МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВПО УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: Конкурентная разведка и обеспечение экономической безопасности, как отдельные направления деятельности в структуре компании, работающей на международном рынке

Департамент магистратуры
Направление Экономика
Программа Конкурентная разведка в международном бизнесе
Кафедра мировой экономики

Дата защиты: 17.02.2015

Студент: Купцов Д.А.
Группа: ЗМ-КРМБ-12
Руководитель: Ющук Е.Л., профессор, к.э.н.
Нормоконтролер: Чупина Д.А., ст. преподаватель
Рецензент: Сухов А.Г., генеральный директор ЗАО «ЦЛЗ»

Екатеринбург
2015

СОДЕРЖАНИЕ

Введение 5
1 Определение конкурентной разведки и экономической безопасности, российские и международные особенности 8
1.1 Определение конкурентной разведки, используемые в России и за рубежом, история развития 8
1.2 Определение экономической безопасности и российская специфика организации и функционирования службы безопасности 26
1.3 Подходы используемые международными компаниями для обеспечения экономической безопасности 38
2 Организация и ведение конкурентной разведки. Российские и международные особенности 51
2.1 Правовые основы конкурентной разведки в России 51
2.2 Методические основы конкурентной разведки 60
2.3 Место конкурентной разведки в структуре международной компании 75
3 Информационные технологии, как современный инструментарий конкурентной разведки и службы безопасности, возможности взаимодействия 81
3.1 Информационные технологии, как инструментарий конкурентной разведки 81
3.2 Информационные технологии, как инструментарий службы безопасности 104
3.3 Формы взаимодействия конкурентной разведки и службы безопасности в международной компании 110
Заключение 117
Список использованных источников 119
Приложение А 131
Приложение Б 134
Приложение В 141

Приложение Г 145
Приложение Д..... 147

РЕФЕРАТ

В выпускной квалификационной работе 152 страницы, 3 главы, 3 таблицы, 22 рисунка, список использованных источников (121 источник), 5 приложений, введение и заключение.

Ключевые слова: конкурентная разведка, экономическая безопасность, методы конкурентной разведки, методы экономической безопасности, поиск информации, анализ информации, мониторинг, информационные технологии, взаимодействие, международный бизнес и др.

Цель выпускной квалификационной работы заключается в анализе форм взаимодействия применимых к конкурентной разведке и службе безопасности, их сильных и слабых сторон. Для обоснования оптимальной формы взаимодействия.

Для достижения поставленной цели были решены следующие задачи: установлены ключевые различия в подходах и методах используемых в конкурентной разведке и экономической безопасности, определена структура этих подразделений и информационные технологии применяемые ими.

В настоящей работе рассмотрены следующие аспекты:

- В первой главе определены различия в подходах, используемых в конкурентной разведке и экономической безопасности в России и за рубежом.
- Во второй главе рассматриваются правовые основы конкурентной разведки и её методические основы. Определяется место конкурентной разведки в структуре компании.
- В третьей главе рассмотрены особенности использования информационных технологий в конкурентной разведке и экономической безопасности, определяется оптимальная форма их взаимодействия.

ВВЕДЕНИЕ

Мировой экономический кризис 2008 года, а так же рецессия Российской экономики в конце 2014 года, привела к ужесточению конкуренции на всех уровнях хозяйствования. Бизнес был вынужден адаптироваться к новым условиям и оптимизировать свои процессы, став более осмотрительным и проактивным одновременно. Это связано с тем, что помимо экономических и политических факторов оказывающих давление на бизнес, в нестабильной обстановке возрастает и роль криминогенных факторов, несущих дополнительные риски финансовых потерь для компаний. Помимо возросших рисков, кризис дал и новые возможности для бизнеса, связанные с увеличением доли рынка через вытеснение и поглощение более слабых конкурентов. Так же появилась острая необходимость выхода на новые рынки с целью диверсификации бизнеса, поиска новых поставщиков и покупателей. Подходы и инструментарий способный помочь в решении подобных задач, мы рассмотрим в данной работе в рамках концепций конкурентной разведки (КР) и экономической безопасности (ЭБ).

Актуальность заявленной темы обусловлена необходимостью формализации и институционализации таких явлений как КР и ЭБ. Существует необходимость комплексного анализа существующих определений КР и ЭБ и их синонимов, а так же выработка сбалансированных определений.

Отсутствие ретроспективного анализа, развития конкурентной разведки за рубежом не позволяет выработать более чёткие подходы к её формированию в России. Некоторые Российские специалисты до сих пор противопоставляют методы ЭБ, методам КР, что связано с непониманием задач, которые в первую очередь призвана решать КР. На наш взгляд они должны работать в рамках единой системы, каждый по своему направлению. Нет однозначного понимания процесса внедрения КР в систему управления компанией. Всё это–ведёт к неоднозначному восприятию КР российскими руководителями. Исходя из чего, мы можем сделать вывод об актуальности

выбранной темы и наличии реальной потребности в решении упомянутых проблем.

Степень разработанности проблемы исследования. Теоретические основы КР и предпосылки к её развитию, заложены в работах: Д. Прескота, Б. Гилада, Я. П. Херринга, М. Портера, П. Д. Браянта, Т. Ф. Крола, Д. Колмана, П. Т. Гибонса, В. Плэтта внесших существенный вклад в исследование темы КР и механизмов её исследования.

В России вклад в разработку проблем КР внесли: Е.Л. Ющук, И.Ю. Нежданов, Роман Ромачёв, Г.Э. Лемке, А. И. Доронин, Ю.П. Воронов, Д. М. Антагулова, В.Л. Берсенёв, П. Кохно и др. Надо отметить, что, несмотря на недостаток соответствующей литературы, у Российских авторов встречаются оригинальные подходы и методы КР.

Тема ЭБ разрабатывалась в трудах западных авторов: Д. Бродера, Е. Такера, Д. Тёрнера, Д. Фэя, Ч. Сенневальда, Н. Коссовски, Т. Миллера, Д. Тусона, Т. Рилса.

А в России предмет ЭБ рассматривается в книгах следующих авторов: В. В. Шлыкова, Н. А. Лебедева, А. В. Сугловова, С. А. Хмелова, Е. А. Орлова, Г. А. Минаева, В. Новикова, В. М. Землянова. Стоит также отметить, что к вопросу экономической безопасности у российских авторов наблюдается более комплексный подход, в то время как зарубежные авторы стремятся разделять ЭБ на отдельные направления и дисциплины.

Объект исследования – компания, осуществляющая свою деятельность на Российском и международном рынке.

Предмет исследования – методы конкурентной разведки и экономической безопасности.

Цель исследования – сформировать модель взаимодействия экономической безопасности и конкурентной разведки в рамках единой системы.

Реализация поставленной цели потребовала постановки и решения следующих задач:

– дать определение КР и ЭБ, раскрыть их цели, задачи и методы;

– показать отличие задач и методов КР от задач и методов ЭБ в России и за рубежом;

– найти инструменты позволяющие эффективно объединить информационные потоки КР и ЭБ.

Источники фактических данных для написания работы включают в себя: аналитические и статистические материалы государственных органов и международных консалтинговых компаний, результаты социологических опросов представителей бизнеса и научного сообщества, законы и подзаконные акты федерального и областного уровней, а так же законодательные акты других государств. Кроме того анализировались профессиональные интернет ресурсы посвященные вопросам ЭБ и КР, как российского, так и зарубежного сегмента сети интернет.

Методологическая основа исследования. При решении поставленных задач применялись: метод контентного анализа, метод анализа основной причины, метод сравнительно-экономического анализа, результаты социологических опросов и экспертные оценки, а так же некоторые другие методы.

1 ОПРЕДЕЛЕНИЕ КОНКУРЕНТНОЙ РАЗВЕДКИ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ, РОССИЙСКИЕ И МЕЖДУНАРОДНЫЕ ОСОБЕННОСТИ

1.1 КОНКУРНТНАЯ РАЗВЕДКА, ОСОБЕННОСТИ ТРАКТОВКИ ПОНЯТИЯ В РОССИИ И ЗА РУБЕЖОМ, ИСТОРИЯ РАЗВИТИЯ

Что представляет из себя конкурентная разведка (КР) в России и на международном уровне? В чём принципиальные отличия в подходах КР и служб безопасности (СБ) в Российских и зарубежных компаниях? Ответить на этот не простые вопросы мы постараемся в этой главе, опираясь на работы общепризнанных российских и зарубежных авторов, а так же другие авторитетные источники.

Хотя международная терминология в области КР сформировалась уже давно, в России этот вопрос всё ещё остаётся открытым. Даже в научных кругах существуют разные взгляды на определение КР. В данной главе, используя научный подход и современные статистические инструменты мы покажем обоснованность нашего определения КР и укажем на недостатки других определений-синонимов.

Так же в этой главе будут даны определения терминологии используемой СБ и показаны основные подходы к работе и решаемым задачам. Что в свою очередь позволит нам разделить сферу деятельности КР и СБ и покажет их основные различия.

В параграфе рассмотрен взгляд на конкурентную разведку как составляющую часть бизнес разведки. Показаны истоки этого ошибочного, на наш взгляд, мнения. И дано чёткое определение бизнес разведки используемое в международной практике.

Дано определение бенчмаркинга и показаны его ключевые отличия от КР. Описан процесс его зарождения и показаны слабые стороны.

С помощью индекса Google Академии выделены наиболее цитируемые книги, содержащие определения терминов, являющихся синонимами КР. Проведён их анализ с сравнение с американскими первоисточниками. Сделаны выводы о целесообразности их применения.

Дано определение конкурентной разведки автором работы. Показаны основные проблемы современной КР в иностранных компаниях. Даны дополнительные разъяснения о том, чем является КР и показано на каких иерархических уровнях она действует.

Приведена хронология развития КР на международном уровне, а так же выделены учебные заведения и организации оказывающие наибольшее влияние на развитие КР в своём регионе.

Перед тем как определить назначение конкурентной разведки в современной компании, мы должны разобраться в её определении. Если на западе, термин конкурентная разведка имеет вполне чёткое и устоявшееся значение, то в России этот вопрос до конца не закрыт. Связана эта проблема отчасти с трудностями перевода термина competitive intelligence (CI), который в свою очередь состоит из двух слов: competitive – конкурентный, конкурентоспособный; intelligence – разведывательный, умственный. У нас в стране наибольшее распространение получил дословный перевод – конкурентная разведка, что в последствии трактовалась некоторыми авторами именно как разведывательная деятельность, направленная на конкурентов. Из-за такой спорной трактовки, это определение поставило конкурентную разведку в один ряд с промышленным шпионажем, что конечно же неверно. Методы промышленного шпионажа незаконны, в отличии от методов КР. На наш взгляд, более корректной будет трактовка определяющая конкурентную разведку, как интеллектуальную деятельность, направленную на анализ конкурентоспособности компании и конкурентной среды в целом.

До сих пор в российской литературе можно встретить термин деловая или бизнес разведка как синоним КР. А у некоторых авторов бизнес разведка

(business intelligence) является даже более комплексным явлением, включающем в себя конкурентную разведку (competitive intelligence) [23, с. 3, 4, 6.]. Это связано с тем, что в своё время существовало распространённое мнение о том, что первоначально на западе было два отдельных направления деятельности: деловая разведка изучала конкурентов во взаимосвязи с макроокружением организации, а конкурентная разведка концентрировалась на исследовании непосредственного окружения организации и конкурента. Получение новых знаний о развитии общества и взаимозависимости компонентов внешней среды привело к пониманию необходимости сквозного анализа внешней среды как единого целого, что повлекло за собой размытие границ между двумя понятиями [60, с. 22].

Нужно отметить, что в России это условное разделение прижилось на начальном этапе развития КР. Отчасти объяснить это явление можно на следующем примере. Так, проведенное обследование 33-х отечественных охранных структур, предоставляющих информационно-аналитические услуги, дало следующие результаты: проверкой деловых партнеров занимаются все 33 фирмы, изучением рынка - 21 фирма, сбором информации для переговоров - 31 фирма, установлением обстоятельств недобросовестной конкуренции - 3 фирмы, и только 2 фирмы проводят анализ деятельности конкурентов и деловых партнеров. С другой стороны, аналогичное обследование 45 фирм, предоставляющих консалтинговые услуги, показало, что 8 из них занимаются маркетинговыми исследованиями и изучением рынка и ни одна не проводит изучение деловых партнеров или конкурентов [56, с. 9].

Тяжёлая экономическая ситуация на тот момент вынуждала бизнес в России активно защищаться от внешних и внутренних угроз. Высокий спрос активно формировал рынок подобных услуг, что привлекало в отрасль большое количество отставных сотрудников силовых ведомств, с их связями, методами работы и опытом. Со временем функционал подобных структур стал расширяться в направлении информационно-аналитической работы, что

в некоторых случаях стали называть КР, хотя по своей сути это была всё та же работа по проверке контрагентов и выявлению других криминальных рисков с фокусом на исследование непосредственного окружения организации и конкурента. Разница в подходах применяемых специалистами, выходцами из силовых структур и специалистами, пришедшими в профессию из бизнеса и стала той разделительной чертой в умах российских авторов. Именно по этому, до сих пор в некоторых трудах можно встретить ошибочный взгляд на конкурентную разведку, как более узкий круг задач по сравнению с бизнес разведкой. Если же говорить про западный опыт, то на ранних этапах встречалось частое употребление термина бизнес-разведка (business intelligence) как синонима конкурентной разведки (competitive intelligence), но принципиальных различий в этих терминах зарубежные авторы не делали. Так же некоторые авторы отмечают, что использование термина BI было больше распространено в Европе, в особенности в Скандинавских странах [91, с. 7]. С развитием компьютерных технологий и интернета, за термином BI закрепилось свое собственное, отличное от CI значение. В российской практике это направление позже стали называть бизнес аналитикой.

