ISSN 2225-4447

Учебно-методический журнал

№ 1(1) 2011

КУРСЫ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ

Электронный журнал издается с 2011 г.

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ:
МЕЖРЕГИОНАЛЬНАЯ
АКАДЕМИЯ БЕЗОПАСНОСТИ И ВЫЖИВАНИЯ

АДРЕС РЕДАКЦИИ:
Россия, 302020, г. Орел, Наугорское ш., д.5 «А»,
Тел. +7-910-300-12-42,
Официальный сайт: www.mabiv.ru,
E-mail: mabiv@mail.ru

Федеральная служба
по надзору в сфере связи, информационных технологий и массовых коммуникаций
(Роскомнадзор)

СВИДЕТЕЛЬСТВО

О РЕГИСТРАЦИИ СРЕДСТВА МАССОВОЙ ИНФОРМАЦИИ

Эл № ФС77-44650 от 15 апреля 2011 г.

Название: Курсы дистанционного образования

Адрес редакции: 302020, г. Орел, Наугорское шоссе, д. 5а

Примерная тематика и (или) специализация: Культурно-просветительская, образовательная, научная

Форма периодического распространения: электронное периодическое издание

Язык(и): русский, английский

Территория распространения: Российская Федерация, зарубежные страны

Учредитель (соучредители): Межрегиональная общественная организация "Академия безопасности и выживания" (302020, г. Орел, Наугорское шоссе, д. 5а)

Заместитель руководителя К.В. Протопопов

Начальник Управления разрешительной работы в сфере массовых коммуникаций М.Ю. Ксензов

Настоящее свидетельство выдано в соответствии с Законом Российской Федерации от 27 декабря 1991 года № 2124-1 "О средствах массовой информации".
Нарушение законодательства Российской Федерации о средствах массовой информации влечет ответственность в соответствии с законодательством Российской Федерации.

022519

ОБЩИЕ СВЕДЕНИЯ
ОБ ЭЛЕКТРОННОМ ЖУРНАЛЕ «КДО»

1. Электронный журнал «КДО» является общедоступным – бесплатным и открытым для неограниченного числа пользователей. Доступ поддерживается в любое время через лицензированного провайдера, стандартный браузер и протокол, используемый большинством пользователей сети Интернет.

2. Электронный журнал «КДО» является:

а) самостоятельным электронным изданием;

б) по природе основной информации: мультимедийным электронным изданием, содержащим текстовую информацию, видео, аудио файлы, флэш-анимацию и иные цифровые форматы передачи информации;

в) по целевому назначению (в соответствии с ГОСТ 7.60-90):

- научным электронным изданием, содержащим сведения о теоретических и (или) экспериментальных исследованиях, научно подготовленные к публикации памятники культуры, исторические и информационные документы;

- учебным электронным изданием, содержащим систематизированные сведения научного или прикладного характера, изложенные в форме, удобной для изучения и преподавания, и рассчитанное на учащихся разного возраста и ступени обучения;

- справочным электронным изданием, содержащим краткие сведения научного и прикладного характера, расположенные в порядке, удобном для их быстрого отыскания;

г) по технологии распространения: электронным изданием комбинированного распространения, которое может использоваться как в качестве электронного издания (доступного потенциально неограниченному кругу пользователей через телекоммуникационные сети), так и в качестве электронного издания, предназначенного для локального использования материалов на переносимых машинопечатных носителях;

д) по характеру взаимодействия пользователя и электронного издания: детерминированным электронным изданием, параметры, содержание и способ взаимодействия с которым определены издателем журнала и не могут быть изменены пользователем;

е) по периодичности и структуре: периодическим сериальным изданием.

3. Электронный журнал «КДО» размещается на информационном сервере МАБИВ и имеет электронный адрес: http://mabiv.ru. Допускается возможность размещения электронных ссылок (указателей) на электронный журнал «КДО» на разных информационных серверах научных учреждений и других организаций по предварительному согласованию.

ДЛЯ АВТОРОВ

1. Электронный журнал «КДО» предлагает молодым ученым, аспирантам, студентам, учителям, специалистам публиковать собственные научные, учебные, методические труды, отражающие основные результаты своей работы. Рассматриваются: материалы научных исследований, учебные пособия, лекции, методические разработки, теоретические статьи, обучающие курсы, практические рекомендации.

2. Тематическая структура электронного журнала «КДО» определяется его редколлегией. Журнал «КДО» включает в себя публикации новейших концепций, методик и технологий в области психологии, педагогики, экономической и личной безопасности, туризма, информационных технологий, менеджмента, маркетинга, права и др. **Публикация в электронном журнале «КДО» бесплатна для авторов.**

3. В публикуемых в электронном журнале «КДО» материалах не должно быть научной и технической информации, содержащей сведения, относящиеся к государственной, служебной или коммерческой тайне. Каждый выпуск журнала «КДО» (или совокупность входящих в него статей) должен проходить экспертизу, подтверждающую возможность его открытой публикации.

4. Электронный журнал «КДО» имеет редколлегию, члены которой представляют отрасли знания, отраженные в электронном журнал «КДО», и имеют ученые степени докторов и кандидатов соответствующих отраслей науки.

5. Порядок публикации в электронном журнале «КДО» предусматривает обязательное рецензирование. В качестве рецензента может выступать, как минимум, один специалист, имеющий ученую степень по специальности соответствующей статьи. Публикации в электронном журнале «КДО» подлежат только оригинальные статьи, ранее не публиковавшиеся в других изданиях.

6. Авторы научных работ и диссертаций могут давать ссылки на научные работы, опубликованные в электронном журнале «КДО», при этом библиографические описания публикация оформляются в соответствии с Межгосударственным стандартом 7.82 -2001 «Библиографическая запись. Библиографическое описание электронных ресурсов».

7. Материалы, содержащиеся в электронных ресурсах локального и удаленного доступа электронного журнала «КДО», считаются опубликованными и являются объектами авторского права.

ТРЕБОВАНИЯ
К ОФОРМЛЕНИЮ МАТЕРИАЛА ДЛЯ ПУБЛИКАЦИИ В «КДО»

1. В редакцию рукопись может быть представлена в электронном виде: на электронном носителе (компакт-диск (CD, DVD), флэш-накопитель) или в виде электронного файла, присланного на адрес редакции: **mabiv@mail.ru.**

2. **Текстовая часть** рукописи, включая формулы, таблицы и иллюстрации, должна быть подготовлена в текстовых редакторах Microsoft Word (не позднее версии 2003) (формат документа *.doc), OpenOffice.Org (формат документа *.odt). Все объекты должны располагаться в пределах границ страницы. Объем рукописи не менее 20 полных страниц формата А4.

3. Текст оформляется в стандартном формате А4 (размер 210297 мм), ориентация книжная, через один интервал 14 кеглем, шрифт Times New Roman. Размер левого поля – 20 мм, правого – 20 мм, верхнего и нижнего – по 20 мм. Абзацные отступы должны быть одинаковыми по всему тексту – 1,25, колонтитулы – 1,25. Текст должен быть выровнен по ширине и без расстановки переносов слов. Нумерация страниц сквозная.

4. Текстовая часть не должна содержать двойных и лишних пробелов, должны быть исключены пробелы перед знаками препинания. Нумерация и маркеры списков должны быть выполнены в ручном режиме с ввода клавиатуры, а не в автоматическом режиме.

5. Иллюстрации (чертежи, схемы, графики, диаграммы, рисунки) имеют одно название – рисунок. Все рисунки должны быть пронумерованы и снабжены подрисуночными надписями.

6. В рукописи необходимо делать ссылки на таблицы, рисунки и литературные источники, приведенные в материалах.

7. Таблицы должны иметь нумерационные или тематические заголовки, однако, во всей рукописи должно быть соблюдено единообразие. Таблицы имеют сквозную нумерацию (глава, порядковый номер), пример: Табл. 1.5. Если в статье один рисунок или одна таблица, они не нумеруются. Если таблица большая, ее необходимо поместить на отдельной странице. Ширина таблицы не должна быть больше полосы набора текста.

8. Рисунки, графики, схемы должны предоставляться в виде отдельных файлов в исходном графическом формате (tiff, jpeg). Все рисунки должны быть пронумерованы и иметь подрисуночные подписи.

9. Библиографическое описание источников регламентировано ГОСТ 7.1-2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления». Литературные источники, приводимые в списках, должны иметь порядковую нумерацию и располагаться в алфавитном порядке.

10. При подготовке объектов мультимедиа необходимо учитывать следующие требования.

Аудиоматериалы должны быть представлены в виде отдельных файлов формата *.mp3. Оптимальные параметры кодирования mp3: битрейт от 64 кбит/с (для голосовых сообщений) до 256 кбит/с (для иных насыщенных звуками материалов), частота дискретизации от 22,05 до 44,10 кГц.

Видеоматериалы должны быть представлены в виде отдельных файлов. Возможны следующие форматы (контейнеры): AVI, MP4, MOV, WMV. Набор видеокодеков: MPEG-4 ASP (Xvid, DivX), MPEG-4 AVC (H.264). Размер кадра 720x576 (лучше 640x480), частота кадров 24 кадра/с. Оптимальный битрейт для видео от 1500 до 2000 кбит/с. Аудиодорожку следует кодировать кодеком MP3 (битрейт от 64 до 256 кбит/с) или AAC.

Flash-анимация передается для публикации как файл формата SWF, размер кадра 640x480, частота кадров 12 кадров/с, шрифты должны быть встроены в публикацию, не допускается использование так называемых «стандартных» шрифтов (_serif, _sans, _typewriter). Flash-ролик должен поддерживать режим масштабирования как на увеличение, так и на уменьшение размеров с сохранением пропорций изображения. Также целесообразно передавать исходный файл Flash-ролика в формате FLA.

11. Материалы, не отвечающие перечисленным требованиям, возвращаются авторам для доработки.

ПОРЯДОК РЕЦЕНЗИРОВАНИЯ РУКОПИСЕЙ МАТЕРИАЛОВ

1. Каждая поступившая рукопись рассматривается редакцией. Если она не соответствует минимальным требованиям (тематике, научному уровню, наличию научных результатов и оформлению), то автору направляется мотивированный отказ. В противном случае рукопись рецензируется. Рецензент выбирается в соответствии с рекомендацией члена Редколлегии, компетентного в области знаний, к которой относится содержание рассматриваемой рукописи.

При необходимости рукопись направляется двум рецензентам (например, когда ее тема находится на стыке различных научных дисциплин).

2. Если в полученной рецензии имеются замечания или она отрицательна, то автору рекомендуется доработать рукопись и учесть эти замечания или, соответственно, ему направляется мотивированный отказ, к которому прилагается рецензия.

3. Если рецензия положительна и не содержит замечаний, то рукопись направляется на заключение члену редколлегии. При положительном заключении он представляет рукопись к публикации, после чего она рассматривается Редколлегией, которая принимает решение о ее публикации или отклонении. При отрицательном заключении или отклонении рукописи Редколлегией автору направляется мотивированный отказ. При публикации статьи указываются фамилия и инициалы члена редколлегии.

4. Доработанный вариант направляется рецензенту на повторное рецензирование.

СОДЕРЖАНИЕ

А.В. Артёмов

кандидат технических наук, доцент кафедры
«Электроника, вычислительная техника и
информационная безопасность»
ФГБОУ ВПО «Госуниверситет – УНПК»

ПОИСК ИНФОРМАЦИИ В ИНТЕРНЕТЕ

(курс лекций)

МАБИВ
АКАДЕМИЯ

СОДЕРЖАНИЕ

ЛЕКЦИЯ 1.
ПРИНЦИПЫ ОРГАНИЗАЦИИ И ПОИСКА ИНФОРМАЦИИ В ИНТЕРНЕТЕ

Поиск информации в Интернете проводится двумя основными способами – с помощью каталогов (их еще называют директориями) и с помощью поисковых машин.

Директории обеспечивают контекстный поиск для структурированного просмотра, тогда как поисковые машины, как следует из их названия, контекста не обеспечивают, однако позволяют находить конкретные слова или фразы. Директории можно уподобить оглавлению книги, а поисковые машины – предметному указателю.

Часто поисковые системы объединяют в себе как поисковую машину, так и директории. Это хорошо видно на примере первой страницы Яндекса, где под поисковой строкой размещается список директорий, которые позволяют пользователю уточнять запрос по мере продвижения в глубь каждой из них.

Ввиду того, что принцип организации директорий понятен каждому, кто пользовался библиотечным каталогом – а среди читателей таких, смеем полагать, подавляющее большинство, – мы не будем подробно останавливаться на технике работы с директориями и уделим больше внимания работе с поисковыми машинами. В завершении же разговора о каталогах приведем пример «цепочки», по которой осуществляется поиск каталоге Яндекса: Бизнес > Реклама > Реклама в Интернете.

Все поисковые машины работают по одному и тому же алгоритму и основаны на одних тех же принципах. Различия между ними возникают лишь на уровне технической реализации этих принципов в работе.

Чтобы понять принцип работы поисковой машины, попробуем разделить вопрос на две части: на чем основан поиск и как он реализован.

На чем основан поиск Все поисковые машины базируются на трех основных операторах, лежащих в основе Булевой алгебры (ее также называют Булевой логикой или Boolean). Это логические операторы «И», «ИЛИ» и «НЕ». Работают они следующим образом.

1. Логическое «И». Если между двумя словами в запросе стоит оператор «И», то в результате поиска будут найдены лишь те документы, в которых содержатся оба слова. Так, например, по запросу собака И кошка будет найден документ, содержащий предложение «собака гналась за кошкой», документов же, состоящих из текста «кошка отдыхала» или «корм для собак», мы не увидим.

2. Логическое «ИЛИ». Если между словами стоит оператор «ИЛИ», то результатом поиска станут документы, в которых содержится хотя бы одно из этих слов. Если мы не сделаем специальных ограничительных оговорок, то материалы, в которых оба эти слова присутствуют, также будут найдены.

По запросу собака ИЛИ кошка мы получим документы, исключенные в прошлом запросе и содержащие текст «кошка отдыхала» или «корм для собак», а также материал с предложением «собака гналась за кошкой».

3. Логическое «НЕ». Если два предыдущих оператора описывали те слова, которые вы хотите включить в запрос, то оператор «НЕ» слова из запроса исключает. Пользователи, впервые сталкивающиеся с операторами запросов, нередко высказывают удивление: мол, не проще ли и вовсе не включать ненужное слово в запрос? Зачем вводить дополнительный оператор? Увы, нет. Не проще. На самом деле, чтобы понять важность логического оператора «НЕ», имеет смысл вспомнить, что наш запрос не создает в Интернете ничего нового. Мы лишь выуживаем то, что нам нужно, из имеющегося огромного, но все же конечного массива. При этом необходимо отсечь информационный мусор. Его-то мы и отсекаем с помощью оператора «НЕ». К сожалению, не нам решать, увидим ли мы этот мусор в выдаче. Так, например, по запросу сведений о коньке крыши неизменно появляется информационный мусор в виде документов о Коньке-Горбунке, фигурном катании, хоккее, лошадях и т. п. Без логического «НЕ» тут никак не обойтись.

Давайте рассмотрим примеры работы логического оператора «НЕ».

По запросу собака НЕ кошка будет найден документ, содержащий текст «корм для собак», а вот документы со словами «кошка отдыхала» или «собака гналась за кошкой», и даже «корма для собак и кошек» из выдачи будут исключены.

Часто встречается чуть более сложный вариант написания запроса, который содержит все или почти все вышеперечисленные операторы. В этом случае лучше пользоваться таким элементом, как круглые скобки. Скобки позволяют отделять однотипные слова запроса от остальных. Кроме того, самому составителю при этом визуально гораздо удобнее различать отдельные фрагменты запроса. Мы не будем чересчур теоретизировать о скобках, а просто продемонстрируем работу указанного элемента на конкретных примерах. На наш взгляд, так будет понятнее, как и для чего используются скобки. Так, запрос пушистые И (собаки ИЛИ кошки) позволит получить документы, относящиеся как к пушистым собакам, так и к пушистым кошкам – по отдельности или вместе. Скобки при этом «раскрываются» по обычным арифметическим правилам вынесения за скобку общего множителя (для тех, кто не любит математику, поспешим сказать, что болеше углубляться в нее мы не будем). А вот запрос пушистые И (собаки ИЛИ кошки) НЕ (собаки И кошки) выдаст документы, в которых написано про пушистых собак или пушистых кошек, но не будет содержать текстов, где одновременно будут упомянуты и кошки, и собаки.

Еще раз повторимся, все поисковые машины сегодня работают на основе анализа этих трех операторов, хотя нюансы их написания в разных поисковых машинах могут отличаться.

Как поиск реализован. Каждая полноценная поисковая машина располагает собственным штатом роботов, или пауков. Их еще называют краулерами (crawlers) и спайдерами (spiders,). Это программы, которые перескакивают со страницы на страницу и сканируют находящиеся на них тексты, не вникая при этом в их содержание. После чего сбрасывают документы на серверы своих хозяев и идут к следующим страницам. Как паук определяет, куда ему пойти? Он находит так называемую гиперссылку (ту самую, при наведении на которую курсор приобретает вид раскрытой ладони, и при клике по которой происходит переход на другую страницу) и идет по ней. Вот почему, если на страницу не ведет ни одна ссылка, паук на нее тоже не придет. Исключение составляет ситуация, когда владелец страницы вручную сообщит о ней поисковой машине, заполнив специальную форму на сайте поисковой машины. На сервере поисковой машины текст разбивается на отдельные слова, каждому из которых присваиваются координаты, после чего они заносятся в таблицу сервера вместе со ссылкой на тот адрес в Интернете, по которому текст размещался в момент посещения его пауком.

Сам по себе поисковик представляет собой большую локальную сеть, состоящую из мощных компьютеров с огромным объемом дисковой памяти. Эти машины разделены на подгруппы (так называемые кластеры), между которыми распределяется информация, собранная пауками.

Когда поисковая система получает запрос, она ищет ответ именно в своей таблице, а не в Интернете. При этом важно понять, как паук решает, с какой частотой ему следует посещать ту или иную страницу. Выглядит этот алгоритм приблизительно следующим образом. Поработав со страницей, паук возвращается на нее, ну, например, через две недели. И если видит, что никаких изменений не произошло, он планирует следующее посещение через более длительный период – скажем, через месяц. А если и тогда не обнаружит ничего нового, то наведается сюда еще позже, месяца через полтора-два. Вот почему нередко бывает так, что поисковая машина по запросу результат выдает, а попытка перейти на страницу по полученной ссылке безрезультатна – вероятнее всего, никакой страницы уже просто не существует на прежнем месте, но паук на нее давно не заходил, и, соответственно, поисковая система о ее удалении не знает. Весь комплекс процессов, описанных выше, называется индексацией.

История развития поисковых машин. История эволюции поисковых машин наиболее полно, на наш взгляд, представлена в книге признанных экспертов в области невидимого интернета Криса Шермана и Гарри Прайса «Невидимый Интернет».

До середины 1960-х годов компьютеров было немного. Изолированные друг от друга, они не могли обмениваться информацией. В 1962 г. профессор Ликлайдер (Licklider) из ведущего технического вуза США – Массачусетского Технологического института – сформулировал концепцию глобальной компьютерной сети «Galactic Network». Идея начала воплощаться в жизнь сотрудником американского министерства обороны Ларри Робертсом (Larry Robberts), который через четыре года после публикации статьи профессора предложил объединить отдельные компьютеры министерства в сеть, описанную Ликлайдером. Таковы предпосылки возникновения сети «ARPANET», которая затем превратилась в то, что сегодня величают Интернетом. Первый узел «ARPANET» появился в 1969 г., и следующие несколько лет к нему подключались университеты и различные контрагенты, работавшие по заказам военного ведомства США.

В 1973 г. американское министерство обороны инициировало новую программу, предполагавшую обеспечивать надежную связь компьютеров между собой с помощью очень большого числа различных соединений. Целью такого решения было повышение устойчивости системы к попыткам массированно нарушить электронные средства коммуникации. Поскольку все это происходило во времена «холодной войны», речь шла об устойчивости к устрашающим последствиям, которыми грозило стратегическое ядерное противостояние. Поскольку «ARPANET» представлял собой одну-единственную сеть, что на системном уровне понижало его способность сопротивляться разрушениям, возникла идея создания «сети из сетей», которая теоретически могла бы быть бесконечно большой. Этот проект и назвали «Internetting», а саму сеть «Internet». По мере того, как количество присоединенных к Интернету машин увеличивалось, объективно назрел вопрос о необходимости инструментов, позволяющих легко находить текст и другие файлы на удаленном компьютере, в идеале – на любом, где бы он ни располагался в Сети.

Доступ к файлам на самых ранних этапах развития Интернета осуществлялся в два этапа, каждый из которых выполнялся вручную: специальные команды вводились с клавиатуры. Кстати, тогда компьютеры могли управляться лишь специалистами, способными вводить команды в соответствующую строку. Графического интерфейса, позволяющего комфортно работать с машиной неподготовленному человеку, еще не изобрели. Так вот первым делом с помощью программы Telnet устанавливалось прямое соединение с компьютером, на котором находится нужный файл. На данном этапе лишь налаживалась связь, ничего и никуда в этот момент еще не передавалось. И только затем с помощью специальной программы – FTP – можно было этот конкретный файл взять. Очевидно, что на поиски нужного документа уходила масса времени: требовалось знать точный адрес компьютера, на котором он находится. Между тем файлов становилось все больше, интерес к ним постоянно рос, и для того, чтобы найти адрес одного из них, обычно приходилось обращаться в дискуссионные группы с просьбой о помощи и в надежде на то, что кто-нибудь из собеседников подскажет заветный адрес, по которому хранится нужная информация.

В результате, стали появляться специальные FTP-серверы, которые представляли собой хранилище файлов, организованных в директории, по принципу хранения информации на персональном компьютере. Такие серверы существуют и по сей день. Первый работоспособный, общедоступный инструмент поиска файлов, хранящихся на FTP-серверах, назывался «Арчи» (Archie) и был создан в 1990 г. группой системных администраторов и студентов старших курсов Университета Мак Джил (McGill) в Монреале. «Арчи» был прототипом сегодняшних поисковых машин, но значительно болеепримитивным и ограниченным в своих возможностях. Он бродил по Интернету, разыскивал файлы на разных FTP-серверах и загружал список директорий каждого найденного сервера на собственный, формируя общий каталог.

Этот каталог затем обрабатывался и хранился в центральной базе данных, внутри которой можно было организовать поиск. Поиск на собственном компьютере к тому моменту существовал уже издавна и, несмотря на то, что тоже требовал ввода команд, трудностей в работе не создавал. Однако без специальной подготовки использовать компьютер полноценно человек не мог. База данных находилась в университете Мак Джилл и обновлялась ежемесячно. В 1991 г. команда Марка Мак Кахилла (Mark McCahill) из Университета Миннесоты создала программу «Голден Гофер» (Golden Gopher – в переводе с английского «золотоискатель» или «старатель»), которая совмещала в себе оба протокола – Telnet и FTP. Все, что нужно было сделать пользователю для получения доступа к нужной информации, – щелкнуть по гиперссылке, приведенной в меню. Таким образом, впервые в истории вводить какие-либо команды уже не требовалось, так что отныне по ресурсам Интернета люди могли «бродить» и без специальной подготовки.

Программа показывала пользователю последовательно возникающие пошаговые меню, что позволяло ему без проблем идти в глубь базы директорий, все более приближаясь к специфическим документам, которые и составляли цель поиска. Этот алгоритм, по сути, сохранен и сегодня в Каталогах, расположенных в Интернете. Стало возможно получать как текстовые документы, так и графические, и музыкальные, без привязки к какому-то определенному формату. А самое главное, стало в принципе возможно легко найти и получить в Интернете нужную информацию.

Однако проблемы все же оставались. Одна из них, и довольно серьезная, была связана с тем, что компьютеры были построены на разных платформах, которые порой не понимали друг друга. Тут можно провести аналогию с людьми, которые говорят на совершенно разных языках и потому не могут построить более или менее осмысленную беседу. В те времена между собой конкурировали не операционные системы, как сейчас, а производители компьютерного «железа». Сегодня в меньшей степени важно, кто произвел компьютер. Гораздо существеннее, что на нем установлено: Windows, Linux, Mac OS или какая-то другая система. А тогда именно производители «железа» определяли лицо Интернета.

Объективно назревала идея, согласно которой компьютеры разных платформ должны иметь возможность работать в одном протоколе, позволяющем просматривать страницы вне зависимости от того, на какой конкретно машине эти страницы созданы. Требовалось придумать такой универсальный протокол и сделать его удобным для пользователей.

Первым, кто догадался объединить известную к тому времени простую форму гипертекста с универсальными коммуникационными протоколами, был Тим Бернерс-Ли (Tim Berners-Lee).

Чтобы пользователь получил в руки независимый от платформы и при этом простой инструмент, Бернерс-Ли создал HTML (HyperText Markup Language, то есть Язык гипертекстовой разметки). Все Web-документы, отформатированные с помощью тегов HTML, видны совершенно одинаково во всем мире, вне зависимости от типа компьютера, на котором человек открыл страницу сайта. Поэтому и сегодня при переводе файла в формат HTML, например, на машине, работающей под управлением операционной системы MacOS, можно быть уверенным в том, что этот файл будет выглядеть точно так же и на компьютере, работающем под управлением Windows. Затем Бернерс-Ли придумал Universal Resource Identifier – метод стандартизации адресов, при котором компьютерам в Интернете присваиваются уникальные адреса (сегодня мы их называем URL, это то, что в привычном для пользователя виде обычно начинается с «www»). Наконец, изобретатель собрал вместе все эти элементы, создав систему в форме Web-серверов, которые хранят HTML - документы и предоставляют их другим компьютерам, создавая HTML-запросы о документах по определенным URL. Но Бернерс-Ли хотел видеть Интернет как информационное пространство, в котором можно получить свободный доступ к данным любых типов. На ранних этапах развития глобальной Сети преобладали простые текстовые документы HTML.

К тому времени существовали системы поиска информации на локальных машинах, поэтому появилось несколько серверов, которые пытались проиндексировать какую-то часть страниц Web и прежде, чем отправляться за чем-то в Интернет, предлагали поискать необходимые сведения на этих серверах. При этом основная проблема заключалась в том, чтобы отыскать страницы, которые в принципе можно бы было индексировать. Поскольку Интернет лишен централизованной структуры и общего оглавления, единственный способ, позволявший добиться этого, состоял в поиске ссылки на страницу и переходе по этой ссылке, с последующим добавлением найденного ресурса к индексу.

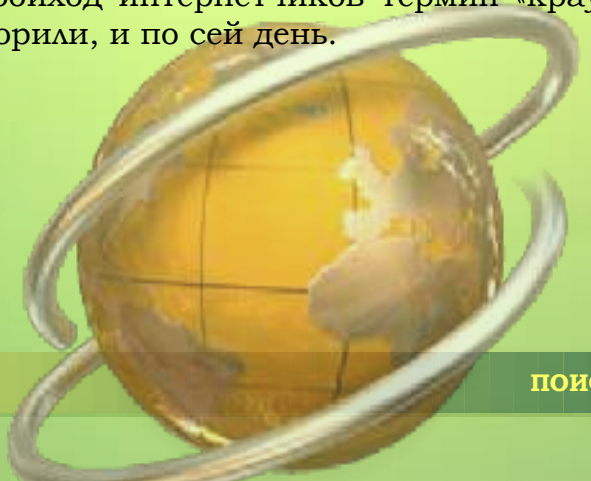
Однако вскоре возникла еще одна проблема. Наиболее популярные страницы посещались пауками чаще остальных, так как на них указывало максимальное количество ссылок.

Пауки, количество и возможности которых были ограничены, «зависали» на таких страницах и впустую расходовали ресурсы, оставляя непосещенным множество других адресов, пока еще менее популярных. Для решения этой проблемы требовалось создать программу, которая позволила бы игнорировать уже проиндексированные страницы и сосредоточиться на поиске новых. Иначе это грозило проблемой с ресурсами.

В 1993 г. студент-физик Массачусетского технологического института Мэтью Грей (Mathew Gray) создал первый широко известный Web-робот, названный «World Wide WebWanderer» или просто «Вандерер», что в переводе с английского означает «скиталец» или «странник». Дело в том, что Грей заинтересовался статистикой. Результатом такого увлечения стало появление «странника»: изобретение было призвано помочь студенту проанализировать размеры Интернета и скорость его роста. «Вандерер» просто приходил на страницу и определял сам факт ее существования, не занося в базу содержимого найденного адреса. Несмотря на то, что создатель робота не преследовал никаких других целей, его детище, фактически дебютировавшее в «забеге» прогрессивных интернет-находок, легло в основу более сложных программ, которые к умению «скитальца» перемещаться по Сети добавили способность сохранять содержимое страниц в базе данных после их посещения.

Случилось так, что 1994 г. стал переломным в истории создания поисковых машин. Студент выпускного курса Вашингтонского университета Брайан Пинкертон (Brian Pinkerton) устал от бесконечной череды электронных писем, которые посылали ему друзья, с информацией о хороших сайтах, найденных ими в Интернете. Безусловно, сайты ему были нужны, однако шквал посланий с их адресами раздражал, а посещение всех страниц отнимало уйму времени. Однако Пинкертон нашел решение проблемы – он создал робота, которого назвал WebCrawler (что-то вроде «вездеход для Интернета»). «ВебКраулер», как и «Вандерер», ползал со страницы на страницу, запоминая при этом весь текст Web-документа и сохраняя его в базе данных, которая была доступна поисковым словам. Изобретатель представил свое детище публике в апреле 1994 г., причем сделал это виртуально – через Web-интерфейс. База данных в тот момент содержала информацию с 6000 самых разных серверов. Уже через неделю она начала расширяться, причем ежедневный прирост составлял более 100 новых серверов. Так родилась первая поисковая машина.

Тогда же был введен в обиход интернетчиков термин «краулер» или «паук», который применяется, как мы уже говорили, и по сей день.



Ну а далее ситуация развивалась еще более стремительно. Крис Шерман и Гари Прайс приводят такую хронологию возникновения и развития современных поисковых машин.

1994 г. – WebCrawler, Lycos, Yahoo!
1995 г. – Infoseek, SavvySearch, AltaVista, MetCrawler, Excite. Появление метапоисковых машин.
1996 г. – HotBot, LookSmart.
1997 г. – NorthernLight.
1998 г. – Google, InvisibleWeb.com.
1999 г. – FAST.
2000 г. и далее – Сотни новых поисковых машин.

Русскоязычные поисковые машины появлялись в такой последовательности:

1996 г. – Rambler (www.rambler.ru);
1997 г. – Yandex (www.yandex.ru);
2004 г. – русскоязычная версия Google (www.google.ru) и русскоязычная версия Yahoo! (http://ru.yahoo.com).

Из чего состоит сайт Прежде, чем перейти к описанию языка запросов поисковых машин, рассмотрим, из каких элементов, с которыми предстоит работать пауку, состоит обычно сайт. Надо сказать, что язык HTML достаточно прост и логичен. Он представляет собой способ разбивки текста с помощью специальных элементов – тегов, которые определяют структуру и внешний вид текста при просмотре его в браузере. О тегах следует знать, что они всегда парные и что они бывают открывающими (обозначают начало определенного форматирования) и закрывающими (обозначают его окончание). Закрывающий тег – такой же по написанию, как открывающий, но перед ним стоит косая черта. Приведем пример очень простого сайта (рисунок 1).

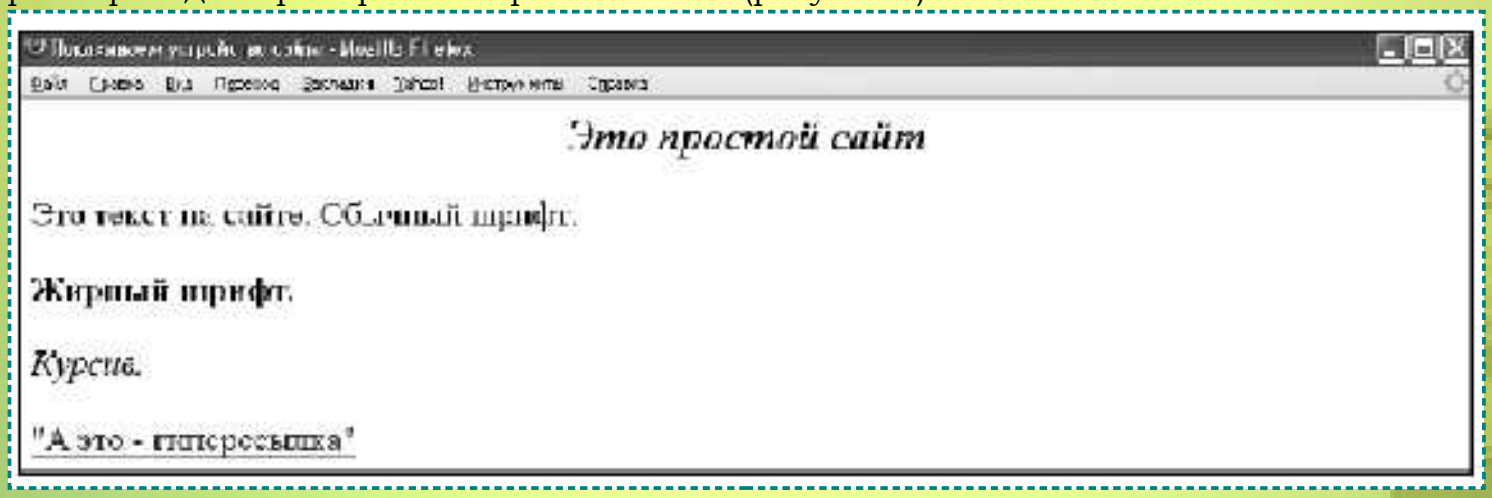


Рисунок 1 *– Пример сайта, как его видно в браузере Мозилла Файрфокс.*

Наверху страницы, изображенной на рисунке, то есть не в тексте сайта, а на верхнем поле рамки страницы, рядом с круглым значком браузера, расположена надпись: «Показываем устройство сайта». Она находится в так называемом заголовке страницы (который заключен между открывающим тегом <TITLE> и закрывающим тегом </TITLE>). Обращаем ваше внимание на то, что это заголовок именно всей страницы, а не текста. Посередине представленного рисунка жирным курсивом выведено: «Это простой сайт». Данная надпись – и есть заголовок текста. Шрифт фразы «Это простой сайт» по размеру

Наверху страницы, изображенной на рисунке, то есть не в тексте сайта, а на верхнем поле рамки страницы, рядом с круглым значком браузера, расположена надпись: «Показываем устройство сайта». Она находится в так называемом заголовке страницы (который заключен между открывающим тегом <TITLE> и закрывающим тегом </TITLE>). Обращаем ваше внимание на то, что это заголовок именно всей страницы, а не текста. …

... Посередине представленного рисунка жирным курсивом выведено: «Это простой сайт». Данная надпись – и есть заголовок текста. Шрифт фразы «Это простой сайт» по размеру превосходит шрифт текста на сайте, он специально выделен как заголовок текста. При разметке с помощью HTML этот текст расположен ниже тега <TITLE>, но при этом вместе с тегом <TITLE> находится внутри тега <Head>. То есть содержимое, заключенное в <TITLE>, – это часть того, что находится в <Head>. Такое расположение дает дополнительную возможность пауку лучше определять ключевые слова на сайте. Ведь если слова вынесены в заголовок текста или, тем более, всей страницы, вероятность того, что страница и текст посвящены теме, формулируемой этими словами, повышается. Ниже фразы «Это простой сайт» приведены четыре варианта написания основного текста сайта:

- обычный;
- жирный (пишется под тегом <B>);
- курсив (пишется под тегом <i>);
- текстовая гиперссылка (пишется под тегом <A HREF=http://www.url. ru>«Текст гиперссылки»</A>).

Основной текст сайта, вне зависимости от того, каким вариантом шрифта он написан, располагается внутри тега <BODY>. Именно содержимое тега <BODY> представляет собой основной объект для паука и рассматривается им как текст страницы (собственно, это действительно текст страницы).

Чтобы увидеть внутреннюю разметку сайта, надо в браузере Мозилла Файрфокс навести курсор на любой незанятый текстом участок поля и нажать правую кнопку мыши. В всплывающем меню следует выбрать пункт «Просмотр исходного кода страницы». Применительно к сайту, который мы рассматривали на рис. 1, этот исходный код будет выглядеть следующим образом:

```
<HTML>
<HEAD>
<TITLE>
Показываем устройство сайта:
</TITLE>
<CENTER>
<B><I>
<SPAN STYLE=«font-size: large»>Это
простой сайт</SPAN>
</CENTER>
</B></I>
</HEAD>
<BODY>
<P>
Это текст на сайте.
Обычный шрифт.
</P> <P> <B>
Жирный шрифт.
</B> </P> <P> <I>
Курсив.
</I> </P>
<A
HREF=http://www.url.ru>«A это
– гиперссылка»</A>
</BODY>
</HTML>
```

Здесь можно увидеть все элементы, описанные нами выше. Кроме того, в исходном коде видны теги <P>, которые обеспечивают расположение текста в новой строке и с промежутком по отношению к тексту, расположенному в предыдущей строке. Разметка HTML по умолчанию не предполагает переноса текста и его форматирования.

Поэтому текст, не содержащий никаких тегов, воспроизводится подряд, но с соблюдением пробелов между словами. Для того чтобы текст оказался написан не просто в новой строке, а с промежутком относительно находящейся выше строки, используется, как мы уже показали, тег <P>, а для того, чтобы текст был написан в новой строке, но без промежутка между выше– и нижерасположенной строками, применяется тег
.

Начало сайта, созданного с помощью разметки HTML, отмечено тегом <HTML>, а его окончание – тегом </HTML>.

ОПИСАНИЕ ЯЗЫКА ЗАПРОСОВ ПОИСКОВОЙ МАШИНЫ ЯНДЕКС

Яндекс

Лучшая, на наш взгляд, работа по изучению операторов поисковой машины Яндекс выполнена специалистом из Санкт-Петербурга Денисом Фурсовым. На его ресурсе постоянно проводятся дополнительные исследования, отслеживаются и оцениваются изменения в работе операторов указанной поисковой машины. Ниже речь пойдет о том, как с помощью специальных фильтров, основанных на Булевой алгебре, создавать запросы, максимально соответствующие потребностям специалиста, который ищет информацию в Интернете. При изучении этого вопроса, не следует забывать, что компьютер очень исполнителен, но лишен способности думать, поэтому следует составлять запрос, исходя из того, что он будет обработан компьютером буквально, а не с учетом того, что же на самом деле имел в виду пользователь, создавая свое обращение.

Итак, перейдем непосредственно к операторам запросов ***Яндекса.***

1. Логическое «И». Яндекс поддерживает три разных оператора, относящихся к логическому «И», что делает его самым гибким из всех поисковиков, работающих с русским языком. Столь развита практически уникальная система операторов поисковых запросов дает возможность предельно точно настроить запрос и сформировать такой фильтр для данных в Интернете который максимально качественно выбирает нужную информацию и отсекает ненужное.

1.1. *Пробел.* Слова, разделенные пробелом, должны располагаться недалеко друг от друга. Специалисты поясняют, что термин «недалеко» отнюдь не фиксированная величина именяется в зависимости от того, с какими словами указанный оператор в каждом конкретном случае используется. Если они часто употребляются, то «недалеко» – значит на расстоянии нескольких слов друг от друга. Если же они редко встречаются в обиходе, то даже их нахождение в разных концах документа будет восприниматься как «недалеко».

При этом, несмотря на то, что логическое «И» в общем виде Булевой алгебры подразумевает присутствие всех упомянутых слов, Яндекс, тем не менее, действительно выдает сначала те документы, в которых есть все ключевые слова, представленные в запросе. После чего начинает выдавать документы, в которых на одно ключевое слов меньше, чем в запросе, затем – на два слова меньше и так далее.

Запрос: [маркетинг менеджмент]
Результат поиска: страниц – 2 442 393, сайтов – не менее 1456
В выдаче: Маркетинг, Финансы, Реклама, Менеджмент

1.2. *Амперсанд* (&).
Слова, разделенные амперсандом, находятся в одном предложении. Важно: амперсанд должен быть отделен пробелами с двух сторон от любых других слов.
Запрос: [маркетинг & менеджмент]
Результат поиска: страниц – 1 190 379, сайтов – не менее 1093
В выдаче: … Филип Котлер в краткой форме представляет все наиболее значительные и интересные положения самой известной своей работы «Маркетинг менеджмент»…

1.3. *Двойной амперсанд* (&&). Слова, разделенные двойным амперсандом, находятся в любом месте одного и того же документа.
Важно: между амперсандами не должно быть пробелов, но сам оператор должен быть отделен пробелами с двух сторон от любых других слов.
Запрос: [маркетинг && менеджмент]
Результат поиска: страниц – 3 641 056, сайтов – не менее 1 295
В выдаче, к примеру, будут присутствовать учебные планы вузов, в которых слова «маркетинг» и «менеджмент» находятся в разных частях текста, в том числе – на разных страницах опубликованного в Интернете многостраничного плана занятий.

В выдаче, к примеру, будут присутствовать учебные планы вузов, в которых слова «маркетинг» и «менеджмент» находятся в разных частях текста, в том числе – на разных страницах опубликованного в Интернете многостраничного плана занятий.

Чтобы увидеть это наглядно, читатели могут нажать в результатах выдачи гиперссылку «Найденные слова», которая приводится во всех итогах поиска. И тогда слова, которые есть в запросе, будут подсвечены и не придется тратить время на их «отлавливание» в тексте.

2. Логическое «НЕ». Логическое «НЕ» представлено двумя операторами. Прежде чем рассказать о них, отвечу на вопрос, который часто возникает у людей, впервые приступивших к изучению операторов поиска: «Зачем нужно логическое „НЕ“? Его ведь можно и вовсе не вводить, и тогда оно нам не понадобится!». Отвечаем: если мы сами решаем, что нам вводить, а что нет, то это утверждение справедливо. Но проблема в том, что часто в выдаче принудительно оказывается «мусор» и другого способа избавиться от него, кроме как убрать эти слова при помощи логического «НЕ», у нас нет. Так, например, если вас интересует конек крыши, то по слову «конек» в выдаче окажется информация и о роликовых, и о фигурных коньках, и даже о Коньке-Горбунке. Для таких-то случаев логическое «НЕ» и придумано.

Итак, вернемся к нашим операторам.

2.1. *Тильда* (~). Знак тильды – это верхняя левая клавиша на буквенно-цифровой клавиатуре. Символ вводится на английском регистре с нажатой клавишей SHIFT. Как и амперсанд, тильда должна быть отделена пробелами с обеих сторон. Часто допускают ошибку, «приклеивая»тильду к следующему за ней слову. Иногда отсутствие пробела между тильдой и последующим словом не влияет на результат, но бывает и наоборот, поэтому лучше внимательно проследить за пробелами вокруг этого знака.

Тильда означает, по аналогии с диаметрально противоположным символом – амперсандом, что слова не должно быть в предложении.

Запрос: [`маркетинг ~ менеджмент`]

Результат поиска: страниц – 12 604 153, сайтов – не менее 4442

В выдаче: … комплексный подход к услуге интернет-маркетинга, охватывающий все возможности для продвижения интернет-представительств компаний в сети Интернет.

2.2. *Двойная тильда* (~~). По аналогии с двойным амперсандом, двойная тильда пишется слитно внутри самого этого оператора, но отделяется от остальных слов пробелами с обеих сторон. Она означает, что слова, которое за ней расположено, не должно быть в документе совсем.

Запрос: [`маркетинг ~~ менеджмент`]

Результат поиска: страниц – 9 675 995, сайтов – не менее 3 976

В выдаче: Форум по маркетингу и рекламе – Маркетинг и Реклама, маркетинговые коммуникации, виды рекламы: реклама в СМИ (печатная реклама, телереклама, радиореклама), наружная реклама, BTL: POS-материалы, У вас есть вопрос по маркетингу и рекламе?

Обратите внимание: в результатах выдачи слова «маркетинг» и «маркетингу» выделены как релевантные, «маркетинговые» же – нет. Это происходит потому, что термин «маркетинг» – существительное, а «маркетингу» – его словоформа, тогда как «маркетинговые» – совсем другая часть речи, а отнюдь не производное от слова «маркетинг». Подобное явление надо учитывать, если вы рассчитываете на способность Яндекса самостоятельно перебирать словоформы. Игнорирование этого факта нередко приводит к искажению результатов выдачи и также является частой ошибкой начинающих специалистов по поиску в Интернете. На самом деле, в Яндексе есть еще один оператор логического «НЕ», который обозначается знаком «минус».

По мнению Дениса Фурсова, с которым автор полностью согласен, _ «минус» – это не всегда корректно работающая двойная тильда, поэтому пользоваться им смысла нет. Мы не знаем наверняка, но предполагаем, что знак «минус» в качестве логического «НЕ» – это способ унифицировать Яндекс с другими поисковыми машинами, поскольку в большинстве своем они обозначают логическое «НЕ» именно этим знаком. Мы не пользуемся оператором «минус» при поиске в Яндексе.

3. Логическое «ИЛИ» (оператор |). Логическое «ИЛИ» представлено оператором, имеющим вид вертикальной черты |. На клавиатуре этот оператор находится обычно выше (реже он расположен ниже) клавиши Enter и вводится в английском регистре, при нажатой клавише SHIFT. В подавляющем большинстве случаев оператор | и слова, с которыми он используется, заключаются в скобки, так как чаще всего этот оператор относится сразу к двум и более словам.

Если мы хотим сделать запрос, который должен показать, что нас интересует документ, содержащий в одном предложении слова «маркетинг» и «менеджмент», но при этом нигде по тексту не должно быть слов «курс», «работа», «конференция», «теория», «книга», «семинар», «бизнес», «прибыль», «клиент», то сформулировать его необходимо следующим образом: [маркетинг & менеджмент ~~ (курс | работа | конференция | теория | книга | семинар | бизнес | прибыль | клиент)] Результат поиска: страниц – 46 082, сайтов – не менее 1483 В выдаче: Форумы на Sostav.ru / Доска объявлений / Продам Маркетинг Менеджмент Котлера Или: Ответы к госам по дисциплине Маркетинг – Менеджмент (по конспектам преподавателей СПбГУ) Обратите внимание, что скобки, как в арифметике при вынесении за скобку общего множителя, позволяют распространить действие оператора «двойная тильда» на все слова, расположенные внутри них. Кстати, для удобства восприятия этот запрос лучше оформить так, чтобы слова «маркетинг» и «менеджмент» были сгруппированы. Смысловой нагрузки это не несет, а потому и на выдачу не влияет, однако снижает вероятность того, что вы сами запутаетесь в своем запросе, если он будет достаточно длинным. Соответственно, мы бы советовали обратиться к поисковику так: [(маркетинг & менеджмент) ~~ (курс | работа | конференция | теория | книга | семинар | бизнес | прибыль | клиент)]

4. Яндекс учитывает морфологию слов. Это означает, что Яндекс по запросу «Учет» выдаст результаты, содержащие слова «Учету», «Учетом», «Учетов» и т. п., которые он выделяет как релевантные теме поиска. Запрос: [Учет] В выдаче: Последний день сдачи индивидуальных сведений персонифицированного учета истекает 1 марта 2006 года. Результат поиска: страниц – 23 287 782, сайтов – не менее 13 745 Запрос: [Учетом] ведение бухгалтерского учета поставщика, прежде всего учета реализации В выдаче: Учет русской морфологии Подсветка найденных...Yandex поисковая система с учетом морфологии русского языка Россия… Результат поиска: страниц – 23 675 161, сайтов – не менее 13 745

5. Можно отключить поддержание морфологии слов. Если слова с изменяющимися окончаниями «замусоривают» результаты, то можно принудительно заставить Яндекс искать только слова в нужной словоформе. Это бывает полезно, например, при совпадении названия компании с общеупотребительными словами. Скажем, маловероятно, чтобы фирма «Река» упоминалась в публикациях со словами «Реке» или «Реку».

Для того чтобы принудительно искать только нужную словоформу в Яндексе, используют оператор восклицательный знак. Он пишется слитно со словом, которое за ним следует, как если бы этот символ был первой его буквой. Запрос: [!Река] В выдаче: Рекламное агентство Река – размещение рекламы… Результат поиска: страниц – 2 267 142, сайтов – не менее 4976 А если запрос сделать без восклицательного знака: Река В выдаче: Речные круизы по рекам России и Европы Результат поиска: страниц – 10 470 689, сайтов – не менее 13 932 Видно, что количество страниц и сайтов в случае запроса с оператором «восклицательный знак» уменьшается почти в пять раз за счет исключения форм слова «река», таких как «реки», «рекой», «рекам» и пр.

6. Заглавные и строчные буквы. Яндекс периодически меняет некоторые нюансы в этом вопросе, стараясь, однако, придерживаться главного правила: слова, написанные с маленькой буквы, будут выдаваться и с маленькой, и с заглавной, а слова, написанные с заглавной буквы, будут выдаваться только с заглавной. Изменения, которые периодически происходят в подходах Яндекса к этой проблеме, обычно касаются попыток исправить наиболее распространенные ошибки пользователей. Ознакомиться с текущим состоянием дел можно как на странице помощи самого поисковика, так и в работе Дениса Фурсова. Однако для эффективной работы достаточно просто следовать приведенному в этом разделе правилу. Если же слово написано целиком заглавными буквами, Яндекс будет рассматривать его как представленное прописными. То есть, результаты ввода в поисковую строку понятия «РИТЕЙЛЕР» будут такими же, как и в том случае, если мы оформим запрос иначе – «ритейлер».

Запрос: [бухгалтерский Учет] Результат поиска: страниц – 556 606, сайтов – не менее 1984 В выдаче: ... Положение по бухгалтерскому учету «Учет основных средств» ПБУ 6/01» Запрос: [бухгалтерский учет] Результат поиска: страниц – 5 742 378, сайтов – не менее 2169 В выдаче: ...постановка, восстановление и ведение бухгалтерского учета

7. Обязательное включение слов запроса в выдачу. Чтобы искомые слова непременно присутствовали в документах к выдаче, используется оператор «плюс» (+). Для того чтобы наглядно показать работу этого оператора, сделаем запрос со словами, которые редко оказываются в одном документе. При этом разделим их пробелом. А затем сделаем точно такой же запрос, но поставим знак «плюс» перед каждым словом, запретив тем самым Яндексу выдавать документы, в которых набор искомых терминов неполный.

Результаты отличаются разительно – вместо тридцати трех тысяч страниц в первом случае, во втором мы имеем всего восемь!

Запрос: [литейщик провизор стоматолог маркшейдер]

Результат поиска: страниц – 33 005, сайтов – не менее 1192

Запрос: [+литейщик +провизор +стоматолог +маркшейдер]

Результат поиска: страниц – 8, сайтов – не менее 4 В выдаче: ОК 010-93: Общероссийский классификатор занятий (ОКЗ) ...

2221 Специалисты в здравоохранении (кроме медицинских сестер)

2221 5 Врачи

2222 Стоматологи

2223 2 Ветеринары

2224 6 Фармацевты

2229 4 Специалисты-... Образование в Кузбассе Литейщик пластмасс Литейщик цветных металлов... № 257 від 27/07/1995, Покажчик, Класифікатор, Держстандарт України для детского и подросткового возраста 2222.1 23667 – Научный сотрудник (стоматология) 2222.2 20459 – Врач-стоматолог 2222.2 20462 – Врач-стоматолог... 8122.2 13382 7 Листобойщик 8122.2 13384 2 Литейщик вакуумного, центробежно-вакуумного и центробежного литья 8122.2 13388 19 Литейщик изделий из...

Оператор «плюс» бывает незаменим и в тех случаях, когда есть необходимость обязательно включить в выдачу стоп-слова. Очень хорошо это описано в работе Дениса Фурсова.

Если какие-то слова должны быть в результатах, поставьте перед ними +'. Помогает со стоп-словами. Сейчас Яндекс, кажется, учитывает стоп-слова только в запросе из трех и менее слов (даже не операндов!). +не покупай (samsung|lg) позволит найти негативные отзывы о продукции этих фирм (сравните с простым 'не покупай (samsung|lg)). Запрос: [+не покупай (samsung | lg)] Результат поиска: страниц – 5 314, сайтов – не менее 1227 В выдаче: phorum – Основной форум – Re: ЛЮДИ, не покупайте Samsung 753 DFX в Wellcome ЛЮДИ, не покупайте Samsung 753 DFX в Wellcome новое Запрос: [не покупай (samsung | lg)] Результат поиска: страниц – 779 096, сайтов – не менее 629 В выдаче: Купля продажа мобильных телефонов на Buy-Mobile.ru – Мобильный друг ждет!

Текст ссылок: купить lg бу дешево… купить lg или sony… Правда, Яндекс игнорирует стоп-слова как-то бессистемно. Так, запросы: [+не покупай (троллейбус | автобус)] и [не покупай (троллейбус | автобус)] — дают одинаковое количество результатов, в которых слово «не» учитывается как релевантное. Тем не менее, поскольку нет возможности проверить, как Яндекс отреагировал на запрос в каждом конкретном случае, мы рекомендуем воспользоваться советом Дениса и ставить «плюс» перед стоп-словами, как, впрочем, и перед теми словами, которые вы обязательно хотели бы видеть в выдаче.

8. Поиск точной фразы. Не исключено, что вам понадобится найти определенную цитату либо рекламный слоган какой-либо компании. Для этого используется оператор «двойные кавычки», аналогичные тем, что применяются в прямой речи. В выдаче при поиске цитаты будут присутствовать документы, содержащие все слова искомой фразы, в той же форме и последовательности, что и в оригинальной ее версии. Важно помнить, что точной цитата будет лишь в том случае, если кроме фразы, указанной в кавычках, в запросе не будет никаких лишних слов. Если помимо фразы в кавычках появится еще хотя бы одно слово, Яндекс будет выдавать документы, которые содержат все слова цитаты, сохранит их последовательность, варьируя при этом их формы. Как следствие, количество документов в выдаче заметно возрастет. Яндекс называет это «слова идут подряд».

Запрос: [«ты всегда думаешь о нас»]

Результат поиска: страниц – 2905, сайтов – не менее 778

В выдаче:

Tefal – ты всегда думаешь о нас! Онли!!

Tefal, ты всегда думаешь о нас!

Х-файлы – Тефаль, ты всегда думаешь о нас.

Тефаль, ты всегда думаешь о нас! (антиреклама 1) (Николай Якимчук) | Проза. ру…

Электронный журнал со свободной публикацией произведений. Ежедневные редакторские обзоры лучших произведений.

Интересно понаблюдать при такой слаженности результатов за тем, как работает оператор исключения слова из предложения:

Запрос: [«ты всегда думаешь о нас» ~ (tefal | тефаль)]

Результат поиска: страниц – 307 773, сайтов – не менее 1197

В выдаче:

Конференции – АвтоКазань – АвтоКазань. Ru

а я вот всегда думал (+) >> OldDaddy 20.05.2005 17:21:24

Chel.ru – Новости бизнеса. Справочник промышленных, торговых, общественных и…

Почему-то я всегда думала, что практические статьи д.б. написаны ПОНЯТНЫМ языком.

