Специальная аппаратура

Использование технического средства защиты (ТСЗ) компьютерного полиграфа в компании позволит провести проверку сотрудников организаций на наличие противоправных действий или намерений в отношении предприятия, а, следовательно, значительно снизить материальные и финансовые потери, а также прекратить все виды деструктивной деятельности и оперативно выявить виновников любых нарушений.

Используемый Вами прибор, разработан академиком Варламовым Валерием Алексеевичем, известным специалистом в области работы с детекторами лжи и создателем ряда уникальных приборов.

Принцип действия устройства заключается в выявлении различных неконтролируемых физиологических реакций человека на тот или иной задаваемый испытуемому вопрос. В зависимости от модели прибора, могут учитываться различные физиологические реакции. Обязательный набор реакций, выявляемых в каждом приборе, включает в себя определение изменений дыхания, кровообращения (работы сердца) и кожное сопротивление. Помимо базовых составляющих, в приборах производится учет таких реакций человека, как тремор конечностей и психоэмоциональное состояние испытуемых. Следует отметить, что использование последнего параметра (психоэмоциональная составляющая) является «know-how» академика Варламова. Определение психоэмоционального состояния испытуемого позволяет выявить общую агрессию к процедуре и степень противодействия, что значительно повышает точность получаемых результатов тестирования.

Основное назначение применения ТСЗ (детектора лжи) – защита предприятий от противоправных умыслов и действий сотрудников, за счет проверки нанимаемых и увольняемых специалистов, проведения плановых проверок персонала, а также проведения служебных расследований.

В целом, использование на предприятиях детекторов лжи позволяет решить следующие задачи:

- ✓ предотвращение и устранение возможностей нанесения ущерба: материального и экономического;
- ✓ снижение утечки информации;
- ✓ оценка степени лояльности сотрудников;
- ✓ повышение эффективности работы сотрудников.

В целом, достоверность применяемой аппаратуры оценивается от 95% и выше, а при проведении испытаний высококвалифицированным специалистом стремится к 100%.

Предоставление услуг

Услуги по диагностике лжи, главным образом предоставляются различным организациям, не планирующим наличия собственного полиграфолога в штате. Услуги могут предоставляться разово или на условиях абонентского обслуживания.

В систему абонентского обслуживания входит контроль над работающим персоналом предприятия (выборочные плановые проверки, неограниченные проверки сотрудников, попавших под подозрение, проверки увольняющегося персонала), а также проверка нанимаемого персонала. Основными темами проверки являются различные злонамеренные действия в отношении предприятия, а также наличие скрываемых обстоятельств, которые могут повлиять на результативность работы сотрудника.

Средняя производительность труда одного специалиста-полиграфолога в день – три тестирования.

Ценовая политика

Средняя стоимость разового тестирования одного человека длительностью 1-2,5 часа составляет 3 000 грн. Если речь идет об абонентском обслуживании предприятий, то средняя стоимость абонентской платы в месяц составляет около 800 грн. на одного сотрудника (см. таблицу 2).

Таблица 2. Стоимость предоставления услуг на основе абонентского обслуживания

Категория персонала	Стоимость, грн./чел./в мес.
Вспомогательный персонал	500
Среднее звено	800
Руководящий состав	1000

Следовательно, ориентировочная стоимость абонентской платы за обслуживание предприятия с количеством сотрудников, например, 20 человек, составляет 16 000 грн.

1.1. Организация и результаты коммерческой деятельности компании

Потребители компании и организация продаж

Очень сложно выделить отраслевую принадлежность потребителей услуг, т.к. ими могут быть любые предприятия, на которых существует возможность хищения материальных и интеллектуальных ценностей, нанесения ущерба путем предоставления недостоверных сведений, недобросовестного выполнения своих обязанностей, преступных сговоров, халатности и пр. Но все же можно выделить такие отрасли, как:

- ✓ добыча, производство ювелирных изделий и драгоценных камней;
- ✓ химическое, фармацевтическое, парфюмерно-косметическое производство;
- ✓ торгово-закупочные сетевые предприятия со складскими помещениями;
- ✓ электроника и высокоточные устройства;
- ✓ компании, оказывающие логистические и складские услуги;
- ✓ развлекательные и игорные заведения;
- ✓ кредитные организации;
- ✓ авиа и морские перевозчики;
- ✓ рекрутинговые и кадровые агентства;
- ✓ спецслужбы, органы МВД и Министерства юстиции

Необходимо отметить, что потенциально большой интерес Услуг может вызвать у организаций, для которых особо важным является предотвращение утечки информации или вступления в сговор, например: кредитные отделы банковских структур, страховые компании, судейские коллективы и другие.

Что касается предоставления разовых услуг по детекции лжи, то в данном случае основными потребителями являются компании малого и среднего бизнеса, не имеющие собственной службы безопасности, однако нуждающиеся в защите бизнеса.

1.2. Организация маркетинга

Как уже было отмечено, на сегодняшний день основным методом привлечения потенциальных потребителей компании являются средства массовой информации (Интернет, медиа).

Прямые продажи обеспечивают 10% - ный положительный результат от контактов с потенциальными заказчиками. Также следует помнить, что при активном сбыте продукции в секторе B2B существует большой временной интервал между первичным контактом с потенциальным покупателем и непосредственно моментом оказания услуги.

В целом, наиболее эффективным каналом продвижения услуг полиграфолога является Интернет. Наиболее эффективным Интернет средством, используемым для продвижения, является контекстная реклама. Это объясняется, прежде всего, тем, что поиск по запросам в Интернет осуществляют уже заинтересованные люди, соответственно, большой процент посетителей, зашедших по контекстной рекламе, являются потенциальными покупателями.

При сопоставлении динамики продаж и распределения затрат на контекстную рекламу достаточно четко прослеживается линейная связь между увеличением затрат на контекстную рекламу и ростом продаж.

Поэтому для увеличения объемов роста продаж целесообразно проводить ежемесячную контекстную рекламную кампанию в Интернет, по необходимости, меняя критерии для выбора ключевых слов.

Что касается баннерной рекламы в Интернет, то она является значительно менее эффективной, чем контекстная, так как обычно размещается на массово посещаемых ресурсах, где присутствует значительное количество незаинтересованной аудитории. По этой причине баннерная реклама может дать прирост заходов на сайт, однако, они не обязательно завершаться покупкой. Возможно, целесообразно использовать баннерную рекламу на других Интернет-ресурсах, например, на сайтах, посвященных безопасности бизнеса либо на отраслевых порталах.

Участие в выставках, а также бесплатные PR-мероприятия в различных СМИ на сегодняшний момент не дают ощутимого эффекта.

В то же время, следует понимать, что эффективность любых PR-мероприятий является отсроченной и, как правило, не приносит моментальный эффект. Кроме того, эффективность PR-кампании зависит от ее интенсивности, следовательно, подобные мероприятия целесообразно продолжать, в частности, активизировать работу с бесплатной прессой. Качественная статья со скрытой рекламой интересна для профильного издания, так как журналисты всегда заинтересованы в поиске новых тем для публикаций. Особенно такая деятельность будет необходима в момент выведения на рынок и популяризации услуг новой компании. Вообще, PR-активность компании может не влиять на объем продаж реализуемой продукции, а, зачастую, носит имиджевый характер.

Необходимо подчеркнуть, что важным фактором при продажах услуг является объяснение потребителям механизма и обоснование эффективности работы прибора и метода, так как большинство потребителей волнует достоверность тестирования и возможность ошибок при проведении тестирований.

Оценивая конкуренцию в области исследуемых услуг, следует отметить, что прямого аналога этому методу на рынке пока нет. Соответственно, в качестве конкурентного окружения также можно рассматривать альтернативные способы защиты, такие как: различные камеры слежения, металлоискатели, контроллеры доступа и так далее. В то же время, альтернативные средства защиты не универсальны и не всегда позволяют произвести или предотвратить противоправные действия.

На сегодняшний день рынок рассматриваемых товаров и услуг практически не насыщен предложением и перенасыщен спросом, в частности, многие компании – конкуренты на сегодняшний день не справляются с имеющимся потоком заказов. Особо активно данное направление начало развиваться, начиная с 2005 года.

Наибольшее положительное влияние на рыночные возможности является общий рост рынка технических средств безопасности. Возможности рынка позволяют активно наращивать объем продаж услуг – полиграфных проверок в секторе B2B, в основном, крупному бизнесу.

2. ОБЩАЯ ХАРАКТЕРИСТИКА РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ БЕЗОПАСНОСТИ

2.1. Масштаб и динамика рынка за последние три года

До недавнего времени рынок систем безопасности не имел практически ничего общего с рынком информационных технологий, а с рынком информационной безопасности его роднило, пожалуй, только само общее понятие — «безопасность». Вопросами физической и информационной безопасности во всем мире традиционно занимались различные службы, которые нередко даже конфликтовали и часто до сих пор конфликтуют между собой. Правда, сегодня ситуация меняется. Рекомендации и требования международных стандартов или таких законов, как акт Сарбейнса–Оксли, вынуждает эти отделы тесно работать друг с другом. По данным PriceWaterhouse&Coopers, в

2006 г. более 50% опрошенных по всему миру компаний высказались в поддержку взаимодействия между отделами информационной и физической безопасности. Двумя годами ранее таких компаний было чуть менее 30%.

Если процесс усиления взаимодействия служб информационной и физической безопасности медленно но верно все же идет, то конвергенция технологий физической безопасности и ИТ — сравнительно новое для рынка явление. Однако по единогласному мнению экспертов, именно оно будет определять развитие систем безопасности в ближайшие годы.

Связующим звеном в этом процессе стали сетевые технологии. Начало конвергенции положили сетевые или IP-камеры. По некоторым прогнозам уже в следующем году до половины продаваемых в мире камер будут сетевыми. Однако на этом процесс не останавливается, сетевая среда все чаще используется при построении систем контроля и управления доступом (СКУД), для совместной работы СКУД и систем учета рабочего времени на местах интегрируются СКУД и сетевые системы видеонаблюдения. Более того, все чаще обеспечение физической и информационной безопасности увязывается в единой системе безопасности.

Рынок систем безопасности имеет давние традиции, и здесь опять же можно провести аналогии с рынком информационной безопасности. Однако есть одно существенное различие. Стремительное развитие ИТ в развитых станах привело к тому, что компании сегодня существенно отстают от западных конкурентов. На рынке же систем безопасности не было резких технологических всплесков, и развивался он значительно более спокойно. Это позволило нашим разработчикам не утратить свои позиции: по итогам 2006 г. около 60% продаж систем безопасности на рынке приходится на отечественные решения. Что касается его динамики, то по оценкам CNews Analytics за прошедший год этот сектор увеличился в объеме на 21% и достиг $1,3 млрд. долл. Ожидается, что к 2011 г. объем рынка увеличится, достигнув $1,6 млрд. долл., а его доля от общего объема ВВП страны увеличится до 0,15%.

Наибольшие темпы роста продемонстрировал сегмент охранного телевидения (CCTV), прибавив за год 34% (см. рис. 7). При сохранении существующих показателей объем продаж оборудования для систем видеонаблюдения превысит в 2011 г. продажи пожарной сигнализации — крупнейшего на сегодня сегмента рынка. Хорошие темпы демонстрирует и сегмент систем контроля и управления доступом (СКУД) - 28%. У остальных показатели гораздо скромнее. Так, продажи охранной и пожарной сигнализации выросли, соответственно, на 18% и 16%, интегрированных систем на 16%, биометрических решений и систем пожаротушения - на 12%.

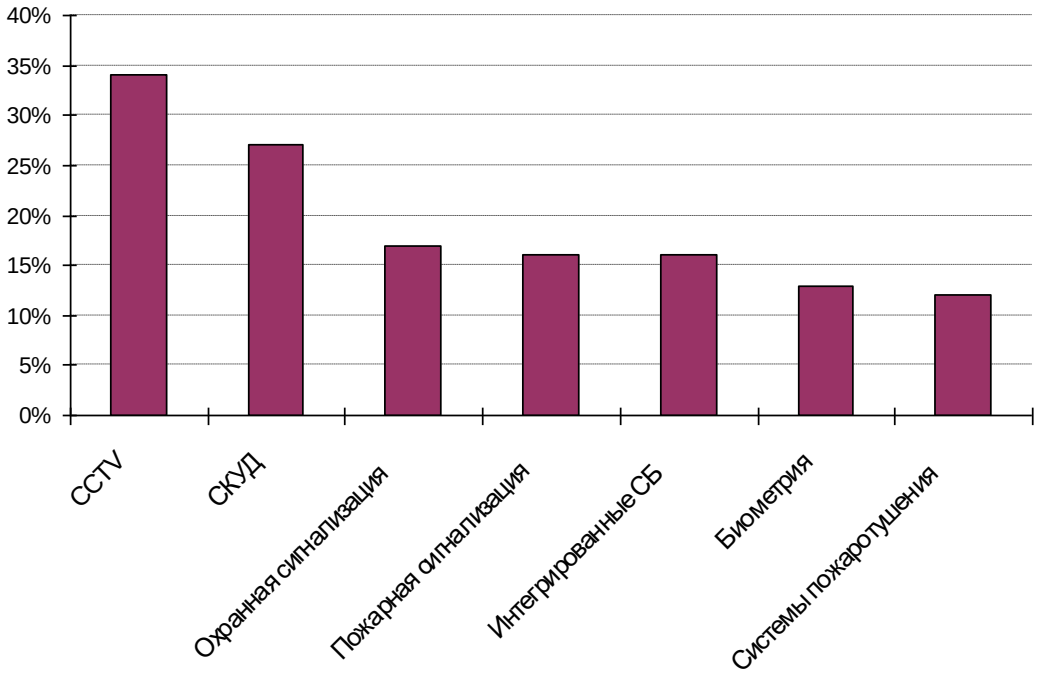

Рис. 7. Рост основных сегментов рынка систем безопасности в 2010 году

Рынок услуг и средств безопасности считается перспективным. По оценкам агентства «Михайлов и партнеры», темпы его роста вдвое превышают европейские и американские показатели. По данным

РБК ежегодно разные сектора рынка растут на 10 - 35%, прогнозируемый рост рынка – 17-19% в год, в зависимости от сегмента.

Несмотря на уверенный рост и потенциал развития, отрасль остается одной из наиболее информационно непрозрачных и неструктурированных.

Глобальной тенденцией рынка систем безопасности является его постепенная конвергенция с ИТ-рынком. IP-технологии позволяют интегрировать системы физической безопасности в ИТ-инфраструктуру организации, а также объединять их между собой. Интеграция физической и информационной безопасности уже наблюдается на Западе. Видимо, в скором времени можно ожидать подобную ситуацию.

По данным кабинетного исследования компании «Келис Консалтинг», основными факторами, влияющими на развитие рынка, являются следующие:

- ✓ положительный финансовый климат;
- ✓ рост культуры использования систем безопасности;
- ✓ рост доли технических средств охраны производства;
- ✓ рост рисков террористических угроз.

Изменения рынка технических средств безопасности начали проявляться с 2000 года. Главным образом, этому способствовали три причины:

- ✓ смена технологических платформ оборудования;
- ✓ набирающий оборот процесс слияния и поглощения фигурантов рынка;
- ✓ сворачивание производства аналоговой аппаратуры.

Все новые модели регистрирующего оборудования, например, для систем видеонаблюдения (спецвидеомагнитофоны, видеопринтеры, контроллеры, мультиплексоры, квадраторы и др.), базируются на цифровых технологиях. Компании постепенно отходят от производства разрозненных и функционально-ориентированных систем. Стандартом отрасли «де-факто» становятся интегрированные системы. Во все интегрированные системы закладываются методики и технологии «открытых систем», пришедших на рынок систем безопасности из ИТ-индустрии.

