телекоммуникационных комплексов и IT-комплексов. По своему технологическому уровню российские интеграторы соответствует самым высоким требованиям, и потенциал ИТ - компаний, работающих на этом рынке, очень велик.
В свою очередь интеграторов можно разделить на:
Интеграторов, основной деятельностью которых является производство;
Интеграторов, основной деятельностью которых является дистрибуция и продажа;
Интеграторов, основной деятельностью которых является интеграция.

При инсталляции систем безопасности конечная стоимость системы для заказчика складывается, главным образом, из следующих составляющих: стоимости разработки, затрат на дистрибуцию, доставку и продажу и стоимости услуг по проектированию и монтажу систем. Как правило, прослеживается следующая тенденция - чем более сложной и комплексной является система, тем большая часть в структуре цены расходуется на ее проектирование и установку.
В представленной ниже таблице представлены компании-интеграторы смежных типов (производство, дистрибуция, чистая интеграция), расположенные в Москве, Санкт-Петербурге, а также крупных регионах.

На данный момент идет ярко выраженная структуризация и сегментация рынка.

Происходит расслоение компаний по размеру и объемам деятельности, и все большее число фирм переходит в узкоспециализированные сегменты рынка. Также наблюдается поглощение мелких компаний более крупными, и в ближайшем будущем борьбу за федеральные проекты смогут вести, предположительно, не более 7-8 крупных компаний.
Охранно-пожарное оборудование
ALL Secutity Systens
Альянс «Комплексная
безопасность»
DCN Telecom
АБРОН Холдинг
«Балта» БКС-Сервис ВИНГС DSSL IP-Центр Гефест-Группа предприятий
Next

Интегратор
Р-Контроль
КСБ «Синяя птица»
Ланит
ОНИКС Центр Охраного Телевидения и Систем
Связи ОПС+ Автоматика
Сервис
Периметр
POLMI GROUP
Равелин
Телрос
ТЦ Монолит
Видеонаблюдение
DCN Telecom
Альянс «Комплексная
безопасность»
АБРОН Холдинг
Аргус Видео
IP-Центр
БКС-Сервис
Группа предприятий
Next
DSSL
Интегратор
Р-Контроль
КСБ «Синяя птица»
Ланит ОПС+ Автоматика
Сервис
POLMI GROUP
Равелин
Телрос
ТЦ Монолит
Формула Безопасности
Контроль доступа
DCN Telecom HID Corporation АБРОН Холдинг
Балта
БКС-Сервис Группа предприятий
Next
Интегратор
Р-Контроль
"КСБ "Синяя птица"
ОПС+ Автоматика
Сервис
POLMI GROUP
Равелин
Формула
Безопасности
Телрос
И нте л л е кту а л ь н ое здание
M.I.SYSTEMS
Аквилон-А
IP-Центр
АйСиЭс-Балтика
Интеллектуальные
дома
"Лаборатория
Комфорта" - Система
Умный Дом
Специальные
решения и системы
Телрос
Формула
Безопасности

Системы связи
IP-Центр БКС-Сервис "КСБ "Синяя
птица"
ОПС+ Автоматика
Сервис

Эксперты рынка делают следующие прогнозы относительно появления новых игроков:
Будут появляться новые российские игроки, которые, вероятнее всего, выберут для себя более узкую специализацию — отраслевую или по группам решений. Скорее всего, это будут выходцы из небольших компаний. Ожидается развитие интеграторского бизнеса крупными западными компаниями, которые раньше предпочитали работать через российских партнеров. В структуре данных компаний будут создаваться собственные консалтинговые и интеграторские подразделения для решения задач заказчика «под ключ». Этот фактор внесет существенные изменения в сложившуюся схему работы на рынке.

В сегменте военно-промышленного комплекса, как и сейчас, будут доминировать российские производители оборудования.

Крупный бизнес будет ориентироваться на типовые западные решения, а отечественным разработчикам уготована роль доводчиков типовых решений под конкретные нужды заказчиков.

Для российских компаний перспективными будут наукоемкие и высокотехнологичные разработки. Малые и средние предприятия будут заинтересованы в российском ПО.

Производители, дистрибуторы и монтажники

Функции производителей оборудования систем безопасностей сводятся к выполнению специальных технических требований российских заказчиков. При этом изготовители также широко применяют импортные комплектующие, которые значительно увеличивают себестоимость производства из-за высокой таможенной пошлины. При реализации продукции производители выстраивают собственную дистрибьюторскую сеть или пользуются сетью торговых домов. Отечественные производители в большей своей части работают непосредственно с интеграторами и торговыми домами. При реализации продукции производители фактически выстраивают собственную дистрибуторскую сеть, или пользуются сетью торговых домов. Часто компании одновременно занимаются несколькими видами деятельности, сочетая производство, дистрибуцию, проектные и монтажно-наладочные работы.

Российский рынок достаточно привлекателен для зарубежных экспортеров в силу следующих причин:
рост уровня преступности повысил понимание необходимости промышленной и личной безопасности;
рынок пока находится на таком уровне, при котором у клиентов еще нет особых предпочтений перед торговыми марками.

Внедрению на рынок зарубежным компаниям мешают 2 фактора: низкая покупательная способность и дешевая рабочая сила. Многие предприятия вместо того, чтобы закупать приборы, нанимают охранников. Кроме того, дешевизной продукции все еще привлекают российских клиентов азиатские поставщики. Эксперты считают, что если западные фирмы не хотят потерять российский рынок, им нужно сделать свою продукцию более доступной по ценам, пусть даже за счет качества.

Самая наибольшая группа игроков рынка по численности - монтажники, которые выполняют инсталляцию оборудования (чаще всего видеодомофона и охранно-пожарной системы), а затем осуществляют его техническое обслуживание. Монтажники используют типовые решения и покупают готовые комплекты оборудования у дистрибьюторов или изготовителей. Например, к сегменту монтажников можно отнести Видеоконтроль-МСК, Комплексные системы Безопасности, Системы безопасности, ЭСКАДА Нэт.