Органы внутренних дел и контрразведывательные подразделения были не единственным источником притока специалистов в бизнес. В 1992 году из разведки было уволено по сокращению большое количество кадровых офицеров. В тот же период предприятия бывшего СССР оказались перед необходимостью конкурировать с зарубежными компаниями, которые в своём большинстве уже имели подразделения CI или пользовались услугами промышленного шпионажа. В этот же период родился проект "Магеллан" - организация разведывательных структур в крупных советских предприятиях. Поначалу офицеры были настроены на изучение конкурентов. Но всего через 1,5 месяца о конкурентах они знали практически всё, включая возможный потенциал их развития. Кроме того, выяснилось, что наибольшие риски бизнес несёт вовсе не от конкурентов, а из-за других факторов (примерно

90%), например, из-за принятия нового закона или из-за изменения моды на товар, или из-за появления новой технологии. Оказалось, что методы разведки в чистом виде не применимы в бизнесе, от каких-то приёмов нужно отказываться, какие-то перенимать у коммерсантов. Так родилась адаптированная для бизнеса версия государственной разведки. Эта версия разведки учитывала особенности информации, необходимой руководителю коммерческого предприятия, особенности добычи такой информации, особенности работы с источниками такой информации. Сами организаторы этого проекта дали ей название «коммерческая разведка» и организовали спец. курсы для сотрудников других коммерческих компаний.

Если же говорить про аббревиатуру BI (business intelligence), то она вошла в обиход еще в 1958 году. Тогда исследователь из IBM, Ханс Питер Лун объяснял BI как «возможность понимания связей между представленными фактами» [85]. Современная трактовка появилась в 1989 году. Будущий аналитик Gartner, Говард Дреснер определил BI как общее понятие, описывающее концепции и методы сбора, интеграции, анализа и представления данных, необходимых для принятия управленческих решений.

По мнению экспертов аналитического агентства IDC, эволюцию BI решений можно условно разделить на три волны. Первая длилась с 70-х до начала 90-х прошлого века. Системы того времени были нацелены на сбор информации и подготовку регламентированной отчетности. Вторая волна, окончившаяся в середине 2000-х, предоставила пользователям инструменты быстрого многомерного анализа на базе технологии OLAP (online analytical processing - аналитическая обработка в реальном времени), а также возможность самостоятельного создания нерегламентированной отчетности. Наконец, системы третьей волны, начавшейся в 2005-м, нацелены на расширение аудитории пользователей и делают акцент на прикладное применение BI решений. В тренде — предсказательная аналитика, интеллектуальный анализ данных (как родственное понятие data mining) и

«горизонтальные» продукты, ориентированные на унифицированные бизнес-задачи, возникающие на предприятиях любой отрасли [28].

Стоит отметить, что с момента появления термина BI, он неразрывно связан с IT технологиями и компьютерным анализом, источником данных для которого обычно выступала финансовая отчётность и статистика по компании. Например, Бенджамин Джилад так высказался по этому поводу: «Производители программного обеспечения (софтверные компании) продают решения, называемые «бизнес-разведка» (business intelligence), которые на самом деле не имеют отношения ни к бизнесу, ни к разведке, но лишь к структурированию массовой количественной информации в базах данных.» [24, с. 39].

Для того чтобы понять что из себя представляет современная BI, стоит посмотреть на исследование «Магический квадрат BI и аналитические платформы» агентства Gartner. Свои исследования, Gartner публикует с 2006 г., однако до сих пор под BI подразумевались способности ПО этого класса в области традиционных запросов и отчетов (описательные возможности). Тем временем, в течение нескольких прошлых лет, интерактивная диагностическая визуализация (interactive diagnostic visualization), как и прогнозирующий и предписывающий анализ (predictive and prescriptive analysis) становились все более понятными и важными для организаций. Таким образом, в 2013 г. исследователи Gartner пришли к выводу, что бизнес-аналитика претерпела к этому времени уже столько эволюционных изменений, что логичнее разделить прежде единый рынок инструментов этого класса на две части — «традиционный» BI и «продвинутый» (advanced) BI, соответственно построив два отдельных MQ для них [66]. В качестве успешного отечественного продукта в BI секторе, можно привести Пермскую компанию «Прогноз» и её систему Prognoz Platform. В 2014 году она укрепила свои позиции в рейтинге «Магический квадрант платформ бизнес-аналитики» компании Gartner, ведущего мирового консалтингового агентства в сфере ИТ.

Так же, стоит разобраться с тем, как соотносятся между собой понятия конкурентная разведка и бенчмаркинг. Под бенчмаркингом обычно понимают инструмент стратегического маркетинга, заключающийся в процессах поиска, получения, изучения и внедрения лучших практик успешного опыта ведения бизнеса, используемых в деятельности других компаний. Другими словами это аналитический процесс, который сравнивает процессы компании с компанией, процесс которой считают лучшим в своем классе в этой области. В результате анализа идентифицируются зоны "разрывов", которые и определяют те конкретные направления деятельности, в которых сравниваемая компания лучше или хуже вашей [77].

Поскольку конкурентная разведка позволяет получить необходимую информацию об анализируемых объектах с минимальными затратами времени и средств, можно сделать вывод что КР и бенчмаркинг зачастую используют схожие инструменты. Но утверждать что это одно и то же не верно, поскольку в задачи КР не входит сравнительный анализ внутренних бизнес процессов и разработка программ внедрения лучших практик.

В качестве одного из ярких примеров бенчмаркинга можно привести компанию Xerox, которая начиная с 1970-х годов столкнулась с серьезной конкуренцией со стороны японских производителей. Руководство компании повело себя неосмотрительно и не придало должного значения появлению на рынке японских копировальных аппаратов. Но уже к началу 1980-х стало ясно, что компания стремительно теряет свою долю рынка. Всего за 6 лет доля корпорация сократилась вдвое, а в 1982 году выяснилось, что всего за год доход снизился на 50%. Проанализировав японские продукты и их цены, компания с удивлением обнаружила, что японцы продают свои машины по ценам, равным себестоимости машин Xerox. Более тщательный анализ показал, что качество японских аппаратов ничуть не хуже, а расходы на их производство оказались втрое ниже, чем у Xerox. После всего этого корпорация занялась сбором информации на трех уровнях: региональном, национальном и глобальном. Основное внимание стало уделяться

бенчмаркингу. Причем анализ проводился не только компаний, работающих в секторе офисного оборудования, но и других компаний – лидеров сферы сервиса.

Практически всю необходимую информацию компании удавалось получать из открытых источников. После чего, собранную информацию распределяли по четырем основным категориям: компании, продукты, каналы и рынок. В корпорации появилась лаборатория оценки конкурентов, главная задача которой – перенять у конкурентов все лучшие бизнес практики. Производились закупки продукции конкурирующих компаний, после чего ее разбирали, подробно изучали и выпускали отчеты для инженеров. Это производилось не для того, чтобы им подражать, а для выявления сильных и слабых сторон конкурентов и последующего завоевания лидерства на рынке. Агентам по продажам и обслуживанию предоставили телефонную «горячую линию», по которой они сообщали оперативную информацию о конкурентах. Вся эта информация стала заноситься в национальную «конкурентную базу данных», к которой торговые представители компании могли подключить свои ноутбуки и воспользоваться нужной им информацией. В конце 1980-х годов, разработанная корпорацией Xerox программа была признана одной из лучших в США членами некоммерческого Американского центра производительности и качества, который выявлял и оценивал основные тенденции в области конкурентной разведки в то время.

Однако ирония истории Xerox заключается в том, что восстановив свои позиции на рынке копировальной техники на какое-то время (позже Canon потеснила глобальное лидерство Xerox), компания упустила из виду другие стратегические возможности, которые кардинально изменили рынок электронно-вычислительной техники навсегда. Речь идёт о подразделении компании Palo Alto Research Center (PARC) – научно-исследовательский центр, основанный по настоянию главного научного сотрудника фирмы, Джека Гольдмана в 1970 году. В 2002 году PARC выделен в отдельную

компанию (в собственности Xerox). На момент основания центра, Xerox потерял патент на ксерографию, и его менеджеры опасались потери части рынка в пользу японских концернов. Поэтому центр должен был заниматься инновационными разработками, которые бы позволили фирме и дальше оставаться лидером на рынке офисных технологий. В PARC были разработаны технологии, которые все ещё очень активно используются. Многие из них стали стандартом в компьютерном мире. Однако маркетинговая политика, направленная в первую очередь на рынок копировальной техники, привела к тому, что разработки центра принесли огромный успех другим фирмам, таким как Adobe, Apple и Microsoft.

В 1970-е годы в центре PARC были разработаны:

– Компьютерная мышь
– Лазерный принтер.
– Язык программирования Smalltalk, а с ним развитие концепции объектно-ориентированного программирования.
– Концепция ноутбука.
– Ethernet.
– Графический пользовательский интерфейс, впервые воплощённый в компьютере Xerox Alto (предшественник Apple Macintosh).
– Принцип WYSIWYG и первый WYSIWYG-ориентированный текстовый редактор Bravo (предшественник Microsoft Word).

Кроме термина бизнес-разведка, в России в качестве синонимов КР так же используются такие понятия: экономическая разведка, корпоративная разведка, аналитическая разведка, деловая разведка и д.р. С помощью сервиса Google Академия (scholar google), были определены самые цитируемые книги по этим терминам, из них были извлечены соответствующие определения. Сводная таблица с результатами представлена в приложении А.

Посмотрев на таблицу, мы сможем увидеть несколько интересных моментов. Во-первых, цитируемость книг по теме КР на западе значительно

выше. Во-вторых, термин "бизнес-разведка" (как синоним) цитируется в России чаще, чем термин "конкурентная разведка". В третьих, прочитав представленные выше определения, можно сделать вывод, что речь в них идёт об одном и том же явлении, на что прямо указывают большинство отечественных авторов. Кроме того, на наш взгляд, термин "корпоративная разведка", указывает лишь на организационную форму юридического лица в интересах которого осуществляется КР. Западные специалисты из сообщества SCIP так же указывают на то, что понятия корпоративная разведка, рыночная разведка, бизнес разведка и конкурентная разведка являются синонимами. [88]

Если говорить про аналитическую разведку, то она является частью КР и представляет из себя этап обработки собранной информации посредством аналитических методов. Хотя некоторые авторы ошибочно ставят знак равенства между аналитической разведкой и компьютерной разведкой (интернет-разведкой), которая представляет из себя поиск открытой информации в сети интернет, что в свою очередь является частью такого направления, как разведка по открытым источникам, которую свою очередь можно отнести к одному из направлений КР. В англоязычной литературе такой вид деятельности принято называть Open Sources Intelligence (OSINT) [13].

Таким образом, на наш взгляд, конкурентная разведка это – регулярный процесс сбора, верификации и анализа информации о конкурентной среде для выявления угроз и возможностей в целях принятия организацией оптимальных управленческих решений. Деятельность эта должна вестись строго в рамках закона и этики, с соблюдением необходимого уровня скрытности.

В связи с тем, что термин competitive intelligence (конкурентная разведка) получил международное признание, а используемые в России термины субституты не несут в себе дополнительного, чётко выраженного

смысла, считаем целесообразным использование термина "конкурентная разведка" как наиболее корректного.

Западные корпорации применяют КР в своей работе уже не один десяток лет. Сегодня, по оценкам американских источников, 100% компаний из списка "Fortune 100", 85% компаний из списка "Fortune 500" и до 50% американских компаний среднего размера в той или иной степени применяют КР [80].

Если же рассматривать процент компаний использующих КР в разрезе стран, то на 2008г. ситуация выглядела следующим образом.

Таблица 1 - Доля коммерческих фирм использующих конкурентную разведку [44 с. 28]

№	Страна	%
1	Япония	97-99
2	США	83
3	Великобритания	75
4	Германия	65-68
5	Франция	47-52
6	Испания	35
7	Россия	7-9
8	Украина	3-5
9	Казахстан	2,5-4

Но наличие службы конкурентной разведки ещё не гарантирует её эффективной работы. Так во многих западных компаниях не хватает хорошего анализа разведданных. Например, ответы на вопросы о прогнозировании конкурентных сдвигов, которые регулярно проводятся в Академии конкурентной разведки, показывают, что только 16% респондентов считали, что их компания обладает эффективным системным подходом к прогнозированию будущих ходов конкурентов. Целых 20% ответили, что их компании очень мало известно об их конкурентах. 30% заявили, что основным методом анализа конкурентов для них были

неформальные обсуждения. Около 22% обсуждали конкурентов один раз в год на ежегодном собрании без помощи сколь-нибудь структурированного анализа разведданных, а 13% сообщили, что их компания вообще не рассматривала конкурентов как стратегическую угрозу. Подавляющее большинство подразделений разведки, работающих сегодня в компаниях из списка Fortune-500, не имеют прямой связи с руководителями. Они не отчитываются перед руководителями на постоянной основе. Многие руководители даже не подозревают, что в недрах их организации существует отдел конкурентной разведки [24, с. 94, 124].

Деятельность КР условно можно разделить на 3 уровня, каждый из которых обладает собственным содержанием по широте спектра исследуемых проблем, их информационному охвату и глубине временной перспективы изучения:

– Стратегический уровень. Призван обеспечить возможности достижения компанией тех долгосрочных стратегических целей бизнеса, которые компания (или отдельный предприниматель) заранее наметила для воплощения в будущем.

– Оперативный уровень. Является – специальным видом расследований, как правило, это расследование либо уже прошедших, либо текущих событий/обстоятельств/фактов/и т.п. Непосредственными объектами изучения оперативного уровня исследований выступают внезапные и неожиданные события, которые уже реализовались и оказали свое негативное воздействие на бизнес и деятельность компании.

– Тактический уровень. Изучает риски и возможности рыночного характера, касающиеся текущего бизнеса компании. Исследования этого уровня призваны обеспечивать в информационно-аналитическом плане – конкурентоспособность и выживаемость компании в условиях реального времени, т.е. непосредственно в процессе повседневной деятельности компании.