Эксперты рынка систем безопасности отмечают рост культуры потребителей систем безопасности. Это выражается как в росте уровня требований по качеству, так и в требовании к интегрируемости различных систем безопасности. С одной стороны, у пользователей накапливается некий объем установленных ранее систем, и при установке новых систем требуется интеграция с уже установленными системами. С другой стороны, все больше клиентов осознают, что наиболее работоспособными будут именно интегрированные (комплексные) системы безопасности.

2.2. Прогнозы и тенденции рынка на перспективу

Государство

При рассмотрении перспектив развития рынка безопасности (РРБ) в условиях присоединения к Всемирной торговой организации эксперты в данной области выделяют ряд очевидных конкурентных преимуществ РРБ, которые еще не реализованы[1]:

- ✓ уникальное евроазиатское положение, в том числе и исторические связи со странами СНГ;
- ✓ высокая квалификация сотрудников. Свыше 700 тыс. сотрудников негосударственных организаций безопасности, допущенных к работе с оружием, это новый социально-профессиональный слой. Из них 30%, по оценкам экспертов, составляют бывшие сотрудники органов внутренних дел, государственной безопасности, других правоохранительных органов;

[1] «Мир безопасности», №12/157, 2006. С.В.ШЕВЧЕНКО, ведущий консультант Комитета Государственной Думы РФ по безопасности

- ✓ впечатляющая адаптация к сложным рыночным отношениям и успешный прорыв в развитии. 15-летний

Вместе с тем, очевидно, что вступление в ВТО само по себе вряд ли будет являться стимулом экономического роста рынка безопасности, так как существуют проблемы внутри самого рынка: он крайне инертен и не может быть быстро изменен, необходимо преодолеть растущий спрос на загрнежные технические средства безопасности и другое.

- ✓ по инкассации и депонированию, перевозке ценных бумаг;
- ✓ по проведению расследований;
- ✓ осуществлению контроля сигналов тревоги.

Это означает, что в будущем в этих секторах можно будет вводить любые ограничения и для иностранцев, вплоть до полного закрытия рынка.

В контексте сектора расследования и обеспечения безопасности, определенные обязательства принимаются только в части предоставления иностранными поставщиками:

- ✓ охранных услуг;
- ✓ консультативных услуг, по определению потребностей клиента и предоставлению консультаций и предложений в отношении наиболее подходящего для клиента способа обеспечения безопасности или в отношении совершенствования существующих систем.

Предполагается, что, в частности, загрнежным поставщикам будет разрешено предоставлять указанные виды услуг путем учреждения коммерческого присутствия, т.е. через создание (либо покупку и перерегистрацию) юридического лица. При этом предусмотрен ряд требований к иностранным поставщикам услуг, выполнение которых является обязательным условием для обеспечения их доступа к функционированию в данной области. Так, им будет необходимо получить предварительное разрешение от компетентных органов власти на осуществление соответствующих видов деятельности. Процедура получения разрешения основана, среди прочего, на учете и оценке таких критериев, как компетентность, профессиональная репутация, независимость, знание соответствующего законодательства в области охранной деятельности, способность обеспечивать защиту общественной безопасности и публичного порядка.

Кроме того, ограничивается круг персон, которые могут являться руководителями таких юридических лиц. Зафиксировано требование, согласно которому руководителями указанных юридических лиц могут являться только граждане, постоянно проживающие на ее территории. В случае необходимости, в частности обусловленной интересами национальной безопасности, страна - член ВТО может отменить или изменить свои обязательства, правда, при условии проведения переговоров со всеми заинтересованными странами - членами ВТО, по итогам которых, возможно, потребуется предоставление уступок в каких-то других секторах.

Технологии

Что касается наиболее распространенных технических средств безопасности, используемых на предприятиях – систем контроля доступа и видеонаблюдения, компания *Frost & Sullivan* опубликовала обзор, в котором анализируется развитие данного сектора рынка.

В качестве ключевых тенденций авторы обзора выделяют интеграцию систем физического и логического доступа и активное внедрение в эти комплексные решения средств биометрической идентификации.

Как отмечается в обзоре, особую актуальность упомянутым тенденциям придают возрастающие потребности правоохранительных органов и ведомств, отвечающих за обеспечение национальной безопасности. Основной вектор развитию систем контроля доступа и видеонаблюдения задают усилия по стандартизации биометрических технологий, усиливающееся внимание к проблемам безопасности и изменение условий, в которых действует бизнес. В свою очередь, данные факторы влияют на рынок в сочетании с разработками в сфере детектирования движения, анализа поведения и технологий биометрической идентификации по изображению лица.

Расширению сферы применения биометрических технологий должно способствовать снижение стоимости средств, реализующих эти технологии, и расширение перечня прикладных продуктов, предоставляющих провайдерам систем контроля доступа возможность интегрировать биометрию в свои решения. Такая интеграция — единственный способ обеспечить эффективность систем контроля доступа и дальнейшее повышение уровня защиты и безопасности, констатируют авторы обзора. В качестве удачного примера подобного подхода они приводят т.н. «биометрические ворота»: идентификация посетителя в них производится с помощью биометрии, а верификация личности — по предъявлении посетителем смарт-карты, в память которой ранее были занесены сведения о его биометрических параметрах.

Еще одно перспективное направление развития систем контроля доступа авторы обзора связывают с внедрением в них технологий мультибиометрической идентификации. Правда, сейчас мультибиометрическая идентификация практикуется лишь при организации доступа к особо важной информации или в помещения, которые необходимо защищать на самом высоком уровне. Констатируя эту ситуацию, авторы обзора отмечают, что на данный момент на рынке в качестве основной, безусловно доминирует технология идентификации по отпечаткам пальцев. Этой технологии авторы обзора пророчат дальнейшее счастливое будущее — при условии, что она и впредь будет доказывать свою высокую точность, расширяя сферу практических применений, а стоимость средств сканирования отпечатков пальцев станет снижаться.

По результатам кабинетных исследований и экспертных интервью представителей компаний, работающих в вышеозначенном секторе, на рынке также активно используются системы голосовой идентификации (как правило, это банки и аэропорты). А идентификатор отпечатков пальцев используется преимущественно в ряде госструктур и в предприятиях нефтегазового комплекса, в частности, в ряде компаний «Лукойл».

Проекты

В настоящее время набирает обороты концепция инновационного мегапроекта «Сокращение теневого оборота драгоценностей» (ТОД). Целью внедрения и реализации данного проекта является организация работы по восстановлению практики вольноприносительства в местах добычи и обработки драгоценных металлов и драгоценных камней (далее ДМ и ДК), прежде всего, на Урале, в Сибири, на Дальнем Востоке и Крайнем Севере, путем гармонизации коренных интересов населения и государства.

Суть концепции состоит в том, что жителям этих отдаленных регионов возвращается их историческое право на законное индивидуальное предпринимательство (это снимает главную причину ТОД) и создаются условия, необходимые для легального оборота ДМ и ДК.

Основным механизмом, обеспечивающим сокращение ТОД, является мегапроект «Треугольник света» (закон, рынок, общество). Мегапроект инициирует создание бизнес-плана, обеспечивающего в ходе сокращения ТОД единство действий государственных органов, участников рынка, а также некоммерческих и общественных организаций при поддержке СМИ. В ходе сокращения ТОД предусматривается применение юридических, административных, социально-экономических, информационно-образовательных, технических средств защиты и иных инноваций как инструментов, открывающих новой категории предпринимателей путь к индивидуальному производительному труду в духе традиций первопроходцев, но на легальных основаниях, обеспечивающих им естественное возвращение в рынок.

2.3. Классификация технических средств безопасности

По сложившейся международной практике безопасности объектами защиты с учетом их приоритетов являются:

- ✓ личность;
- ✓ информация;
- ✓ материальные ценности.

Понятие «безопасная деятельность» любого предприятия или организации включает в себя:

- ✓ физическую безопасность, под которой понимается обеспечение защиты от посягательств на жизнь персонала;
- ✓ экономическую безопасность;
- ✓ информационную безопасность;
- ✓ материальную безопасность, т.е. сохранение материальных ценностей от всякого рода посягательств, начиная от краж и заканчивая угрозами пожара и других стихийных бедствий.

Обобщая вышеприведенные примеры угроз безопасности, можно выделить 3 основные составляющие направления безопасности предприятий:

- ✓ правовая защита;
- ✓ организационная защита;
- ✓ информационно-техническая защита.

Виды технических систем безопасности, относящихся к последнему направлению, можно классифицировать следующим образом:

- ✓ Интегрированные системы безопасности.
- ✓ Системы контроля и управления доступом (включая: турникеты, электрические и электромеханические замки, домофоны, контроллеры, карты доступа, ПО и пр./не включая: ворота, приводы, шлагбаумы, ограждения и пр.).
- ✓ Системы видеонаблюдения (камеры, видеорегистраторы, мониторы, пульты управления).
- ✓ Охранная сигнализация.
- ✓ Пожарная сигнализация.
- ✓ Средства и системы пожаротушения (без учета тяжелой техники, например, пожарные машины).
- ✓ Биометрические технологии.

Наиболее растущими сегментами по данным кабинетных исследований и экспертных интервью являются сегменты систем видеонаблюдения, систем с использованием биометрических технологий и интегрированных систем.

Сегодня рост сегмента систем пожарной и охранной сигнализации составляет 15% в год. Здесь работает много отечественных производителей, в том числе благодаря государственной поддержке. По мнению экспертов, господдержка неконкурентоспособных игроков долго затрудняла выход в сектор новых производителей и не позволяла повысить надежность систем.

Наибольшие темпы роста ожидаются на рынках систем видеонаблюдения (охранного телевидения) и систем контроля и управления доступом (СКУД).

Объем сегмента видеонаблюдения в 2009 г. составлял 200 млн. долларов и ежегодно увеличивается на 25%[2]. Если в ближайшие 5 лет эти темпы сохранятся, то к 2014 г. сегмент станет самым крупным на рынке. Отечественные производители представлены здесь слабо. Львиная доля продукции принадлежит иностранным разработчикам, чьи решения часто лучше и дешевле отечественных. В настоящее время используются в основном аналоговые камеры наблюдения (крупнейшие производители: Watec, Computar, Panasonic, Sony, JVC). Цифровые камеры мало распространены (по оценке IMS Research, их продажи составляют 4%), но продажи ежегодно растут почти на 30%. Поэтому уже через 1-2 года ожидается превалирование цифровых и гибридных систем.

На СКУД в 2010 г. приходилось 15% отечественного рынка. Здесь наши разработчики достигли наибольших успехов, наладив производство и самих СКУД, и практически всех составляющих. Доля систем на рынке СКУД составляет не менее 70%, а по некоторым направлениям достигает 90%. Наиболее перспективны биометрические и Smart-технологии идентификации, растет роль программного обеспечения для интегрированных СКУД.

Эксперты выделяют 5 основных сегментов рынка технических средств безопасности (см. рис. 8).

[2] По данным РосБизнесКонсалтинг

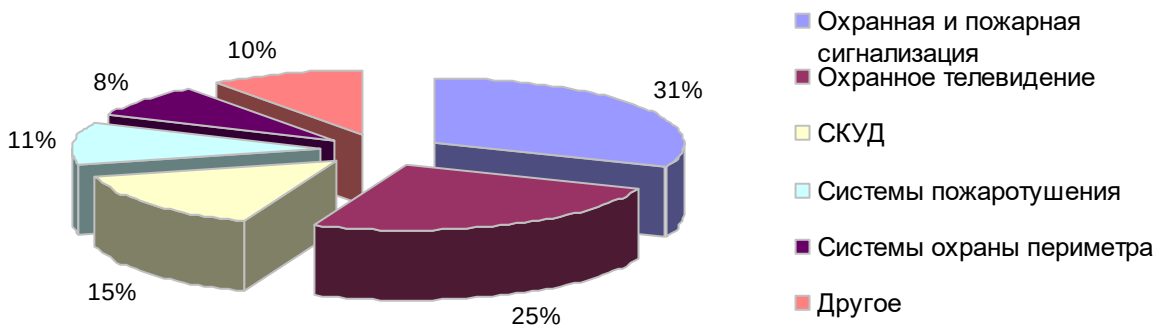

Рис. 8. Структура рынка систем безопасности

Как видно на рисунке 8, крупнейшим сегментом рынка по-прежнему остается 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 – CCTV - занимает 25% рынка, а замыкает тройку СКУД с 15%. На сегменты систем пожаротушения и охраны периметра приходится 11% и 8% соответственно.

Отечественным компаниям-разработчикам удалось сохранить за собой большую часть рынка средств технической безопасности. Отчасти это произошло благодаря тому, что эволюция технологий проходила здесь не столь стремительно, как на ИТ-рынке, игроки успевали адаптироваться к новым условиям. Отчасти - благодаря созданной в советские времена хорошей производственной и научной базе, которую удалось сохранить (в немалой степени за счет поддержки со стороны государства) в перестроечный и после перестроечный периоды. Так или иначе, но на сегодняшний день почти 60% рынка принадлежит отечественным компаниям, а решения успешно конкурируют с западными аналогами.

Стоит, однако, отметить, что подобные оптимистичные показатели, в первую очередь, обязаны сегменту пожарной сигнализации, который составляет половину рынка систем безопасности. Не менее 80% подобных решений, а в денежном эквиваленте, учитывая объем сегмента, это составляет около 400 млн. долл. Подобный успех во многом простимулирован государством, и часто можно слышать, что оно, так или иначе, поддерживает неконкурентоспособные компании, не давая, тем самым, проявить себя пусть пока и небольшим, но перспективным.

Хорошие позиции также сложились у отечественных производителей систем охранной сигнализации — на их продукцию приходится около 70% продаж. Уверенно чувствуют себя и разработчики СКУД, которые «держат» 65% рынка. В то же время, многие эксперты отмечают, что отечественные СКУД преобладают в нижнем и среднем ценовых сегментах. В крупных проектах, требующих глубокой интеграции с другими системами безопасности, и рассчитанных на большое количество точек контроля и пользователей, исполнители предпочитают использовать более дорогие западные решения. Здесь ситуация схожа с той, что наблюдается на ИТ-рынке, где программные продукты в большинстве случаев уступают иностранным в возможностях масштабируемости и интегрируемости в ИТ-инфраструктуру.

Несмотря на хорошие в целом позиции отечественных компаний на биометрическом рынке, в сегменте систем безопасности они сильно уступают своим загрнежным конкурентам. Здесь биометрические технологии применяются исключительно в составе систем контроля и управления доступом, с постепенным распространением на контроль рабочего времени. Есть всего два-три

подобных решения, тогда как иностранные аналоги представлены примерно двумя десятками компаний.

Хуже всего обстоят дела в сегменте охранного телевидения. В свое время это направление было не развито, поэтому практически ничего не досталось. Та небольшая часть компаний, которая имеет отношение к производству камер наблюдения, занимается их механической сборкой, однако и здесь продукция зачастую уступает не только по качеству, но и по цене более совершенным загрнежным аналогам. В сегменте PC-based видеосистем позиции отечественных разработчиков более уверенные. Но в этом случае нельзя говорить о производстве, большая часть таковых относится к интеллектуальным системам, а здесь весь интеллект заключается в соответствующем программном обеспечении. В целом по сегменту, не более 10% CCTV остается за отечественными компаниями.

2.4. Основные участники рынка

В нашем случае мы будем рассматривать производителей и дистрибьюторов средств технической безопасности, реализованных на технологиях, которые могут составить конкуренцию полиграфу. К ним относятся металлодетекторы, голосовые анализаторы и программа «Майнд Ридер», поскольку вышеозначенная продукция используется также на проходных и помогает решать сходные задачи.