Открытки Всегда думаю о тебе!!

> Красивые фотографии, открытки > Открытки > Всегда думаю о тебе!! Я Всегда думаю о тебе!!

9. Слова находятся на определенном расстоянии. Этот оператор очень часто используется на практике, так как позволяет достаточно четко ограничить поиск. Вид он имеет следующий: /n, где n, по определению самого Яндекса, – это «максимально допустимое расстояние между двумя любыми словами запроса».

Денис Фурсов дает такое определение оператору: «Расстояние между словами». Мы предлагаем следующим образом запомнить значение цифры в операторе: эта цифра (n) показывает, каким по счету будет второе слово после первого. Например, если в запросе написано:

[годовой /1 отчет], то в выдаче будет присутствовать фраза «годовой отчет». Потому что слово «отчет» будет первым после слова «годовой». Если в запросе написано: [годовой /2 отчет] то в выдаче может появиться «годовой финансовый отчет», потому что слово «отчет» может быть вторым после слова «годовой», а первым может быть любое другое слово.

Надеемся, мы объясняем доступно, потому что хотим рассказать еще о двух нюансах оператора расстояния между словами.

На самом деле, по запросу: [`годовой /2 отчет`] документы, содержащие выражение «годовой отчет», также будут выданы, потому что меньшее значение расстояния возможно, а большее – нет. Мало того, в выдачу попадет не только сочетание «годовой отчет», но и «отчет годовой». Расстояние между словами распространяется на оба слова.

Если же есть необходимость ограничить выдачу фразой «годовой отчет», исключив из нее выражение «отчет годовой», то оператор можно написать вот так: [годовой /+1 отчет]. Это практически эквивалентно запросу: [годовой /1 отчет ~ «отчет годовой»]. Количество документов в выдаче совпадает, и в первых рядах в момент составления запроса был документ: Годовой отчет – 2005. О книге. Только с «Годовым отчетом – 2005» от журнала «Главбух» вы получите удобный мини-справочник по годовому отчету…

Мы не будем чрезмерно загружать читателя описанием оператора расстояния между словами, так как сказанного вполне достаточно для работы, а изучение всех нюансов функционирования поискового движка Яндекса не входит в круг основных наших задач. Чтобы увидеть разницу между наличием и отсутствием знака «плюс» в операторе расстояния между словами, проведем напоследок такой эксперимент: сначала сделаем запрос, который позволяет появиться в выдаче документам, содержащим, согласно оператору расстояния, как фразе «годовой отчет», так и «отчет годовой», при этом исключив из результатов «годовой отчет»; а затем создадим запрос, требующий, за счет написания оператора расстояния между словами, выдачи только «годового отчета», и убедимся, что при попытке исключения конкретной фразы «годовой отчет» результат получить не удастся.

Запрос: [годовой /1 отчет ~ «годовой отчет»]

Результат поиска: страниц – 2042, сайтов – не менее 701

В выдаче:

Энциклопедии и словари

Энциклопедии и словари

ОТЧЕТ ГОДОВОЙ

Запрос: [годовой /+1 отчет ~ «годовой отчет»]

Результат поиска: страниц – 0

10. Числоформы (термин, введенный Денисом Фурсовым). Для того чтобы при запросе какого-либо нужного номера (например, номера приказа или телефона) в выдаче вам не попадались посторонние ИНН, маркировки радиоламп и микросхем, а также прочие лишние результаты, рекомендуется перед номером, который вы ищете, поставить восклицательный знак или взять его в кавычки. Сами номера надо написать во всех возможных вариантах, разделив их оператором «ИЛИ» и объединив в круглую скобку.

Запросы:

[(тел | телефон) (!123-45-67 |!1234567)]

[(тел | телефон) («123-45-67» | «1234567»)] — дадут одинаковые результаты, в выдаче мы увидим следующее:

Все услуги через телефоны доступа – Услуги – Главная страница || Инфосвязь. Например, чтобы позвонить из Москвы в Москву на номер 123-45-67, достаточно ввести телефон 1234567, что будет аналогично введению номера 84951234567!… абонента (в этом случае на дисплее вашего мобильного телефона будет отображаться следующая запись, например для телефона 123-45-67 в Санкт-Петербурге…

11. Поиск на определенном сайте. Оператор имеет вид url=www.url.ru/cat*. Хотим обратить внимание читателя на то, что на сайте Яндекса этот оператор имеет вид url=www.url.ru/cat/* с косой чертой в конце. Наш опыт показывает, что эта косая черта ухудшает результаты выдачи, поэтому мы рекомендуем записывать оператор без нее, как было показано в начале этого подраздела. Что касается знака «звездочка» в конце адреса, то это символ маски, который означает, что нас устраивает любая страница сайта, адрес которой начинается так, как написано слева от указанного символа.

Чтобы воспользоваться оператором, позволяющим проводить поиск на определенном сайте, лучше скопировать этот оператор целиком из таблицы на сайте Яндекса, нежели вводить вручную, а затем заменить в нем адрес на нужный пользователю. Так можно свести к минимуму риск орфографической ошибки. Операторы поиска на определенном сайте можно сгруппировать так, чтобы поиск проводился на группе сайтов. Денис Фурсов приводит такой пример поиска слова «работа» на сайтах www.ko.by и www.superjob.ru, который находит в общей сложности порядка 800 страниц:

Запрос: [работа && (#url=«www.ko.by*» | #url=«www.superjob.ru*»)]

Результат поиска: страниц – 791, сайтов – не менее 2

В выдаче: Работа, вакансии, подбор персонала, резюме, поиск работы – SuperJob.ru

Работа: быстрый поиск работы

Еще работа» www.superjob.ru (25 КБ) 05.03.2006 и Кадровое агентство Коллекция Открытий —… кадры, работа в Минске, работа в… Кадровое агентство Коллекция Открытий – работа, подбор персонала, кадровые агентства, трудоустройство, персонал, кадровый, кадры главная | о нас | подбор персонала | поиск работы | контакты | карта www.ko.by (16 КБ) 16.11.2005

12. Оператор ссылки (link). Этот оператор показывает, какие внешние сайты содержат ссылку на сайт, указанный в запросе. Это один из самых важных для конкурентной разведки операторов, поскольку позволяет найти друзей или союзников конкурента, часто ведет на личные странички бывших либо нынешних сотрудников компаний, может обнаружить размещенные членами их персонала объявления о поиске работы или, например, выявить аффилированные структуры. Записывается оператор следующим образом: link=www.url.ru/cat/*

Как и в предыдущем случае, мы рекомендуем убирать последнюю косую черту, после которой следует символ «звездочка». Если надо найти ключевое слово в ссылающихся на сайт страницах, то оператор link сочетается с обычными ключевыми словами, отделяясь от них двойным амперсандом. Например, зададим поиск понятия «креатив» в сайтах, ссылающихся на адрес издательства «Вершина»: www.vershinabooks.ru. Запрос: [креатив && link=www.vershinabooks.ru*] Результат поиска: страниц – 238, сайтов – не менее 26 В выдаче: Консалтинг и тренинги Москвы | Новости | Вышла книга Блестящие ответы на трудные… ТРИЗ и технологии креатива http://www.vershinabooks.ru msk.treko.ru/show_news_476 (23 КБ) 02.03.2006

При этом можно еще раз проиллюстрировать влияние знака «плюс» на результат выдачи в Яндексе. При запросе: [+креатив && link=www.vershinabooks.ru*] Результат поиска: страниц – 10. Остальные страницы, показанные в предыдущем запросе, ссылались на сайт издательства «Вершина», но слова «креатив» не содержали.

13. Оператор поиска в заголовке страницы. Для тех, кто не занимается сайтами профессионально, напомним, что заголовок страницы – это то, что написано на синем (для Windows XP) поле в самом верху экрана, как бы ужеза пределами страницы, на ее рамке. А с точки зрения разметки HTML, эта часть сайта заключена внутри тега <TITLE>.

Яндекс справедливо считает, что если ключевое слово содержится в самом заголовке страницы, значит, она однозначно имеет непосредственное отношение к запросу. Синтаксис оператора выглядит таким образом (на примере поиска слова «разведка» на страницах, содержащих в заголовке словосочетание «ИПК УГТУ»):

Запрос: [+разведка && $title (ИПК УГТУ)] Результат поиска: страниц – 1

В выдаче: Институт переподготовки кадров УГТУ (ИПК УГТУ) – Екатеринбург, Свердловская… проф. бухгалтеров, семинары и тренинги по управлению недвижимостью, изменениями, бизнес-разведке, технологиям продаж, тренинги личностного роста. www.uralfirm.ru/catalog/card/66.19517 (13 КБ) 18.06.2005

Остальные операторы языка запросов Яндекса представляют меньший практический интерес, хотя и значительно расширяют возможности поиска. Ознакомиться с ними можно на странице помощи в Яндексе, пройдя по ссылкам Помощь > Синтаксис запросов.

ЛЕКЦИЯ 3.
ОПИСАНИЕ ЯЗЫКА ЗАПРОСОВ ПОИСКОВОЙ МАШИНЫ ГУГЛ

Поиск в Гугле (Google). Гугл (google.ru) становится все более популярным. За ним стоит колоссальный финансовый ресурс, которым грамотно распоряжаются. Так, по информации из интервью инженера по программному обеспечению Google Мэта Катса, уже в 2002 г. «каждые 28 дней Google индексировал 3 млрд веб-документов, в том числе более трех млн новых страниц каждый день». Этот поисковик в чем-то проигрывает Яндексу, а в чем-то выигрывает у него. Поскольку Для удобства читателя при рассказе об операторах Гугла будем в ряде случаев проводить их сравнение с аналогичными операторами Яндекса.

1. Основы поиска. Чтобы ввести запрос, напечатайте ключевые слова и нажмите ENTER либо щелкните кнопку «Поиск в Google». Гугл использует интеллектуальную технику анализа текстов, которая позволяет искать важные и вместе с тем релевантные страницы по вашему запросу. Для этого система анализирует не только саму страницу, которая соответствует запросу, но и те, которые на нее ссылаются, чтобы определить ценность этой страницы для целей вашего поиска. Кроме того, Гугл предпочитает страницы, на которых ключевые слова, введенные вами, расположены недалеко друг от друга.

2. Показ ключевых слов в результатах. Каждый раз в списке найденных страниц Гугл показывает отрывок из текста на странице, выделяя в нем ключевые слова. Тем самым облегчается их обнаружение по всему тексту. Второй способ увидеть ключевые слова – загрузить страницу по ссылке «Сохранено в кэше». Недостаток данного способа (хотя конкурентной разведкой это нередко рассматривается как преимущество) – в том, что вы видите не ту страницу, которая есть сегодня, а т у, которая сохранена в базе Гугла. Изначально эта опция была придумана для того, чтобы сохранить возможность просмотра страницы даже в тех случаях, когда сервер, на котором она расположена, недоступен.

Третий способ – традиционный для просмотра текста в браузере – заключается в использовании сочетания клавиш CTRL+F. В результате должно появиться окно «найти», в которое необходимо ввести искомые слова. Раскладка клавиатуры, установленная в этот момент на компьютере, значения не имеет.

3. Логическое «И». В отличие от Яндекса, в Гугле всего одно логическое «И», оно наиболее близко к рассмотренному ранее поисковому механизму «&&» в сочетании с оператором «плюс», поставленным перед каждым словом запроса.

Это логическое «И» позволяет выдавать документы, которые принудительно содержат ключевые слова в любом месте текста. По умолчанию при написании слов запроса через пробел Гугл ищет документы, содержащие все слова запроса.

Запрос: [литейщик провизор стоматолог маркшейдер]

Результаты 1 – 10 из примерно 18 для литейщик провизор стоматолог маркшейдер.

В выдаче: Общероссийский классификатор занятий ОК 010-93 (ОКЗ) (утв… Общероссийский классификатор занятий ОК 010-93 (ОКЗ) (утв. постановлением Госстандарта РФ от 30 декабря 1993 г. N 298) Russian Classification of Occupations…

Работа для вас в Самаре. Поиск работы, подбор персонала, вакансии… Медсестра (стоматологический кабинет, ЕТС). Тел. 39-52-53, Адрес: ул… провизор (аптека, в/о, наличие сертификата, опыт работы в производственной аптеке,… Интересно, что Гугл может показать и те источники, которые ключевых слов не содержат, однако они присутствуют в ссылках на показанную страницу. В таком случае при просмотре информации с помощью ссылки «Сохранено в кэше» будет видна надпись:

«Эти слова присутствуют только в ссылках на эту страницу».

Описанный механизм работы Гугла хорошо виден, если посмотреть ключевые слова на странице сайта о работе в Самаре, сохраненной в кэше.

Эти слова выделены: литейщик провизор маркшейдер. А это слова присутствуют только в ссылках на страницу: стоматолог

4. Логическое «ИЛИ». Оно пишется с помощью оператора OR. Обратите внимание: оператор этот должен быть написан заглавными буквами и отделен пробелами с обеих сторон от слов, расположенных перед ним и после него. Важно знать, что, в отличие от Яндекса, Гугл не поддерживает такой оператор, как скобки.

Запрос: [литейщик OR провизор OR стоматолог OR маркшейдер]

Результаты 1 – 10 из примерно 2 030 000 для литейщик OR провизор OR стоматолог OR маркшейдер

5. Заглавные буквы или строчные? В отличие от Яндекса Гугл не различает регистр букв. Все буквы воспринимаются как строчные, вне зависимости от того, как их вводили в поисковую строку. Запросы: [Эйфелева Башня], [Эйфелева башня] и [эйфелева башня] дадут одинаковые результаты.

Результат поиска на момент написания книги:

Результаты 1 – 10 из примерно 543 000 для Эйфелева Башня.

Результаты 1 – 10 из примерно 543 000 для эйфелева башня.

6. Стоп-слова. Во вспомогательных инструкциях (хэлпах) написано, что Гугл, подобно большинству поисковых систем, игнорирует стоп-слова. Кроме того, хэлпы утверждают, будто, как и многие другие поисковики, Гугл имеет механизм принудительного включения стоп-слов в результаты поиска. К таким элементам относится большинство артиклей английского языка, союзов и предлогов русского языка. В реальности ситуация, похоже, складывается иначе.

Тест: вводим по-русски букву [в]

Результат: Результаты 1 – 10 из примерно 48 600 000 для в.

Вводим по-английски артикль [the]

Результат: Результаты 1 – 10 из примерно 8 670 000 000 для the.

7. Оператор «Плюс» (+). Тем не менее, бывают ситуации, когда надо принудительно включить в текст какое-либо слово, которое может иметь варианты написания. В хэлпе Гугла приводится пример с запросом «Star Wars Episode I», где римская единица представляет собой латинскую букву «I» («ай»). Если сделать запрос просто как:

[Star Wars Episode I], — то результат будет следующий:

Результаты 1 – 10 из примерно 13 200 000 для Star Wars Episode I.

В том числе в выдаче появятся слова «Episode II», «Episode IV» и т. п.

Если сделать запрос: [Star Wars Episode +I], — то результат будет такой:

Результаты 1 – 10 из примерно 9 290 000 для Star Wars Episode +I.

И в него войдут только тексты, содержащие слово «Episode I».

8. Морфология слов. Гугл не поддерживает морфологию слов. Их изначально следует вводить в нужных формах. Правда, отчасти это компенсируется интеллектуальной системой поиска, которая может найти нужную словоформу в ссылках на страницу. Чтобы проверить утверждение об отсутствии поддержки морфологии, возьмем такое языковое сочетание, по которому можно увидеть все без исключения результаты. А сочетание следующее: «Глоклая куздра».

Тест:

Запрос: [глоклая куздра]

Результаты 1–4 из примерно 16 для глоклая куздра.

В выдаче три адреса:

1. www.flame.ws/txt/index.php/t737.html
2. www.dom.no/modules.php?name=Forums&file=viewtopic&p=31986&highlight=
3. www.gb.anekdot.ru/vm.html?file=vm&date=1998-08-07

Запрос: [глоклую куздру]

Результаты 1–1 из 1 для глоклую куздру.

В выдаче один адрес: gb.anekdot.ru/vm.html?file=vm&date=1998-08-07

Запрос: [глоклой куздре]

Результат: Не найдено ни одного документа, соответствующего запросу глоклой куздре.

Правда, это не мешает Гуглу иногда выделять по запросу «площадь» слово «площади» как релевантное. Однако подобное встречается на странице выдачи, но не в кэше. Просто для сравнения приведем результат Яндекса. По всем трем запросам о «глоклой куздре» система дала на момент написания книги одинаковый результат:

Результат поиска: страниц – 13, сайтов – не менее 5.

9. Улучшение запроса во время поиска. Поскольку Гугл выдает все слова, которые вы вводите в запросе, имеет смысл составлять новые запросы, содержащие те слова, которые вы забыли ввести в начале поиска, но обнаружили в ходе его выполнения в найденных текстах. В ряде случаев это помогает улучшить результат. Подчеркнем особо – это должны быть именно отдельные запросы. Добавление же новых слов к уже имеющемуся списку порой приводит к излишнему сужению диапазона результатов, ведь Гугл будет пытаться выдать документ, в котором содержатся все искомые слова.

10. Исключение слов из запроса. Логическое «НЕ». Как известно, часто при составлении запроса встречается информационный мусор. Чтобы его удалить, стандартно используется оператор исключения – логическое «НЕ». В Гугле такой оператор представлен знаком «минус». Здесь он идентичен поисковому механизму Яндекса «двойная тильда» («~~»), исключающему слово из всего документа. Используя его, можно исключать из результатов поиска те страницы, которые содержат в тексте определенные слова.

Тест:

Запрос: [Журавль колодец]

Результаты 1 – 10 из примерно 778 для Журавль колодец.

Запрос: [Журавль колодец-птица]

Результаты 1 – 10 из примерно 715 для Журавль колодец – птица.

Запрос: [Журавль —колодец-птица]

Результаты 1 – 10 из примерно 120 000 для Журавль – колодец – птица.

Запрос: [Журавль – колодец-птица – птиц]

Результаты 1 – 10 из примерно 106 000 для Журавль – колодец – птица – птиц.

Запрос: [Журавль – колодец – птица – птиц – журавли]

Результаты 1 – 10 из примерно 104 000 для Журавль-колодец-птица-птиц-журавли.

11. Поиск точной фразы. Найти точную фразу, как мы уже говорили, требуется либо для поиска текста определенного произведения, либо для поиска определенных продуктов или компаний, в которых название или часть описания представляет собой стабильно повторяющееся словосочетание. В отличие от Яндекса, который может менять формы слов, входящих в текст, заключенный в кавычки, Гугл такой способностью не обладает. Мы отмечали, что эта система словоформы вообще не поддерживает.

Чтобы справиться с поиском точной фразы при помощи Гугла, требуется заключить запрос в кавычки (имеются в виду двойные кавычки, которые применяются, например, для выделения прямой речи).

Забавным, но показательным примером может быть задание из учебника русского языка для 7 класса под ред. Н. М. Шанского, где на стр. 45 предлагается разделить текст на абзацы. Автор – М. Шолохов. Произведение не указано. Приведем фрагмент текста:

[«За Доном в лесу прижилась тихая, ласковая осень. С шелестом падали с тополей сухие листья. Кусты шиповника стояли, будто объятые пламенем, и красные ягоды в редкой листве их пылали, как огненные язычки.»].

Введем этот текст в кавычках в Гугл и получим следующий результат:

Результаты 1 – 10 из примерно 15 для «За Доном в лесу прижилась тихая, ласковая осень. С шелестом падали с тополей сухие листья. Кусты шиповника стояли, будто объятые пламенем, и красные ягоды в редкой листве их пылали, как огненные язычки». Как выяснилось, этот фрагмент относится к произведению «Тихий дон» (книга четвертая).

Курьез же состоит в том, что у М. Шолохова этот текст оказался вообще не разбитым на абзацы.

Гугл воспринимает в качестве знаков, связывающих слова в единую фразу, не только кавычки, но и такие символы, как дефис, слэш (косая черта), точка, знак равенства, апостроф.

Результаты 1 – 10 из примерно 27 400 для мать-и-мачеха.
Результаты 1 – 10 из примерно 27 300 для мать/и/мачеха.
Результаты 1 – 10 из примерно 27 300 для мать=и=мачеха.
Результаты 1 – 10 из примерно 27 300 для мать.и. мачеха.
Результаты 1 – 10 из примерно 27 300 для мать'и'мачеха.

Во всех вышеприведенных случаях первым в выдаче стоит текст, фрагмент которого приведен ниже: «Мать-и-мачеха (Tussilago farfara) – одно из самых раноцветущих растений: зацветает в… Как лекарственное растение мать-и-мачеха применяется, прежде всего,…». При этом все три слова: «мать», «и», «мачеха» — рассматриваются как отдельные, но стоящие рядом и в этой же самой последовательности. Интересно, что по запросу: [мать-и-мачеха] — оказалось на 100 документов больше, чем по остальным, но если взять это слово в кавычки, то результат уравнивается: Результаты 1 – 10 из примерно 27 300 для «мать-и-мачеха». Чтобы прояснить этот казус, введем следующий запрос: [мать-и-мачеха «мать-и-мачеха»]. В итоге получим: Результаты 1 – 10 из примерно 27 для мать-и-мачеха – «мать-и-мачеха». В выдаче появятся тексты такого содержания: Санкт-Петербургская Федерация Настольного Футбола Матьимачеха. Королев Петр Трушков Кирилл. 2. Экспромт. Гриневич Василий… Матьимачеха – игроки получают по 60 рейтинговых очков; Экспромт – игроки… www.kickerclub.spb.ru/tournaments/2005-09-03.html– 17k.

12. Количество слов в строке поиска. Во многих источниках встречается информация, согласно которой поисковая строка Гугла вмещает 10 слов или что Гугл проводит поиск лишь по 10 словам. Проведенный нами эксперимент эти данные не подтвердил. Так, введем запрос из 23 слов: [крупа мука яйца масло соль перец лук макароны молоко хлеб сметана сахар помидоры рубленое мясо фарш говядина майонез салат огурцы гамбургеры булочки сыр] Результат: Результаты 1–3 из примерно 5 для крупа мука яйца масло соль перец лук макароны молоко хлеб сметана сахар помидоры рубленое мясо фарш говядина майонез салат огурцы гамбургеры булочки сыр. Ресторан. Ru | Кулинария | Кулинарные рецепты | Вторые блюда | С… (салат, помидоры, огурцы, гамбургеры, булочки, сыр, майонез)… (макароны, лук, перец, помидоры, мука, масло, рубленое мясо, мясной бульон, сыр)… www.restoran.ru/index.phtml?t=1&pid=2516

В КЭШе подчеркнуты все 23 слова, и в тексте они также присутствуют. Если изменить запрос, используя логическое «ИЛИ» вместо логического «И», то результат прогнозируемо меняется, но все слова в выдаче по-прежнему выделены Гуглом. [крупа OR мука OR яйца OR масло OR соль OR перец OR лук OR макароны OR молоко OR хлеб OR сметана OR сахар OR помидоры OR рубленое OR мясо OR фарш OR говядина OR майонез OR салат OR огурцы OR гамбургеры OR булочки OR сыр]

Результат: Результаты 1 – 10 из примерно 3 430 000 для крупа OR мука OR яйца OR масло OR соль OR перец OR лук OR макароны OR молоко OR хлеб OR сметана OR сахар OR помидоры OR рубленое OR мясо OR фарш OR говядина OR майонез OR салат OR огурцы OR гамбургеры OR булочки OR сыр.

13. Стемминг (а также wildcard). Стемминг – возможность усечения слова до его корня. После усечения слова до его корня производится поиск релевантных вариантов слов, производных от этого корня. Другими словами, стемминг позволяет искать все однокоренные слова. Техника поиска по маске (wildcard) представляет собой написание базового слова (или части слова), после которых идет символ маски – «звездочка» (*), заменяющая собой любое возможное продолжение слова. Таким образом, если поисковая машина поддерживает поиск по маске, то ищутся все слова, которые одинаково начинаются. Эта техника особенно удобна, когда вам неизвестно точное написание конкретного слова, либо когда вы хотите включить все возможные варианты слова в свой поиск.

Например, когда по запросу [тарт*] получают как «тарталетку», так и «тартар».

Так вот, Гугл эти технологии не поддерживает (как, впрочем, и Яндекс). Зато он поддерживает вариант, когда вместо целого слова вводится звездочка.

Например, по запросу: [красная * площадь] будет выдано: «Красная и Манежная площади», с подчеркиванием всех этих слов, в том числе буквы «и». В какой-то степени это похоже на поиск с расстоянием между словами, применяемый в Яндексе. По запросу: [красная * площадь – «красная площадь»] — будут получены результаты: «Красная (Семеновская) площадь», где слово «Семеновская» не считается релевантным и не подчеркивается Гуглом.

14. Дополнительные операторы.

14.1. Оператор cache: Поисковая машина хранит версию текста, которая проиндексирована поисковым пауком, в специальном хранилище в формате, называемом кэшем. Кэшированную версию страницы можно извлечь, если оригинальная страница недоступна (например, не работает сервер, на котором она хранится). Кэширо-ванная страница показывается в том виде, в котором она хранится в базе данных поисковой машины, и при показе пользователю сопровождается надписью наверху страницы о том, что это страница из кэша. Там же содержится информация о времени создания кэшированной версии. На странице из кэша ключевые слова запроса подсвечены, причем каждое слово для удобства пользователя подсвечено своим цветом. Например:

«Это сохраненная в кэше G o o g l e копия страницы http://www.kickerclub.spb.ru/tournaments/2005-09–03.html, записанная 4 янв 2006 06:07:09 GMT.». Можно создать запрос, который сразу будет выдавать кэшированную версию страницы с определенным адресом: Так, запрос: [cache:www.bstm.ru] будет сразу выдавать версию страницы www.bstm.ru из кэша, а не проверять ее нынешнее состояние. Внимание: пробела между оператором cashe: и URL'ом запрашиваемой страницы быть не должно.

Если вы хотите, чтобы ключевые слова на кэшированной версии страницы были подчеркнуты, их надо через пробел указать после оператора cashe: и адреса страницы. Например: [cache:www.bstm.ru библиотека].

14.2. Оператор info: Оператор info: позволяет увидеть информацию, которая известна Гуглу об этой странице. Например, запрос: [info:www.bstm.ru] дает следующий результат: BSTM – Бизнес-школа технологий менеджмента | Екатеринбург: Новости phpsm, phpsitemanager... Президентская программа. О программе – Стратегический менеджмент – Менеджмент качества – Маркетинг на предприятии...www.bstm.ru/ Google может показать следующую информацию об этом адресе:

Показать сохраненную в Google версию www.bstm.ru

Найти страницы, похожие на www.bstm.ru

Найти страницы, ссылающиеся на www.bstm.ru

Найти страницы на сайте www.bstm.ru

Найти страницы, упоминающие ссылку «www.bstm.ru»

Внимание: пробела между оператором info: и URL'ом запрашиваемой страницы быть не должно.

14.3. Оператор site: Этот оператор ограничивает поиск конкретным доменом. То есть, если сделать запрос:[маркетинг разведка site:www.acfor-tc.ru], — то результаты будут получены со страниц, содержащих слова «маркетинг» и «разведка» именно в домене «acfor-tc.ru», а не в других частях Интернета. Если сделать запрос: [scip site: ru], — то будут получены документы, содержащие слово «scip» и расположенные в доменной зоне «.ru».

Внимание: пробела между оператором site: и URL'ом запрашиваемой страницы быть не должно.

14.4. Оператор link: Этот оператор позволяет увидеть все страницы, которые ссылаются на страницу, по которой сделан запрос.

Например, по запросу:[link:www.livejournal.com/community/kubok/45852.html] — будут получены известные Гуглу ссылки на статью о поиске через Яндекс, написанную liveuser. Внимание: пробела между оператором link: и URL'ом запрашиваемой страницы быть не должно.

14.5. Оператор allintitle: Если запрос начать с оператора allintitle:, что переводится как «все – в заголовке», то Гугл выдаст тексты, в которых все слова запроса содержатся в заголовках (внутри тега Title в HTML).

Например, запрос: [allintitle: википедия яндекс] — даст результаты, где слова «википедия» и «яндекс» содержатся внутри тега Title на просмотренных поисковой машиной страницах. На момент написания статьи результат был таким: Результаты 1–3 из примерно 7 для allintitle: википедия яндекс.

14.6. Оператор intitle: Показывает страницы, в заголовке которых содержится слово, расположенное непосредственно после опретора intitle:,; все остальные слова запроса могут находиться в любом месте текста. Если поставить оператор intitle: перед каждым словом запроса, это будет эквивалентно использованию оператора allintitle: [intitle: википедия яндекс]. На момент написания статьи результат был таким: Результаты 1 – 10 из примерно 888 для intitle: википедия яндекс. Внимание: пробела между оператором intitle: и последующим словом быть не должно.

14.7. Оператор allinurl: Если запрос начинается с оператора allinurl:, то поиск ограничивается теми документами, в которых все слова запроса содержатся исключительно в адресе страницы, то есть в URL. Так, на момент написания статьи для запроса: [allinurl: narod razvedka] — результат был таким: Результаты 1 – 10 из примерно 14 для allinurl: narod razvedka. Внимание: оператор allinurl: работает лишь со словами, а никак не со служебными фрагментами URL. Такие специальные символы, как слэш или точка, не окажут положительного влияния на результат. Напротив, влияние будет отрицательным, поскольку они могут быть восприняты Гуглом как попытка ввести в запрос точную фразу.

Например, запрос: [allinurl: narod.razvedka],равно как и [allinurl: narod/razvedka] — результата не дал вообще.

14.8. Оператор inurl: Слово, написанное слитно с оператором inurl:, будет найдено лишь в адресе страницы Интернета, а остальные слова – в любом месте такой страницы.

Например, для того, чтобы найти слово «разведка „на сайтах, содержащих в адресе сочетание букв «tc“, можно сделать такой запрос: [inurl: tc razvedka]. Результат на момент написания статьи: Результаты 1–1 из 1 для inurl: tc razvedka. Был представлен следующим текстом: «Otryady-5 Razvedka okazalas' neskol'ko utomitel'noi (obratno shli V lavirovku). Poetomu k pirsu my podoshli sovershenno izmuchennye: no ne stol'ko samoi razvedkoi.... www-lat.rusf.ru/tc/tc08/08otr5.htm».

Если оператор inurl: поставить перед каждым словом запроса, это будет эквивалентно использованию оператора allinurl:. Внимание: пробела между оператором inurl: и последующим словом быть не должно. Внимание: оператор inurl: работает только со словами и не работает со служебными фрагментами URL. Такие специальные символы, как слэш или точка, не окажут положительного влияния на результат. Влияние будет отрицательным, так как они могут быть восприняты Гуглом как попытка ввести в запрос точную фразу.

Например, запрос [inurl: tc/razvedka], равно как и [inurl: tc.razvedka] — результата не дал вообще. Результат мог бы быть, если бы в адресе какой-то страницы содержалась точная фраза «tc/razvedka» или «tc.razvedka».

В этом можно убедиться, введя запрос: [inurl: kubok]. Результаты 1 – 10 из примерно 28 400 для inurl: kubok. И этот результат начинается с текста: «Кубок Яндекса. Как искать эффективно

– Вопросы и ответы
– Предложение организаторам соревнований
– Форум
– Кубок в LiveJournal kubok...kubok.yandex.ru/»

По запросу: [inurl: kubok/45852] Результаты 1–2 из примерно 44 для inurl: kubok/45852. И этот результат начинается с текста: «kubok: Хозяйке на заметку. Хозяйке на заметку. Материал рассчитан на подготовленного читателя, знающего, что такое стоп-слова и операнды, чем ~~ отличается от && и зачем их...www. livejournal.com/community/kubok/45852.html».

14.9. Оператор related: Этот оператор описывает страницы, которые «похожи» на какую-то конкретную страницу. Так, запрос [related: it2b.ru] дает результат: Результаты: 1 – 10 из приблизительно 29 подобных it2b.ru.

Мы не считаем, что все страницы действительно подобны странице сайта it2b. ru, с точки зрения человека, а не робота. Хотя некоторые из них действительно посвящены схожей тематике. На самом деле первым в выдаче стоит сайт it2b.ru, который специализируется на вопросах использования технологий разведки для бизнеса. А вот вторым – сайт компании «SW-Trans», предлагающей услуги по перевозке грузов.

Можем предположить, что основанием для сравнения двух сайтов послужило упоминание на ресурсе грузовой компании услуг по охране маршрутов, их сопровождению машинами со спецсигналами, о предусмотренных в таких случаях пропусках и о «решении всех возможных дополнительных проблем, возникающих при транспортировке». Наряду с транспортной компанией, Гугл включил в «подобные» страницы и такие источники, как журнал «Sales/Business (Продажи)», в котором встречается немало публикаций о предпринимательских рисках и о конкурентной разведке, а также компанию «Информзащита», работающую в области обеспечения информационной безопасности. Внимание: пробела между оператором related: и последующим словом быть не должно.

14.10. Оператор define: Этот оператор выполняет роль, своего рода, толкового словаря, позволяющего быстро получить определение того слова, которое введено после оператора. Например: [define: разведка]. Результат: Определения разведка в интернете: совокупность мер для сбора данных о действительном или возможном противнике.www.examen.ru/db/Examine/catdoc_id/50EFFB02B0ADF8B2C3256A3A003D797D/rootid/9327995FB7A6D40FC3256A02002CE0D5/defacto.html

Интересная особенность оператора define: состоит в его способности искать толкования конкретных выражений. В качестве фразы он понимает все слова, написанные после оператора, в том числе и без кавычек, просто через пробел.

Например: [define: большой взрыв]. Результат: Определения большой взрыв в интернете: Большой Взрыв – взрывной процесс в котором, по данным современной науки, наша Вселенная родилась из так называемой космологической сингулярности. ru.wikipedia.org/wiki/Большой_Взрыв. Правда, иногда этот оператор может и повеселить, представив материал, в котором мало кто разберется. Например, по запросу [define: ложка] — результат будет следующим: Определения ложка в интернете: *блесна, основанная на подражании раненой рыбке. fisherman.com.ua/files/fishsay.php. А по запросу: [define: осел] — результат такой: Похожие фразы: буриданов осел Определения осел в интернете: *строгий, собранный в кучу, материал astro.rin.ru/htmls/nostradamus/astro1826-5.html.

ВНИМАНИЕ: наличие или отсутствие пробела между оператором define: и последующим словом на результате не сказывается.

14.11. Поиск синонимов. В хэлпе Гугла сказано, что если вы хотите найти тексты, содержащие не только ваши ключевые слова, но и их синонимы, то можно воспользоваться оператором «~». Нам не удалось найти подтверждения этому заявлению.

Так, мы сравнили два запроса и не нашли разницы: [~опережающий ~разведка] Результаты 1 – 10 из примерно 33 100 для ~опережающий ~разведка. [опережающий разведка] Результаты 1 – 10 из примерно 33 100 для опережающий разведка.

14.12. Поиск числовых значений. Для тех, кому приходится работать с цифрами, Гугл дал возможность искать диапазоны между числами. Для того чтобы найти все страницы, содержащие числа в неком диапазоне «от – до», надо между этими крайними значениями поставить две точки. Например, по запросу [численность населения 1913..1917] будут выданы страницы: Народная энциклопедия городов и регионов России. Города. Санкт… Подчиненные поселки городского типа, численность населения на 1.01.2000… Вскоре после начала Первой мировой войны актом от 18 (31) августа 1914 г… rfdata.al.ru/auto/city/18/667.HTM — с выделенным числом «1914», а также: Известия Уральского государственного университета № 9(1998… За 192 года своего существования с 1723 по 1915 гг. численность населения города увеличилась в 28 раз, достигнув 112 тыс. чел. Следует отметить, что город… proceedings.usu.ru/
…/0009(03_051998)&xsln=showArticle.xslt&id=a14&doc=../content.jsp с выделенным числом «1915». Подобный пример приведен в хэлпе Гугла на примере цены DVD: [DVD player $50..$100].

14.13. Кнопка «Мне повезет» (в английском варианте – «I'm Feeling Lucky»).Кнопка «Мне повезет» расположена на главной странице Гугла. На наш взгляд, это замечательная идея. По этой кнопке система выдает наиболее релевантный, с ее точки зрения, результат. Обычно это помогает при быстром поиске какой-то фактической информации, когда не требуется подробного изучения вопроса. После нажатия кнопки «Мне повезет» вы попадаете непосредственно на сайт, который Гугл предлагает в качестве искомого. Например, запрос по указанной кнопке: [активные формы] — открывает непосредственно сайт одноименной консалтинговой компании http://www.acfor.ru/.

ЛЕКЦИЯ 4.
ОПИСАНИЕ ЯЗЫКА ЗАПРОСОВ ПОИСКОВОЙ МАШИНЫ РАМБЛЕР

Операторы Рамблера в данном разделе рассматриваются в сравнении с операторами Яндекса и Гугла. И, соответственно, те из них, которые имеют аналоги в двух других поисковых системах, здесь будут описаны не слишком подробно. Детальную характеристику мы сочли необходимым дать отличиям Рамблера от Яндекса и Гугла. Рамблер, на наш взгляд, – третья по значимости поисковая машина для работы с русскоязычными текстами. Причем, это третье место находится на очень значительном расстоянии от первых двух. Мы нечасто обращаемся к Рамблеру, поскольку, в зависимости от задачи, обычно начинаем поиск с Яндекса, после чего переходим в Гугл, или наоборот – начинаем с Гугла, а затем уточняем результат в Яндексе. В большинстве случаев этого бывает достаточно при работе с каким-то фактическим материалом, главным критерием которой выступает не полнота ответа, а его правильность. Вместе с тем, и специалисты конкурентной разведки, и представители других специальностей, которым часто приходится заниматься профессиональным поиском в Интернете, сходятся во мнении, что лишь использование нескольких поисковых машин может дать результат, претендующий на полноту ответа на вопрос. Одна поисковая система не способна справиться с подобной задачей. Связано такое положение вещей с тем, что, во-первых, поисковые роботы физически не успевают угнаться за стремительно растущим Интернетом, а во-вторых, с тем, что у разных поисковых машин – разные алгоритмы обработки собранной информации, а значит, и разные результаты этой обработки.

Как следствие, нет и не может быть полного совпадения результатов поиска, особенно когда речь идет о редком запросе.

Например, поиск во всех трех системах точной фразы (фрагмента песни) «дым, дым в твоих глазах» дал на момент написания статьи такие результаты: Запрос: [«дым, дым в твоих глазах»] Результат:

Яндекс: Результат поиска: страниц – 0

Гугл: Не найдено ни одного док-та, соответствующего запросу «дым, дым в твоих глазах».

Рамблер: Вы искали: «дым, дым в твоих глазах», найдено сайтов: 1, документов: 1 Результат этого поиска можно увидеть здесь: http://cirazvedka.narod.ru/Rambler_Cash_Examples_Folder/Dym_Dym_v_Glazakh.html

Это не значит, что Рамблер лучше всех. Знать заранее, в какой поисковой системе и что именно удастся найти, невозможно. В этом смысле показателен пример с поиском фразы – фрагмента редкой песни: «аэропорт аэропорт ночное зарево огней».

Запрос: [«аэропорт аэропорт ночное зарево огней»] Результат:

Яндекс: Результат поиска: страниц – 133, сайтов – не менее 4. http://cirazvedka.narod.ru/Rambler_Cash_Examples_Folder/Aeroport_Yandex.html

Гугл: Результаты 1–6 из примерно 32 для «аэропорт аэропорт ночное зарево огней». http://cirazvedka.narod.ru/Rambler_Cash_Examples_Folder/Aeroport_Google.html

Рамблер: Не найдено ни одного документа, полностью соответствующего запросу «„аэропорт аэропорт ночное зарево огней“». http://cirazvedka.narod.ru/Rambler_Cash_Examples_Folder/Aeroport_Rambler.html

Итак, перейдем к рассмотрению работы с ***Рамблером***. Основу этой работы составляет раздел «Помощь», расположенный по адресу: http://www.rambler. ru/doc/help.shtml – и форма расширенного поиска, находящаяся по адресу: http://www.rambler.ru/cgi-bin/advanced.cgi?set=www.

1. Какие ресурсы Рамблер индексирует. По утверждению создателей системы, Рамблер индексирует сайты, размещенные в следующих доменах первого уровня:

Российская Федерация:.ru,su
Украина:.ua Белоруссия:.by
Казахстан:.kz Киргизия:.kg
Узбекистан:.uz Грузия:.ge

Сайты, находящиеся в других доменах, поисковик игнорирует.

Для тех, кто хочет, чтобы их сайт, расположенный в другой доменной зоне, был проиндексирован Рамблером, эта поисковая машина оставляет небольшую надежду на успех. Если Ваш сайт находится вне названных доменов (например, в зонах. com,org,net), но существенная часть сайта содержит русскоязычные материалы или, по Вашему мнению, он может представлять интерес для русскоязычной аудитории Рамблера, Вы можете отослать письмо на адрес search.support@rambler-co.ru с просьбой включить Ваш сайт в число сканируемых, либо заполнить форму обратной связи. Наши сотрудники рассмотрят эту просьбу и примут решение о целесообразности такого включения. Кроме того, Рамблер утверждает, что «умеет извлекать гиперссылки из объектов Macromedia Flash», но не индексирует непосредственно сами тексты flash-объектов. Для таких технически продвинутых сайтов специалисты поисковой системы советуют создавать HTML-копию.

2. Поддержка морфологии слов. По умолчанию, Рамблер поддерживает морфологию слов. Отключение поддержки морфологии предусмотрено, но требует использования специального оператора – слово должно быть взято в кавычки. Наш эксперимент подтвердил, что система морфологию слов действительно поддерживает.

3. Скобки. Рамблер позволяет использовать скобки для группировки слов и применения ко всем словам, расположенным в скобках, одного оператора, который пишется перед скобкой. В этом описываемая в данном разделе система ничем не отличается от Яндекса, поэтому подробнее применение скобок мы рассматривать не станем.

4. Транслитерация. Люди довольно часто делают ошибки при вводе текста и вместо русских букв печатают их английских «близнецов». Например, букву «с». Рамблер говорит, что старается исправлять такие огрехи, однако не гарантирует результата.

Эксперимент показал, что система действительно справляется с опечатками транслитерации, если количество таких ошибок в слове невелико. Убедитесь сами. Запрос (все буквы русские): [«глОКлАя кУздРА»]

Результат: Вы искали: «глОКлАя кУздРА», найдено сайтов: 5, документов: 37. Запрос (заглавные буквы – латинские): [«глОКлАя кYздРА»]

Результат: Не найдено ни одного документа, полностью соответствующего запросу ««глОКлАя кYздРА»».

Запрос (заглавные буквы – латинские): «глОклая куздРа»

Результат: Вы искали: ««глОклая куздРа»», найдено сайтов: 5, документов: 37. Чтобы не загружать читателя лишними примерами, скажем лишь, что при трех опечатках правильный поиск еще проводился, но после появления четвертой неправильно написанной буквы результат поиска стал нулевым. Рамблер в комментариях к результату поиска в этом случае просто порекомендовал пользователям быть внимательнее при вводе текста.

5. Регистр букв. Как правило, Рамблер не учитывает регистр букв, причем он распространяет это правило не только на слова запроса, но и на операторы. Действительно, запросы «глоклая куздра» и «ГлоКЛаЯ КУздРа» дали одинаковые результаты.

Запрос: [«глоклая куздра»]

Результат: Вы искали: «„глоклая куздра“«, найдено сайтов: 8, документов: 45

Запрос: [«ГлоКЛаЯ КУздРа»]

Результат: Вы искали: «„ГлоКЛаЯ КУздРа“«, найдено сайтов: 8, документов: 45

Однако Рамблер сообщает, что он делает исключение из этого правила: если в запросе, как минимум, два слова, идущих подряд, написаны с заглавной буквы, система, как утверждают ее создатели, старается искать эти слова также с заглавной буквы. То есть, Рамблер пытается помочь тем, кто ищет имена собственные или географические названия. Проведенный нами эксперимент этого не подтвердил.

Запросы: [слава зайчиков] и [Слава Зайчиков] выдали в Рамблере одинаковое количество страниц в выдаче. Вы искали: слава зайчиков, найдено сайтов: 813, документов: 2621

Вы искали: Слава Зайчиков, найдено сайтов: 815, документов: 2621.

Это похоже на результаты Гугла, который не различает заглавные и прописные буквы:

Результаты 1 – 10 из примерно 138 000 для слава зайчиков

Результаты 1 – 10 из примерно 138 000 для Слава Зайчиков.

Тогда как в Яндексе, который различает заглавные и прописные буквы, результат был иным:

Запрос: [слава зайчиков] Результат поиска: страниц – 403, сайтов – не менее 173. Запрос: [Слава Зайчиков] Результат поиска: страниц – 64, сайтов – не менее 33. Совершенно идентичные предыдущим результаты были получены и на запросах из трех слов: [одна баба сказала] и [Одна Баба Сказала] Результат: Вы искали: одна баба сказала, найдено сайтов: 42056, документов: 619112 Результат: Вы искали: Одна Баба Сказала, найдено сайтов: 42054, документов: 619112.

6. Стоп-слова и оператор «кавычки». Подобно Яндексу, Рамблер при обработке запроса может проигнорировать стоп-слова. Авторы системы утверждают, что для принудительного включения указанных элементов (или каких-либо других, подобных им) в выдачу, нужное слово следует заключить в кавычки. Эксперимент расставил акценты иначе. Стоп-слова, независимо от того, закавычены они или нет, одинаково попадают в выдачу. А вот остальным словам (не входящим в список стоп-слов), которые необходимо в обязательном порядке включить в выдачу, кавычки действительно обеспечивают обязательное включение в результат. Это эквивалентно оператору «плюс» в Яндексе и Гугле.

Вы искали: «с» пингвином, найдено сайтов: 15468, документов: 166651

Вы искали: с пингвином, найдено сайтов: 15468, документов: 166651.

Вы искали: «the» apple please, найдено сайтов: 2700, документов: 16047

Вы искали: the apple please, найдено сайтов: 2700, документов: 16047.

Пример работы кавычек в иных случаях, а не только со стоп-словами, приведен в следующем разделе – Логическое «И».

Кроме того, как мы уже говорили, кавычки могут выступать аналогично оператору «восклицательный знак» в Яндексе. Слово, указанное в запросе в кавычках, будет присутствовать в результатах поиска лишь в той форме, в которой вы его зададите.

7. Логическое «И». Как и в Яндексе с Гуглом, роль логического «И» в Рамблере выполняет пробел. В принципе, можно ввести вместо пробела слово AND, но на практике, по вполне понятным причинам, так обычно не делается. Подобно Яндексу, Рамблер достаточно вольно обращается со словами, которые соединены пробелом – он может легко выдать не только те документы, где присутствуют ВСЕ слова запроса, но и те, где на одно-два слова меньше. В этом можно убедиться, сравнив два запроса: [кошки собаки верблюды зебры носороги] Вы искали: кошки собаки верблюды зебры носороги, найдено сайтов: 42, документов: 296

http://cirazvedka.narod.ru/Rambler_Cash_Examples_Folder/Rambler_bez_Nosorogov.html и [«кошки» «собаки» «верблюды» «зебры» «носороги»]

Вы искали: «кошки» «собаки» «верблюды»…, найдено сайтов: 9, документов: 53

http://cirazvedka.narod.ru/Rambler_Cash_Examples_Folder/Rambler_s_Nosorogami.html. Во втором случае все без исключения элементы запроса принудительно включены в выдачу – за счет кавычек, поэтому документов в выдаче значительно меньше.

8. Логическое «ИЛИ». Написание этого оператора приспособлено как для любителей Яндекса, так и для тех, кто предпочитает работать с Гуглом.

Как и в Яндексе, в Рамблере логическое «ИЛИ» может быть представлено вертикальной чертой |.

Для тех, кто привык к логическому «ИЛИ» Гугла, данная система предоставляет возможность пользоваться также оператором OR. Приоритета нет ни у одного из этих двух указанных вариантов.

Наример: Вы искали: дуоденогастрэктомия OR циклопентанпергидрофенантрен,

найдено сайтов: 266, документов: 813.

Вы искали: дуоденогастрэктомия | циклопентанпергидрофенантрен,
найдено сайтов: 266, документов: 813

9. Логическое «НЕ». Логическое «НЕ» в Рамблере похоже на таковое в Гугле и распространяется на весь документ. Сузить запрос, подобно Яндексу, до предложения, эта система не позволяет. Записывается логическое «НЕ» как NOT.

Запрос: [журавль] Вы искали: журавль, найдено сайтов: 43085, документов: 554542
Запрос: [журавль NOT колодец]
Вы искали: журавль NOT колодец, найдено сайтов: 41447, документов: 528644
Запрос: [журавль NOT (колодец | птица)]
Вы искали: журавль NOT (колодец | птица), найдено сайтов: 33059, документов: 390789
Запрос: [журавль NOT (колодец | птица | «журавль»)]
Вы искали: журавль NOT (колодец | птица | «журавль»), найдено сайтов: 23824, документов: 225549
Запрос: [журавль NOT (колодец | птица | «журавль» | «журавлей»)]
Вы искали: журавль NOT (колодец | птица | «журавль» | «журавлей»), найдено сайтов: 21197, документов: 192387

10. Стемминг (а также wildcard).

Рамблер НЕ поддерживает ни стемминг, ни вилдкард.

11. Поиск с заданным расстоянием. Рамблер не очень качественно поддерживает поиск с расстоянием, несмотря на то, что его «Помощь» утверждает обратное. Рамблер говорит о том, что когда он ищет слова «в документе», то он реально ищет их на расстоянии не более 40 слов друг от друга. Это, конечно, не поиск с расстоянием, а скорее ограничение расстояния, но, по крайней мере, это прямо заявленное ограничение. Однако при этом Рамблер утверждает, что уменьшить расстояние в 40 слов можно. Запрос, при котором слова должны находиться рядом, в «Помощи» выглядит так: [2, красная армия]

Интересно, что при проверке этого утверждения мы обнаружили, что поисковик, похоже, – рекордсмен по числу сайтов, которые можно реально открыть в результатах запроса. Так, в случае с запросом про «красную армию» Рамблер показал более двух с половиной тысяч сайтов и был готов демонстрировать их и дальше, если бы мы не прекратили свой эксперимент. Результат можно увидеть по адресу: http://cirazvedka.narod.ru/Rambler_Cash_Examples_Folder/Three_Thousands_Sites.html.

Еще нам показался необычным (и неудобным) способ перехода к следующей группе сайтов в результатах выдачи. Так, если в Яндексе можно уйти, например, на 20-ю страницу выдачи, после чего внизу страницы с результатами последней доступной для просмотра в группе страниц станет 30-я, то в Рамблере для того, чтобы эта 30-я страница стала видна, требуется сначала выбрать переход к следующей группе сайтов вверху страницы, под строкой с запросом, и только после этого можно выбрать последнюю страницу следующей группы сайтов и перейти на нее. Подобная организация перехода в два приема совершенно непонятна. Однако вернемся к непосредственным результатам запроса [2, красная армия], — который, согласно хэлпу Рамблера, должен рассматривать цифру «2» как служебную информацию о расстоянии между словами, и выдавать результаты, где слова «красная» и «армия» находятся рядом.

Наше внимание привлекло то, что цифра «2», которая в поиске должна была играть роль элемента оператора запросов, в выдаче обозначалась как слово, релевантное искомому. Чтобы не пролистывать результаты по «красной армии» до 47-тысячного сайта, мы попробовали испытать поиск с расстоянием, как он описан в разделе «Помощь», на другом запросе и не получили положительного результата. Для того чтобы провести такую работу, мы взяли за основу фразу из песни: «Майскими короткими ночами, отгремев, закончились бои».

Запрос: [2, «майскими» «ночами» +отгремев] Вы искали: 2, «майскими» «ночами» +отгремев, найдено сайтов: 48, документов: 293.

В выдачу попали документы, не содержащие слова запроса непосредственно рядом друг с другом, более того, цифра «2» опять оказалась рассмотрена в качестве части введенного в поисковую строку выражения: Фотографии, рекомендованные автором Roman Mezenin:: Галерея:: Клуб Foto.ru… Портрет Комм. 6 / Рек. 2 Майскими короткими ночами / отгремев, закончились бои 05.06.2005 – 26 Kb – http://www.club.foto.ru/gallery/photos/recommended… – Восстановить текст – Найти похожие – Рубрика: Фото Морской интернет-клуб Майскими короткими ночами, Отгремев, закончились бои. Где же вы теперь, друзья – однополчане, Боевые спутники мои? Страницы: 1 2 3 4 5 6 7 18.10.2005 – 10 Kb – http://randewy.ru/pes/stol2.html – Восстановить текст – Найти похожие. Остальные операторы Рамблера вынесены в «Форму расширенного поиска», расположенную по адресу: http://www.rambler.ru/cgi-bin/advanced.cgi?set=www.

11.1. Поиск в заголовках страниц (<title>). Этот оператор, существующий в Яндексе и Гугле как самостоятельный, в Рамблере тоже есть, но в «Помощи» системы он не указан и найти его нам удалось лишь в «Форме расширенного поиска». Ссылка на форму расширенного поиска находится непосредственно справа от поисковой строки Рамблера.

11.2. Поиск ссылающихся страниц (link). Этот оператор также встретился нам только в «Форме расширенного поиска». Возможность использования его на практике проверена. Работает.

12. Язык документа. Принудительное назначение конкретного языка документа возможно в «Форме расширенного поиска». При этом Рамблер предлагает на выбор один из трех языков: русский, украинский или английский.

По умолчанию в поле выбора языка отмечен вариант «любой».

13. Формат документа. Выбор форматов, как и языков, по современным меркам не впечатляет. Предлагаются HTML, Word (.doc) и Adobe Acrobat (.pdf).

14. Дата документа. Рамблер, подобно Яндексу, предлагает интересную возможность выбора даты в «Форме расширенного поиска», но если Яндекс, помимо конкретного диапазона с датами, позволяет выбрать, скажем, «последние 2 недели» или «последний год», то в Рамблере можно провести выборку лишь в конкретном временном диапазоне.

15. Поиск на определенном сайте. Представлен строкой в «Форме расширенного поиска» с названием: «Искать документы только на следующих сайтах:». Таким образом, на наш взгляд, Рамблер представляет определенный интерес для поиска страниц, когда требуется полнота выборки, но чаще эта поисковая система выполняет роль «запасного игрока» – на тот случай, если запросы, введенные в Яндекс и Гугл, не дадут желаемых результатов. Сам Рамблер, похоже, с этим смирился и не стремится каким-либо образом менять ситуацию, о чем косвенно свидетельствует довольно бедный набор возможностей настройки запроса. Однако порой система может быть весьма полезна, что вновь и вновь подтверждается практикой.