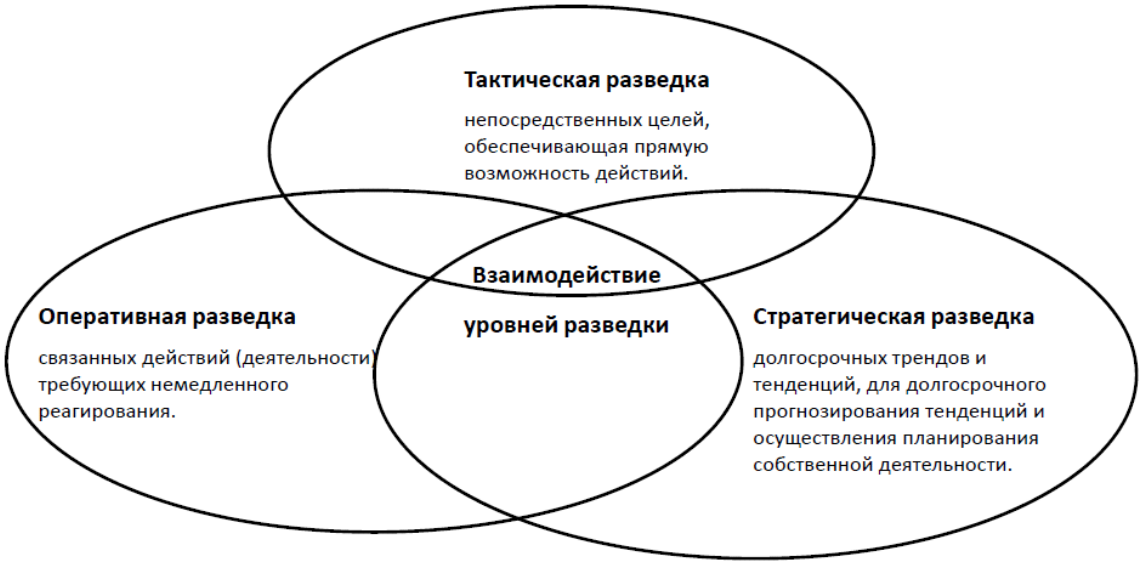

Рисунок 1 - Взаимодействие различных уровней КР [45]

Принято считать, что современная конкурентная разведка сформировалась во второй половине 20 века. Теоретические основы её были заложены в работах Фрэнсиса Агилара, Джона Прескота, Майкла Портера. По результатам исследования [76] уже в 1959 году вышла полноценная книга, имевшая название «Competitive Intelligence» [73], а в 1966 вышла книга «Business intelligence and espionage» [79]. В то время CI часто воспринималась как что-то родственное информационному шпионажу [75].

В конце 1970-х в США стали появляться компании, предлагающие различные варианты прикладного применения конкурентной разведки – в частности Fuld & Co., под руководством Леонарда Фулда и Washington Researchers, которую возглавляла Лейла Кайт. Они были пионерами в области предложения услуг конкурентной разведки корпоративным клиентам. В 1985 году Леонард Фулд опубликовал свою книгу "Разведка конкурента – как этим заняться, и как использовать" (Competitor Intelligence - How to Get it, How to Use it), которая стала первым бестселлером по тематике КР. В том же 1985 году Ян Херринг – отставник ЦРУ, возглавлявший там отдел технологического анализа, создал первое корпоративное подразделение конкурентной разведки в компании Моторола. В 1989 году его примеру последовал Бен Гилад, профессор стратегии в

университете Ратджерса (Rutgers University). Гилад создал подразделение конкурентной разведки в компании Келлог (Kellogg).

В 1986 в Америке было образовано первое сообщество профессионалов конкурентной разведки Society of Competitive Intelligence Professionals в дальнейшем переименованное в Strategic and Competitive Intelligence Professionals (SCIP), в задачи которой входило выработка единых стандартов работы, обучение специалистов, а так же популяризация методов КР. Кроме того, SCIP начал выпускать первое специализированное издание, по тематике КР - "Ревю Конкурентной Разведки" (Competitive Intelligence Review). По индексу цитирования основанного на репринтном издании, подготовленном к 10-летнему юбилею SCIP, в которое вошли лучшие статьи, опубликованные в "Ревю Конкурентной Разведки" за десять лет - с 1986 по 1996 год, можно узнать ключевые работы, оказавшие серьёзное влияние на дальнейшее развитие КР:

– Advances in Competitive Intelligence, Prescott, J. E., (1989) SCIP

– Global Perspectives on Competitive Intelligence, Prescott, J. E., and Gibbons, P. T., (1994) SCIP

– Competitive Advantage: Creating and Sustaining Superior Performance, Porter, M. E., (1985) New York: The Free Press

– The Business Intelligence System: A New Tool For Competitive Advantage, Gilad, B., and Gilad, T.,(1988)Amacom [60, с. 83]

Как раз книга «Система разведки в бизнесе: Новый инструмент для конкурентного превосходства» Б. Гилад и Т. Гилад, в которой подробно описана организационная модель правильно структурированного подразделения конкурентной разведки и стала тем толчком к институциолизации КР, как упорядоченного и формализованного вида деятельности. Эта книга была впоследствии широко адаптирована к практике большинством крупнейших компаний США, а затем также и ведущими европейскими компаниями – такими, как Shell и Novartis.

В 1996 году Леонард Фулд, Бен Гилад и Ян Херринг создали *Академию конкурентной разведки (Academy of Competitive Intelligence)* [105], и в 1999 году начали первую аккредитованную программу подготовки специалистов конкурентной разведки, предлагающую сертификат IACET (International Association for Continuing Education & Training). Сертифицированный курс CIP™ предлагает аккредитованную программу обучения от азов до продвинутого уровня знаний.

Но США является не единственной страной, в которой вопросу обучения КР уделяли внимание. Ниже мы рассмотрим институты и организации, чьи обучающие программы в области КР и смежных дисциплинах, оказывают значительное влияние на свой регион.

Австралийский институт профессиональных офицеров разведки (Australian Institute of Professional Intelligence Officers - AIPIO) [107]. Был образован в 1991 году на базе Австралийского института криминологии. Раз в год, проводит крупную отраслевую конференцию посвящённую разведке и смежным областям (National conference of the AIPIO). Основными направлениями обучения являются:

– Борьба с отмыванием денег (AML) и финансированием терроризма;
– Геопространственные информационные системы;
– Спортивная аналитика (договорные матчи);
– Аналитика активов;
– Кибербезопасность;
– Конкурентная разведка.

Военная экономическая школа в Париже (Ecole de Guerre Economique - EGE) [114]. Она была создана в 1997 году генералом Жаном Пишо Дюкло (Jean Pichot Duclos), как ответ на существующие потребности в сферах высшего образования и повышения квалификации в новых на то время областях. Обучение состоит из следующих основных модулей:

– Введение в экономическую разведку;

– Геоэкономика и глобализация;

– Управление информацией и производство знаний;

– Анализ и методология;

– Управление рисками;

– Развитие бизнеса и экономическая разведка;

– Операции влияния.

Компания Competia [110], является лидером в Канаде в программах обучения по направлению КР. Образована в 1998 году специалистом по конкурентной разведке Эстель Метьэ (Estelle Métayer). Вот примеры курсов 2014 года:

– Интернет как инструмент получения конкурентоспособности и разведки рынка;

– Продвинутые аналитические методы в стратегии;

– Социальные СМИ как источник понимания потребителя и конкурентная разведка.

Харьковский национальный университет радиоэлектроники (ХНУРЭ) [104]. В 2002 году усилиями кафедры социальной информатики, в классификатор профессий Украины введен новый подкласс 2433 и группа 2433.2 – «Профессионалы в области информации и информационные аналитики». Появилась новая специальность 8.18010015 «Консолидированная информация» с присвоением квалификации «Аналитик консолидированной информации».

Институт конкурентной разведки (The Institute for Competitive Intelligence - ICI) [120]. Основан в Германии в 2004 году, специалистом по конкурентной разведке Райнером Михаэли (Rainer Michaeli). Институт является одним из европейских лидеров по обучению КР, регулярно проводит курсы и рабочие секции, раз в год проводит крупную отраслевую конференцию, посвящённую конкурентной разведке (International Competitive Intelligence Conference). Производит обучение по собственным программам и выдаёт следующие сертификаты:

– Фундаментальный сертификат в конкурентной разведке (Fundamental Certificate in Competitive Intelligence - FCCI). Включает в себя следующие разделы: исследования в КР; Анализ в КР; конкурентная стратегия; менеджмент КР.

– Сертификат о мастерстве в конкурентной разведке (Certificate of Proficiency in Competitive Intelligence - CPCI). Углублённый курс по КР.

– Инженер конкурентной разведки (Competitive Intelligence Engineer - CIE). Курс для специалистов IT поддержки КР.

Институт конкурентной разведки и стратегического управления Амити (Amity Institute of Competitive Intelligence and Strategic Management) [106]. Образован в Индии в 2005 году и является единственным профильным учебным заведением по программам КР в своём регионе. Проводит полноценное обучение по программам бакалавриата, MBA и Ph.D в области конкурентной разведки.

Уральский государственный экономический университет (УрГЭУ) [103]. В 2011 году на кафедре мировой экономики была запущена первая в России магистерская программа по конкурентной разведке, направление 080100.68 - «Конкурентная разведка в международном бизнесе».

Кроме того активное содействие в развитии КР в России оказывают: *Сообщество практиков конкурентной разведки (СПКР)* [102] и *Российское общество профессионалов конкурентной разведки (РОПКР)* [99].

В настоящее время в США, практически в каждом крупном университете штата запущены программы и курсы по направлению КР. В других странах мира этот процент значительно меньше. [113]

Таким образом в данном параграфе были рассмотрены истоки мнения о том, что конкурентная разведка (competitive intelligence) является составной частью бизнес разведки (business intelligence). Исследование этого вопроса показало, что авторы использующие этот тезис ссылались на американскую практику организации этого вида деятельности, но при этом не привели никаких ссылок на зарубежные первоисточники в которых бы эта

информация содержалась. Кроме того изучение зарубежных источников показало, что на первоначальном этапе развития, эти два термина существовали как синонимы. В дальнейшем термин BI стал использоваться для определения конкретного направления анализа бизнес информации с использованием информационных систем.

Использование индекса Академии Google позволило выделить наиболее цитируемые книги содержащие определения: бизнес разведки, конкурентной разведки, корпоративной разведки, экономической разведки, аналитической разведки, деловой разведки (приложение А). Анализ этих определений показал, что все они по своей сути являются синонимами и вписываются в рамки определения Competitve Intelligence, которое появилось намного раньше.

Ретроспективный анализ даёт нам понять, что современная КР появилась на стыке новых экономических теорий, опыта гос. разведки и бизнес практик консалтинговых компаний. Так например, одно из лучших американских учебных заведений обучающих конкурентной разведке - The Academy of Competitive Intelligence (ACI). Его основателями являются: Леонард Фулд - бизнес консультант, автор множества книг по CI, основатель одного из первых консалтинговых агентсв предоставляющих услуги CI; Бенджамин Гилад - в своё время служил в Израильских вооружённых силах, работал офицером разведки в полиции Тель-Авива, бывший профессор стратегии, автор множества публикаций посвящённых CI; Ян Херринг - отставной офицер ЦРУ, один из пионеров организации подразделений CI в крупных корпорациях.

1.2 ОПРЕДЕЛЕНИЕ И РОССИЙСКАЯ СПЕЦИФИКА ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ СЛУЖБЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

В этом параграфе рассмотрены основные концепции экономической безопасности. Определены её цели и задачи. Дано определение автора этого вида деятельности.

Определены источники угроз и факторы, оказывающие наибольшее на них воздействие. Приведены результаты профильных исследований, показывающих основные риски с которыми работает служба безопасности (СБ).

Выделены основные мероприятия, проводимые контролирующими подразделениями. Приведены наиболее критичные индикаторы сопутствующие криминальным схемам.

Для того чтобы дать определение экономической безопасности и перейти к описанию существующих схем её организации, нужно разобраться в подходах и взглядах относительно её фокуса, которые существуют у российских специалистов. Потому что фокус службы экономической безопасности будет определять используемые в работе подходы и инструменты.

Первая концепция заключается в том, что экономическая безопасность организации рассматривается, прежде всего, с позиции защиты её от действия внешних факторов, степень отрицательного влияния которых выше влияния факторов внутренней финансово-хозяйственной среды предприятия.

Вторая концепция заключается в том, что экономическая безопасность организации сконцентрирована, по большей части, на внутренних факторах хозяйственной деятельности, работа с внешними факторами происходит по остаточному принципу или переложена на другие подразделения.

Третья концепция заключается в том, что под экономической безопасностью понимают состояние защищенности жизненно важных экономический интересов предприятия от всех видов угроз, как внешних, так и внутренних.

При этом экономическая безопасность в данном аспекте трактуется как комплекс мероприятий, направленных на обеспечение условий для предотвращения несанкционированного доступа к экономической тайне, сохранение конфиденциальности экономической информации, обеспечение сохранности материальных ценностей, проверке деловых партнеров и т.д. [67, с. 20]

Каждая из концепций имеет как свои плюсы, так и свои минусы, но третья, на наш взгляд, в наибольшей степени отвечает экономическим интересам организации как наиболее универсальная. Служба безопасности должна быть вариативна, другими словами, закрывать основные направления угроз и защищать каналы коммерческой информации и источники прибыли.

Таким образом, экономическая безопасность хозяйствующего субъекта - это состояние защищенности от внешних и внутренних угроз, с целью достижения конкурентных преимуществ и увеличения доли рынка.