Много независимых дистрибьюторов, представляющих довольно широкий ассортимент продукции, обеспечивающей техническую безопасность. Наиболее известная и рекомендуемая ведущими экспертами рынка компания в области комплексной защиты – «Луис+» (системы видеонаблюдения и охранно-пожарная сигнализация).

2.5. Результаты экспертного опроса

Специалистами «Келис Консалтинг» был проведен экспертный опрос компаний, работающих в области производства средств безопасности как для обеспечения технической защиты, так и для обеспечения защиты информации. Выборка включала 1000 глубинных интервью.

Участники опроса предлагали различные классификации средств технической безопасности, относя к этой же категории и средства информационной защиты. Большинством были выделены следующие виды средств технической безопасности:

- ✓ охранно-пожарные средства;
- ✓ теле- и видео оборудование;
- ✓ СКУД (системы контроля и управления доступом).

Также были предложены классификации по охвату аудитории, а именно:

- ✓ индивидуальные средства защиты;
- ✓ массовые средства защиты.

Классификация по противодействию угрозам:

- ✓ пассивные средства защиты, которые позволяют регистрировать угрозу;
- ✓ активные средства защиты, которые позволяют предотвратить угрозу.

Специалистами в области информационной безопасности была предложена своя классификация средств безопасности:

- ✓ средства внешней безопасности (защиты от хакеров);
- ✓ средства внутренней безопасности (защита от вредоносной деятельности сотрудников - инсайдерства).

Рассматривая виды технической безопасности, большинство участников опроса выделяли как одни из самых востребованных следующие:

- ✓ видеонаблюдение;

- ✓ системы контроля доступа;
- ✓ охранно-пожарная сигнализация;
- ✓ контроль технологических процессов;
- ✓ теле- и радио- связь.

В области информационной безопасности были отмечены следующие средства защиты: создание хранилищ данных, использование специализированного программного обеспечения.

Среди производителей рассмотренных видов технической безопасности были экспертами названы следующие компании, занимающиеся производством *средств видеонаблюдения*:

- ✓ EverFocus;
- ✓ Electronics Corp.;
- ✓ ISS (Intelligent security systems);
- ✓ Panasonic;
- ✓ Bosch;
- ✓ Видеонэт.

Компании-производители *систем контроля доступа*:

- ✓ Apollo;
- ✓ TSS;
- ✓ Perco;
- ✓ Парсек;
- ✓ Болид;
- ✓ Кодос;
- ✓ ADT;
- ✓ DSC.

Основными производителями *охранно-пожарной сигнализации* были названы:

- ✓ Сибирский Арсенал;
- ✓ Болид;
- ✓ Реконет;
- ✓ Аккорд;
- ✓ Tyco.

Практически всеми участниками опроса была отмечена тенденция роста в развитии рынка средств технической безопасности. Отмечается возрастание спроса на системы наблюдения и интегрированные решения, распространение GPS-навигации. Кроме того, возникает модернизация и усовершенствование самих средств технической безопасности. Среди новых разработок, экспертами были выделены: новые разработки систем контроля и доступа (HID), «Умный дом» (СКАДО-интеллект, мониторинг движения, модули оставленных вещей, модуль парковки, фэйс-интеллект, безопасность на тоннеле БАМ, система бесконтактного опознавания), интеграция глобальной системы безопасности, GSM, GPRS.

Сейчас наблюдается активное участие иностранных компаний (Франция, США, Германия, Китай, Корея) на рынке технических средств и их сотрудничество с предприятиями. В перспективе, специалистами отмечается продолжение роста и развития рынка ТСЗ. По мнению некоторых участников через 2-3 года возможен всплеск новых технологий.

Средства обеспечения технической безопасности направлены на большой спектр потребностей предприятия, который, прежде всего, зависит от его индивидуальных требований. В числе основных потребностей предприятий в сфере безопасности эксперты выделяют совершенствование систем контроля доступа, возможность интеграции новых средств безопасности с существующими системами.

В настоящее время, то количество средств безопасности, которое представлено на рынке, по мнению большинства экспертов, может удовлетворить потребности предприятий в области технической защиты примерно на 70-80%.

Для того, чтобы технические средства покрывали все потребности предприятий, необходимо учесть индивидуальные условия предприятий. В качестве универсальных действий, направленных на удовлетворение спроса, специалисты отметили тот факт, что производителям необходимо делать акцент на удобстве и простоте в обращении с продуктом, который они выпускают.

2.6. Нормативно-правовая база

Использование полиграфов прямо или косвенно регламентируется следующими нормативно-правовыми актами:

- ✓ Конституция
- ✓ Гражданский кодекс
- ✓ Трудовой Кодекс
- ✓ Уголовный кодекс
- ✓ «О связи».
- ✓ «О безопасности».
- ✓ «Об информации, информатизации и защите информации».
- ✓ «О техническом регулировании».
- ✓ «О коммерческой тайне».
- ✓ «О персональных данных».
- ✓ «О полиграфе» (проект).
- ✓ «О частной детективной и охранной деятельности».
- ✓ Постановление правительства № 1233 от 3 ноября 1994 г. (регламентирует использование служебной информации ограниченного распространения).
- ✓ Указ Президента №188 от 6 марта 1997 г. «Об утверждении перечня сведений конфиденциального характера»

Использование полиграфа или аналогичных разработок может прямо или косвенно регламентироваться также внутренними документами предприятия: устав, коллективный договор, трудовые договора, правила внутреннего распорядка, технологические руководства и инструкции, должностные инструкции.

2.6.1. Группа 2. Конкурентные технологии

В связи с тем, что применение полиграфа возможно практически в любой отрасли, сотрудники «Келис Консалтинг в ходе исследования столкнулись с необходимостью сегментирования потребителей в зависимости от сфер их деятельности, в которых возможно эффективное использование Полиграфа. На основании результатов экспертных и глубинных интервью (см. Приложение 2) было выделено несколько наиболее важных аспектов в области защищенности и безопасности деятельности компаний респондентов, а именно:

- ✓ Регулирование доступа и скрытного перемещения предметов:
  - хищение материальных ценностей и проноса их через пункты доступа;
  - пронос запрещенных предметов через пункты контроля.
- ✓ Выявление факта сокрытия сведений и оценка степени лояльности сотрудников компаний:
  - достоверность сведений, предоставляемых при приеме на работу;
  - выявление скрытых нарушений в ходе выборочного мониторинга;
  - и выявление негативных настроений сотрудников, которые могут оказать отрицательное влияние на результат деятельности компании.

- ✓ Предупреждение и выявление нежелательных намерений сотрудников и третьих лиц в отношении интересов компании:

  - сговор при заключении предпринимательских сделок;

  - планирование уклонения от исполнения обязательств.

В рамках конкурентного анализа были изучены предложения компаний, реализующих продукты, построенные на технологиях, отличных от технологий, использованных в полиграфе, но позволяющих обеспечить защиту вышеперечисленных областей ответственности. В результате анализа были отобраны следующие технологии:

- ✓ sense-технология голосовые анализаторы Nemesysco;
- ✓ психосемантический анализ с помощью продукта «MindRider 2.0»;
- ✓ рентгенографические сканеры;
- ✓ арочные металлоискатели;
- ✓ скоринговые системы.

Голосовые анализаторы (приложение 4) представляют собой технологии, основанные на анализе голоса. На рынке представлены следующие марки:

- ✓ «ЛоРеАн» - логический речевой анализатор, компьютеризированная система, основанная на технологии анализа голосового стресса. В 2003 году признано специально-техническим средством и запрещено для массового использования ФСБ. По мнению сотрудников компаний, принимавших участие в телефонном интервью, наиболее результативный речевой анализатор. Несомненным преимуществом «ЛоРеАн» является бесконтактный характер и скрытое (при необходимости) применение, хотя последний фактор при определенных обстоятельствах может стать недостатком.

- ✓ GK1 – система контроля доступа, использующая технологию анализа голоса, для проверки правомочности входа на подконтрольную территорию. Система GK1 предназначена для использования в аэропортах, на таможне, на пограничных пунктах, в пунктах охраны правопорядка, в подразделениях по борьбе с наркотиками, в тюрьмах для пресечения попыток передачи недозволенных предметов заключенным, а также для контроля доступа в любую охраняемую зону.

  Система группирует и анализирует различные эмоциональные структуры с целью выявить те из них, которые сигнализируют о реальном намерении совершить преступление или акт терроризма. Система способна функционировать в самых разных конфигурациях, от одноязычной системы, управляемой вручную, до многоязычного автоматического пункта. Проверяемому человеку задается от 3 до 5 вопросов. Ответ на каждый вопрос записывается и анализируется системой. Сразу после завершения процесса опроса (для 5 вопросов требуется около 60 секунд) система выдает результат: «зеленый» или «красный» коридор, что определяет возможность доступа в контролируемую зону. Система проходила испытания в аэропорту Домодедово.

- ✓ Ex-Sense PRO-R – голосовой анализатор эмоций, инструмент для тестирования процессов переговоров о купле/продаже, процессов интервьюирования новых сотрудников, выяснения, чем в действительности занимаются торговые агенты и так далее.

- ✓ «К-Фактор» - программное обеспечение, специально спроектированное для кадровых агентств, отделов кадров и руководителей, принимающих ответственные решения по приему и оценке кадров. Принцип работы основан на технологии SENSE. SENSE-технология может анализировать разные слои в голосе формируемые подсознанием, проводя глубокий анализ круга эмоций субъекта. Она может определить, взволнован ли собеседник, смущен, напряжен, охотно ли делится информацией, сосредоточен. SENSE-технология - многоуровневый анализ голоса, использующий множество параметров, определенных для каждого речевого сегмента. Компьютер задает вопрос испытуемому, который отвечает в микрофон.

Также есть специально написанные технологии для проведения телефонных продаж TS-1 и технологии RA5 (оценка рисков по страховым выплатам или кредитам) и QA5 (контроль за работой

менеджеров), которые могут также использоваться для оценки финансовых рисков и для принятия решений о выдаче кредита (производство Израиль, компания Nemesysco).

Достоинства голосовых анализаторов:

- ✓ высокая пропускная способность (возможность охвата большого количества людей);
- ✓ обработка информации занимает небольшое время, в зависимости от модуля вопросов. Среднее время обработки 30-40 минут;
- ✓ простота применения, программой может пользоваться новичок;
- ✓ период обучения специалиста составляет 2-3 дня;
- ✓ невысокая цена на продукт;
- ✓ возможность скрытого тестирования испытуемого;
- ✓ возможность тестирования собеседника по телефону.

Недостатки:

- ✓ необходимость приобретения лицензии у поставщика продукта на обследование ограниченного числа человек (от 20), затем лицензию надо продлевать;
- ✓ достоверность полученной информации у голосовых анализаторов ниже, чем у полиграфов;
- ✓ необходимо «разговорить» испытуемого.

Психосемантический компьютерный анализ (Приложение 5)**.** Технология представляет собой исследовательский метод, основанный на 25 кадре. То есть, при прохождении тестирования сознание испытуемого видит цифры, а подсознание - зашифрованные за этими цифрами любые вопросы.

Преимущества методики:

- ✓ простота применения (может пользоваться новичок);
- ✓ высокая пропускная способность (от 50 чел. в день);
- ✓ достоверность (до от 90%);
- ✓ обработка информации занимает небольшое время (около 15 минут).

Недостатки:

- ✓ высокая стоимость – 11 000 Евро;
- ✓ есть ряд ограничений для лиц с повышенной возбудимостью.

Рентгенографические сканеры (Приложение 6) используют слабое рентгеновское излучение для обнаружения скрытых запрещенных или опасных предметов. Считаются одними из наиболее информативных видов аппаратуры, позволяющей визуально идентифицировать запрещенные предметы, находящиеся не только на теле, но и внутри.

Рентгенографические сканеры работают по принципу последовательного облучения досматриваемого объекта узким плоским рентгеновским лучом или пучком лучей и регистрации излучения с помощью многоэлементного чувствительного детектора.

Достоинства прибора:

- ✓ высокая пропускная способность;
- ✓ минимальное время сканирования (не более 10 секунд);
- ✓ высокая чувствительность сканера, позволяющая обнаружить не только высококонтрастные металлические предметы, но и малоконтрастные неметаллические предметы (наркотики, драгоценные камни, взрывчатые вещества, биологические вещества, электронные устройства и т.д.);
- ✓ возможность многократного увеличения и одновременного наблюдения за испытуемым и его одеждой и выявления наличия мелких ценных предметов и предметов, запрещенных к выносу;

- ✓ возможность подключения дополнительного оборудования (сканеры, фотоаппараты, системы передачи данных на большие расстояния).

Недостатки:

- ✓ высокая стоимость 200 000 евро;
- ✓ облучение человека.

Арочные металлоискатели (Приложение 7) представляют собой устройства в виде металлических арок для обнаружения только металлических предметов от 5 грамм весом, а также металлосодержащие предметы.

Достоинства прибора:

- ✓ высокая пропускная способность;
- ✓ короткое время сканирования;
- ✓ относительно низкая цена;
- ✓ возможность быстрого монтажа;
- ✓ не требует специальной подготовки персонала.

Недостатки:

- ✓ способность обнаруживать только металлы.

Скоринговые карты или просто – скоринг (Приложение 9) не является техническим устройством, это модель классификации клиентской базы на различные группы, если неизвестна характеристика, которая разделяет эти группы, но известны другие факторы, связанные с интересующей характеристикой. Представляет собой тестовую таблицу, заполняемую оператором и обрабатываемую специальной программой.

Достоинства:

- ✓ Простота заполнения;
- ✓ Не требует специальной подготовки оператора.

Недостатки:

- ✓ Короткий период актуальности карт.