ПРОИЗВОДИТЕЛИ СИСТЕМ БЕЗОПАСНОСТИ

В следующей таблице приведен список российских производителей и поставщиков оборудования для рынка систем безопасности:

Наименование сегмента рынка	Российские производители и поставщики
Интегрированные системы безопасности	ААМ Система, Болид, Дедал, ИСТА-Техника, Контур безопасности, Союзспецавтоматика, Сфера безопасности

Охранная, пожарная, охранно-пожарная системы	Аврора-БиНиБ (Россия), Автоматика, Алпро, Альтоника, Атис, Атэкс, Бастион, Болид, Гириконд, Горпожтехника, Градиент, Гранит-Саламандра, Дедал, Деловой мир, Завод «Красное знамя», Сигналспецавтоматика, Ивхимпром, Институт физико-технических проблем, Интекс, Интертехнолог, Источник Плюс, К-Инженеринг, Каланча, КАСПО, КБ «Прибор», Квазар, КНЦ-Сенсор, Комплектстройсервис, Контакт, Космы, КРОЗ, Ливенский машиностроительный завод, ЛИГАРД, Магнито-Контакт, Матек, Меридиан, МЗЭП, Молния, Нанко, Никирэт, Нота, Ортин, Охрана, Охранная техника, Плазма-Т, Пламя, Пожарная автоматика сервис, Пожтехника, Полисервис, Промсервис, Протект, Радий, Риэлта, Рубеж, Санком, Свит, Септима, Си-Норд, Сигма-ИС, Сигнал, Системы безопасности, СИТАЛ, Соболевский завод, Сократ, Сопот, Союзспецавтоматика, Средства пожарной безопасности, Спекгрон, Спецвилеопроект, Специнформатика, Спецпожижиниринг, Спецприбор, СПЭК^СТАЛТ, Старт-7, Телесистемы, термоавтоматика, Тульский завод
Оборудование систем контроля и управления доступом	ААМ Системз, Аккорд, Алеко, Аргус, АСВ-Техникс, Атис, БайтЭрг, Бастион, Биометрические системы, Виком, Витек, Градиент, Интегратор, Инфотек, ИСТА-Техника, К-Инженеринг, КБ Юпитер, КОМКОМ Электронике, Контур безопасности, Конфидент, Метаком, Модус-С, Нанко, Нейроинформатика, Никирэт, Олевс-ТВ, ОМА, Пентакон, Проксимус, Протон, Росси-СП, Росевростроой, Спецвилеопроект, Тайфун, телеинформсвязь, Телесистемы,
Система видеонаблюдения	АСВ-Техникс, БайтЭрг, Безопасность, Биометрические системы, Виком, Витек, Гард, Децима, Защита информации, Интегратор, Инфотек, ИСТА-Техника, КБ Юпитер, КОМКОМ Электронике, Метаком, Микролайт, Модус-С, Молния, Нанко, Нейроинформатика, Олевс-ТВ, Оникс, Охранная техника, Полисервис, Протон, Растр, Росси-СП, Русист безопасность, Себокс, Спецвилеопроект, Спецлаборатория, Старт-7, Тахион, Телесистемы, Тирекс, Трал, Цифрал, ЭВС, Электрон, Электронные системы, Элтис
Специальный транспорт	Автокад, Бронто, Гас, Диса, Евраком-Авто, Защита, Ижмаш, Имя-М, Лаура, Практик, САР, Техника, Эллина, Энергия,
Досмотровое и антитеррористи чес кое оборудование	Ака, Нелк, Сфинкс, Эльбрус

Наименование сегмента рынка	Российские производители и поставщики
Извещатели пожарной сигнализация	Алпро, Аргус, Атэкс, Гириконд, Гранит-Саламандра, Сигналспецавтоматика, Интертехнолог, КАСПО, КБ «Прибор», Квазар, КНЦ-Сенсор, Меридиан, Оникс, Радий, Риэлта, Септима, Сигнал, Спектрон, Специнформатика, Фактор Спецэлектроника, Элекос
Средства защиты автомобиля	Альтоника, Градиент, Проксимус, Эльбрус
Защита информации	Анна, Градиент, Дикси, Защита информации, Информзащита, КБ Юпитер, Нелк, Приборостроитель, Радиосервис, Реном, Сапр,
Автоматические установки пожаротушения	Артсок
Системы телекоммуникации и связи	АТ, Бастион, Вэбр, Градиент, Гранит, Децима, Дикси, Интекс, Интеркросс, Информатика и связь, Кб «Пилот», Максиком, Маском, Мультиком СПб, ПИК, Си-Би-Град, Таис, Тахион
Биометрические системы идентификации	Биометрические системы

Таблица Распределение российских производителей и поставщиков оборудования (в т.ч. небольшие компании) по сегментам рынка

Как показывает таблица, наибольшее количество российских компаний сосредоточено в сегментах:
охранных, пожарных и охранно-пожарных систем;
оборудования для систем контроля и управления доступом;
систем видеонаблюдения..

Наименьшим числом российских фирм характеризуются сектора досмотрового и антитеррористического оборудования, средств защиты автомобилей, а также биометрических систем идентификации.

ПОТРЕБИТЕЛИ СИСТЕМ БЕЗОПАСНОСТИ

Классификация основных потребителей систем безопасности и средств защиты информации. Рынок систем безопасности сегментируется по конечным клиентам.

Среди покупателей различных систем безопасности преобладают технические специалисты фирмы по безопасности и проектировщики систем безопасности, в 2008 году их было по 12% от всех покупателей. Количество менеджеров по логистике и закупкам снизилось по сравнению с 2007 годом с 10% до 9%. Менеджеры по продажам занимают 8%, руководство фирм на рынке систем безопасности - 7%, покупатель оборудования для собственных нужд - 6%, менеджер проектов - 6%.

Распределение покупателей систем безопасности по специальностям

Развитие производства и торговли также стимулирует рост числа потребителей во многих секторах промышленности, доля данного сегмента также постоянно растет.

Увеличение на рынке недвижимости элитных квартир и коттеджей также приводит к росту потребителей со стороны владельцев жилья (в основном, спросом пользуются камеры видеонаблюдения, предназначенные для домашнего использования). В основном, системы домашнего видеонаблюдения устанавливаются в домах площадью от 450 до 900 кв.м., в которых хозяева отсутствуют на протяжении длительных периодов времени, потому что дом является вторым. Достаточно высокий уровень преступности приводит к тому, что даже в обычные квартиры жильцы стараются установить стандартное сигнализационное оборудование (пульт). Согласно исследованию, проведенному компанией Parks Associates, от 2 до 4 % американских жилищ оборудованы видеонаблюдением с помощью компьютерных камер, либо профессионально установленных систем безопасности, в России пока это доля значительно меньше.