В свою очередь, исходя их сложившейся практики, источники угроз можно сгруппировать по следующим восьми основным направлениям:

- Персонал;
- Контрагенты;
- Конкуренты;
- Криминал;
- Контролирующие органы;
- Государство;
- Стихийные и техногенные катастрофы;
- Собственник и его окружение.

Степень реализации угрозы называется риском, который напрямую зависит от трёх основных факторов, которые представлены на рисунке 2. Это: мотивация и давление внешних обстоятельств, возможность, самооправдание.

Рисунок 2 - «Треугольник мошенничества» Дональда Кресси [33]

Иногда вместо мотивирующего фактора на источник может воздействовать инициатор угроз. В качестве инициатора может выступить любой из источников, за исключением стихийных и техногенных катастроф. Например, криминал + персонал или конкурент + криминал, и т.д. В общем виде соподчинённость этих терминов приведена на рисунке 3.

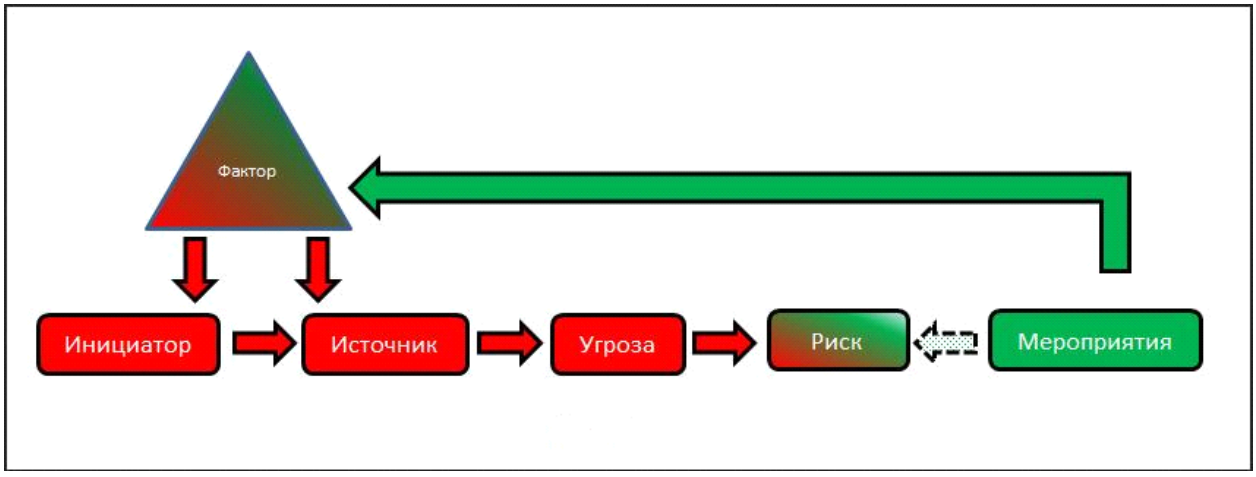

Рисунок 3 – Влияние факторов на степень риска [55]

Сущность экономической безопасности хозяйствующего субъекта реализуются в системе критериев и индикаторов, которая оценивает его состояние с точки зрения основных показателей финансово-хозяйственная деятельности. Такая система вырабатывается службой экономической безопасности для каждого хозяйствующего субъекта самостоятельно, так как специфика хозяйственной деятельности в каждой отрасли имеет свои особенности, что обуславливает разнообразное поведение хозяйствующих субъектов в той или иной ситуации [57, с. 6].

Система экономическая безопасности - это совокупность сил и средств, методов и мероприятий, направленных на защиту имущественных интересов организации.

К целям системы экономической безопасности относятся:

– предотвращение ущерба от деятельности (производственной, финансовой, управленческой и т.д.) и минимизации последствий такого ущерба, если он уже нанесен;

– защита имущества и ресурсов (финансовых, материальных, имущественных, интеллектуальных и т.д.), а так же выработка рекомендаций по их эффективному использованию;

– обеспечения нормального функционирования структурных подразделений, персонала, технических средств посредством своевременного выявления и профилактики опасностей и угроз;

– обеспечение безопасности взаимоотношений с партнерами и клиентами.

Из целей вытекают основные задачи системы экономической безопасности:

– анализ причин и факторов возникновения опасности угроз, с одной стороны и степени защищенности объектов безопасности, с другой;

– прогнозирование возможно ущерба или негативных последствий;

– мониторинг и устранение угроз хозяйствующему субъекту, его ресурсам и деятельности;

– формирование организационной структуры и разработка механизмов обеспечение безопасности, том числе отнесение информации других ресурсов различным уровням уязвимости и выработка, соответствующих мер защиты;

– расчет сил и средств, для оперативного реагирования на возникающие угрозы и появление негативных тенденций в деятельности хозяйствующего субъекта;

– минимизация последствий ущерба, нанесенного неправомерными действиями физических и юридических лиц, эффективное пресечение посягательств на деятельность, ресурсы и персонал хозяйствующего субъекта [57, с. 8].

Таким образом служба экономической безопасности (СЭБ) - это сервисная служба, обладающая контрольными функциями, входящая в общую службу безопасности (СБ), в которую так же входит служба охраны и подразделение обеспечивающее безопасность первых лиц компании. В её основные задачи входит: разработка и внедрение мероприятий по предупреждению рисков; выявление искажений в текущих бизнес-процессах и моментальное на них реагирование; проведение служебных расследований. СЭБ, прежде всего, должна работать на профилактику, то есть создавать такие условия, при которых реализация любых угроз была бы крайне затруднительна, если не невозможна. Конечно в задачи СЭБ входит и расследование случаев корпоративного мошенничества и воровства, но затраты (денежные, трудовые, временные) на их проведение значительно выше, чем затраты необходимые для профилактических мероприятий.

Кроме того, Российское государство обязывает собственников уделять вопросам организации системы внутреннего контроля должное внимание. Обратим внимание на вступивший в силу с 1 января 2013 г. Федеральный закон от 06.12.11 №402-ФЗ «О бухгалтерском учете». В статье 19 этого Закона прямо указано, что «экономический субъект обязан организовать и осуществлять внутренний контроль совершаемых фактов хозяйственной жизни».

Для того чтобы лучше понять какие задачи решает СЭБ и какое место она занимает среди других контролирующих подразделений организации, давайте обратимся к исследованию Российского отделения Ассоциации сертифицированных специалистов по расследованию хищений, результаты которого отражены на рисунке 4.

Рисунок 4 - Оценка актуальности угроз по мнению экспертов СЭБ [31, с. 6]

Как мы видим наибольшие угрозы, по мнению экспертов, представляют такие явления, как коммерческая коррупция и хищения со стороны высшего менеджмента. В меньшей степени угрозу представляют: коррупция в отношениях с регуляторами; хищения со стороны служащих и менеджеров среднего звена; информационная безопасность; отсутствие корпоративной культуры; недобросовестная конкурентная и промышленный шпионаж. Замыкает список угроза терроризма, что может быть актуально для крупных государственных предприятий, но маловероятно для большинства коммерческих организаций.

Результаты исследования ACFE очень сильно перекликаются с исследованием, проведённым PricewaterhouseCoopers в России. Состав экономических преступлений незначительно изменился в 2014 году по сравнению с 2011 годом. Основным видом экономических преступлений остается незаконное присвоение имущества (примерно 70% в России и по всему миру). При этом стоит отметить, что ситуация со взяточничеством и коррупцией выглядит совершенно иначе: за последние два года с этой проблемой в России столкнулись 58% респондентов по сравнению с 27% по

всему миру. Аналогичные показатели, полученные в 2011 году – 40% и 24% соответственно. Уровень мошенничества в сфере закупок в России (52%) также существенно превышает аналогичный показатель по всему миру (29%). В результате исследования также выяснилось, что портрет «внутреннего мошенника» меняется. Отмечается существенный рост количества экономических преступлений, совершенных представителями высшего и среднего управленческого звена. О таких преступлениях заявили 82% всех российских респондентов (в сравнении с 73% в 2011 году). Можно предположить, что мошенник, занимающий более высокую позицию, будет более информированным и будет использовать более изощренные методы совершения мошеннических действий, которые будет труднее обнаружить. В то же время мы полагаем, что риск мошенничества способны снизить сотрудники компании, отвечающие за предотвращение противоправных действий. При этом ни высота занимаемой должности, ни стаж работы в компании не являются безусловными факторами, способствующими снижению вероятности совершения преступления. Согласно результатам исследования, ситуация скорее противоположная [62, с. 11].

Если же говорить о бизнес процессах, то наиболее критичные из них в Российском бизнесе с точки зрения уровня потерь от хищений отражены на рисунке 5.

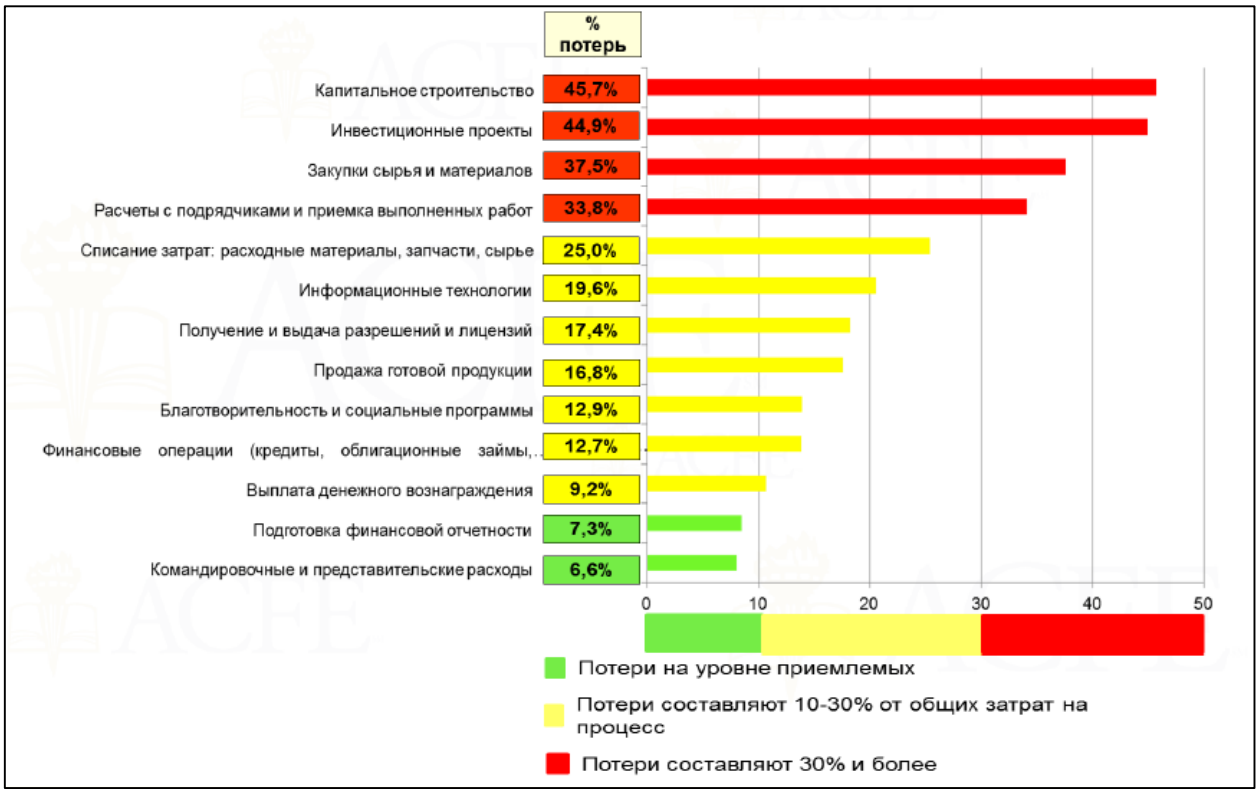

Рисунок 5 – Бизнес процессы подверженные риску хищений [31, с. 9]

После того как были обозначены угрозы и наиболее критичные процессы, давайте рассмотрим основные мероприятия проводимые подразделениями которые обладают контролирующими функциями, призванными бороться с этими угрозами. В структуре современной российской коммерческой организации можно выделить следующие службы, отвечающие за эти задачи: служба безопасности (СБ); контрольно-ревизионная служба (КРС); служба внутреннего аудита (СВА); юридическая служба (ЮС); служба управления персоналом (СУП). Основные этапы: предупреждение, выявление, реагирование, привлечение к ответственности и возмещение ущерба. Процесс управления рисками должен проводиться на регулярной основе и каждый из этапов должен прорабатываться с одинаковым вниманием. Распределение зон ответственности управления риском мошенничества представлено в таблице 2.

Таблица 2 - Распределение задач управления риском мошенничества [22, с. 9]

№ п.п.	Наименование этапа	Мероприятия	Ответственный исполнитель	Исполнители
1.	Предупреждение	Оценка риска мошенничества и злоупотреблений	СБ, КРС, СВА	СБ, КРС, СВА, ЮС
2.		Разработка и внедрение Кодекса корпоративной этики	СУП, СБ	СБ, СУП, ЮС
3.		Обеспечение безопасности при приеме на работу Обеспечение кадровой безопасности	СУП, СБ	СБ, СУП, ЮС
4.		Учебная подготовка персонала по вопросам предотвращения мошенничества	СБ, КРС, СВА, Подразделения	СБ, КРС, СВА, Подразделения
5.		Внедрение системы мотивации не предотвращение внутрикорпоративного мошенничества и минимизацию потерь	СУП	СУП, КРС, СВА, СБ, ЮС
6.	Выявление	Применение технических систем безопасности Применение системы физической охраны и контрольно-пропускного режима для целей контроля персонала	СБ	СБ
7.		Организация «горячих линий» и «телефонов доверия» для получения информации о фактах мошенничества и подготовки мошенничества	СБ	СБ
8.		Аудит и текущий контроль финансово-хозяйственной деятельности и движения активов	СБ, КРС, СВА	СБ, КРС, СВА, Подразделения
9.		Анализ данных, используемых в процессе мониторинга	СБ, КРС, СВА	СБ, КРС, СВА
10.	Реагирование	Процедуры проведения внутренних служебных расследований	СБ, КРС, СВА	СБ, КРС, СВА, СУП, подразделения
11.		Разработка процедур и мер дисциплинарного воздействия и системы материальной ответственности	СБ, СУП, ЮС	Подразделения
12.		Информирование сотрудников Компании о раскрытых фактах мошенничества в части касающейся	СУП	Подразделения
13.		Корректировка организации бизнес-процессов и организации системы контроля по результатам расследования фактов мошенничества	Управления	Система управления риском мошенничества
14.	Привлечение к ответственности и возмещение ущерба		СБ, ЮС	СБ, ЮС, СУП

Как мы видим, в большинстве случаев требуется взаимодействие различных контрольных служб и отделов, так как отдельно взятая служба не в состоянии перекрыть все риски хищения на различных стадиях бизнес процесса. Для того что бы это продемонстрировать, давайте рассмотрим в

качестве примера процесс закупок, как одного из процессов наиболее подверженных риску хищения.