А.Н. Кришталюк

аспирант кафедры «Туризм, рекреация и спорт»
ФГБОУ ВПО «Госуниверситет – УНПК»

ЗАЩИТА БИЗНЕСА

(курс лекций)

МАБИВ
АКАДЕМИЯ

СОДЕРЖАНИЕ

Скорее всего, многие согласятся с тем, что совершенно безразлично, будет ли предприятие разорено бандитами, вымогателями, штрафами налоговой инспекции, либо в результате недобросовестных действий деловых партнеров, конкурентов или собственного персонала, - в любом случае оно может прекратить свое существование. Следовательно - речь надо вести об обеспечении безопасности деятельности организации. Обеспечение безопасности необходимо для любых организаций, независимо от форм их собственности, начиная от государственных организаций и заканчивая маленькой палаткой, занимающейся розничной торговлей. Различие будет состоять лишь в том, какие средства и методы и в каком объеме требуются.

Что же следует понимать под безопасностью предприятия, из чего она собственно состоит и какие вопросы требуют Вашего повышенного внимания?

Конечно, о чем бы мы ни говорили - какие меры безопасности ни рассматривали, так или иначе, все направлено на обеспечение экономической стабильности в деятельности предприятия. Однако, достижение этой стабильности невозможно без анализа всех сторон деятельности предприятия.

Что такое безопасность

Под безопасностью предприятия обычно понимается защита от угрозы нанесения ему ущерба, т.е. безопасность предприятия - это состояние защищенности его жизненно важных интересов от внутренних и внешних угроз (источников опасности). Подобная защищенность достигается применением комплекса мер правового, экономического, организационного, инженерно-технического и социально-психологического характера.

Существующее мнение о том, что безопасность - это, прежде всего, физическая защищенность, не совсем верно.

Безопасность предпринимательской деятельности сегодня - это не только автомат и бронестекло "шестисотого", а, прежде всего, это вычисление и всесторонний анализ угроз деятельности предприятия; прогноз и создание систем и мер защиты и минимизации коммерческих рисков. При этом угрозами считаются не только такие очевидные факты, как, например, посягательство на личность: грабеж, рэкет или физическое насилие, то есть те, которые носят явно криминальный характер, но и такие неочевидные как: недобросовестность деловых партнеров и некомпетентность персонала, необоснованные претензии налоговых либо правоохранительных органов и т.д.

Для лучшего понимания того, что же такое система безопасности предприятия (для чего она создается, какие задачи решает, как строится) и для того чтобы в дальнейшем эффективно построить свою систему безопасности, необходимо четко определить следующие моменты:

- Правовые основы
- Цель построения системы безопасности
- Правила построения (см. Законы безопасности п.п. 1.3.)
- Рассмотрим эти вопросы подробнее.

Правовые основы обеспечения безопасности определяют соответствующие положения Конституции Российской Федерации, Закон "О безопасности" (см. Приложение 7.3.), федеральные законы и другие нормативные акты.

Правовая защита персонала, материальных и экономических интересов предприятия от преступных посягательств обеспечивается на основе норм Уголовного и Уголовно-процессуального кодексов, законов Российской Федерации о прокуратуре, о федеральной службе безопасности, о милиции, об оперативно-розыскной деятельности, о частной детективной и охранной деятельности, об оружии и др.

Защиту имущественных и иных материальных интересов, деловой репутации коммерческих предприятий призваны обеспечить, также, гражданское, гражданско-процессуальное, арбитражное и арбитражно-процессуальное законодательство (более подробная информация в Приложении).

Целью создания системы безопасности предприятия является комплексное воздействие на потенциальные и реальные угрозы, позволяющее организации:

- успешно функционировать в нестабильных условиях внешней и внутренней среды,
- предотвращать угрозы собственной безопасности,
- защищать свои законные интересы от противоправных посягательств,
- охранять жизнь и здоровья персонала,
- не допускать хищения финансовых и материально-технических средств, уничтожения имущества и ценностей, разглашения, утраты, утечки, искажения и уничтожения служебной информации, нарушения работы технических средств, обеспечения производственной деятельности, включая и средства информатизации.

Достижение этой цели требует решения следующих задач:

- выявления угроз стабильности работы предприятия и его развитию и выработка мер противодействия;
- обеспечения защиты технологических процессов;
- реализации мер противодействия всем видам шпионажа (промышленного, научно-технического, экономического и т.д.);
- своевременного информирования руководства предприятия о фактах нарушения законодательства со стороны государственных и муниципальных органов, коммерческих и некоммерческих организаций, затрагивающих интересы предприятия;
- предупреждения переманивания сотрудников предприятия, обладающих конфиденциальной информацией;
- всестороннего изучения деловых партнеров;
- своевременного выявления и адекватного реагирования на дезинформационные мероприятия;
- разработки и совершенствования правовых актов предприятия, направленных на обеспечение его безопасности;
- реализации мер по защите коммерческой и иной информации;
- организации мероприятий по противодействию недобросовестной конкуренции;
- обеспечения защиты всех видов ресурсов предприятия;
- реализации мер по защите интеллектуальной собственности;
- организации и проведения мер по предотвращению чрезвычайных ситуаций;
- выявления негативных тенденций среди персонала предприятия, информирования о них руководства предприятия и разработки соответствующих рекомендаций;
- организации взаимодействия с правоохранительными и контрольными органами в целях предупреждения и пресечения правонарушений, направленных против интересов предприятия;
- разработки и реализации мер по предупреждению угроз физической безопасности имуществу предприятия и его персоналу;
- возмещения материального и морального ущерба, нанесенного предприятию в результате неправомерных действий организаций и отдельных физических лиц.

Результатом деятельности по обеспечению комплексной безопасности предприятия являются: стабильность (надежность) его функционирования и финансово-экономического состояния, личная безопасность персонала.

Когда надо задумываться о безопасности

Безопасность предпринимательской деятельности, а часто это и Ваша личная безопасность - это тот случай, когда лучше предупредить возможные неприятности, чем решать возникающие проблемы. Многие риски в предпринимательской деятельности можно просчитать заранее. Лучше всего задуматься о безопасности Вашего бизнеса в тот момент, когда Вам пришла идея создать свое предприятие. Потратить некоторое количество сил и средств на начальном этапе и исправить свои возможные просчеты и ошибки на бумаге, когда Ваше представление о том, что такое Ваш бизнес, как он выглядит, как будет развиваться, еще только формируется, - значительно проще и дешевле чем ломать уже выстроенный и работающий механизм. Кроме того, задумываться о проблемах безопасности надо всякий раз, как Ваш бизнес претерпевает какие-либо изменения. Постарайтесь ответить на вопрос: кто от Ваших действий (хотя бы косвенно) может пострадать?

Например: Вы решили установить систему автоматизации бухгалтерского учета. В результате двое из четырех работников бухгалтерии становятся не нужны. Одну из работниц Вы переводите на новый участок, другую увольняете, и она направляет к Вам налоговую полицию. Даже если проверка налоговыми органами ничего криминального не выявит, то время и нервы отнимет точно.

Другой вариант: Вы решили внедрить новую технологию, существенно упрощающую и удешевляющую процесс переработки нефти. Можете не сомневаться, что компании занятые в этой отрасли сделают все, чтобы Ваше техническое решение так и осталось нереализованным - для них это потеря дохода (рынок любит стабильность и добровольно начинать ценовые войны, передел зон влияния никто не хочет). Возможно, последний пример кому-то покажется надуманным, но … это случай из практики.

Вы решили распространить через сеть розничной торговли новый вид товара, выгодно отличающийся от того, что сейчас представлено на рынке. И все начинается довольно неплохо - спрос высокий, продажи растут. Но при этом продукция кого-то другого, кто на этом рынке работал до Вас, безнадежно "встала". Скорее всего, этот "кто-то" обязательно поинтересуется, кто Вы такой, насколько Вы сильны и нельзя ли Вас каким-то образом "потеснить"…

Законы безопасности

Система безопасности предприятия должна быть построена с соблюдением следующих правил:

- *Профилактика возможных угроз.*

Необходимо своевременное выявление возможных угроз, анализ которых позволит разработать соответствующие профилактические меры.

- *Законность.*

Меры по обеспечению безопасности разрабатываются на основе и в рамках действующих правовых актов. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам.

- *Комплексное использование сил и средств.*

Для обеспечения безопасности используются все имеющиеся в распоряжении предприятия силы и средства. Каждый сотрудник должен, в рамках своей компетенции, участвовать в обеспечении безопасности предприятия. Организационной формой комплексного использования сил и средств является программа (план работ) обеспечения безопасности предприятия.

- *Координация и взаимодействие внутри и вне предприятия.*

Меры противодействия угрозам осуществляются на основе взаимодействия и координации усилий всех подразделений, служб предприятия, а также установления необходимых контактов с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности предприятия.

- *Сочетание гласности с секретностью.*

Доведение информации до сведения персонала предприятия и общественности в допустимых пределах мер безопасности выполняет важнейшую роль - предотвращение потенциальных и реальных угроз.

- *Компетентность.*

Сотрудники должны решать вопросы обеспечения безопасности на профессиональном уровне, а в необходимых случаях специализироваться по основным его направлениям.

- *Экономическая целесообразность.*

Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

- *Плановая основа деятельности.*

Деятельность по обеспечению безопасности должна строиться на основе комплексной программы обеспечения безопасности предприятия, подпрограмм обеспечения безопасности по основным его видам (экономическая, научно-техническая, экологическая, технологическая и т.д.) и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников.

- *Системность.*

Этот принцип предполагает учет всех факторов, оказывающих влияние на безопасность предприятия, включение в деятельность по его обеспечению всех сотрудников, использование всех сил и средств.

Оцените Ваш бизнес - постарайтесь понять, для кого и какой он может представлять интерес

Необходимо отметить, что среди возможных проблем чаще всего, отмечаются случаи неправомерного использования материальных (финансовых) ресурсов предприятия. Но, кроме того, существует угроза непосредственного подчинения предпринимателя (или его фирмы) сторонним организациям и тем самым получения экономических выгод от его деятельности.

Рейтинг обращений отечественных бизнесменов за помощью в охранные фирмы выглядит следующим образом (по убывающей):

1) Проблема возврата средств (не поступает плата за отгруженный товар, не поступает оплаченный товар, не возвращается в указанный срок кредит);

2) Проблема личной безопасности бизнесменов и членов их семей в связи с угрозами и вымогательством;

3) Хищение грузов на транспорте;

4) Кражи личного имущества в квартирах, офисах, коттеджах, загородных строениях; ограбления; угоны автомобилей;

…

...

5) Похищение коммерческой информации (кража документов, их копирование, съем информации с компьютеров и факсов, прослушивание и запись телефонных сообщений, разговоров в помещениях, подкуп сотрудников);

6) Кражи и ограбления в магазинах, складских и производственных помещениях;

7) Порча имущества и товаров. Поджоги.

Итак, Вы посмотрели статистику обращений отечественных предприятий в охранные фирмы. Теперь попробуем понять, как определить, для кого и какой интерес будет представлять деятельность Вашей фирмы.

В настоящее время в России, деятельностью любого хозяйствующего субъекта в основном интересуются: государство, конкуренты, криминальные структуры и его собственный персонал.

Государство в основном контролирует правовую основу Вашей деятельности - зарегистрировано ли предприятие, есть ли лицензии, соответствующие вашему виду деятельности и исправно ли вы платите налоги. Кроме того, у правоохранительных органов интерес могут вызвать любые ваши действия нарушающие действующее законодательство. Поэтому, для того чтобы определить степень интереса государства к вам, посмотрите, какие ваши действия могут быть расценены различными контролирующими государственными органами как сомнительные или противоправные. Например, налоговой инспекцией.

У остальных "интересующихся" интерес носит, как правило, сугубо материальный характер.

Интерес криминальных структур - необходимо отдавать себе отчет в том, что если ваше предприятие в силу специфики своей деятельности попадает в зону повышенного интереса криминальных структур, то избежать общения с ними вам вряд ли удастся. Так что в этом случае лучше заранее оценить свои силы. Круг этих интересов на данной территории, если вы сами их не очень хорошо представляете, вам помогут определить специалисты (например, сотрудники детективных агентств или информационно-аналитических служб)

Кроме того, необходимо помнить, что Вы рискуете привлечь к себе повышенное внимание преступных группировок, применяя методы, нарушающие требования законодательства или деловой этики.

Но, даже если Вы будете вести бизнес по всем правилам, все равно есть риск встретиться с криминальным давлением. Такое давление может возникнуть не только в случае проявления непосредственного интереса к Вашей деятельности со стороны криминальных структур, но и как форма недобросовестной конкуренции. Дело в том, что часто недобросовестная конкуренция не только осуществляется незаконными методами, но и при этом, в качестве средств воздействия используются криминальные структуры. Кроме того, предприятие, а вернее его финансовые средства, представляют большой интерес и для разного рода мошенников, деятельность которых так же можно отнести к криминальной.

Мошенничество в экономической сфере

Основными способами для достижения цели у мошенников являются обман, введение в заблуждение, злоупотребление доверием. Один из видов мошенничества - использование фальшивых документов (подделка печатей и штампов) реальных или вымышленных фирм. Данный способ основан на индивидуальных способностях мошенника, использующего доверие сотрудников, внушаемость, некомпетентность, халатность. Встречаются и более изощренные способы мошенничества. Например, фирмы, созданные только для того, чтобы, набрав заказы, получить деньги по предоплате и исчезнуть. Здесь встречаются и довольно хитроумные комбинации.

Одна из фирм, занимающаяся перепродажей товара из-за рубежа, для того чтобы привлечь клиентов снизила отпускные цены на товары ниже закупочных. От клиентов не было отбоя. Договоры поначалу точно выполнялись, имидж компании сомнений не вызывал, число клиентов росло. Создалась обычная пирамида. Естественно, вскоре руководство фирмы исчезло с деньгами, перечисленными по предоплате.

Изощренные мошенники часто проходят процедуру регистрации вполне легально и некоторое время добросовестно работают. При этом ни учредители, ни непосредственные руководители могут и не быть замеченными в каких-либо махинациях ранее. Выявить таких можно только с помощью системы достаточно сложных проверок руководителей, учредителей, их связей и анализа деятельности. Это под силу только специализированной фирме. Но обычно, для выявления возможного мошенничества достаточно получить информацию об организации, ее деятельности (прошлой и настоящей) и учредителях. Поэтому, всегда нужно четко знать, где и какую информацию Вы можете получить.

Выбор способа получения информации зависит от Вас. Но нецелесообразно использовать какой-то один: рациональное решение лежит в области их комбинирования в зависимости от ситуации. Конкуренты всегда проявляют интерес к вашей деятельности, даже если вы об этом и не догадываетесь. Вопрос лишь в том - что является предметом столь пристального внимания, и какие методы используются для его удовлетворения. Наиболее вероятно, что интерес вызовут используемые вами новые технологии, методы работы, программы расширения и НИОКР и т.д.

Другое направление проявления повышенного интереса - это информация по настоящим и предполагаемым партнерам, клиентам, перехват выгодных контрактов и инвестиционных проектов, поставщиков и каналов сбыта. Но не стоит забывать и о недобросовестной конкуренции, основной принцип которой заключается в стремлении любыми, даже незаконными средствами, укрепить свое положение за счет ослабления позиций конкурентов, либо за счет обмана потребителей, или путем сочетания того и другого.

Недобросовестная конкуренция осуществляется в форме:

- экономического шпионажа,
- лживой рекламы,
- компрометации фирмы,
- фальсификации и подделки продукции,
- посредством прямого обмана, нанесения материального ущерба, психологического и физического подавления.

Персонал, как правило, интересует стабильность в деятельности Вашей организации, так как от этого зависит и стабильность заработной платы. Но бывают и исключения - это те, кто о размере своего дохода заботится сам, но... за ваш счет. Основные способы при этом - мошенничество либо воровство.

Внутреннее мошенничество

К таковому относятся любые действия самих сотрудников, либо совершенные при их пособничестве и направленные на использование активов предприятия в личных целях. Формы его бывают различными: это и хищение, и растрата, и присвоение, и приобретение права на чужое имущество.

В соответствии с американской статистикой, в среднем каждая организация в США теряет от мошенничества более $9 в день на каждого работника и приблизительно 6% годового дохода от мошенничеств всех своих, нечистых на руку сотрудников. Однако стоимость мошенничества и злоупотреблений в целом трудно поддается количественному измерению. Причин тому несколько: не все мошенничества и злоупотребления раскрываются; не все раскрытые факты предаются огласке; о некоторых случаях мошенничества собрана неполная информация; гражданское или уголовное преследование часто не возбуждается.

Каким бывает внутреннее мошенничество?

Выделяют три категории внутреннего мошенничества, характеризуемые такими образующими признаками, как незаконное присвоение активов, коррупция и мошеннические утверждения.

Незаконное присвоение активов является основной формой внутреннего мошенничества, составляя более четырех пятых известных нарушений, причем нарушения с наличными средствами и чековыми расчетами организаций равны общей доле потерь всех других активов (инвентарь, поставки, оборудование и информация). Это получение “навара” с продажи “неучтенки”, незаконное списание, неприкрытое изъятие и т.д.

Коррупция, в смысле внутреннего мошенничества, обычно заключается в том, что должностное лицо, менеджер или служащий организации вступает в сговор с посторонними. Известны несколько основных типов внутренней коррупции, ведущих к ущербу для интересов предприятия: взяточничество, запрещенные денежные вознаграждения, специальное завышение цены по договоренности и пр. На долю коррупции приходится около 10% всех случаев внутреннего мошенничества.

Кто сколько ворует?

Статистические данные указывают, что приблизительно 58% известных случаев мошенничества и злоупотреблений совершаются служащими, 30% - менеджерами и 12% - топ-менеджерами и собственниками.

Семейные служащие совершают самое большое количество мошенничеств и злоупотреблений и наносят самый высокий средний ущерб - в 72% случаев. А потери, вызываемые мужчинами, в 4 раза больше потерь, вызываемых женщинами. Средние потери, вызванные виновными с высшим образованием, более чем в пять раз превышают потери, вызванные выпускниками средней школы. Доля мошенничества с материальными ценностями непременно увеличивается в процессе роста организации, так как небольшие организации более оперативны при выявлении фактов мошенничества.

Менеджеры среднего звена образуют наиболее многочисленную группу лиц, совершающих мошенничество, хотя, в свою очередь, мошенничества, совершенные топ-менеджерами, имеют более высокую цену потерь. Если говорить о предварительном сговоре, то он встречается более чем в 50% случаев от всех совершаемых мошенничеств, которые для предприятия-жертвы обходятся всегда намного дороже, чем другие его виды. Наиболее же чреваты последствия для предприятия, если оно оказалось жертвой сговора внутренних и внешних преступников.

Воровство

Считается, что самое большее, на что способен обычный сотрудник - мелкое воровство: либо кража имущества родной компании, либо личных вещей коллег по работе. Расследовать и предотвращать такие преступления довольно просто. Да и ущерб от них не очень большой. Пока кто-то не украдет бумажник крупного клиента или зарубежного партнера. Обычно, если на фирме появляется воришка, то об этом становится известно довольно быстро, и персонал сам включаются в динамичную игру "поймай вора", так как сам заинтересован в скорейшей нейтрализации этой угрозы. А вот с "несунами" бороться труднее. Мелкие "несуны" не исчезли с распадом Советского Союза. Они и сейчас живут во многих организациях. Правда, об этом знают только их коллеги и бухгалтерия, которая регулярно списывает украденное имущество. Ущерб зависит от объема и рыночной стоимости товара, вынесенного ими за территорию организации или той сферы бизнеса, где работает компания. Кроме того, не стоит забывать и о таком виде воровства, как использование в личных целях предоставляемых предприятием ресурсов: средств связи, оргтехники, машин и т.д. Это так же может нанести существенный урон, особенно малому предприятию. Примеров подобного поведения может быть множество. Поэтому, никогда не помешает знать имена главных транжиров внутренних ресурсов компании.

Например, иногда таких "негативных" фактов бывает достаточно, чтобы заставить уволиться человека, которого подозревают в связях с конкурентами или криминальными структурами. Особенно если по тем или иным причинам нельзя объявить истинную причину увольнения. Такое в жизни случается значительно чаще, чем можно представить.

Ваши первые шаги по обеспечению безопасности

Вряд ли стоит лишний раз говорить о том, что для того чтобы свободно ориентироваться в ситуации надо обладать полной информацией о том что, где, когда и почему происходит или может произойти. Вы и сами знаете это, легко ориентируясь в том бизнесе, которым занимаетесь или хотите заняться.

В вопросах безопасности работает тот же самый принцип, и Вашим первым шагом по обеспечению безопасности своего бизнеса, будет установление четкого понимания того что, где и когда может Вам угрожать. И только тогда, когда вы будете хорошо представлять, в чем состоит потенциальная опасность для вашего бизнеса, вы сможете определить возможные и доступные средства защиты и методы обеспечения безопасности.

Для этого необходимо ответить на следующие вопросы:

- что необходимо охранять (имущество, информацию, ценные бумаги, непосредственно персонал фирмы)?
- кто может представлять угрозу (преступные группы, персонал самого предприятия, спецслужбы)?
- как может быть осуществлена угроза (проникновение в помещение с улицы, использование персонала в корыстных целях и т.д.)?
- сопоставимы ли стоимость охраняемых объектов и стоимость охраны?

Остановимся на данных моментах подробнее:

Прежде всего, попробуйте определить, *что* надо *защищать* и надо ли вообще что-то защищать. Определите объекты защиты. Например, Ваше предприятие занимается исключительно торговой деятельностью. Что может подлежать защите в этом случае? Конечно же, товар. Причем защита требуется всегда - в торговом зале, на складе, в дороге (при перевозке) т. д. Но, кроме того, возможно, Вы используете и свои собственные, разработанные лично Вами формы и методы продажи. Либо за время работы, Ваша торговая марка стала широко известной, и сама привлекает покупателей, т.к. является гарантий высокого качества продаваемого товара. Тогда они также должны являться объектом Вашего внимания и защиты - ведь это Ваше преимущество перед конкурентами. Не стоит забывать и о работающих у Вас сотрудниках.

Затем, ответьте на вопрос: *зачем?* То есть, другими словами Вы определите цель построения системы безопасности предприятия и задачи, которые при этом должны решаться.

В рассматриваемом нами примере торгового предприятия ответ будет выглядеть так:

Товар - требуется обеспечение сохранности, необходимо принять меры для предотвращения кражи, порчи товара, в том числе и умышленной.

Методы продажи (и другие секреты фирмы в области работы с клиентом) - требуется защита от навязчивого интереса конкурентов. Ведь именно ваша эксклюзивность обеспечивает предприятию дополнительный доход, способствует привлечению новых клиентов.

Персонал - часто возникает необходимость обеспечения физической или психологической защиты.

Следующий вопрос, на который требуется ответить - *от кого?* Ответив на этот вопрос, Вы определите источники опасности.

В рассматриваемом нами случае:

Товар требуется защищать: от покупателей-воришек (в торговом зале), от небрежности персонала (продавцов, грузчиков) - неумышленная или умышленная порча товара, от грабителей - в дороге. Кроме того, необходима защита и от природных катаклизмов - если склад, например в результате сильного ливня, будет затоплен, то Вы понесете весьма ощутимые убытки.

Секреты фирмы защищаются в основном от конкурентов, но иногда требуется защита и от не в меру любопытных собственных сотрудников.

Персонал - в основном от разного рода преступных посягательств, таких как, например: вооруженное ограбление, угроза похищения или убийства, психологический террор, шантаж, вымогательство.

И, наконец, последний вопрос - *как?* Ответив на него, вы определите, методы и средства защиты. Правда иногда, для того чтобы получить ответ на этот вопрос, требуется обратиться к специалистам.

Затем, используя результаты проведенного Вами анализа, Вы можете приступить к планированию работ по обеспечению безопасности Вашего предприятия, определить необходимые организационные и технические меры, рассчитать стоимость затрат и оценить эффективность проводимых мероприятий. При этом важно понимать, какие работы Вы в состоянии выполнить собственными силами, а в каких случаях требуется прибегнуть к помощи профессионалов

ЛЕКЦИЯ 2.
КАК АНАЛИЗИРОВАТЬ ПОТРЕБНОСТИ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ

Выработка всестороннего плана обеспечения безопасности требует методичного и продуманного анализа. Начав с общего понимания организации и дойдя до множества частных задач, вам придется применить структурный подход, чтобы собрать воедино и проанализировать этот план. Получаемые в результате рекомендации должны дополнять и поддерживать одна другую.

Задача эта не так проста, поскольку сложились уже определенные промышленные образцы таких планов. Лишь некоторые из них являются продуктом всестороннего анализа, остальные же разработаны для конкретных ситуаций применения в порядке реакции на произошедший объекте инцидент. Фактически, многие из действий охраны предназначены для производства расследования по факту события, а не для предотвращения этого события.

Объектом анализа при составлении плана безопасности являются все возможные уязвимости, которые необходимо выявлять методично и всесторонне, чтобы программа безопасности имела в основе обширный анализ, а не опыт действий по устранению последствий последнего из произошедших на объекте инцидентов. Аналитический подход позволяет гарантировать, что средства, затрачиваемые на обеспечение безопасности, расходуются в соответствии с конкретными нуждами, защищая более важные объекты и подвергая большему риску менее критичные.

Цель, однако же, состоит не в том, чтобы разработать план безопасности с высокой степенью "защиты от дурака". Стоит помнить о том, что полностью защитить объект возможно, лишь затратив несоразмерные деньги и прекратив его функционирование в целях осуществления бизнеса. Взамен этого цель ставится такая: сделать нарушение режима безопасности максимально затруднительным (но не невозможным!) для злоумышленника. Степень трудности зависит от того, насколько ценен данный объект и насколько организация-заказчик готова к рискам.

Процесс анализа делится на пять фаз - подразделение на объекты, оценка угроз, анализ уязвимости, выбор мер противодействия и их внедрение. Процесс этот рассчитан на тщательный анализ, и приступать к каждой следующей фазе следует, лишь полностью завершив предыдущую.

Подразделение на объекты

Начинается определение объектов с понимания деятельности организации в широком смысле слова, ее задач и функций, а также среды, в которой эта деятельность осуществляется. В начальной стадии анализа следует провести интервью с руководящим составом и специалистами организации, чтобы определить необходимые для осуществления ее деятельности ресурсы. В их число входит производственное оборудование, операционные системы, сырье и материалы, готовая продукция, системы учета и управления, а также инфраструктурные сети - электрические, водяные, природного газа и связи. Зачастую наиболее значимыми являются нематериальные активы, получить представление о которых можно лишь основательно вникнув в деятельность организации. В результате этого шага определяются объекты возможного нападения.

Каждый производственный объект можно разбить на более мелкие составные части. Анализ может показать, что такая детализация объекта необходима вследствие его критической важности. Примером подобного объекта может выступить информационная технология, которая делится на обширный список системных компонентов -- аппаратной части, операционных систем, прикладного программного обеспечения, систем управления базами данных, каналов связи и системной документации. И материальные, и нематериальные активы должны быть категоризированы как жизненно важные (потеря равносильна катастрофе), важные (потеря приведет к серьезным сбоям, но в принципе восполнима) и второстепенные (утрата относительно незначительна).

Оценка угроз

Всесторонний план безопасности требует определения обширного списка угроз - чтобы принять во внимание целый спектр разрушительных воздействий. Путем анализа список угроз редуцируется, чтобы сосредоточить внимание лишь на наиболее вероятных из них.

Оценка начинается со сбора данных о произошедших в прошлом инцидентах, связанных с нарушением режима безопасности, включая происшествия на охраняемом объекте, на всех объектах, принадлежащих компании, а также статистика по всей отрасли. Определите, существуют ли устойчивые образцы криминального поведения, и установите их природу. Изучите информацию о понесенных убытках, нарушениях безопасности и судебные дела, в которых фигурировала организация. Проконсультируйтесь с корпоративными юристами и изучите судебные определения, содержащие факты, имеющие отношение к безопасности. Проинтервьюируйте руководящий состав компании, страховых поручителей и руководство местных экстренных служб на предмет определения существующих угроз. Проанализируйте статистику преступности и сравните показатели с общенациональными, региональными, районными и муниципальными.

Определите виды угроз, являющихся уникальными для данного региона и данной организации, места сосредоточенного хранения опасных веществ и материалов, а также пути транспортировки, обычно используемые для доставки грузов. Прикиньте угрозы, которые ни разу не были осуществлены, но характер бизнеса и социально-политическая обстановка не исключают попыток их реализации.

Оценка угроз является процедурой качественного анализа, хотя в ней могут применяться и некоторые процедуры количественной оценки. Важно понимать, что такая оценка является валидной лишь на определенный момент времени. Изменение внешней обстановки сказывается и на спектре угроз. Следовательно, оценка должна периодически обновляться, чтобы убедиться в соответствии программы безопасности вызовам момента.

Каждую из угроз следует категоризировать как вероятную (ожидается ее событийное воплощение), возможную (обстоятельства могут привести к событию) и маловероятную (событийное воплощение не ожидается). Степень тяжести последствий вызванных реализацией угрозы событий может также подразделяться на катастрофическую (разрушительное событие), умеренную (последствия принципиально устранимы) и легкую (последствия относительно несущественны).

Анализ уязвимости

Меры противодействия, по сути, являются помехами на пути к осуществлению угрозы. Соответственно, задача этих мер - сделать событие менее вероятным, не давая возможности злоумышленнику осуществить угрозу. Однако прежде чем ставить барьеры на пути осуществления события, необходимо представить себе весь ход его развития. Анализ уязвимости представляет собой механизм создания детальных пошаговых сценариев тревожных событий.

К конструированию сценариев должны привлекаться представители организации, обладающие обширными знаниями о внутренней механике ее рабочих процессов. Рабочей группе следует смоделировать ролевое поведение преступника, осуществляющего нападение на организацию - и это позволит определить ключевые зоны ее уязвимости. Планы безопасности, способные остановить действия хорошо информированного сотрудника организации, смогут помешать пришедшему извне преступнику в равной степени - а точнее, даже в большей. Это упражнение позволит выделить зоны уязвимости и обеспечить исходные данные для следующей фазы работы над планом - выбора мер противодействия.

Анализ уязвимости создает пакеты мер защиты - то есть, основываясь на четко сфокусированной проблеме, дает пути ее разрешения путем применения контрмер безопасности. Пакеты эти лучше всего описываются путем составления электронной таблицы, в которой сопоставляются объекты и угрозы и обозначается, каким специфическим угрозам подвержен тот или иной объект.

Каждый сценарий должен сопровождаться таблицей его характеристик -- правдоподобности (не слишком ли далеко простирается действие?), последствий события и степенью приемлемого для организации риска.

Выбор мер противодействия

Точно так же, как это происходит в здравоохранении, когда самочувствию пациента может быть нанесен ущерб неправильным лечением, уровень безопасности организации может быть ослаблен либо поставлен под вопрос неверным применением мер противодействия. Выработка таких мер - скорее искусство, чем сухая наука, и потому требует объединения усилий персонала управления и службы охраны; только в этом случае способна появиться на свет программа, соответствующая нуждам организации.

В качестве мер противодействия могут выступать электронные системы безопасности, физические барьеры, охранники, политики и процедуры.

Электронные системы безопасности объединяют системы контроля доступа, обнаружения, наблюдения и сбора свидетельских показаний. В число подсистем могут входить обнаружение вторжения, тревожные кнопки, охранное телевидение, проводные и радиопереговорные устройства, громкоговорящие системы, средства индивидуальной защиты и телефонные системы.

Физические и психологические барьеры применяются для затруднения доступа к объекту. В число физических барьеров входят хранилища, сейфы, шлагбаумы, ограждения и ворота, изделия из пуленепробиваемых материалов, колючая проволока, капканы, ловушки для транспортных средств, бронезащита автомобилей, механические замки, "лежачие полицейские" и бордюры, бомбоубежища, средства освещения, щиты, панели из прочных материалов и специальные элементы ландшафта.

Персонал службы безопасности исполняет различные охранные функции, включая оперирование электронными системами, несение вахты на постах и осуществление патрулирования. Большинство действий охраны предусматривают наблюдение за событиями и - в случае инцидента - постановка в известность правоохранительных органов. В некоторых случаях охранники могут быть вооружены и иметь специальную подготовку и право вмешиваться в ход событий.

Политики устанавливают позицию управляющего звена и общий подход к практике разрешения бизнес-проблем. Процедуры определяют средства осуществления политики. Это наиболее критичная часть программы безопасности. Здесь определяются программы, необходимые для того, чтоб механизмы обеспечения безопасности работали эффективно.

Внедрение

В этой фазе рекомендации преобразуются в спецификации и инструкции, направленные на действия людей и систем, а также формирование политик. Задача внедрения - перевести план безопасности в запросы и приобретение документов, процедур, организационных программ и процессов. В СЛУЧАЕ ОПАСНОСТИ по каждому из элементов реагирования необходимо создать детальное описание предпринимаемых действий на всех четырех фазах происшествия:

ФАЗА ПРЕДУПРЕЖДЕНИЯ: Определите процедуры эвакуации и завершения работы системы, а также расположение укрытий и убежищ.

ФАЗА СОБЫТИЯ: Определите технологии укрепления и обеспечения выживания, а также методы локализации зоны инцидента - такие, как выставление нее кордонов для предотвращения возможности расширения круга участвующих в ситуации лиц.

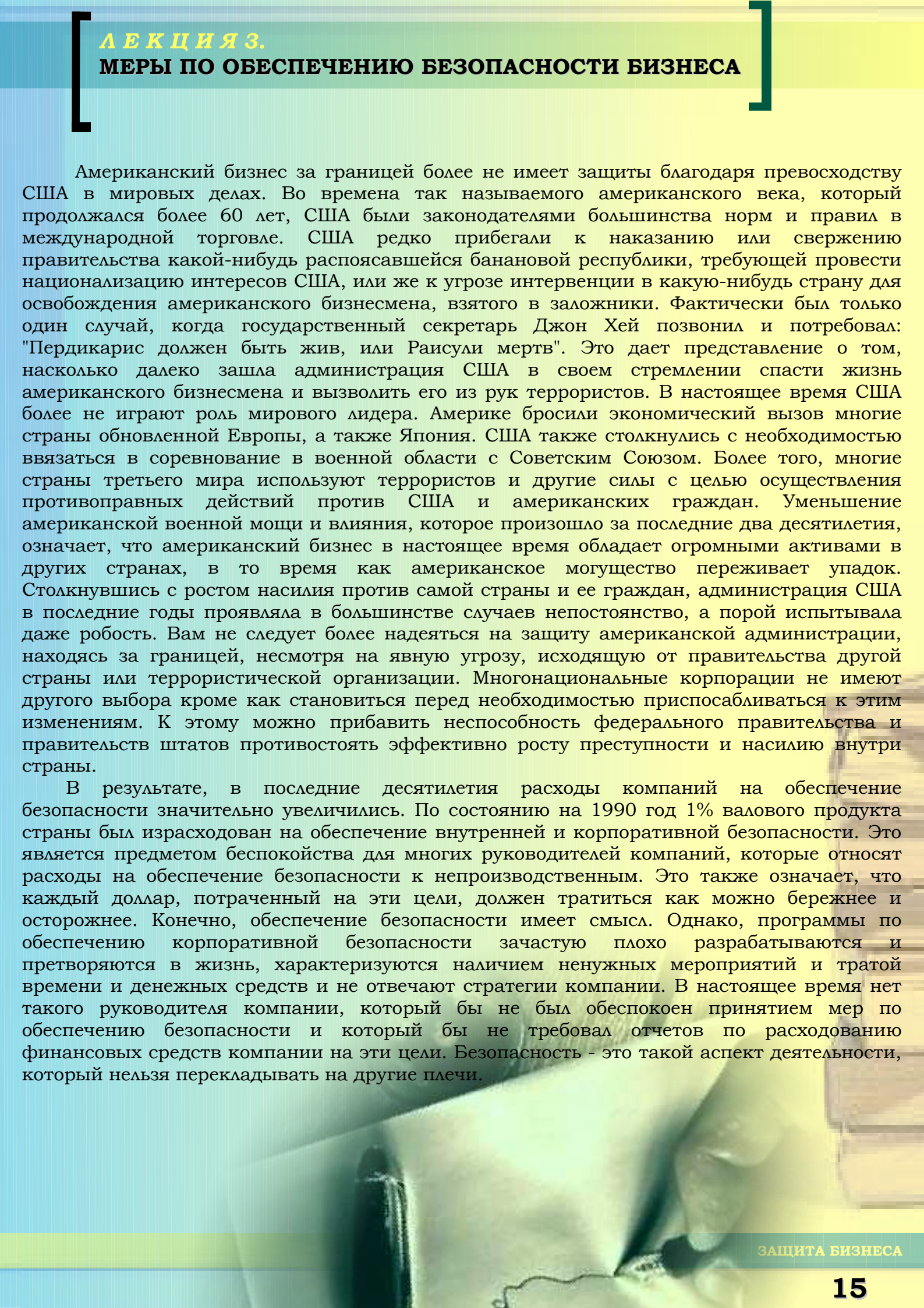
ПО ГОРЯЧИМ СЛЕДАМ: Определите процедуры оказания первой помощи, уведомления властей и экстренных служб, ограничения доступа к месту преступления, управления движением, эвакуации пострадавших и стратегию сдерживания распространения ситуации.

ПОСЛЕ СОБЫТИЯ: Определите процессы постановки в известность родственников, очистки и ремонта, деятельности на запасной территории и проведения разъяснительной работы.

ЛЕКЦИЯ 3.
МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ БИЗНЕСА

Американский бизнес за границей более не имеет защиты благодаря превосходству США в мировых делах. Во времена так называемого американского века, который продолжался более 60 лет, США были законодателями большинства норм и правил в международной торговле. США редко прибегали к наказанию или свержению правительства какой-нибудь распоясавшейся банановой республики, требующей провести национализацию интересов США, или же к угрозе интервенции в какую-нибудь страну для освобождения американского бизнесмена, взятого в заложники. Фактически был только один случай, когда государственный секретарь Джон Хей позвонил и потребовал: "Пердикарис должен быть жив, или Раисули мертв". Это дает представление о том, насколько далеко зашла администрация США в своем стремлении спасти жизнь американского бизнесмена и вызволить его из рук террористов. В настоящее время США более не играют роль мирового лидера. Америке бросили экономический вызов многие страны обновленной Европы, а также Япония. США также столкнулись с необходимостью ввязаться в соревнование в военной области с Советским Союзом. Более того, многие страны третьего мира используют террористов и другие силы с целью осуществления противоправных действий против США и американских граждан. Уменьшение американской военной мощи и влияния, которое произошло за последние два десятилетия, означает, что американский бизнес в настоящее время обладает огромными активами в других странах, в то время как американское могущество переживает упадок. Столкнувшись с ростом насилия против самой страны и ее граждан, администрация США в последние годы проявляла в большинстве случаев непостоянство, а порой испытывала даже робость. Вам не следует более надеяться на защиту американской администрации, находясь за границей, несмотря на явную угрозу, исходящую от правительства другой страны или террористической организации. Многонациональные корпорации не имеют другого выбора кроме как становиться перед необходимостью приспосабливаться к этим изменениям. К этому можно прибавить неспособность федерального правительства и правительств штатов противостоять эффективно росту преступности и насилию внутри страны.

В результате, в последние десятилетия расходы компаний на обеспечение безопасности значительно увеличились. По состоянию на 1990 год 1% валового продукта страны был израсходован на обеспечение внутренней и корпоративной безопасности. Это является предметом беспокойства для многих руководителей компаний, которые относят расходы на обеспечение безопасности к непроизводственным. Это также означает, что каждый доллар, потраченный на эти цели, должен тратиться как можно бережнее и осторожнее. Конечно, обеспечение безопасности имеет смысл. Однако, программы по обеспечению корпоративной безопасности зачастую плохо разрабатываются и претворяются в жизнь, характеризуются наличием ненужных мероприятий и тратой времени и денежных средств и не отвечают стратегии компании. В настоящее время нет такого руководителя компании, который бы не был обеспокоен принятием мер по обеспечению безопасности и который бы не требовал отчетов по расходованию финансовых средств компании на эти цели. Безопасность - это такой аспект деятельности, который нельзя перекладывать на другие плечи.



Получение корпоративной информации

От наличия информации зависит успех или неудача любого мероприятия и дела в целом. Мы живем в эпоху информатики, и любая компания, которая игнорирует этот факт, подвергает себя большому риску. Согласно данным одного исследования, проведенного недавно, 80% из 500 компаний, входящих в корпорацию "Фортчун", за последние 3 года увеличили свои расходы на сбор разведывательной информации, "Контрразведывательные операции". Не думайте, что вы живете в мире дураков, где все как в раю. Представьте себе, что ваша компания является предметом разведки ваших конкурентов, а возможно и средств массовой информации. Если ваша компания специализируется на высокотехнологических исследованиях или оборонном производстве, вы можете также стать объектом иностранной разведки. Обеспечьте свою защиту и защиту активов вашей корпорации, не только используя эффективные меры безопасности, но и создайте надежную контрразведывательную службу внутри корпорации. Не ждите, когда ваша деятельность привлечет внимание агентов промышленной разведки. Упредите их.

"Определение степени риска". Многонациональные компании требуют от международной системы если не стабильности, то, по крайней мере, предсказуемости. В бизнесе, который связан с другими странами, нельзя обойтись без риска. Поэтому ваша цель - справиться с этим риском. Как сказал генерал Паттон:

"Риск должен быть продуманным. Здесь спешить некуда". Если ваша компания имеет интересы за границей, необходимо создать группу уменьшения риска, целью которой являлась бы оценка и прогноз политических и экономических изменений в стране, уровня стабильности и насилия и других аспектов. Это даст вам возможность оценить политический риск в вашей международной деятельности и учесть этот фактор в своих стратегических планах. Если нет возможности найти специалистов для этого в вашей компании, привлеките экспертов со стороны. Такие компании как Ackerman & Palumbo, расположенная в Майами, Control Risks Ltd., в Лондоне и Risks International в Вашингтоне, округ Колумбия, предпринимают попытки вести учет террористических актов, а также оценивают и прогнозируют экономические, социальные и политические условия во всех странах мира.

"Оценка риска пребывания и деятельности компании в конкретной стране". Важным элементом прогнозирования являются ответы на следующие вопросы:

- Как стабильна политическая система страны?
- Как долго правительство этой страны будет оставаться у власти?
- Существует ли активное политическое насилие в стране? От кого оно исходит? Какие группировки вовлечены? Получают ли они внешнюю помощь? Какие цели они обычно выбирали и какие операции уже были проведены?
- Как близки отношения США с этой страной?
- Какие последствия на развитие бизнеса будет иметь насильственная смена правительства?

Уязвимые места

Угрозы в адрес вашей компании могут иметь разные формы. На первом месте стоят похищения и применение взрывных устройств. Однако этими акциями угрозы не могут быть ограничены. Человеческое воображение не имеет границ.

"Контроль инвентаря и имущества". Мелкие кражи и воровство представляют одну из самых серьезных проблем фактически для всех американских компаний.

"Обман и угрозы". Половина из всех террористических акций оказываются обманом. А если они воспринимаются серьезно (а это так и происходит), они могут оказать очень разрушительный и негативный эффект на вашу компанию, ее прибыль и моральное состояние сотрудников. "

"Саботаж и диверсии". Существует много способов по организации диверсий на производственных линиях и саботажа деятельности корпорации. В топливо или в движущиеся части механизмов могут добавляться абразивные материалы, например, песок. Могут использоваться клейкие вещества, например, сахар, который высыпается в бензобаки, в механизмы вставляться гаечные ключи. Различные детали могут ослабляться и отвертываться, чтобы создать вибрацию, что может привести к разрушению всего механизма. Саботажник может испортить измерительные приборы или вывести из строя системы предупреждения о неисправностях. Могут вводиться вирусы в компьютерные программы и компьютеры управления технологическим процессом, что может привести к остановке и простою оборудования, перегруппировке и стиранию файлов, а также заблокировать поступление важной технологической информации.

"Промышленный шпионаж". Корпоративные секреты могут быть украдены конкурентами или иностранными агентами. Этому очень трудно противостоять, т.к. физически пропажу трудно обнаружить. "Поджог". Огонь представляет постоянную угрозу для большинства фирм-изготовителей. Запасы топлива, опасных химикатов и других горючих веществ являются легкой целью для поджигателя. Также учтите возможные последствия для вашей фирмы, если будут сожжены компьютеры с файлами.

"Нападение на сотрудников компании". Террористы и преступники могут предпринять нападение на сотрудников вашей компании, которые имеют право на защиту от нападений по причине их принадлежности к компании.

"Порча изделий и продукции может иметь самые серьезные негативные последствия для компании". В результате отравлений тиленолом в 1982 году, несмотря на то, что президент компании и ее сотрудники предприняли все возможные меры по устранению последствий этих отравлений, ущерб компании составил 500 миллионов долларов.

Служба безопасности

"Нанимайте на работу людей, серьезно относящихся к делу". В общем смысле вы получаете то, за что платите. Сотрудники службы безопасности, которые получают маленькую зарплату, плохо подготовленные и не имеющие стимула в работе, вряд ли будут выполнять свои каждодневные обязанности качественно, а особенно в критические моменты. Кроме этого, это послужит причиной частых прогулов без уважительных причин, небрежного выполнения своих обязанностей и потери уважения к своей профессии и недисциплинированности. Проверка карточек безопасности, просмотр телевизионных мониторов, проверка сумок и портфелей при помощи рентгеновских установок, патрулирование требуют повышенной концентрации внимания. Большая часть работы монотонна и скучна. Охранник, работающий на контрольно-пропускном пункте и формально относящийся к делу, не рассматривая внимательно пропуска сотрудников, не выполняет своих обязанностей должным образом. Существует большое количество разных шпионских историй. Меры по обеспечению безопасности в компании TRW, ведущем военном подрядчике, были настолько слабыми, что приговоренный в последствии к тюремному заключению советский шпион Христофер Дж. Бойс рассказывал, как его непосредственный разработчик надевал маску шимпанзе на свой значок-пропуск и регулярно проходил через КПП. В другом случае сотрудник федерального правительства приклеил на свой пропуск фотографию ливийского лидера Муаммара Каддафи. На странице, где указывается принадлежность к партии или организации, он написал, что является членом организации "Исламский джихад". Охранник не обратил на это никакого внимания и пропустил его.

"Требуйте, чтобы сотрудники службы безопасности были тактичны и вежливы". Для того, чтобы хорошо исполнять свои обязанности, сотрудники службы безопасности должны быть в постоянном контакте с остальными служащими компании. Сотрудник или службы безопасности, злоупотребляющий своим положением, создает трения в отношениях, вызывает недовольство других сотрудников принимаемыми мерами безопасности.

"Проинформируйте сотрудников, с какой целью предпринимаются те или иные меры предосторожности". В этом случае не возникнет непонимания и возражений. От сотрудников, понимающих и разделяющих вашу озабоченность по поводу обеспечения безопасности, всегда можно ожидать проявления большей сознательности и помощи.

"Проследите за тем, чтобы все сотрудники службы безопасности имели хорошую профессиональную подготовку". Они должны быть способны решать каждодневные проблемы, проявляя вежливость и профессионализм. Хорошо подготовленный охранник вряд ли поведет себя неадекватно в стрессовой ситуации. Если сотрудники службы безопасности имеют разрешение на ношение и применение какого-либо вида оружия (включая полицейскую дубинку и особенно огнестрельное оружие), убедитесь, что они могут пользоваться ими, и что оружие применяется в полном соответствии с законом. Границы и случаи применения оружия должны быть оговорены и утверждены руководством, юрисконсультом и начальником службы безопасности компании. Помните, что охранник неподготовленный к рукопашному бою может применить в случае опасности оружие. Личный состав службы безопасности должен быть хорошо подготовлен также и для того, чтобы иметь инициативу в критической ситуации. Сотрудники службы безопасности должны знать все уязвимые места компании и периодически осуществлять оценку возможной угрозы. Хорошо подготовленный охранник также должен знать основы оказания первой медицинской помощи и способы пожаротушения.

*"Рутина и скука - враги хорошей службы безопасности".*Механическая часто повторяющаяся работа притупляет реакцию личного состава службы безопасности и приводит к невнимательности. Оставленные на долгое время на изолированных постах сотрудники службы безопасности утрачивают бдительность и становятся уязвимыми для внезапных нападений. По возможности меняйте их каждодневные обязанности. Устраивайте частые тренировки и учения. Чем их больше, тем лучше, т.к. это не только оттачивает их навыки, но и поддерживает моральный дух. Вы должны чаще проверять их бдительность и реакцию. Не информируйте служащих компании о запланированной учебной попытке сотрудников службы безопасности прократься на ваш завод или в головной офис или же попытайтесь пройти КПП с фальшивым пропуском и под различными предлогами. Припаркуйте подозрительную машину около здания и проследите, как долго она не будет замечена службой охраны, и какие меры они предпримут в этой связи. Проследите, могут ли посторонние люди получить доступ к секретной документации и главному производственному оборудованию.

"Дайте почувствовать сотрудникам службы безопасности, что их работа важна". Существует тенденция относится к сотрудникам службы безопасности как к огнетушителю, запрятанному где-то за стеклянной дверью и необходимому только в крайнем случае. Это не правильно. Сотрудники службы безопасности должны знать, что они являются частью компании, важным элементом производства продукции и услуг, которые вы продаете, и не менее важными, чем инженерно-технический состав, исследователи рыночных условий и юристы. В любой ситуации не относитесь к сотрудникам службы безопасности, как к носильщикам или просто, как: к неквалифицированным рабочим, которым можно поручить любую грязную работу. Если вы не будете к ним относиться как к профессионалам, они также непрофессионально будут действовать в критической ситуации.

"Не подвергайте сотрудников службы безопасности необоснованному риску". Хорошо укрепленная будка и телевизионная камера с замкнутым контуром уменьшат степень уязвимости охранников и позволят им оперативно и четко отреагировать на внезапное нападение или на другую опасность. Более того, охранники, несущие службу на внешних постах, у ворот или других стратегических объектах, будут более бдительны и полезны, чем когда они будут не защищены. Охранник, выполняющий часами свои обязанности под проливным дождем или под палящим тропическим солнцем, будут больше беспокоиться о своем состоянии, чем заниматься проверкой пропусков и осмотром машин.

"Регулярно интересуйтесь мнением сотрудников службы безопасности". Никто не может знать лучше сотрудников службы безопасности, есть ли уязвимые места в системе безопасности вашей компании.

Охрана территории

"Забор". Не ждите, пока опасность проникнет в здание вашей компании. Все объекты должны быть обнесены двойным забором, чтобы опасность не распространилась на вас, ваш офис или производственные цеха. Забор позволит охранникам контролировать доступ к важным объектам.

"Забор должен быть бетонным". Сверху на заборе можно укрепить колючую проволоку. Но помните, что злоумышленник может набросить сверху одеяло или одеть на себя толстую плотную одежду. "Комбинируйте участки с забором с датчиками". Датчики (инфракрасные, датчики движения и т.д.) определят, когда и где незнакомец проник на вашу территорию. При выборе и установке датчиков необходимо исходить из принципа их надежности. Система, которая выдает слишком много ложных тревог, в конце концов заставляет охранников не обращать никакого внимания на эти сигналы. Также можно установить телевизионные камеры с закрытым контуром в важных местах вдоль забора.

"Ограждения должны образовывать "обстреливаемую" зону". Они должны опоясывать территорию и образовывать участки голой земли вокруг определенных объектов, т.е. злоумышленнику придется пересекать этот участок, не имея возможности укрыться где бы то ни было. Имейте это в виду и установите ограждения на некотором расстоянии от здания или других препятствий с тем, чтобы облегчить охранникам наблюдение за злоумышленником.

"Запомните, что препятствия не остановят злоумышленника, если у вас нет специального подразделения для патрулирования". Заборы и стены не остановят злоумышленника. Они просто затруднят его продвижение и сделают его уязвимым. Поэтому по мере возможности необходимо иметь специальное подразделение, которое бы осуществляло периодическое патрулирование территории с целью выявления и задержания нарушителя.

"Высокая многозвенная стена может выдержать взрывы гранат и даже управляемых снарядов, однако целесообразнее укрепить ваши здания". В результате взрыва гранаты или управляемого снаряда осколки разлетятся по обширной территории.

"Создайте глубоко эшелонированную оборону". Создайте дополнительные зоны или участки обороны вокруг важных объектов, таких как компьютерный центр, склады, в которых хранятся горючие материалы, а также вокруг головного офиса.

"Устройте дополнительные пути отхода". Если ваша территория представляет собой большое поместье или плантацию, постройте дополнительные дороги вокруг периметра территории для машин службы безопасности. Если это возможно, покрытие дороги должно быть твердым и проходимым в любую погоду, т.к. террористы могут воспользоваться холодной погодой, чтобы незаметно напасть на ваш объект. Срубите кустарник и деревья по обе стороны дороги для того, чтобы террористы не смогли устроить засаду.

"Сократите количество брешей в вашей системе обороны". Чем меньше входов, тем больше внимания сотрудники службы безопасности будут уделять определенным участкам. Нарушители могут легко прорваться через ворота, охраняемые одним человеком, или же проскользнуть, когда его внимание будет отвлечено. Сократите количество ненужных входов-выходов и сконцентрируйте основные сипы на оставшихся точках.

"Продумайте меры по выявлению нарушителей, прячущихся за машинами, въезжающими на территорию, или под их днищем". Все ворота для въезда машин должны находиться в зоне видимости охранника или телевизионной камеры. Еще лучше, если все въезжающие и выезжающие машины осматривались охранниками. Для осмотра днища машины на предмет наличия взрывных устройств или "нежданных гостей" рекомендуется пользоваться зеркалом, укрепленном на шесте.

"Обозначайте заборы". В зависимости от законов страны пребывания вы будете нести ответственность за причинение физического ущерба лицам, пострадавшим из-за ваших заграждений. Колючую проволоку или мотки проволоки можно легко увидеть, однако рекомендуется повесить или прикрепить яркие полоски материала, чтобы они были видны еще лучше. Также необходимо через интервалы пометить специальными знаками участки забора, находящиеся под напряжением.

Освещение

Если ваши сотрудники службы безопасности не имеют приборов ночного видения, они в основном будут полагаться на свое зрение для выявления нарушителей. Свободная зона между двумя рядами забора должна освещаться прожекторами, не образующими тени в местах, где могут укрыться злоумышленники. Обеспечьте дополнительное освещение вокруг постов охраны, чтобы нарушитель не смог спрятаться за ними. Также обеспечьте освещение КПП с тем, чтобы охранники могли видеть, что они делают, но не следует делать слишком много яркого света, т.к. яркий свет помешает тем, кто выполняет здесь какие-либо работы.