К «охранным» системам связи относят, прежде всего, транкинговую связь, которая позволяет при ограниченном частотном ресурсе подключить большое число абонентов. К основным потребителям такой связи относят не только силовые ведомства и охранные структуры, но и производственные предприятия, таксопарки. Также на базе транкинговых технологий можно создать сеть радиосвязи для небольшого поселка, что может помочь решить проблему низкой телефонизации в сельской местности.

Что касается потребителей по отраслям, 33% потребителей работают в сфере безопасности, 10% - в строительстве, 7% - в сфере информационных технологий, 6% - в армии и правоохранительных органах, 6% - в торговле, 5% - связи, 4% - электроэнергетике.

Потребительские предпочтения на рынке систем безопасности.

Спрос на системы безопасности подвержен сезонным колебаниям. Например, охранное телевидение с большей интенсивностью покупается с августа по март. Спад спроса на системы контроля доступа наблюдается с августа по декабрь. Системы охранной и пожарной сигнализации в спросе с марта по июнь. Увеличение потребления систем пожаротушения приходится на февраль-март, а также июль и август. Досмотровое оборудование покупается в меньшей степени с августа по декабрь. Спрос на системы предотвращения краж увеличивается весной и летом. А оборудование интеллектуального здания наблюдается в основном летом и осенью, также как и оснащение, специальной техникой контроля информации. Средства индивидуальной защиты покупаются потребителями в канун отпусков. Маркетинговое исследование «Российский рынок систем безопасности»

ПРОДВИЖЕНИЕ НА РЫНКЕ
ДИСТРИБУЦИЯ И СБЫТ СИСТЕМ БЕЗОПАСНОСТИ

Наиболее распространенный путь продвижения товара до потребителя на рынке систем безопасности:
Производитель
Дистрибьютор
Дилер
Потребитель
Дистрибьютор - это независимый оптовый посредник, действующий на основе договора, который он заключает с производителем. Дилер-посредник осуществляет продажу от своего имени и за свой счет. В коротком сбытовом канале дилер может непосредственно покупать товары у производителя.

Наибольшее количество российских дистрибьютеров расположены в Москве и Санкт-Петербурге, поскольку эти города - самые большие потребители оборудования безопасности. В этих российских коммерческих столицах располагается самое большое число компаний по безопасности и интеграторов, которые имеют опыт работы более 6 лет, а также высококвалифицированных сотрудников. Кроме того, оба эти города - главные таможенные пункты России. Одна из особенностей российских дистрибьюторов в том, что почти все из них не являются компаниями-дистрибьюторами в чистом виде, а работают также как системные интеграторы и разработчики изделий.

Существует два основных направления при поставке товаров для систем безопасности в Россию:
импорт через российских дистрибьюторов, которые производят таможенную очистку и прочие процедуры,

представительские офисы иностранных компаний в России, которые выполняют все таможенные процедуры и затем распределяют свои товары через российских дистрибьюторов.

Большинство иностранных компаний предпочитает поручать маркетинг и продажи своим российским дистрибуторам. Преимущество этой схемы состоит в том, что местные дистрибьюторы знают рынок, легко устанавливают контакты с клиентами и знают все особенности проведения таможенной очистки.

Местные дистрибьюторы считают, что для зарубежных производителей лучший способ проникновения на российский рынок состоит в том, чтобы выбрать одного дистрибьютора и работать через эту фирму. Однако иностранные поставщики не могут давать местной фирме статус эксклюзивного представителя, поскольку это требует от них определенных квот. Это указывает на то, что некоторые российские дистрибьюторы могут быть заинтересованы в получении статуса эксклюзивного дистрибьютора.

На начальном этапе такой дистрибьютор мог бы демонстрировать товары и изучать спрос. На этом этапе продукция бы не имела цены и не продавалась. При тестировании такого товара дистрибьютор мог бы начинать процесс его сертификации, которое требует значительных затрат времени и финансов. Когда изделие получает все требуемые сертификаты, его можно продавать. К этому времени дистрибьютор уже знает спрос на продукцию, а это может сказать иностранному партнеру о перспективах данного товара.

Подобная нацеленность на одного конкретного партнера обеспечивает более точное продвижение товара, что может привести к созданию региональной дистрибьютерской сети по всей России.

Первичными факторами, влияющими на выбор дистрибьюторов, являются отношение цена/качество, финансовые условия и поддержка продвижения товаров. Вторичными факторами являются возможность обслуживания, послепродажный сервис и обучение специалистов. Иностранный партнер должен предвидеть расходы по продвижению товаров и сертификации своих товаров на российском рынке.

Эксперты рынка систем безопасностей (в частности представители ООО «Актив-СБ», www.aktivsb.ru) предлагают определенную политику распределения товаров на рынке в зависимости от категории систем безопасностей.

С этой точки зрения маркетинга выделяются следующие виды сбыта:

прямой - продажа товара производится непосредственно потребителю;

непрямой - продажа осуществляется через посредников;

комбинированный.

В зависимости от числа посредников канал сбыта может быть: коротким (1-2 посредника) и длинным (более 2 посредников, перекупающих товар друг у друга). Чем длиннее канал сбыта, тем дороже он обходится потребителю. Прибыль и расходы канала составляют до 50% цены, которую платит при приобретении товара конечный потребитель.

Длинные каналы тяжелы в управлении и относительно затратные. Однако зачастую иного выбора у производителя, желающего выйти на массовый рынок, может не быть, особенно если целью является завоевание массового рынка не только в своем регионе, но и по всей стране.