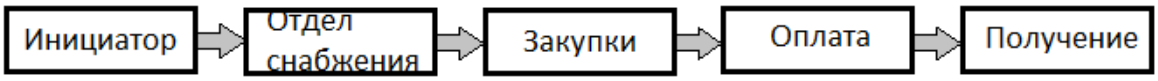

Рисунок 6 - Незащищённый процесс закупок

На рисунке 6 представлена упрощённая схема процесса закупок, без внедрения контролирующих мероприятий. На каждом из этапов возможны хищения и искажения выходной информации, что на практике практически всегда ведёт к финансовым потерям организации. Для того что бы избежать этих потерь и сделать процесс закупок максимально прозрачным, необходимо внедрять контролирующие мероприятия. Общая схема подобного защищённого процесса представлена ниже, на ней отражены этапы процесса закупок, на которых внедрён контроль со стороны соответствующих отделов и служб организации, что позволяет более эффективно предупреждать возможности хищений.

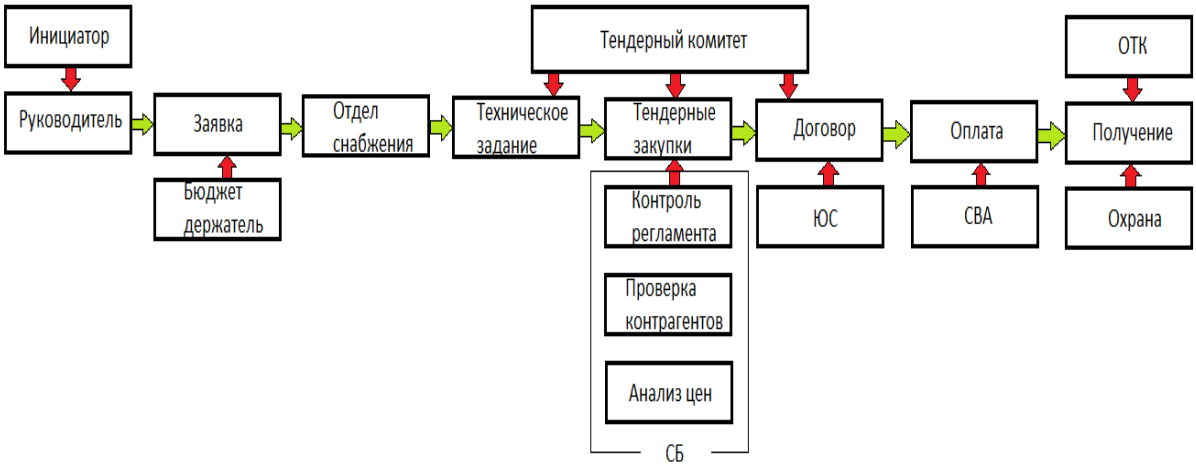

Рисунок 7 - Контролируемый процесс закупок

Общую схему защищённого процесса мы рассмотрели на рисунке 7. Далее мы перейдём к методике оценке рисков хищения. Этот процесс достаточно сложный и сильно варьируется в зависимости от отрасли и размера организации. В настоящее время известен ряд методов оценки рисков хищений. К сожалению, ни один из этих методов не стал широко

применимым на практике, так как все они основываются на субъективной оценке степени риска аудитором. Это означает, что применяя одну и ту же методику к одному и тому же объекту исследования, разные аудиторы могут прийти к разным оценкам риска хищений, в зависимости от своего профессионального опыта и толерантности к риску. Поэтому задача создания методики оценки рисков, которая зависела бы от суждения аудитора в меньшей степени, остаётся актуальной [32, с. 7].

Далее будет рассмотрена методика, разработанная Российским отделением ACFE при поддержке Эрнст энд Янг (СНГ), она основана на выявлении и оценке индикаторов хищений. Метод выявления скрываемого факта по его косвенным проявлениям (в нашем случае, «индикаторам») часто используется аналитиками в разных сферах деятельности, например, в аналитике и в разведке.

Индикатор хищения – это факт, который не скрывается или легко устанавливается и который обычно сопутствует хищению, но не является его прямым доказательством. По смыслу, индикатор близок к косвенному доказательству преступления, то есть к факту, который кроме криминального объяснения, может иметь другие, некриминальные версии.

Например, образ жизни сотрудника, не соответствующий его доходам, является типичным индикатором хищения, однако не может быть доказательством, так как теоретически может существовать множество некриминальных объяснений того, откуда у данного сотрудника деньги (наследство, выигрыш в лотерее и т.д.). Существует достаточно большое количество индикаторов, которые используются профессионалами на практике для выявления хищений. Наличие одного и более индикаторов рисков хищений является для профессионала исходной информацией для углублённого изучения процесса на предмет наличия хищений. Наличие одновременно нескольких индикаторов свидетельствует о повышенном риске хищений.

В приложении Б представлена таблица Б.1 из 48 индикаторов хищений расположенных в порядке убывания их значимости, сформированная путём экспертного опроса специалистов экономической безопасности.

Количество и приоритет индикаторов хищения должна определять СЭБ в зависимости от специфики организации самого бизнеса. После выявления индикаторов хищения, следующим этапом является внутреннее расследование мошенничества. Общая последовательность действий на этом этапе представлена на рисунке 8.

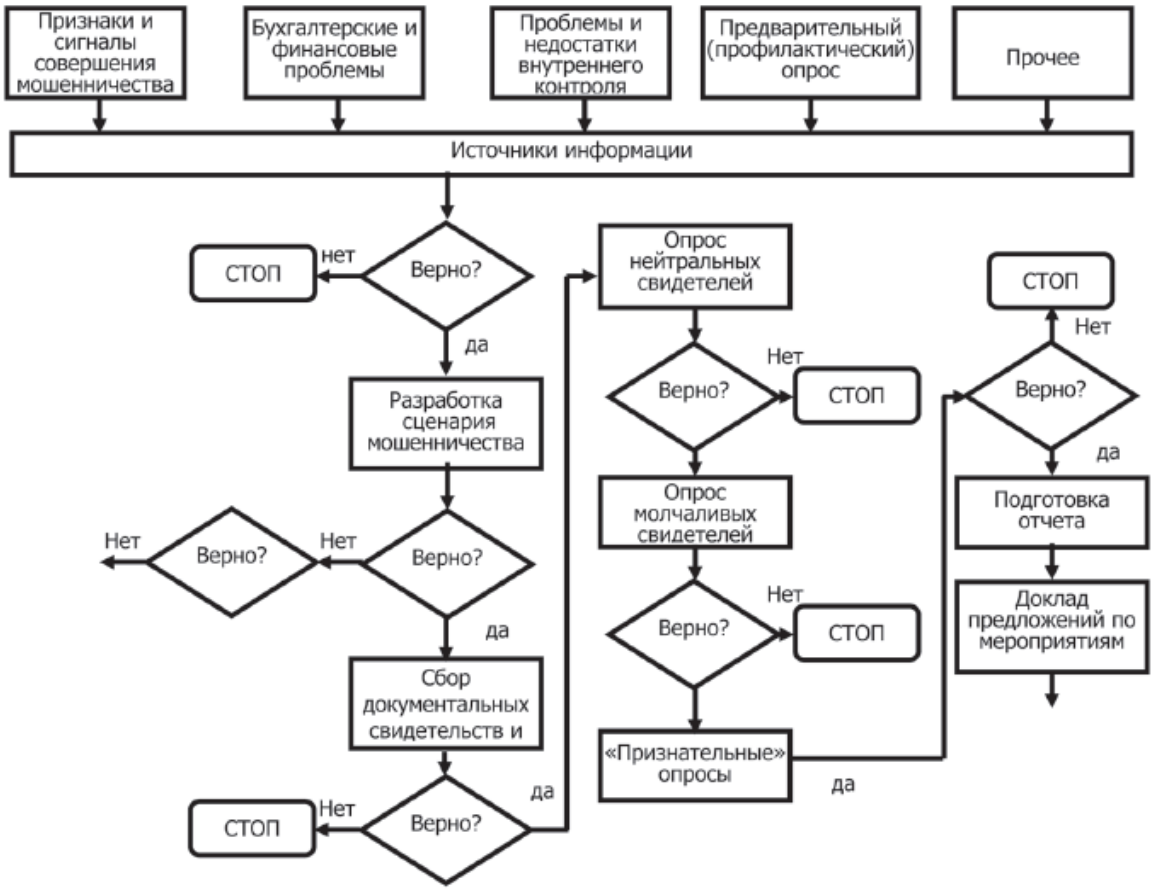

Рисунок 8 - Алгоритм выявления и расследования внутрикорпоративного мошенничества [22, с. 10]

В рамках уголовного кодекса РФ, большинство экономических преступлений против хозяйствующего субъекта совершается в рамках следующих статей:

– Статья 158 УК, кража. В уголовном законодательстве определяется как "тайное хищение чужого имущества".

– Статья 159 УК, мошенничество. Сущность мошенничества заключается в завладении чужим имуществом путём обмана или путём злоупотребления доверием.

– Статья 160 УК, присвоение или растрата. Данный вид хищений - это осуществляемое в форме присвоения или растраты противоправное изъятие имущества или денежных средств из ведения собственника, с целью владения и распоряжения ими как собственными. В отличии от кражи, мошенничества, разбоя и других преступных посягательств на имущество, присвоение или растрату может совершить лишь тот, в чьём ведении находятся товарно-материальные ценности.

На основе представленного материала можно сделать вывод, что СБ имеет дело с рисками криминального характера и наибольшую угрозу представляют источники находящиеся внутри организации. Своевременное выявление признаков сопутствующих преступлению, способствует минимизации экономического ущерба. Именно решение подобных задач и определяет инструментарий используемый СБ, которые будут рассмотрены в третьей главе.

1.3 ПОДХОДЫ ИСПОЛЬЗУЕМЫЕ МЕЖДУНАРОДНЫМИ КОМПАНИЯМИ ДЛЯ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Международные подходы и терминология несколько отличается от сложившейся Российской практики. Ниже мы рассмотрим законодательные акты и подходы, которые оказывают наибольшее влияние на формирование современной практики обеспечения экономической безопасности в транснациональных компаниях. Будут описаны следующие подходы: гавернанс, риск менеджмент, комплаенс, дью дилидженс.

Большую роль на международном уровне играет «Группа разработки финансовых мер борьбы с отмыванием денег» (Financial Action Task Force on Money Laundering — FATF). Организация была создана в 1989 году по

решению стран «Большой семерки» и является основным международным институтом, занимающимся разработкой и внедрением международных стандартов в сфере противодействия отмыванию преступных доходов и финансированию терроризма (ПОД/ФТ), а также осуществляет оценки соответствия национальных систем ПОД/ФТ по этим стандартам. Россия является членом этой организации с 2003 года, а так же является членом Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма (EAG). Основным инструментом ФАТФ в реализации своего предназначения являются 40 рекомендаций в сфере ПОД/ФТ, которые подвергаются ревизии в среднем один раз в пять лет, самой свежей на данный момент является редакция 2012 года.

Если же говорить о международных конвенциях регулирующих вопросы борьбы со взяточничеством, то наиболее влиятельной будет «Конвенция о борьбе с подкупом иностранных должностных лиц при осуществлении международных коммерческих сделок» (The OECD Anti-Bribery Convention). На текущий момент к конвенции присоединилось более 40 стран, включая Россию. Страны, подписавшие конвенцию, обязаны ввести в действие законодательство, которое предусматривает уголовную ответственность за акт подкуп иностранного публичного должностного лица [87].

Большое влияние на международную практику оказывает Американский «Закон о коррупции за рубежом» (Foreign Corrupt Practices Act - FCPA) принятый в 1977 году. Закон регулирует факты предложения, обещания, предоставления материальных и нематериальных благ любому иностранному должностному лицу, а также кандидату на политический пост и политической партии с целью получения выгоды. В американском законодательстве, под "должностным лицом" понимается не только государственные служащие и лица, осуществляющие публичные функции, но и сотрудники государственных учреждений и предприятий.

Внесенные в 1998 году изменения, расширили сферу действия закона, таким образом, под юрисдикцию подпадают любые физические лица и компании, вне зависимости от национальной принадлежности. Под действие Закона неамериканская компания подпадает в случае, если она ведет свою деятельность в Соединенных Штатах, если акции компании котируются на американской бирже, а также, если она действует от имени американской компании. Виновные во взяточничестве несут гражданско-правовую и уголовную ответственность. Один из ярких примеров его применения, это дело о подкупе должностных лиц компанией Simens для получения выгодных контрактов на поставку медицинского оборудования для Китая и Индонезии, телекоммуникационного оборудования для армий Венгрии и Норвегии, контракта на строительство ядерной электростанции в Сербии и еще в ряде преступлений. Напомним, что Simens является Германской компанией, но её акции торгуются с 2001 года на Нью-Йоркской фондовой бирже. Общие издержки компании, связанные с этим делом составили порядка 1,5 млрд. евро [17].