Таблица 9. Преимущества и недостатки потенциально конкурентных технологий

	Технология /продукт	Достоинства	Недостатки
1.	Голосовой анализатор	✓ высокая пропускная способность ✓ простота применения ✓ короткий срок обучения ✓ невысокая стоимость продукта и обучения ✓ возможность скрытого тестирования	✓ необходимость приобретения лицензии на ограниченное число тестов ✓ достоверность ниже, чем у полиграфов ✓ необходимо разговорить испытуемого
2.	Психосемантический компьютерный анализ	✓ высокая пропускная способность ✓ простота применения	✓ высокая стоимость ✓ ограничения для лиц с повышенной эмоциональной возбудимостью

Детектор лжи, Полиграф

3.	Рентгенографический сканер	✓ высокая пропускная способность ✓ минимальное время сканирования ✓ обнаружение мелких предметов на теле	✓ высокая стоимость ✓ доза облучения при тестировании
4.	Арочный металлодетектор	✓ высокая пропускная способность ✓ минимальное время сканирования ✓ относительно низкая цена ✓ возможность быстрого монтажа ✓ не требует специальной подготовки персонала	✓ обнаруживает только металлы
5.	Скоринг	✓ простота использования ✓ минимальная подготовка персонала	✓ короткий период актуальности

Таблица 10. Сравнительный анализ технологий, потенциально конкурентных технологии Полиграфа

	Факторы	Голосовой анализатор (продукция компании Nemesysco)	Психосемантический компьютерный анализ («Майнд Ридер»)	Рентгенографи-ческие сканеры и арочные металлодетекторы	Технология Полиграфа	Скоринг
1.	Стоимость продукта	цена 10 000 дол. США)	цена 11 000 евро	От 94 600 грн. до 6 896 000 грн.	От 100000 до 255000 грн	От 1 000 000 до до 1 500 000 грн.
2.	Количество каналов считываемой информации	1	1	От 1 до 3	11	Нет
3.	Степень достоверности полученной информации	От 70 до 90% (по отзывам специалистов)	До 90%	До 99%	От 90%.	До 90%
4.	Объем затраченного времени на обработку информации	Калибровка (настройка информации) за 1-2 минуты, зависит от объема беседы, в целом, 30-40 минут достаточно	15 минут	10-15 секунд	40 минут – 2 часа	До 60 мин.
5.	Необходимый объем для получения информации	Необходимо, чтобы респондент разговорился, давал обширные ответы	Идет стандартный набор символов	Прохождение человека через турникет/рамку	Достаточно ответов «Да» - «Нет», причем необязательно вслух	Большое количество персональных данных
6.	Возможность охвата широкой аудитории	Неограниченная	Неограниченная	Неограниченная	Неограниченная	Неограниченная
7.	Возможность работать скрытно от информационного донора	Есть	Нет	Нет	Нет	Нет

	Факторы	Голосовой анализатор (продукция компании Nemesysco)	Психосемантический компьютерный анализ («Майнд Ридер»)	Рентгенографические сканеры и арочные металлоискатели	Технология Полиграфа»	Скоринг
8.	Необходимость приобретения лицензии	На «К-Фактор» требуется, цена от 10 266 грн. (20 проверок) до 239 540 грн. (за 1000 проверок), на другие -нет	Не требуется	Не требуется	Не требуется	Не требуется
9.	Продвижение продукта	Интернет, публикации в прессе	Интернет, публикации в прессе	Выставки, публикации и реклама в Интернет, публикации в СМИ	См. «Рекомендации по стратегии»	Интернет, СМИ
10.	География присутствия		Молдова (Кишинев), Украина (Днепропетровск), Северный Кавказ (Ростов-на-Дону), Нижний Новгород и Санкт-Петербург	По всей	По всей	Нет
11.	Выявленные коммерческие потребители (не включая спецслужбы)	Несколько банков, «Ист Лайн» (уже не работают с продуктом в связи с судебным разбирательством), страховые компании, брачные агентства	Аэропорт в Самаре	Аэропорты, тюрьмы, лечебные учреждения, промышленные предприятия, границы (для таможенных досмотров), рудники,	См. «Рекомендации по стратегии»	Кредитные учреждения

Анализ методов продвижения продукции

Как правило, участники рынка при продвижении услуг, чаще всего используют Интернет-рекламу, рекламу в печатных изданиях, выпуск и тиражирование учебников.

Практически все представители опрошенных компаний по телефону назвали наиболее эффективной Интернет-рекламу через систему «Бегун». По этой рекламе совершается большая часть Интернет-продаж. Наименее эффективной многие признали рекламу в массовых E-mail рассылках. Баннерная реклама, главным образом, только привлекает посетителей на сайт, но покупок по ней практически не совершается.

При анализе деятельности методов продвижения Услуг, компаниями-конкурентами, мы видим, что помимо участия в выставках и Интернет - маркетинговых мероприятий, занимаются публикациями в печатных изданиях («Элитный Персонал», «Антенна», Business Week, «Свой бизнес», «Деловой еженедельник», «Консультант № 1»).
Большинство компаний размещаются в специализированных изданиях, посвященных, помимо безопасности («Служба безопасности», «Милиция»), также кадровой тематике, юриспруденции («Адвокат»), бизнесу и предпринимательству («Санкт-Петербургский бизнес- журнал», «Белорусская деловая газета»), аналитике («Итоги»). Наибольшее число публикаций размещается в специализированных изданиях по безопасности и кадрам.

Сотрудники большинства компаний рекомендовали издания компании «Гротек» (журнал «Системы безопасности» и каталог «Системы безопасности», а также «CCTV Фокус».

Компании-конкуренты, реализующие полиграфные проверки, не занимаются активными продажами. Профессионалов телефонных продаж не выявлено.

По мнению специалистов «Келис Консалтинг», необходимо обеспечить расширение каналов продаж Услуг, в частности, при работе на данном рынке целесообразно активное использование метода прямых продаж.

Потенциальные клиенты

Большинство клиентов опрошенных компаний являются нефтегазовыми предприятиями, вневедомственными и правительственными структурами, производственными компаниями (пищевая, фармацевтическая и ювелирная промышленность), охранными предприятиями, банками и финансовыми компаниями, строительными компаниями, торговыми фирмами, энергетическими структурами, инвестиционными компаниями. Также, обращаются кадровые агентства (например, Global Consulting одними из первых агентств стали использовать в своей работе детектор лжи). Недавно стали обращаться службы знакомств (элитарные) и брачные агентства.

2.7. Актуальность проблемы хищений на предприятиях

С целью выявления актуальности проблемы хищений и способов ее решения на предприятиях целевой группы, а также с целью рекрутинга респондентов для изучения спроса на новый продукт Заказчика (услуги полиграфолога), был проведен предварительный телемаркетинг компаний из сфер деятельности, являющих потенциальными покупателями услуг проверок на полиграфе. Выборка составляла 500 крупных производителей и дистрибуторов товаров, представляющих ценность для инсайдеров. Из них результативными были признаны ответы 313-ти компаний.
Результаты телемаркетинга свидетельствуют о том, что тема обеспечения безопасности деятельности предприятий остается закрытой для большинства респондентов. Так, 65% участников опроса заявили, что краж и хищений производимой продукции у них не происходит, и существующими мерами и системами безопасности они вполне довольны.

Отраслевая структура опрошенных компаний представлена на рисунке 9. В структуре выборки преобладают компании, относящиеся к следующим отраслям: фармацевтика и медицина (24%), косметика и парфюмерия (22%), ювелирная промышленность (19%), электроника (11%) и химическая промышленность (9%). В остальные 15% вошли компании, деятельность которых связана с электротехнической промышленностью, автомобилестроением, торговлей, производством сувенирных изделий, взрывоопасными и горюче-смазочными материалами, а также государственные режимные предприятия.

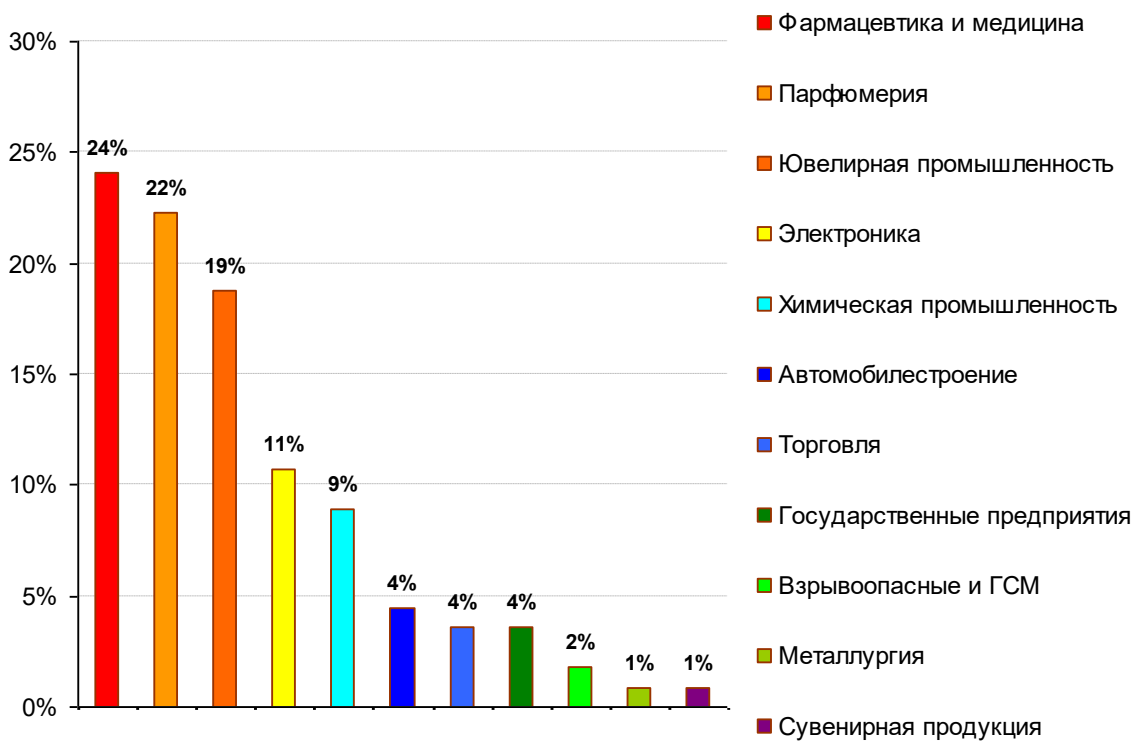

Рис. 9. Отраслевая структура опрошенных компаний

Среди участников телемаркетинга 43% компаний утверждают, что не сталкивались с проблемой пропажи имущества за последние 2-3 года, 22% - сталкивались с подобной проблемой, но не уделяют этому должного внимания, и 35% не смогли точно ответить на этот вопрос (см. рис. 10).

Количество парфюмерных компаний, которые не сталкивались с проблемой воровства на производстве, составляет 32% от общего числа парфюмерных компаний в выборке. У 20% из них нет собственной службы безопасности.

Количество компаний, занимающиеся производством и продажей ювелирных изделий, которые не сталкивались с проблемой пропажи имущества за последние 2-3 года, составляет 33% от общего числа представителей данной отрасли в выборке. 11% из них не имеют собственной службы безопасности.

Процент фармацевтических компаний, отрицательно ответивших на вопрос о хищениях, значительно ниже, чем в указанных выше сферах деятельности, а именно, составляет 17% от общего числа опрошенных фармацевтических компаний. Согласно полученным данным, к наиболее уязвимым к кражам на производстве относятся фармацевтические компании, так как 35% от всех фармацевтических компаний отмечали случаи пропажи имущества за последние 2-3 года.

Среди компаний, деятельность которых связана с химической промышленностью, 20% сталкивались с случаями пропажи имущества на производстве.

Сравнительно низкий процент зарегистрированных случаев пропажи имущества на предприятии может быть связан как с наличием эффективной системы технических средств защиты, так и с закрытостью респондентов к диалогу (в большей степени).

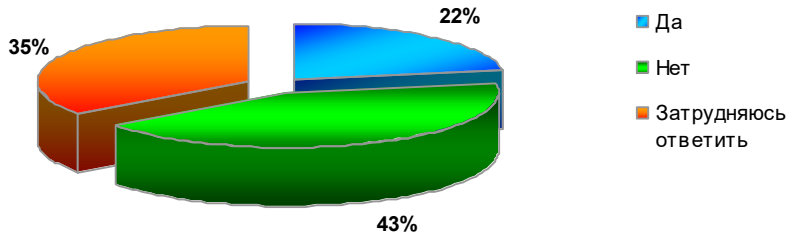

Рис. 10. Зафиксированные случаи пропажи имущества за последние 2-3 года

Согласно рисунку 11, около 60% респондентов используют технические средства защиты (далее – ТСЗ). Остальные 40% указали, что на их предприятиях не используются средства безопасности.

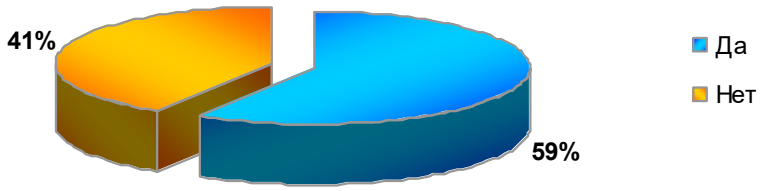

Рис. 11. Использование технических средств защиты

Из числа всех компаний, использующих ТСЗ, около половины довольны работой ТСЗ, что объясняется снижением и исчезновением краж на предприятии (см. рис. 12). Количество респондентов, недовольных работой своих ТСЗ, составляет 17%, причем большинство из них пользуются ТСЗ от 4 до 7 лет. Их недовольство может быть обусловлено низкой скоростью модернизации действующих на предприятии систем безопасности, непросвещенностью в области новых разработок в сфере безопасности или недоверием к новым рыночным предложениям.

Затруднились ответить на вопрос об эффективности существующих ТСЗ, в основном, те компании, которые недавно используют ТСЗ (год и менее), и, соответственно, выводы о результатах работы средств зашиты пока делать рано.

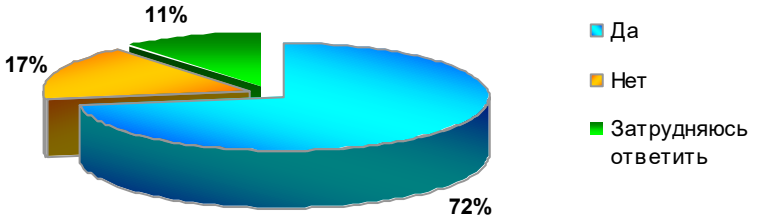

Рис. 12. Удовлетворенность эффективностью работы ТСЗ

Большинство участников опроса используют ТСЗ 4 года и более – 74% компаний, использующих ТСЗ. К числу компаний, которые используют ТСЗ от 4 до 7 лет, относятся, в основном, фармацевтические и парфюмерные компании, в меньшей степени – предприятия ювелирной и химической промышленности.

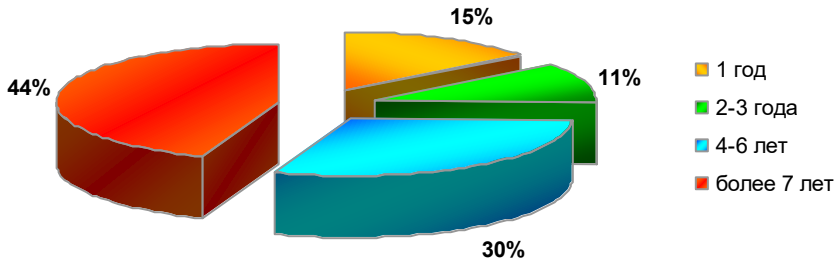

Рис. 13. Период использования ТСЗ на предприятиях

Из рисунка 14 видно, что основным направлением использования ТСЗ в целом по выборке является контроль перемещения сотрудников (19%), затем контроль входа/выхода для производственных предприятий и прохождения спецконтроля пассажирами аэропортов (16%). В торговых компаниях ТСЗ направлены на контроль за перемещением посетителей (13%). Для крупных производственных предприятий автомобильной, ювелирной, фармацевтической и парфюмерно-косметической промышленности одним из важных направлений ТСЗ является контроль над производственным процессом (11%).