В зависимости от особенности покупателей товара на рынке систем безопасности могут использоваться следующие каналы сбыта:

Основные критерии покупателей товара	Пример товара	Прямой канал	Непрямой канал		Значение критериев покупателей для предприятия
			короткий	длинный	
Многочисленность покупателей	Инфракрасные извещатели	-	+/-	+	Сокращение числа контактов может негативно сказаться на сбыте продукции
Высокая концентрация покупателей	-	+/-	+	-	Предприятие имеет возможность снизить издержки на один контакт
Продукция подразумевает единовременные крупные продажи	Проекты адресной охранно-пожарной сигнализации	+•	-	-	Издержки на установление контакта для предприятия быстро амортизируются
Покупки носят нерегулярный характер. Покупатели часто меняются	Системы охранной сигнализации для дома или дачи	-	+/-	+	Повышенные издержки предприятия при частых и малых заказах
Для покупателей важна оперативная поставка	Установка домофонов	-	+/-	+	Обязательно наличие запасов продукции вблизи точки продажи

Таблица Каналы сбыта в зависимости от особенностей покупателей

В зависимости от особенности предлагаемого товара могут использоваться следующие каналы сбыта:

Основные критерии товара	Пример товара	Прямой канал	Непрямой канал		Значение критерия товара для предприятия
			короткий	длинный	
Расходуемые продукты	Монтажные материалы	-	-	+	Необходимость быстрой доставки
Технически несложные продукты	Звуковые или световые опо вещатели	-	+/-	+	Низкие требования по обслуживанию
Нестандартизированное оборудование	Сложные интегрированные системы	+	-	-	Товар должен быть адаптирован к специфичным потребностям потребителя
Новые товары	IP-видеонаблюдени е	+	+/-	-	Необходимо тщательное "слежение" за новым товаром
Высокая ценность и стоимость продукта	Системы пожаротушения	+	-	-	Издержки на установление контракта быстро амортизируются

Таблица . Каналы сбыта в зависимости от особенностей продаваемого товара

Стратегия распределения того или иного товара во многом зависит от его качеств. Например, если это товар повседневного спроса и недорогой (элементарные охранные и пожарные извещатели, коммутационные устройства, монтажное оборудование и т.п.), то к нему должно применяться «интенсивное распределение», когда компания стремится к максимальному увеличению количеству торговых точек.

Для товаров класса «Премиум» и сверхсложной техники, когда необходим жесткий контроль над посредниками со стороны производителя, высокий уровень сервиса и ориентация на создание и сохранение безупречного имиджа торговой марки, приемлемо«эксклюзивное распределение». Оно ограничивается небольшим числом посредников с эксклюзивными правами распространения на определенной территории.

Для продаж B2B и товаров повышенной ценности (например, системы контроля доступа или сложное видеооборудование), когда компания-производитель старается работать с ограниченным количеством посредников на стандартных взаимовыгодных условиях, применяется«селективное распределение»,которому присуще достижение достаточного охвата и в то же время его ограничение, что позволяет работать только с квалифицированными дилерами.

ПРОДВИЖЕНИЕ СИСТЕМ БЕЗОПАСНОСТЕЙ НА РЫНКЕ

Наиболее успешные продажи в России на рынке систем безопасностей достигаются при взаимодействии с дистрибьюторами. При выборе дистрибутора российским и зарубежным поставщикам следует придерживаться определенных критериев, дистрибутор должен иметь:

современные склады для хранения товара (важно, чтобы товар содержался в соответствующих климатических условиях – неправильный способ хранения может привести к деформации или порче товара, и при продаже это обязательно негативно скажется на имидже бренда);

собственную распределительную сеть (для некоторых товаров, например, систем видеонаблюдения, очень важна скорость доведения продукта до потребителя, поэтому необходимо, чтобы дистрибьютор имел развитую систему логистики);

хорошие связи с потребителями (обратная связь - одна из главных нематериальных выгод сотрудничества производителя с дистрибьютором);

представительный офис, соответствующий имиджу производителя;

квалифицированный персонал (это особенно важно при продаже сложнотехнического оборудования или оборудования, предназначенного для персональных пользователей);

значительный опыт работы в данной индустрии, который в России составляет 5-8 лет.

Интернет

Интернет является одним из ведущих источников информации для профессиональных конечных пользователей систем безопасности. Почти все компании по безопасности являются корпоративными пользователями интернета. Некоторые фирмы имеют свой собственный веб-сайт и быстро движутся в направлении электронной торговли.

Среди наиболее популярных сайтов по системам безопасности следует назвать:

http://price.security-bridge.com/

Портал «Мост Безопасности», в котором можно найти и продать оборудование, воспользовавшись поисковой системой Единого Прайс-листа систем безопасности; контролировать ситуацию на рынке систем безопасности, объективно знать положение своей компании на нем. Порталом представлена электронная газета «Охранные системы», новости, статьи и книги о рынке в разделе «Библиотека по безопасности», проводятся также Интернет-семинары по безопасности, форумы.

Портал предоставляет площадку для проектировщиков систем безопасности, в которой можно найти расчеты on-line, методики подбора оборудования по безопасности, инструменты проектировщика, англо-русский словарь терминов, список поставщиков импортного оборудования.
http://www.scrf.gov.ru (Сайт Совета Безопасности Российской Федерации)
www.wisp.ru (Главной задачей портала является создание каталога фирм, связанных с безопасностью человека и информации. Всего в «коллекции»ресурса более 530 сайтов.)
http://www.sec.ru (предприятия, товары, форум, гипермаркет, публикации)
www.sec4all.net (крупнейшая техническая библиотека по безопасности, является базой организации НАСТРФ (Национальная Ассоциация Телохранителей РФ))
http://www.enginery.ru

Сервер предоставляет информацию по фирмам и товарам в отрасли инженерного обеспечения строительства, отдельным разделом в котором выступают системы безопасности.

Стоит выделить проект Centers, который включает в себя:
Система Интернет-продвижения компаний сферы безопасности и связи
Система Интернет-продвижения производителей, брэндов и торговых марок
Контекстная система запросов/заказов и организации тендеров
Развитая система партнерских программ и бесплатных услуг для отраслевых компаний-участниц
Система формирования и размещения mini-сайтов и centre-сайтов компаний на тематических ресурсах Интернета (создание и хостинг сайтов)
Многофункциональные, независимые системы управления содержанием(контентом) для mini-сайта и centre-сайта каждой компании
Система регистрации, продвижения и анализа статистики посещаемости mini-сайта и centre-сайта каждой компании
Система публикации технических описаний на оборудование и новостей компаний
Система отраслевых Интернет-каталогов и справочников
Отраслевая информационно-поисковая система
Тематическая, контекстно-зависимая рекламная площадка
Тематический рейтинг сайтов
Структурно система Centers представляет совокупность взаимосвязанных web-ресурсов с многовариантным рубрикатором и развитой поисковой системой. В настоящее время открыто четыре ресурса:
http://www.centers.ru - основной портал системы
http://www.centres.ru - отраслевой Прайс-Центр
http://www.center-s.ru - отраслевой каталог компаний
http://www.brandcenter.ru- отраслевой каталог производителей и торговых марок

В области информационной безопасности ситуация несколько иная. Эти компании уже осознали, что на федеральную политику легче влиять совместно и, таким образом, в конце 2001 года, они создали Союз информационный безопасности.