Так же большое влияние на международную практику оказывают нормы Британского законодательства. «Закон о мошенничестве» (Fraud act) от 2006 года, формулировки которого получили международно-правовое признание, а так же «Закон о взяточничестве» (Bribery Act) от 2010 года, нормы которого имеют почти универсальную юрисдикцию, что позволяет преследовать частных лиц или компании со ссылками на Соединенное Королевство, вне зависимости от того, где произошло преступление. Основными критериями для попадания под действие этого закона, являются признаки видимого бизнес присутствия в Великобритании. К этим признакам относится:

– Ведение бизнеса, в т.ч. оказание услуг, через представительство или дочернюю компанию в Великобритании;
– Владение активами в Великобритании;

– Подписание контрактов в Великобритании или контрактов, имеющих отношение к Великобритании;

– Ведение коммерческих переговоров на территории Великобритании для заключения контрактов;

– Импорт/экспорт товаров и/или услуг в/из Великобритании;

– Реклама и/или продвижение товаров и услуг в Великобритании (в том числе через Интернет);

– Уплата налогов, таможенных пошлин, лицензионных и патентных платежей в Великобритании или имеющих отношение к Великобритании.

За последние несколько лет работы отдел по борьбе с крупным мошенничеством в Великобритании (Serious Fraud Office - SFO) обеспечил эффективное влияние на бизнес еще до вступления в силу закона:

– Innospec - штраф $40 млн. и отстранение от участия в тендерах по всему миру;

– Mabey&Johson - штраф более £ 6 млн. и отстранение от участия в тендерах в Европе;

– Alstom - арест трех директоров в связи с предложением взятки за рубежом при совместном с швейцарскими властями расследовании [29].

Так же стоит отметить, что стандарт системы управления борьбы со взяточничеством, Британского института стандартов (British standards institution - BSI) - BS 10500:2011, является базой для разработки международного стандарта ISO/NP 37001 Anti-bribery management systems [74].

Во всём мире, а в США в наибольшей степени, общепринятой практикой в сфере внутреннего контроля деятельности корпораций является подход GRC (governance, risk management, compliance). Популярность этого подхода в Америке значительно возросла после принятия Закона Сарбейнза — Оксли (Sarbanes-Oxley Act - SOX) в 2002 г., так же известного

как «Реформа бухгалтерского учёта открытых акционерных обществ и закон о защите прав инвесторов». В нём рассматриваются вопросы независимости аудиторов, корпоративной ответственности, полной финансовой прозрачности, конфликта интересов, корпоративной финансовой отчетности и др. Но ключевой момент заключается в том, что топ менеджеры теперь несут персональную ответственность за достоверность предоставляемой финансовой информации.

Подход GRC состоит из трёх основных направлений, которые мы сейчас разберём:

Гавернанс (англ. *governance* – управление, руководство, власть.) – система взаимодействия между акционерами и руководством компании (акционерного общества, корпорации), включая её совет директоров, а также с другими заинтересованными лицами, с помощью которой реализуются права акционеров; комплекс механизмов, позволяющих акционерам (инвесторам) контролировать деятельность руководителей компании и разрешать возникающие проблемы с прочими группами влияния.

“Корпоративное управление отличается от менеджмента. Менеджмент управляет предприятием. Правление или руководящий орган удостоверяется, что этим управляют хорошо и в правильном направлении”

Менеджмент может быть представлен как иерархия: треугольник в рисунке 9. Совет директоров или другой руководящий орган наложены на него в виде круга. Его участники не формируют иерархию. У всех есть равные права и обязанности.

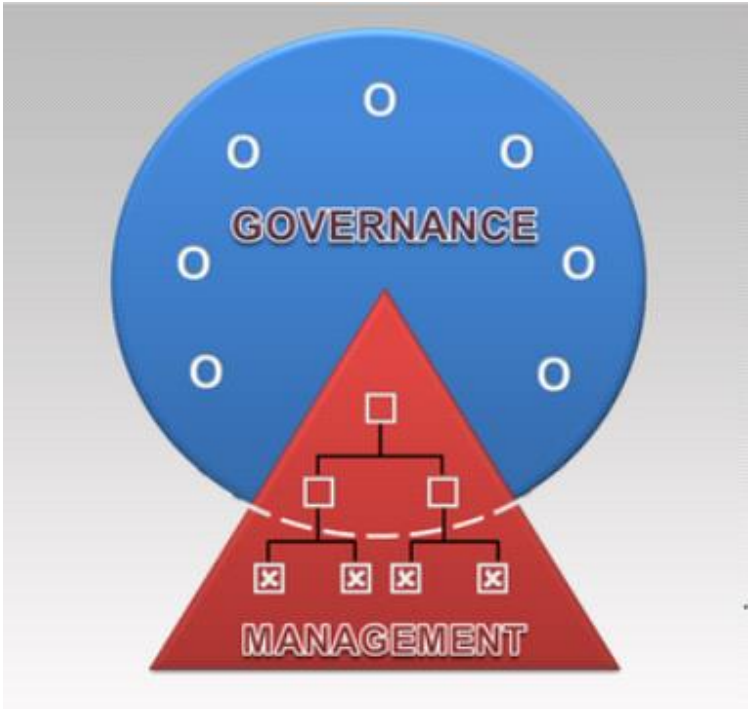

Рисунок 9 - Корпоративное управление и менеджмент [90]

Риск-менеджмент (англ. *risk management* – управление риском) - организации всех типов и размеров сталкиваются с внутренними и внешними факторами и воздействиями, из-за которых становится невозможно определить, каким образом и когда они достигнут своих целей. Влияние неопределенности на цели организации определяется как “риск”. Любая деятельность организации связана с риском. Организации управляют риском посредством его идентификации, анализа и последующего решения, следует ли его подвергнуть обработке с целью удовлетворения критериев риска. Риски, которым подвержена организация, могут возникать в силу как внутренних, так и внешних факторов. Нижеприведенная диаграмма показывает ключевые риски, возникающие в силу внутренних и внешних факторов. Риски могут быть дифференцированы по следующим категориям – стратегические, финансовые, операционные опасности и опасности, как показано на рисунке 10.

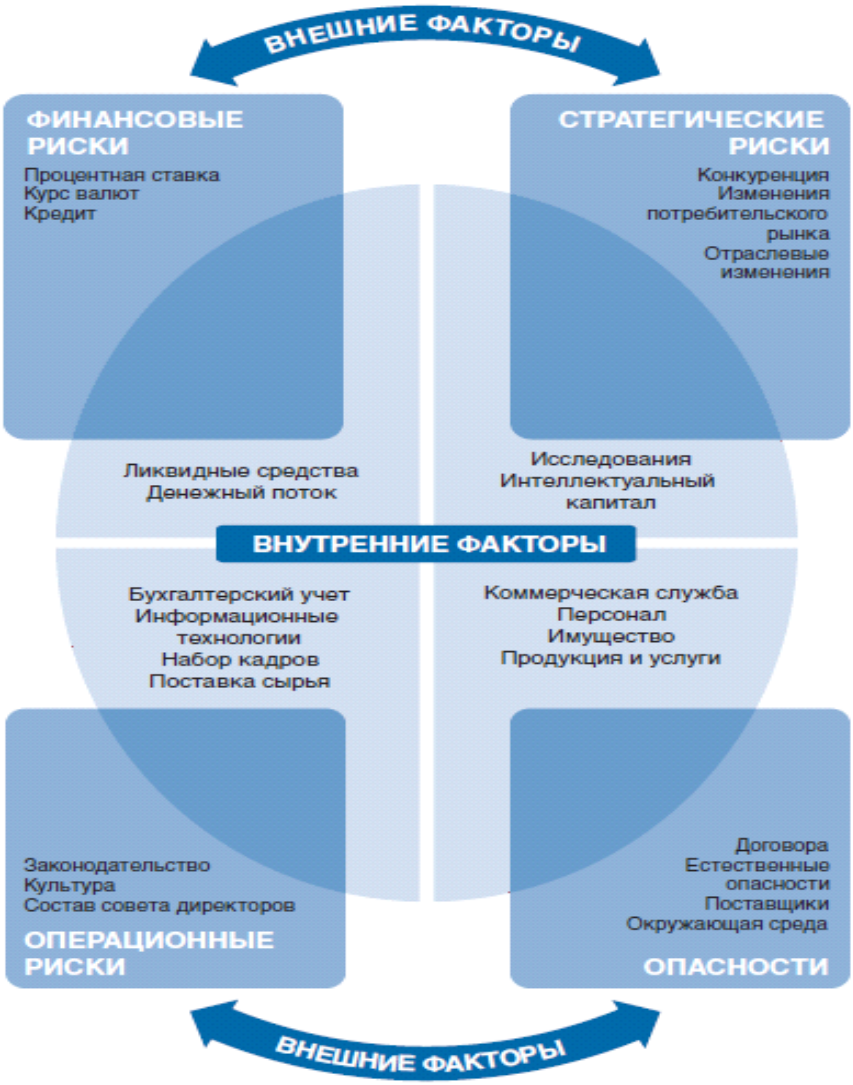

Рисунок 10 - Внутренние и внешние факторы риска [64, с. 4]

Менеджмент риска (риск-менеджмент) - скоординированные действия по управлению организацией с учетом риска.

Структура менеджмента риска – взаимосвязанные элементы, которые обеспечивают реализацию принципов и организационные меры, применяемые при проектировании, разработке, внедрении, мониторинге, анализе и постоянном улучшении менеджмента риска организации. Международным стандартом в области риск менеджмента является ISO 3100-2010, ISO/IEC 31010 и ISO Guide 73:2009. Его российским вариантом является ГОСТ Р ИСО / МЭК 31010-2011, а так же ГОСТ Р 51897-2011 / Руководство ИСО 73:2009.

В общем виде на рисунке 11 представлен процесс риск-менеджмента, который состоит из следующих этапов: 1) Взаимодействие и консультирование; 2) Определение контекста риск-менеджмента; 3) Идентификация рисков; 4) Анализ рисков; 5) Оценка рисков; 6) Принятие и реализация рискового решения; 7) Мониторинг и анализ.

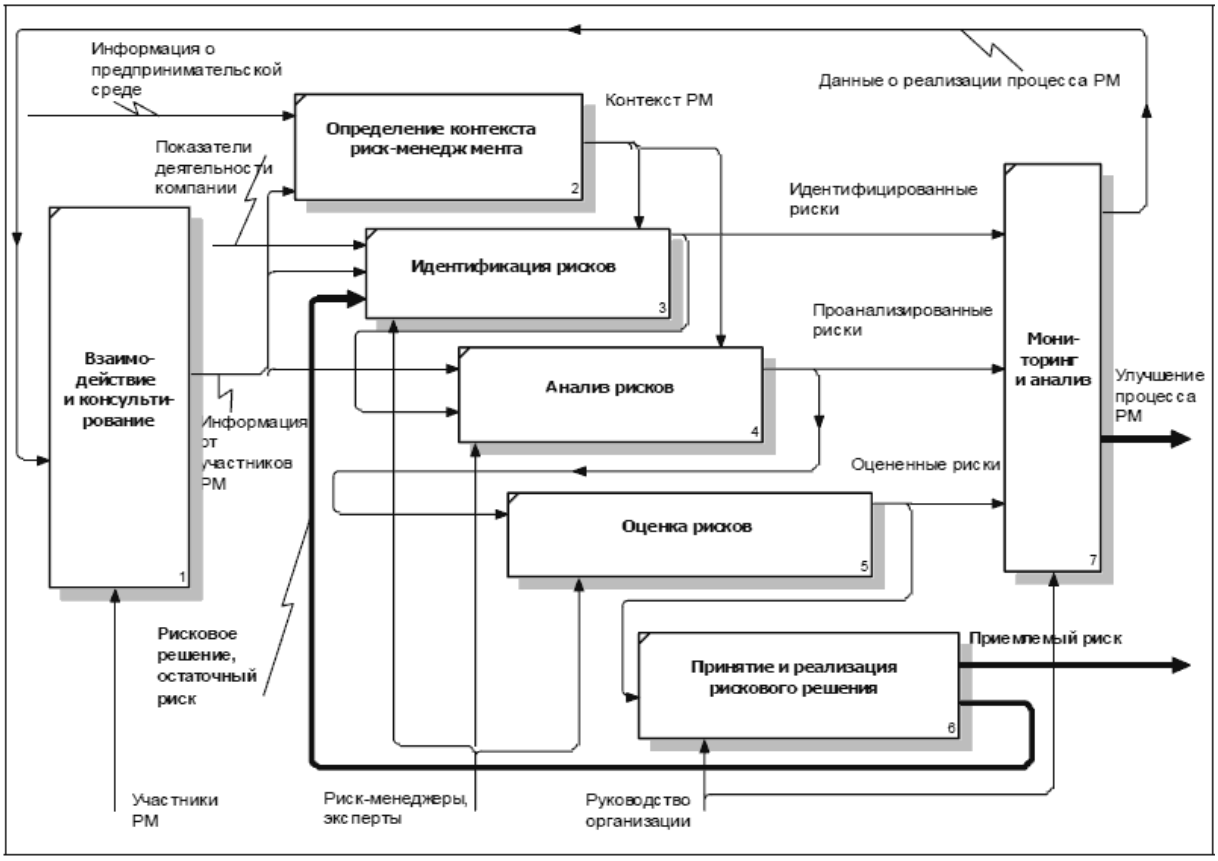

Рисунок 11 - Взаимодействие стадий процесса риск-менеджмента [47]

Комплаенс (англ. *compliance* — согласие, соответствие; происходит от глагола *to comply* — соответствовать) - соблюдение законов, правил и стандартов регулирующих органов и в целом охватывает ряд таких вопросов, как надлежащее исполнение стандартов рыночного поведения, управление конфликтом интересов, справедливое обращение с клиентами и выполнение их пожеланий. Обычно они включают в себя определенные области вроде противодействия легализации доходов, полученных преступным путем, и финансированию терроризма и могут охватывать законы налогового

характера, уместные для банковских продуктов. Комплаенс (в широком смысле) - это процесс управления комплаенс-риском [51].