"Охранники не должны находиться в местах, где отбрасывается их тень, чтобы не стать целью для снайпера". Охранники должны иметь возможность видеть и наблюдать и быть при этом незаметными. Разместите осветительные приборы так, чтобы они были направлены на злоумышленника и так, чтобы он по возможности не видел, что происходит на территории. В этом случае охранники будут находиться в тени.

"Увеличьте эффект, создаваемый осветительными приборами, раскрасив здания и стены яркой краской". В этом случае будет легче обнаружить нарушителя, одетого в темную одежду. К тому же, ярко окрашенные предметы и строения отражают больше света и тем самым как бы увеличивают мощность ваших ламп. Темные строения поглощают свет и для их освещения требуются более мощные лампы для поддержания такого же уровня освещения.

"Обобщение". Ваша служба безопасности обнаружит нарушителей по их движениям и по световым контрастам, которые они создают. Широкие, чистые участки вокруг ваших объектов, правильно установленное освещение и световые контрасты являются важными элементами обеспечения надежной системы безопасности.

Системы сигнализации и замки

В продаже имеется большое количество различных систем сигнализации. Вам, конечно, расскажут о преимуществах каждой системы, но мне хотелось бы остановиться на их недостатках.

"Системы сигнализации с током, проходящим через провод или полоску металлической фольги". Когда окно или дверь, защищенные таким образом, открыты, провод или контакт фольги обрываются, прерывая поступление тока и включая систему сигнализации. Несмотря на то, что данный тип системы прост по конструкции и довольно дешев, нарушитель может зашунтировать ток, используя свой собственный провод. Кроме этого, он может обойти всю систему, обрезая провода, проложенные по периметру, от отштукатуренных стен. Такая система даст сигнал сотрудникам службы безопасности, что кто-то пытался проникнуть внутрь территории и действительно проник. Но эта система не поможет обнаружить злоумышленника.

"Системы, применяющие инфракрасный луч света, которые при поломке издают сигнал тревоги". Этот тип системы надежен и прост в обращении. Система используется в зонах, которые нельзя закрыть при помощи дверей или стен. Она также может быть использована для обнаружения пожара. Однако эту особенность не нужно переоценивать, т.к. лучи обычно ложатся близко к земле, а не к потолку, где, как правило, собирается дым. Имейте в виду, что от пыли или дыма инфракрасные системы сигнализации могут самопроизвольно включаться. Более того, если они установлены на улице, дождь, листья, кусты или звери могут спровоцировать их включение.

"Ультразвуковые и микроволновые системы сигнализации". Эти системы передают сигнал в помещение, а затем прослушивают часть отраженного сигнала, любое движение в комнате исказит сигнал и включит звуковую сигнализацию. При помощи этих систем можно обнаружить присутствие нарушителя, но если он двигается медленно или ползет ниже столов и стульев, он может обойти систему сигнализации. Кроме этого, некоторые материалы поглощают звук и, если на вашем объекте много предметов, изготовленных из такого материала, это создаст трудности в использовании системы. И наконец, воздушные потоки, создаваемые кондиционерами и отопительными приборами также могут привести к ложному срабатыванию системы сигнализации.

"Системы, определяющие звуки с использованием микрофона". В эту систему можно вставить микрофон для того, чтобы услышать кто или что включает систему. Системы этого класса легко включаются от вибрации и шума, идущего с улицы или от пролетающих самолетов. Поэтому их можно применять только в отдельно стоящих зданиях или на удаленных объектах. Частые ложные срабатывания системы могут заставить охранников уменьшить уровень чувствительности, тем самым позволив нарушителю пробраться незамеченным. Будьте осторожны и не подслушивайте сами себя. Любой микрофон, установленный в вашем офисе, может быть использован как подслушивающее устройство. Сотрудники службы безопасности вашей компании смогут подслушивать ваши разговоры в помещениях, защищенных такой системой.

"Электромагнитные системы сигнализации". Электромагнитные системы сигнализации создают электронное поле вокруг незаземленного металлического объекта и издают сигнал предупреждения при нарушении этого поля. По сравнению с вышеупомянутыми системами данная охранная система имеет меньше недостатков.

"Дополнительные источники питания". Как и другое высокочувствительное оборудование система сигнализации должна иметь резервный источник питания для обеспечения постоянного функционирования вашей системы обороны в случае, если противник обрежет все силовые кабели. Подумайте о применении дополнительных приспособлений, которые можно было бы использовать в ваших системах сигнализации.

"Установка и обслуживание систем сигнализации". Рынок охранных систем в США нестабилен. Кроме этого, большинство охранных систем очень дороги, а конструкции и качество изготовления не отвечают требованиям, поэтому будьте осторожны при покупке. Проверьте историю компании, которую вы рассматриваете в качестве поставщика. Как долго существует эта компания? Предоставят ли они вам ссылки на других своих клиентов, которые были бы удовлетворены качеством их оборудования, продадут ли они вам лучшие образцы оборудования, которые имеются на рынке, или же оборудование, в распространении которого эта компания является только дилером? Отвечает ли каждая система вашим специфическим требованиям или же компания просто изготавливает систему по уже отработанному шаблону? В крайнем случае получите несколько предложений от нескольких компаний и убедитесь в том, что вы понимаете принцип работы каждой предложенной системы. Особенно ее преимущества и недостатки с тем, чтобы прийти к обоснованному решению. Запомните, что дешевая система не обязательно означает лучшую или рентабельную систему. Остерегайтесь компаний, которые предлагают системы по искусственно заниженным ценам, а затем увеличивают цену за обслуживание и другие накладные расходы. В конечном счете вашей целью является приобретение наиболее эффективной и надежной системы.

"Меры по недопущению создания помех в кабелях, проложенных от охранных систем к постам". Ваш консультант по вопросам безопасности может порекомендовать вам несколько способов решения этой проблемы. Можно установить устройства для определения падения или скачка напряжения, вызванного установкой шунтирующего устройства. Вы также можете присоединить при помощи провода электропроводящую фольгу к охранной системе. Провода лучше спрятать или поместить в оплетку или чехол.

"Ключи". Ко всем замкам можно подобрать ключи, поэтому не облегчайте задачу нарушителям. Ведите счет всем ключам, особенно дубликатам, которые должны храниться в службе безопасности. Проводите периодическую инвентаризацию ключей. Необходимо тщательно охранять ключ-отмычку, которым можно открыть почти все замки, и сделать на нем специальные отличительные надписи (например, "Укради меня"). Помните, что ко всем замкам, сконфигурированным под универсальные ключи, можно намного легче подобрать ключи, чем к другим замкам, поэтому не создавайте себе проблемы - покупайте замок без ключей-отмычек.

"Приобретайте замки и охранные системы, которые можно переделать". Наиболее частой причиной необходимости переделки замка является лишение бывшего сотрудника доступа к документации компании. Поэтому приобретайте замки со съемными запорами. Кроме этого, большинство ультразвуковых и электромагнитных систем сигнализации поступают в продажу в модулях, которые в зависимости от предназначения можно сменить или добавить при необходимости.

Сотрудники

"Проверяйте всех сотрудников, включая руководство компании". Недавно после проведения анализа в одной фирме, находящейся в Нью-Йорке, было обнаружено, что 50% резюме руководящих работников имели явно преувеличенную информацию. Некоторые просто не соответствовали истине от начала до конца. Поэтому целесообразно проверять прежние должности, места работы и квалификацию ваших потенциальных сотрудников. Также полезно узнать о том, употребляют ли ваши сотрудники наркотики, алкогольные напитки и имеют ли другие вредные привычки, которые могут негативно сказаться на их производительности. В некоторых странах важно также знать, кого вы нанимаете. Известные террористы проникали в многонациональные компании перед совершением террористических актов.

"Использование детектора лжи". Хотя использование детекторов лжи является для многих организаций и компаний спорным вопросом, автор данного руководства является сторонником проведения регулярного тестирования всех сотрудников компании на детекторе лжи. Конечно, нельзя уволить сотрудника только на основании результатов тестирования, проведенного на детекторе лжи. Однако детектор лжи может указать вам на какую-то негативную сторону сотрудника, которую можно проверить, используя другие методы. Кроме этого, факт использования детектора лжи часто служит сдерживающим фактором для потенциальных воров, промышленных шпионов и террористов, которые исследуют возможность проникновения в вашу компанию или организацию. Относитесь с осторожностью к временным рабочим в связи с тем, что проверить прежнюю деятельность временных рабочих порой достаточно трудно, проследит за тем, чтобы за их работой и поведением постоянно наблюдали их непосредственные начальники и начальник службы безопасности компании. У этих рабочих должны быть отличные от других сотрудников таблички с указанием их имени и должности. Такие таблички не должны давать им доступ на ключевые объекты вашей компании. Субподрядчики и их персонал также должны иметь специальные таблички, по которым можно определить их принадлежность к той или иной компании-субподрядчику и должность. Они должны находиться под постоянным наблюдением сотрудников службы безопасности и сопровождаться ими для работы в наиболее важных местах компании. Данной категории рабочих и служащих не рекомендуется давать разрешение на свободное перемещение по территории вашей компании.

"Увольняйте сотрудников, которые нарушают правила безопасности". Если сотрудник, нарушивший правила безопасности, увольняется, не понеся наказания, другие сотрудники могут последовать его или ее примеру.

ЛЕКЦИЯ 4.
ФУНКЦИИ И ЗАДАЧИ СЛУЖБЫ ПЕРСОНАЛА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Введение

Сегодня мы вместе с вами рассмотрим и проанализируем содержание основных функций службы персонала в разрезе кадровой безопасности.

Начнем с того, что сгруппируем функции по блокам, каждый из которых, в свою очередь, напомним перечнем мер или мероприятий, прямо или опосредованно влияющих на состояние кадровой составляющей экономической безопасности предприятия. Здесь необходимо отметить, что службе персонала не принадлежат все без исключения рассматриваемые ниже функции обеспечения безопасности, однако организация либо действенное участие этой столь важной службы в описываемых мероприятиях все же необходимо для достижения наилучшего результата. Кроме того, постановка и выполнение указанных далее задач в рамках этого функционала является основополагающим моментом для управления безопасностью по кадровой составляющей, дает необходимый базовый инструментарий для разработки и внедрения перечисленных далее мероприятий.

Полномочия

Безусловно, для правильного восприятия своей роли в обеспечении жизнедеятельности компании служба персонала, ее ключевые сотрудники должны быть, в известной мере, наделены соответствующими полномочиями в сфере обеспечения экономической безопасности. Прежде всего, эти полномочия просто должны быть. Реальные, они должны быть публично делегированы и документированы. Роль носителя этих полномочий сама по себе должна четко пониматься сотрудниками этого подразделения. Кроме того, представляется значительным понимание этого факта руководителями бизнеса. Ведь службы персонала – это не отдел кадров советских времен, это не механизм по приему на работу и увольнению, это один из важнейших ресурсов предприятия по обеспечению его устойчивости на рынке. На всех уровнях должно декларироваться: “Служба персонала обеспечивает безопасность”. В ходе семинаров по кадровой безопасности, которые проводятся автором, слушатели из числа директоров или менеджеров по персоналу часто - кто с надеждой, а кто и безнадежно - говорят: “Ваши бы слова о нашей значимости да руководству в уши!”, “Сюда надо сначала руководителей приглашать, а потом нас, им сперва надо “мозги вправить”.

Таким образом, мы вынуждены отметить у руководителей, к сожалению, низший уровень владения таким ресурсом, как служба персонала, в целях обеспечения всесторонней безопасности предприятия.

Одним из согласованных полномочий при обеспечении кадровой безопасности должен быть непосредственный доступ должностных лиц службы персонала к необходимым для этого корпоративным ресурсам. Эти ресурсы очевидны: планы стратегического развития (или стратегические планы развития) компании, информационные массивы, в том числе конфиденциального характера, аналитика, внутрифирменные и внешние исследования, финансы на соответствующие программы кадровой безопасности (на привлечение квалифицированных кадров, на управление лояльностью) и т.д.

Следующее полномочие заключается и в праве, и в обязанности службы персонала участвовать в разработке документационного обеспечения безопасности. В Трудовом Кодексе РФ, например, прямо указан ряд документов, непосредственно влияющих на безопасность предприятия, и служба персонала как раз обязана обеспечить их наличие, правильность, работоспособность и отсутствие негативных юридических последствий. К таким документам, в первую очередь, относятся:

- трудовой договор;
- правила внутреннего трудового распорядка;
- договор о полной индивидуальной (коллективной) материальной ответственности;
- документация по охране труда и пр.

Кроме того, в состав “бумажного” обеспечения безопасности, находящегося в прямой компетенции службы, входит документирование дисциплинарной практики на предприятии и в подразделениях.

Правом же службы персонала в рамках данного полномочия является участие - прямое или косвенное, инициативное или экспертное - в работе по созданию иной документации, связанной с безопасностью, например, пакета документов по обеспечению сохранности конфиденциальной информации или положения о внутрифирменной “горячей линии”.

Когда мы говорим о полномочиях, нелишне сказать и о том, что на предприятии должно быть регламентировано и описано распределение компетенции в рассматриваемой области с коллегами из службы безопасности и других подразделений. Иногда для этих целей создается документ, который так и называется - “Положение о взаимодействии в области обеспечения безопасности”.

Взаимодействие

Конечно, результативность в системе кадровой безопасности немыслима без четкого и эффективного взаимодействия подразделений. Исходя из принципов разделения полномочий и распределения компетенции, в каждой компании должны быть выстроены горизонтальные связи управления активами (временем, финансами, людьми, информацией) между службой персонала и другими службами и отделами.

Взаимодействие со стороны службы безопасности, как правило, если судить по наиболее часто приводимым ответам слушателей семинаров из числа менеджеров по безопасности, сводится только к вопросам проверки кандидатов. Действительно, такие проверки разносторонни, и мы перечислим здесь основные:

- пресловутая проверка по “милицейским” учетам – наличие судимости, наложение существенных административных взысканий, утеря паспорта, наличие розыскных дел;
- проверка рекомендаций с прошлых мест работы через службы безопасности тех предприятий или легендированно;
- проверка соответствия регистрации по месту жительства (пребывания);
- проверка кредитной истории через службы безопасности или кредитные отделы банков, предоставляющих потребительские и иные кредиты;
- проверки на наличие связей в криминальном мире, в том числе через родственников;
- проверка наличия недвижимого и движимого (автомобилей) имущества, в том числе на соответствие заявленному;
- проверка участия в капитале (учреждение, акционирование) юридических лиц, как коммерческих, так и некоммерческих, в т.ч. общественных организаций;
- проверка предоставляемых документов (диплом, паспорт) на соответствие формы и содержания действительности и т. д.

Более подробно о такого рода поверках мы с вами поговорим в будущем. Сейчас же отметим, что, кроме проверок, есть и другие виды взаимодействия со службой безопасности, и это взаимодействие также многогранно. Например, сотрудничество при оценке благонадежности как кандидатов, так и сотрудников, постоянный обмен неофициальной информацией, участие в разработке программ физической защиты персонала, участие службы безопасности в процедурах увольнения работников, совместное участие в комиссиях при разбирательствах по материальной ответственности и т.д. Вопросы взаимодействия именно со службой безопасности, как с профильным подразделением, будут проходить красной нитью через всю нашу тему, и мы еще к этому не один раз вернемся.

Взаимодействие с финансовыми подразделениями должно быть налажено при решении вопросов текущих задолженностей сотрудников, что важно при подготовке к увольнению, в процессе планирования корпоративных финансовых ресурсов на обеспечение кадровой безопасности (обучение, мотивация, страхование и пр.), при расчете и начислении заработной платы и других элементов компенсационного пакета.

Взаимодействие с указанными подразделениями не такое простое, как кажется на первый взгляд. Директору (менеджеру) по персоналу должен уметь ясно и аргументированно доказать необходимость выделения достаточных на мероприятия кадровой безопасности средств в рамках отведенного бюджета и четко указать при этом цели, которые могут быть достигнуты этими мероприятиями. Далеко не всем и не всегда это удается.

Взаимодействие с субъектами процесса развития. Так несколько неожиданно обозначены руководители учебных центров, тренеры, консультанты, психологи и другие специалисты, принимающие участие в том или ином виде образования сотрудников компании. Обучение – это развитие компании, упрочение ее конкурентоспособности, безопасности и устойчивости на рынке. Именно так надо позиционировать рутинное обучение (может, тогда и денег больше выделят?). То есть, само по себе обучение в разных формах – уже усиление кадровой безопасности, и служба персонала планирует и организует эту работу.

Но есть и еще более тонкие элементы взаимодействия с этими субъектами. Автор часто приводит один пример такого взаимодействия: тренеру, проводящему тренинг по продажам с отделом сбыта компании, ставится задача, связанная с выявлением наиболее ярких и активных участников тренинга, с оценкой уровня авторитета руководителя отдела как формального лидера, с выявлением других лидеров в коллективе, может, более сильных, нежели руководитель, с оценкой общего “морального” климата в коллективе и т.п. Ведь эта информация вам нужна? А ценность ее еще и в том, что оценку проводит внешний независимый специалист, часто даже на уровне просто здравого смысла. Более того, постановка такой задачи имеет форму “обратите внимание”, а отработка ее ничего не стоит для вашей компании. И такие моменты взаимодействия существуют везде, надо только обратить внимание на пропагандируемый здесь подход к рассмотрению этих вопросов.

Взаимодействие в области кадровой безопасности с профсоюзными организациями на сегодняшний день очевидно - по вопросам отражения в коллективных договорах прав и обязанностей работников в сфере обеспечения экономической безопасности предприятия, по вопросам участия профкома в процедурах увольнения и других случаях, более или менее регламентированных трудовым законодательством. Хотя и здесь тонкостей много. Для примера - ситуация, сложившаяся на одном из государственных предприятий, руководство которого автор консультировал по системе экономической безопасности. При изучении документации, имеющей отношение к кадровой безопасности, пришлось “проштудировать” коллективный договор. После его изучения автору захотелось навечно остаться работать на этом предприятии, потому что работодатель обязан предоставлять работникам в соответствии с этим документом такие блага, что можно было особенно не работать – только на работу ходи! Компенсационный пакет можно было смело назвать “динозавром”, вышедшим из советских времен - такой не каждому западному предприятию и приснится! “Полный шоколад”, как сейчас принято говорить, и аплодисменты председателю профсоюзного комитета. Налицо явный перекос обязанностей работодателя перед работниками при отсутствии какой-либо адекватной ответственности работников перед работодателем. А это уже угроза не только кадровой, но и экономической безопасности в целом. Хорошо, что на тот момент готовился проект новых правил внутреннего трудового распорядка, и автору пришлось включиться в эту работу, чтобы установить хоть какой-то баланс, скомпенсировав неравенство ограничениями и расширенными правами работодателя именно в этом документе. Так что конструктивное взаимодействие и с профсоюзными организациями, имеющими авторитет в коллективе, надо лелеять и поддерживать.

Коммуникации

В этом блоке функций рассматриваются близкие к взаимодействию, но все же отличающиеся от него вопросы налаживания особых, “безопасных” отношений с внешними или внутренними субъектами - благоприятных, полезных и доверительных отношений.

Здесь, в первую очередь, необходимо выделить наличие прямого выхода на руководство предприятия при получении сигнала о нарушении в системе кадровой безопасности. Выход должен быть не только прямым, т.е. без посредников, но и оперативным, экстренным при надобности. Не забудем также и оперативную связь руководителя службы персонала с начальником службы безопасности.

Важен также коммуникационный канал, который направлен на поддержание благожелательных контактов с территориальными органами инспекции по труду. Зачем? Не только для налаживания “хороших” связей, но и для получения “горячей” информации об изменениях в трудовом законодательстве, о трактовке этих новаций самими инспекциями и т.д. Кроме того, эти связи нам нужны для превентивной работы по предотвращению убытков предприятия в виде штрафов, накладываемых государственными инспекторами по труду и по охране труда. Неумение налаживать и поддерживать такие коммуникации дорого выйдет “некоммуникабельному” менеджеру по персоналу. В связи с этим обратите внимание на то, что в последнее время законодательство усиливает роль государственных инспекций, предоставляя им новые права и полномочия. Не секрет, что часто эти органы используются, в том числе, в целях конкурентной борьбы, и здесь от уровня и глубины отношений зависит многое.

То же самое и с военкоматами. Их роль и влияние на бизнес в последнее время также усиливаются. Бытуют истории, когда несговорчивого партнера с помощью коррумпированных представителей военкомата “упекали” не только на военные сборы, но и призывали на действительную военную службу. И хотя конкретно в этих случаях необходимо подключаться службе безопасности, есть вопросы попроще, но не менее значимые, ответственность за которые несет служба персонала. Штрафы за нарушение воинского учета пробовали? Это тоже ущерб, это тоже ваша ответственность. Это нарушение кадровой безопасности. С вашего предприятия прямо с рабочего места увозили сотрудников на призывной пункт? Значит, вам не удалось их уберечь – это тоже ваша ответственность. Это нарушение кадровой безопасности. Можно еще перечислять проблемы, возникающие во взаимоотношениях с людьми в погонах, однако лучше с этими людьми дружить.

Коммуникации с профессионалами рынка труда - *head-hunters*, рекрутерами, кадровыми агентствами. Вы скажите: “Да, мы знаем, что они с точки зрения безопасности нам тоже кое-что должны, а именно, проверять кандидатов и стараться поставлять благонадежных”. Но это далеко не все. Обратите внимание, что можно приобрести, имея доверительные отношения с вашим постоянным партнером – кадровым агентством, например. Можно получать (при определенных условиях) информацию о параметрах мотивации и реальных составляющих компенсационного пакета у конкурентов, о новых проектах и открывающихся направлениях деятельности конкурентов (что не всегда видно из массированных объявлений о приеме на работу ввиду их отсутствия по причинам коммерческой тайны), другую информацию - вплоть до сведений, что иное предприятие “заказало” на вашем специалиста (профилактика переманивания).

Мониторинг

Мониторинг, то есть отслеживание определенных параметров, а в нашем случае – видов информации, является одной из важнейших функций службы персонала при обеспечении кадровой безопасности компании.

Мониторинг каналов неофициальной (кулуарной) информации – задача, которая должна не просто присутствовать, она должна быть четко обозначена, а на ее отработку должны выделяться особые средства и силы (люди, время и место).

Контроль неформальных информационных потоков осуществляется различными способами для отслеживания общего уровня мотивации, выявления неформальных лидеров, признаков падения авторитета руководства, получения любой иной информации, вплоть до конкретных виновников внутренних преступлений. К слову, западный опыт сравнения адекватности различных источников информации показывает, что самый результативным источником, например, о внутрифирменных нарушениях и злоупотреблениях являются частные сообщения служащих. Отечественный опыт автора подтверждает такую статистику. Контроль слухов очень важно для выполнения задач кадровой безопасности!

Мониторинг изменений в законодательстве. Пропустить принятие нового Трудового кодекса РФ мы, конечно же, не могли. А вот отследить новации связанного с ним налогового и пенсионного законодательства, законодательства о персональных данных, изменения и дополнения нормативных правовых актов, затрагивающих трудовые отношения, удается не всегда. Инициируйте такую задачу вашему юридическому отделу. Упущения на этом участке работы также дорого стоят.

Мониторинг рынка труда. Частично мы уже затронули эту тему в разделе о коммуникациях. Здесь вы самостоятельно, с помощью имеющихся у вас ресурсов в виде информации, отслеживаете условия труда и мотивации у конкурентов, состояние рынка труда по “горячим” вакансиям, уровень безработицы в регионе и т.д. И не говорите, что это неблагодарная работа – она воздастся сторицей! Нередки случаи, когда специалисты предприятия не отслеживали вовремя ситуацию и, как следствие, предприятие “выпадало из рынка труда” тогда, когда производство или сбыт требовали усиленного кадрового потенциала в короткие сроки, но условия мотивации не менялись. Народ не идет, и получается серьезный провал с крупным ущербом и миллионами упущенной прибыли.

На схеме вы можете видеть и такую задачу как мониторинг уровней лояльности. Да, должна быть и такая. Ее выполнение связано с проведением периодического тестирования “на лояльность” кандидатов и работников предприятия специальным инструментарием, оценкой сотрудников и отслеживанием динамики изменений. Таким образом, мы можем достигать несколько целей: оценивать эффективность существующих средств мотивации, фиксировать изменения уровня лояльности людей и подразделений в целом, определять меры по коррекции ситуации.

Конфликтология

Конфликты на предприятии, в коллективах логично рассматривать с точки зрения кадровой безопасности. За редким исключением конфликты, как межличностные, так и организационные, могут рассматриваться как угрозы безопасности. Поэтому знание если уж не всей дисциплины, то, по крайней мере, основ конфликтологии, обязательно для менеджера по персоналу, тем более, что литературы и соответствующих курсов сейчас довольно много.

Кроме общей конфликтологии, мы выделяем и специальный ее вид – конфликты персонала с сотрудниками охраны и безопасности. Последние по своему профилю своему имеют прямое отношение к безопасности, и порождаются они различием в статусе конфликтующих, например, тогда, когда топ-менеджер вынужден подчиняться простому охраннику.

Контроль

Изучив и уже установив в компании ряд процедур кадровой безопасности, служба персонала обязана и вынуждена контролировать выполнение сотрудниками и смежными подразделениями этих процедур. Принцип постоянства и всеобъемлемости контроля работает и здесь. Его важность также проиллюстрирована на схеме.

ЛЕКЦИЯ 5.
ДИВЕРСИОННЫЙ АНАЛИЗ КОМПАНИИ

Каждый начальник желает знать: откуда может прийти беда? Будет ли это ошибка бухгалтерии? Или не сработает сигнализация на складе? Что вы будете делать, если ведущий менеджер компании вдруг уйдет налево вместе с клиентской базой? А вдруг, наоборот, обороты компании вдруг вырастут вдвое? В пять раз? Где именно компания треснет?

Традиционная боязнь руководителя компании – "пакости со стороны зловредных конкурентов". Конечно, образ "внешнего врага" необходим, чтобы поддерживать коллектив фирмы в тонусе. Но, как известно, наш главный враг – мы сами, и наибольшая опасность исходит изнутри. Ряд экспертов утверждает, что собственные сотрудники могут нанести своей фирме гораздо больший ущерб, чем конкуренты...

Итак, вот проблема: когда в компании всё вроде бы благополучно – как определить, откуда ждать удара? И дальше: как смоделировать провал, чтобы "не слишком проваливался"? Чтобы предупредить диверсии, приходится самим строить версии. Сегодня мы поиграем в шпионов.

Знай своего врага

Один сотрудник компании-провайдера тратил большую часть рабочего времени, используя корпоративное оборудование в своих целях – в частности, качал из Интернет кинофильмы, закатывал их на CD-болванки (которые списывал как бракованные), печатал на корпоративном принтере обложки к ним, через корпоративный же Интернет давал объявления на соответствующих сайтах ("mpeg4-видео оптом недорого") и неплохо зарабатывал. В конце концов уволенный (как он считал, несправедливо) сотрудник унес с собой пароли к серверу, которые по халатности не поменяли. В течение полугода он раздавал своим знакомым "халявный" интернет, а сам, никем не замеченный, вовсю удаленно хозяйничал на бывшем рабочем месте – сделав себе сайтик и продолжая свой маленький бизнес на ресурсах бывшего работодателя.

"Какой негодяй!" – скажете вы. Это эмоциональная реакция. А реакция с точки зрения бизнеса – как сделать, чтобы подобные ситуации не повторялись?

В прошлом мы уже говорили о методе "check-list'ов", страхующем сотрудников от типичных (воспроизводящихся) ошибок. Но вред компании может быть нанесен и намеренно. Попробуем сформулировать основные риски.

риск вредительства и воровства

Популярная в советские времена фраза "На работе ты не гость..." (продолжите сами), увы, остается актуальной и по сей день. Работники несут домой бумагу, картриджи для принтера, канцелярские принадлежности, специализированные книги и журналы, выписываемые компанией, программное обеспечение, компьютеры, мебель... Что повезет.

Известно, что сотруднику фирмы гораздо легче совершить хищение, чем постороннему вору – сотрудник лучше знает все слабые места, недостатки системы безопасности, а также осведомлен и о ценности того или иного товара.

"На базе одной розничной сети, занимающейся сотовыми телефонами, открылся Интернет-магазин. Потребовались новые работники. В частности, был произведен набор курьеров для доставки телефонов заказчикам. Через месяц работы двое курьеров сами сделали крупный заказ в Интернет-магазине на вымышленный адрес и подтвердили его по сотовому телефону. Потом они вызвались произвести доставку, забрали товар, а на следующий день не вышли на работу. Руководитель отдела принялся разыскивать двух курьеров, однако оказалось, что у него были записаны только номера их сотовых телефонов, которые уже давно были заблокированы. Также выяснилось, что при приеме на работу никто не проверил паспортные данные, и они оказались "липовыми". В итоге Интернет-магазин не досчитался 2,5 тысячи долларов". (Зимин А., Модель оценки рисков предприятия по степени зависимости от персонала. Журнал "Управление персоналом", январь 2004.)

К тому же редкий сотрудник доволен своей зарплатой, поэтому считает, что нет ничего предосудительного в том, чтобы слегка поправить свое положение за счет родной компании. А уж набить карманы подарками (предназначенными для клиентов в рамках промо-акции) – вообще милое дело.

Существуют и иные способы дополнительного заработка – например, многочисленные варианты откатов.

риск увольнения ценного кадра

Ах, какой урон может нанести компании ценный сотрудник, просто-напросто уволившись! Опытный специалист уходит, как правило, вместе с клиентской базой. А уход менеджера высшего звена с предприятия иногда может быть равносилен его банкротству.

Что советуют специалисты в подобных случаях?

"На заводе на однотипном оборудовании (определенной сложности) работали около 50 "операторов-наладчиков". Число единиц оборудования росло, стали возникать проблемы. Работа несложная и монотонная, но требуется физическая сила, а также навыки работы с техникой (машина нуждалась в периодической отладке). Специалисты шантажируют руководство, постоянно и необоснованно требуя повышения оплаты труда. Эта задача принципиально не решается воздействием на людей – их воспитанием, уговорами, иными "психотропными" способами. Эта задача решается усовершенствованием самого процесса, разделением функций по разным качественным уровням.

Для решения задачи должность "оператор-наладчик" разделили... на 4 должности: наладчика технологического оборудования (высококвалифицированная функция), оператора (стандартная функция) и грузчика (неквалифицированная функция). В результате - резко упростилось выполнение сменных заданий.

Наладчик, настроив оборудование, затем постоянно находится в цехе и наблюдает за работой сразу нескольких станков, но не работает сам. А только, если происходит сбой, подходит и устраняет его. Квалификация наладчика отделена от выполнения текущей работы. Оператор, наоборот, работает за станком, но в случае сбоя или необходимости перенастройки, зовет наладчика. Высокой квалификации, связанной с настройкой оборудования тут не требуется - так оператору ЭВМ не требуется знания устройства компьютера. С грузчиком вообще все понятно. Работа грузчиков - неквалифицированная, низкооплачиваемая. Она вполне допускала текучесть кадров. Наладчиков, в отличие от "операторов-наладчиков", уже требовалось в 4 раза меньше (т.к. каждого прикрепили сразу к нескольким машинам). Ткаим образом, стало возможным сокращение числа "буйных гениев", увольнения которых ранее боялись, и повышение оплаты оставшимся (лучшим специалистам). На должность операторов станков взяли женщин из сельской местности. С зарплатой гораздо меньшей, чем была у "гениев", но существенно более высокой, чем у женщин в сельской местности.

Хотя число должностей стало больше, но управляемость выросла, а фонд заработной платы даже сократился. Вот так решается данная задача".

Итак, проблема "излишне ценного кадра" может быть решена разделением "квалифицированных" и "неквалифицированных" функций между разными сотрудниками.

"Включаем голову раньше, чем... кнопку вызова охраны", – такая надпись была вывешена на одном петербургском складе. И верно: вопросы хищений решаются службой безопасности. Проблема в том, что помимо явных "сбоев", существуют т.н. "скрытые дефекты" системы, которые долго время могут никак не проявляться. Другая проблема – как еще при составлении плана, проектировании нового изделия и т.п. предсказать возможные аварии, дефекты, которые могут произойти в будущем? По данным VERITAS Software, 43% организаций во всем мире остаются в основном неподготовленными к крупным катастрофам. В результате опроса 1259 ИТ-профессионалов во всем мире, оказалось, что всего 38% респондентов имеют планы послеаварийного восстановления и обеспечения непрерывности бизнеса, несмотря на то, что 92% признают, что крупная авария их ИТ-инфраструктуры привела бы к серьезным последствиям.

В качестве причин аварий вычислительных систем называют:

- отказы аппаратуры или программного обеспечения (37%)
- внешние компьютерные угрозы, включая атаки вирусов и хакеров (26%)
- природные катастрофы, такие как пожары и наводнения (14%)
- внутренние компьютерные угрозы, включая ошибки или злонамеренные действия сотрудников (13%)
- рукотворные катастрофы, такие как военные действия и терроризм (10%).

Когда респондентам предлагали сценарий, в котором естественная катастрофа (например,пожар или ураган) полностью выводит из строя главный вычислительный центр компании, свыше 40% не смогли сказать, сколько времени потребуется для восстановления нормального или хотя бы элементарного функционирования бизнеса.

Всего 3% уверены, что они смогут немедленно восстановить полноценное функционирование предприятия и всего 28% верят, что им удастся восстановить элементарные операции меньше, чем за 12 часов. Согласно результатам исследования, среднее время, которое требуется компаниям для восстановления элементарной работы после крупного пожара, превышает 72 часа.

Потенциальное влияние катастрофы на бизнес заключается в снижении производительности труда (62%), сокращении доходов (40%) и причинении ущерба отношениям с заказчиками (38%). Еще несколько десятков лет назад над подобной задачей задумался инженер, специалист по ТРИЗ Борис Злотин. Он предложил следующее: чтобы предотвратить аварию, надо сначала подумать, как эту аварию… устроить, да еще так, чтобы никто не заметил. По существу, нам предлагается поиграть в эдакого агента 007: представьте себе, что вас внедрили на родную фирму, дабы снизить эфективность ее работы либо совсем ее развалить. Как бы вы действовали? Добавим, что "вредить" нужно, используя внутренние ресурсы компании, т.е. бомбу приносить нельзя.

Например, вопрос: как организовать зарплату персонала, чтобы сотрудники работали плохо?

"В 30-е годы прошлого века, чтобы поддержать энтузиазм пожарных, им стали платить за время пребывания на пожаре. За год число пожаров удвоилось, и гасить их стали не спеша". Вот в чем состоит суть "диверсионного анализа: "Мы не ждем, а специально моделируем возникновение нежелательных явлений, чтобы затем, найдя способы их нейтрализации, упредить их реальное появление… Поскольку речь идет об обнаружении, как правило, скрытых дефектов, то и в обращенной задаче дефект необходимо получить скрытый, который не в состоянии вовремя обнаружить отдел контроля, заказчик и т. п. По сути дела, речь идет о придумывании диверсии, отсюда и название подхода. Естественно, после того, как диверсия придумана, следует проверить, не реализована ли она на практике, есть ли вероятность ее реализации. И если такая возможность не исключается, необходимо решить следующую задачу: как этого не допустить", – пишет Борис Злотин.

Он приводит пример диверсионного анализа для обычного выключателя, производившегося на одном советском заводе. Во время дискуссии по поводу его конструкции ведущий задал вопрос: "Допустим, этот выключатель идеальный, и мы не можем его улучшить. А как его испортить? Причем так, чтобы дефект оказался скрытым?".

Слушатели с охотой стали предлагать свои способы. Кто-то предложил вот что: если части выключателя спаивать не по всей площади соприкосновения, а только по краям, то при пропускании малых токов ничего плохого не произойдет, но при больших токах спай начнет интенсивно греться, и в итоге выключатель может развалиться на две половинки. "Неожиданно это предложение вызвало замешательство технолога, который сообщил, что именно так и происходит при пайке из-за того, что рабочие экономят дорогостоящий припой, что в свою очередь вывело из себя инженера-исследователя, чья лаборатория уже больше 10 лет исследовала причины перегрева и разрушения контактов… Добавим от себя: и все 10 лет получала зарплату.

Итак, процесс анализа состоит из множества этапов, в течение которых анализируемая система рассматривается с различных позиций. Мы приводим упрощенный вариант.

1. Сначала нужно сформулировать диверсионную задачу в виде: "Дана система, предназначенная для (указать основную функцию). Необходимо создать максимально возможное количество вредных эффектов, связанных с данной системой".

2. Затем нужно выписать основные параметры системы и их значения для нормального режима работы системы.

3. Далее нужно выявить вредные явления, которые могут возникнуть при нарушении нормального режима – с помощью т.н. числовой оси., т.е. резко увеличивая или, наоборот уменьшая один из параметров.

Например: что будет, если увеличить оборот компании в 10 раз? Уменьшить в 10 раз? Что получается, если резко возрастает штат сотрудников? Резко падает?

"В 2000 г. российская фирма–производитель пельменей с огромным успехом провела дегустацию своей продукции на выставке в одной из западных стран. Для иностранцев пельмени – экзотическая русская еда, естественно, попробовать хотелось всем. Ряд местных оптовиков, увидев такую реакцию посетителей, счел необходимым заключить договор на поставку пельменей из России. Окрыленная успехом, фирма решила устроить аналогичную акцию на выставке в одном из российских городов. Но ринувшиеся за угощением посетители чуть не затоптали несчастных стендистов".(Екатерина Михайлова, заместитель директора ЗАО "Мобильные выставочные технологии")

4. Теперь надо найти типовые опасные зоны (болевые точки). Какие места нашей организации наиболее уязвимы? Вот фрагмент перечня типовых опасных зон:

- зоны концентрации проходящих через систему потоков (потоки людей, денежные потоки, информационные потоки и т.п.);
- зоны, узлы, сотрудники, выполняющие большое количество разных функций (вспомним пример про операторов-наладчиков!).
- так называемые "стыки" – зоны стыковки разных систем, отделов (например, отдел закупок – отдел продаж – рекламный отдел – бухгалтерия …) Из-за несогласованности на стыках этих отделов часто возникают аварийные ситуации.
- зоны контакта с внешней средой (в частности, зоны контакта с клиентами, с конкурентами, с проверяющими органами и т.п.).
- зоны, в которых уже происходили те или иные аварии, подвергавшиеся ранее исправлениям, ремонтам и т.п. Так сказать, "самое слабое звено".
- зоны, в которых ответственные решения должны приниматься в условиях высокой неопределенности, недостатка времени и информации (в стрессовых обстоятельствах) и т. п.

5. Теперь надо рассмотреть перечень типовых причин вредных эффектов и решить, какие из них можно реализовать в нашей задаче.

Фрагмент перечня причин вредных эффектов:

- волевые решения, принятые без обоснования, пренебрежение "неугодными" фактами, мнениями специалистов;
- недооценка опасности из-за привыкания к ней, из-за надежды, что "пронесет";
- снижение внимания, скорости и точности реакций из-за усталости, монотонности, психологического напряжения и т.п.;
- формальное отношение к безопасности, направленное не столько на ее действительное обеспечение, сколько на снятие ответственности в случае аварии.
- преобладание личных или групповых интересов. Вредные эффекты появляются потому, что оказываются выгодными для кого-то, либо потому, что работа по их предупреждению кому-то невыгодна;
- отсутствие "защиты от дурака" – системы, предохраняющей от неверных (ошибочных или умышленных) действий сотрудника.

Рассказывает бизнесмен: "Когда-то мне пришлось побывать на заводе, где методом штамповки изготовлялись некие металлические изделия. Основной элемент процесса – здоровенный пресс, под который нужно совать заготовку. Я обратил внимание, что у большей части сотрудников не хватает пальцев на руках. Оказывается, их зарплата была прямо пропорциональна количеству произведенных изделий.

Вроде бы, все было сделано для обеспечения безопасности: сотрудник должен специальным пинцетом положить заготовку под пресс. А затем, чтобы пресс опустился, нужно обеими руками нажать две большие кнопки. Кажется, в таких условиях травма исключена... Не тут-то было! Сообразительные работники пинцетом блокировали одну из кнопок и, нажимая вторую рукой, одновременно совали заготовки прямо под опускающийся пресс..."

6. Этап обострения смоделированной ситуации. Допустим, мы найти способ, как навредить родной организации. Теперь думаем, как усилить вредные эффекты.

Фрагмент перечня усилений вредных эффектов:

- задержки в устранении аварии, вызванные попытками скрыть ее, страхом перед начальством и т.п.
- задержки в надежде, что "как-нибудь пронесет"...
- использование при устранении аварии средств, усугубляющих положение (гашение горящей проводки водой и т.п.)
- несовершенство системы безопасности, которая может сработать по ошибке, сама нанести урон...

Ложные срабатывания автомобильных подушек безопасности как правило приводили в неприятным последствиям, в том числе даже к смертельным исходам — в особенности среди детей и пожилых людей. Ведь устройство надувается за 50 миллисекунд, а столкновение водителя с ним происходит еще примерно спустя 30 миллисекунд, что сравнимо с ударом боксера. Причиной ложного срабатывания чаще всего являются "ошибки" электронных датчиков, от которых подушка получает команду.

Полностью исключить "нехорошую" статистику при колоссальном объеме производства (90 млн. фронтальных и 33 млн. боковых подушек только в 2000 году) невозможно даже при высочайшей степени надежности, закладываемой при разработке таких устройств.

7. И, чтобы никто не догадался, надо позаботиться о надежной маскировке нашей диверсии. Например, как воровать компьютерные комплектующие, чтобы никто этого не заметил?

"Лучше всего в этом отношении себя чувствуют системные администраторы, которые "под шумок" домой могут снести целый компьютер. Ведь мало кто из сотрудников на предприятии (если оно, конечно, не специализируется на ПК) разбирается в компьютерном "железе". Проводя на фирме часто необоснованные модернизации ПК, сисадмин может списать в свой счет довольно много компьютерных комплектующих, все равно никто не поймет, что он там поменял или настроил. Я знаю таких людей, которые могут "правильно" вывести из строя ПК так, что какая-то его часть временно перестает работать. Они докладывают начальству о поломке, просят выделить деньги на замену, покупают новую, а старую (полностью рабочую) оставляют себе". (Зимин А., Модель оценки рисков предприятия по степени зависимости от персонала)

Анализируй то и это. Диверсионный анализ разрабатывался первоначально для предотвращения в первую очередь аварий на производстве. Но очевидно, что подобные методы могут быть с успехом использованы и в иных областях. В частности, в настоящее время диверсионный анализ эффективно применяется при проверке на защищенность брэнда, товарного знака, элементов фирменного стиля компании. Так, Вадим Усков (руководитель юридической компании "Усков и Партнеры") называет это "диверсионный анализ брэнда – теоретическое моделирование всевозможных атак на брэнд и его составляющие с целью проверки степени юридической защищенности брэнда и его владельца".

Всем известно о маркетинговых войнах, происходивших как на Западе, так и в России, когда неопытный хозяин товарного знака, не защитивший вовремя свое детище, становился жертвой злоумышленников.

Чтобы этого не произошло, предлагается проверить, как можно атаковать ваш брэнд (со стороны конкурентов или, скажем, депутатов Госдумы), промоделировать различные внутренние конфликты (например, злоупотребление авторскими правами со стороны дизайнера) и т.п.

При этом рассматриваются несколько типовых видов диверсий:

- *паразитирование на брэнде* путем использования точно такого же идентификатора в другой товарной группе.

"Например, появившиеся сигареты "Балтика" напрямую копировали почти все идентификаторы пива "Балтика", включая номера, которые не являются охраняемыми с точки зрения интеллектуальной собственности". (В. Усков, "Диверсионный анализ брэнда")

- *"хулиганство" с брэндом*

Один политтехнолог откровенно похвалялся тем, что в предвыборной борьбе "легко" разделался с кандидатом по фамилии Банько: нанял за гроши студентов, вручил им маркеры и поручил пририсовывать на всех плакатах к фамилии всего лишь одну букву…

Рекомендуется проверить написание и произношение своих брэндов на так называемые "дурако-устойчивость" – как можно его исказить? Спародировать? Произнести неправильно (особенно, если в названии используются иностранные слова)? С чем его можно перепутать?

- *имитация брэнда* – т.е. создание различных клонов именно с целью, чтобы клиент принял товар-фальшивку за ваш.

Известно около 20 видов имитации: фонетическая имитация – клонирование имени брэнда за счет работы с буквами и звуками (Ариэль – Апрель); цветографическая имитация – подражание фирменным цветам в упаковке и т.п.

Возникает естественный вопрос: А что, если этот диверсионный анализ в самом деле попадет в руки злоумышленника? Не роем ли мы сами себе яму? Ведь и ядерное оружие, и ЛСД создавались в свое время с благими целями… "Может ли кто-нибудь воспользоваться нашей методикой для организации настоящих диверсий? В принципе это возможно, – писал Борис Злотин. – Многие годы наша страна болела шпиономанией. Но оказалось, что мы себе сами враги из-за некомпетентности, недобросовестности… Именно поэтому подавляющее большинство аварий происходит не по злому умыслу, а по незнанию. Разрушить это незнание и призван "диверсионный» подход". (Злотин Б.Л., Зусман А.В., Решение исследовательских задач, Кишинев, 1991 г., с. 116).

А суеверным – тем, кто боится накликать смоделированную беду – мы скажем следующее: если стараться совсем не думать о грустном, потом придется грустить всерьез. Сон разума рождает чудовищ.

Александр Соколов
Источник: Технологии разведки для бизнеса

СИЛОВЫЕ ЗАХВАТЫ ПРЕДПРИЯТИЙ

Аналитическая записка

Справка подготовлена на основании опыта предприятий-жертв, пострадавших от противоправных действий рейдеров, осуществляющих недружественные поглощения и силовые (безосновательные) захваты имущественных комплексов в целях дальнейшей их перепродажи как площадок для инвесторов-застройщиков.

Нападение и противостояние

Два современных взаимно устанавливающихся процесса, отражающих эскалацию криминального передела собственности. Оба — опасны для государства, но по разным причинам. Процесс нападения опасен для развития частного малого и среднего бизнеса, как наиболее перспективной группы налогоплательщиков будущего. Процесс противостояния опасен государству, потому что в условиях пробелов в законодательстве собственник будет вынужден уходить в тень. Выбор процесса нападения на собственника всегда зависит от его возможностей противостояния. Рейдеры всегда используют два метода: «силовой захват» и «правовой спектакль».

Правовой спектакль преследует две цели:

1)Создание правовой и информационной легитимности приемлемого качества;

2)Подбор «оснований» для захода на предприятия силовым способом методом перехвата управления.

Самым удачным нападением считается такое, при котором жертве потребуется максимальное время для «идентификации» правового спектакля и реакции на происходящие события. Если все-таки предприятие идентифицировало начало правового спектакля, то основой их тактики становится настройка на противодействие и ожидание силового захвата.

Прозрачные компании не хотят и не могут предпринимать альтернативных (теневых) методов защиты, потому что они в этом случае выйдут за правовое поле и станут уголовниками. Чем прозрачней компания, тем более легкой добычей она является. Чиновники исполняют свои обязанности только при наличии дополнительного стимула, которым налогоплательщики не располагают, ведя бизнес прозрачно. Конфиденциальность процесса нападения — залог успеха рейдеров, так как сокрытие намерений и действий приводит к невозможности реагирования.

Так или иначе, все действия рейдеров должны в конечном итоге оказаться в правовом поле. Действия рейдеров никогда не бывают прозрачными, и все их действия — всегда конфиденциальны. Информационно-правовая атака планируется рейдерами по каскадному методу, создавая непрерывное обременение сразу по нескольким направлениям. Такая атака сродни компьютерному спаму, когда система информационной безопасности уже не справляется с потоком атак и дает пробой. И тогда, как в Матрице, охотники проникают в систему и разрушают ее изнутри.СИЛОВЫЕ ЗАХВАТЫ ПРЕДПРИЯТИЙ.

Каскадная атака в рамках правового спектакля

В зависимости от ситуации, рейдеры запускают один или несколько каскадов:

Арбитражный каскад - возбуждение исполнительных производств в различных регионах России или, в редких случаях, за рубежом с еженедельным/ежедневным каскадом. Цель — не выигрыш в суде, а создание обеспечительных мер, которые снимаются через определенный срок. К этому моменту подходят другие дела.

Уголовный каскад - возбуждение заказных уголовных дел по слабым и сильным статьям УК РФ. В рамках данных дел выносятся определения, постановления и аресты. Иногда дела возбуждаются по персоналиям. Цель — арестовать имущество в рамках следственных мероприятий и передать на ответственное хранение менеджеру, близкому рейдерам. Дела по персоналиям часто возбуждаются против руководителей жертвы для оказания психологического давления на них.

Налоговый каскад - организация серии заказных налоговых проверок, как по предприятию жертвы, так и по ее контрагентам. Цель — ослабить финансово-хозяйственные показатели жертвы.

Милицейский каскад - организация серии заказных проверок в рамках Закона о милиции. Проверки производятся как по персоналиям, так и по фирмам жертвы. Мотивы проверок — различны. От оружие/наркотики до готовящееся преступление, в том числе и в экономической области.

Прокурорский каскад - организация мер противодействия следствию и уголовным делам против самих рейдеров. Проверки, объединения и перемещения уголовных дел с целью их закрытия или приостановки. Часто при объединении дел, следственная документация перепрофилируется для использования против предприятий-жертв.

Надзорный каскад - организация документальных проверок и проверок личного состава охранных предприятий и действий должностных лиц, по закону выступающих на стороне жертвы в целях их нейтрализации.

Информационный каскад - организация мероприятий для формирования негативного имиджа жертвы и ее партнеров в глазах общественности и правоохранительной системы, а также информационная атака на союзы, ассоциации, государственные органы, так или иначе защищающие права законных собственников. Присвоение роли жертвы самим рейдерам.

Международный каскад - организация мероприятий, уводящих арбитражные, административные и уголовные процессы, имущественные споры и платежи за пределы юрисдикции России в труднодоступные уголки мира (оффшоры).

Регистрационный каскад - бесконечная смена собственников предприятия и менеджмента предприятия без их ведома, перевод реестров акционеров, подделка реестров, в результате чего число акций предприятия превышает 100%.

Имущественный каскад - многократная перепродажа имущества, акций, векселей и прочих активов через технические фирмы, почти всегда являющимися собственностью рейдера. Цель — отмывание и отбеливание активов предприятия для формирования в конечном итоге добросовестного покупателя, права которого уже защищает закон.

Силовой каскад - совершение криминально-наказуемых деяний, таких как клевета, мошенничество, самоуправство, злоупотребление полномочиями, получение и дача взяток, коммерческий подкуп, шантаж, вымогательство, угроза применения насилия, причинение вреда здоровью различной степени тяжести, похищение людей...

Каскад надежды - доброхоты, якобы случайно узнавшие о проблемах предприятия-жертвы, вступают с ним в контакт и предлагаются те или иные мероприятия по защите его интересов. Как правило, добрые люди, прикрываясь важными именами и названиями хорошо известных структур и общественных объединений, на самом деле действуют с рейдерами заодно и сообща. Они либо предлагают купить предприятие по заведомо низкой цене, мотивируя сложностью проблемы, либо предоставляют себя в качестве переговорщика с агрессором. Признак каскадности соблюдается за счет череды доброхотов. Один не помог, так поможет другой...

Корпоративное плутовство. Мошенничество. Контрафактный и легитимный документооборот.

Корпоративное плутовство - наиболее сильный инструмент рейдеров. Его цель — запутать всех на свете и создать «иллюзию сложного корпоративного спора». В силу того, что рейдеры не ставят себе задач по существу, но лишь хотят все запутать, то их цель — информационная. Чтобы избежать персональной ответственности, рейдеры в качестве контрагентов спора подставляют мертвые души, фигурантов, потерявших свои документы, а иногда и самих директоров предприятий-жертв, якобы учредивших фирмы-однодневки по поддельным документам. Схема запутывания является основой для запуска основного, отвлекающего и юридического каскадов. Это — по сути бизнес и календарный план захвата предприятия.

Комбинированный документооборот.

В своих атаках рейдеры применяют комбинированный документооборот:

- Вход в процесс нападения происходит на основе документального контрафакта, т.е. с изготовлением заведомо ложных документов от однодневных фигурантов:
  - Оффшорные фирмы с разрывами по собственности и российские однодневки;
  - "Мертвые души" в качестве учредителей и директоров;
  - Менеджеры и независимые директора, действующие по доверенностям;
  - Юристы, действующие по доверенностям, полученным от доверенных лиц.
- «Среднее звено» процесса нападения предназначено для отбеливания однодневок методом перевода собственности на площадку для продажи и для уничтожения документального контрафакта. Платежи являются чисто техническими и представляют собой перекладывание из одного кармана в другой с использованием банковских кредитов и прочих схем, в том числе зачетных. Для юридической зачистки рейдеры предпринимают следующие действия:
  - Закрытие обременяющих арбитражных и уголовных дел;
  - Частичная или полная утеря первичной документации;
  - Отказы от претензий со стороны однодневок и ликвидация самоарестов;
- «Выход» из процесса нападения. Формирование добросовестного покупателя. Продажа собственности по остаточной стоимости инвестору-застройщику с приличной репутацией. Комиссионные — всегда наличными. В интегральных схемах, где заказчик нападения и рейдер — одно лицо (бенефициар), платежи носят чисто технический характер. На данном этапе могут возникнуть копеечные налоговые платежи. Все звенья процесса нападения разделены информационно: в цепочке документооборота никто не знает предыдущее и следующее звено. Кроме координатора, разумеется.
- *Документный контрафакт. Печатный станок.*

В рейдерских схемах документооборот создается хорошо организованным печатным станком. Печатный станок документного контрафакта является уникальным изобретением "черных адвокатов". Это автоматизированная система, с помощью которой создается полный пакет заведомо поддельных документов в кратчайшие сроки и практически без ошибок. В офисе печатного станка имеются все необходимые бланки, печати и подписи. Печатный станок может создавать бумаги любого содержания, в том числе и на государственных бланках. Судебные решения, постановления, выписки, свидетельства на право собственности, резолюции чиновников различного уровня. Не говоря уже об уставах, хозяйственных договорах, актах, акциях и векселях! Управляется такой офис адвокатами нападения. Данная процедура называется продажей ситуации с обременением. Иногда ситуация продается по несколько раз.

Теневая экономика

- снижает возможности частного бизнеса зарабатывать прибыль и формировать свою «кредитную историю»;
- снижает показатели банковского и межбанковского кредитования;
- приводит к росту инфляции и банковскому кризису;
- увеличивает отток капитала за рубеж и ограничивает приток реальных иностранных инвестиций;
- снижает покупательную способность граждан за счет ограничения их доступа к кредитным ресурсам (низкая белая зарплата);
- снижает бюджет и социальные возможности государства за счет отдаления перспективы создания высокооплачиваемых рабочих мест;
- приводит к отсрочке внедрения пенсионной реформы, рынков страхования и ипотеки и механизмов защиты доходов населения;
- ограничивает возможность государству опереться на средний класс собственников, как наиболее перспективного налогоплательщика и создает перспективу монополизации экономики.