Специализированные журналы

Существует около 20 журналов индустрии безопасности, издаваемых в России.

Наиболее популярные журналы	Сайт
Системы безопасности	http://ss.groteck.ru
Грани безопасности	http://www.tinko.ru
Мир безопасности	http://mb.sec.ru/
Мир и безопасность	www.secur.ru
Индустрия безопасности	http://www.rasi.ru/
Безопасность. Достоверность. Информация	http://www.bdi.spb.ru/
Алгоритм безопасности	www.algoritm.org
Все о вашей безопасности	http://www.totalsec.ru/
CNEWS	www.cnews.ru
Security News	http://www.secnews.ru

Таблица . Основные отраслевые журналы и газеты

Основными подписчиками специализированных журналов являются проектно-монтажные организации. В меньшей мере к ним относятся торговые организации, подразделениям МЧС, подразделения вневедомственной охраны и производственные предприятия. По географии подписчиков наибольшая доля приходится на Москву и московскую область, Центральный ФО в целом, а также Северо-Западный. 18% потребителей предпочитают журнал Системы безопасности, 10% - Мир безопасности, 7% - Security News.

АНАЛИЗ ЭКСПОРТА И ИМПОРТА СИСТЕМ БЕЗОПАСНОСТИ

Анализ таможенной статистики экспорта и импорта систем безопасности проводился на основе следующих кодов ТНВЭД:
853110-УСТРОЙСТВАСИГНАЛИЗАЦИОННЫЕОХРАННЫЕИЛИУСТРОЙСТВАДЛЯ ПОДАЧИ ПОЖАРНОГО СИГНАЛА И

АНАЛОГИЧНЫЕУСТРОЙСТВА (включая устройства для гражданской авиации);
853120 - ПАНЕЛИ ИНДИКАТОРНЫЕ, ВКЛЮЧАЮЩИЕ В СЕБЯ УСТРОЙСТВАНА ЖИДКИХ КРИСТАЛЛАХ ИЛИ НА СВЕТОДИОДАХ;

АНАЛИЗ ИМПОРТА И ЭКСПОРТА ИНДИКАТОРНЫХ ПАНЕЛЕЙ

Объем экспортно-импортных операций

По итогам 2008 года объем импорта индикаторных панелей составил 19 840 тыс. долл., или 368 тонн. Объем экспорта находился на уровне 7 362 тыс. долл. в стоимостном выражении и 17 тонн в натуральном выражении.

Наименование	Экспорт	Импорт
Индикаторные панели, тонн	7 362	19 840
Индикаторные панели, тыс. долл.	17	368

Таблица . Объем экспортно-импортных операций на рынке индикаторных панелей.

Необходимо отметить, что для рынка индикаторных панелей характерно значительное преобладание объема импорта над объемом экспорта. В 2008 году импорт индикаторных панелей в стоимостном выражении превышает экспорт в 2,7 раз

В натуральном выражении импорт также превалирует над экспортом. В 2008 году импорт в натуральном выражении превысил экспорт в 21,6 раз.

Объем импорта индикаторных панелей в 2008 году составил 19 840 тыс. долл. в стоимостном выражении и 368 тонн в натуральном выражении. Темпы роста импорта индикаторных панелей в стоимостном выражении увеличились на 19% в 2008 году, а в натуральном выражении объем импорта сократился на 3%.

Необходимо отметить, что в натуральном выражении объем импорта на всем рассматриваемом интервале времени с 2003 по 2007 гг. увеличивается. Однако в 2008 году произошел спад объема импорта на 3%В структуре импорта индикаторных панелей в стоимостном выражении по странам-поставщикам большая часть приходится на Францию, которая ввозит в Россию 36% всех ввозимых индикаторных панелей, доля Китая в общем импорте составляет около 22%. На долю Германии приходится 9%.

В структуре импорта индикаторных панелей в натуральном выражении основными поставщиками являются Китай и Тайвань. Доля Китая в импорте в натуральном выражении значительно выше, чем в стоимостном (61% против 22%), доля Германии в общем импорте в натуральном выражении составляет 7%.

Объем экспорта индикаторных панелей в 2008 году составил 7 362 тыс. долл. в стоимостном выражении и 17 тонн в натуральном выражении. Экспорт индикаторных панелей в стоимостном выражении увеличился на 96%, а в натуральном выражении рост экспорта составил 339%.

Необходимо отметить, что в натуральном выражении объем экспорта на всем рассматриваемом интервале времени с 2003 по 2007 гг. то увеличивается, то сокращается. Рекордные темпы роста экспорта были зафиксированы в 2008 году, когда они достигли 339

В структуре экспорта индикаторных панелей в стоимостном выражении по странам-получателям большая часть приходится на Узбекистан, в который вывозится из России 24% всех вывозимых индикаторных панелей, доля Украины в общем экспорте составляет около 23%. Доля Казахстана составляет 12%.

В структуре экспорта индикаторных панелей в натуральном выражении основными получателями являются Казахстан и Украина. Доля Казахстана в экспорте в натуральном выражении значительно выше, чем в стоимостном (34% против 12%), доля Украины в общем экспорте в натуральном выражении составляет 31%, на долю Латвии приходится 13%.

АНАЛИЗ ИМПОРТА И ЭКСПОРТА СИГНАЛИЗАЦИОННЫХ УСТРОЙСТВ

Объем экспортно-импортных операций

По итогам 2008 года объем импорта сигнализационных устройств составил 60 931 тыс. долл., или 1 570 тонн. Объем экспорта находился на уровне 17 201 тыс. долл. в стоимостном выражении и 183 тонн в натуральном выражении.

Наименование	Экспорт	Импорт
Сигнализационные устройства, тыс. долл.	17 201	60 931
Сигнализационные устройства, тонн	183	1 570

Таблица . Объем экспортно-импортных операций на рынке сигнализационных устройств

Необходимо отметить, что для рынка сигнализационных устройств характерно значительное преобладания объема импорта над объемом экспорта. В 2008 году импорт сигнализационных устройств в стоимостном выражении превышает экспорт в 3,5 раз.

В натуральном выражении импорт также превалирует над экспортом. В 2008 году импорт в натуральном выражении превысил экспорт в 8,6 раз.