Комплаенс-риски – риски упущенной прибыли или убытков вследствие возникновения конфликтов интересов и вследствие несоответствия действий сотрудников внутренним и внешним нормативным документам.

Конфликт интересов – противоречие между имущественными и иными интересами субъектов финансового рынка, в результате которого действие (или бездействие) одной стороны причиняет убытки (или приводит к уменьшению прибыли) другой стороне или влечет иные неблагоприятные последствия для другой стороны.

Международным стандартом для управления системой комплаенс контроля является - ISO/DIS 19600, который в данный момент находится в разработке. [83]

Основные объекты комплаенс контроля:

– Конфликты: сотрудник-Корпорация, клиент-Корпорация;
– Торговля на личную позицию (Personal attitude dealing - PAD);
– Критерии «отмывочной» деятельности и финансирования терроризма (Anti money laundering / Combating the Financing of Terrorism - AML / CFT);
– Списки стран находящихся под санкциями, списки политически значимых лиц (Countries under sanctions / Politically exposed persons – CUS / PEP`s)
– Соблюдение международного законодательства в области борьбы со взяточничеством (FCPA, UK BA и др.)
– Соблюдение принципа «Знай своего клиента» (Know your customer - KYC);

Важность подобного контроля не стоит недооценивать, в качестве яркого примера можно привести обвинение США в адрес французского банка BNP Paribas в том, что он с 2002 по 2009 гг. совершил сделок на сумму $30 млрд. в нарушение санкций США, введенных против Ирана,

Судана и Кубы. Сумма предполагаемого штрафа составляет $10 млрд., хотя по закону США банк могут обязать выплатить сумму, вдвое превышающую объем незаконных транзакций. Так же обсуждается возможность того, что банк в течение года не сможет оказывать клиентам услуги долларового клиринга. Речь идет об обслуживании клиентских платежей, при которых необходимо конвертировать валюты в доллары. Стоит отметить, что действия BNP Paribas не могли стать основанием для аналогичных расследований в Европе, так как у Евросоюза вообще нет санкций против Кубы, а санкции против Ирана и Судана не такие жесткие, как у США.

В приложении В, представлена таблица В.1, в которой для различных сфер деятельности компании выделены зоны комплаенс-риска и необходимые меры контроля.

В системе обеспечения корпоративной безопасности используется процедура Due Diligence (Дью Дилидженс), этот термин часто переводят как «должная осмотрительность», подразумевая всестороннее исследование достоверности предоставляемой информации.

Считается, что этот термин был введен в оборот финансистами в 1930-е гг. в США. Первоначально он обозначал процедуру раскрытия информации брокером перед инвестором о компании, акции которой реализовались на открытом фондовом рынке, а также систему сбора и последующего анализа банками информации о потенциальных или существующих клиентах и партнерах в целях защиты их собственности от возможного ущерба, в том числе репутации банка.

Современные стандарты Due Diligence были заложены в Швейцарии в 1970-х гг. с целью избежать жесткого государственного регулирования и контроля за деятельностью банков. Соглашение швейцарских банков о должной проверке (The Swiss Bank's Due Diligence Agreement), подписанное в 1977 г., установило единый подход к сбору информации о клиентах при открытии счетов и в процессе их обслуживания [52].

Понятие enhanced due diligence (EDD) впервые появилось в Американском патриотическим акте (USA Patriot Act) в 2001 году. И определяет необходимость проведения процедур усиленной проверки, а так же введения соответствующих политик контроля, которые в разумной степени призваны выявлять и сообщать о случаях отмывания денег через банковские счета. Фактически представляет собой требования более тщательной проверке клиентов:

– Принадлежащих к странам, сотрудничество с которыми ограничено (NCCTs) или относящихся оффшорным юрисдикциям;
– Участвующих в бизнесе с большим оборотом наличных денег;
– Доходы которых получены из сомнительных источников.

На основе патриотического акта, Министерством финансов в 2003 были сформированы требования по проверке клиентов (Customer Identification Program - CIP) для финансовых институтов США. CIP представляет из себя программу по верификации данных, предоставляемых клиентом о себе (ФИО, дата рождения, место проживания, подпись и т.д.) и составление профиля рисков.

В Европе же, в третьей директиве по борьбе с отмыванием денег от 2005 года (The Third Anti-Money Laundering Directive 2005/60/EC) используется понятие customer due diligence (CDD) – процедура должной осмотрительности в отношении клиента. Основные этапы входящие в CDD:

– Сбор документов и верификацию содержащейся в ней информации о клиенте;
– Определение структуры компании и определение конечных бенефициаров;
– Сбор информации о деловой и финансовой активности клиента.

Обычно CDD подразделяют на три уровня, в зависимости от предполагаемого риска:

– Упрощённая процедура должной осмотрительности (Simplified due diligence - SDD). Проводится в отношении доверенного круга клиентов, с низким уровнем риска.

– Стандартная процедура должной осмотрительности (Normal due diligence). Проводится в отношении всех новых клиентов.

– Усиленная процедура должной осмотрительности (Enhanced due diligence - EDD). Проводится в отношении рискованных клиентов.

Таким образом можно сделать вывод, что современной компании работающей на международном рынке нельзя игнорировать законодательные акты

Если же говорить о дью дилидженс в широком смысле этого термина, то он может означать сбор и анализ информации о потенциальных или существующих клиентах и партнерах в целях оценки их финансового состояния и благонадежности. Основанием для его проведения могут послужить:

– Продажа или покупка компании;

– Слияние и поглощение;

– Создание совместного предприятия;

– Оценка инвестиционной привлекательности компании;

– Публичное предложение ценных бумаг на фондовом рынке;

– Коммерческое кредитование;

– Проверка надежности своего контрагента.

В ходе проведения процедуры должной осмотрительности, подробному анализу подвергаются следующие аспекты деятельности компании:

– Информация о создании компании (подтверждение правового статуса);

– Развитие и организационная структура компании;

– Система корпоративного управления;

– Данные о трудовых ресурсах;

– Информация о производственных ресурсах предприятия и квалификации менеджмента;

– Данные об особенностях отрасли;

– Маркетинг взаимоотношений с клиентами;

– Антимонопольное регулирование финансового состояния и вопросы налогообложения;

– Объем кредиторской и дебиторской задолженности;

– Основные средства, нематериальные и иные активы (правильность оформления прав);

– Информационные технологии;

– Договора предприятия;

– Препятствия в осуществлении хозяйственной деятельности.

Описанные в этой главе подходы, помогают понять вектор развития методов, обеспечивающих экономическую безопасность компании работающей на международном рынке. Спектр рисков у таких компаний значительно шире, чем у компаний работающих только на своём национальном рынке и их игнорирование способно нанести значительный экономический ущерб.

Как мы видим, в этой главе были описаны подходы к конкурентной разведке и экономической безопасности, применяемые в нашей стране и на международном уровне. Содержание этих подходов и их фокус значительно отличаются друг от друга, что позволяет говорить о КР и обеспечении экономической безопасности, как о отдельных видах деятельности. И утверждение о том, что КР является частью СБ, будет ошибочным на наш взгляд. Хотя для большей эффективности и решения определённых оперативных задач, эти службы должны взаимодействовать, особенно в рамках международного бизнеса.

2 ОРГАНИЗАЦИЯ И ВЕДЕНИЕ КОНКУРЕНТНОЙ РАЗВЕДКИ, РОССИЙСКИЕ И МЕЖДУНАРОДНЫЕ ОСОБЕННОСТИ

2.1 ПРАВОВЫЕ ОСНОВЫ КОНКУРЕНТНОЙ РАЗВЕДКИВ РОССИИ

Как мы говорили раньше, конкурентная разведка отличается от промышленного шпионажа строгим соблюдением закона. И именно понимание правовых основ поможет нам в этом. И хотя в российском законодательстве нет отдельного закона, регламентирующего эту деятельность, существует множество других законодательных актов влияющих на то, как конкурентная разведка должна осуществляться.

Так же в этой главе описаны методические основы конкурентной разведки, те базовые механизмы, что лежат в основе её деятельности. Понимание этих основ является первоочередным шагом к созданию эффективной конкуренткой разведки в любой организации.

И в третьем параграфе описаны конкретные схемы организации отдела конкурентной разведки. А так же показаны ключевые точки, которые позволят сделать работу этого подразделения эффективной. Поскольку структуры международных компаний могут значительно отличаться друг от друга, в работе приведены различные варианты организации подразделения КР.

Прежде чем перейти к рассмотрению методик используемых в конкурентной разведке сначала необходимо рассмотреть правовые основы её деятельности. Нужно уточнить, что в России нет специального закона регулирующего деятельность КР в отличии, например от частной детективной деятельности, которая регулируется законом от 11 марта 1992 г. N 2487-I "О частной детективной и охранной деятельности в Российской Федерации". В связи с этим можно сказать, что КР находится в обще правовом поле, так же как например и деятельность служб экономической безопасности. В связи с чем, иногда сотрудники частных детективных агентств пытаются упрекать специалистов КР противоправной

деятельностью, пересекающейся с их профессиональной сферой и нарушением федерального закона №144-ФЗ "Об оперативно-розыскной деятельности". Это заблуждение связано в первую очередь с непониманием базовых задач КР и его инструментария, а во вторых с незнанием юридических основ её деятельности.

Базовым положением Конституции РФ на которое опирается КР, является четвёртая часть статьи 29 – «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». Перечень сведений, составляющих государственную тайну, определяется федеральным законом от 21 июля 1993 г. N 5485-I "О государственной тайне" (ред. от 21 декабря 2013 г.).

Так же можно выделить Федеральный закон от 8 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» [4]. Этот закон устанавливает, что информация в зависимости от категории доступа к ней подразделяется на общественную информацию, а так же на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). В свою очередь информация ограниченного доступа подразделяется на информацию, составляющую государственную, коммерческую, служебную, иную профессиональную тайну, а так же личную и семейную тайну. Нужно отметить, что КР работает с источниками информации относимым к категории общественные.

В условиях конкурентной среды, при проведении легальных изысканий в отношении юридического лица, большое значение приобретает соблюдение норм закона от 29.07.2007 №98-ФЗ «О коммерческой тайне» (ред. От 11.07.2011). Закон определяет коммерческую тайну, как режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. А информацию, составляющую коммерческую тайну (секрет производства), как сведения

любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Такое широкое определение требует уточнения, что не может являться коммерческой тайной. Статья 5 закона определяет, что режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

– содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
– содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
– о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
– о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
– о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях

производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

– о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

– о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

– об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

– о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

– о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

– обязательность раскрытия которых или недопустимость ограничения доступа, к которым установлена иными федеральными законами.

Так же существует ряд законодательных актов, которые уточняют к какой информации доступ так же открыт. В соответствии со статьёй 6 Федерального закона от 8 августа 2001 г. №129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей» [3], считаются открытыми и общедоступными сведения и документы, содержащиеся в государственных реестрах. Так из Единого государственного реестра юридических лиц мы можем получить следующую информацию, вот неполный список:

– Размер уставного фонда. Например, минимальный размер в 10000р. может свидетельствовать о признаках фирмы «однодневки»;

– Сведения об учредителях (за исключением персональных данных), что помогает определить аффилированность интересующих нас структур;

– Сведения о филиалах и представительствах, что при отслеживании вновь открываемых обособленных подразделений помогает определить приоритетные территории для расширения компании;

– Сведения о полученных лицензиях, что помогает определить изменения в сферах деятельности компании.

– Сообщения о принятии решений о ликвидации, о реорганизации, об уменьшении уставного капитала, о приобретении обществом с ограниченной ответственностью 20% уставного капитала другого общества, а также иные сообщения юридических лиц, которые они обязаны публиковать в соответствии с законодательством Российской Федерации.

Другой важной информацией о юр. лице является его бухгалтерский баланс, в котором отражается в денежном выражении состояние средств предприятия по их видам и источникам образования на определенную дату. Получение доступа к этой информации регламентируется Приказом от 20 мая 2013 г. № 183 об утверждении административного регламента предоставления Федеральной службой государственной статистики (Росстат) государственной услуги "Обеспечение заинтересованных пользователей данными бухгалтерской (финансовой) отчётности юридических лиц, осуществляющих свою деятельность на территории Российской Федерации". Пункт 2 говорит, что получателями результатов предоставления государственной услуги являются: физические лица; юридические лица (за исключением государственных органов и их территориальных органов, органов государственных внебюджетных фондов и их территориальных органов, органов местного самоуправления).

Для получения сведений необходимо подать запрос в Росстат или его территориальное отделение (приложение N 2 к Регламенту). Это можно сделать разными способами: лично, по электронной почте, через сайт или почтовое отделение. В конце запроса необходимо поставить свою подпись с

расшифровкой и дату. Если запрос идет от имени организации, его подписывает уполномоченный представитель. При направлении запроса в электронном виде подпись не требуется, но вам нужно указать Ф.И.О.

В соответствии с пунктом 12.2 отказано может быть в том случае, если запрашиваемая информация относится к информации ограниченного доступа. В этом случае к запросу должны прилагаться документы, подтверждающие выполнение требований, установленных статьей 16 Закона Российской Федерации от 21 июля 1993 г. N 5485-1 "О государственной тайне", а также разрешение органа государственной власти, в распоряжении которого в соответствии с Перечнем сведений, отнесенных к государственной тайне, утвержденным Указом Президента Российской Федерации от 30 ноября 1995 г. N 1203, находятся сведения, содержащиеся в годовой бухгалтерской (финансовой) отчетности.