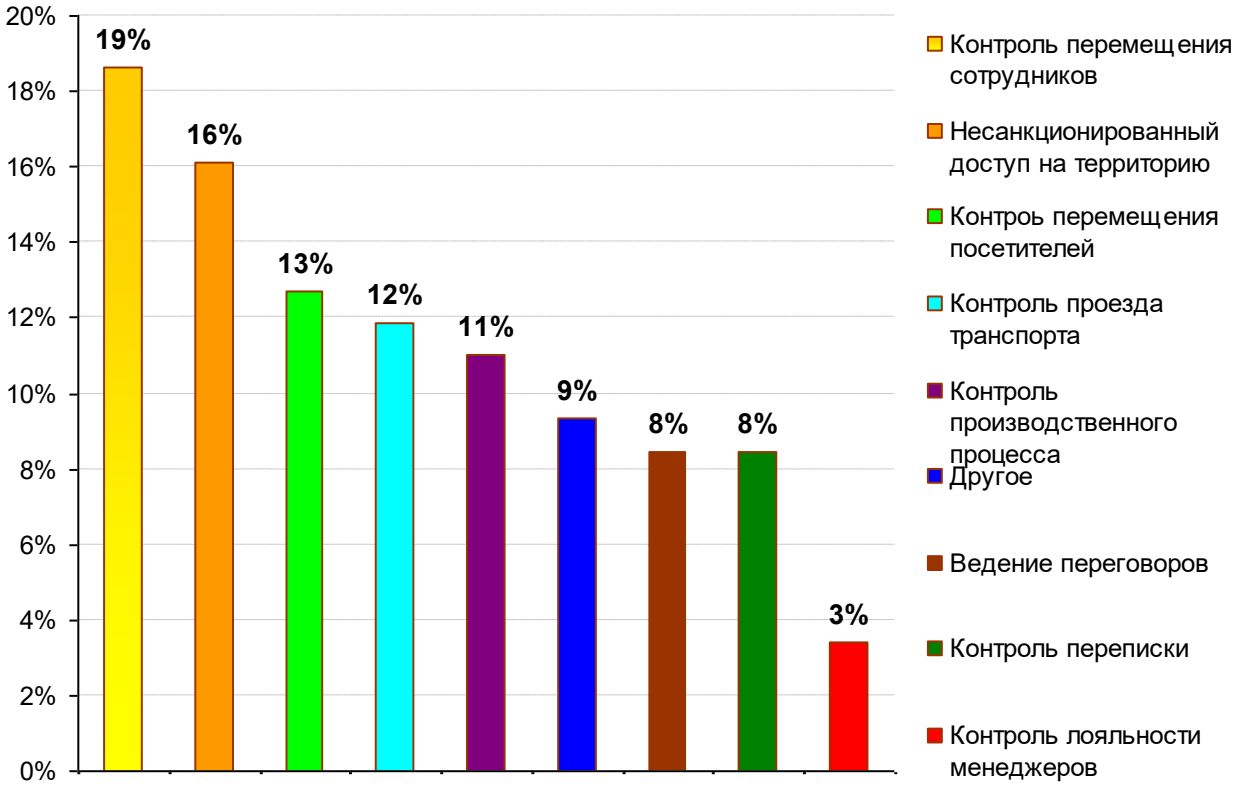

Рис. 14. Области использования ТСЗ

Большинство компаний, занятых в ювелирной промышленности, данный вопрос либо оставляли без ответа, либо сообщали, что все перечисленные сегменты контроля у них «закрыты» соответствующими средствами безопасности.

2.8. Актуальность получения достоверных сведений и лояльности сотрудников для компаний и отделов по работе с кадрами

С необходимостью получать достоверные сведения от сотрудников как при приеме на работу, так и во время исполнения своих служебных обязанностей, с потребностью достоверной оценки степени лояльности персонала сталкивается любая организация, имеющая в своем штате более одного наемного сотрудника. Потребность в контроле сотрудников и сложность его осуществления

руководством компаний растет по мере увеличения штатной численности сотрудников и количества подразделений, особенно удаленных, а также степени ответственности, сложности и уровню качества, предъявляемого к окончательному продукту компании, будь то товар или услуга. Поэтому участниками изучения данной проблематики стали компании:

- ✓ имеющие в своем штате более 100 сотрудников;
- ✓ имеющие не менее 2-х территориально обособленных подразделений;
- ✓ опирающиеся в своей деятельности предоставляемую информацию;
- ✓ с высокой степенью ответственности рядовых сотрудников;

Респондентами данной области исследования были сотрудники;

- ✓ подразделений отвечающих за работу с кадрами производственных, торговых и логистических компаний;
- ✓ рекрутинговых и кадровых агентств;
- ✓ кредитных учреждений;
- ✓ служб безопасности.

Все опрошенные респонденты высоко оценили необходимость достоверности информации, добросовестного исполнения сотрудниками своих обязанностей, высокой степени лояльности сотрудников к компании. Но, не смотря на это, для контроля деятельности сотрудников, технические средства используют только 31 % респондентов (см. рисунок 15),

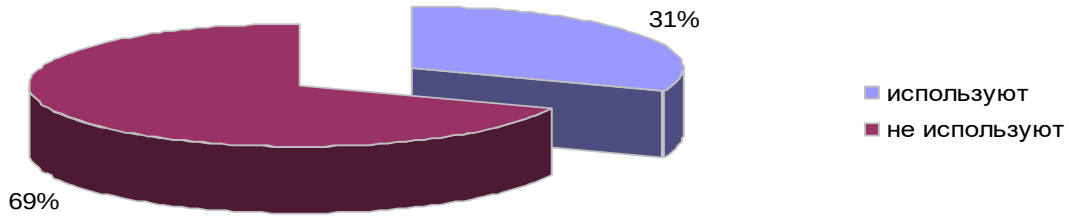

Рис. 15. Использование технических средств для контроля деятельности сотрудников

а доля компаний, использующих технические средства для проверки достоверности сведений предоставляемых сотрудниками, в том числе и при приеме на работу, как видно из рисунка 16, еще ниже и равна 7%.

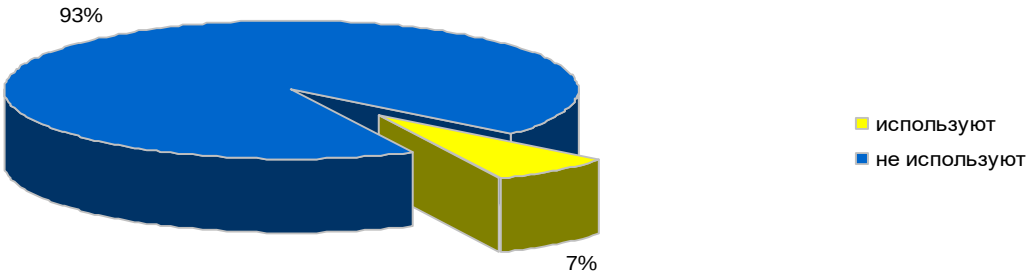

Рис.16. Использование технических средств для проверки достоверности сведений

В качестве основного технического средства контроля выполнения сотрудниками своих служебных обязанностей используются системы видеонаблюдения открытого и скрытого размещения. При этом наблюдение за работой сотрудников осуществляется, в основном, в рамках контроля общей ситуации в помещении или на объекте.

Исследование показало низкую осведомленность респондентов, отвечающих за работу с кадрами на предприятиях, о возможности использования технических средств в сфере их деятельности. Те же, кто располагает какой-либо информацией, основной причиной их не использования в текущей деятельности назвали их высокую стоимость, хотя и не смогли назвать какую-либо точную цифру. Оказалось, что среди респондентов, не использующих данное оборудование, уровень заинтересованности HR-подразделений компаний значительно выше, чем в рекрутинговых и кадровых агентствах (см. рис.17).

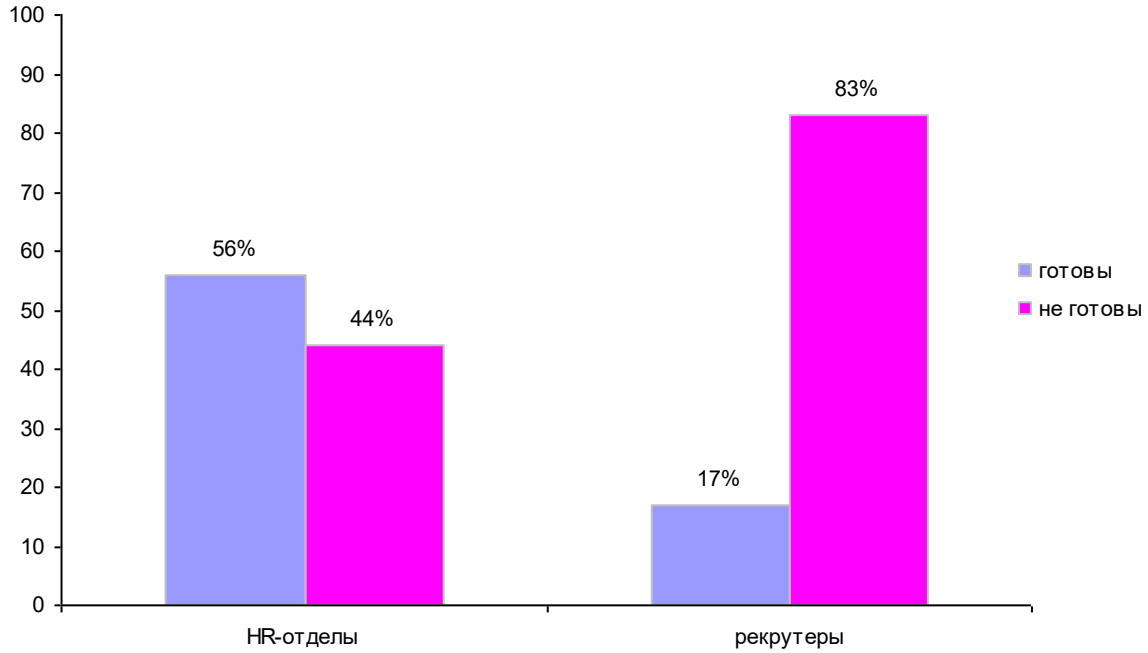

Рис.17. Готовность использовать технические средства в текущей деятельности

Неготовность рекрутинговых и кадровых агентств использовать технические средства для проверки данных соискателей вызвана (см.рис. 18):

- ✓ высокой стоимостью технических средств;
- ✓ продолжительностью процесса проверки;
- ✓ законностью данного способа проверки;
- ✓ этическими соображениями;

- ✓ отсутствием необходимости.

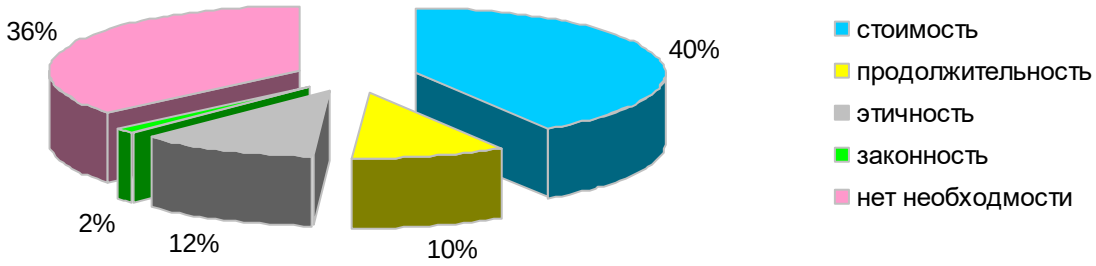

Рис.18. Причины не использования технических средств рекрутинговыми агентствами

В HR-службах предприятий ситуация несколько иная (см. рис.19).

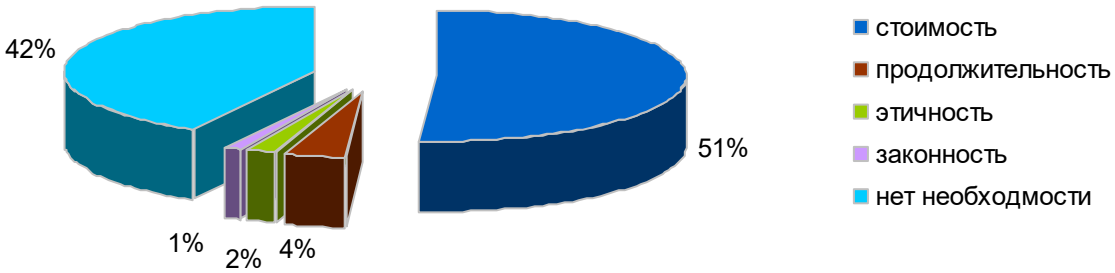

Рис.19. Причины не использования технических средств HR-службами предприятий

В результате глубинных интервью было выделены основные ситуации, при которых необходимо применение технических средств:

- ✓ потоковый прием на работу;
- ✓ единичные проверки сотрудников (повышение в должности и т.п.);
- ✓ проведение служебных расследований;
- ✓ поиск причин утечки информации;

основные сведения, которые обычно пытаются не афишировать:

- ✓ степень удовлетворенности;
- ✓ уровень лояльности;
- ✓ криминальные наклонности;
- ✓ криминальное прошлое;

- ✓ неприемлемые признаки (алкоголизм, наркомания, психические заболевания).

а методы, которые респонденты используют или могут использовать для получения информации о скрываемых сведениях:

- ✓ опрос сотрудников, руководителей;
- ✓ анкетирование;
- ✓ использование специальной техники для скрытого наблюдения;
- ✓ собеседование;
- ✓ психологическое тестирование;
- ✓ опрос с использованием «Полиграфа»;

При анализе методов проверки сведений можно выделить следующие характеризующие их параметры:

- ✓ достоверность результата;
- ✓ гласность применения;
- ✓ официальность применения;
- ✓ время проведения проверки;
- ✓ время получения результата.

При рассмотрении ситуаций и основных методов проверки скрываемых сведений с учетом характеризующих параметров можно оценить эффективность применения каждого из методов проверки этих сведений.

На рисунке 20 наглядно показана значимость каждого параметра методов проверки в ситуациях, в которых возможно использование технических средств.

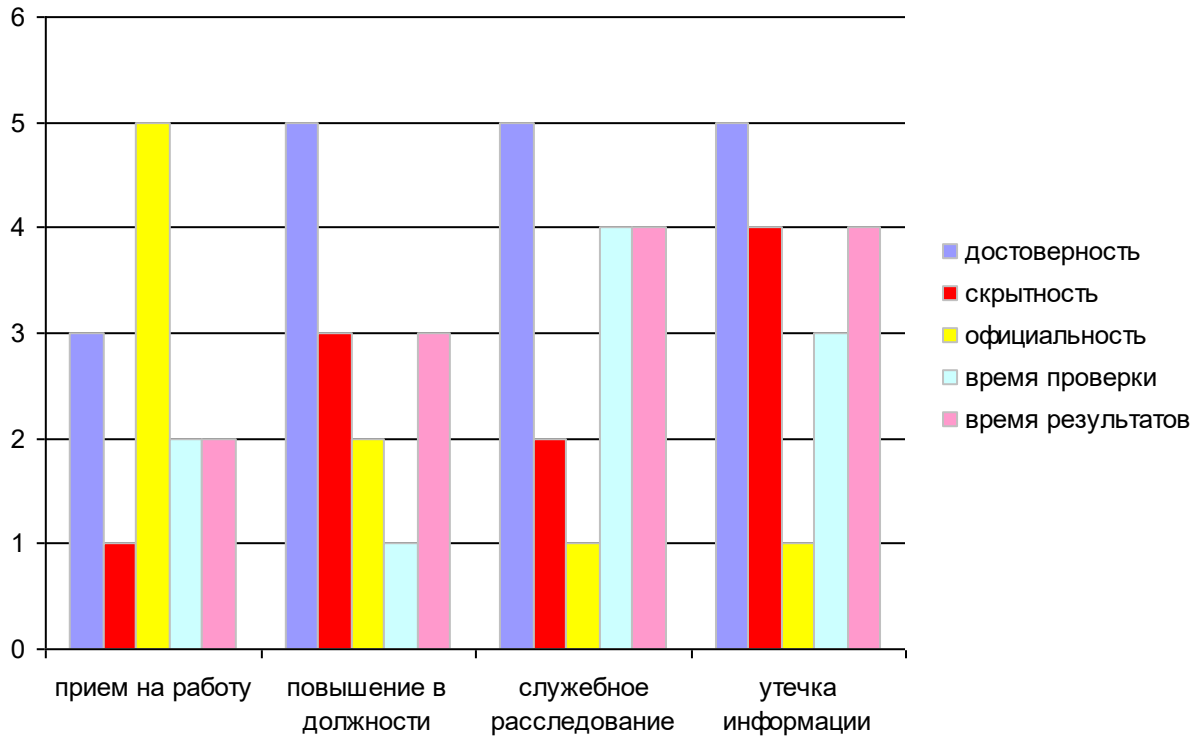

Рис. 20. Степень важности параметров проверки в различных ситуациях

Рисунок 21 иллюстрирует характеристики параметров, которых можно достичь различными методами проверки.