Импорт сигнализационных устройств

Объем импорта сигнализационных устройств в 2008 году составил 60 931 тыс. долл. в стоимостном выражении и 1 570 тонн в натуральном выражении. Темпы роста импорта сигнализационных устройств в стоимостном выражении увеличились на 15% в 2008 году, а в натуральном выражении объем импорта сократился на 22%.

Необходимо отметить, что в натуральном выражении объем импорта на всем рассматриваемом интервале времени с 2003 по 2006 гг. увеличивается. Однако в 2007-2008 гг. произошел спад объема импорта на 33% и 22% соответственно.

В структуре импорта сигнализационных устройств в стоимостном выражении по странам-поставщикам большая часть приходится на США, которые ввозят в Россию 29% всех ввозимых сигнализационных устройств, доля Италии в общем импорте составляет около 16%. На долю Украины приходится 11%.

В структуре импорта сигнализационных устройств в натуральном выражении основными поставщиками являются Китай и Украина, доля Китая в импорте в натуральном выражении значительно выше, чем в стоимостном (24% против 6%), доля Украины в общем импорте в натуральном выражении составляет 15%.

Экспорт сигнализационных устройств

Объем экспорта сигнализационных устройств в 2008 году составил 17 201 тыс. долл. в стоимостном выражении и 183 тонны в натуральном выражении. Экспорт сигнализационных устройств в стоимостном выражении увеличился на 3%, а в натуральном выражении спад экспорта составил 9%.

Необходимо отметить, что в натуральном выражении объем экспорта на всем рассматриваемом интервале времени с 2003 по 2007 гг. увеличивался. Однако в 2008 году впервые за рассматриваемый период был зафиксирован спад объема экспорта на 9%.

В структуре экспорта сигнализационных устройств в стоимостном выражении по странам-получателям большая часть приходится на Казахстан, в который вывозится из России 35% всех вывозимых сигнализационных устройств, доля Украины в общем экспорте составляет около 16%. Доля Туркмении составляет 14%.

В структуре экспорта сигнализационных устройств в натуральном выражении основными получателями являются те же страны. Доля Казахстана в экспорте в натуральном выражении значительно выше, чем в стоимостном (60% против 35%), доля Украины в общем экспорте в натуральном выражении составляет 12%, на долю Киргизии приходится 8%.

НОРМАТИВНАЯ БАЗА РФ ПО БЕЗОПАСНОСТИ
ЗАКОНЫ, УКАЗЫ, РАСПОРЯЖЕНИЯ И ПОСТАНОВЛЕНИЯ

Наименование нормативного документа	Текст документа в электронном формате
Законы РФ и Федеральные Законы	
«О безопасности» от 5 марта 1992 г. N 2446-I (с изменениями от 25 декабря 1992 г.)	http://svr.gov. ru/svr_today/doc04.htm
«О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 г. N 3523-I	http://www.relcom.ru/Archive/1997/ ComputerLaw/RussiaLaws/Zak_soft.htm
ЗаконРФ№3526-1 от 23.09.1992«О правовой охране топологий интегральных микросхем»	http://cyber-crimes.ru/laws/Z/3526_1-Z.doc
Федеральный закон РФ от 21 декабря 1994 года N 69-ФЗ «О ПОЖАРНОЙ БЕЗОПАСНОСТИ»	http://www.mchs.gov. ru/article.html?id=8327
Федеральный закон РФ № 128-ФЗ от 8.08.2001 «О лицензировании отдельных видов деятельности»	http://cyber-crimes.ru/laws/FZ/128-FZ.doc
Федеральный закон от 27 декабря 2002 года № 184-ФЗ «О техническом регулировании»	http://www.akdi.ru/gd/proekt/089768GD.SHTM
Федеральный закон ФЗ № 126-ФЗ от 18.06.2003 «О связи»	http://nalog.consultant.ru/doc49254.html
Федеральный закон Российской Федерации от 6 марта 2006г.N35-ФЗ«О противодействии терроризму»	http://www.rg. ru/2006/03/10/borba-terrorizm. html
Федеральный закон Российской Федерации от 27 июля2006г.N 149-ФЗ«Об информации, информационных технологиях и о защите информации»	http://www.rg.ru/2006/07/29/informacia-dok.html
Указы и Распоряжения Президента РФ	
Указ Президента Российской Федерации от 17 декабря1997года №1300 Об утверждении Концепции национальной безопасности Российской Федерации	http://www.fstec.ru/_docs/doc_1 _3_001.htm
Постановления Правительства РФ	

Постановление Правительства Российской Федерации от 15 апреля 1995 года № 333 О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и(или)оказанием	http://www.fstec.ru/_docs/doc_1_4_001.htm
услуг по защите государственной тайны	
Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации	http://www. rg. ru/2006/08/29/i nformacia-zashita-dok.html
Постановление Правительства Российской Федерации от 27 мая 2002 года № 348 Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации	http://www.businesspravo.ru/Docum/ DocumShow_DocumlD_29825.html
Постановление Правительства Российской Федерации от26 июня 1995 года № 608 Об утверждении Положения о сертификации средств защиты информации	http://emoney.ru/laws/p4.htm
Положения	
Положение о Федеральной службе по техническому и экспортному контролю - Утверждено Указом Президента Российской Федерации от 16 августа 2004 года №1085	http://www.fstec.ru/_docs/doc_2_2_001.htm http://www.elcode.ru/obzor/6.html?year= 2006&month=12&day=11
Положение о государственном лицензировании деятельности в области защиты информации -Решение Гостехкомиссии России и ФАПСИ от 27 апреля 1994 года № 10	http://www.fstec.ru/_docs/doc_2_2_006.htm
Положение о лицензировании деятельности по технической защите конфиденциальной информации - Утверждено постановлением Правительства Российской Федерации от 30 апреля 2002 года № 290	http://www.fstec.ru/_docs/doc_2_2_032.htm
Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации- Утверждено постановлением Правительства Российской Федерации от 27 мая 2002 года № 348	http://www,fstec.ru/_docs/doc_2_2_037.htm
Положение о сертификации средств защиты информации по требованиям безопасности информации - Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 года № 199	http://www.fstec.ru/_docs/ doc_2_2_011.htm
Положение по аттестации объектов информатизации по требованиям безопасности информации –Утверждено председателем Гостехкомиссии России от 25 ноября 1994 года	http://www.fstec.ru/_docs/doc_2_2_012.htm
Положение об аккредитации испытательных	http://www.fstec.ru/_docs/doc_2_2_049.htm

лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации - Решение председателя Гостехкомиссии России от 25 ноября 1994 года	
Типовые требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте (одобрено решением от 03.10.95 г. №42 Гостехкомиссии России)	http://security.softwaretesting.ru/wiki/ Ti povyeTrebov anijaKRu kov odstvu PoZI OtTS R? v= 12f w

Таблица . Основные нормативные документы по безопасности

ГОСУДАРСТВЕННЫЕ СТАНДАРТЫ ПО СИСТЕМАМ БЕЗОПАСНОСТИ

ГОСТ 26342-84 СРЕДСТВА ОХРАННОЙ, ПОЖАРНОЙ И ОХРАННО-ПОЖАРНОЙСИГНАЛИЗАЦИИ ТИПЫ, ОСНОВНЫЕ ПАРАМЕТРЫ И РАЗМЕРЫ

ГОСТ 28147-89. СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТАКРИПТОГРАФИЧЕСКАЯ. АЛГОРИТМ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

ГОСТ 28689-90. РАДИОПОМЕХИ ОТ ПЭВМ. НОРМЫ И МЕТОДЫ ИСПЫТАНИЙ. ТУНА КОНКРЕТНЫЙ ВИД ПРОДУКЦИИ

ГОСТ 34.936-91. ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. ЛВС. ОПРЕДЕЛЕНИЕ УСЛУГУРОВНЯ УПРАВЛЕНИЯ ДОСТУПОМ

ГОСТ 29339-92. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ЗА СЧЕТ ПЭМИН. ОБЩИЕТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

ГОСТ Р 50600-93. ЗАЩИТА СЕКРЕТНОЙ ИНФОРМАЦИИ ОТТЕХНИЧЕСКИХРАЗВЕДОК. СИСТЕМА ДОКУМЕНТОВ. ОБЩИЕ ПОЛОЖЕНИЯ

ГОСТР34.11-94. ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯЗАЩИТА ИНФОРМАЦИИ. ФУНКЦИЯ ХЭШИРОВАНИЯ

ГОСТ Р 50752-95. ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. ЗАЩИТА ИНФОРМАЦИИОТ УТЕЧКИ ЗА СЧЕТ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ПРИ ЕЕОБРАБОТКЕ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. МЕТОДЫИСПЫТАНИЙ

ГОСТР50739-95.Средствавычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

ГОСТ Р 50775-95 Системы тревожной сигнализации. Часть 1.Общие требования. Раздел 1.Общие положения.

ГОСТ Р 50776-95 Системы тревожной сигнализации. 1.Общие требования. Раздел4. Руководство по проектированию, монтажу и техническому обслуживанию.

ГОСТ Р 50842-95 Совместимость радиоэлектронных средств электромагнитная. Устройства радиопередающие народнохозяйственного применения. Требования к побочным радиоизлучениям. Методы измерения и контроля.

ГОСТ Р 50862-96 «Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость»

ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Читать

ГОСТ Р 51028-97 Устройство защиты от ошибок аппаратуры передачи данных. Методы защиты.

ГОСТР51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

ГОСТРИСО7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.

ГОСТР ИСО7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

ГОСТ Р 50839-2000. Совместимость технических средств электромагнитная. Устойчивость средств вычислительной техники и информатики к электромагнитным помехам. Требования и методы испытаний.

ГОСТР51583-2000.Защитаинформации.ПОРЯДОКСОЗДАНИЯАВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ. Общие положения.

ГОСТ Р 51624-2000. ЗАЩИТА ИНФОРМАЦИИ. АВТОМАТИЗИРОВАННЫЕСИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ. ОБЩИЕ ТРЕБОВАНИЯ

ГОСТ Р34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Ведение и общая модель.

ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

ГОСТ Р 6.30-2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов.

СПЕЦИАЛЬНЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ ПО СИСТЕМАМ БЕЗОПАСНОСТИ И ЗАЩИТЕ ИНФОРМАЦИИ

1.Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации - Решение председателя Гостехкомиссии России от 30 марта 1992 года
2.Защита от несанкционированного доступа к информации. Термины и определения- Решение председателя Гостехкомиссии России от 30 марта 1992 года
3.Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации - Решение председателя Гостехкомиссии России от 30 марта 1992 года
4.Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации - Решение председателя Гостехкомиссии России от 30 марта 1992 года
5.Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники - Решение председателя Гостехкомиссии России от 30марта 1992 года
6.Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации –Решение председателя Гостехкомиссии России от 25 июля 1997 года
7.Защита информации. Специальные защитные знаки. Классификация и общие требования - Решение председателя Гостехкомиссии России от 25 июля 1997 года
8.Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации. Сборник руководящих документов по защите информации от несанкционированного доступа - Гостехкомиссия России, 1998 год
9.Средства защиты информации. Специальные и общие технические требования, предъявляемых сетевым помехоподавляющим фильтрам – Гостехкомиссия России, 1998 год
10. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей - Приказ председателя Гостехкомиссии России от 4 июня 1999 года № 114
11.Безопасность информационных технологий. Критерии оценки безопасности информационных технологий - Приказ председателя Гостехкомиссии России от 19 июня 2002 года № 187
12.Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности - Гостехкомиссия России, 2003 года
13. Безопасность информационных технологий. Руководство по регистрации профилей защиты - Гостехкомиссия России, 2003 год
14. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты - Гостехкомиссия России, 2003 год
15. Руководство по разработке профилей защиты и заданий по безопасности - Гостехкомиссия России, 2003 год
16.РД 78.36.003-2002 МВД РОССИИ. ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯУКРЕПЛЕННОСТЬ.ТЕХНИЧЕСКИЕСРЕДСТВА ОХРАНЫ. ТРЕБОВАНИЯ И НОРМЫ ПРОЕКТИРОВАНИЯПО ЗАЩИТЕ ОБЪЕКТОВ ОТ ПРЕСТУПНЫХ ПОСЯГАТЕЛЬСТВ
17.ПРАВИЛА ПОЖАРНОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ ППБ-01-93 - Введены Приказом МВД от 14 декабря 1993 г. N 536
18.СН 512-78 ИНСТРУКЦИЯ ПО ПРОЕКТИРОВАНИЮ ЗДАНИЙ И ПОМЕЩЕНИЙ ДЛЯ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ МАШИН – Утверждена постановлением Государственного комитета СССР по делам строительства от 22 декабря 1978 г.№ 244, изменения Постановлением Госстроя России от 24.02.2000 № 17 введены в действие с 1 июля 2000 г.
19.Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (Приказ ФАПСИ от 13 июня 2001 г. N 152)
20. РЕКОМЕНДАЦИИР78.36.010-2000ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯЗАЩИТА НЕТЕЛЕФОНИЗИРОВАННЫХ ОБЪЕКТОВ
21.РД78.143-92СИСТЕМЫ И КОМПЛЕКСЫ ОХРАННОЙ СИГНАЛИЗАЦИИ, ЭЛЕМЕНТЫ ТЕХНИЧЕСКОЙ УКРЕПЛЕННОСТИ ОБЪЕКТОВ, НОРМЫ ПРОЕКТИРОВАНИЯ
22.РД 78.148-94 ЗАЩИТНОЕ ОСТЕКЛЕНИЕ. КЛАССИФИКАЦИЯ, МЕТОДЫИСПЫТАНИЙ, ПРИМЕНЕНИЕ
23.РД 78.36.003-2002 ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ УКРЕПЛЕННОСТЬ. ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ. ТРЕБОВАНИЯ И НОРМЫ ПРОЕКТИРОВАНИЯ ПО ЗАЩИТЕ ОБЪЕКТОВ ОТ ПРЕСТУПНЫХ ПОСЯГАТЕЛЬСТВ
24.РД 78.145-93 Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ
25.Пособие к РД78.145-93 Пособие к руководящему документу «Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ»
25.РД 78.36.004-2005 Рекомендации о техническом надзоре за выполнением проектных, монтажных и пусконаладочных работ по оборудованию объектов техническими средствами охраны
26.РД 78.36.005-2005 Рекомендации о порядке обследования объектов, принимаемых под охрану (взамен РМ 78.36.002-98)
27.РД 78.36.006-2005Выборипримененение технических средств охранной, тревожной сигнализации и средств инженерно-технической укрепленности для оборудования объектов: Рекомендации.