ЛЕКЦИЯ 7.
КАПКАН НА АФЕРИСТА

Мошенничество является неизбежным злом всякой торговли. Искоренить его невозможно. Там, где крутятся большие деньги, там всегда будут крутиться всевозможные мошенники. При этом аферисты считают себя "благодетелями человечества", "санитарами рынка". Они искренне убеждены в том, что "дураков учить надо", что "предприниматели сами мошенники", что поговорка "не обманешь - не продашь" выражает внутреннюю суть каждого торговца, а поэтому обмануть обманывающего не грех.

Исполняя свою "историческую" миссию, мошенники проявляют "чудеса" изобретательности, глубочайшее знание рынка и человеческой психологии. Однако, не смотря на высокую техническую оснащённость лже предпринимателей, их махинации можно просчитать и поймать комбинаторов с поличным. Для этого достаточно придерживаться некоторых правил и не торопиться ни на одном этапе сделки.

Предположим, что к вам обратился новый человек с выгодным коммерческим предложением. Попросите у него паспорт, если его не окажется, то спросите полные данные, телефон и домашний адрес. Возможно, кто-то возразит: "Нельзя же при первой встрече задевать человека подозрительностью. Это может вызвать у него негативные чувства". Что же, если вы столь щепетильны, то можете в качестве первого шага продемонстрировать свои документы (например, лицензию или учредительные документы). После осмотра ваших документов незнакомцу будет трудно отказаться от предъявления собственных. Получив паспорт посетителя, передайте его своему сотруднику. Он за время вашей беседы с новым клиентом должен снять ксерокопию со всех страниц паспорта. Разговаривая с посетителем, поинтересуйтесь его связями, с кем и когда он заключал последние сделки, давно ли работает в своей организации, где работал раньше. Постарайтесь найти общих знакомых. В первую встречу лучше не говорить что-то определённое. Сразу отказываться или наоборот хвататься за предложенное сотрудничество двумя руками. Скажите, что вы заинтересованы в совместной деятельности, но вам нужно её полностью обдумать. Не покупайтесь на намёки на более сговорчивых конкурентов. Вам никто не собирается делать дорогих подарков. Если клиент пришёл к вам, значит вы ему выгодны. Просто так, обидевшись на вашу несговорчивость, ни один заинтересованный предприниматель не уйдёт. Если ваш посетитель на машине, то запомните её номер. Не помешает и скрытая видео съемка. В этом случае объектив видео камеры прикрывается подкрашенной в чёрный цвет марлевой повязкой. После ухода посетителя, проведите проверку представленных вам документов.

Паспорт проверяется на утрату, на соответствие адреса в паспорте с данными Центрального адресного бюро, на соответствие клееной фотографии с фотографией в форме N1 паспортной службы. Если вам оставлен номер сотового телефона, то проверка данных его владельца проводится аналогичным образом. Контактные телефоны фирмы проверяются по независимым источникам (например, по телефонному справочнику или в банке, где посетитель имеет расчетный счёт). Свяжитесь с организациями, поддерживающим деловые отношения с новым клиентом, поинтересуйтесь их надёжностью и долговременностью. Проверьте номер автомашины. Наведите справки о помещении предприятия и о складе посетителя, о сроках и условиях их аренды, о наличии на складе продукции, кроме той, которую вам предлагают. До получения всей достоверной информации к сделке лучше не преступать.

Установив личность вашего посетителя, не расслабляйтесь. Перед оформлением сделки убедитесь в качестве и количестве всей партии приобретаемого товара, а так же в его принадлежности вашему партнёру. При заключении договора, не допускайте в нём положений, которые могут иметь двойственный смысл, перекладывать ответственность за сделку на третьи организации. В договоре должны быть чётко указаны штрафные санкции за плохое качество, неполную и несвоевременную поставку товара.

При дальнейшем прохождении сделки рекомендуется придерживаться правил:

при продаже:

- Получив оплаченную "платёжку", проверьте в банке факт поступления денег на счёт.
- Не отправляйте товар случайными попутными машинами без надёжного сопровождения.
- В дороге не вступайте в конфликт с незнакомыми людьми, предлагающими на одной из стоянок выпить за компанию.
- Если в середине пути к вам подходит представитель предприятия, оплативший товар, и просит изменить маршрут или конечный пункт следования, то обязательно свяжитесь с представителем своей организации.
- При проверке ваших документов сотрудниками милиции, налоговой полиции не забудьте внимательно осмотреть их удостоверения и записать их данные. В том случае, когда правоохранительных органов просят вас пройти (проехать) с ними, следуйте со своей машиной. Не оставляйте товар без присмотра.
- До получения денег никому не передавайте документы на свой товар.
- Передавая оплаченный товар, установите личность получателя. Он может оказаться мошенником, знающим о вашей сделке. Сама передача товара должна производится исключительно на склад получателя, а не перегружаться из машины в машину.
- При наличном расчёте за доставляемый вами товар, сначала получите деньги и убедитесь в их подлинности.
- Не перегружайте свой товар до получения денег.

при покупке:

- Не рассчитывайтесь за товар на чужих складах без надёжной охраны.
- Не оставляйте клиента с вашими деньгами, не получив товар и не убедившись в его количестве и качестве.
- Оплатив товар, не соглашайтесь на расторжение сделки. Если её всё-таки приходится расторгать, проверьте возвращаемые вам деньги и будьте осторожны при следовании с деньгами на своё предприятие.

в ежедневной работе:

- Не разрешайте посторонним свободно передвигаться по вашим складам и помещениям предприятия, где хранятся денежные средства.
- Не проштамповывайте чистые бланки с печатью предприятия.
- При долгосрочной аренде помещения интересуйтесь вашими соседями, особенно если вас разделяет одна кирпичная перегородка.
- Принимая на работу на материально-ответственные должности, проверьте личность кандидата и не доверяйте ему сразу больших сумм.
- Утратив печать, сообщите об этом в милицию и всем своим знакомым, поддерживающим с вами деловые отношения.
- Столкнувшись на своём рабочем месте с человеком, предъявившем поддельные документы, не спешите его выпроваживать из вашего кабинета. Сделайте вид, что не подозреваете его в преступной деятельности. Попросите мошенника зайти через день-два, когда вы сможете дать утвердительный ответ на его предложение. После ухода жулика, сообщите о его визите в милицию.

Если вас пытаются обмануть на базе (просят перегрузить товар до оплаты в другую машину, оставит товар и пойти вместе пообедать, предъявят поддельные документы на получение вашего товара), то, сославшись на необходимость отойти на минуту в туалет, направьтесь к телефону и сообщите о преступниках в ближайший отдел милиции.

При встрече с мошенниками в дороге, вы должны убедить их в необходимости свернуть с предложенного ими маршрута и подъехать к ближайшему посту милиции. Если они на машине, то обязательно запомните её номер.

Иногда мошенники изготавливают макеты, составленные из коробок, мешков, наполненных речным песком. В этом случае покупателю, пришедшему за образцом продукции, не дают возможности самостоятельно выбрать коробку. Ему просто всовывают коробку с настоящей продукцией прямо в руки. В этом случае лучше попросить одного из своих знакомых придти за ещё одним образцом, который бы он выбрал самостоятельно. При бурных протестах сотрудников склада надо не споря взять предложенную коробку и сообщить в милицию о своих подозрениях.

Придерживаясь этих несложных рекомендаций, вы сможете избежать мошенничества и помочь сотрудникам уголовного розыска в поимке изобретательных аферистов.

"Кидало" под "ментов".

Доверие граждан к сотрудникам милиции является хорошим признаком улучшения работы органов правопорядка. Однако, как показывает практика, полностью доверять человеку в форме милиции нельзя. Многие мошенники, артистически преобразившись в стражей порядка, обирают доверчивых граждан среди бела дня и в присутствии настоящих сотрудников милиции. Наглость аферистов доходит до того, что они спокойно входят в различные подразделения МВД и держатся в них своими людьми. При этом "оборотни" в форме умело опираются на психологическую обработку терпил, она состоит из следующих элементов:

- На доверии граждан к милицейской символике и их готовности подчинится представителям власти.
- На невнимательности к предъявляемым документам и уверенности, что по ним они без труда найдут, стоящего перед ними милиционера
- На подчинении требованиям, которые могут нарушать их законные интересы.
- На использовании мошенниками слов и оборотов правового лексикона (Вы как свидетель, Вас необходимо допросить, у нас имеется санкция прокурора).

Вот несколько примеров "кидков" под "ментов".

"Менты" с "уазика". Сотрудники солидной фирмы, получив в банке зарплату, возвращались в свой офис. На одном из перекрёстков их остановили "омоновцы", стоящие у милицейского "уазика". Началась проверка документов и содержимого машины. Неожиданно один "милиционер" заявил, что деньги, находящиеся в машине, фальшивые и требуют проверки в ОБЭП. Суровые "омоновцы" без лишних слов пристёгивают коммерсантов наручниками к сиденьям автомашины. Перегружают многомиллионные денежные мешки в "уазик" и удаляются. Осознание "подставы" приходит медленно, но неизбежно.

"Мент" со справкой. Мясов Михаил, освободившись из мест лишения свободы, проблему своего трудоустройства решил довольно быстро. Для начала он согнул справку об освобождении так, чтобы была видна только его фамилия и фото с печатью МВД. Затем Мясов стал подходить к парнишкам четырнадцати - пятнадцати лет. Представлялся сотрудником милиции, мимолётом демонстрируя свою справку. Просил подростка назвать имя, фамилию и домашний адрес. Мальчик отвечал. "Вот ты как раз мне и нужен, - говорил мошенник, - На тебя поступило заявление, что ты совершил кражу. Расскажи мне о себе и о своих знакомых". Испуганный паренёк выкладывал всю свою подноготную. Попутно аферист узнавал о вещах, находящихся в квартире. Получив необходимую информацию, Мясов требовал немедленно пройти домой, взять "похищенное" и отнести его в милицию до выяснения всех обстоятельств. Придя в квартиру, "милиционер" быстро представлялся родителям и рассказывал им массу подробностей из жизни их сына и о совершённой им краже. Недоумённые родители представляли доказательства законности приобретения "похищенного". Тогда Мясов предлагал им подать исковое на "лжезаявителей" на сумму якобы похищенного у них имущества. Подстрекаемые мошенником родители, охотно соглашались воздать должное своим обидчикам. Для соблюдения необходимых формальностей, "милиционер" просил отпустить сына с "похищенным" в милицию. Родители не возражали.

Не доходя двести-триста метров до ближайшего отдела милиции, аферист спрашивал у подростка есть ли у него свидетельство о рождении. Естественно его не находилось. Тогда Мясов отправлял мальчика за свидетельством, строго наказывая явиться в его кабинет на втором этаже. Разумеется "похищенное" он великодушно брался донести до отдела милиции сам. Мальчик шёл домой, а мошенник ловил частника и ехал на съёмную квартиру. В ней он оставлял добычу посреднику, который созванивался с перекупщиком. Тот приезжал, осматривал вещи, расплачивался и уезжал. Вечером Мясов приезжал к посреднику и забирал у него деньги.

"Милицейский конфискат". Владимир Неретин не спеша вошёл в здание районной поликлиники. Посмотрел расписание приёма врачей и направился к кабинету терапевта. Очередь к врачу нескончаемая. Владимир спросил кто последний и присел рядом с ветхой старушкой. Вскоре она стала ему жаловаться на своё здоровье и маленькую пенсию. Владимир посочувствовал и предложил ей пройти курс лечебного массажа в областной поликлинике. Платить Авдотье Юрьевне Ракитиной ни за что не надо. Владимир работает капитаном милиции. Когда-то он смог помочь главному врачу поликлиники найти украденную у него машину. Теперь они друзья. Единственное, что от неё требуется - это назваться его родственницей, поскольку за больную бабушку просить значительно удобнее. Авдотья Юрьевна охотно согласилась. Договорились встретиться в поликлинике через день.

В назначенный день Неретин пришёл к главному врачу областной поликлинике Игорю Владимировичу Сергееву в форме капитана милиции. Он попросил главврача провести его больной родственнице вне очереди лечебный массаж. Игорь Владимирович пошёл ему на встречу. Капитан заплатил положенный тариф и в тот же день Авдотью Юрьевну массажировал внимательный специалист. Через две недели курс массажа закончился и ожившая пенсионерка не знала как и благодарить своего благодетеля. Внимательный капитан, не взяв с неё ни одной копейки, отправился благодарить главврача.

Придя к нему в кабинет, капитан искренне поблагодарил Игоря Владимировича за оказанное содействие, а в качестве более существенной благодарности предложил купить из "конфиската" милиции "форд". Цена бросовая. Две тысячи долларов за почти новую машину. Сергеев поинтересовался, можно ли купить по такой же цене машину и его другу. Неретин ответил, что можно, но вероятней всего не сразу. Игорь Владимирович попросил неделю на сбор денег. Неретин, в свою очередь, пообещал за это время решить вопрос со второй машиной.

Через неделю Неретин зашёл к Сергееву. Тот сообщил ему о наличии у него необходимой суммы и поинтересовался насчёт машины для друга. Капитан ответил, что приобрести машину возможно, только желательно это сделать побыстрее. За конфискатом всегда очередь. Сергеев сказал: "У моего друга деньги на руках. У меня тоже. Мы готовы завтра подъехать, осмотреть машины и рассчитаться за них". Капитан предложил не откладывать дело в долгий ящик и встретиться на следующий день у его отдела милиции.

На следующий день капитан Неретин встретил Сергеева с другом у отделения милиции. Он попросил их пройти с ним в отдел, где ему надо перед отъездом сделать несколько распоряжений. Капитан, зайдя на минуту в два-три кабинета, вскоре действительно освободился. Они поехали на одну из баз ГУВД. Прибыв на место, капитан взял паспорта покупателей и пошёл в административный корпус. Примерно через полчаса он вернулся с готовыми документами. Отдал их будущим владельцам иномарок. Сергеев с другом осмотрели документы. Всё в порядке, тогда капитан предложил пройти на базу для осмотра машин. Едва они прошли на место и стали у блестящих "фордов", к капитану подошёл сердитый майор, строго спросивший когда же тот собирается платить за машины. Неретин обратился к покупателям: ", я же деньги у вас не взял". Те, достав заветные доллары, передали их капитану, который вместе с майором ушёл заканчивать оформление документов. К концу дня "покупатели" знали, что мошенник, представившийся капитаном Неретиным, такой же капитан и родственник Ракитиной, как и они наследники китайского императора и владельцы заветного конфиската.

ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

Техническое обеспечение безопасности должно базироваться на:

- системе стандартизации и унификации;
- системе лицензирования деятельности;
- системах сертификации средств защиты;
- системе сертификации технических средств и объектов информатизации;
- системе аттестации защищенных объектов информатизации.

Основными составляющими обеспечения безопасности ресурсов коммерческого предприятия являются:

- система физической защиты материальных объекте и финансовых ресурсов;
- система безопасности информационных ресурсов.

Система физической защиты (безопасности) материальных объектов и финансовых ресурсов должна предусматривать:

- систему инженерно-технических и организационных мер охраны;
- систему регулирования доступа;
- систему мер (режима) и контроля вероятных каналов утечки информации;
- систему мер возврата материальных ценностей.

Система охранных мер должна предусматривать:

- многорубежность построения охраны (территории, здания, помещения) по нарастающей к наиболее ценной оберегаемой конкретности;
- комплексное применение современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;
- надежное инженерно-техническое перекрытие вероятных путей несанкционированного вторжения в охраняемые пределы;
- устойчивую (дублированную) систему связи и управления всех взаимодействующих в охране структур;
- высокую подготовку и готовность основных и резервных сил охраны к оперативному противодействию преступным действиям;
- самоохрану персонала.

Система регулирования доступа должна предусматривать:

- объективное определение "надежности" лиц, допускаемых к работе;
- максимальное ограничение количества лиц, допускаемых на объекты коммерческого предприятия;
- установление для каждого работника (или посетителя) дифференцированного по времени, месту и виду деятельности права доступа на объект;
- четкое определение порядка выдачи разрешений и оформления документов для входа (въезда) на объект;
- определение объемов контрольно-пропускных функций на каждом проходном и проездном пункте;
- оборудование контрольно-пропускных пунктов (постов) техническими средствами, обеспечивающими достоверный контроль проходящих, объективную регистрацию прохода и предотвращение несанкционированного (в том числе силового) проникновения посторонних лиц;
- высокую подготовленность и защищенность персонала (нарядов) контрольно-пропускных пунктов.

Система мер (режим) сохранности ценностей и контроля должна предусматривать:

- строго контролируемый доступ лиц в режимные зоны (зоны обращения и хранения финансов);
- максимальное ограничение посещений режимных зон лицами, не участвующими в работе;
- максимальное сокращение количества лиц, обладающих досмотровым иммунитетом;
- организацию и осуществление присутственного (явочного) и дистанционного - по техническим каналам (скрытого) контроля за соблюдением режима безопасности;
- организацию тщательного контроля любых предметов и веществ перемещаемых за пределы режимных зон;
- обеспечение защищенного хранения документов, финансовых средств и ценных бумаг;
- соблюдение персональной и коллективной материальной и финансовой ответственности в процессе открытого обращения финансовых ресурсов и материальных ценностей;
- организацию тщательного контроля на каналах возможной утечки информации;
- оперативное выявление причин тревожных ситуаций в режимных зонах, пресечение их развития или ликвидацию во взаимодействии с силами охраны.

Система мер возврата утраченных материальных и финансовых ресурсов слагается из совместных усилий объектовых служб безопасности и государственных органов охраны правопорядка и безопасности.

На объектовую службу безопасности возлагаются:

- обнаружение противоправного изъятия материальных и финансовых средств из обращения или хранения;
- оперативное информирование правоохранительных органов о событиях и критических ситуациях;
- установление субъекта преступления;
- проведение поиска возможного "схоронения" утраченных средств в районе объекта.

Дальнейший поиск и возврат пропавших ресурсов организуются в установленном порядке через соответствующие органы правопорядка и безопасности.

Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс организационных, технических, программных и криптографических средств и мер по защите информации в процессе традиционного документооборота при работе исполнителей с конфиденциальными документами и сведениями, при обработке информации в автоматизированных системах различного уровня и назначения, при передаче по каналам связи, при ведении конфиденциальных переговоров.

При этом основными направлениями реализации технической политики обеспечения информационной безопасности в этих сферах деятельности являются:

- защита информационных ресурсов от разглашения; от хищения, уничтожения, искажения и подделки за счет несанкционированного доступа и специальных воздействий;
- защита информации от утечки вследствие наличия физических полей за счет ПЭМИН (побочные электромагнитные излучения и наводки) на электрические цепи, трубопроводы и конструкции зданий.

В рамках указанных направлений технической политики обеспечения информационной безопасности необходимы:

- реализация разрешительной системы допуска исполнителей (пользователей) к работам, документам и информации конфиденциального характера;
- ограничение доступа исполнителей и посторонних лиц в здания, помещения, где проводятся работы конфиденциального характера, в том числе на объекты информатизации, на которых обрабатывается (хранится) информация конфиденциального характера;
- разграничение доступа пользователей к данным автоматизированных систем различного уровня и назначения;
- учет документов, информационных массивов, регистрация действий пользователей информационных систем, контроль за несанкционированным доступом и действиями пользователей;
- криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;
- снижение уровня и информативности ПЭМИН, создаваемых различными элементами технических средств обеспечения производственной деятельности и автоматизированных информационных систем;
- снижение уровня акустических излучений;
- электрическая развязка цепей питания, заземления и других цепей технических средств, выходящих за пределы контролируемой территории;
- активное зашумление в различных диапазонах;
- противодействие оптическим и лазерным средствам наблюдения;
- проверка технических средств и объектов информатизации на предмет выявления включенных в них закладных устройств ("жучков");
- предотвращение внедрения в автоматизированные информационные системы программ вирусного характера.

Защита информационных ресурсов от несанкционированного доступа должна предусматривать:

- обоснованность доступа, когда исполнитель (пользователь) должен иметь соответствующую форму допуска для ознакомления с документацией (информацией) определенного уровня конфиденциальности и ему необходимо ознакомление с данной информацией или необходимы действия с ней для выполнения производственных функций;
- персональную ответственность, заключающуюся в том, что исполнитель (пользователь) должен нести ответственность за сохранность доверенных ему документов (носителей информации, информационных массивов), за свои действия в информационных системах;
- надежность хранения, когда документы (носители информации, информационные массивы) хранятся в условиях, исключающих несанкционированное ознакомление с ними, их уничтожение, подделку или искажение;
- разграничение информации по уровню конфиденциальности, заключающееся в предупреждении размещения сведений более высокого уровня конфиденциальности в документах (носителях информации, информационных массивах) с более низким уровнем конфиденциальности, а также предупреждение передачи конфиденциальной информации по незащищенным линиям связи;
- контроль за действиями исполнителей (пользователей) с документацией и сведениями, а также в автоматизированных системах и системах связи;
- очистку (обнуление, исключение информативности) оперативной памяти, буферов при освобождении пользователем до перераспределения этих ресурсов между другими пользователями;

Требование обоснованности доступа реализуется в рамках разрешительной системы допуска к работам, документам и сведениям. В ней устанавливается: кто, кому, в соответствии с какими полномочиями, какие документы и сведения (носители информации, информационные массивы)! для каких действий или для какого вида доступа может предоставить и при каких условиях. Система допуска предполагает определение для всех пользователей автоматизированных систем информационных и программных ресурсов, доступных им для конкретных операций (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

Персональная ответственность достигается путем:

- росписи исполнителей в журналах, карточках учета, других разрешительных документах, а также на самих документах;
- индивидуальной идентификации пользователей и инициированных ими процессов в автоматизированных системах;
- проверки подлинности (аутентификации) исполнителей (пользователей) на основе использования паролей, ключей, магнитных карт, цифровой подписи, а также биометрических характеристик личности при доступе как в автоматизированные системы, так и в выделенные помещения (зоны).

Условие надежности хранения реализуется с помощью:

- хранилищ конфиденциальных документов, оборудованных техническими средствами охраны в соответствии с установленными требованиями, доступ в которые ограничен и осуществляется в установленном порядке;
- выделения помещений, в которых разрешается работа с конфиденциальной документацией, оборудованных сейфами и металлическими шкафами, а также ограничения доступа в эти помещения;
- использования криптографического преобразования информации в автоматизированных системах.

Правило разграничения информации по уровню конфиденциальности реализуется с помощью предварительно учтенных тетрадей для ведения конфиденциальных записей или носителей информации, предназначенных для информации определенного уровня секретности.

Система контроля за действиями исполнителей реализуется посредством:

- организационных мер контроля при работе исполнителей с конфиденциальными документами и сведениями;
- регистрации (протоколирования) действий пользователей с информационными и программными ресурсами автоматизированных систем с указанием даты и времени, идентификаторов запрашивающего и запрашиваемых ресурсов, вида взаимодействия и его результата, включая запрещенные попытки доступа;
- сигнализации о несанкционированных действиях пользователей.

Очистка памяти осуществляется организационными и программными мерами, а целостность автоматизированных систем обеспечивается комплексом программно-технических средств и организационных мероприятий.

Защита информации от утечки за счет ПЭМИН.

Основным направлением защиты информации от утечки за счет ПЭМИН является уменьшение отношения информативного сигнала к помехе до уровня, определяемого "Нормами эффективности защиты АСУ и ЭВМ от утечки информации за счет ПЭМИН", при котором восстановление сообщений становится принципиально невозможным. Решение этой задачи достигается как снижением уровня излучений информационных сигналов, так и увеличением уровня помех в соответствующих частотных диапазонах.

Первый способ реализуется выбором системно-технических и конструкторских решений при создании технических средств ЭВТ в "защищенном исполнении", а также рациональным выбором места размещения технических средств относительно направлений возможного перехвата информативного сигнала.

Второй способ реализуется в основном за счет применения активных средств защиты в виде "генераторов шума" и специальной системы антенн.

Защита информации в линиях связи.

К основным видам линий связи, используемых для передачи информации, можно отнести проводные (телефонные, телеграфные), радио- и радиорелейные, тропосферные и космические линии связи. При необходимости передачи по ним конфиденциальной информации основным способом защиты ее от перехвата, искажения и навязывания ложной информации является использование криптографического преобразования информации, а на небольших расстояниях, кроме того, — использование защищенных волоконно-оптических линий связи.

Безопасное использование технических средств информатизации.

Одним из методов технической разведки и промышленного шпионажа является внедрение в конструкцию различных технических средств закладных устройств перехвата, трансляции информации или вывода технических средств из строя.

В целях противодействия такому методу воздействия на объекты технических средств информатизации, предназначенных для обработки конфиденциальной информации, в обязательном порядке проводится проверка этих средств, осуществляемая специализированными организациями с помощью специального оборудования, как правило, в стационарных условиях в соответствии с установленными требованиями.

Защита речевой информации при проведении конфиденциальных переговоров.

Исходя из возможности перехвата речевой информации при проведении разговоров конфиденциального характера с помощью внедрения закладных устройств, акустических, виброакустических и лазерных технических средств разведки, противодействие этим угрозам должно осуществляться всеми доступными средствами и методами.

Обеспечение качества работ в системе безопасности.

Необходимой составляющей системы безопасности должно быть обеспечение качества работ и используемых средств и мер защиты, нормативной базой которого является система стандартов и других руководящих нормативно-технических и методических документов по безопасности, утвержденных федеральными органами государственного управления в соответствии с их компетенцией и определяющих нормы защищенности информации и требования к различным направлениям защиты информации. В соответствии с этими требованиями должны проводиться предпроектное обследование и проектирование информационных систем, заказ средств защиты информации и контроля, предполагаемых к использованию в этих системах, аттестация объектов информатики, а также контроль защищенности информационных ресурсов.

К основным стандартам и нормативно-техническим документам в области защиты информации от НСД относятся: комплект руководящих документов Гостехкомиссии России (1992 г.), в том числе "Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации", "Положение по организации разработки, изготовления и эксплуатации программ и технических средств защиты информации от НСД в АС и ЭВТ".

В совокупности с системой стандартизации единую систему обеспечения качества продукции и услуг по требованиям безопасности информации составляют:

- сертификация средств и систем вычислительной техники и связи по требованиям безопасности информации;
- лицензирование деятельности по оказанию услуг в области защиты информации;
- аттестация средств автоматизации объектов по требованиям безопасности информации.

В соответствии с требованиями, право оказывать услуги сторонним организациям в области защиты информации, предоставлено только организациям, имеющим на этот вид деятельности разрешение (лицензию). Средства и системы вычислительной техники и связи, предназначенные для обработки (передачи) секретной информации, средства защиты и контроля эффективности защиты такой информации, подлежат обязательной сертификации по требованиям безопасности информацию. А объекты информатики, предназначенные для обработки секретной и иной конфиденциальной информации, а также для ведения секретных переговоров, подлежат обязательной аттестации по требованиям безопасности информации.

При разработке системы комплексной защиты информации объекта необходимо максимально использовать имеющиеся сертифицированные по требованиям безопасности информации средства вычислительной техники и связи, средства защиты и контроля защищенности, разрабатывая или заказывая оригинальные технические или программные средства защиты только в случаях, когда имеющимися средствами нельзя достигнуть необходимых результатов. Исходя из этого, при разработке автоматизированных систем различного уровня и назначения, серьезное внимание следует уделить выбору технических средств и общесистемного матобеспечения. Этими же обстоятельствами следует руководствоваться при выборе стратегии развития систем информатизации.

ЛЕКЦИЯ 9.
ОСНОВНЫЕ НАПРАВЛЕНИЯ ПОСТРОЕНИЯ СИСТЕМЫ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ КОМПАНИИ

1. Экономическая разведка - организация добывания своевременной информации для выработки руководством компании наиболее рациональных управленческих решений по вопросам финансово-хозяйственной деятельности, соответствующих складывающейся обстановке, стратегическим целям и оперативным задачам, позволяющим избежать неудач в своей деятельности.

Сбор, анализ и обработка данной информации является наиболее ответственным звеном не только системы обеспечения безопасности, но и маркетинга, поскольку на ее основе вырабатывается политика компании.

Сбор, анализ и обработка данной информации является наиболее ответственным звеном не только системы обеспечения безопасности, но и маркетинга, поскольку на ее основе вырабатывается политика компании.

2. Экономическая контрразведка и внутренняя безопасность:

- противодействие внутренней коррупции, попыткам нанесения ущерба компании ее работниками, причем речь идет не только о воровстве, но и о некомпетентности;
- проведение служебных расследований фактов подлога, хищений и иного нанесения ущерба компании;
- противодействие криминальным угрозам;
- выявление источников информации структур организованной преступности и промышленного шпионажа среди сотрудников компании;
- проверка устраивающихся на работу и периодическая профилактическая проверка лояльности персонала компании;
- обеспечение физической безопасности руководства компании и ее персонала (силовое и оперативное);
- предупреждение негативных процессов в трудовом коллективе компании, которые могут привезти к чрезвычайным происшествиям;
- обеспечение безопасности движимого и недвижимого имущества компании.

3.Информационно-аналитическая работа. Это направление обеспечивает упорядоченное накопление, научно обоснованное обобщение и анализ информации по различным направлениям безопасности компании с выделением как положительных, так и отрицательных тенденций процесса обеспечения безопасности и на этой основе выработку предложений по дальнейшему развитию данных тенденций либо их нейтрализации. В регионах оно может быть оформлено в виде одного-двух человек, поддерживающих постоянную связь с центром и накапливающих и оценивающих текущую ситуацию на местах.

4. Информационная безопасность (обеспечение защиты сведений, составляющих, как коммерческую тайну, так и жизненно важных для бесперебойного функционирования предприятия информационных массивов):

- организационно-режимные меры по работе с конфиденциальной информацией во всех ее формах (бумажные, электронные и др. носители информации);
- противодействие частным техническим разведкам;
- полный комплекс обеспечения безопасности локальных компьютеров и внутренних компьютерных сетей, обеспечение безопасной работы выходов в Интернет;
- обеспечение безопасности каналов связи.

5. Взаимодействие с местными властными структурами и правоохранительными органами. Это взаимодействие обычно строится по следующему принципу: головное подразделение безопасности - федеральная исполнительная власть и центральные аппараты МВД, ФСБ, ФСНП, ГТК и прокуратуры; подразделения безопасности на местах - территориальные органы.

6. Обучение персонала, по адаптированным программам согласно организационно-штатной расстановке и выполняемым служебным обязанностям, основным направлениям обеспечения корпоративной безопасности компании.

7. Пропагандистское обеспечение политики компании («активные мероприятия»).

Если говорить о воплощении этой концепции на практике, то одним из возможных решений является введение горизонтальной системы подчинения региональных подразделений безопасности первому вице-президенту компании по административно-правовым вопросам, который курирует службу безопасности, информационно-аналитический отдел, юридический отдел, отдел кадров и отдел по связям с общественностью.

Именно на административно-правовой блок и должен возлагаться весь комплекс проблем, связанных с обеспечением безопасности компании.

В региональных предприятиях, которые составляют основную массу «дочек», оперативный состав подразделений безопасности насчитывает обычно до пяти человек. Они работают в тесном контакте с подразделениями центрального аппарата компании, относящимися к сфере обеспечения безопасности. Заместители директоров «дочек» по административно-правовым вопросам помимо оперативного подчинения своим непосредственным руководителям должны быть напрямую подчинены шефу всей системы корпоративной безопасности. Большинство региональных топ-менеджеров такую систему воспринимают настороженно, не без основания чувствуя себя «под колпаком».

Можно по-разному относиться к этой действительно непростой ситуации, но нельзя не отметить, что помимо комплексного обеспечения безопасности такая система способствует решению стратегической для каждой молодой российской компании проблемы - консолидации вошедших в нее структур и их работе на единый конечный результат.

Хотелось бы отметить еще один важный момент: вся работа системы корпоративной безопасности снизу доверху строится на доверии. Если СБ не пользуется доверием руководства компании, ее информация ничего не стоит, и вся ее многосторонняя деятельность теряет смысл.

Если сотрудник СБ не пользуется доверием своего непосредственного руководства, то ему здесь не место. Каждый оперативник должен быть абсолютно уверен, что ему полностью доверяют, должен ценить это доверие и никогда им не злоупотреблять. Однако доверие не исключает, а, напротив, подразумевает соответствующий контроль за деятельностью всех элементов системы корпоративной безопасности, а в кадровой политике - разработку таких критериев оценки деятельности каждого отдельного работника, которые бы стимулировали его активность, способствовали объективной оценке его достижений, его служебному росту и не толкали на злоупотребления.

В заключение хотелось бы еще раз напомнить, что полученная информация, как и сама система корпоративной безопасности вообще - не самоцель. Эта система является всего лишь предпосылкой и одним из средств эффективной экономической политики и стратегии, но сама по себе никак не может заменить ни политику, ни стратегию, ни экономическую мощь хозяйствующего субъекта.

Решающим фактором конкурентной борьбы является способность руководителей предприятия эффективно использовать полученную и обработанную информацию. Без мудрой и реалистичной политики даже самые своевременные и достоверные разведывательные данные будут бесполезны и не принесут никакой пользы предприятию. Поэтому полезность и необходимость системы корпоративной безопасности полностью зависит от того, как она направляется и используется людьми, принимающими стратегические для компании решения.

ЛЕКЦИЯ 10.
ИССЛЕДОВАНИЕ СЛУЖБОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ АНОНИМНЫХ ТЕКСТОВ НА ПРЕДМЕТ ВЫЯВЛЕНИЯ ИХ АВТОРОВ

1. Экономическая разведка - организация добывания своевременной информации для выработки руководством компании наиболее рациональных управленческих решений по вопросам финансово-хозяйственной деятельности, соответствующих складывающейся обстановке, стратегическим целям и оперативным задачам, позволяющим избежать неудач в своей деятельности.

Сбор, анализ и обработка данной информации является наиболее ответственным звеном не только системы обеспечения безопасности, но и маркетинга, поскольку на ее основе вырабатывается политика компании.

Сбор, анализ и обработка данной информации является наиболее ответственным звеном не только системы обеспечения безопасности, но и маркетинга, поскольку на ее основе вырабатывается политика компании.

2. Экономическая контрразведка и внутренняя безопасность:

- противодействие внутренней коррупции, попыткам нанесения ущерба компании ее работниками, причем речь идет не только о воровстве, но и о некомпетентности;
- проведение служебных расследований фактов подлога, хищений и иного нанесения ущерба компании;
- противодействие криминальным угрозам;
- выявление источников информации структур организованной преступности и промышленного шпионажа среди сотрудников компании;
- проверка устраивающихся на работу и периодическая профилактическая проверка лояльности персонала компании;
- обеспечение физической безопасности руководства компании и ее персонала (силовое и оперативное);
- предупреждение негативных процессов в трудовом коллективе компании, которые могут привезти к чрезвычайным происшествиям;
- обеспечение безопасности движимого и недвижимого имущества компании.

3.Информационно-аналитическая работа. Это направление обеспечивает упорядоченное накопление, научно обоснованное обобщение и анализ информации по различным направлениям безопасности компании с выделением как положительных, так и отрицательных тенденций процесса обеспечения безопасности и на этой основе выработку предложений по дальнейшему развитию данных тенденций либо их нейтрализации. В регионах оно может быть оформлено в виде одного-двух человек, поддерживающих постоянную связь с центром и накапливающих и оценивающих текущую ситуацию на местах.

4. Информационная безопасность (обеспечение защиты сведений, составляющих, как коммерческую тайну, так и жизненно важных для бесперебойного функционирования предприятия информационных массивов):

- организационно-режимные меры по работе с конфиденциальной информацией во всех ее формах (бумажные, электронные и др. носители информации);
- противодействие частным техническим разведкам;
- полный комплекс обеспечения безопасности локальных компьютеров и внутренних компьютерных сетей, обеспечение безопасной работы выходов в Интернет;
- обеспечение безопасности каналов связи.

5. Взаимодействие с местными властными структурами и правоохранительными органами. Это взаимодействие обычно строится по следующему принципу: головное подразделение безопасности - федеральная исполнительная власть и центральные аппараты МВД, ФСБ, ФСНП, ГТК и прокуратуры; подразделения безопасности на местах - территориальные органы.

Анонимки еще с незапамятных времен являются неотъемлемой частью жизни нашего общества, поэтому поиск их авторов - постоянная головная боль для сотрудников подразделений безопасности государственных и негосударственных структур. Назначение анонимных писем может быть различным: это и угроза террористического акта, слив компромата и, наконец, тривиальное вымогательство определенных денежных сумм.

У нашей страны давняя традиция написания «подметных листов». Ни одно событие в истории нашей страны не обходилось без бурной информационной подпитки анонимщиками. Кто-то действительно хотел хоть что-то поменять в этой жизни, большинство же преследовало и преследует более меркантильные цели.

В данной статье мне хотелось бы детально разобраться с методикой выявления источников анонимных писем и анализом целей их написания, так как помимо возможной утечки информации они могут быть и своеобразной «идеологической диверсией» в ходе развязанной против Вас и Вашего бизнеса информационной войны.

В подтверждении своих слов сошлюсь на книгу И.Г. Атаманенко «Шпионские страсти». Там, в качестве первооткрывателей использования метода целенаправленного потока писем с целью формирования определенного общественного мнения называется Пятое управление КГБ СССР. Именно с подачи его светлых голов, начиная с конца семидесятых годов, посольства США и Великобритании в Москве буквально засыпались мешками писем протеста по любому мало-мальски приемлемому поводу, будь то арест Анджелы Девис или размещение новых американских ракет в Европе. И как показала практика, это воздействие было весьма эффективным.В последствии, где-то к середине восьмидесятых, целенаправленная засылка анонимных писем была взята на вооружение и успешно использовалась западными спецслужбами уже против самих органов госбезопасности СССР. В эпоху «перестройки» верховные органы советской власти буквально захлестнула волна анонимок в отношении определенного контингента - сотрудников КГБ. Письма шли десятками тысяч. И если раньше невидимые правдолюбцы чаще всего старались информировать о нетрудовых доходах своего соседа или об амурных похождениях его жены, то в указанный период, они почему-то особенно невзлюбили именно отечественные спецслужбы.

Закон перехода количественного в качественное верен не только для таблицы Менделеева. Уже одно количество анонимок само по себе свидетельствовало о работе хорошо слаженного и неплохо оплачиваемого трудового коллектива. Да и качество исполнения «подметных» писем, поступавших сначала в ЦК КПСС, а затем в администрацию Президента РФ вызывает изрядные вопросы. Исполнение писем было весьма профессиональным, текст был составлен из вырезанных в газетах слов, если необходимых слов не находили, их составляли и выкладывали по слогам, на абсолютном большинстве писем не было отпечатков пальцев, т.е. полностью была исключена вероятность идентификации не только самих авторов, но и их количества.

Этот непрерывный бумажный поток совместно с оголтелой разоблачительной вакханалией в СМИ явно выполнял чей-то заказ - опорочить органы госбезопасности в глазах тогдашнего руководства СССР. Способ был очень дешевый, но эффективный. Проверка следовала за проверкой, выбивая из рабочей колеи целые подразделения, на недели и месяцы, практически парализуя их повседневную работу.

Но вернемся к реалиям сегодняшнего дня. Что же все таки можно реально сделать для выявления авторов анонимных текстов? Если анонимка легла непосредственно Вам на стол, то алгоритм работы тут более - менее ясен. Ну а если не на Ваш стол?

Для сбора сигнальной информации об анонимных текстах в Ваш адрес необходимо наличие специальной системы информирования о данных фактах. Факты появления злобных измышлений или частичной относительно достоверной информации о Вас и Вашем бизнесе не должны застать вас врасплох. Поэтому, как завещал великий Дейл Карнеги, заводите друзей и связи во всех контролирующих и т.д. и т.п. органах.

Кстати, по заявлению в СМИ одного из старших офицеров налоговой полиции одним из самых эффективных способов выявления злостных неплательщиков налогов являются анонимные письма, авторами которых в большинстве случаев бывают обманутые жены и брошенные любовницы бизнесменов.

Естественно, что на самом первом этапе выявления фактов рассылки анонимных писем о Вас и Вашем бизнесе необходимо тщательно проанализировать насколько излагаемая в документе фактура может быть подтверждена документально или свидетельскими показаниями, и предусмотреть план мероприятий по нейтрализации возможных последствий. В этом плане, очень интересно проследить, насколько связаны сообщения в СМИ с излагаемой в документе информацией. И решить для себя, не скрывается ли за данным документом попытка своеобразной «идеологической диверсии».

При получении информации о распространении анонимных писем в отношении Вас или Вашего бизнеса необходимо обязательное исследование оригинала письма (далее документ), желательно также получить и оболочку, в которой оно пришло (конверт или что-то подобное). Причем наличие именно оригинала, а не копии, очень важно для проведения дальнейшего расследования по многим причинам.

Можно предложить следующий алгоритм исследования имеющегося анонимного текста.

1. Исследование способа распространения и доставки документа: почтовое отправление, доставка курьером, расклейка в виде объявлений, скрытая доставка, связанная с проникновением на охраняемый объект.

2. Исследование конверта при почтовой отправке: место отправления, дата отправления, наличие штампов отделений связи, индивидуальные особенности конверта.

3. Исследование материала-носителя текста документа: насколько он соответствует тому, что имеется в вашем офисе, какие отличительные особенности он имеет, насколько носитель дефицитен, и где можно найти аналогичный материал.

4. Способ нанесения информации на документ: рукописный, составлен из наклеенных букв газет и журналов, пишущая машинка, принтер компьютера, индивидуальные особенности техники нанесения информации на носитель.

5. Психографологическая экспертиза решает вопросы зависимости между почерком объекта и чертами его характера, психическим состоянием и поведенческими характеристиками. Данный вид экспертизы позволяет диагностировать исследуемый объект, выполнив экспертную оценку всех его характерологических черт личности по образцу его почерка

К сожалению, данный вид экспертизы в реальных условиях мало применим, т. к. требует привлечения экспертов очень высокой квалификации. Аналогичное исследование с помощью компьютерных методик затруднено из-за высокой стоимости данного программного обеспечения.

6. Морфологический и контент-анализ в ряду методов обработки информации занимают особое место. Причем они оба настолько просты и универсальны, что успешно используются как аналитиками Спецслужб; так и экспертами коммерческих структур Даже небольшая фирма, не располагающая значительными материальными и интеллектуальными ресурсами в состоянии провести подобные исследования и получше определенные результаты. Контент - анализ занимается исследованием смыслового содержания текста, морфологический - его внешней формой. При их совместном использовании они позволяют достаточно полно нарисовать психологический портрет автора анонимного текста. Данные методы пригодны также и для исследования разговорной речи объекта оперативного интереса.

В основном эти методики базируются на нескольких принципах психологического плана.

1. Каждым человек сугубо индивидуален, и следовательно, создавая какой-то текст, от обязательно привнесет в него что-то личное, то есть информацию о самом себе Задачи состоит в том, чтобы правильно расшифровать скрытое между строк. Любой текст обязательно несет в себе информацию о своем авторе, об его жизненном кредо, опытности, профессиональном и общеобразовательном уровне.

2. Достаточно ясно и то, что любой текст отражает текущее состояние автора, его психики и эмоций, Вспомните самого себя во время написании чего-либо, и Вы сразу поймете, что каждый человек проецирует себя самого на то, что он пишет.

К сожалению, достаточно трудно идентифицировать тексты, написанные формализованным казенным языком. Чем текст ближе к стереотипу, чем труднее понять сущность его автора И наоборот, чем больше текст отходит от шаблона, тем больше различной информации о его авторе можно получить.

Хочу отметить, что в данной статье будут даны только общие основы анализа, и к вершинам мастерства Вам по большей мере придется идти самостоятельно. Помимо этого надо обязательно учитывать, что любые предположения всегда носят исключительно вероятностный характер, поэтому не спешите делать по ним глобальные выводы, и пытаться строить математически точные и далеко идущие прогнозы.

Как я уже говорил контент - анализ является одним из самых эффективные средств оценки текста. Эта методика имеет давнюю историю. Первые упоминания о его применении на практике относятся к восемнадцатому веку, в то время подсчитывая частоту появления тем, связанных с Христом, церковь принимала решения о еретичности той или иной книги, и, следовательно, богопослушности того или иного автора. Т.е. с самого начала именно репрессивный аппарат был его самым ярым приверженцем.

В новейшей истории самым ярким примером использования контент-анализа является работа. американской военной цензуры в годы второй мировой войны. Основанием для обвинения в связях с нацистами редакторов СМИ служило выявление схожести в повторении определенных тем на страницах тех или иных изданий. Как метод количественного изучения содержания информации для обнаружения в ней интересующих нас фактов контент - анализ строг, систематичен и, что самое главное, ориентирован на количественные показатели. Задача метода сводится к тому; чтобы просчитать, как представлены в имеющемся информационном массиву те или иные смысловые единицы

Алгоритм анализа:

1. Выбор смысловых единиц текста подлежащих исследованию.

2. Диагностика каждой смысловой единицы на предмет выявления того или иного психологического фактора.

3. Формулировка выводов и предположений по каждой смысловой единице об эмоциональном состоянии и психологическом описании объекта.

4. Синтез в итоговом заключении всех выявленных моментов, заслуживающих внимания.

Необходимо отметить, что смысловой единицей при анализе может быть слово, символ (наименьшие единицы). Смысловой единицей, представляющей собой отдельное высказывание об отдельном предмете может быть какая-то тема.

Существуют достаточно четкие требования к возможной единице анализа:

а) она должна выражать какое-то значение,

б) одновременно она не должна выражать слишком много значений,

в) она должна легко идентифицироваться,

г) к тексте должно быть эначительное количество единиц, необходимое для создания выборки.

Необходимо определиться с тем, какие именно смысловые единицы Вы будете искать. Это могут быть оскорбления и угрозы, призывы и порывы благородного негодования, элементы личной позиции автора или что-то другое, т. е. то что Вам необходимо продиагностировать.

Следующий шаг это определение того, по каким критериям должен будет осуществляться подсчет. Чаще всего это частота употребления.

Очень показательно в этом плане количество разных слов, которые человек употребляет в своей речи в текстовых массивах в 100, 200, 500 и 1000 слов, У шизофреников, например, это количество намного меньше. Тексты, написанные ими, идентифицируются по следующим показателям:

- все изображается в негативном тоне,
- они ориентированы на прошлое,
- очень много места уделено собственным переживаниям и высказыванию собственного мнения обо всем.

Проведенный учеными анализ лингвистических различий между шизофреником и нормальным человеком, показывает например, что количество прилагательных на 100 глаголов, у нормального человека значительно больше, чем у шизофреника.

При анализе стоит обратить внимание на следующие ключевые моменты:

- насколько автор текста привержен у шаблонности формы письма,
- информативность стиля текста,
- стиль и манера изложения, увод мысли в сторону, витиеватость - сухость, размытость понятий, канва послания, уходы и т.д,
- общая структура текста: концепция построения письма (планомерность изложения или хаотичная импровизация),
- правильность построения отдельных фраз — синтаксис и пунктуация,
- лексика и фразеология языка: удельный вес различных компонентов, наличие ненормативной лексики,
- частота употребления слов,
- расставленные акценты внимания,
- эмоциональная окраска текста и возможное эмоциональное состояние автора,
- наличие состояния аффекта при написании документа,
- наличие или отсутствие у автора чувства юмора. Ярко выраженный сарказм текста обычно свидетельствует о наличии у автора документа определенных неврозов, более известных как человеческие комплексы,
- адекватность оценки автором описываемых событий
- смыслообразуюший мотив написания документа и определение общих целей его воздействия Смыслообразующий мотив определяет главную идею написания автором данного документа.

Наиболее эффективным контент - анализ бывает если выполняются три условия развития коммуникативных процессов:

1. Наличие непрямого выхода на автора. Если при разговоре, мы имеем возможность, в случае чего переспросить собеседника, то в ситуации с анонимным текстом данный поворот событий практически невозможен, т.е. в данном случае мы имеем только непрямой выход на автора.

2. В случаях с анонимным текстом очень важен как сам языковой фактор, который является решающим для проводимого исследования, так и доступный для исследования языковой подтекст.

3. Индивидуальное прочтение одного-двух текстов не дает возможности оценить того, что показывает анализ целого массива. В любом случае для качественного анализа необходимо наличие достаточно большого объема текстового материала.

4. При обработке текстов малого объема, а анонимные документы чаще всего имеют небольшой объем, качественный анализ имеет больше преимуществ перед количественным. Если обратится к истории, то например в семидесятые годы аналитики американской разведки при анализе китайских средств массовой информации отметили смену одного из терминов и предположили переход Китая к более агрессивным действиям, вскоре за этим действительно последовал вьетнамо-китайский пограничный вооруженный конфликт.

5. На практике отслеживая и анализируя анонимные письма с угрозами исходящими из одного источника, также можно сделать определенные выводы либо о нарастании у их авторов агрессивности к объекту угрозы, либо наоборот, об утрате ими всяких надежд на исполнение желаемого и простому эмоциональному выбросу бессильной злобы.

6. Кстати, методики контентного и морфологического анализа текста также применяются и при анализе прессы. Подробнее об аналитической обработке открытых источников, смотри «БДИ» № 3 за 1999 год. Эти методики в данной статье не рассматривались, но их применение возможно и в описываемых там случаях.

7. Интенсивность распространения документа и стоимость усилий по распространению анонимного текста. Анализ целевого назначения документа включает в себя несколько моментов. Список адресатов рассылки документа (некоторые указывают их в документе, а при наличии грамотно отработанной системы оповещения о появлении подобных документов это устанавливается оперативным путем) показывает насколько автор ориентируется в хитросплетениях государственных правоохранительных, налоговых и контролирующих органов. Насколько он адекватен в оценке значимости для подобных структур информации, излагаемой в документе.

Следующим шагом после проведения мероприятий по составлению психологического портрета автора анонимного текста, следует выявление круга лиц имевших доступ к информации, изложенной в документе с определением временного промежутка, к которому относятся события изложенные в документе.

Предметом тщательного анализа также должно стать выявление круга лиц заинтересованных в предании изложенных в документе сведений гласности, это могут быть конкуренты, сотрудники Вашей организации, имеющие обиды на руководство, просто завистник и т.д. и т.п.

Простое совмещение очерченных предварительными исследованиями множеств (групп лиц относящихся к той или иной категории) может позволить выявить анонимщика аналитическим путем или сузить круг подозреваемых и дать новые направления для информационно-поисковой работы Службы Безопасности

ЛЕКЦИЯ 11.
ПРЕДСТАВЛЕНИЕ О СИСТЕМЕ БЕЗОПАСНОСТИ ТОРГОВОГО ПРЕДПРИЯТИЯ

В самом начале статьи хочу обратить внимание читателей на то, что данный материал является моим мнением по обсуждаемой теме и не претендует на инструкцию к действию. Все изложенное необходимо для понимания того, как может вестись данная работа, какие методы могут использоваться против кого бы то ни было и не более того.

Прежде чем говорить о проблемах и путях их решения необходимо для себя четко определить, что такое безопасность и из чего она состоит. Очень многие руководители вкладывают в понятие системы безопасности лишь физическую охрану объекта, некоторые добавляют систему контроля за персоналом, еще меньшее число управленцев добавляют систему наблюдения за конкурентами и рынком. Это ошибочное суждение при неблагоприятном стечении обстоятельств приносит огромные потери.

На мой взгляд безопасность чего либо это во первых такое состояние исследуемого предмета, при котором нет ни внутренних ни внешних угроз его нормальному существованию. Во вторых под безопасностью нужно понимать комплекс мероприятий направленных на недопущение и/или прекращение дестабилизации системы. Исходя из этого система безопасности некоего экономического объекта это комплекс мер и мероприятий направленных на выявление дестабилизирующих факторов (ДФ), предупреждение проявления ДФ, пресечение проявления ДФ, устранение последствий воздействия ДФ. Исходя из вышесказанного, безопасность затрагивает все без исключения области жизнедеятельности предприятия.

Вначале разговора необходимо определится с терминологией. Это становится особенно актуально, когда идет общение между людьми занимающими разные социальные ниши, имеющие разное образование, разный жизненный и профессиональный опыт. Итак, предприятиям предлагаю называть структуру, независимо от организационно-правовой формы и формы собственности, которая с одной стороны занимается оптовой закупкой и/или производством товаро-материальных ценностей (ТМЦ), а сдругой стороны - продажей этих ТМЦ другим лицам. Дестабилизирующий фактор - это любое изменение, приводящее к нарушению нормальной (планируемой) работы предприятия. Злоумышленник (ЗУ) - лицо, физическое или юридическое, стремящееся нанести предприятию ущерб.

Теперь, для рассмотрения конкретных ситуаций, нужно понять общую картину деятельности торгового предприятия и те элементы, которые могут быть подвергнуты атаке злоумышленников. Выбор пал на торговое предприятие поскольку любая коммерческая структура зарабатывает тем, что продает что либо - это может быть товар, услуга, все что угодно, но элемент продажи присутствует всегда. Проще всего представить себе элементы деятельности торгового предприятия можно анализируя движение ТМЦ. Предположим предприятие работает. В этом случае лицо, ответственное за снабжение, находит поставщика и привлекает его к сотрудничеству. Далее следует активное сотрудничество. В результате чего ТМЦ поступают на предприятие и начинается их реализация. В процессе реализации привлекается потребитель, который и приобретает ТМЦ. Казалось бы все просто, но увы нет. Возможности для дестабилизации у ЗУ есть с самого первого шага предприятия в этой цепочке и для их понимания нужно четко обозначить кто может оказаться злоумышленником.

К *первой* группе можно отнести физических лиц, желающих получить средства за счет других. Это могут быть простые воришки, грабители, нечистоплотные работники и т. п.

Ко *второй* группе, на мой взгляд, следует отнести конкурентов и организованную преступность.

В *третью* группу, несмотря на весь патриотизм, просто необходимо включить государство, со всеми его силовыми, фискальными, контрольными и прочими органами, и крупные монополии поскольку они пользуются значительной поддержкой (в том числе и незаконной) государства.

Причем представители любой из трех групп могут объединяться в самые разнообразные симбиозы.