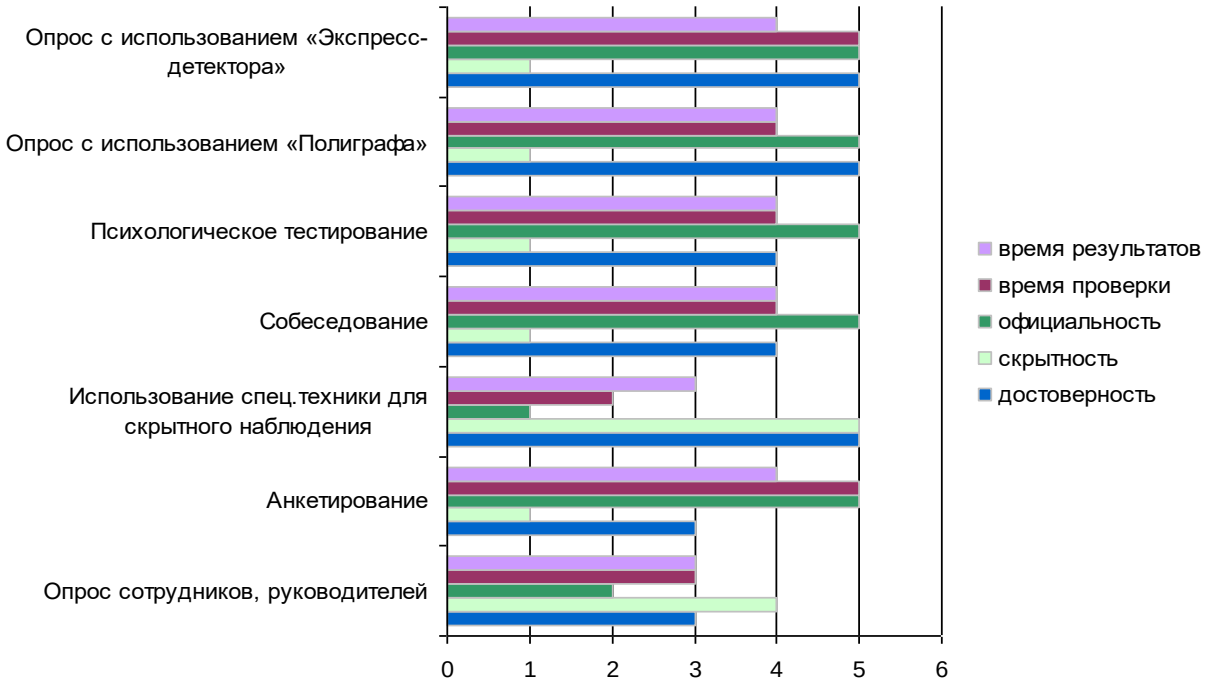

Рис. 21. Уровень параметров проверки в каждом из методов

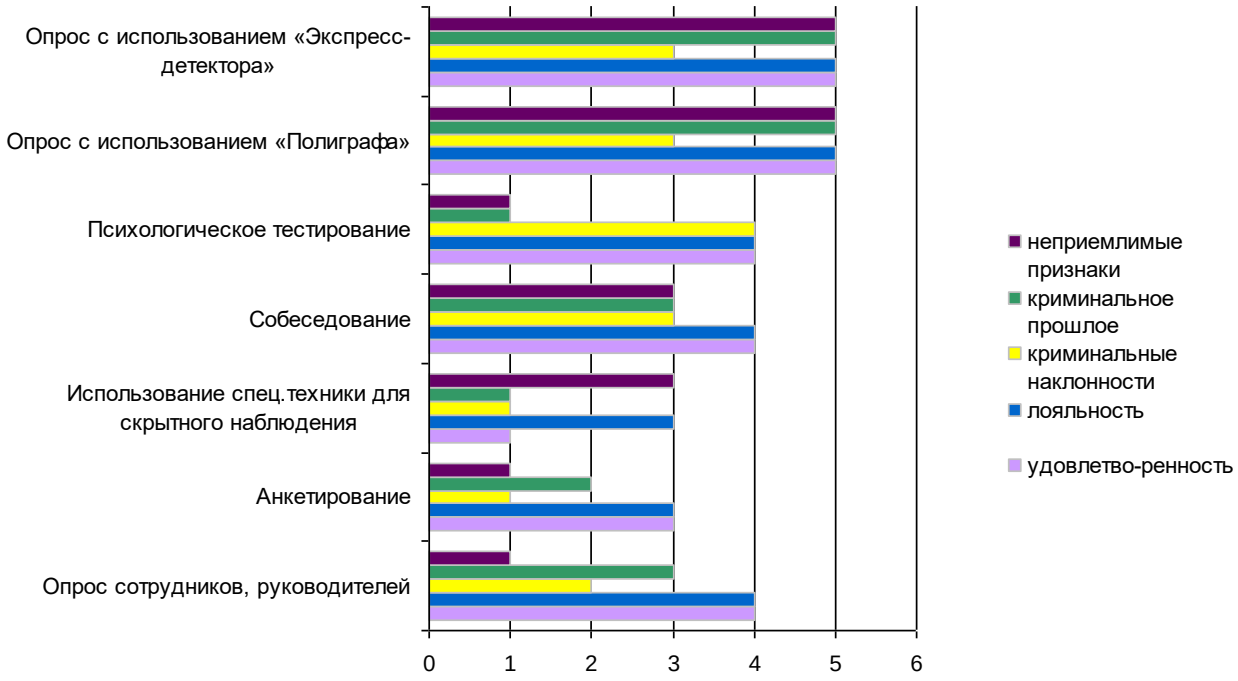

Рис. 22. Уровень достоверности сведений, определяемый с помощью различных методов

Рисунок 22 наглядно иллюстрирует, что наилучшим методом проверки достоверности информации является метод опроса с использованием Полиграфа.

2.9. Актуальность выявления недобросовестных заемщиков на стадии проверки данных для принятия решения по выдаче кредита

В последние годы наблюдается устойчивый рост экономики, который сопровождается оживлением финансового рынка страны, в частности сферы кредитования как юридических, так и физических лиц.

Объем выданных кредитов за 2010 год составил более 84 триллионов грнлей, из них около 22 процентов от общего объема составили кредиты частным лицам (рис. 23).

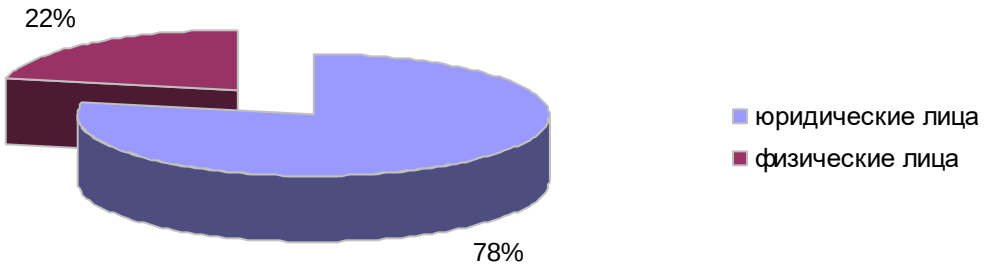

Рис.23. Соотношение кредитов, выданных в 2010 году коммерческими банками юридическим и физическим лицам

Такая высокая активность на рынке кредитования физических лиц вызвана необходимостью расширения рынка сбыта основного продукта банковской деятельности – кредита. Освоив рынок кредитования предприятий и организаций, который отличается высокой степенью надежности и обеспеченности, банки достаточно быстро освоили рынок залогового кредитования физических лиц, ипотечное и автомобильное кредитование. Необходимость дальнейшего развития заставляет кредитные учреждения осваивать наиболее рискованную область – кредитование физических лиц, и предложение все большего количества без залоговых вариантов потребительского кредитования. Интенсивное развитие данного сегмента рынка кредитования привело к тому, что просроченная задолженность по кредитам физических лиц позволило некоторым финансовым аналитикам говорить об угрозе банковского кризиса. К сожалению, данные процессы всегда сопровождали бурный рост развития потребительского кредитования.

Глубинные интервью с работниками банковской сферы позволили выяснить основные способы снижения угрозы нежелательных действий третьих лиц, т.е. недобросовестных заемщиков, и борьбы с просроченными задолженностями.

Основными документами, регулирующими взаимоотношения Банка-кредитора и заемщика, являются Договор о кредите, Закон о правах потребителей, Гражданский кодекс РФ, Кодекс РФ об административных правонарушениях. Именно низкая степень определенности взаимоотношений банка и заемщика заставляет Минфин ускоренно работать над новым Законом о потребительском кредите.

Основными средствами воздействия на недобросовестных заемщиков в настоящий момент являются судебные разбирательства, коллекторские агентства и собственные службы безопасности. Как показывает практика, эффективность работы судебных органов и собственных служб безопасности в данной области крайне низка. Чуть эффективнее действуют коллекторские агентства (см. Приложение 10). Это пока новый вид деятельности, которому необходимо пройти период становления, но и он борется только с последствиями.

На стадии принятия решения о выдаче кредита банки пытаются защитить себя с помощью следующих основных средств:

- ✓ повышение процентной ставки в зависимости от степени риска кредита;
- ✓ скоринг;
- ✓ различные базы данных.

Базы данных

При принятии решения о выдаче кредита банки подают запросы в различные организации с целью проверки информации, которую предоставляет заемщик. В основном, это проверки через базы данных МВД, Федеральной Миграционной Службы (ФМС), созданного в 2005 году по инициативе Федеральной Службы по Финансовым Рынкам (ФСФР) Бюро Кредитных Историй (БКИ)

Скоринг (см. Приложение 9)

Банкам, выдающим кредиты, требуется каким-либо образом оценить нового клиента и принять решение о выдаче или невыдаче ему запрашиваемого кредита. В мировой практике существует два основных метода осуществления этой процедуры, которые могут применяться как отдельно, так и в сочетании друг с другом:

- ✓ субъективное заключение экспертов или кредитных инспекторов;
- ✓ автоматизированные системы скоринга.

Методика оценки кредитного риска посредством скоринговых систем, позволяет, оценив набор социальных признаков, характеризующих заемщика, сказать, стоит ли выдавать ему кредит. Эта методика используется уже на протяжении более полувека для оценки кредитоспособности, как предприятий, так и физических лиц. Важной особенностью скоринговых систем является то, что решение о выдаче кредита может приниматься автоматически без участия специалиста.

Согласно общей философии скоринга, не требуется искать объяснения, почему данный клиент не вернул выданные деньги. Скоринг выделяет те характеристики, которые наиболее тесно связаны с ненадежностью или, наоборот, с надежностью клиента. Основным недостатком скоринговых систем является непродолжительный срок «жизни», который обусловлен необходимостью частой корректировки признаков, характеризующих заемщика.

Процентная ставка

Бизнес-модель, господствующая на рынке потребительского кредитования, описывается так: добросовестный заемщик платит за себя и за недобросовестного заемщика. Платить приходится много: несмотря на то, что на рынок выходят все новые игроки, эффективные ставки остаются очень высокими. В целом по стране девять добросовестных заемщиков платят за одного неплательщика. Логика банков проста, пусть эти девять клиентов заплатят больше, чем судебным приставам и коллекторам бегать за десятым и отбирать у него мобильный телефон.

Учитывая вышесказанное, можно констатировать, что кредитные организации не располагают в настоящий момент каким-либо действенным универсальным средством, которое можно использовать в противостоянии с недобросовестными заемщиками. Потребительский рынок и Закон о потребительском кредите заставят банки не только открыто информировать о реальных эффективных ставках по кредитам, но и снижать их. Это вызовет необходимость использования новых средств определения достоверности информации. И именно в области проверки и мониторинга информации для принятия решения о предоставлении потребительского кредита необходимо в полной мере использовать все технические возможности Полиграфа.

2.10. Характеристика основных сегментов

Для определения потенциального спроса на новый продукт в области обеспечения технической безопасности и изучения факторов, влияющих на выбор системы безопасности, был выбран метод глубинных интервью. В выборку вошли представители предприятий-производителей или крупных дистрибуторов ювелирной и фармацевтической продукции, кредитных подразделений банков, служб безопасности, логистических и складских предприятий, а также крупных заводов.

Исследование показало, что основная масса предприятий закрыта в части обсуждения темы безопасности, использования средств безопасности. Некоторые сотрудники дали исчерпывающую информацию в ходе интервью, но просили их не упоминать. Все участники интервью проявили заинтересованность в получении дальнейшей информации о возможностях полиграфа».

В структуре выборки преобладают компании с численностью сотрудников более 1000 человек и от 100 до 300 человек (по 4 и 5 компаний соответственно). В число компаний-респондентов с численностью более 1000 человек вошли МТУСИ, фармацевтический завод «Акрихин» (1500 сотрудников) и аптечная сеть «36’6» (1000 человек на складах и 8000 сотрудников в аптеках), ЗАО «Аэромаш» (около 1500 человек). От 500 до 1000 сотрудников работают на Ювелирном Заводе (500 сотрудников) и в группе компаний «Симплекс» (850 сотрудников). И последний сегмент компаний с численностью сотрудников до 100 человек составляют ювелирные заводы «Олин» и «Элит». Сегмент респондентов с численностью сотрудников от 300 до 500 человек остался не занят (см. рис. 25).

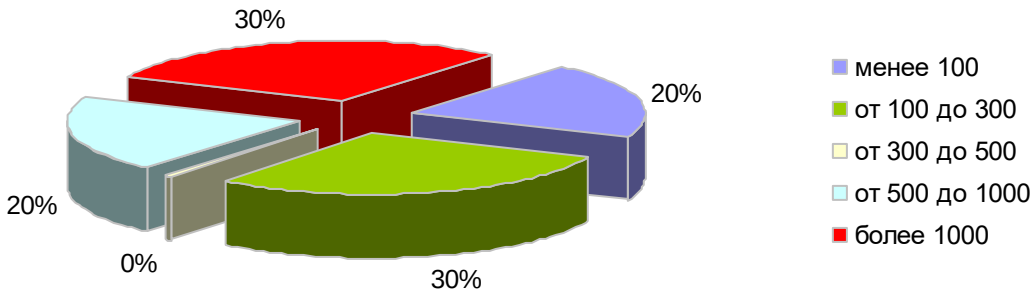

Рис. 25. Сегментация респондентов по численности сотрудников.

Среди участников интервью специальные меры для предотвращения случаев хищения на производстве используют только компании-производители ювелирных изделий. К таким мерам относятся: критичный отбор сотрудников при приеме на работу, их проверка службой безопасности, жестко регламентированная приемка-сдача драгоценных металлов и драгоценных камней в начале и конце смены, отслеживание движения металла и камней по цехам.
Специальных технических систем и устройств, направленных на пресечение хищений, не использует никто из компаний-респондентов, кроме ЗАО «Аэромаш», применяющее в своей работе различную досмотровую технику.
Кредитные организации пользуются описанными выше методами и способами, логистические и складские компании используют обычные системы видеонаблюдения и сигнализацию. В целом компании используют следующие технические средства:

- ✓ видеонаблюдение;
- ✓ контроль доступа на предприятие и в различные помещения;
- ✓ металлодетекторы;
- ✓ личный досмотр;
- ✓ детекторы лжи используют 30% респондентов;
- ✓ сигнализация;
- ✓ складской учет, наблюдение, предусмотрение материальной ответственности в трудовом договоре – это самые распространенные методы предотвращения и регистрации хищений и недостач в компаниях респондентов.

У всех респондентов на предприятии организована служба безопасности, ее численность варьируется от 2-х до 1000 человек, все сотрудники прошли специальную подготовку и оснащены технически. Некоторые респонденты разделяют СБ и охрану, в этом случае обычно охрану объектов осуществляют привлеченные ЧОПы или вневедомственная охрана.