28.Р 78.36.005-99 Выбор и применение систем контроля и управления доступом
29.Р 78.36.007-99 Выбор и применение средств охранно-пожарной сигнализации и средств технической укрепленности для оборудования объектов. Рекомендации
30.СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕКОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (СТР-К)
31.СН 512-78 СТРОИТЕЛЬНЫЕ НОРМЫ Инструкция по проектированию зданий и помещений для электронно-вычислительных машин
32.Стандарт Банка России СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»
33.Стандарт взаимодействия систем автоматизации документационного обеспечения управления. - М.: Гильдия Управляющих Документацией, 2003
34.ТТ78.36.001-99Типовые требования по технической укрепленности и оборудованию сигнализацией предприятий торговли
35.ТТ78.36.002-99Типовые требования по технической укрепленности и оборудованию сигнализацией учреждений культуры, расположенных в зданиях, не являющихся историческими и архитектурными памятниками
36.ТТ 78.36.003-99 Требования к оборудованию учреждений центрального банка Российской Федерации инженерно-техническими средствами охраны
37.СО 153-34.21.122-2003 ИНСТРУКЦИЯ ПО УСТРОЙСТВУ МОЛНИЕЗАЩИТЫЗДАНИЙ, СООРУЖЕНИЙ И ПРОМЫШЛЕННЫХ КОММУНИКАЦИЙ

ПРОГНОЗ РАЗВИТИЯ РЫНКА НА 2009-2010 гг.

По итогам 2008 года темпы роста рынка систем безопасности упали. Главной причиной роста спроса на системы безопасности в последние годы был рост экономического благосостояния и, как следствие, рост покупательской способности.

До финансово-экономического кризиса, рынок систем безопасности являлся быстрорастущим рынком, каждый год объем оборотов на нем увеличивается от 10 до 35% в зависимости от сектора. Однако в связи с изменением экономической ситуации, темпы роста резко сократились. В 2008 году в стоимостном выражении объем рынка остался на уровне предыдущего года.

В 2009 году положение на рынке систем безопасности ухудшиться. Текущая ситуация на финансовом рынке неблагоприятно сказывается на деятельности компаний по продаже и производству систем безопасности. По прогнозам, в 2009 году объем рынка систем безопасности сократиться на 2% в стоимостном выражении.

В сегменте информационной безопасности в период финансово-экономического кризиса, даже в столь неблагоприятном климате на рынке важность ИБ не вызывает сомнений. По итогам исследования было выяснено, что большинство компаний считают информационную защиту первоочередной задачей даже в период кризиса, и экономить на безопасности готовы только 5,2% компаний.

Таким образом, в 2008-2009 гг. произойдет незначительное сокращение рынка, однако общая позитивная тенденция к необходимости установки и поддержания функционирования систем безопасности в компаниях приведет к тому, что к 2010 году ситуация на рынке может немного выправиться.

	2006	2007	2008 (оценка)	2009 (прогноз)	2010 (прогноз)
Объем рынка, млрд. долл.	5,1	6,0	6,0	5,9	5,95
Темп роста объема рынка в стоимостном	45%	17%	0%	-2%	1%
Доля сегмента продаж продуктов в структуре рынка информационной безопасности	75%	71%	64%	59%	55%
Доля сегмента аудита в структуре рынка информационной безопасности	8%	10%	10%	12%	12%
Доля сегмента внедрения в структуре рынка информационной безопасности	15%	17%	24%	27%	30%
Доля сегмента аутсорсинга в структуре рынка информационной безопасности	2%	2%	2%	2%	3%
Курс доллара	27,17	25,58	24,8	32	33
Таможенная пошлина					
Устройства сигнализационные {используемые в зданиях), % от стоимости	5%	5%	5%	5%	5%
Устройства сигнализационные (для гражданской авиации), % от стоимости	10%	10%	10%	10%	10%
Устройства сигнализационные (прочие), % от	нет	нет	нет	нет	нет
Панели индикаторные, включающие в себя устройства на жидких кристаллах или на	10%	10%	10%	10%	10%

Панели индикаторные (прочие), % от стоимости	15%	15%	15%	15%	15%
НДС	18%	18%	18%	18%	18%
Инфляция	9,0%	12,0%	13,0%	12,5%	12%
Темп роста ВВП, в % к предыдущему периоду	107,4	108,1	106%	102%	103%

Таблица . Прогноз основных параметров рынка