Итак, первый этап работы торгового предприятия, нахождение поставщика и привлечение его к сотрудничеству. ЗУ может использовать следующее:

- предоплата несуществующего товара
- вовлечение в финансовые махинации
- подсовывание несуществующей/недееспособной фирмы
- подталкивание к заранее убыточному сотрудничеству
- перекупка перспективных поставщиков
- дискридитация предприятия
- навязывание крыши

Наиболее реальное проявление ЗУ второй группы, второй в сочетании с первой, возможно участие и третьей группы, но это уже игра по крупному - "высший пилотаж", что само по себе явление редкое. Причины могут быть следующие:

- отсутствия системы проверки потенциальных партнеров на предмет состоятельности и благонадежности
- отсутствие системы коммерческой тайны
- отсутствия системы контроля за работой персонала
- отсутствие системы изучения конкурентов и анализа ситуации на рынке
- отсутствие системы анализа и противодействия криминалу
- халатное отношение персонала к своим обязанностям
- личная заинтересованность работника

Второй этап - активное сотрудничество с поставщиком. Для ЗУ есть следующие возможности:

- поставка некондиционного товара
- поставка не того товара который заказывали
- поставка некомплектного товара
- утрата/порча оплаченного товара в пути
- утрата/порча оплаченного товара на складе
- неполная поставка
- просрочка поставок
- навязывание крыши

Здесь также могут проявится все три группы ЗУ, причем проявление третьей имеет гораздо большую вероятность. А причины такие же:

- отсутствия системы проверки потенциальных партнеров на предмет состоятельности и благонадежности
- отсутствие системы коммерческой тайны
- отсутствия системы контроля за работой персонала
- отсутствие четкой системы официальной финансовой отчетности
- отсутствие системы анализа ситуации
- отсутствие системы анализа и противодействия криминалу
- халатное отношение персонала к своим обязанностям
- личная заинтересованность работника
- отсутствие нормальной системы физической охраны

Третий этап - реализация ТМЦ. У ЗУ появляются новые возможности:

- хищение ТМЦ со склада и из торгового зала
- порча ТМЦ на складе и в торговом зале
- приостановка деятельности предприятия
- дискридитация предприятия
- "очернение" свойств ТМЦ
- навязывание крыши

На этом этапе могут легко проявиться все три группы ЗУ.

Причины в общем примерно те же:

- отсутствия системы контроля за работой персонала
- отсутствие системы коммерческой тайны
- отсутствие четкой системы официальной финансовой отчетности
- отсутствие системы контроля конкурентов и анализа ситуации
- отсутствие системы анализа и противодействия криминалу
- халатное отношение персонала к своим обязанностям
- личная заинтересованность работника
- отсутствие нормальной системы физической охраны

Вырисовывается достаточно четкая картина. На основе этой картинки можно определиться с целями системы безопасности. Цель, ради достижения которой строится вся система безопасности, это "исключить неплановые расходы", как может помочь система безопасности этого достичь? Посредством исключения воздействия на бизнес негативных факторов (негативность в данном случае рассматривается как способность нарушить плановое развитие событий либо как способность к дестабилизации сложившегося положения). Система безопасности должна включать в себя большое, но вполне определенное количество подсистем, отвечающих за свои участки деятельности.

Практически деление на подсистемы было показано в начале:

1 подсистема - выявления дестабилизирующих факторов

2 подсистема - предупреждения (недопущение) воздействия ДФ

3 подсистема - выявление случаев дестабилизации, пресечение проявления ДФ

4 подсистема - принудительная стабилизация, устранение последствий воздействия ДФ

Разберем более подробно.

1 подсистема,- ее задача выявить ДФ, т.е. основываясь на опыте, каких то косвенных данных, конкретных фактов, анализе ситуации, предвидение возникновения ДФ, либо своевременно фиксирование появления новых ДФ. Сюда например входят такие элементы как:

Прогнозирование ситуации на рынке

- наблюдение и анализ экономической ситуации в стране
- наблюдение и анализ тенденций на рынке

Прогнозирование ситуации в компании

- анализ технологических процессов в компании
- анализ межличностных отношений
- анализ адекватности поведения сотрудников
- наблюдение за внутренними финансовыми потоками

2 подсистема,- ее задача предупредить воздействие ДФ, т.е. основываясь на данных первой подсистемы планировать и проводить работу так, чтобы не дать возможности проявиться ДФ, либо сделать проявление ДФ бессмысленным. К ней можно отнести:

Оптимизация структуры предприятия

- разработка оптимальной структуры предприятия
- разграничение полномочий сотрудников и исключение дублирования

Оптимизация технологий и процессов в предприятии

- разработка (планирование) процессов
- проверка партнеров на благонадежность/платежеспособность
- финансовый контроль
- дублирование ценной информации

Оптимизация режима

- разработка внутреннего трудового распорядка
- разработка внутри объектового режима
- разработка института коммерческой тайны
- использование преимуществ зарегистрированного товарного знака и авторского права
- физическая охрана объекта, ТМЦ, персонала
- видеонаблюдение за объектом, ТМЦ, персоналом
- противопожарная безопасность
- охранная сигнализация

Оптимизация микроклимата в коллективе

- выявление лояльности работников и кандидатов
- создание атмосферы нетерпимости к мошенничеству

3 подсистема,- ее задача выявлять случаи дестабилизации и пресекать проявление ДФ, т.е. остановить развитие вывленного ДФ.

Это:

Выявление фактов мошенничества и ошибок персонала

Контроль за выполнением должностных обязанностей
- контроль рабочего времени
- контроль эффективности работы
- контроль отчетности

Контроль контактов
- наблюдение, опрос
- контроль АТС
- видеонаблюдение

Контроль доходы/расходы
- наблюдение за бытом
- сравнение доходов и расходов

Контроль соблюдения технологических процессов
- ОТК
- финансовый контроль/бухгалтерия
- документооборот и делопроизводство

Выявление фактов недобросовестной конкуренции

Сбор информации о конкурентах
- получение общей (официальной) информации
- получение специальной (оперативной) информации
- взаимодействие с силовыми структурами

Наблюдение за рынком
- сбор общей информации
- сбор специальной информации

Проверка персонала на лояльность
- наблюдение
- провокации
- взаимодействие с силовыми структурами

Контроль технической защищенности
- наблюдение
- плановые проверки
- внеплановые проверки

4 подсистема,- ее задача стабилизировать систему и устранить последствия влияния ДФ, т.е. привести систему в то состояние (предприятие), в котором она прибывала до проявления ДФ.

Восстановление ситуации и реституция
- добровольное возмещение
- возмещение через суд
- силовое возмездие
- восстановление имиджа
- возврат ценных работников

Возмездие
- экономическое возмездие
- ущерб имиджу
- силовое возмездие

Нетрудно заметить, что выполняемые функции подсистем пересекаются. А соответственно проводя какие то работы для достижения одной цели нужно помнить, что результаты могут понадобиться совершенно для другого. Поэтому очень важно с первого дня взять себе за правило фиксировать всю получаемую информацию. Каким образом организовать хранение и структуризацию такой информации будет показано в соответствующей части.

Теперь нужно разобрать каждую из этих функций примерно по такому плану:

1) что она (функция) делает и зачем нужна

2) как, с минимальными затратами сделать чтобы эта функция выполнялась - буквально пошаговый план реализации.

Именно этому и посвящены дальнейшие разделы.

Хотелось бы заострить ваше внимание на том, что данная рекомендация не является панацеей или инструкцией, претендующей на звание абсолютно точной. В ней рассматривается наиболее часто встречающаяся ситуация, но в каждом конкретном случае есть свои нюансы, требующие отдельной проработки.

Постановка цели. Подбор руководителя. Разработка базовой документации.

Теперь, имея общее представление о системе экономической безопасности предприятия можно сделать первый шаг в ее создании -определить то, что вы хотите достичь, иначе говоря, сформулировать задачи. А для постановки реально выполнимой задачи необходимо оценить сложившуюся ситуацию. Проще всего, на мой взгляд, сделать это по следующей схеме:

- определить тот уровень финансирования, который вы в состоянии пустить на СБ
- оценить уровень угроз вам и вашему бизнесу
- расставить акценты в работе системы безопасности и определить задачи

При определении уровня финансирования системы безопасности нужно учитывать некоторые обстоятельства:

Во-первых - система безопасности это непроизводственная сфера, она не зарабатывает деньги, она способствует их сохранению, хотя вполне реально сделать так чтобы и описываемая система приносила доход в виде денег. Поэтому, чаще всего, оценивать ее рентабельность можно только по косвенным показателям и то с определенной долей достоверности. Как оценить, к примеру, предотвращение грабежа кассы магазина, если злоумышленник отказался от своих планов до начала их реализации, увидев, что не сможет преодолеть систему безопасности.

Во-вторых полноценная отдача от системы безопасности в целом может быть получена примерно через полгода после начала ее создания, хотя отдельные подсистемы могут начать активно функционировать и выполнять поставленные задачи с первых дней.

В-третьих безопасность сама по себе довольно дорогая штука - она требует серьезных вложений. Для примера стоимость простенькой системы видеонаблюдения состоящей из 4 видеокамер, монитора, квадратора и видеомагнитофона колеблется в районе полутора тысяч долларов США, и это без монтажа, а стоимость одного часа наружного наблюдения стоит в среднем сто долларов.

Если после этих раздумий вы еще хотите создать свою полнокровную систему безопасности, то нужно переходить к оценке потенциальных угроз. Удобнее такую оценку производить рассматривая внешние и внутренние факторы, влияющие на ваш бизнес. При этом особо обратите внимание на следующие моменты:

- на сколько вы доверяете своим сотрудникам и как сильно они могут вам "насолить"
- в каком состоянии находится ваш сектор рынка, есть ли на нем "монстры", как часто происходит передел сфер влияния, насколько остро идет борьба за клиента, как проявляется конкуренция, какие у вас отношения с конкурентами и кто за этими конкурентами стоит
- как складываются у вас и у вашего предприятия отношения с государственными органами, в особенности с правоохранительными и фискальными
- какие у вас отношения с криминалом
- на сколько легко можно реализовать производимый вами товар (услуги) на черном рынке (без документов)

После получения ответов на эти вопросы можно будет говорить о постановке задачи и о том какие части СБ и как нужно развивать. Если наибольшую опасность представляют сотрудники, то соответственно больший упор нужно делать на контрразведывательное обеспечение, а при гипертрофировании угрозы со стороны конкурентов - на разведывательное обеспечение. Не менее важным является и ответ на вопрос кто будет заниматься созданием и управлением системой безопасности. Если вы возьмете все на себя то нужно быть готовым к постоянному цейтноту и учебе. Поэтому лучше всего подобрать стороннего человека, который сможет целиком посвятить себя решению данных проблем.

Сразу подобрать человека с нужными качествами вряд ли получится - придется долго перебирать. При появлении первых кандидатов нужно проводить их комплексные проверки, которые обязательно должны включать в себя следующее:

- сбор официальной информации и формальные проверки
- заполнение специально составленной анкеты
- предоставление копии паспорта, трудовой книжки, военного билета, документов об образовании, водительского удостоверения и т.п.
- проверка полученных документов на подлинность и сопоставление содержащейся в них информации с анкетными данными
- получение информации из баз данных
- получение отзывов с предыдущих мест работы по официальным каналам
- ряд собеседований (минимум три)
  - первое собеседование проводит кадровик и в процессе беседы уточняет полученные из документов данные, также получает общее представление о кандидате
  - второе собеседование также проводит кадровик устраняя разногласия между предоставленной информацией и полученной из других источников
  - третье собеседование проводит руководитель, имея на руках результаты предыдущих собеседований и проверок, ставятся конкретные проблемы и выясняются знания и профессионализм
- сбор субъективной информации и неформальные проверки
- неформальное общение (опрос) с бывшими сослуживцами, соседями
- создание искусственных ситуаций (провокации) и наблюдение за тем как человек реагирует, как ведет себя
- наблюдение за поведением в стандартных ситуациях и сопоставление с декларируемыми идеями и принципами
- последним этапом в предварительной проверке является сопоставление всей полученной информации, и принятие решения о пригодности кандидата.

Важно во время проведения собеседований фиксировать их содержание на магнитофон для дальнейшего более глубокого анализа. Для проверки профессионализма можно использовать такой прием как "гонка с преследованием", суть его сводится к тому, что человека просят дать совет в решении какой то отвлеченной задачи связанной с его профессиональной деятельностью, предварительно получив информацию как эта задача должна быть решена. И по тому как быстро он приходит к правильному решению можно судить о его профессионализме. Второй способ заключается в углублении в суть вопроса настолько, что нужно оперировать не общими данными, а конкретными цифрами и способами. Можно дать проверочные задания такие как:

- составить концепцию безопасности фирмы
- составить план мероприятий по созданию системы безопасности фирмы
- составить перечень затрат для решения конкретных вопросов безопасности
- выяснить информацию общего плана о каком то юридическом лице или человеке
- предложить варианты оснащения объекта техническими средствами безопасности

Прохождение кандидатом всех проверок еще на означает его абсолютную пригодность, поэтому нельзя сразу отдать ему в руки все козыри. Целесообразнее договориться об испытательном сроке, в течении которого кандидат начнет создание системы безопасности с менее проблемных узлов, например с создания физической охраны объекта, режима объекта, системы контроля доступа... И по тому как он будет работать можно будет судить и о его отношении к делу в целом.

После того как человек найден нужно четко определить ему цель - поставить задачу, выяснить его видение проблемы, найти наиболее подходящий путь и составить общий план с указанием затрат и сроков.

Еще один вопрос, который необходимо решить с самых первых шагов это создание соответствующей правовой базы. Сюда входит следующее:

- положение о коммерческой тайне
- список информации, отнесенной к коммерческой тайне
- положение о делопроизводстве
- положение о внутриобъектовом режиме или о внутреннем трудовом распорядке
- соглашение о неразглашении коммерческой тайны

Наверное необходимо разобрать каждый документ отдельно. Начнем с "Положения о коммерческой тайне". Этот документ нужен для четкого определения режима использования, хранения, перемещения и уничтожения сведений, содержащих коммерческую тайну. В нем необходимо описать кто и как может работать с коммерческой тайной, кто и как определяет принадлежность информации к категории коммерческая тайна, какова ответственность за разглашение коммерческой тайны и каков порядок действий сотрудников в случае обнаружения факта разглашения коммерческой тайны. По большому счету все описанные здесь документы нужны для возможности привлечь к ответственности нерадивого сотрудника.

Соглашение о неразглашении коммерческой тайны в принципе нужно для тех же целей, что и Положение о неразглашении коммерческой тайны. Сложность заключается в том, Положение регулирует данный вопрос с точки зрения трудового законодательства, а Соглашение - с точки зрения гражданского.

Список информации отнесенной к коммерческой тайне является приложением к Положению о коммерческой тайне. В нем ясно и четко перечисляется какая информация отнесена к категории коммерческой тайны. Причем чем точнее описывается каждый вид информации тем лучше. Нужен он во первых для ясного представления сотрудниками того, что отнесено к коммерческой тайне и во вторых (как следствие первого) для возможности доказать прямой умысел в случае разглашения.

Положение о делопроизводстве является документом, описывающим порядок создания, движения и хранения документов. Важность его заключается в подведении всех документов на предприятии под единый стандарт закреплением общеобязательных правил по передаче и хранению документов. А зная точный порядок легче отследить где, когда и по чьей вине произошел сбой в работе.

Положение о внутриобъектовом режиме или о внутреннем трудовом распорядке описывают режим работы объекта, режим работы подразделений и отдельных работников, порядок допуска сотрудников и посетителей на объект, уровни доступа и т.п.. Эти два документа достаточно схожи и поэтому могут быть объединены в один. Они также нужны для четкого представления существующих (утвержденных) порядков и доказывания вины сотрудника.

Указанные шаги и процедуры описаны очень кратко, но имея такое весьма урезанное описание уже можно исключить наиболее распространенные ошибки при создании системы безопасности и понимать что и зачем делать. Достаточно важным моментом является и понимание того, как можно использовать уже имеющиеся возможности на предприятии для обеспечения безопасности его функционирования, а соответственно с какими структурами и каким образом может и должна взаимодействовать система безопасности. Наиболее часто встречающееся взаимодействие описано ниже.

Маркетологи

Легальное получение информации. По роду своей деятельности маркетологи постоянно имеют свежую и достоверную информацию об официальной стороне бизнеса конкурентов. Собирая информацию о данном секторе рынка, общаясь с сотрудниками конкурирующих компаний маркетологи и менеджеры побочно получают сведения, которые могут пригодиться в работе системы безопасности: координаты конкурентов, их представительств, номенклатуру продукции и ее цены, ФИО сотрудников конкурента, их увлечения, пристрастия, частную информацию, поставщиков/клиентов конкурирующей фирмы и т.п. Все это хорошее подспорье в работе системы безопасности.

Анализ тенденций на рынке. Отслеживая регулярно цены конкурентов, рекламу конкурентов сотрудники маркетингового отдела видят изменения в данном секторе рынка. А по изменению этих показателей у конкретной фирмы можно судить о политике, проводимой в данный момент ее руководством и с определенной долей уверенности судить о планах. Так уменьшение цены говорит либо о начале демпинговой политике, либо о распродаже остатков, усиление рекламной компании явно указывает на начало экспансии на рынке. Соответственно в случае значительного изменения цен и/или рекламы информация об этом должна быть передана в систему безопасности, желательно с приведением показателей по данным фирмам за три последних месяца. Увеличение объемов продажи определенного вида продукции указывает на увеличение спроса на эту продукцию, что может быть связано с сезонными либо структурными изменениями рынка. Также имеет определенное значение составление общего представления о процессах, происходящих на рынке: изменение ценовой политики, общее увеличение или уменьшение цен, происходят ли глобальные изменения.

Восстановление имиджа. В случае нанесения ущерба имиджу предприятия работники системы безопасности совместно с маркетологами разрабатывают мероприятия по восстановлению опороченного имени и реализуют каждый свою часть программы.

Руководители направлений

Анализ технологических процессов. Руководители направлений постоянно контролируют выполнение технологических процессов (от переговоров с клиентом и заключения договора до изготовления деталей и сборки). Они видят как происходит исполнение того или иного задания и почему происходят сбои. На основании этих наблюдений можно прогнозировать возникновение нештатных ситуаций и либо их предотвращать либо ослаблять их негативное влияние.

Разработка (планирование) процессов. Основываясь на условиях производственной необходимости и анализе существующих технологических процессов можно планировать новые процессы заранее избегая моментов способных повлечь возникновение нештатной ситуации.

Разработка внутриобъектового режима. При разработке внутриобъектового режима необходимо четкое представление всех технологических процессов, происходящих на объекте для исключения ситуации когда режим мешает работе.

Создание атмосферы нетерпимости к мошенничеству. Путем идеологической, разъяснительной, просветительской работы и системы стимулирования в коллективе создается атмосфера нетерпимости к обману, лжи, мошенничеству и т.п.

Поощрение и наказание. Видя отношение к работе каждого сотрудника и его квалификацию руководители направлений принимают решение о стимулировании. Своевременное принятие решений по этому вопросу и их реализация благотворно влияют на микроклимат в коллективе. Постоянный контроль выполнения заданий не дает возможности отвлекаться на непроизводственные дела.

Управление персоналом

Проверка кандидатов. Проводя набор персонала УП осуществляет проверку кандидатов на проф пригодность при осуществлении данного мероприятия совместно с СБ можно значительно повысить достоверность и глубину получаемой информации. Кроме того параллельно с оговоренной проверкой (и под ее прикрытием) можно проводить и проверку на склонность к мошенничеству, проверку на связь с криминалом, силовыми структурами, с конкурентами.

Анализ рынка труда. Регулярно проводя работу по подбору персонала, УП видит положение дел на рынке труда и происходящие тенденции, а именно:

- какие профессии (специалисты) каким спросом пользуются
- как изменяется спрос и в зависимости от чего
- каковы предложения по тем или иным вакансиям
- какие специалисты требуются той или иной фирме

На основании этого можно прогнозировать:

- изменение спроса и предложения на ту или иную специальность, а значит и оплату
- потребности конкурентов, а значит и изменения в их политике

Анализ межличностных отношений. Общаясь с персоналом сотрудники УП получают информацию об отношении одних работников к другим, что позволяет прогнозировать и предупреждать возникновение конфликтов. Информация об увлечениях работника, его наклонностях, стиле его поведения, круге общения и т.п. дает возможность оценить работника с точки зрения склонности к мошенничеству.

Анализ адекватности поведения. Общаясь с персоналом сотрудники УП видят как ведет себя сотрудник в той или иной ситуации, как реагирует на те или иные раздражители. Сравнивая это с поведением сотрудника ранее можно говорить о происходящих с ним изменениях и причинах их вызвавших.

Разработка, внедрение и коррекция организационной структуры предприятия. Разработка и внедрение организационной структуры предприятия позволяет через систематизацию рабочих процессов и процедур избежать ненужных затрат, неразберихи, конфликтов. А поэтому имеет важное значение для СБ, хотя и является прерогативой УП. Разграничение полномочий, являясь частью орг. структуры предприятия, тем ни менее выделяется в отдельную область поскольку позволяет существенно снизить вероятность потери коммерческой информации посредством разграничения доступа к КТ и снижает вероятность мошенничества должностных лиц.

Создание атмосферы нетерпимости к мошенничеству (совместно с руководителями направлений). Путем идеологической, разъяснительной, просвятительской работы и системы стимулирования в коллективе создается атмосфера нетерпимости к обману, лжи, мошенничеству и т.п.

Поощрение и наказание (совместно с руководителями направлений). Общеизвестная (в коллективе) и работающая система поощрения и наказания через создание ощущения стабильности благотворно влияет на микроклимат в коллективе.

Контроль рабочего времени. Проводимый совместно с руководителями направлений, службой охраны и УП контроль рабочего времени позволяет добиться более полного использования трудовых ресурсов.

Финансовая служба, бухгалтерия

Анализ общеэкономической ситуации на предприятии. Видя финансовые потоки, движение ТМЦ и изменение данных показателей финансисты, каждый на своем участке, может оценить общее положение дел, изменение и причину этого изменения.

Контроль отчетности. Практически любая сколь либо значимая операция имеет отражение в бухгалтерской документации.

Разработка института КТ. В процессе разработки института КТ необходимо оценить стоимость отдельных элементов информации отнесенной к КТ и ущерб, могущий возникнуть в случае ее утраты.

Добровольное возмещение. В случае согласия виновного лица возместить причиненный ущерб бухгалтерия рассчитывает и обосновывает общую сумму ущерба.

Юридическая служба

Разработка института коммерческой тайны. Юридическая служба принимает активное участие в разработке документов, необходимых для создания института коммерческой тайны.

Использование товарного знака. Юридическая служба разрабатывает и осуществляет общее и судебное сопровождение.

Возмещение через суд. Юридическая служба осуществляет досудебное разбирательство и судебное сопровождение всей хозяйственной деятельности.

Основываясь на вышесказанном можно говорить о том, какую систему безопасности вы хотите получить, какими путями нужно к этой цели идти и каковы могут быть затраты. Естественно это только малая часть той работы, которую предстоит сделать.

О.А. Фирсова

кандидат экономических наук, доцент
кафедры «Предпринимательство и маркетинг»
ФГБОУ ВПО «Госуниверситет – УНПК»

УПРАВЛЕНИЕ РИСКАМИ ОРГАНИЗАЦИЙ ПРЕДПРИНИМАТЕЛЬСКОЙ СФЕРЫ

(учебное пособие)

МАБИВ
АКАДЕМИЯ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Существование рисков как неотъемлемой части предпринимательской деятельности привело к необходимости разработки конкретных методов и приемов их выявления при принятии и реализации управленческих решений. Предприятия работают в различных условиях конкурентной среды, имея разную внутреннюю среду, уровень производственного потенциала, кадровый состав и т.д. В связи с этим у каждого предприятия возникают риски, непосредственно присущие только данной компании и связанные со спецификой производственной, технологической, коммерческой, финансовой и других видов деятельности. Важно своевременно их выявить и определить вероятность наступления, время наступления, а также возможный ущерб.

Методы управления рисками, получившие широкое применение в банковской деятельности, рассматриваются как инструмент управления предприятиями. Многие из этих методов могут применяться для снижения рисков в деятельности компаний различных отраслей и видов бизнеса.

Сегодня одним из наиболее прогрессивных способов повышения эффективности бизнеса по праву считается бюджетирование. Вопросам организации бюджетного процесса в предприятиях посвящено множество научных исследований и специализированной литературы. Польза бюджетирования очевидна. Поэтому многие предприятия уже внедрили или планируют внедрение соответствующих методов корпоративного управления. Именно это обстоятельство — ключевой момент в решении вопроса об организации риск-ориентированного управления предприятием. Управление рисками требует определенного уровня развития корпоративной культуры и органов корпоративного управления, во многом схожего с тем, которое необходимо для успешной организации бюджетного процесса. Это вполне логично, так как само по себе бюджетирование можно рассматривать как метод управления одним из основных рисков деятельности предприятий — стратегическим риском. Внедрение бюджетного процесса, как и организация системы управления рисками, нередко требует пересмотра организационной структуры предприятия, процедур принятия управленческих решений, а также определенной работы по повышению квалификации персонала (в том числе руководителей среднего и высшего звена) и даже набора новых сотрудников — специалистов в данной области. Более того, постановка бюджетирования может рассматриваться как первый шаг к внедрению риск-ориентированного управления предприятием, предоставляя удачную базу для дальнейшего развития, так как предполагает выполнение ряда аналогичных условий.

Целью предпринимательства является получение максимальных доходов при минимальных затратах капитала в условиях конкурентной борьбы. Реализация указанной цели требует соизмерения размеров вложенного (авансированного) в производственно-торговую деятельность капитала с финансовыми результатами этой деятельности. Вместе с тем, при осуществлении любого вида хозяйственной деятельности объективно существует опасность (риск) потерь, объем которых обусловлен спецификой конкретного бизнеса.

Цель данного учебного пособия раскрыть политику управления финансовыми рисками.

Для этого необходимо реализовать следующие основные задачи:

- дать понятие риска, рассмотреть его основные виды;
- раскрыть сущность и содержание риск-менеджмента;
- проследить тенденции риск-менеджмента в различных отраслях;
- рассмотреть методы управления финансовым риском.

ГЛАВА 1.
ПОНЯТИЕ РИСКА, ВИДЫ РИСКОВ

1.1 История развития исследования теории риска

В 1855 г. представитель немецкой классической школы Г. фон Мангольдт опубликовал работу "Действительное назначение предпринимателя и истинная природа предпринимательской прибыли". В центр своих теоретических исследований предпринимательства он поставил несение риска как важнейшую ролевую функцию предпринимателя.

Относительно теории риска Мангольдт разделил понятия "производства на заказ" и "производство на рынок". В производстве на заказ гарантирован доход, поскольку заранее ясен заказчик и определена цена, следовательно, риск минимален или вообще отсутствует.

В подобных ситуациях фактически устраняется неопределенность, сопутствующая процессу между началом производства и продажей конечного продукта. В производстве на рынок такая неопределенность присутствует, так как продукт предназначен для продажи при неопределенном спросе и неизвестной цене.

Относя деятельность предпринимателя к "производству для рынка", Мангольдт первым ставит вопрос об оценке степени риска, который несет предприниматель. Для его оценки он вводит в свое исследование фактор времени. Чем больше отрезок времени, отделяющий начало производства товара от его продажи, тем больше неопределенность успеха, больше риск возможных потерь для предпринимателя и, соответственно, больше ожидаемое вознаграждение.

Наиболее полное развитие фактор риска как важнейшая составляющая предпринимательской функции получила у американского экономиста Фрэнка Найта. Он связывал появление предпринимательского дохода не с любым видом риска. Риск, измеренный вероятностным распределением, следует относить к категории страхуемых заранее. Такой риск может учитываться в первоначальных инвестиционных решениях и превращается, по словам Ф. Найта, в "постоянный элемент издержек" в виде страховки. Поэтому такой риск не является фактором неопределенности для предпринимателя и, соответственно, служит причиной его прибыли или потерь.

Риск, по Ф. Найту, представляет собой объективную вероятность того или иного события и может быть выражен количественно, в частности в виде математически вероятностного распределения доходов. Чем больше вероятность стандартного отклонения от ожидаемой величины при таком распределении, тем меньше риск, и наоборот. В то же время существует неопределенность, означающая, что ожидаемый доход в принципе может быть получен, однако вероятность такого события нельзя измерить или просчитать. К таким ситуациям Ф. Найт относил, например, невозможность предсказать поведение или направленность потребительского спроса.

Для понимания природы предпринимательского риска фундаментальное значение имеет связь риска и прибыли. Адам Смит в "Исследованиях о природе и причинах богатства народов" писал, что достижение даже обычной нормы прибыли всегда связано с большим или меньшим риском. Известно, что получение прибыли предпринимателю не гарантировано, вознаграждением за затраченные им время, усилия и способности могут оказаться как прибыль, так и убытки.

Предприниматель проявляет готовность идти на риск в условиях неопределенности, поскольку наряду с риском потерь существует возможность дополнительных доходов. И. Шуймпетер в книге "Теория экономического развития" пишет о том, что, если риски не учитываются в хозяйственном плане, тогда они становятся, с одной стороны, источником убытков, а с другой - прибылей. Можно выбрать решения, содержащие меньше риска, но при этом меньше будет и получаемая прибыль.

Поскольку основной целью любого коммерческого предприятия является получение прибыли, то в ситуации с созданием или функционированием любого финансового субъекта возникает проблема его доходности.

Доходность - это относительная величина, характеризующая эффективность предпринимательской деятельности, представляющая собой отношение дохода к затратам, измеряется в процентах.

Если доходность предприятия, бизнеса ниже средней банковской процентной ставки или отсутствует совсем, то его существование бессмысленно с точки зрения получения прибыли. Стремление предпринимателя получить наибольшую прибыль ограничивается возможностью понести убытки. Риск предпринимательской деятельности означает вероятность того, что фактическая прибыль предпринимателя окажется меньше запланированной, ожидаемой. Чем выше ожидаемая прибыль, тем выше риск. В рамках дилеммы "доходность - риск" предприниматель вынужден ограничивать норму прибыли, страхуя себя от излишнего риска. Связь между доходностью предпринимателя и его риском в очень упрощенном варианте может быть выражена прямолинейной зависимостью.

Таким образом, можно сделать вывод, что прибыли и потери предпринимателя есть следствия риска и неопределенности, сопровождающих его решения. Сама прибыль или доход зависят от разницы между вполне определенной закупочной ценой факторов производства или товаров и той неопределенной ценой, по которой их или результирующий продукт можно будет продать.

Необходимо отметить, что неопределенность и риск в предпринимательской деятельности играют очень важную роль, заключая в себе противоречие между планируемым и действительным.

Риск объективно составляет неизбежный элемент принятия любого хозяйственного решения в силу того, что неопределенность - неизбежная характеристика условий хозяйствования. В момент принятия решения не всегда возможно получить полные и точные знания об отдаленной во времени среде реализации решения, обо всех действующих или потенциально могущих проявиться внутренних и внешних факторах.

Объективно существует и неустранимая неопределенность, имеющая место при принятии решений, приводящая к тому, что риск никогда не бывает нулевым. Следствием этого является неуверенность в достижимости поставленной цели, и в результате реализации выбранного решения намеченная цель в большей или меньшей степени не достигается. Неопределенность ситуации предопределяется тем, что она зависит от множества переменных, контрагентов и лиц, поведение которых не всегда можно предсказать с приемлемой точностью. Сказывается также и отсутствие четкости в определении целей, критериев и показателей их оценки (сдвиги в общественных потребностях и потребительском спросе, появление технических и технологических новшеств, изменение конъюнктуры рынка, непредсказуемые природные явления).

1.2 Система рисков

Понятие риска имеет различные трактовки в литературе, что усложняет изучение данного явления. Риск определяют как действие, событие, ситуацию, неопределенность, вероятность. Попробуем разобраться, что же представляет собой риск и почему его трактовки столь многогранны.

По сущности рисков вообще не сложилось до сих пор однозначного толкования. Это объясняется сложностью данного явления и его недостаточным теоретическим изучением.

В словаре Ожегова дается следующее определение риска.

Риск - возможная опасность; и риск - действие наудачу в надежде на счастливый исход. Сразу встречаем две трактовки понятия риск - как возможность и как действие.

Продолжим наше исследование: "Риск - действие, направленное па привлекательную цель, достижение которой сопряжено с элементом опасности, угрозой потери или неуспеха. Ситуация риска предполагает возможность выбора из двух альтернативных вариантов поведения; рискованного, связанного с риском, и надежного, т.е. гарантирующего сохранность достигнутого. Различают объективную и субъективную оценку проявления риска. Действия, воспринимаемые наблюдателем как осторожные, могут ощущаться самим субъектом как рискованные, и наоборот.

Таким образом, в данном определении риск понимается как действие субъекта, либо ведущее к потере, либо гарантирующее сохранность достигнутого, но не предусматривающее возможность успеха, получения прибыли и т.п., что несколько сужает понятие риска (об этом речь пойдет ниже).

В другом определении риска используется как раз более широкая трактовка риска. Риск - это деятельность субъектов хозяйственной жизни, связанная с преодолением неопределенности в ситуации неизбежного выбора, в процессе которой имеется возможность оценить вероятность достижения желаемого результата, неудачи, отклонения от цели, содержащиеся в выбираемых альтернативах.

Но правомерно ли определять риск как деятельность? Деятельность - специфически человеческая форма активного отношения к окружающему миру, содержание которой составляет его целесообразное изменение и преобразование. Таким образом, не все проявления риска на практике можно определить через форму активного отношения человека к окружающему миру. Объективно существуют такие виды риска, как риск стихийных бедствий, систематический риск и т.п. Конечно, можно их связать с проявлениями человеческой деятельности, но цепь причинно-следственных связей будет очень длинна.

Таким образом, определение риска как деятельности субъектов хозяйственной жизни не вполне корректно. Проанализируем следующее определение: риск - ситуативная характеристика деятельности любого субъекта рыночных отношений, отображающая неопределенность ее исхода и возможные неблагоприятные (или, напротив, благоприятные) последствия в случае неуспеха (или успеха).

Сущность риска состоит в возможности отклонения полученного результата от запланированного. Однако полученный результат может отклоняться от запланированного и в положительную сторону. Следовательно, можно говорить не только о риске потерь, но и о риске выгоды.

Таким образом, можно выделить две позиции относительно сущности риска. Первая состоит в том, что риск рассматривается в виде возможного ущерба от реализации того или иного решения, в виде финансовых, материальных и иных потерь. Вторая позиция выражается в том, что риск рассматривается с точки зрения возможной удачи, получения доходов или прибыли в результате реализации решения.

Риск в данном определении рассматривается как ситуация. Чем же ситуация отличается от деятельности? Ситуация - совокупность обстоятельств, положение, обстановка. Ситуация включает как совокупность событий, приведших к данному исходу в результате деятельности человека, так и объективно действующие факторы. На данном этапе нашего исследования определим риск как ситуацию. Рассмотрим, какие признаки присущи ситуации риска. Функционированию и развитию многих экономических процессов присущи элементы неопределенности. Это обуславливает появление ситуаций, не имеющих однозначного исхода. Понятие "ситуация риска" можно определить как сочетание, совокупность различных обстоятельств и условий, создающих определенную обстановку для того или иного вида деятельности.

Если существует вероятность количественно и качественно определять степень вероятности того или иного варианта, то это и будет ситуация риска. Ей сопутствуют три условия: наличие неопределенности; необходимость выбора альтернативы; возможность оценить вероятность осуществления выбираемых альтернатив.

Ситуацию риска следует отличать от ситуации неопределенности. Последняя характеризуется тем, что вероятность наступления результатов решений или событий в принципе неустанавливаема. Ситуацию же риска можно охарактеризовать как разновидность неопределенности, когда наступление событий вероятно и может быть определено, т.е. объективно существует возможность оценить вероятность событий, предположительно возникающих в результате осуществления хозяйственной деятельности.

Стремясь снять рискованную ситуацию, субъект делает выбор и стремится реализовать его. Тем самым риск предстает моделью снятия субъектом неопределенности, способом практического разрешения противоречия при неясном (альтернативном) развитии противоположных тенденций в конкретных обстоятельствах. Понимание того, что субъект столкнулся с "ситуацией риска" и ему предстоит выбор из нескольких альтернативных вариантов поведения, называется "осознанием риска". Кроме того, при рассмотрении сущности риска надо учитывать, что это понятие включает в себя не только наличие рисковой ситуации и ее осознание, но и принятие решения, сделанного на основе количественного и качественного анализа риска.

Таким образом, риск как ситуация, связанная с наличием выбора из предполагаемых альтернатив, имеет важное свойство - вероятность. Вероятность - математический признак, означающий возможность рассчитать частоту наступления события при наличии достаточного количества статистических данных. Вот почему риск нельзя определять через вероятность (вероятность - признак риска) и тем более неопределенность (отсутствующую возможность определить вероятность исхода события). Помимо этого необходимо отметить основную особенность риска - риск имеет свойство уменьшаться с увеличением предсказуемости рискосодержащего события. Под рискосодержащим событием понимается то событие, от совершения или несовершения которого зависит соответственно успех или неудача предполагаемого предприятия. И так как риск в таком случае выражается процентной (или количественной) возможностью несовершения благоприятного события, то чем больше существует возможностей предвидеть, совершится или не совершится это событие, тем меньше значение риска.

В современной экономической литературе категория риск представляет собой событие, которое может произойти или не произойти. В случае совершения такого события возможны три экономических результата: отрицательный (проигрыш, ущерб, убыток), нулевой, положительный (выигрыш, выгода, прибыль). Другими словами, риск можно охарактеризовать как опасность потенциально возможной, вероятной потери ресурсов или недополучения доходов по сравнению с вариантом, рассчитанным на рациональное использование ресурсов в данном виде деятельности. Сказанное характеризует категорию "риск" с качественной стороны и создает основу для перевода понятия "риск" в количественное.

Действительно, если риск - это опасность потери ресурсов или дохода, то существует его количественная мера, определяемая абсолютным или относительным уровнем потерь. В абсолютном выражении риск может определяться величиной возможных потерь в материально-вещественном (физическом) или стоимостном (денежном) выражении, если только ущерб поддается такому измерению. В относительном выражении риск определяется как величина возможных потерь, отнесенная к некоторой базе, в виде которой наиболее удобно принимать либо имущественное состояние, либо общие затраты ресурсов на данный вид деятельности, либо ожидаемый доход (прибыль) от операции. Выбор той или иной базы не имеет принципиального значения, но следует предпочесть показатель, определяемый с высокой степенью достоверности. Как правило, в абсолютном выражении риск исчисляется, когда речь идет об одной конкретной сделке. Если же необходимо определить допустимый уровень риска при совершении различных коммерческих операций, то применяются относительные показатели.

1.3 Классификация рисков

Эффективность организации управления рисками во многом определяется их классификацией, которая создает возможности для эффективного применения соответствующих методов и приемов управления риском.

К *природным рискам* относятся риски стихийных бедствий, такие как землетрясения, наводнения, ураганы, тайфуны, удары молнии и т.д.

Техногенные риски связаны с хозяйственной деятельностью человека.

Смешанными рисками являются события природного характера, ставшие результатом хозяйственной деятельности человека.

*Чистые (простые) риск*и, или статические, практически всегда наносят предприятию ущерб, то есть связаны только с потерями для предпринимательской деятельности. Это риск потерь реальных активов вследствие нанесения ущерба собственности или неудовлетворительной организации.

Спекулятивные риски, или динамические, — это риски непредвиденных изменений стоимостных оценок управленческих решений фирмы, а также изменения рыночных отношений или политических обстоятельств. Они характеризуются тем, что могут быть связаны как с потерями, так и с получением дополнительной прибыли по отношению к ожидаемым результатам.

Производственные риски — это риски, характерные для производственной деятельности и связанные с убытками от остановки производства по различным причинам, а также с неадекватным использованием техники и технологии, основных и оборотных фондов, производственных ресурсов и рабочего времени.

Финансовые риски — это риски, связанные с вероятностью потерь финансовых ресурсов (денежных средств). Финансовые риски подразделяются на два вида: риски, связанные с покупательной способностью денег, и риски, связанные с вложением капитала (инвестиционные риски, кредитные риски, риски прямых финансовых потерь). По типу потерь финансовые риски разделяют на прямые имущественные риски и риски, связанные с обязательствами, т.е. риск убытков по вине конкурентов, сотрудников или партнеров в связи с изменениями условий выполнения обязательств.

Имущественные риски — это риски, связанные с возможностью потерь имущества по различным причинам: кражи, диверсии, халатность, перенапряжения технической и технологической систем, порчи и т.п.

Под коммерческим риском понимается риск, связанный с предпринимательской деятельностью, ориентированной на получение максимальной прибыли и возникающий в процессе реализации товаров и услуг, произведенных или закупленных предприятием.

Социальные риски непосредственно связаны с жизнью, здоровьем и трудоспособностью работников предприятия, а также их личностными характеристиками и условиями труда.

Предпринимательский риск связан со случайными потерями предпринимательской прибыли. Потери в предпринимательской деятельности разделяют на материальные, трудовые, финансовые, потери времени и специальные виды потерь.

Причины возникновения внешних и внутренних рисков представлены в таблице 1.

Материальные потери проявляются в дополнительных затратах или прямых потерях оборудования, имущества, продукции, сырья, энергии и т.д. Материальные потери измеряются в тех же единицах, в которых измеряется количество данного вида материальных ресурсов, т.е. в физических единицах веса, объема, площади и др., а также в стоимостном выражении, в денежных единицах. Для этого потери в физическом измерении переводятся в стоимостные путем умножения его на цену единицы соответствующего материального ресурса. Для достаточного количества материальных ресурсов, стоимость которых заранее известна, потери можно сразу оценивать в денежном выражении.

Таблица 1.

Основные причины возникновения внешних и внутренних рисков

Риски	***Основные причины возникновения***	***Объект направления***
	Внешние риски	
Стразовый	нестабильность государственной власти, особенности государственного законодательства, национализация и т.п.	имущество, имущественный
Валютные	изменение валютных курсов, валютного регулирования	имущественный интерес
Налоговый	изменение налоговой политики, налоговых ставок	имущественный интерес
Форс-мажорные	природные катастрофы, войны, революции, путчи	имущество, имущественный интерес, человек
	Внутренние риски	
Организационный	низкий уровень организации, ошибки планирования, прогнозирования, слабое регулирование, плохая организация труда сотрудников и т.д.	имущество, имущественный интерес, человек
Ресурсный	нехватка производственных запасов, срывы поставок, недостаточная квалификация рабочей силы, отсутствие запаса прочности по ресурсам	имущество, имущественный интерес, человек
Инвестиционный	риски реального инвестирования: перебои в поставках стройматериалов, ошибки в разработке инвестиционного проекта строительства или реконструкции, неудачный выбор месторасположения строительства. портфельные риски: изменение условий контракта, ошибки в выборе объектов инвестирования, неправильный подбор финансовых инструментов	имущество, имущественный интерес, человек
Кредитный	Невозврат долга и процентов по нему, невыполнение условий кредитного договора, невольное банкротство заемщика, изменение платежеспособности заемщика	Имущественный интерес
Инновационный	Неправильный выбор нововведений, неверные расчеты, применение научно-технических новшеств	Имущественный интерес
Правовые	Используемые лицензии, патентные права, невыполнение контрактов, судебные процессы с внешними партнерами, внутренние судебные процессы	Имущество, имущественный интерес, человек

Трудовые потери представляют собой потери рабочего времен, вызванные случайными, непредвиденными обстоятельствами. В непосредственном измерении трудовые потери выражаются в человеко-часах, человеко-днях или просто часах рабочего времени. Перевод трудовых потерь в стоимостное, денежное выражение осуществляется путем умножения трудочасов на стоимость одного часа. Финансовые потери — это прямой денежный ущерб, связанный с непредусмотренными платежами, выплатой штрафов, уплатой дополнительных налогов, потерей денежных средств и ценных бумаг, невозвратом долгов, неоплатой покупателем поставленной ему продукции.

Временные финансовые потери могут быть обусловлены замораживанием счетов, несвоевременной выдачей средств, отсрочкой выплаты долгов, изменением валютного курса рубля, инфляцией и др. Потери времени существуют тогда, когда процесс предпринимательской деятельности идет медленнее, чем было намечено. Прямая оценка таких потерь осуществляется в часах, днях, неделях, месяцах запаздывания в получении намеченного результата. Чтобы перевести оценку потерь времени в стоимостное измерение, необходимо установить, к каким потерям дохода и прибыли приводят случайные потери рабочего времени. Специальные виды потерь проявляются в виде нанесения ущерба здоровью и жизни людей, окружающей среде, престижу предприятия, а также в виде других неблагоприятных социальных и морально-психологических последствий, чаще всего их крайне трудно определить в количественном и тем более в стоимостном выражении.

Предпринимательский риск связан с конечным финансово-хозяйственным результатом деятельности предприятия, в котором объединяются многочисленные частные риски (рис. 1).

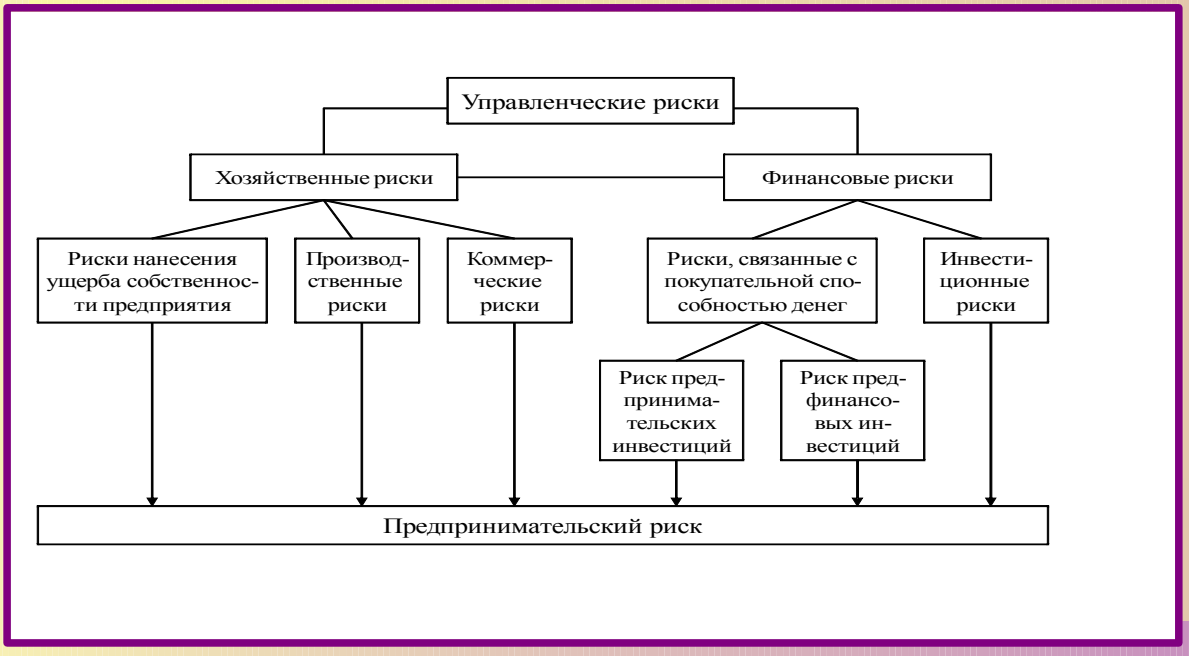


Рис 1. ***Основные группы рисков деятельности предприятия***

Финансовый риск представляет собой функцию времени. Как правило, степень риска для данного финансового актива или варианта вложения капитала увеличивается во времени. Например, убытки импортера сегодня зависят от времени от момента заключения контракта до срока платежа по сделке, так как курсы иностранной валюты по отношению к российскому рублю продолжают расти.

В зарубежной практике в качестве метода количественного определения риска вложения капитала предлагается использовать древо вероятностей.

Этот метод позволяет точно определить вероятные будущие денежные потоки инвестиционного проекта в их связи с результатами предыдущих периодов времени. Если проект вложения капитала приемлем в первом периоде времени, то он может быть также приемлем и в последующих периодах времени.

Если же предполагается, что денежные потоки в разных периодах времени являются независимыми друг от друга, тогда необходимо определить вероятное распределение результатов денежных потоков для каждого периода времени.

В случае, когда связь между денежными потоками в разных периодах времени существует, необходимо принять данную зависимость и на ее основе представить будущие события так, как они могут произойти.

В качестве примера произведем древо вероятностей для трех периодов времени (рис. 2).

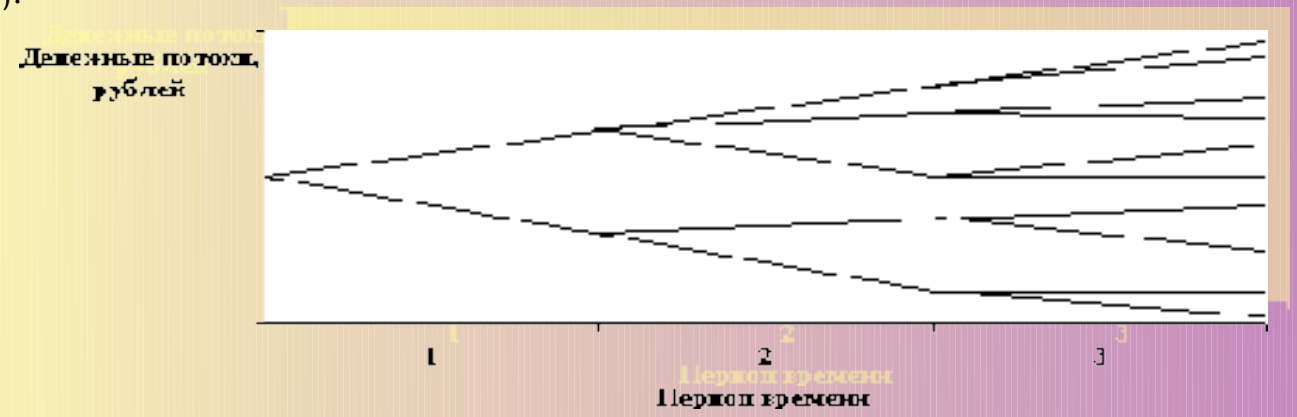


Рис 2. ***Древо вероятностей***

Древо вероятностей показывает, что если в периоде 1 результа-том будет верхняя ветвь, то она приведет в периоде 2 к другому множеству возможных результатов, чем это было бы, если бы ре-зультат в периоде 1 выражался нижней ветвью. Аналогичная кар-тина наблюдается и при переходе от периода времени 2 к периоду 3. Поэтому в момент временного периода 0 древо вероятностей представляет наилучшую оценку того результата, который, веро-ятно, будет иметь место в будущем, в зависимости от того, что происходило прежде. Для каждой из ветвей денежные потоки привязаны к вероятности.

В периоде 1 результат денежного потока не зависит от того, что было прежде. Поэтому вероятности, связанные с двумя ветвями, называются исходными вероятностями. Для всех последующих периодов (т.е. периодов 2, 3 и т.д.) результаты денежных потоков зависят от предыдущих результатов. Поэтому вероятности этих периодов называются условными. Кроме того, существует сов-местная вероятность, которая представляет собой вероятность по-явления определенной последовательности денежных потоков. Совместная вероятность равна произведению исходной и услов-ной вероятностей.

Профессиональные риски связаны с выполнением должностными лицами своих профессиональных обязанностей.

Инвестиционные риски возникают при вложении инвесторами средств в инвестиционные объекты с целью получения прибыли. Различают систематический и несистематический риски; риски реального и финансового инвестирования.

Транспортные риски представляют собой риски, связанные с убытком по причине транспортировки товара; различают морские, воздушные и наземные.

Банковские риски представляют собой опасность потерь в банковских операциях, они могут иметь внешние причины возникновения (страновый и валютный) и внутренние, такие как риски пассивных и активных операций, риски, связанные со спецификой клиента.

Страховой риск связан с неэффективной страховой деятельностью как на этапе, предшествующем заключению договора страхования, так и на последующих этапах перестрахования, формирования страховых резервов и т.п.

1.4 Прогнозирование рисковой ситуации

Рассматривая риск как экономическую категорию, необходимо глубоко понимать и применять на практике системы прогнозирования, оценки, анализа и управления предпринимательскими рисками. Рассмотрим поэтапно весь алгоритм действий предпринимателя, направленный на оптимизацию рисковой ситуации в своей деятельности.

Изначально рисковая ситуация подвергается прогнозированию, причем важное место здесь занимает предупреждение неопределенности возможного риска. На данном этапе решается целый комплекс задач, основными из которых являются:

- определение источников информации, которые позволяют выявить причины риска и возможные его виды;
- выяснение источников риска;
- прогнозирование основных видов риска для конкретного предприятия;
- определение объектов, на которые воздействует тот или иной вид риска.

Определение источников информации. Для того чтобы определить источники риска и возможные их виды, необходимо иметь надежное информационное обеспечение. Все источники такой информации могут быть классифицированы:

- внутренние и внешние;
- учтенные и неучтенные;
- разовые и постоянные;
- полученные легальным и нелегальным путем;
- полученные с магнитных носителей, с документов, от партнеров, приобретенные за плату, от осведомителей, агентов и т.д.;
- достоверные и сомнительные;
- другие.

Их может быть великое множество, и каждое предприятие выбирает для себя наиболее важные. Назовем некоторые из наиболее значимых и доступных: каталог факторов риска и рисковых ситуаций; личный опыт руководителей предприятия и специалистов группы оценки и управления риском; прогнозная информация; материалы ревизий, аудита, проверок налоговой службы, лабораторного и врачебно-санитарного контроля, печати, объяснительных и докладных записок, совещаний, переписки, получаемые в результате личных контактов; бухгалтерский учет и отчетность; статистические данные; сведения о конкурентах, партнерах, поставщиках и потребителях; материалы маркетинговых исследований о состоянии рынка; сведения правоохранительных органов о криминальной обстановке; экономическая, политическая и т.д. ситуации в стране и регионе; платежеспособность покупателей и т. п.

Информация, необходимая для определения уровня риска, может быть оценена с количественной, смысловой и ценностной точек зрения. Количество информации должно быть достаточным для оценки риска. Ее смысловое выражение должно быть доступным и применимым для управления рисками, а ценностность состоит в том, что она должна способствовать достижению поставленной цели.

Выяснение источников риска. Информация является питательной средой для определения источников хозяйственного риска. В каждом конкретном случае они могут быть различны для каждого предприятия. Поэтому руководители и специалисты предприятия могут их заблаговременно определить, сгруппировать и отранжировать в зависимости от опасности для хозяйственной деятельности предприятия. Для примера выделим лишь самые главные. К ним можно отнести:

- недобросовестное поведение конкурентов, партнеров, поставщиков, потребителей;
- промышленный шпионаж;
- непредсказуемость колебаний спроса и предложения;
- рэкет;
- внезапные изменения налогового, таможенного, валютного законодательства;
- колебания цен, валютных и биржевых курсов, инфляция;
- ошибки в планировании, организации и управлении производством;
- разглашение конфиденциальной информации и противоправные действия сотрудников фирмы;
- форс-мажорные обстоятельства;
- другие.

Прогнозирование основных видов риска. Как уже отмечалось, каждое предприятие работает в разных условиях конкурентной среды, имеет свои кадровый и производственный потенциалы, свои производственные связи, деловых партнеров и т.д. Исходя из этого у различных предприятий могут возникать свои виды рисков и их разновидности.