2.11. Оценка потребности в технических средствах безопасности

Больше половины участников исследования затруднились оценить приблизительную сумму ущерба предприятия в год. Часть из них сослались на закрытость подобной информации, а часть не располагала об этом информацией.
Из тех ювелирных заводов, кто признался в фактах воровства, также никто не смог оценить финансовые потери компании, но сложность подобной оценки объясняли тем, что на производстве используются драгоценные камни с различными характеристиками (существует шкала оценок камней с разным набором характеристик по цвету, прозрачности, огранке и т.п.), соответственно, цена камня тем больше, чем больше оценка по данной шкале. Были случаи подмен этих камней сотрудниками при приемке-сдаче ценностей в начале и конце смены – в этом случае сумма ущерба будет зависеть от стоимости камня, которая, в свою очередь, зависит от его оценки по набору характеристик. Существуют также технические потери драгоценного металла (определенный % потерь при переплавке, остаток стружки и т.п.), что провоцирует некоторых сотрудников выдать кражу за технические потери – здесь также сумма производственных потерь будет зависеть от многих факторов конкретного технологического процесса.

В качестве возможного использования нового продукта Заказчика участникам исследования были предложены две гипотезы (см. рис. 26 и 27):

- ✓ определение нарушений и их составляющих по факту их совершения (выявление и наказание виновного);
- ✓ предотвращение нарушений и их составляющих на этапе появления умысла у сотрудника или третьего лица (выявление и профилактика злоумышленников).

Первая гипотеза позиционирования нашла подтверждение у 90 % респондентов, которые отметили, что уличать преступников, совершивших кражу продукции на рабочем месте, для них «очень важно» (60% ответов) и «важно» (30% ответов). Представитель одного ювелирного завода заявил, что краж на данном предприятии не происходит, чему способствуют принятые меры по регламенту сдачи-приемки сырья в начале и конце смены, поэтому данное позиционирование на него не будет иметь действия.

Возможность определять появление у работника намерения о краже заинтересовала всех участников исследования, из них 70% присвоили второй гипотезе позиционирования оценку «очень важно» и 30% - оценку «важно».

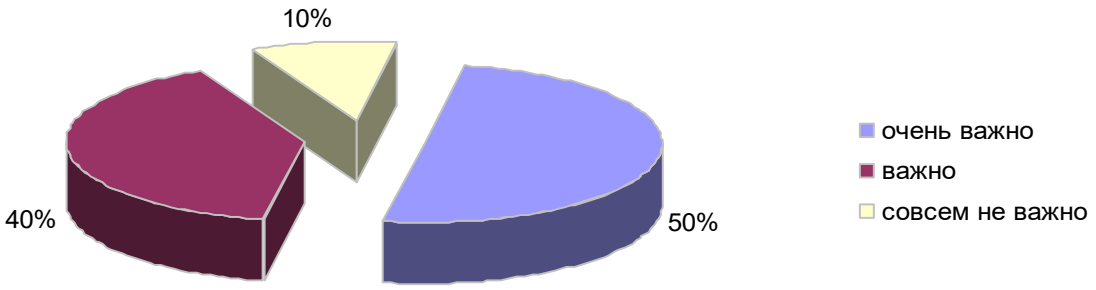

Рис. 26. Важность определения нарушений по факту

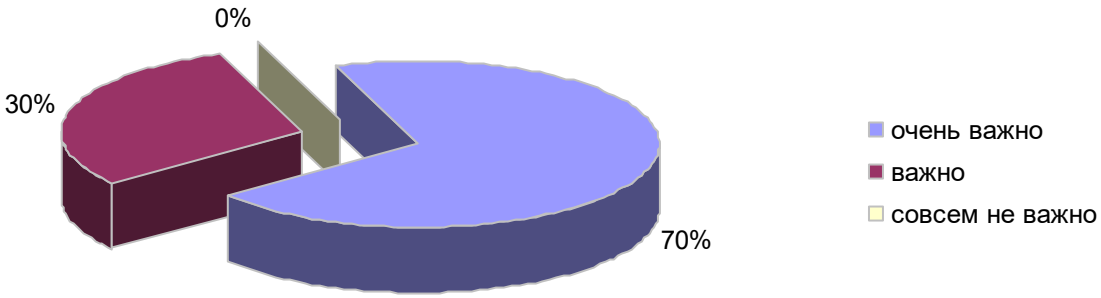

Рис. 27. Важность определения негативных намерений

Предложение использовать Полиграф в повседневной деятельности, показалось интересным всем респондентам, причем 70% из них в подтверждение своего интереса стали активно задавать интервьюеру вопросы по данному устройству, а интерес остальных 30% можно охарактеризовать, как пассивный (похоже на стандартное «направляйте предложение – будем рассматривать»).
Вопросы тех респондентов, которые проявили активный интерес к Полиграфу:

- ✓ принципа действия устройства;
- ✓ преодоления недоверия в отношении его эффективности;
- ✓ точность диагностики правдивых и ложных ответов;

2.12. Факторы, влияющие на потенциал спроса

В ходе интервью респондентам задавался вопрос, каким требованиям, влияющим на потенциал спроса, должно отвечать новое техническое средство безопасности. Анализ ответов показывает, что ключевые позиции среди характеристик, которым при покупке будет уделено пристальное внимание, занимают:

- ✓ степень достоверности информации должна быть максимально приближена к 100 %;
- ✓ вероятность ошибки при диагностике должна быть сведена к минимуму и, желательно, документально подтверждена;
- ✓ техническая надежность аппарата, устойчивость к намеренным и случайным повреждениям.

При выборе систем безопасности в целом и систем защиты от действий инсайдеров в частности, оценки респондентами факторов, которые будут влиять на их выбор, распределились следующим образом (см. рис. 28):

- ✓ максимальные оценки по пятибалльной шкале получили основная цель внедрения «сокращение финансовых потерь» и фактор выбора «срок эксплуатации оборудования» - по 4,9 балла;
- ✓ чуть меньшая важность присвоена факторам «точность полученной информации» и «бесплатное обучение специалистов» компании-покупателя оборудования – 4,8 и 4,7 балла соответственно;
- ✓ факторы «наличие сертификатов и лицензий» на предлагаемое рынку оборудование и «стоимость оборудования при установке и обслуживании» получили также оценки выше среднего, а именно: 4,4 и 4,2 балла соответственно;
- ✓ оценки ниже среднего получили такие факторы выбора ТСЗ, как: «длительность гарантийного периода» (4,0), «время, затраченное на диагностику ложных ответов» (3,8), «бесплатное обслуживание специалистами производителя или продавца оборудования» во время гарантийного периода (3,7) и «марка и известность производителя оборудования» (3,1).

Рис. 28. Факторы, влияющие на выбор ТСЗ

В 30-ти % опрошенных компаний решение о привлечении полиграфолога в данной области принимает непосредственно начальник службы безопасности. Это крупные компании с численностью сотрудников

около 1000 человек или больше, где функции решения оперативных вопросов и вопросов обеспечения делегированы в соответствующие структурные подразделения в рамках выделяемых бюджетов.

В небольших компаниях (численность в пределах 300 человек) решение о привлечении полиграфолога или закупки средств технической защиты принимает первое лицо компании – генеральный директор или владелец бизнеса/учредитель.

В компаниях оставшихся 50% респондентов решения о выборе систем безопасности принимаются коллегиально, по представлению руководителя СБ с аргументацией и экономическим обоснованием, но последнее слово за первым лицом компании.

2.13. Основные каналы информации потребителей

В ходе исследования были выявлены источники информации для респондентов, принимающих решение о закупке ТСЗ либо влияющих на принятие решения, о профильном рынке и о рынке средств безопасности. Каналы информации потребителей были разделены на несколько подгрупп и представлены в таблице 16. Кроме того, специалистами «Келис Консалтинг» был проведен дополнительный анализ отраслевых журналов, предприятий не участвовавших в исследовании (парфюмерно-косметическая и химическая промышленность), результаты также можно увидеть в таблице 16.

Таблица 16. Источники информации респондентов

Отрасли	Название
Специализированная пресса	Формула безопасности
	Мир безопасности
	Системы безопасности
	Безопасность бизнеса
Профессиональная пресса (юв. отрасль)	Навигатор ювелирной торговли
	Русский ювелир
	Ювелирное обозрение
	Драгоценные металлы. Драгоценные камни
Профессиональная пресса (фарм. отрасль)	Ремедиум (фармацевтика и медтехника)
	Аптека
	Фармацевтическая промышленность
	Фармацевтическая служба
Профессиональная пресса (парфюм. отрасль)	Косметика и парфюмерия (сектор B2B)
	Косметический рынок сегодня
Профессиональная пресса (химич. отрасль)	Химия и бизнес
	Химия и рынок
	Химическая промышленность сегодня
Деловые издания	РБК daily
	Коммерсант
	Ведомости
	Кадровый менеджмент
	Логистика и склад
	HR-digest
	Банковское обозрение
	газета

Отрасли	Название
Электронные ресурсы	
Выставки/форумы по безопасности	
	Технологии безопасности

Рисунок 29 иллюстрирует, что уровень доверия участников опроса к информации, получаемой из отраслевых и деловых изданий, самый низкий – до 3х баллов по пятибалльной шкале.

Далее по степени доверия, по мнению респондентов, следует информация о средствах безопасности, опубликованная на корпоративных сайтах производителей и дистрибуторов данных средств, на специализированных ресурсах по безопасности, а также рекомендации известных экспертов в мире безопасности – по 3,3 балла.

На второе место в рейтинге доверия к каналам информации участники исследования поставили информацию, получаемую на различных тематических и отраслевых выставках, конференциях, форумах по безопасности – оценка 3,6 балла.

На первом же месте по степени доверия респондентов к источникам информации о ТСЗ стоит мнение коллег, знакомых и существующий опыт компаний, использующих предлагаемое производителем оборудование – оценки 4,0 и 3,9.

Полученные результаты анализа источников информации подтверждаются комментариями некоторых участников исследования, которые категорично утверждали, что при выборе новой системы защиты предприятия или при рассмотрении предложения об использовании полиграфа в этой области, будут обязательно обращаться к своим знакомым из спецслужб и госорганов (это, в основном, руководители СБ – выходцы из этих самых служб).

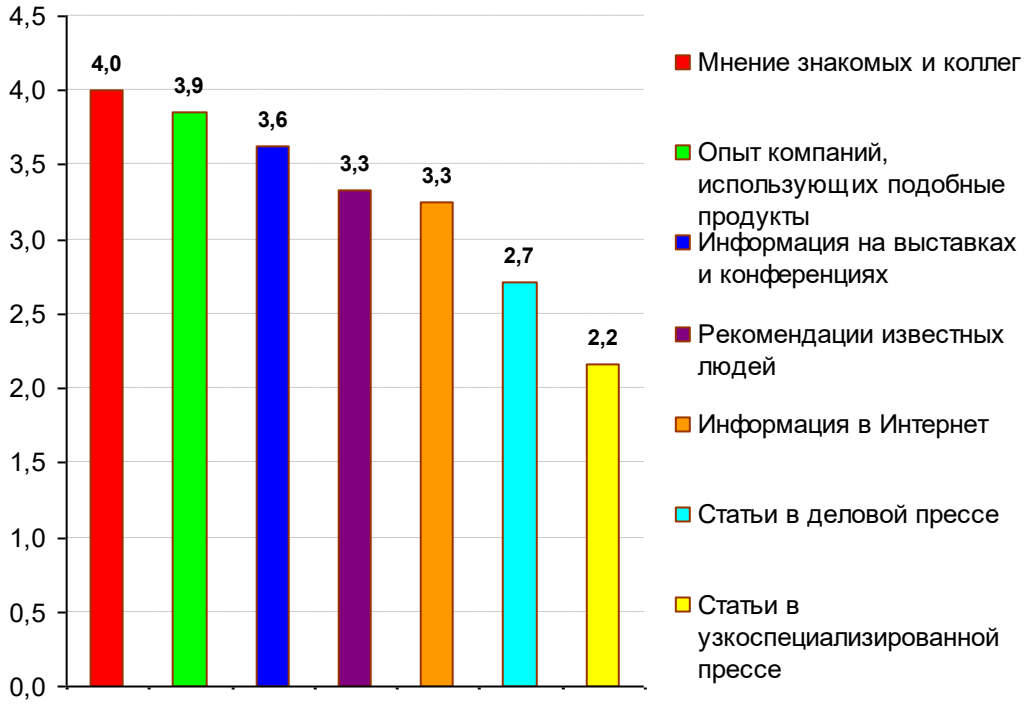

Рис. 29. Уровень доверия к источникам информации о ТСЗ

2.14. Общие выводы

- Сейчас все больше набирает обороты распространение концепции удовлетворения потребностей (а не концепция товаров и услуг), что означает, что производители и продавцы различной продукции конкурируют между собой не аналогичными товарами и услугами, а способами удовлетворения одинаковых потребностей покупателей своей продукции.

- Полиграфам приходится конкурировать с другими методами и средствами, которые удовлетворяют потребность промышленных предприятий в обеспечении безопасности от преступных действий и намерений собственного персонала.

- Компании характеризуются закрытостью информации.

- Около 60% производственных предприятий выявляются случаи хищения, а происходит больше, но не все руководители в этом признаются.

- Около 40% респондентов не используют средств технической защиты, а из оставшихся 60-ти % большинство используют СТЗ более 4-х лет, но 17% активных пользователей не довольны эффективностью работы своих СТЗ.

- Основной сегмент средств безопасности, используемых на предприятиях, составляют системы контроля и управления доступом (СКУД), чуть меньше – видеонаблюдение, а из-за повсеместной распространенности в банках - скоринговые карты.

- **В целом, среднестатистический портрет потенциального потребителя полиграфных услуг можно описать, как предприятие:**

  - ✓ численностью сотрудников от 100 до 1000 человек;
  - ✓ имеющее собственную службу безопасности, имеющую традиционное техническое оснащение;
  - ✓ которое не в состоянии обеспечить необходимый уровень защиты и безопасности традиционными средствами;
  - ✓ где решения о применении новых методов и ТСЗ принимает первое лицо по обоснованию от руководителя ответственного подразделения заинтересованного в предотвращении этих случаев с помощью действенных ТСЗ по приемлемой стоимости.

- Основное влияние на выбор технических средств безопасности руководителями СБ оказывают рекомендации их коллег и знакомых из сферы безопасности и силовых структур.

3. РЕКОМЕНДУЕМАЯ СТРАТЕГИЯ ВЫВОДА УСЛУГ НА РЫНОК

Из всего многообразия существующих технических средств безопасности были выбраны наиболее часто и эффективно используемые:

- ✓ рентгенографический сканер;
- ✓ металлодетектор;
- ✓ система MindReader;
- ✓ голосовой анализатор Nemesysco;
- ✓ скоринговые карты;
- ✓ биометрический прибор (как опция);
- ✓ классический полиграф.

На основании экспертных оценок были определены основные потребности, которые способны удовлетворить существующие технические средства:

- ✓ визуальное отображение не металлических предметов в одежде, на теле, в теле человека;
- ✓ выявление не разрешенных предметов;

- ✓ выявление склонности человека к противоправным действиям;
- ✓ неплатежеспособность;
- ✓ определение степени благонадежности человека;
- ✓ отображение металлических предметов в одежде, на теле, в теле человека;
- ✓ персональная регистрация человека;
- ✓ регистрация присутствия металлических предметов в одежде, на теле, в теле человека;
- ✓ составление психологического портрета;
- ✓ установление возможного утаивания информации человеком;
- ✓ фиксация психологической реакции человека.

В сравнительной таблице 17 был проведен анализ удовлетворения каждой из потребностей выбранными техническими средствами.
Таблица наглядно иллюстрирует, что ни рентгенографический сканер, ни скоринговая система не являются прямым конкурентом полиграфному оборудованию.

Таблица 17. Сравнительная таблица удовлетворения потребностей техническими средствами безопасности.

		Рентгено-графический сканер	Металло-детектор	MindReader	Голосовой анализатор	Полиграф	Скоринг	Биометрия
1.	Визуальное отображение не металлических предметов в одежде, на теле, в теле человека	ДА						
2.	Выявление не разрешенных предметов	ДА				ДА		
3.	Выявление склонности человека к противоправным действиям			ДА	ДА	ДА		
4.	Неплатежеспособность					ДА	ДА	
5.	Определение степени благонадежности человека				ДА	ДА		
6.	Отображение металлических предметов в одежде, на теле, в теле человека	ДА						
7.	Персональная регистрация человека							ДА
8.	Регистрация присутствия металлических предметов в одежде, на теле, в теле человека	ДА	ДА					
9.	Составление психологического портрета			ДА				
10.	Установление возможного утаивания информации человеком				ДА	ДА		
11.	Фиксация психологической реакции человека			ДА	ДА	ДА		

В отношении более четкого определения сегментов потенциальных потребителей можно выбрав некоторые критерии, такие как:

- ✓ платежеспособность высокая или низкая;
- ✓ практика использования средств безопасности – есть или нет;
- ✓ направление использования – внешнее или внутреннее.

можно более четко сформировать круг наиболее перспективных потенциальных покупателей. В первую очередь это:

- ✓ банки;
- ✓ аэропорты;
- ✓ предприятия добывающей промышленности (драгоценные металлы и камни);
- ✓ крупные торговые организации;
- ✓ производственные предприятия.

специалисты «Келис Консалтинг» рекомендуют позиционировать услуги полиграфолога, который с высокой степенью точности определит достоверность информации по широкому спектру вопросов.

3.1. Стратегия вывода нового продукта на рынок

Согласно матрице Ансоффа в нашем случае применима стратегия вывода нового продукта на старый рынок («стратегия роста», см. таблицу 18, квадрат 3). Данная стратегия характеризуется средней степенью риска, вероятность успеха при выборе данной стратегии оценивается, по данным научных международных исследований, в 33%.

Таблица 18. Матрица Ансоффа

	Существующие Товары (Услуги)	**Новые Товары (Услуги)**
Существующие Рынки	1. Рост на существующих товарных рынках • Увеличение доли рынка • Интенсификация потребления ❑ Увеличение частоты использования ❑ Увеличение используемого количества ❑ Поиск новых способов применения для существующих потребителей	3. Разработка новых товаров • Расширение функций • Разработка товара нового поколения • Разработка новых товаров для того же рынка
Новые рынки	2. Расширение рынка • Географическое расширение • Выход на новые сегменты	4. Диверсификация товара • Родственная • Неродственная

При выводе данных услуг на рынок необходимо учитывать такие факторы и особенности менталитета людей и особенностей работы предприятий, как:

- ✓ сопротивление нововведениям, производимым организацией;
- ✓ восприятие внедрения новых услуг, как попытку вторжения в личную жизнь сотрудников;
- ✓ восприятие внедрения новых услуг, как недоверие к собственным сотрудникам, что может повлечь снижение лояльности;

Как уже было упомянуто ранее, услуги полиграфолога, с одной стороны, удовлетворяют уже имеющиеся потребности предприятий в защите, с другой стороны, являются новыми услугами а, следовательно, при выводе его на рынок для успешного продвижения необходимо привлечение к нему внимания потенциальных потребителей, объяснение принципов его действия и аргументация преимуществ по сравнению с существующими на рынке продуктами, привычными для решения схожих задач.

3.2. Стратегия продвижения, каналы коммуникаций

Ввозможно использование различных стратегий продвижения и каналов маркетинговых коммуникаций, но есть элементы, которые должны в обязательном порядке присутствовать в любом варианте стратегий.

1. Демонстрационные испытания.

Эти испытания должны проводиться в значимых организациях, имеющих определенный вес в обществе. Их положительные отзывы о работе компании окажут большее влияние на формирование положительного имиджа и станут гарантом продвижения услуг для других организаций

2. Пропаганда.

В качестве основного способа информирования потенциальных покупателей о полиграфных услугах, использовать методы пропаганды, т.е. информационные сообщения, статьи или очерки в СМИ, которые кажутся более правдоподобными, чем прямая реклама, т.к. сообщение поступает виде новостей. А прямая реклама может вызвать отторжение.

3. СМИ.

При выборе СМИ, через которые планируется воздействовать использовать отраслевую периодику для воздействия на конкретное подразделение предприятия, которое сможет получить дополнительный экономический эффект при использовании оборудования.

4. Интернет.

Высокий результат продвижения новой услуги обеспечивается за счет контекстной рекламы. Эффективность продвижения новой услуги может быть значительно повышена созданием нового сайта или странички.

6. Рекламные материалы.

При изготовлении рекламных материалов особое внимание необходимо уделить качеству полиграфии, фотографий, текстов, которые должны содержать ровно столько информации, сколько необходимо для формирования вопроса, на который можно получить ответ только у продавца. Рекламные материалы так же желательно ориентировать на конкретные группы потребителей.

7. Коммерческое предложение

При формировании коммерческих предложений в обязательном порядке учитывать интересы того сегмента потребителя, которому оно направляется.

При выводе на рынок полиграфных услуг, рекомендуется использовать позиционирование, направленное на удовлетворение двух потребностей целевой аудитории:

- ✓ профилактика и выявление хищений материальных ценностей;
- ✓ профилактика и выявление несанкционированного использования интеллектуальной собственности компании.

Тема инсайдерства последние два года активно муссируется в средствах массовой информации и различных аналитических обзорах. Основные игроки рынка безопасности, формирующие паблисити на тему инсайдерства и привлекающие внимание общественности к данной проблеме, это:

- ✓ компания InfoWatch (ведущий производитель программного обеспечения для защиты информации);
- ✓ LETA IT-company (их основной дистрибутор и компания, специализирующаяся на внедрении ПО и оборудования для защиты информации, здесь внедрена система InfoWatch);
- ✓ Gartner, Ernst&Yong (ведущие мировые исследовательские и консалтинговые компании).

Баннерную рекламу необходимо использовать эпизодически и параллельно с основными маркетинговыми коммуникациями, с целью их поддержки и усиления эффекта привлечения внимания к новому устройству. Размещение баннерной рекламы необходимо планировать только на тех интернет-ресурсах, которые посещают лица, заинтересованные в использовании услуг полиграфолога.

Участие в выставках, также нельзя игнорировать, так как это очень эффективный способ привлечения новых клиентов. Такие мероприятия необходимо тщательно выбирать в соответствии с целевой аудиторией (посетители должны являться лицами, принимающими решения о приобретении услуг).

Варианты участия в выставках могут быть различны, это не обязательно присутствие со стендом: можно договориться о присутствии на стенде партнера, организаторы также предоставляют дополнительные рекламные опции, например, вложение материалов в пакет посетителя выставки или участника конференции, можно организовать стойку-ресепшн с демонстрацией работы и раздачу рекламных материалов, и т.д. Рекламные возможности могут меняться в зависимости от выставки и ее организаторов.

PR-мероприятия. Можно подготовить ряд публикаций и направить в электронные и печатные СМИ. Далее необходимо наладить обратную связь с адресатами с целью отслеживания размещения публикаций и возникновения интереса к услугам, возможно, интервью, запрос на статью и т.п.

В качестве призыва к покупке (4-я стадия формирования спроса) можно провести несколько семинаров по услугам для потенциальных и очень заинтересовавшихся клиентов с обязательной демонстрацией услуг. На семинары можно пригласить представителей отраслевых и специализированных СМИ.

В качестве дополнительного канала продвижения рекомендуется рассмотреть членство в некоммерческой организациях, относящихся к индустрии безопасности. Участие в PR-мероприятиях и организуемых этими организациями даст возможность заявить о своих услугах, рассказать и механизмах их работы действия и преимуществах использования, а также расширит круг профессионального общения. Возможно использование ассоциативных каналов информации при продвижении услуг, в рамках основного коммуникативного сообщения (если они будут совпадать по тематике).

Преимущества членов ассоциаций:

- ✓ Позиционирование компании участника как профессиональной, надежной, клиентоориентированной, нацеленной на лидерство как в отраслевой среде, так и на потребительском рынке.
- ✓ Организация бизнес-коммуникаций компании участника с загрнежными предприятиями различных сегментов индустрии безопасности, международными организациями, потребителями.
- ✓ Возможность влиять на развитие рынка путем выдвижения инициатив решения актуальных проблем на профессиональном и общенациональном уровнях.
- ✓ Участие в выработке предложений, рекомендаций, деклараций и т.п. от имени Ассоциации.
- ✓ Гарантированное привилегированное участие во всех мероприятиях Ассоциации.
- ✓ Возможность получения скидок и льгот при участии в мероприятиях, организуемых членами Ассоциации, а также при участии Ассоциации.
- ✓ Информационная поддержка деятельности участников за счет инфраструктуры и ресурсов Ассоциации и ее участников.
- ✓ Продвижение компании участника с помощью PR-возможностей Ассоциации.
- ✓ Предоставление информации о компании-участнике и ее новостей на сайте Ассоциации.
- ✓ Использование рекламных носителей Ассоциации в интересах компаний-участников.
- ✓ Получение методической и содержательной поддержки в исследованиях потребительских и конкурентных рынков индустрии безопасности и продвижении на них.

3.3. Рекомендации по структуре отделов продаж и маркетинга

В случае роста продаж необходимо будет пригласить в штат одного специалиста в области продаж, в обязанности которого будут входить:

- ✓ консультации интересующихся новым устройством по телефону с описанием преимуществ сотрудничества с компаний Заказчика;
- ✓ создание и ведение базы данных потенциальных и (на перспективу) активных клиентов;
- ✓ прямые продажи: первичный контакт с потенциальным покупателем, подготовка коммерческого предложения, встречи и отслеживание статуса интереса к продукту;
- ✓ контроль за проведением прямой почтовой рассылки и обработка поступающих запросов;
- ✓ заключение договоров и координация доставки и установки;
- ✓ отслеживание информации и новостей по продуктам на корпоративном сайте;
- ✓ работа с активными клиентами после заключения договора;
- ✓ разработка условий программы лояльности клиентов (поздравления с личными, профессиональными и опраздниками, подарки и т.п.);

При планировании бюджета на комплекс маркетинга при выводе нового продукта на рынок необходимо ориентироваться на сумму, составляющую около 10-20% планируемого торгового оборота (стоимость продукции, умноженная на подтвержденное количество заказов на новой устройство).

Учитывая высокий уровень консервативности потенциальных потребителей, наибольший эффект можно получить, используя в качестве основного способа маркетинговых коммуникаций метод пропаганды. Ненавязчивое ознакомление с уникальными характеристиками метода, через отраслевые СМИ вызывает у такого рода потребителей высокий уровень доверия, что положительно влияет на осознание потребности в данных услугах.

ПРИЛОЖЕНИЕ 2. АНКЕТА ДЛЯ ПРОВЕДЕНИЯ ИНТЕРЬВЬЮ ВЛАДЕЛЬЦА ПРЕДПРИЯТИЯ (ПОЛЕЗНА ДЛЯ ПРЕДВАРИТЕЛЬНОЙ ОЦЕНКИ СИТУАЦИИ ПРИ ПОСТАНОВКЕ ПРЕДПРИЯТИЯ НА АБОНЕНТСКОЕ ОБСЛУЖИВАНИЕ)

ОБЯЗАТЕЛЬНЫЕ ВОПРОСЫ К РЕСПОНДЕНТУ

1. **Сколько человек работает на предприятии?**

- ❑ менее 100
- ❑ от 100 до 300
- ❑ от 300 до 500
- ❑ от 500 до 1000
- ❑ более 1000

2. Предпринимает ли компания какие-либо меры по борьбе с воровством на рабочих местах? Если «да», то какие?

_____

3. Используются ли на предприятии какие-либо системы, помогающие предотвратить хищения продукции?

- ❑ Видеонаблюдение
- ❑ Контроль доступа
- ❑ Металлодетекторы
- ❑ Личный досмотр
- ❑ Детекторы лжи
- ❑ Анализ голосовых вибраций
- ❑ Сигнализация
- ❑ Не используются

4. Существует ли на предприятии собственная служба безопасности?

_____

5. Важно ли для предприятия определять кражи продукции по факту их совершения?

- ❑ Очень важно
- ❑ Важно
- ❑ Совсем не важно

6. Важно ли для предприятия предотвращать кражи продукции на этапе появления умысла у сотрудника?

- ❑ Очень важно
- ❑ Важно
- ❑ Совсем не важно

7. Приблизительный ущерб предприятия от хищений продукции сотрудниками в месяц?

- ❑ до 50 тыс. грн.
- ❑ от 50 до 100 тыс. грн.
- ❑ Другая сумма _____
- ❑ от 100 до 200 тыс. грн.
- ❑ более 200 тыс. грн.

8. **Кто на предприятии принимает решение о выборе той или иной системы предотвращения хищений продукции?**

- ❑ Учредитель / владелец бизнеса
- ❑ Генеральный директор
- ❑ Коммерческий директор
- ❑ Финансовый директор
- ❑ Директор по персоналу
- ❑ Начальник службы безопасности
- ❑ Другой сотрудник

  _____

9. Какой информации о способах борьбы с кражами на предприятиях доверяет руководство?(1 – не важно, 5 – очень важно)?

	Характеристика	*1*	*2*	*3*	*4*	*5*
1	Мнение знакомых и коллег					
2	Опыт компаний, использующих подобные продукты					
3	Рекомендации известных людей					
4	Статьи в узкоспециализированной прессе					
5	Статьи в деловой прессе					
6	Информация в Интернет					
7	Информация на выставках и конференциях					
8	Другие источники *(какие именно?)* _____					

10. **Сфера деятельности компании?**

- ❑ Производство ювелирных изделий
- ❑ Парфюмерная промышленность
- ❑ Химическая промышленность
- ❑ Фармацевтическая промышленность
- ❑ Производство и дистрибуция алкоголя
- ❑ Гражданская авиация
- ❑ Свой ответ _____

ДОПОЛНИТЕЛЬНЫЕ ВОПРОСЫ

11. Случаются ли на предприятии случаи хищения производимой продукции?

- ❑ Да
- ❑ Нет
- ❑ Не знаю

12. Что руководителю дает основание быть на 100% уверенным в отсутствии хищений?

_____

_____

13. Каким образом у Вас на предприятии регистрируются кражи, выявляются хищения и недостачи?

_____

_____

14. Как на предприятии организована служба безопасности?

- ❑ Количество человек
- ❑ Возраст
- ❑ Зарплата
- ❑ Подготовка (образование, навыки, сертификаты, обучение)
- ❑ Техническое оснащение СБ

15. Насколько существующая СБ эффективна? Каким образом оценивается эффективность?

_____

_____

16. Какие системы, помогающие предотвратить хищения продукции, используются ли на предприятии?

- ❑ Производитель
- ❑ Модификация/модель
- ❑ Год выпуска
- ❑ Стоимость установки
- ❑ Стоимость обслуживания в месяц
- ❑ Сколько человек обслуживают эти системы
- ❑ Зарплаты этих сотрудников

17. Являются ли эти системы частью службы безопасности (в случае, если она организована)?

18. Есть ли у предприятия складские помещения, где хранится товар?

- ❑ Нет
- ❑ Сколько сотрудников обслуживают складские помещения?
- ❑ Зарплаты этих сотрудников?
- ❑ Затраты на аренду и обслуживание складских помещений в месяц?