Например, производственный, коммерческий, финансовый, технологический, страховой и т.д. На данном этапе важно своевременно выявить их и по возможности определить наиболее опасные как по вероятному ущербу, так и по времени наступления. Это послужит основой для принятия своевременных и правильных мер по предотвращению риска.

Определение объектов, на которые воздействует тот или иной вид риска. Для оптимального выбора наиболее предпочтительного варианта действий по управлению риском важно иметь четкую информацию и о том, какой объект подвергается риску. Это может быть и информация, и какой-то объект, и персонал, и руководители фирмы, и прибыльность производства, и т.д.

Владея этой информацией и зная реальную степень защищенности объекта, можно рассчитать потребность в объеме необходимых сил и средств для предотвращения риска, выработать правильные меры по защите объекта

1.5 Способы оценки степени риска

Оценка риска - это совокупность аналитических мероприятий, позволяющих спрогнозировать возможность получения дополнительного предпринимательского дохода или определенной величины ущерба от возникшей рисковой ситуации и несвоевременного принятия мер по предотвращению риска.

В данном разделе особое значение имеет своевременный подсчет величины возможного ущерба. Оценка предпринимательских рисков может осуществляться как с позиции качественных характеристик, так и количественно.

Качественная оценка рисков. Человек от природы стремиться избегать риска. Если мы не можем контролировать риск, то обычно предпочитаем избежать его. Вынужденные признать наличие риска в нашей жизни, мы желаем свести его к минимуму. Также мы хотим иметь возможность выбора наименее рискованной из двух и более альтернатив. Или мы хотим соотнести риск какого-либо события или рискованности предприятия с возможными выгодами, т.е. мы хотим выбрать оптимальное соотношение риска и выгоды какого-либо предприятия.

Для того чтобы выбрать наименее рискованную или предлагающую наиболее привлекательное соотношение риска и выгод альтернативу, мы должны оценить риск, что позволит сравнить величину риска различных вариантов решения и выбрать из них тот, который больше всего отвечает выбранной предприятием стратегии риска.

Основная часть оценки риска сегодня основана на теории вероятности - систематическом статистическом методе определения вероятности того, что какое-то будущее событие произойдет. Однако надо заметить, что вероятность не каждого будущего события можно измерить.

Несмотря на разработанность критериев риска, которые позволяют ранжировать альтернативные события в зависимости от степени риска, зачастую, чтобы применить эти критерии, нам необходимо сделать ряд допущений по этому вопросу.

С другой стороны, существует множество ситуаций, в которых мы имеем в своем распоряжении обширные массивы информации о наблюдавшихся в прошлом событиях, которые позволяют нам делать полновесные выводы о вероятности осуществления будущего события. Многие финансовые операции (венчурное инвестирование, по-купка акций, селинговые операции, кредитные операции и др.) связаны с довольно существенным риском. Они требуют оценить степень риска и определить его величину.

Степень риска - это вероятность наступления случая потерь, а также размер возможного ущерба от него.

Риск может быть(Смотрите рис 3.):

- допустимым - имеется угроза полной потери прибыли от реализации планируемого проекта;
- критическим - возможны непоступление не только прибыли, но и выручки и покрытие убытков за счет средств предпринимателя;
- катастрофическим - возможны потеря капитала, имущества и банкротство предпринимателя.

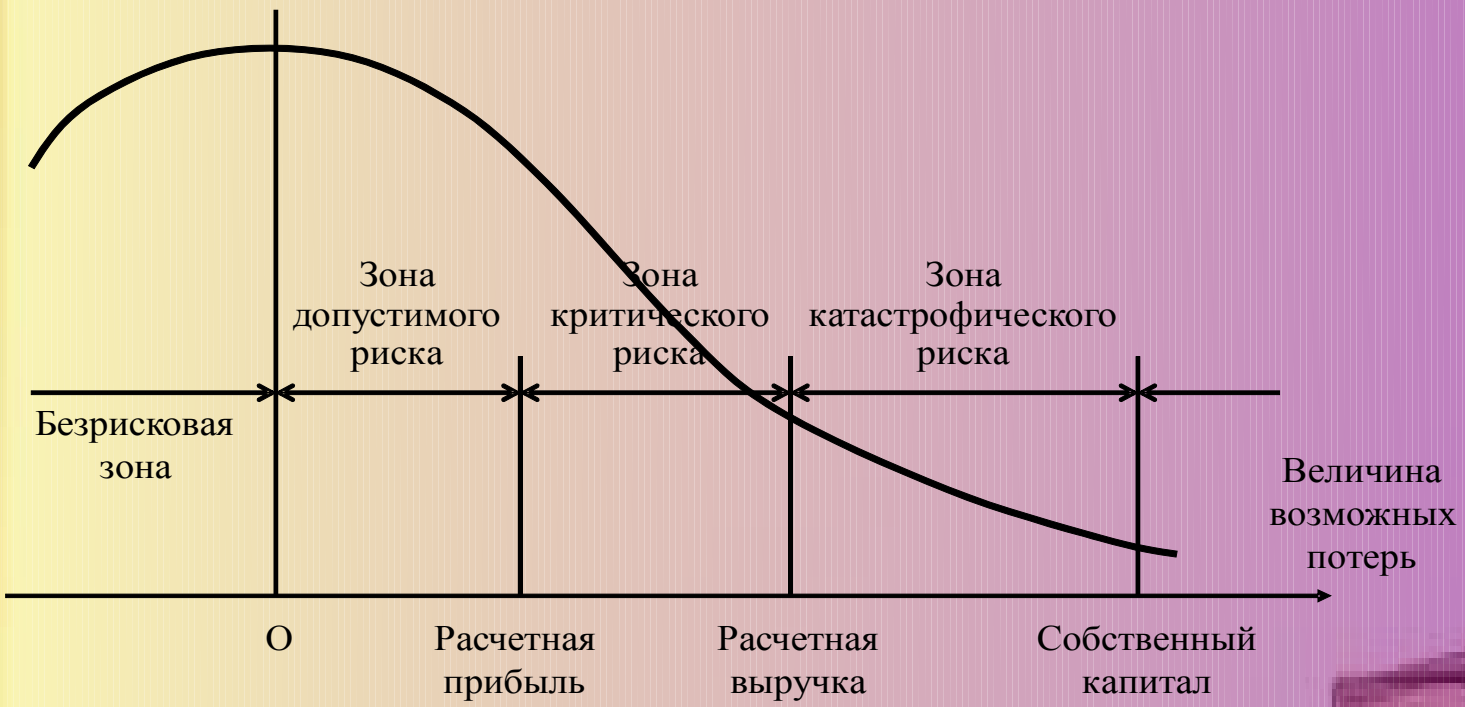


Рис 3. ***Схема границ и зон риска, кривая риска***

Область, в которой потери не ожидаются называется безрисковой зоной. Ей соответствуют нулевые потери или даже отрицательные (превышение прибыли над ожидаемой).

Под зоной допустимого риска понимается область, в пределах которой данный вид предпринимательской деятельности сохраняет свою экономическую целесообразность, т.е. потери имеют место, но они меньше ожидаемой прибыли. Граница зоны допустимого риска соответствует уровню потерь, равному расчетной прибыли от предпринимательской деятельности.

Более опасная область – зона критического риска. Это область, характеризуемая возможностью потерь, превышающих величину ожидаемой прибыли и достигающих в пределе величины денежного объема операции, исчисляемого полной расчетной выручкой от предпринимательской сделки, т.е. суммой затрат и прибыли. Иначе говоря, зона критического риска характеризуется опасностью потерь, которые заведомо превышают ожидаемую прибыль и в пределе, максимуме могут привести к невозместимой потере всех средств, вложенных предпринимателем в проект. В последнем случае предприниматель не только не получает от сделки никакого дохода, но и несет убытки в сумме всех своих бесплодных затрат.

Зона катастрофического риска представляет область потерь, которые по своей величине превосходят критический уровень, ожидаемую выручку и в максимуме могут достигать величины, равной всему собственному капиталу, имущественному состоянию фирмы или превосходить его.

Количественный анализ - это определение конкретного размера денежного ущерба отдельных подвидов финансового риска и финансового риска в совокупности.

Иногда качественный и количественный анализ производится на основе оценки влияния внутренних и внешних факторов: осуществляются поэлементная оценка удельного веса их влияния на работу данного предприятия и ее денежное выражение. Такой метод анализа является достаточно трудоемким с точки зрения количественного анализа, но приносит свои несомненные плоды при качественном анализе. В связи с этим следует уделить большее внимание описанию методов количественного анализа финансового риска, поскольку их немало и для их грамотного применения необходим некоторый навык.

В абсолютном выражении риск может определяться величиной возможных потерь в материально-вещественном (физическом) или стоимостном (денежном) выражении.

В относительном выражении риск определяется как величина возможных потерь, отнесенная к некоторой базе, в виде которой наиболее удобно принимать либо имущественное состояние предприятия, либо общие затраты ресурсов на данный вид предпринимательской деятельности, либо ожидаемый доход (прибыль). Тогда потерями будем считать случайное отклонение прибыли, дохода, выручки в сторону снижения. в сравнении с ожидаемыми величинами. Предпринимательские потери - это в первую очередь случайное снижение предпринимательского дохода. Именно величина таких потерь и характеризует степень риска. Отсюда анализ риска прежде всего связан с изучением потерь. В зависимости от величины вероятных потерь целесообразно разделить их на три группы:

- потери, величина которых не превышает расчетной прибыли, можно назвать допустимыми;
- потери, величина которых больше расчетной прибыли относятся к разряду критических - такие потери придется возмещать из кармана предпринимателя;
- еще более опасен катастрофический риск, при котором предприниматель рискует понести потери, превышающие все его имущество.

Если удается тем или иным способом спрогнозировать, оценить возможные потери по данной операции, то значит получена количественная оценка риска, на который идет предприниматель. Разделив абсолютную величину возможных потерь на расчетный показатель затрат или прибыли, получим количественную оценку риска в относительном выражении, в процентах. Говоря о том, что риск измеряется величиной возможных. вероятных потерь, следует учитывать случайный характер таких потерь. Вероятность наступления события может быть определена объективным методом и субъективным.

Объективным методом пользуются для определения вероятности наступления события на основе исчисления частоты, с которой происходит данное событие.

Субъективный метод базируется на использовании субъективных критериев, которые основываются на различных предположениях. К таким предположениям могут относиться суждение оценивающего, его личный опыт, оценка эксперта по рейтингу, мнение аудитора-консультанта и т.п.

Таким образом, в основе оценки финансовых рисков лежит нахождение зависимости между определенными размерами потерь предприятия и вероятностью их возникновения. Эта зависимость находит выражение в строящейся *кривой вероятностей возникновения определенного уровня потерь.*

Построение кривой - чрезвычайно сложная задача, требующая от служащих, занимающихся вопросами финансового риска, достаточного опытами знаний. Для построения кривой вероятностей возникновения определенного уровня потерь (кривой риска) применяются различные способы: статистический; анализ целесообразности затрат; метод экспертных оценок; аналитический способ; метод аналогий. Среди них следует особо выделить три: статистический способ, метод экспертных оценок, аналитический способ.

Суть *статистического способа* заключается в том, что изучается статистика потерь и прибылей, имевших место на данном или аналогичном производстве, устанавливаются величина и частотность получения той или иной экономической отдачи, составляется наиболее вероятный прогноз на будущее.

Несомненно, риск - это вероятностная категория, ив этом смысле наиболее обоснованно с научных позиций характеризовать и измерять его как вероятность возникновения определенного уровня потерь. Вероятность означает возможность получения определенного результата.

Финансовый риск, как и любой другой, имеет математически выраженную вероятность наступления потери, которая опирается на статистические данные и может быть рассчитана с достаточно высокой точностью. Чтобы количественно определить величину финансового риска, необходимо знать все возможные последствия какого-либо отдельного действия и вероятность самих последствий.

Применительно к экономическим задачам методы теории вероятности сводятся к определению значений вероятности наступления событий и к выбору из возможных событий самого предпочтительного исходя из наибольшей величины математического ожидания, которое равно абсолютной величине этого события, умноженной на вероятность его наступления.

Главные инструменты статистического метода расчета финансового риска: вариация, дисперсия и стандартное (среднеквадратическое) отклонение.

Вариация - изменение количественных показателей при переходе от одного варианта результата к другому.

Дисперсия - мера отклонения фактического знания от его среднего значения.

Степень риска измеряется двумя показателями: средним ожидаемым значением и колеблемостью (изменчивостью) возможного результата.

Среднее ожидаемое значение связано с неопределенностью ситуации, оно выражается в виде средневзвешенной величины всех возможных результатов E(x), где вероятность каждого результата (A) используется в качестве частоты или веса соответствующего значения (x). В общем виде это можно записать так:

E(x)=A1X1 +A2X2+⋯+AnXn.

Пример: при вложении денежных средств в мероприятие А из 150 случаев прибыль в сумме 20,0 тыс. руб. была получена в 75 случаях (вероятность - 75: 150 = 0,5), прибыль 25,0 тыс. руб. - в 60 случаях (вероятность - 60 : 150 = 0,4) и прибыль 30,0 тыс. руб. - в 15 случаях (вероятность - 15 : 150 = 0,1).

Среднее ожидаемое значение прибыли составит:

20,0 х 0,5 + 25,0 х 0,4 + 30.0 х 0,1 = 23.

Осуществление мероприятия Б из 150 случаев давало прибыль 19,0 тыс. руб. в 60 случаях (вероятность - 60 : 150 = = 0,4), прибыль 24,0 тыс. руб. - в 45 случаях (вероятность 45 : 150 = 0,3), 31,0 тыс. руб. - в 45 случаях (вероятность 45: 150=0,3).

При проведении мероприятия Б средняя ожидаемая прибыль составит:

19,0 х 0,4+24,0 х 0,3+1,0 х 0,3=24,1.

Сравнивая величины ожидаемой прибыли при вложении денежных средств в мероприятия А к Б, можно сделать вывод, что величина получаемой прибыли при мероприятии А колеблется от 20,0 до 30,0 тыс. руб., средняя величина составляет 23 тыс. руб.; в мероприятии Б величина получаемой прибыли колеблется от 19,0 до 31,0 тыс. руб. и средняя величина равна 24,1 тыс. руб.

Средняя величина представляет собой обобщенную количественную характеристику и не позволяет принять решение в пользу какого-либо варианта вложения капитала.

Для окончательного решения необходимо измерить колеблемость (размах или изменчивость) показателей, т.е. определить меру колеблемости возможного результата.

Колеблемость возможного результата представляет собой степень отклонения ожидаемого значения от средней величины. Для ее определения обычно вычисляют дисперсию или среднеквадратическое отклонение:

Коэффициент вариации - это отношение среднего квадратичного отклонения к средней арифметической.

Он показывает степень отклонения полученных значений.

$$V = \sigma / X_{ср} \times 100\%,$$

где V — коэффициент вариации, %

Коэффициент вариации позволяет сравнивать колеблемость признаков, имеющих разные единицы измерения.

Чем выше коэффициент вариации, тем сильнее колеблемость признака.

Установлена следующая оценка коэффициентов вариации:

до 10% - слабая колеблемость;
10-25% - умеренная колеблемость;
свыше 25% - высокая колеблемость.

В нашем примере среднее квадратическое отклонение составляет:

в мероприятии А - 6,68;
в мероприятии Б - 4,95.

Коэффициент вариации:

для мероприятия А: V А = 29%;
для мероприятия Б: VБ = 20%.

Коэффициент вариации при вложении денежных средств в мероприятие А больше, чем при мероприятии Б. Следовательно, мероприятие Б сопряжено с меньшим риском, а значит, предпочтительнее.

Дисперсионный метод успешно применяется и при наличии более чем двух альтернативных признаков. Таким образом, величина риска, или степень риска, может быть измерена двумя критериями: среднее ожидаемое значение, колеблемость (изменчивость) возможного результата. Среднее ожидаемое значение - это то значение величины события, которое связано с неопределенной ситуацией. Оно является средневзвешенной всех возможных результатов, где вероятность каждого результата используется в качестве частоты, или веса, соответствующего значения. Таким образом вычисляется тот результат, который предположительно ожидается.

Анализ целесообразности затрат ориентирован на идентификацию потенциальных зон риска с учетом показателей финансовой устойчивости фирмы. В данном случае можно просто обойтись стандартными приемами финансового анализа результатов деятельности основного предприятия и деятельности его контр-агентов (банка, инвестиционного фонда, предприятия-клиента, предприятия-эмитента, инвестора, покупателя, продавца и т.п.)

Метод экспертных оценок обычно реализуется путем обработки мнений опытных предпринимателей и специалистов. Он отличается от статистического лишь методом сбора информации для построения кривой риска.

Метод экспертных оценок основан на обобщении мнения специалистов-экспертов о вероятностях риска. Интуитивные характеристики, основанные на знаниях и опыте эксперта, дают в ряде случаев достаточно точные оценки. Экспертные методы позволяют быстро и без больших временных и трудовых затрат получить информацию, необходимую для выработки управленческого решения.

Метод экспертных оценок применяется в случаях, когда:

1) длина исходных динамических рядов недостаточна для оценивания с использованием экономико-статистических методов;

2) связь между исследуемыми явлениями носит качественный характер и не может быть выражена с помощью традиционных количественных измерителей;

3) входная информация неполная и невозможно предсказать влияние всех факторов;

4) возникли экстремальные ситуации, когда требуется принятие быстрых решений. Суть экспертных методов заключается в организованном сборе суждений и предположений экспертов с последующей обработкой полученных ответов и формированием результатов.

Выделяют следующие стадии экспертного опроса:

1) формулировка цели экспертного опроса;

2) подбор основного состава рабочей группы;

3) разработка и утверждение технического задания на проведение экспертного опроса;

4) разработка подробного сценария проведения сбора и анализа экспертных мнений (оценок), включая как конкретный вид экспертной информации (слова, условные градации, числа, ранжирование, разбиения или иные виды объектов нечисловой природы), так и конкретные методы анализа этой информации;

5) подбор экспертов в соответствии с их компетентностью;

6) формирование экспертной комиссии;

7) проведение сбора экспертной информации;

8) анализ экспертной информации;

9) интерпретация полученных результатов и подготовка заключения;

10) принятие решения - выбор альтернативы. Данный способ предполагает сбор и изучение оценок, сде-ланных различными специалистами (данного предприятия или внешними экспертами) вероятностей возникновения различных уровней потерь. Эти оценки базируются на учете всех факторов финансового риска, а также статистических данных. Реализация способа экспертных оценок значительно осложняется, если количество показателей оценки невелико.

Существует масса методов получения экспертных оценок. В одних с каждым экспертом работают отдельно, он даже не знает, кто еще является экспертом, а потому высказывает свое мнение независимо от авторитетов.

В других - экспертов собирают вместе, при этом эксперты обсуждают проблему друг с другом, учатся друг у друга, и неверные мнения отбрасываются. В одних методах число экспертов фиксировано, в других - число экспертов растет в процессе проведения экспертизы.

Среди наиболее распространенных методов получения экспертных оценок можно выделить:

1) метод "Дельфы"

2) метод "снежного кома";

3) метод "дерева целей";

4) метод "комиссий круглого стола";

5) метод эвристического прогнозирования;

6) матричный метод

Рассмотрим пример количественной оценки экспертами возможного приращения платежеспособного спроса на пищевую продукцию (по методу Дельфы).

К участию в эксперименте привлечено 8 человек, после оценки уровня компетентности - 5 человек. На первом этапе ответы на вопросы даются в произвольной форме (числовые характеристики, словесные описания). На второй стадии называются конкретные значения возможного приращения платежеспособного спроса с аргументацией данных значений. Далее проводится статистическая обработка результатов экспертизы. Для этого находят медиану и квартили. Медиана - серединное или центральное значение признака, делит числовой ряд пополам. Квартиль - значения переменной, делящей ряд распределения на четыре равные части.

Считается, что медиана характеризует обобщенное мнение группы экспертов, а значения нижнего и верхнего квартилей ограничивают доверительную зону прогноза.

Предположим, что в данном примере экспертиза дала следующие результаты, представленные в таблице 2.

Таблица 2.

Результаты экспертизы по определению возможного приращения платежеспособного спроса на пищевую продукцию

№ п/п	Коэффициент компетентности	Величина приращения платежеспособного спроса, %
1.	0,5	4
2.	0,6	5
3.	0,6	6
4.	0,5	8
5.	0,5	9
6.	0,7	10
7.	0,6	11

Результаты доводятся до сведения экспертов. Экспертам, чьи прогнозы не попали в доверительный интервал, предлагается аргументировать свою точку зрения или пересмотреть ее и присоединиться к мнению большинства.

Последующие этапы корректировки данных позволят усилить согласованность результатов.

Аналитический способ построения кривой риска наиболее сложен, поскольку лежащие в основе его элементы теории игр доступны только очень узким специалистам. Чаще используется под-вид аналитического метода - анализ чувствительности модели.

Анализ чувствительности модели состоит из следующих шагов: выбор ключевого показателя, относительно которого и производится оценка чувствительности (внутренняя норма доходности и т.п.); выбор факторов (уровень инфляции, степень состояния экономики и др.); расчет значений ключевого показателя на различных этапах осуществления проекта. Сформированные таким путем последовательности затрат и поступлений финансовых ресурсов дают возможность определить потоки фондов денежных средств для каждого момента (или отрезка времени), т.е. определить показатели эффективности. Строятся диаграммы, отражающие зависимость выбранных результирующих показателей от величины исходных параметров. Сопоставляя между собой полученные диаграммы, можно определить так называемые ключевые показатели, в наибольшей степени влияющие на оценку доходности проекта.

Анализ чувствительности имеет и серьезные недостатки: он не является всеобъемлющим и не уточняет вероятность осуществления альтернативных проектов.

Метод аналогий при анализе риска нового проекта весьма полезен, так как в данном случае исследуются данные о последствиях воздействия неблагоприятных факторов финансового риска на другие аналогичные проекты других конкурирующих предприятий.

Индексация представляет собой способ сохранения реальной величины денежных ресурсов (капитала) и доходности в услови-ях инфляции. В основе ее лежит использование различных индексов.

Например, при анализе и прогнозе финансовых ресурсов необходимо учитывать изменение цен, для чего используются индексы цен. Индекс цен - показатель, характеризующий изменение цен за определенный период времени.

Метод целесообразности затрат. Этот метод позволяет определить критический объем производства или продаж, т.е. нижний предельный размер выпуска продукции, при котором прибыль равна нулю.

Производство продукции в объемах меньше критического приносит только убытки. Критический объем производства необходимо оценивать при освоении новой продукции и при сокращении ее выпуска, вызванного падением спроса, сокращением поставок материалов и комплектующих изделий, заменой продукции на новую, ужесточением экологических требований и другими причинами. Для проведения соответствующих расчетов все затраты на производство и реализацию продукции подразделяют на переменные и постоянные. Под переменными понимают издержки, общая величина которых находится в непосредственной зависимости от объемов производства и реализации, а также от их структуры при производстве и реализации нескольких видов продукции. Это затраты на сырье и материалы, топливо, энергию, транспортные услуги, большую часть трудовых ресурсов и т.д. К постоянным издержкам производства относят затраты, величина которых не меняется с изменением объемов производства.

Они должны быть оплачены, даже если предприятие не производит продукцию (отчисления на амортизацию, аренда зданий и оборудования, страховые взносы, оплата высшего управленческого персонала и т.д.).

Критический объем производства (Vкр) можно представить в следующем виде:

Vкр = Зпост/ (Ц - Зпер),

где Ц - цена издения (единицы продукции), руб.;

Зпост - постоянные затраты, руб.;

Зпер - переменные затраты, руб.

Некоторые зарубежные авторы называют критический объем производства порогом рентабельности и используют этот показатель для оценки финансовой устойчивости предприятия.

Чем больше разность между фактическим объемом производства и критическим, тем выше финансовая устойчивость.

Любое изменение объема производства (продаж) оказывает существенное влияние на прибыль. Данная зависимость называется эффектом производственного (или операционного) левериджа.

Производственный леверидж показывает степень влияния постоянных затрат на прибыль (убытки) при изменениях объема производства.

Чем больше удельный вес постоянных затрат в общей сумме издержек при некотором объеме производства, тем выше производственный леверидж, следовательно, тем выше предпринимательский риск.

Работать с высоким производственным левериджем могут только те предприятия, которые в состоянии обеспечить большие объемы производства и сбыта; имеют устойчивый спрос на свою продукцию.

Метод аналогий обычно используется при анализе рисков нового проекта.

Проект рассматривается как "живой" организм, имеющий определенные стадии развития.

Жизненный цикл проекта состоит из

- этапа разработки,
- этапа выведения на рынок,
- этап роста,
- этапа зрелости и
- этапа упадка.

Изучая жизненный цикл проекта, можно получить информацию о каждом этапе проекта, выделить причины нежелательных последствий, оценить степень риска. Однако на практике бывает довольно трудно собрать соответствующую информацию.

Нельзя забывать, что последствия неверных оценок рисков или отсутствия возможности противопоставить действенные меры могут быть самыми неприятными.

1.6 Специфика сбора информации для оценки рисков на различных предприятиях

Каждое предприятие имеет свою информационную среду для определения источников хозяйственного риска, и одна из функций риск-менеджера как раз и заключаются в своевременном выявлении, группировке и ранжировании опасностей.

Важной составной частью организации работ по сбору информации и выявлению рисков является разработка специальной программы по контролю и выявлению новых рисков, которая имеет собственный бюджет и экономическое обоснование.

Итак, к основным методам получения исходной информации и выявления опасностей относятся:

1. Опросные листы. Существует два типа — стандартизированные и специализированные. Стандартизированные, или универсальные, листы разрабатываются и используются международными ассоциациями консультантов или страховщиков для унификации статистических данных и применимы для большинства предприятий. Опросный лист включает несколько разделов, каждый из которых содержит перечень вопросов, позволяющих составить полное представление о структуре и количественных показателях описываемого объекта. Специализированные опросные листы разрабатываются для конкретных видов деятельности и стимулируют респондентов выявлять характерные для них особенности рисков.

2. Структурные диаграммы, позволяющие выявлять, прежде всего, внутренние риски, связанные с качеством менеджмента, маркетинга, организацией работы и т.д. Структурные диаграммы описывают особенности структуры предприятия и зависят от сложившегося типа управления и принципов разделения функций. В основном структурные диаграммы предоставляют возможность выявления внутренних рисков, таких как дублирование функций одного отдела другими, зависимость и концентрация, а также позволяют определить отсутствие или недостаточность хорошо налаженных связей между подразделениями.

3. Карты потоков или потоковые диаграммы выявляют основные опасности производственного процесса и позволяют примерно оценить надежность и устойчивость узловых элементов производства. В то же время, без привлечения дополнительных источников информации потоковые диаграммы не дают возможности определить степень вероятности наступления риска. Виды карт потоков делятся на три группы: описывающие отдельный технологический процесс внутри предприятия; совокупность производственных процессов и элементов управления; технологическую цепочку, в которой предприятие является отдельным звеном.

4. Инспектирование дает возможность получения дополнительной информации и проверки ее достоверности и полноты на местах. Существует практика неожиданных инспекций объектов и заблаговременного извещения. В любом случае при планировании посещения объекта прежде всего необходимо четко определить перечень задач и вопросов, которые могут быть решены либо уточнены в процессе прямой инспекции. После предварительной оценки задач и учета различных особых факторов составляется программа посещения объекта, содержащая логическую схему выявления рисков, которая позволяет не упустить что-либо существенное. Все результаты инспекции оформляются в виде отчета, в котором указывается цель обследования, дата и место проведения, краткое содержание, результаты, заключение. Эффективность инспекции зависит от умения риск-менеджера отмечать важные нюансы, которые могут быть упущены респондентами опросных листов или специалистами, осуществляющими определенные технологические операции.

5.Анализ отчетности важен для выявления финансовых, коммерческих, предпринимательских рисков. В финансовой и управленческой документации фиксируются все события, имеющие отношение к увеличению или уменьшению риска. Риск-менеджер, анализируя финансовые и управленческие документы, систематически использует всю доступную информацию для идентификации опасностей, связанных с условиями заключения договоров, эффективностью использования финансовых ресурсов предприятия и выполнением обязательств. Наличие у менеджера надежной деловой информации позволяет ему быстро принимать оптимальное финансовое или коммерческое решение, влияет на правильность таких решений и ведет к снижению потерь и увеличению прибыли. Надлежащее использование информации при заключении сделок сводит к минимуму вероятность финансовых потерь.

В целом риск-менеджмент весьма динамичен. Эффективность его функционирования во многом зависит от скорости реакции на изменение условий рынка, экономической ситуации, финансового состояния объекта управления. Поэтому риск-менеджмент должен базироваться на знании стандартного набора приемов управления риском, на умении быстро и адекватно оценивать конкретную экономическую ситуацию, на способности быстро найти оптимальное, если не единственное, решение.

Таким образом, существующие способы построения кривой вероятностей возникновения определенного уровня потерь не совеем равноценны, но так или иначе позволяют произвести приблизительную оценку общего объема финансового риска.

ГЛАВА 2.
СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ В ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

2.1 Система управления рисками

Система управления представляет собой сложный механизм воздействия управляющей системы на управляемую с целью получения желаемого результата. Таким образом, управление риском как система состоит из двух подсистем:

- управляемой подсистемы (объекта управления) и
- управляющей подсистемы (субъекта управления).

В системе управления риском объектом управления являются риск, рисковые вложения капитала, экономические отношения между хозяйствующими подразделениями в процессе реализации риска.

Субъектом управления в системе управления риском является специальная группа людей (руководитель, финансовый менеджер, менеджер по риску и другие), которая посредством различных приемов и способов управления осуществляет целенаправленное воздействие на объект управления.

Существует интересное мнение по поводу использования термина "система управления риском". Специалисты считают, что с точки зрения исследования операций словосочетание управление риском лишено смысла, поскольку неопределенностью управлять нельзя.

Таким образом, когда говорят о системе управления риском, речь идет о системе поддержки принятия решения того или иного субъекта, главная задача которой в максимальной степени снизить неопределенность, имеющую место при принятии решений субъектом. На наш взгляд, такая трактовка системы управления риском несколько сужает ее предназначение.

Система управления РИСКОМ, несомненно, включает процесс принятия решений, однако на этом ее функции не ограничиваются. Система управления риском включает также дальнейший мониторинг рисковых позиций, их хеджирование, порядок взаимодействия подразделений в процессе контроля за принятыми рисками и т.п.

При анализе системы управления рисками целесообразно использовать в качестве основного методологического инструмента системный подход.

Системный подход представляет собой всесторонний подход, фокусирующий внимание не только на организации, но и на окружающей ее среде. Центральным понятием системного подхода является понятие "система", которое отражает понятие о том, что различные элементы, соединяясь, приобретают новое качество, которое отсутствует у каждого из них в отдельности.

Новое качество возникает благодаря наличию связей в системе, которые осуществляют перенос свойств каждого элемента системы ко всем остальным элементам системы. Такие связи называются интегральными или системными.

Эффективность функционирования системы управления риском, исходя из основных положений системного подхода, определяется эффективным взаимодействием между частями системы, нежели результативной работой ее отдельных частей.

Таким образом, система управления рисками представляет собой совокупность взаимосвязанных и взаимозависимых элементов, конечной целью существования которых является минимизация рисков.

Систему управления риском можно охарактеризовать как совокупность методов, приемов и мероприятий, позволяющих в определенной степени прогнозировать наступление рисковых событий и принимать меры к исключению или снижению отрицательных последствий наступления таких событий. На систему управления риском оказывают влияние как внутренние, так и внешние факторы.

Системный подход предписывает искать истоки проблем, возникающих в работе, в первую очередь во внешней среде.

2.2 Принципы риск-менеджмента

Для организации корпоративной системы управления рисками необходимо соблюдение четырех основополагающих принципов.

Первый принцип. Коллегиальный орган управления. Многолетний опыт, накопленный банкирами-лидерами в решении задач корпоративного риск-менеджмента, свидетельствует о том, что для эффективного управления рисками нужна децентрализация функций по принятию управленческих решений. Решения, связанные с риском, не должны приниматься одним человеком, или, если это необходимо, полномочия такого лица должны быть ограничены в разумных пределах. Как говорится, одна голова — хорошо, а две или десять — лучше. Это объясняется потребностью в устранении конфликта интересов (злоупотреблений в целях получения личной выгоды) и однобоких суждений (ясно, что ни один человек не обладает сверхспособностями). Как правило, такой коллегиальный орган управления формируется из наиболее разносторонних и опытных руководителей высшего и среднего руководящего звена. Здесь можно провести параллель с организацией бюджетного процесса, когда из общего числа руководителей предприятия разного уровня выделяется ряд лиц, ответственных за его создание и подготовку стратегических планов развития предприятия, которые рассматривают проекты бюджетов до их утверждения на высшем уровне и периодически собираются на оперативные совещания (планерки). Именно эти люди могут рассматриваться в качестве членов коллегиального органа управления предприятием, на который будут возложены функции по управлению рисками.

Второй принцип. Независимое аналитическое подразделение. Для поддержки процесса принятия управленческих решений требуется формирование специализированного и самостоятельного аналитического подразделения, сотрудники которого, являясь высококвалифицированными экономистами, должны обладать также знаниями во всех специфических областях деятельности предприятия. Нельзя сказать, что подобного подразделения и сотрудников у предприятий никогда не было. Речь идет о планово-экономическом отделе, который может послужить в качестве базы для создания подразделения, отвечающего за независимую оценку рисков и информационно-аналитическую поддержку решений, принимаемых упомянутым коллегиальным органом управления.

Третий принцип. Система внутреннего контроля. Как в любой сфере деятельности, для обеспечения эффективности принимаемых управленческих решений в сфере управления рисками необходима система контроля над их выполнением, как подразделениями предприятия, так и отдельно взятыми должностными лицами. Это, кстати, тоже нельзя назвать новшеством, так как действующий бюджетный процесс предполагает контроль исполнения утвержденных бюджетов. Если на предприятии внедрено бюджетирование, создание системы внутреннего контроля будет в значительной степени облегчено. Кроме того, в штате крупных предприятий нередко встречаются внутренние аудиторы, на которых могут и должны быть возложены соответствующие функции.

Четвертый принцип. Мотивация персонала. Как уже неоднократно отмечалось, важным (если не ключевым) условием внедрения предприятием риск-ориентированного менеджмента является развитие культуры корпоративного управления — культуры управления рисками. Практика показывает, что ни одна инициатива со стороны высшего руководства предприятия (кроме индексации зарплаты) не будет восприниматься рядовыми сотрудниками и менеджерами среднего звена должным образом без соответствующей мотивации, будь то административные, в том числе материальные поощрения либо взыскания или же какие-нибудь иные способы.

Как видно из сказанного выше, управление рисками нельзя назвать чем-то принципиально новым для менеджмента предприятия — многие его составляющие в том или ином виде уже знакомы руководящему составу и даже присутствуют в повседневной работе предприятия. Поэтому интерес к внедрению риск-ориентированного менеджмента можно охарактеризовать как очередной эволюционный этап развития предприятия, который является закономерной реакцией на постоянный рост технологичности бизнеса и объективное ужесточение конкуренции как на внутреннем рынке, так и на международной арене. Это становится особенно актуальным, если учесть, что Россия находится на пороге вхождения во Всемирную торговую организацию (ВТО).

Еще одним аргументом в пользу сделанных выводов может послужить бурный рост интереса к такой, казалось бы, не связанной с обсуждаемой темой, но очень популярной в последнее время проблеме, как контроль качества. Можно даже говорить о настоящем буме вокруг получения предприятиями сертификатов соответствия международным стандартам контроля качества серии ISO 9000. Это связано с тем, что сертификат ISO давно уже является знаком качества продукции или услуг для конечного потребителя, а значит, дополнительной гарантией надежности и профессиональной компетентности предприятия, его руководителей и персонала. Наличие таких сертификатов в значительной степени распространено среди иностранных предприятий, которые из сегодняшних партнеров завтра смогут превратиться в прямых конкурентов.

2.3 Функции риск-менеджмента

Риск-менеджмент выполняет определенные функции. Различают два типа функций риск-менеджмента: функции объекта управления и функции субъекта управления.

К функциям объекта управления в риск-менеджменте относится организация:

- разрешения риска;
- рисковых вложений капитала;
- работы по снижению величины риска;
- процесса страхования рисков;
- экономических отношений и связей между субъектами хозяйственного процесса.

К функциям субъекта управления в риск-менеджменте относятся:

- прогнозирование;
- организация;
- регулирование;
- координация;
- стимулирование;
- контроль.

Прогнозирование в риск-менеджменте представляет собой разработку на перспективу изменений финансового состояния объекта в целом и его различных частей. Прогнозирование - это предвидение определенного события. Оно не ставит задачу непосредственно осуществить на практике разработанные прогнозы. Особенностью прогнозирования является также альтернативность в построении финансовых показателей и параметров, определяющая разные варианты развития финансового состояния объекта управления на основе наметившихся тенденций. В динамике рис-ка прогнозирование может осуществляться как на основе экстраполяции прошлого в будущее с учетом экспертной оценки тенденции изменения, так и на основе прямого предвидения изменений. Эти изменения могут возникнуть неожиданно. Управление на основе предвидения этих изменений требует выработки у менеджера определенного чутья рыночного механизма и интуиции, а также применения гибких экстренных решений.

Организация в риск-менеджменте представляет собой объединение людей, совместно реализующих программу рискового вложения капитала на основе определенных правил и процедур. К этим правилам и процедурам относятся: создание органов управления, построение структуры аппарата управления, установление взаимосвязи между управленческими подразделениями, разработка норм, методик и т.п.

Регулирование в риск-менеджменте представляет собой воздействие на объект управления, посредством которого достигается состояние устойчивости этого объекта в случае возникновения отклонения от заданных параметров. Регулирование охватывает главным образом текущие мероприятия по устранению возникших отклонений.

Координация в риск-менеджменте представляет собой согласованность работы всех звеньев системы управления риском, аппарата управления и специалистов.

Координация обеспечивает единство отношений объекта управления, субъекта управления, аппарата управления и отдельного работника.

Стимулирование в риск-менеджменте представляет собой побуждение финансовых менеджеров и других специалистов к заинтересованности в результате своего труда.

Контроль в риск-менеджменте представляет собой проверку организации работы по снижению степени риска. Посредством контроля собирается информация о степени выполнения намеченной программы действия, доходности рисковых вложений капитала, соотношении прибыли и риска, на основании которой вносятся изменения в финансовые программы, организацию финансовой работы, организацию риск-менеджмента.

2.4 Организация системы риск-менеджмента на предприятии

Одни и те же риски могут встречаться в различных областях производственно-хозяйственной деятельности. Поэтому при управлении рисками главное — идентифицировать возможные области риска применительно к исследуемому предприятию. Риск количественно характеризуется субъективной оценкой ожидаемой величины максимального и минимального доходов (убытков) от конкретного вложения капитала. При этом чем больше диапазон между возможным максимальным и минимальным доходами (убытками) при равной вероятности их получения, тем выше степень риска. Степень риска — это вероятность наступления рискового события; чем больше неопределенность хозяйственной ситуации при принятии решения, тем больше и степень риска. Факторы, влияющие на величину степени риска, можно разделить на объективные и субъективные. К объективным факторам относятся причины, возникающие во внешней среде предприятия, то есть не зависящие непосредственно от деятельности фирмы. Например, политические или экономические кризисы, таможенная, налоговая политика государства. Субъективные факторы связаны непосредственно с внутренней средой фирмы и характеризуют ее деятельность: уровень производительности труда, уровень технического и технологического оснащения.

Риск-менеджмент характеризуется совокупностью методов, приемов и мероприятий, позволяющих в определенной степени прогнозировать наступление рисков и принимать решения по воздействию на них. Стратегия управления риском строится в зависимости от направлений деятельности предприятия. Для эффективного управления риском на предприятиях может создаваться специальное подразделение — отдел управления рисками. Во главе его стоит риск-менеджер, который занимается исключительно проблемами управления риском и координирует деятельность всех подразделений в плане регулирования риска и обеспечения компенсации возможных потерь и убытков. Риск-менеджер формирует организационную структуру управления риском на предприятии и разрабатывает основные положения и инструкции, связанные с этой деятельностью.

2.5 Задачи и процесс управления рисками

Важнейшим этапом, следующим за прогнозированием оценкой и анализом риска в предпринимательской деятельности, является управление риском.

Управление риском имеет целью решение следующих задач:

1. Выживание. Удержание издержек и других параметров (моральных, экологических, юридических и др.) организации в границах, которые позволяют сохранить фирму как работающую и прибыльную.

2. Приемлемый уровень беспокойства. Иногда эту задачу называют "обеспечением покоя и нормального сна". Следует добавить, что эта задача ставится, как правило, с точки зрения руководства или владельца фирмы, но вопрос стоит более широко.

Все, кто так или иначе заинтересован судьбой фирмы, должен спать по возможности спокойно. Чувство безопасности, вера в устойчивость достигнутого благосостояния и в возможность улучшения благосостояния - это базовые потребности человека.

Человек спокойный обычно лучше работает. Однако человек слишком спокойный и уверенный в том, что ему гарантирована хорошая жизнь, начинает расслабляться.

Следовательно, уровень беспокойства должен быть по заданным критериям оптимальным. Критерии могут быть разными.

3. Стабильность доходов. Эту задачу следует трактовать как стабильность благосостояния всех сторон, заинтересованных в фирме.

4. Приемлемая непрерывность работы. В любой организации возможны сбои в работе. Задача - не допустить сбоев и остановок, чреватых гибелью фирмы.

5. Целесообразный темп устойчивого роста фирмы. Требуется подготовленность к риску срыва роста и ситуационное обеспечение возможных потерь, которые могут замедлить рост или сделать его неустойчивым.

6. Социальная ответственность. Прямого отношения к бизнесу данной фирмы это может и не иметь, но любой индивидуальный и групповой член общества должен вносить свою лепту в благосостояние общества.

7. Удовлетворение ограничений внешнего характера: юридических, регуляторных, традиционных и т.п.

8. Экономичность, удержание себестоимости управления предпринимательским риском на уровне, минимально достаточном для нормальной работы фирмы.

Все эти задачи имеют разную окраску и должны по-разному планироваться до потерь, во время кризиса и после потерь.

Например, решение задачи выживания до потерь может планироваться как прогнозирование сокрушительных потерь, проведение профилактических мероприятий.

Во время кризиса возникает необходимость оперативного планирования управления кризисом, снижение фактических потерь и недопущение сокрушительных потерь.

После потерь: оценка потенциально сокрушительных потерь:

- защита страховых интересов фирмы по сокрушительным потерям;
- преследование виновных и судебная защита фирмы.

Четкое определение задач очень важно при организации службы управления рисками, а также при согласованной деятельности ее различных компонент.

Процесс управления рисками фирмы - это прежде все принятие стратегии отношения фирмы к рискам вообще и каждому конкретному риску в отдельности.

Для обеспечения рисковой стратегии создается программа интегрированного управления рисками фирмы. После принятия программы к исполнению и внедрению на этой основе ведется мониторинг рисковой обстановки. При необходимости производится корректировка рисковой стратегии, и, соответственно, программы управления рисками.

Говоря о процессах управления риском, не следует иметь в виду только продукт, производимый фирмой. Сама фирма является "живым", целостным организмом, проходящим различные циклы своей деятельности. На этапах этих циклов возникают риски, источники которых могут быть как внутри, так и вне самой фирмы.

На первых этапах жизни фирма расходует деньги, разрабатывает продукт, подготавливая производство и обустраивая рыночную нишу, а доходов не зарабатывает.

На этапе быстрого роста возникает необходимость постоянного внешнего финансирования, которое относительно легко доступно, но опасна эйфория роста и избыточное заимствование.

На этапе зрелости темп роста замедляется, а фирма производит больше денег, чем может эффективно реинвестировать в свой бизнес.

На последней стадии фирма может быть умеренно прибыльной при снижающихся продажах, но неспособна реинвестировать в свою деятельность.

Этапы жизненного цикла организации могут быть представлены самым различным образом. Целесообразно анализировать прежде всего ее внутреннюю и внешнюю динамику.

1 . Внутренняя динамика

1 .1. Создание коммерческой организации:

- разработка миссии и стратегических целей бизнеса;
- определение рыночной ниши;
- определение продуктового ряда;
- выбор источника финансирования проекта создания фирмы;
- проведение PR-компании;
- запуск проекта.

1.2. Управление текущей деятельностью коммерческой организации:

- трансакции;
- максимизация прибыли;
- сокращение издержек;
- технологические переходы;
- решение социальных задач;
- решение экологических задач;
- страхование;
- фондовые операции.

1.3. Стратегическое управление коммерческой организацией:

- реструктуризация в рамках сложившейся структуры;
- рост фирмы;
- замедление;
- стабилизация;
- рецессия;
- упадок или новый цикл.

2. Внешняя динамика

2.1. Интеграционные процессы:

- слияние;
- разделение;
- приобретение;
- альянсы;
- партнерство;
- вертикальная интеграция.

2.2. Освоение новых рынков:

- горизонтальная интеграция;
- диверсификация;
- развитие экспортного потенциала.

Внутренняя и внешняя динамика коммерческой организации формирует одно измерение задач управления рисками, которые могут иметь место на каждом этапе жизненного цикла коммерческой организации.

Другое - виды финансовых ресурсов, используемых для реализации внутренней и внешней динамики фирмы (внутреннее финансирование, привлечение средств акционеров - пассивные инвесторы, заемное финансирование).

Можно построить матрицу, дающую самое общее представление о видах рисков, "разнесенных" по источникам финансирования и источникам жизненного цикла. На пересечении осей матрицы будет сформировано пять (в соответствии с приведенными ранее жизненными циклами) основных классов задач управления рисками.

Тот факт, что организационные системы - деловые организации, фирмы, корпорации и т.д. - многомерные не нов. Через всю последнюю треть прошедшего века красной нитью проходит идея системности. Это произошло в результате эволюции теории управления и бурного развития компьютеров, компьютерных сетей и программ обработки знаний.

В приложении к формирующейся ныне теории рисков фирмы многомерный подход к управлению может опираться на следующие идеи:

- необходимо выявление логично строгих информационных иерархий, через которые фирма получает данные;
- процесс детализации структур информации создает основу для дальнейшего манипулирования информацией на разных должностных позициях в фирме с разной степенью обобщения информации без нарушения целостности подхода;
- база данных строится на многомерном пересечении этих иерархий, образующих многомерный параллелепипед. Каждая рисковая экспозиция имеет по крайней мере три измерения:

1) тип ценности, находящийся под угрозой;
2) источник, вызывающий риск;
3) величина возможных и фактических финансовых и других последствий.

Кроме того, классификация экспозиций фирмы должна учитывать еще одно измерение, а именно - внутрифирменные, внефирменные, отечественные, зарубежные риски.

Важно отметить особую значимость информационного обеспечения управления риском, состоящего из разного рода и вида информации: статистической, экономической, коммерческой, финансовой и т.д., а также методов ее обработки, хранения и обновления.

2.6 Этапы организации риск-менеджмента

Риск-менеджмент по экономическому содержанию представляет собой систему управления риском и финансовыми отношениями, возникающими в процессе этого управления.

Как система управления, риск-менеджмент включает в себя процесс выработки цели риска и рисковых вложений капитала, определение вероятности наступления события, выявление степени и величины риска, анализ окружающей обстановки, выбор стратегии управления риском, выбор необходимых для данной стратегии приемов управления риском и способов его снижения (т.е. приемов риск-менеджмента), осуществление целенаправленного воздействия на риск. Указанные процессы в совокупности составляют этапы организации риск-менеджмента.

Первым этапом организации риск-менеджмента является определение цели риска и цели рисковых вложений капитала. **Цель** риска - это результат, который необходимо получить. Им может быть выигрыш, прибыль, доход и т.п. Цель рисковых вложений капитала - получение максимальной прибыли.

Любое действие, связанное с риском, всегда целенаправленно, так как отсутствие цели делает решение, связанное с риском, бессмысленным. Цели риска и рисковых вложений калитка должны быть четкими, конкретизированными и сопоставимыми с риском и капиталом.

Следующим важным моментом в организации риск-менеджмента является получение информации об окружающей обстановке, которая необходима для принятия решения в пользу того или иного действия. На основе анализа такой информации и с учетом целей риска можно правильно определить вероятность наступления события, в том числе страхового события, выявить степень риска и оценить его стоимость. Управление риском означает правильное понимание степени риска, который постоянно угрожает людям, имуществу, финансовым результатам хозяйственной деятельности.

Для предпринимателя важно знать действительную стоимость риска, которому подвергается его деятельность.

Под стоимостью риска следует понимать фактические убытки предпринимателя, затраты на снижение величины этих убытков или затраты по возмещению таких убытков и их последствий. Правильная оценка финансовым менеджером действительной стоимости риска позволяет ему объективно представлять объем возможных убытков и наметить пути к их предотвращению или уменьшению, а в случае невозможности предотвращения убытков обеспечить их возмещение.

На основе имеющейся информации об окружающей среде, вероятности, степени и величине риска разрабатываются различные варианты рискового вложения капитала и проводится оценка их оптимальности путем сопоставления ожидаемой прибыли и величины риска. Это позволяет правильно выбрать стратегию и приемы управления риском, а также способы снижения степени риска. На этом этапе организации риск-менеджмента главная роль принадлежит финансовому менеджеру, его психологическим качествам. Об этом подробнее будет рассказано в следующей главе.

При разработке программы действия по снижению риска необходимо учитывать психологическое восприятие рисковых решений. Принятие решений в условиях риска является психологическим процессом. Поэтому наряду с математической обоснованностью решений следует иметь в виду проявляющиеся при принятии и реализации рисковых решений психологические особенности человека: агрессивность, нерешительность, сомнения, самостоятельность, экстраверсию, интроверсию и др.

Одна и та же рисковая ситуация воспринимается разными людьми по-разному. Поэтому оценка риска и выбор финансового решения во многом зависит от человека, принимающего решения. От риска обычно уходят руководители консервативного типа, не склонные к инновациям, не уверенные в своей интуиции и в своем профессионализме, не уверенные в квалификации и профессионализме исполнителей, т.е. своих работников.

Экстраверсия - есть свойство личности, проявляющееся в ее направленности на окружающих людей, события. Она выражается в высоком уровне общительности, живом эмоциональном откли-ке на внешние явления.

Интроверсия - это направленность личности на внутренний мир собственных ощущений, переживаний, чувств и мыслей. Для интровертивной личности характерны некоторые устойчивые особенности поведения и взаимоотношений с окружающими, опора на внутренние нормы, самоуглубленность. Суждения, оценки интравертов отличаются значительной независимостью от внешних факторов, рассудительностью. Обычно человек совме-щает в определенной пропорции черты экстраверсии и интроверсии.

Неотъемлемым этапом организации риск-менеджмента является организация мероприятий по выполнению намеченной программы действия, т.е. определение отдельных видов мероприятий, объемов и источников финансирования этих работ, конкретных исполнителей, сроков выполнения и т.п.

Важным этапом организации риск-менеджмента являются контроль за выполнением намеченной программы, анализ и оценка результатов выполнения выбранного варианта рискового решения.

Организация риск-менеджмента предполагает определение органа управления риском на данном хозяйственном субъекте. Органом управления риском может быть финансовый менеджер, менеджер по риску или соответствующий аппарат управления: сектор страховых операций, сектор венчурных инвестиций, отдел рисковых вложений капитала и т.п. Эти секторы или отделы являются структурными подразделениями финансовой службы хозяйствующего субъекта.

Отдел рисковых вложений капитала в соответствии с уставом хозяйствующего субъекта может осуществлять следующие функции:

- проведение венчурных и портфельных инвестиций, т.е. рисковых вложений капитанов в соответствии с действующим законодательством и уставом хозяйствующего субъекта;
- разработка программы рисковой инвестиционной деятельности;
- сбор, обработка, анализ и хранение информации об окружающей обстановке;
- определение степени и стоимости рисков, стратегии и приемов управления риском;
- разработка программы рисковых решений и организация ее выполнения, включая контроль и анализ результатов;
- осуществление страховой деятельности, заключение договоров страхования и перестрахования, проведение страховых и перестраховых операций, расчетов по страхованию;
- разработка условий страхования и перестрахования, установление размеров тарифных ставок по страховым операциям;
- выполнение функции аварийного комиссара, выдача гарантии по поручительству российских и иностранных страховых компаний, возмещение убытков за их счет, поручение другим лицам исполнение аналогичных функций за рубежом;
- ведение соответствующей бухгалтерской, статистической и оперативной отчетности по рисковым вложениям капитала.

2.7 Внешние и внутренние факторы системы управления рисками

Внешними факторами системы управления риском являются:

- нормативная база в сфере регулирования риска (нормативы, методики, рекомендации, стандарты бухгалтерского учета и т.п.);
- макроэкономические факторы;
- зарубежный опыт управления риском.

Наиболее характерными чертами внешней среды является динамичность многообразие и интегрированность.

Динамичность предполагает быструю изменчивость внешней среды. Задача - создавать адаптивные системы управления риском, которые не сопротивляются изменениям внешней среды, а меняются вместе с ней.

Следующая характерная черта внешней среды - многообразие. Современная организация взаимодействует с огромным числом различных объектов - акционерами, клиентами, партнерами, Центральным банком, органами власти, конкурентами и т.д. Все это многообразие усугубляется еще и тем, что все объекты связаны между собой множеством нитей - экономических, информационных, политических, административных, постоянно влияют друг на друга, то есть внешняя среда интегрирована.

Следовательно, изменение взаимодействия организации с любым из этих объектов влечет за собой изменение отношений и с остальными.

Внутренние факторы системы управления риском включают:

1. Специфику деятельности организации, его политику, стратегию и тактику,
2. Организационную структуру,
3. Квалификацию персонала.

Основными чертами внутренней среды являются:

- стремление к выживанию,
- постоянное изменение, развитие, направленное на приспособление к внешней среде,
- совершенствование,
- наличие целостности, единого предназначения для всех элементов.

Как система управления, управление риском предполагает осуществление ряда процессов и действий, которые представляют собой элементы системы управления риском. К ним можно отнести:

- идентификацию и локализацию риска;
- анализ и оценку риска;
- способы минимизации и предотвращения риска;
- мониторинг рисковых позиций.

Процесс управления риском можно упрощенно представить в виде блок-схемы (рис4).

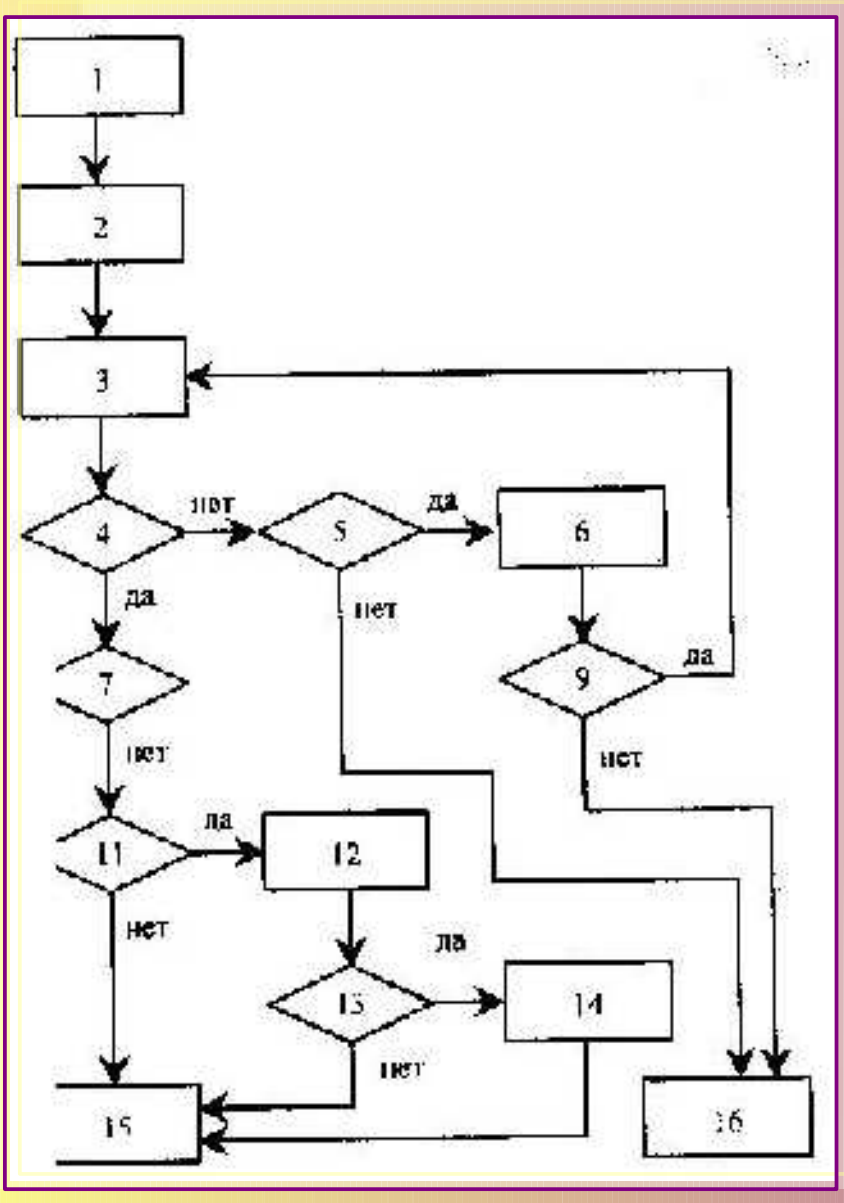


Рис. 4. ***Блок-схема процесса управления риском:***
1 - сбор и обработка данных;
2 - качественный анализ риска;
3 - количественная оценка риска;
4 - оценка приемлемости риска;
5, 11 - оценка возможности снижения риска;
6,12 - выбор методов и формирование вариантов снижения риска,
7 - оценка возможности увеличения риска;
8- формирование и выбор вариантов увеличения риска;
9,13 - оценка целесообразности снижения риска;
10 -оценка целесообразности увеличения риска;
14 - выбор варианта снижения риска;
15 - реализация проекта (принятие риска);
16 - отказ от реализации проекта (избежание риска)

Следует отметить, что сбор и обработка информации является важным этапом процесса управления независимо от его конкретного содержания. В процессе управления риском к полноте и качеству информации предъявляются особые требования, так как отсутствие полной информации является одним из существенных факторов риска, и принятие решения в условиях неполной информации служит источником дополнительных финансовых потерь. На схеме для упрощения блок-схемы сбор и обработка информации по аспектам риска представлены в качестве первого этапа. В действительности эта работа осуществляется на протяжении всего процесса принятия решения. По мере перехода от одного этапа к другому при необходимости может уточняться потребность в дополнительной информации, осуществляться ее сбор и обработка. Особую роль играет информация в процессе качественного и количественного анализа риска.

Качественный анализ предполагает: выявление источников и причин риска, этапов и работ, при выполнении которых возникает риск, т.е. установление потенциальных зон риска, идентификацию всех возможных рисков, выявление практических выгод и возможных негативных последствий, которые могут наступить при реализации содержащего риск решения. Результаты качественного анализа служат важной исходной информацией для осуществления количественного анализа.

Количественный анализ предполагает численное определение отдельных рисков и общего риска. На этом этапе определяется вероятность наступления рисковых событий и их последствий, осуществляется количественная оценка степени риска, определяется также допустимый уровень риска.

В результате проведения анализа риска получается картина возможных рисковых событий, вероятность их наступления и последствий. После сравнения полученных значений рисков с предельно допустимыми вырабатывается стратегия управления риском, и на этой основе - меры предотвращения и уменьшения риска.

Меры по устранению и минимизации риска включают следующие этапы:

1. Оценку приемлемости полученного уровня риска;
2. Оценку возможности снижения риска или его увеличения (в случае, когда полученные значения риска значительно ниже допустимого, а увеличение степени риска обеспечит повышение ожидаемой отдачи);
3. Выбор методов снижения (увеличения) рисков;
4. Оценку целесообразности и выбор вариантов снижения (увеличения) рисков.

После выбора определенного набора мер по устранению и минимизации риска следует принять решение о степени достаточности выбранных мер. Если мер недостаточно целесообразно отказаться от реализации проекта (избежать риска).

Следует отметить, что нами рассмотрена лишь общая схема процесса управления риском. Характер и содержание перечисленных этапов и работ, используемые методы их выполнения в значительной степени зависят от специфики предпринимательской деятельности и характера возможных рисков.

2.8 Особенности выбора стратегии и методов решения управленческих задач

На этом этапе организации риск-менеджмента главная роль принадлежит финансовому менеджеру, его психологическим качествам. Финансовый менеджер, занимающийся вопросами риска (менеджер по риску), должен иметь два права: право выбора и право ответственности за него.

Право выбора означает право принятия решения, необходимого для реализации намеченной цели рискового вложения капитала. Решение должно приниматься менеджером единолично. В риск-менеджменте из-за его специфики, которая обусловлена прежде всего особой ответственностью за принятие риска, нецелесообразно, а в отдельных случаях и вовсе недопустимо коллективное (групповое) принятие решения, за которое никто не несет никакой ответственности.

Коллектив, принявший решение, никогда не отвечает за его выполнение. При этом следует иметь в виду, что коллективное решение в силу психологических особенностей отдельных индивидов (их антагонизма, эгоизма, политической, экономической или идеологической платформы и т.п.) является более субъективным, чем решение, принимаемое одним специалистом.

Для управления риском могут создаваться специализированные группы людей, например сектор страховых операций, сектор венчурных инвестиций, отдел рисковых вложений капитала (т.е. венчурных и портфельных инвестиций) и др.

Данные группы людей могут подготовить предварительное коллективное решение и принять его простым или квалифицированным (т.е. две трети, три четверти, единогласно) большинством голосов.

Однако окончательно выбрать вариант принятия риска и рискового вложения капитала должен один человек, так как он одновременно принимает на себя и ответственность за данное решение.

Ответственность указывает на заинтересованность принимающего рисковое решение в достижении поставленной им цели.

При выборе стратегии и приемов управления риском часто используется какой-то определенный стереотип, который складывается из опыта и знаний финансового менеджера в процессе его работы и служит основой автоматических навыков в работе. Наличие стереотипных действий дает менеджеру возможность в определенных типовых ситуациях действовать оперативно и наиболее оптимальным образом. При отсутствии типовых ситуаций финансовый менеджер должен переходить от стереотипных решений к поискам оптимальных, приемлемых для себя рисковых решений.

Подходы к решению управленческих задач могут быть самыми разнообразными, потому риск-менеджмент обладает многовариантностью.

Многовариантность риск-менеджмента означает сочетание стандарта и неординарности финансовых комбинаций, гибкость и неповторимость тех или иных способов действия в конкретной хозяйственной ситуации. Главное в риск-менеджменте - правильная постановка цели, отвечающая экономическим интересам объекта управления.

Риск-менеджмент весьма динамичен. Эффективность его функционирования во многом зависит от быстроты реакции на изменения условий рынка, экономической ситуации, финансового состояния объекта управления. Поэтому риск-менеджмент должен базироваться на знании стандартных приемов управления риском, на умении быстро и правильно оценивать конкретную экономическую ситуацию, на способности быстро найти хороший, если не единственный выход из этой ситуации.

В риск-менеджменте готовых рецептов нет и быть не может. Он учит тому, как, зная методы, приемы, способы решения тех или иных хозяйственных задач, добиться ощутимого успеха в конкретной ситуации, сделав ее для себя более или менее определенной.

Особую роль в решении рисковых задач играют интуиция менеджера и инсайт.

Интуиция представляет собой способность непосредственно, как бы внезапно, без логического продумывания находить правильное решение проблемы. Интуитивное решение возникает как внутреннее озарение, просветление мысли, раскрывающее суть изучаемого вопроса. Интуиция является непременным компонентом творческого процесса. Психология рассматривает интуицию во взаимосвязи с чувственным и логическим познанием и практической деятельностью как непосредственное знание в его единстве со знанием опосредованным, ранее приобретенным.

Инсайт - это осознание решения некоторой проблемы. Субъективно инсайт переживают как неожиданное озарение, постижение. В момент самого инсайта решение осознается очень ясно, однако эта ясность часто носит кратковременный характер и нуждается в сознательной фиксации решения.

2.9 Правила риск-менеджмента

В случаях, когда рассчитать риск невозможно, принятие рисковых решений происходит с помощью эвристики. Эвристика представляет собой совокупность логических приемов и методических правил теоретического исследования и отыскания истины. Иными словами, это правила и приемы решения особо сложных задач. Конечно, эвристика менее надежна и менее определенна, чем математические расчеты. Однако она дает возможность получить вполне определенное решение.

Риск-менеджмент имеет свою систему эвристических правил и приемов для принятия решений в условиях риска. Основные правила риск-менеджмента:

1. Нельзя рисковать больше, чем это может позволить собственный капитал.
2. Надо думать о последствиях риска.
3. Нельзя рисковать многим ради малого.
4. Положительное решение принимается лишь при отсутствии сомнения.
5. При наличии сомнений принимаются отрицательные решения.
6. Нельзя думать, что всегда существует только одно решение.

Реализация первого правила означает, что прежде, чем принять решение о рисковом вложении капитала, финансовый менеджер должен:

1)определить максимально возможный объем убытка по данному риску;

2)сопоставить его с объемом вкладываемого капитала;

3)сопоставить его со всеми собственными финансовыми ресурсами и определить, не приведет ли потеря этого капитала к банкротству данного инвестора.

Объем убытка от вложения капитала может быть равен объему данного капитала, чуть меньше или больше его. При прямых инвестициях объем убытка, как правило, равен объему венчурного капитала. При портфельных инвестициях, т.е. при покупке ценных бумаг, которые можно продать на вторичном рынке, объем убытка обычно меньше суммы затраченного капитала.

Соотношение максимально возможного объема убытка и объема собственных финансовых ресурсов инвестора представляет собой степень риска, ведущую к банкротству.

Исследования рисковых мероприятий, проведенные автором, позволяют сделать вывод, что оптимальный коэффициент риска составляет 0,3, а коэффициент риска, ведущий к банкротству инвестора, - 0,7 и более.

Реализация второго правила требует, чтобы финансовый менеджер, зная максимально возможную величину убытка, определил бы, к чему она может привести, какова вероятность риска, и принял решение об отказе от риска (т.е. от мероприятия), принятии риска на свою ответственность или передаче риска на ответственность другому лицу.

Действие третьего правила особенно ярко проявляется при передаче риска, т.е. при страховании. В этом случае он означает, что финансовый менеджер должен определить и выбрать приемлемое для него соотношение между страховым взносом и страховой суммой. Страховой взнос - это плата страхователя страховщику за страховой риск. Страховая сумма - это денежная сумма, на которую застрахованы материальные ценности, ответствен-ность, жизнь и здоровье страхователя. Риск не должен быть удержан, т.е. инвестор не должен принимать на себя риск, если размер убытка относительно велик по сравнению с экономией на страховом взносе.

Реализация остальных правил означает, что в ситуации, для которой имеется только одно решение (положительное или отрицательное), надо сначала попытаться найти другие решения. Возможно, они действительно существуют. Если же анализ показывает, что других решений нет, то действуют по правилу «в расчете на худшее», т.е. если сомневаешься, то принимай отрицательное решение.

3.1 Риск-профиль финансовых организаций

Как уже отмечалось, компании реального сектора экономики и финансовые организации — это как бы два разных, но в то же время очень похожих друг на друга мира. Значит, и риски в их деятельности должны быть сопоставимы. Поэтому обратимся к уже накопленному финансовыми организациями опыту.

В относительно устоявшейся в настоящее время практике управления рисками принято выделять следующие основные виды рисков:

- кредитные риски — риски возникновения потерь вследствие несвоевременных платежей или неплатежей со стороны контрагентов;
- рыночные риски (в том числе фондовые, процентные и валютные) — риски возникновения убытков вследствие неблагоприятного изменения рыночных цен (например, котировок ценных бумаг, уровня процентных ставок по кредитам, обменных курсов валют и т. д.);
- риски ликвидности— риски возникновения неблагоприятных последствий (в том числе убытков) в результате неспособности организации своевременно и в полном объеме исполнить обязательства перед кредиторами;
- операционные риски (в том числе правовые) — риски возникновения непредвиденных убытков следующего характера:
- внутреннего — из-за неадекватности бизнес-процессов, квалификации персонала и надежности применяемых технических средств масштабам деятельности организации;
- внешнего — в результате негативного воздействия неконтролируемых организацией факторов (например, катастрофы, стихийные бедствия, преступность и коррупция);
- стратегические риски — риски возникновения убытков вследствие принятия высшим руководством организации компетентных управленческих решений, однако основанных на оказавшихся ошибочными предположениях о развитии внешней экономической среды; другими словами, непредсказуемые риски деловых неудач;
- репутационные риски — риски сужения масштабов деятельности организации (вплоть до ликвидации) вследствие утраты доверия к ней со стороны клиентов и деловых партнеров.

Все указанные виды рисков называют типичными банковскими рисками. По крайней мере, потому, что так делают центральные банки (регуляторы) подавляющего большинства развитых стран. Однако считать, что сфера влияния этих рисков ограничивается лишь банковским сектором экономики, по меньшей мере, некорректно.

Чтобы проиллюстрировать ход мысли регуляторов банковского сектора экономики, приведем простой пример: если завтра назвать закупку карандашей типичным видом банковской деятельности, то любой банк будет вынужден под страхом отзыва лицензии приобретать карандаши в строгом соответствии с предъявляемыми требованиями. Другими словами, чтобы заставить банки задумываться о чем-то важном, но непривлекательном с финансовой точки зрения, регуляторам проще всего назвать это типичным для банковской деятельности, а затем устанавливать соответствующие требования. Поэтому, учитывая широту затрагиваемых проблем, приведенный список типичных банковских рисков с некоторыми допущениями можно признать если не исчерпывающим, то хотя бы достаточным для организации абсолютно любой отраслевой принадлежности. Так, например, кредитные риски для предприятий часто проявляются в виде недоставок и неплатежей со стороны клиентов и поставщиков. Однако предприятия также принимают кредитные риски в классическом понимании этого слова на обслуживающие банки, не говоря уже о предоставлении займов (по сути, тех же кредитов) другим организациям.

Пожалуй, единственное серьезное отличие списка типичных рисков для предприятий от соответствующего списка для финансовых организаций — наличие в деятельности первых существенных концентрационных рисков. Сущность этих рисков заключается в объективно меньшей способности предприятий диверсифицировать свой бизнес как географически, так и по отраслям экономики, чем это могут позволить себе финансовые организации, перемещая свои капиталы с помощью фондового рынка буквально за считанные дни.

3.2 Основные направления нейтрализации предпринимательских рисков

Предпринимательская организация в процессе осуществления производственно-хозяйственной деятельности может отказаться от совершения отдельных операций или видов деятельности, связанных с высоким уровнем риска, т.е. уклониться от риска. Данное направление нейтрализации рисков является наиболее простым и радикальным. Оно позволяет полностью избежать потенциальных потерь, связанных с предпринимательскими рисками, но, с другой стороны, не позволяет и получить прибыли, связанные с рискованной деятельностью. Кроме того, в отдельных случаях уклонение от риска может быть просто невозможным, а также избежание одного вида риска может привести к возникновению других. Поэтому, как правило, данный способ применим лишь в отношении очень серьезных и крупных рисков.

Решение об отказе от определенных предпринимательских рисков может быть принято как на предварительной стадии принятия решения, так и позднее, путем отказа от дальнейшего осуществления деятельности, в том случае, если риск оказался выше предполагаемого. Однако большинство решений об избегании риска принимается на предварительной стадии принятия решения, так как отказ от продолжения деятельности часто влечет значительные финансовые и иные потери для предприятия, а иногда затруднителен в связи с контрактными обязательствами предпринимательской организации.

Применение такого способа нейтрализации предпринимательских рисков, как уклонение от риска, эффективно при выполнении определенных условий.

Отказ от одного вида предпринимательского риска не влечет за собой возникновения других видов рисков более высокого или однозначного уровня.

Уровень риска намного выше уровня возможной доходности предпринимательской сделки или деятельности в целом.

Финансовые потери по данному виду риска предпринимательская фирма не имеет возможности возместить за счет собственных финансовых средств, так как эти потери слишком высоки.

Естественно, что не от всех видов предпринимательских рисков предприятие может уклониться, большую часть из них оно "принимает на себя", т.е. сознательно идет на риск и занимается бизнесом до тех пор, пока убытки от последствий наступивших рисков не приведут к невосполнимым потерям.

Некоторые риски принимаются, так как несут в себе потенциал возможной прибыли, другие принимаются в силу своей неизбежности.

При "принятии риска на себя" основной задачей является изыскание источников необходимых ресурсов для покрытия возможных потерь. В данном случае потери покрываются из любых ресурсов, оставшихся после наступления предпринимательского риска, и, как следствие, наступления потерь. Если оставшихся ресурсов у предприятия недостаточно, то это может привести к сокращению объемов бизнеса.

Ресурсы, имеющиеся в распоряжении предпринимательской организации для покрытия потерь, можно разделить на две группы:

- ресурсы внутри самого бизнеса;
- кредитные ресурсы.

Ресурсы внутри самого бизнеса. При возникновении потерь крайне редко бывают повреждены все виды собственности одновременно, поэтому к внутренним ресурсам относятся:

- наличность в кассе, которая не страдает при физическом повреждении зданий и сооружений, принадлежащих предприятию;
- остаточная стоимость поврежденной собственности;
- доход от частичного продолжения финансовой и производственной деятельности;
- дивиденды и процентный доход от ценных бумаг и доходных инвестиций;
- дополнительные средства, вносимые владельцами бизнеса с целью его поддержания;
- нераспределенный остаток прибыли, полученной в отчетном периоде, до его распределения он может рассматриваться как резерв финансовых ресурсов, направляемых в необходимом случае на ликвидацию негативных последствий отдельных финансовых рисков.

Резервный фонд образуется за счет отчислений от прибыли в размере, определенном уставом, но не менее 15% его уставного капитала. Ежегодно в резервный фонд должно отчисляться не менее 5% чистой прибыли до тех пор, пока резервный капитал не достигнет установленного уставом размера. Резервный капитал в узком смысле предназначен для покрытия его убытков, а в акционерных обществах также для погашения облигаций общества и выкупа их акций в случае отсутствия иных средств.

Кредитные ресурсы. В том случае, если предпринимательская организация не в состоянии покрыть все потери, возникающие в результате воздействия предпринимательских рисков, из внутренних ресурсов, часть из них можно покрыть с использованием кредитных ресурсов. Однако в данном случае доступность кредитных ресурсов имеет существенные ограничения. И главным из них является перспектива будущей прибыльности предприятия. Доступность кредитных ресурсов во многом зависит от остаточной стоимости бизнеса после возникновения потерь. Другим ограничением в привлечении кредитных ресурсов после возникновения рисков может быть их цена. Использование кредитных ресурсов может ослабить финансовое положение предпринимательской организации.

Следующий возможный метод нейтрализации рисков, возникающих в процессе осуществления предпринимательской деятельности предприятия, - это передача или трансферт риска партнерам по отдельным сделкам или хозяйственным операциям путем заключения контрактов. При этом хозяйственным партнерам передается та часть предпринимательских рисков предприятия, по которой оно имеет больше возможностей нейтрализации их негативных последствий и, как правило, располагает более эффективными способами внутренней страховой защиты. В современной практике управления рисками получили распространение следующие основные направления передачи рисков.

Передача рисков путем заключения договора факторинга. Предметом передачи в данном случае является кредитный риск предприятия, который в преимущественной его доле передается коммерческому банку или специализированной факторинговой компании, что позволяет предприятию в существенной степени нейтрализовать негативные финансовые последствия кредитного риска.

Передача риска путем заключения договора поручительства. Российское законодательство предусматривает возможность заключения договора поручительства. В силу договора поручитель обязывается перед кредитором третьего лица отвечать за исполнение последним его обязательства полностью или частично. При неисполнении или ненадлежащем исполнении должником обеспеченного поручительством обязательства поручитель и должник отвечают перед кредитором солидарно. Предприятие использует поручительства для привлечения заемного капитала и при этом несет ответственность перед поручителем за четкое исполнение договора поручительства. Таким образом, предприятие-кредитор передает риск невозврата кредита и связанные потери поручителю.

Существует еще один вид гаранта – это банковская гарантия, - письменное обязательство кредитной организации, выданное по просьбе другого лица - принципала, уплатить кредитору принципала – бенефициару в соответствии с условиями даваемого гарантом обязательства денежную сумму по представлении бенефициаром письменного требования о ее уплате. За выдачу банковской гарантии принципал уплачивает гаранту вознаграждение. Банковская гарантия позволяет предпринимательской организации избежать риски при заключении сделок с оплатой в будущем или по факту предоставления услуг, выполнения работ, отгрузки товаров.

Передача рисков поставщикам сырья и материалов. Предметом передачи в данном случае являются прежде всего риски, связанные с порчей или потерей имущества в процессе транспортировки и осуществления погрузочно-разгрузочных работ. Однако потери, связанные с падением рыночной цены продукции, несет предприятие, даже если подобное падение вызвано задержкой в доставке груза.

Передача рисков путем заключения биржевых сделок. Этот метод передачи риска осуществляется путем хеджирования.

Биржевые сделки снижают риск снабжения в условиях инфляционных ожиданий и отсутствия надежных оперативных каналов закупок. Минимизация рисков снабжения в данном случае также осуществляется за счет передачи риска путем:

- приобретения опционов на закупку товаров и услуг, цена на которые в будущем увеличится;
- заключения фьючерсных контрактов на закупку растущих в цене товаров.

Контракты продажи, обслуживания, снабжения. Договоры, связанные с распространением товаров и услуг, также предоставляют предприятию широкие возможности по снижению риска путем их передачи. Производитель или дистрибьютор обычно предлагает потребителю гарантию устранения дефектов либо замены недоброкачественного товара или недоброкачественно выполненной услуги. При этом потребитель, покупая товар или услугу, передает риски, связанные с его эксплуатацией, производителю или дистрибьютору на период гарантии.

Возможно также соглашение между оптовым торговцем и производителем или между розничным и оптовым торговцами о возврате части непроданных товаров. В данном случае речь идет о передаче рыночного риска.

К этой же группе контрактов относятся:

- соглашение о снабжении товаром на условиях поддержания неснижаемого остатка на складе;
- аренда оборудования с гарантией его технического обслуживания и текущего ремонта;
- гарантия поддержания производительности (определенных технических характеристик) используемого оборудования;
- договоры на сервисное обслуживание техники.

В целом же передача риска происходит, если в заключенном сторонами контракте существует специфическое положение относительно передачи конкретных (или всех) предпринимательских рисков контрагенту. Сторона, принявшая на себя риск, обычно вторично передает его, заключив договор страхования ответственности.

Еще одним способом минимизации или нейтрализации рисков является распределение риска путем объединения (с разной степенью интеграции) с другими участниками, заинтересованными в успехе общего дела. Предприятие имеет возможность уменьшить уровень собственного риска, привлекая к решению общих проблем в качестве партнеров другие предприятия и даже физических лиц. Для этого могут создаваться акционерные общества, финансово-промышленные группы; предприятия могут приобретать или обмениваться акциями друг друга, вступать в различные консорциумы, ассоциации, концерны.

Таким образом, под объединением предпринимательского риска понимается метод снижения риска, при котором риск делится между несколькими субъектами экономики. Объединяя усилия в решении проблемы, несколько предпринимательских организаций могут разделить между собой как возможную прибыль, так и убытки от ее реализации. Как правило, поиски партнеров проводятся среди тех предприятий, которые располагают дополнительными финансовыми ресурсами, а также информацией о состоянии и особенностях рынка.

Одним из эффективных способов нейтрализации рисков является диверсификация. В качестве основных форм диверсификации предпринимательских рисков предприятием могут быть использованы следующие основные виды диверсификации.

Диверсификация предпринимательской деятельности предприятия, которая предусматривает использование альтернативных возможностей получения дохода от различных видов деятельности, не посредственно не связанных друг с другом. В таком случае, если в результате непредвиденных событий один вид деятельности окажется убыточным, другие будут приносить прибыль.

Диверсификация портфеля ценных бумаг. Данный вид диверсификации позволяет снижать инвестиционные риски, не уменьшая при этом уровень доходности инвестиционного портфеля.

Диверсификация программы реального инвестирования. В области формирования реального инвестиционного портфеля фирме рекомендуется отдавать предпочтение программам реализации нескольких проектов, относительно небольшой капиталоемкости перед программами, состоящими из единственного крупного инвестиционного проекта.

Диверсификация кредитного портфеля, которая направлена на снижение кредитного риска предприятия и предусматривает разнообразие покупателей продукции или услуг предпринимательской организации.

Диверсификация поставщиков сырья, материалов и комплектующих. В случае сбоя в поставках предпринимательской фирме не придется искать альтернативных поставщиков, а можно будет увеличить объемы закупок у других поставщиков.

Диверсификация покупателей продукции.

Диверсификация валютной корзины предприятия. Данный вид диверсификации предусматривает выбор нескольких различных видов валют в процессе осуществления предприятием внешнеэкономических операций. В результате использования этого вида диверсификации предпринимательская организация имеет возможность минимизировать валютные риски.

Существуют еще так называемые упреждающие методы нейтрализации предпринимательских рисков. Эти методы, как правило, более трудоемки, требуют обширной предварительной аналитической работы, от полноты и тщательности которой зависит эффективность их применения. К методам компенсации относятся:

- стратегическое планирование деятельности предпринимательской организации;
- обеспечение компенсации возможных финансовых потерь за счет включаемой в контракты системы штрафных санкций;
- сокращение перечня форс-мажорных обстоятельств в контрактах с партнерами;
- совершенствование управления оборотными средствами предприятия;
- сбор и анализ дополнительной информации о финансовом рынке;
- прогнозирование тенденций изменения внешней предпринимательской среды и конъюнктуры рынка.

В данном разделе были рассмотрены лишь основные пути нейтрализации предпринимательских рисков. Применение отдельных из них в деятельности конкретной предпринимательской организации зависит от опыта и возможностей, которыми она обладает. Для получения более эффективного результата, как правило, используется не один, а совокупность способов.

Следующий метод минимизации риска – это страхование. Страхование хозяйственных рисков представляет собой отношения по защите имущественных интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов (страховых премий). Следует отметить, что данный метод минимизации) риска имеет ряд ограничений:

- в первую очередь – это слишком высокая цена (иногда премия), запрашиваемая страховщиком за принятие на себя риска. Нередко она превышает ту цену, которую принципиальный страхователь полагает разумной за передачу данного риска;
- во вторую – ограниченная доступность страхования – некоторые риски не принимаются к страхованию. Так, если вероятность наступления рискового события очень велика, страховые организации либо не берутся страховать данный вид риска, либо назначают непомерно высокие платежи.

Цена и доступность страхования прямо связаны между собой, так как страхователь принимает на себя тот риск, потери от которого он может оценить.

Страхуемый вид риска характерен для таких чрезвычайных ситуаций, когда существует статистическая закономерность их возникновения, т.е. определена вероятность убытка. Отметим, что с помощью страхования можно минимизировать практически все имущественные, а также многие кредитные, коммерческие и производственные риски. Вместе с тем страхованию, как правило, не подлежат риски, связанные с недобросовестностью партнеров, - задержка платежей, неоплата продукции и т.п.

3.3 Управления рисками организаций инвестиционно-строительного комплекса

Сегодня одним из важнейших условий успешного функционирования предприятий инвестиционно-строительной сферы, обеспечивающих увеличение стоимости их активов, стабильное получение прибыли и реализацию социальных программ, является управление рисками. Вопросы риск-менеджмента в строительстве приобретают все большую актуальность. Управление рисками предприятия становится одним из ключевых конкурентных преимуществ независимо от формы собственности, и организационно-правовой формы предприятия инвестиционно-строительного комплекса.

Процесс управления и оценки рисков при принятии инвестиционных решений имеет большое значение, поскольку позволяет оценить возможные потери, запланировать процедуры для возможного их снижения, а также определить экономический эффект от управления рисками. Целью управления риском является снижение вероятности, частоты событий совпадения проявления рисков по различным причинам и, как следствие, снижение суммарных потерь (ущерба) по проекту.

При разработке и реализации инвестиционного проекта в строительстве преследуются две основные цели:

- создать объект, удовлетворяющий требованиям, предъявляемым заказчиком, инвестором или покупателем и соответствующий действующим нормам и правилам;
- создать механизм для покрытия понесенных заказчиком затрат и дальнейшего получения прибыли.

Непосредственным решением этих задач и занимается система риск-менеджмента в инвестиционном строительстве.

Управление риском в инвестиционном строительстве является сложной проблемой, на сегодняшний день мало изученной как в России, так и за рубежом. Основная причина такого положения — отсутствие аналитического описания воздействия возмущающих факторов, оказывающих влияние на систему управления и её составляющие. Неизбежность возникновения рисковых ситуаций при строительстве требует разработки и применения соответствующих методов предупреждения, идентификации и реагирования на них с целью исключения или максимально возможного снижения убытков.

Эффективное управление рисками в строительстве должно базироваться на принципах управления, являющихся одной из составляющих управленческой методологии, к которым следует отнести:

- осознанность принятия рисков;
- управляемость принимаемых рисков;
- независимость управления рисками;
- сопоставимость уровня управления принимаемых рисков с доходностью;
- сопоставимость уровня управления принимаемых рисков с финансовыми возможностями предприятия;
- экономичность управления рисками;
- учет временного фактора;
- учет финансовой стратегии предприятия;
- возможность передачи рисков.

Современный этап эволюции теории управления характеризуется появлением новой парадигмы – управление рисками, где в качестве интегрированного объекта управления выступает интегрированный риск предприятия. В соответствии с данной парадигмой риск-менеджмент должен быть:

- системным и интегрированным, т. е. управление рисками должно осуществляться в рамках всего предприятия, охватывая все уровни наблюдений: исполнителей, подразделения, стратегические бизнес-единицы, бизнес-процессы;
- непрерывным, т. е. управление рисками не должно зависеть от желаний менеджеров и должно охватывать все уровни управления: стратегический, тактический, оперативный;
- расширенным и комплексным, т. е. объектом управления должны быть все риски: внешние и внутренние, страхуемые и не страхуемые, частные и интегрированные. Предприятия должны на основе предлагаемого рискового спектра разрабатывать свой рисковый профиль;
- структурированным и последовательным, т. е. при управлении рисками должны реализовываться все функции управления: анализ и синтез, прогнозирование и планирование, организация и координация, учет и контроль, мотивация;
- целевым и стоимостноориентированным, т. е. управление рисками должно быть направлено на увеличение стоимости предприятия за счет выявления факторов неопределенности, рискообразующих факторов и управления ими, а также за счет непосредственного воздействия на риски методами страхования и самострахования.

Укрупненная схема управления рисками предприятия должна быть представлена в определенной логической последовательности.

1. Выявление и анализ рисков предприятия.
2. Описание угроз и классификация рисков.
3. Выявление и идентификация рисков.
4. Оценка рисков.
5. Выбор методов управления (воздействия) рисками при сравнении их эффективности.
6. Принятие решений о воздействии на риски.
7. Непосредственное управление (воздействие) рисками.
8. Мотивация менеджеров и сотрудников к максимальному выявлению и эффективному управлению рисками.
9. Контроль и корректировка результатов управления рисками.

При управлении рисками предприятия целесообразно использовать стоимостный подход, при этом необходимо разработать и внедрить систему управления рисками, включающую стратегию, структурные решения, совокупность методов воздействия на риски, кадровое и информационное обеспечение.

Система риск-менеджмента на предприятиях инвестиционно-строительного комплекса имеет свои особенности, которые во многом объясняются сложностью, многоэтапностью и длительными сроками процесса строительства. Процесс возведения объектов строительства осуществляется в общем случае в сферах инвестиций, изысканий, проектирования, управления и контроля качества строительства.

В процессе строительства стоимость возведенного объекта изменяется от нуля – в начале работ, до полной стоимости в соответствии с исполненным проектом – при сдаче объекта заказчику. Соответственно, изменяется и тяжесть возможного ущерба. Однако нельзя не отметить тот факт, что по мере строительства уменьшается количество монтажных нагрузок и воздействий, а следовательно, и риск возникновения ущерба от превышения их расчетных значений. По мере завершения строительства увеличивается риск возникновения ущерба от превышения эксплуатационных нагрузок и воздействий. Указанные характерные особенности строительства как процесса создания недвижимого имущества, безусловно, важны при оценке рисков возникновения ущербов, однако, как показывает опыт аварий строительных объектов в России, значительные материальные ущербы возникают в основном не из-за воздействий на объекты строительства опасностей, размеры которых превышают учтенные при расчетах в проектах, а по другим причинам. Анализ информации о крупных авариях зданий и сооружений показывает, что в половине случаев причинами являются низкое качество строительства и монтажа, материалов и конструкций.

Международная практика страхования строительных рисков предусматривает страховое покрытие не отдельных рисков, оговоренных в договоре страхования, а от всех рисков, которые могут произойти на строительной площадке. Именно такой полис, заключенный на условиях CAR (Contractors All Risks) может обеспечить по-настоящему эффективную защиту сооружаемого объекта от строительных рисков.

Однако время идет вперед, и сегодня строительным организациям необходимо уже не просто страхование, а комплексная система управления рисками – риск-менеджмент, поэтому некоторые страховые компании начали предлагать подрядчикам профессиональные услуги по управлению рисками. Сущность риск-менеджмента в на предприятиях инвестиционно-строительного комплекса заключается в исследовании возможных рисков, которым подвержен конкретный проект, оценке по специальным методикам их вероятности и разрушительности, в выявлении альтернативы, где величина риска остается приемлемой, и в выборе методов управления риском, способствующих устранению или минимизации возможных отрицательных последствий.

Для построения эффективной системы управления рисками предприятия необходимо применять различные методы воздействия па них. К методам воздействия на риски предприятий инвестиционно-строительной сферы, существующим в настоящее время и реально используемым в практической деятельности, можно отнести: страхование рисков; уклонение от рисков (избежание), передача рисков; распределение (разделение) и диверсификация рисков; объединение рисков; лимитирование рисков; резервирование средств (создание фондов), локализация и предупреждение рисков; компенсация рисков.

Страхование рассматривается в этой системе как один из инструментов управления рисками, но инструмент наиболее эффективный, позволяющий решать вопросы комплексной защиты не только строительного процесса, а всего строительно-инвестиционного проекта.

Страхование риска является одним из наиболее распространенных способов снижения его степени. Страхование – это особые экономические отношения. Для них обязательно наличие двух сторон: страховщика и страхователя. Страховщик создает за счет платежей различных страхователей единый денежный фонд (страховой или резервный фонд). Сущность страхования выражается в том, что стратег готов отказаться от части доходов для того, чтобы минимизировать риск, т. е. он готов заплатить определенную сумму (очевидно меньшую ожидаемого дохода) за снижение степени риска до нуля.

ГЛАВА 4.
СПОСОБЫ СНИЖЕНИЯ ФИНАНСОВОГО РИСКА

Высокая степень финансового риска проекта приводит к необходимости поиска путей ее искусственного снижения.

Снижение степени риска - это сокращение вероятности и объема потерь.

Для снижения степени риска применяются различные приемы. Наиболее распространенными являются:

- диверсификация;
- приобретение дополнительной информации о выборе и результатах;
- лимитирование;
- самострахование;
- страхование;
- страхование от валютных рисков;
- хеджирование;
- приобретение контроля над деятельностью в связанных областях и др.

Диверсификация представляет собой процесс распределения капитала между различными объектами вложения, которые непосредственно не связаны между собой.

Диверсификация позволяет избежать части риска при распределении капитала между разнообразными видами деятельности. Например, приобретение инвестором акций пяти разных акцио-нерных обществ вместо акций одного общества увеличивает вероятность получения им среднего дохода в пять раз и соответственно в пять раз снижает степень риска.

Диверсификация является наиболее обоснованным и относительно менее издержкоемким способом снижения степени финансового риска.

Диверсификация - это рассеивание инвестиционного риска. Однако она не может свести инвестиционный риск до нуля. Это связано с тем, что на предпринимательство и инвестиционную деятельность хозяйствующего субъекта оказывают влияние внешние факторы, которые не связаны с выбором конкретных объектов вложения капитала, и, следовательно, на них не влияет диверсификация.

Внешние факторы затрагивают весь финансовый рынок, т.е. они влияют на финансовую деятельность всех инвестиционных институтов, банков, финансовых компаний, а не на отдельные хозяйствующие субъекты. К внешним факторам относятся процессы, происходящие в экономике страны в целом, военные действия, гражданские волнения, инфляция и дефляция, изменение учетной ставки Банка России, изменение процентных ставок по депозитам, кредитам в коммерческих банках, и т.д. Риск, обусловленный этими процессами, нельзя уменьшить с помощью диверсификации.

Таким образом, риск состоит из двух частей: диверсифицируемого и недиверсифицируемого риска.

Диверсифицируемый риск, называемый еще несистематическим, может быть устранен путем его рассеивания, т.е. диверсификацией.

Недиверсифицируемый риск, называемый еще систематическим, не может быть уменьшен диверсификацией.

Причем исследования показывают, что расширение объектов вложения капитала, т.е. рассеивания риска, позволяет легко и значительно уменьшить объем риска. Поэтому основное внимание следует уделить уменьшению степени недиверсифицируемого риска. С этой целью зарубежная экономика разработала так называемую «портфельную теорию». Частью этой теории является модель увязки систематического риска и доходности ценных бумаг (Capital Asset Pricing Model – CAPM).

Информация играет важную роль в риск-менеджменте. Финансовому менеджеру часто приходится принимать рисковые решения, когда результаты вложения капитала не определены и основаны на ограниченной информации. Если бы у него была более полная информация, то он мог бы сделать более точный прогноз и снизить риск. Это делает информацию товаром, причем очень ценным.

Стоимость полной информации рассчитывается как разница между ожидаемой стоимостью какого-либо приобретения или вложения капитала, когда имеется полная информация, и ожидаемой стоимостью, когда информация неполная.

Лимитирование - это установление лимита, т.е. предельных сумм расходов, продажи, кредита и т.п. Лимитирование является важным приемом снижения степени риска и применяется банками при выдаче ссуд, при заключении договора на овердрафт и т.п. Хозяйствующими субъектами он применяется при продаже товаров в кредит, предоставлении займов, определении сумм вложения капитала и т.п.

Самострахование означает, что предприниматель предпочитает подстраховаться сам, чем покупать страховку в страховой компании. Тем самым он экономит на затратах капитала по страхованию. Самострахование представляет собой децентрализованную форму создания натуральных и страховых (резервных) фондов непосредственно в хозяйствующем субъекте, особенно в тех, чья де-ятельность подвержена риску.

Создание предпринимателем обособленного фонда возмещения возможных убытков в производственноторговом процессе выражает сущность самострахования. Основная задача самострахования заключается в оперативном преодолении временных затруднений финансово-коммерческой деятельности. В процессе самострахования создаются различные резервные и страховые фонды. Эти фонды в зависимости от цели назначения могут создаваться в натуральной или денежной форме. Так, фермеры и другие субъекты сельского хозяйства создают прежде всего натуральные страховые фонды: семенной, фуражный и др. Их создание вызвано вероятностью наступления неблагоприятных климатических и природных условий.

Резервные денежные фонды создаются прежде всего на случай покрытия непредвиденных расходов, кредиторской задолженности, расходов по ликвидации хозяйствующего субъекта. Создание их является обязательным для акционерных обществ. Акционерные общества и предприятия с участием иностранного капитала обязаны в законодательном порядке создавать резервный фонд в размере не менее 15% и не более 25% от уставного капитала. Акционерное общество зачисляет в резервный фонд также эмиссионный доход, т.е. сумму разницы между продажной и номинальной стоимостью акций, вырученной при их реализации по цене, превышающей номинальную стоимость. Эта сумма не подлежит какому-либо использованию или распределению, кроме случаев реализации акций по цене ниже номинальной стоимости. Резервный фонд акционерного общества используется для финансирования непредвиденных расходов, в том числе также на выплату процентов по облигациям и дивидендов по привилегированным акциям в случае недостаточности прибыли для этих целей. Хозяйствующие субъекты и граждане для страховой защиты своих имущественных интересов могут создавать общества взаимного страхования.

Наиболее важным и самым распространенным приемом снижения степени риска является страхование риска.

Сущность страхования выражается в том, что инвестор готов отказаться от части своих доходов, чтобы избежать риска, т.е. он готов заплатить за снижение степени риска до нуля.

Хеджирование (англ. *heaging* - ограждать) используется в банковской, биржевой и коммерческой практике для обозначения различных методов страхования валютных рисков. Так, в книге Долан Э. Дж. и др. «Деньги, банковское дело и денежно-кредитная политика» этому термину дается следующее определение: «Хеджирование - система заключения срочных контрактов и сделок, учитывающая вероятностные в будущем изменения обменных валютных курсов и преследующая цель избежать неблагоприятных последствий этих изменений». В отечественной литературе термин «хеджирование» стал применяться в более широком смысле как страхование рисков от неблагоприятных изменений цен на любые товарно-материальные ценности по контрактам и коммерческим операциям, предусматривающим поставки (продажи) товаров в будущих периодах.

Контракт, который служит для страховки от рисков изменения курсов (цен), носит название «хедж» (англ. *hedge* - изгородь, ограда). Хозяйствующий субъект, осуществляющий хеджирование, называется «хеджер». Существуют две операции хеджирования: хеджирование на повышение; хеджирование на понижение.

Хеджирование на повышение, или хеджирование покупкой, представляет собой биржевую операцию по покупке срочных контрактов или опционов. Хедж на повышение применяется в тех случаях, когда необходимо застраховаться от возможного повышения цен (курсов) в будущем. Он позволяет установить покупную цену намного раньше, чем был приобретен реальный товар. Предположим, что цена товара (курс валюты или ценных бумаг) через три месяца возрастет, а товар нужен будет именно через три месяца. Для компенсации потерь от предполагаемого роста цен необходимо купить сейчас по сегодняшней цене срочный контракт, связанный с этим товаром, и продать его через три месяца в тот момент, когда будет приобретаться товар. Поскольку цена на товар и на связанный с ним срочный контракт изменяется пропорционально в одном направлении, то купленный ранее контракт можно продать дороже почти на столько же, на сколько возрастет к этому времени цена товара. Таким образом, хеджер, осуществляющий хеджирование на повышение, страхует себя от возможного повышения цен в будущем.

Хеджирование на понижение, или хеджирование продажей - это биржевая операция с продажей срочного контракта. Хеджер, осуществляющий хеджирование на понижение, предполагает совершить в будущем продажу товара, и поэтому, продавая на бирже срочный контракт или опцион, он страхует себя от возможного снижения цен в будущем. Предположим, что цена товара (курс валюты, ценных бумаг) через три месяца снижается, а товар нужно будет продавать через три месяца. Для компенсации предполагаемых потерь от снижения цены хеджер продает срочный контракт сегодня по высокой цене, а при продаже своего товара через три месяца, когда цена на него упала, покупает такой же срочный контракт по снизившейся (почти настолько же) цене. Таким образом, хедж на понижение применяется в тех случаях, когда товар необходимо продать позднее.

Хеджер стремится снизить риск, вызванный неопределенностью цен на рынке, с помощью покупки или продажи срочных контрактов. Это дает возможность зафиксировать цену и сделать доходы или расходы более предсказуемыми. При этом риск, связанный с хеджированием, не исчезает. Его берут на себя спекулянты, т.е. предприниматели, идущие на определенный, заранее рассчитанный риск.

Спекулянты на рынке срочных контрактов играют большую роль. Принимая на себя риск в надежде на получение прибыли при игре на разнице цен, они выполняют роль стабилизатора цен. При покупке срочных контрактов на бирже спекулянт вносит гарантийный взнос, которым и определяется величина риска спекулянта. Если цена товара (курс валюты, ценных бумаг) снизилась, то спекулянт, купивший ранее контракт, теряет сумму, равную гарантийному взносу. Если цена товара возросла, то спекулянт возвращает себе сумму, равную гарантийному взносу, и получает дополнительный доход от разницы в ценах товара и купленного контракта.

ЗАКЛЮЧЕНИЕ

Актуальность темы рисков определяется процессами, происходящими в экономике России и направленными на реформирование всего хозяйственного механизма в связи с его переориентацией на рыночный тип хозяйствования. В подобной ситуации стремление экономического субъекта стабильно и успешно развиваться сталкивается с только формирующимся (и зачастую нефункционирующим) аппаратом управления деятельностью субъекта. Особенно ярко это проявляется в условиях непрерывных изменений, происходящих в политической и социально-экономической сферах жизни общества на предприятиях реального сектора. Это объясняется, с одной стороны, производственным характером их деятельности, а с другой — неразвитостью механизма снижения воздействия негативных факторов на состояние предприятий, что не позволяет им своевременно и адекватно реагировать на динамику процессов, определяющих социальную и экономическую ситуацию в стране.

На Западе, даже в относительно стабильных экономических условиях, субъекты хозяйствования уделяют пристальное внимание вопросам управления рисками. В то же время, в российской экономике, где факторы экономической нестабильности и без того усложняют вопросы эффективного управления предприятиями, проблемам анализа и управления всем комплексом рисков, возникающих в процессе их экономической деятельности, уделяется явно недостаточное внимание.

До недавнего времени подобный подход доминировал не только на предприятиях реального сектора экономики, но и в финансовокредитных организациях. Пристальное внимание вопросу управления рисками стало уделяться только после финансового кризиса, который отчетливо обозначил всю остроту данной проблемы в России.

Понятие «риск» известно с давних времен. В отечественной экономике исследование вопросов теории риска было в определенной степени востребовано лишь до конца 20-х годов 20 в. В дальнейшем, по мере становления социалистической системы хозяйствования усиливалась роль командно-административных методов управления. Все это в соединении с устранением рыночной мотивации экономики привело к отрицанию проблемы хозяйственного и социального риска. Отдельные же разработки по вопросам производственных, хозяйственных рисков не могли претендовать на право считаться научным направлением.

Таким образом, и в монетарном, и реальном секторах экономики проблема риска попросту игнорировалась.

Таким образом можно дать определение риску – это вероятность возникновения потерь, убытков, недопоступлений, планируемых доходов, прибыли.

Риск – это действие, совершаемое в надежде на счастливый исход по принципу «повезет - не повезет». Конечно риска можно избежать, т.е. просто уклониться от мероприятия, связанного с риском. Однако для предпринимателя избежание риска зачастую означает отказ от возможной прибыли. Хорошая поговорка гласит : «Кто не рискует, тот ничего не имеет».

Поэтому и существуют методы управления финансовыми рисками: упразднение, предотвращение потерь и контроль, страхование, поглощение. При выборе конкретного средства разрешения финансового риска инвестор должен исходить из следующих принципов:

- нельзя рисковать больше, чем это может позволить собственный капитал;
- нельзя рисковать многим ради малого;
- следует предугадывать последствия риска;

ЛИТЕРАТУРА

1.Бабин В.А. Практические аспекты оценки риска в бизнесе / В.А. Бабин // Управление риском. 2004. № 3. С. 18-20.
2.Багиев Г.Л. Маркетинг: Учебник / Г.Л. Багиев. В.М. Тарасевич, Х. Анн. М.: Экономика, 2001. 703 с.
3.Балабанов И.Т. Риск-менеджмент: Учебное пособие / И.Т. Балабанов. М.: ФиС, 1996. 192 с.
4.Бараненко С.П. Риски и управление ими в системе управления предприятием /С.П. Бараненко, В.В. Шеметов / Управление риском. 2004.№ 2. С. 32-35.
5.Бланк Н.А. Финансовый менеджмент: Учебныи курс / И.А. Бланк. К: Ника-Центр, 2002. 528 с.
6.Борисов А.Б. Большой экономический словарь / А.Б. Борисов. М.: Книжный мир, 2001.895 с.
7.Бусыги А.В. Предпринимательство. Основной курс: Учебник/ А.В. Бусыгин. М.: ИНФРА-М, 1998.608 с.
8.Буянов В.П. Анализ рисков в деятельности предприятия / В.П. Буянов // Вопросы экономики. 2004. № 8. С. 128-134.
9.Буянов В.П. Рискология (Управление рисками) /В.П. Буянов. М.: Экзамен, 2002. 620 с.
10.Викторов, М.Ю. , Л.А. Роботова. Проблемы эффективного управления рисками предприятий инвестиционно-строительного комплекса
11.Грабовый П.Г. Риски в современном бизнесе / П.Г. Грабовый. М.: АЛАНС, 1994. 286 с.
12.Гранатуров В.М. Экономический риск: сущность, методы измерения, пути снижения: Учебное пособие / В.М. Гранатуров. М.: ДиС, 2002. 160 с.
13.Грунин О.А. Экономическая безопасность организации: Учебное пособие / О.А. Грунин, С.О. Грунин. СПб.: Питер, 2002. 160 с.
14.Егорова Е.Е. Еще раз о сущности риска в системном подходе ... / Е.Е. Егорова // Управление риском. 2002. № 2. С.9-12.
15.Енгалычев О.В. Риск ... на завтра: предпосылки и этапы развития риск-менеджмента / О.В. Енгалычев // Российское предпринимательство. 2004. № 6. С. 44-47; № 7 С. 51-54.
16.Ишутин Р.В. Еще раз о предпринимательстве / Р.В. Ишутин // Управление риском. 2002. № 3. С. 10-12.
17.Казанцев А.К. Менеджмент в предпринимательстве: Учебное пособие / А.К. Казанцев, А.А. Крупанин. М.: ИНФРА-М, 2003. 230 с.
18.Коломина М.Е. Инвестиционные риски / М.Е. Коломина. М., 1993. 160 с.
19.Курчеева Г.И. Информационное обеспечение управления риском / Г.И. Курчеева, В.А. Хворостав // Управление риском. 2003. № 4. С. 15-22.
20.Лавров А.С Риски высокотехнологичных предприятий при трансформации отношений собственности / А.С. Лавров // Управление риском. 2004. № 3. С. 21-24.
21.Лисицына Е.В. Технология риск-менеджмента / Е.В. Лисицына, Г.С. Токаренко // Управление риском. 2004. № 1.с.11-14.
22.Манахова И. Риски потребителя / И. Манахова // Управление риском. 2004. № 1. С. 43-50.
23.Минат В.Н. Финансовая среда предпринимательства и предпринимательские риски. Учебное пособие/"Экзамен"/2006

24.Минат В. Н. Корпоративные конфликты как форма проявления взаимоотношений между участниками корпоративного управления в России / В.Н. Минат // Проблемы корпоративного права и управления в современной России. Рязань: РФ МАЭП, 2003. С. 15-17.
25.Минат В.Н. Развитие фирмы и управление рисками / В.Н. Минат // Современные проблемы гуманитарных и естественных наук: Сборник научных трудов. Рязань: РИУП, 2004. С.55-60.
26.Миронов М.Г. Финансовый менеджмент: Учебное пособие / М.Г. Миронов, Е.А. Замедлина, Е.В. Жарикова. М.: Экзамен, 2004. 224 с.
27.Моделирование рисковых ситуаций в бизнесе / Под ред. Б.А. Лагоши. М.: Фис, 2001. 224 с.
28.Мур А.И. Руководство по безопасности бизнеса: Практическое пособие по управлению рисками: Пер. с англ. / А.И. Мур. М.: Филинч, 1998. 376 с.
29.Ожегов С.и. Словарь русского языка / С.И. Ожегов.М.: Русский язык, 1978. 900 с.
30.Основы предпринимательской деятельности. Финансовый менеджмент / Под ред. В.М. Власовой. М.: ФиС, 2000. 180 с.
31.Паштова Л.Г.
32.Полоюва А,Н Угрозы, риски и неопределенности в бизнес-деятельности сложных организационных систем / А.Н. Полозова // Управление риском. 2004. № 1. С. 59-64.
33.Ревинский И.А. Предпринимательство: Учебное пособие / И.А. Ревинский. Новосибирск: НГПУ, 1996. 91 с.
34.Рэдхэд К. Управление финансовыми рисками / К. Рэдхэд. М.: Перспектива, 1996.646 с.
35.Смит А. Исследование о природе и причинах богатства народов / А. Смит. М.: Наука, 1992. 572 с.
36.Сычев А.Ю. История управления рисками / А.Ю. Сычев // Управление риском. 2003. № 4. С. 2-14.
37.Тэпман Л.Н. Риски в экономике: Учебное пособие / Л.Н. Тэпман / Под ред. В.А. Швандара. М.: ЮНИТИ-ДАНА, 2002.382 с.
38.Усов В.Н. Предупреждение неопределенности в управлении риском / В.Н. Усов // Управление риском. 2003. № 4. С.23-26.
39.Фадеев С. Не рисковать многим ради малого / С. Фадеев // РИСК. 2003. № 1. с. 59-64.
40.Финансовый менеджмент: теория и практика: Учебник / Под ред. Е.С. Стояновой. М.: Перспектива, 2002. 656 с.
41.Финансовый менеджмент: Учебное пособие / Под ред.Е.И. Шохина. М.: ИД ФБК·ПРЕСС, 2002. 408 с.
42.Черкасова В. Идентификация рисков / В. Черкасова // РИСК, 2004. № 2. С. 31-34.
43.Чупров С.В. Риск и управление устойчивостью промышленного предприятия / С.В. Чупров // Управление риском. 2004. № 2. С. 20-24.
44.Шинкаренко И.Э. Риск-менеджмент - философия управления рисками корпораций / И.Э. Шинкаренко, В.В. Храмов // Управление риском. 2004. № 2. С. 56-60.
45.Шутов П.В. Модель риска предпринимателя / П.В. Шутов // Управление риском. 2004. № 3. С. 56-61.