В отношении акционерных обществ (АО), закон определяет какую информацию они обязаны публиковать в открытых источниках. В частности, Федеральный закон от 26 декабря 1995 г. №208-ФЗ «Об акционерных обществах» [1] предписывает Открытым акционерным обществам ежегодно публиковать:

- Годовой отчёт общества, годовую бухгалтерскую отчётность;
- Проспект эмиссии акций общества в случаях, предусмотренных правовыми актами РФ;
- Сообщение о проведении общего собрания акционеров в порядке, предусмотренным настоящим Федеральным законом.

Данная информация может стать полезной при анализе финансово хозяйственной деятельности конкурента. Так же нужно уточнить, АО обязано обеспечить акционерам доступ к определенным документам вне зависимости от числа принадлежащих им акций (Ст. 91 Закона об АО). Наиболее важным документом, который должен предоставляться акционерам, является годовой отчет Общества. Он представляет собой официальный документ, который отражает финансовое положение АО и

который должен распространяться среди акционеров в соответствии с требованиями ФКЦБ. В годовой отчет включается описание деятельности Общества, а также его бухгалтерский баланс, отчет о прибылях и убытках и иные статьи.

Годовой отчет – это не только документ, который АО обязано готовить в силу требований закона. Годовой отчет следует рассматривать, в первую очередь, как инструмент предоставления информации акционерам. В нем может сообщаться о достижениях компании, и он может способствовать привлечению инвесторов. Годовой отчет должен, тем не менее, отражать сбалансированную картину деятельности Общества, т.е. не только успехи, но и неудачи. [21]

Очень важной для анализа компании является информация о правах собственности на недвижимость. В соответствии с Федеральным законом от 21 июля 1997 г. №122-ФЗ «О государственной регистрации прав на недвижимое имущество и сделок с ним» статья 7, государственная регистрация прав носит открытый характер [2]. Орган, осуществляющий государственную регистрацию прав, обязан предоставлять сведения, содержащиеся в Едином государственном реестре прав, о любом объекте недвижимости любому лицу, предъявившему удостоверение личности и заявление в письменном виде (юридическому лицу – документы, подтверждающие регистрацию данного юридического лица и полномочия его представителя).

Выписки из Единого государственного реестра прав, утверждённые в установленном порядке, должны содержать:

- Описание объекта недвижимости;
- Зарегистрированные права на объект недвижимости;
- Информацию об ограничении (обременении) прав;
- Сведения о существующих на момент выписки судебных спорах о праве собственности.

В то же время, для выявления интереса к собственным объектам недвижимости можно получать информацию о запросах. Орган, осуществляющий государственную регистрацию прав, обязан по запросу правообладателя предоставлять ему информацию о лицах получивших сведения об объекте недвижимости, на который он имеет права [14, с. 24].

Если же говорить о внешне экономической деятельности, то в соответствии с пунктом 3 статьи 46 Федерального закона от 27.12.2002 №184-ФЗ "О техническом регулировании" Правительство Российской Федерации постановило утвердить единый перечень продукции, подлежащей обязательной сертификации и единый перечень продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии. Постановлением правительства РФ от 1 декабря 2009 г. №982 эти перечни были утверждены.

Таким образом, в случае если объект вашего интереса ввозит в страну продукцию, входящую в выше обозначенные перечни, то он обязан получить декларацию о соответствии, данные которой Федеральная служба по аккредитации (Росаккредитация) разместит в открытой части реестра зарегистрированных деклараций о соответствии в течение суток с момента публикации [96]. Информация содержащаяся в декларации является важным источником информации как о заявителе, так и о изготовителе продукции и может использоваться службой КР для анализа деятельности конкурента.

Если же ваша компания работает в высоко технологичной области, то четвёртая часть Гражданского кодекса РФ [5] устанавливает нормы регулирующие отношения в области изобретений, полезных моделей, промышленных образцов. В задачи современной КР несомненно входит и отслеживание инновационной деятельности конкурента. В соответствии со статьей 1394 ГК РФ федеральный орган исполнительной власти по интеллектуальной собственности публикует в официальном бюллетене сведения о выдаче патента на изобретение, полезную модель или промышленный образец, включающие имя автора, имя или наименование

патентообладателя, название и формулу изобретения или полезной модели, либо перечень существенных признаков промышленного образца и его изображение. Состав публикуемых сведений определяет федеральный орган исполнительной власти, осуществляющий нормативно-правовое регулирование в сфере интеллектуальной собственности. Кроме того, в статье 1235 Гражданского кодекса РФ предусмотрена регистрация лицензионных договоров о подаче исключительного права на результаты интеллектуальной деятельности, что даёт нам возможность получить информацию о лицензиарах и лицензиатах законным способом [14, с. 25].

Нужно ещё раз акцентировать внимание, на то что КР всегда должна работать в рамках закона и соблюдать морально-этические нормы. Например, в СПКР была сформулирована следующая позиция по этому поводу: «Не нарушай закон - он может наказать. Не игнорируй общественное мнение - оно может уничтожить.»

С таким определением согласны не все, например существует достаточно большое количество специалистов СБ, которые считают что функционал их служб полностью перекрывает задачи КР. Это связано в первую очередь с большим количеством бывших сотрудников силовых ведомств в рядах СБ, профессиональный опыт которых накладывает определённый отпечаток на методы их работы. Для того что бы лучше понять о чём речь, ниже на рисунке 12 приведены результаты небольшого опроса с одного из закрытых форумов посвящённых безопасности.

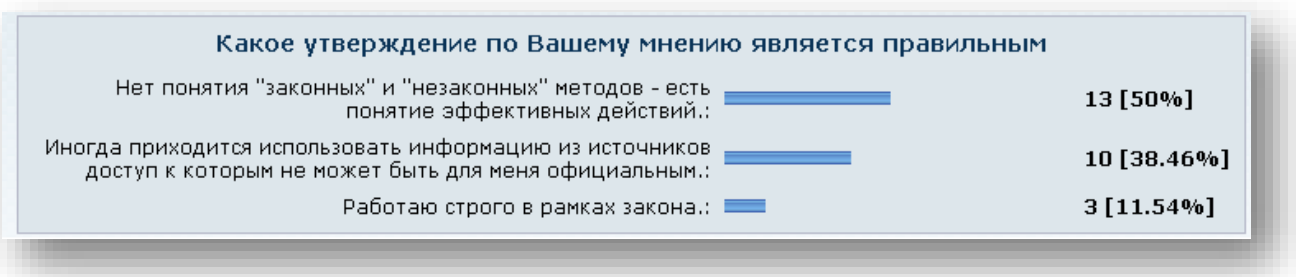

Рисунок 12 – Результаты опроса

Конечно, ни о какой конкурентной разведке в рамках таких подходов речи идти не может, не говоря уже о морально-этических нормах. Несовершенство законодательства, разрыв между практикой работы СБ и существующими законами, так же являются значительными факторами влияния. Для того что бы преодолеть подобную разницу в подходах между специалистами потребуется достаточно много времени, а так же активная законотворческая позиция государства основанная на диалоге между всеми заинтересованными сторонами.

2.2 МЕТОДИЧЕСКИЕ ОСНОВЫ КОНКУРЕНТНОЙ РАЗВЕДКИ

В параграфе рассмотрена теория пяти сил Портера, как основа модели стратегических угроз, используемой в конкурентной разведке.

Так же рассмотрены теоретические основы информационно-аналитического процесса, который стал базой для формирования «разведывательного цикла» применяемого в государственных разведывательных структурах, а позже перенесённого в практику КР.

Описан подход - «ключевые темы разведки», который позволяет актуализировать цели КР на регулярной основе. А так же рассмотрены механизмы повышения эффективности этого процесса.

Показана роль информационно-аналитических систем в работе современной КР. Рассмотрены функции сбора и хранения, обмена данными и аналитики.

В основе концепции современной КР, как инструмента достижения конкурентных преимуществ лежит модель «пяти сил» Майкла Портера, которые воздействуют на уровень конкуренции в отрасли, а так же влияют на конкурентную среду в целом. Эта модель используется для выявления стратегических угроз в отношении фирмы и планирования собственных действий с их учетом. Стоит отметить, что некоторые отечественные авторы выделяют еще один аспект, которые оказывает серьезное воздействие на конкурентную среду. Это «административный и криминальный ресурс» (рисунок 13), в странах с «переходной» экономикой эта сила может оказывать серьёзное влияние.

Рисунок 13 - Расширенная модель «пяти сил» Портера [37]

Майкл Портер выделил пять основных конкурентных сил и отметил, что все пять конкурентных сил, совместно определяют интенсивность отраслевой конкуренции и её прибыльность.

Конкурентные силы по классификации Майкла Портера выглядят следующим образом:

– Рыночная власть потребителей. Портер утверждал, что покупателей нужно рассматривать, как конкурентов отрасли, поскольку они требуют постоянного снижения цен, повышения качества продуктов и услуг, и качества обслуживания. Удовлетворение всех этих аспектов происходит за счет снижения прибыли компании. Потребители могут либо снижать уровень потребления, либо вовсе переключаться на продукцию конкурентов;

– Рыночная власть поставщиков. Благосостояние компании непосредственно связано с деятельностью ее поставщиков. Проблемы, возникающие у поставщиков с кредитами, ресурсами, поставками,

платежами автоматически переходят на компанию, у которой и без этого немало непредвиденных расходов. Более того поставщики имеют право изменить цены за оказываемые услуги и снизить качество поставляемой продукции в виду возможности потери прежнего положения на рынке. Кроме этого есть вероятность, что поставщики уйдут к конкурентам, которые предлагают им более выгодные условия. Получается, что поставщики могут выкачивать прибыль из отрасли, которая окажется неспособной возместить этот рост цен повышением собственных цен;

– Угроза появления товаров-субститутов или услуг-субститутов. Товары-субституты выполняют те же функции, что и стандартные товары отрасли, но могут быть представлены на рынке особым образом. Эти товары ограничивают потенциальную прибыльность, устанавливая потолок цен для всех фирм, работающих в отрасли. Основной угрозой товаров-субститутов является снижение спроса на продукцию и доли рынка компании. Противостояние субститутам вполне может стать предметом коллективных усилий отрасли;

– Угроза появления новых или потенциальных конкурентов. Наличие новых конкурентов приводит к снижению прибыли, усилению конкуренции и снижению доли рынка компании. Это происходит как из-за переманивания ряда клиентов, так и из-за снижения среднерыночных цен в отрасли. Степень угрозы вхождения в отрасль новых участников зависит от барьеров входа в сочетании с реакцией конкурентов на появление этих самых участников. К барьерам вхождения М. Портер относит экономию на масштабе, дифференциацию, дистрибуцию, патенты, государственные облигации и преданность бренду;

– Угроза со стороны существующих конкурентов. Основной проблемой, связанной с текущими конкурентами, является взаимозависимость компаний. Естественно, каждая фирма стремится

внести изменения в управление для сокращения издержек, следовательно, в результате этого изменяется вся конкурентная среда. Наблюдается повышение качества продукции и уровня обслуживания, разработка новых, более конкурентоспособных товаров, снижение себестоимости и активизация рекламной деятельности. [59, с. 64]

Пять сил М. Портера помогают нам увидеть, что из себя представляют основные стратегические угрозы для компании, но для понимания механизмов действия системы КР, целесообразно рассмотреть основные стадии информационно-аналитического процесса и его составные элементы (рисунок 14). Информационно-аналитический процесс это в первую очередь мыслительная деятельность, направленная на решение поставленной задачи и из неё можно выделить четыре основных стадии: накопления знаний и сведений, осмысливание материала, умозаключения и выводы, проверка выводов. В свою очередь, эти крупные блоки можно конкретизировать и разбить на более мелкие, используя научный подход. В методе научного исследования выделяют семь этапов:

- Общее знакомство с проблемой. Ознакомление с проблемой в целом, а также со смежными вопросами, изучение которых может оказаться полезным; составление общего плана работы с указанием срока выполнения, исполнителей и основных источников, которые предположительно могут быть использованы.
- Определение используемых терминов и понятий. Необходимо определить и объяснить тот или иной термин или понятие так, чтобы это было ясно нам самим, тем, кто контролирует нашу работу, и тем, кто пользуется нашей информацией.
- Сбор фактов. Другими словами, собранная информация должна быть проверена на достоверность.
- Истолкование фактов. Этот этап включает оценку, классификацию, анализ и уяснение фактов.

– Построение гипотезы. Рабочие гипотезы, выдвигаемые на этом этапе, обычно связаны с какими-либо конкретными вопросами, отвечая на которые можно проверить сами гипотезы. Многие считают построение гипотезы важнейшим моментом любого исследования как в области естественных или общественных наук, так и в области информационно-аналитической работы. Построение гипотезы, взятое в широком смысле, всегда присуще любой исследовательской работе. В самом начале исследования, когда вырабатывается общий план, мы исходим из определенных предположений (или гипотез) о том, какие факторы, возможно, играют важную роль и какие почти определенно не имеют отношения к делу. Аналогичными гипотезами мы руководствуемся при сборе и истолковании фактов, формулировании выводов и изложений. Гипотеза — термин, прочно утвердившийся в научной литературе. Разведчики для обозначения рассматриваемого этапа чаще применяют термин «интеграция», хотя эти два термина имеют не совсем одинаковое значение.
– Выводы. На этом этапе производятся исследования, необходимые для доказательства или опровержения рабочих гипотез, выдвинутых на предыдущем этапе, и формулируются окончательные выводы, являющиеся сутью практически любого информационного документа.
– Изложение. Составление документа, завершающего работу. Составитель информационного документа должен не только ясно представлять себе то, о чем он пишет, но и уметь выразить свои мысли в ясной форме. Описанные этапы метода научного исследования применительно к информационной работе схожи с теми этапами, на которые обычно делят свою работу аналитики.

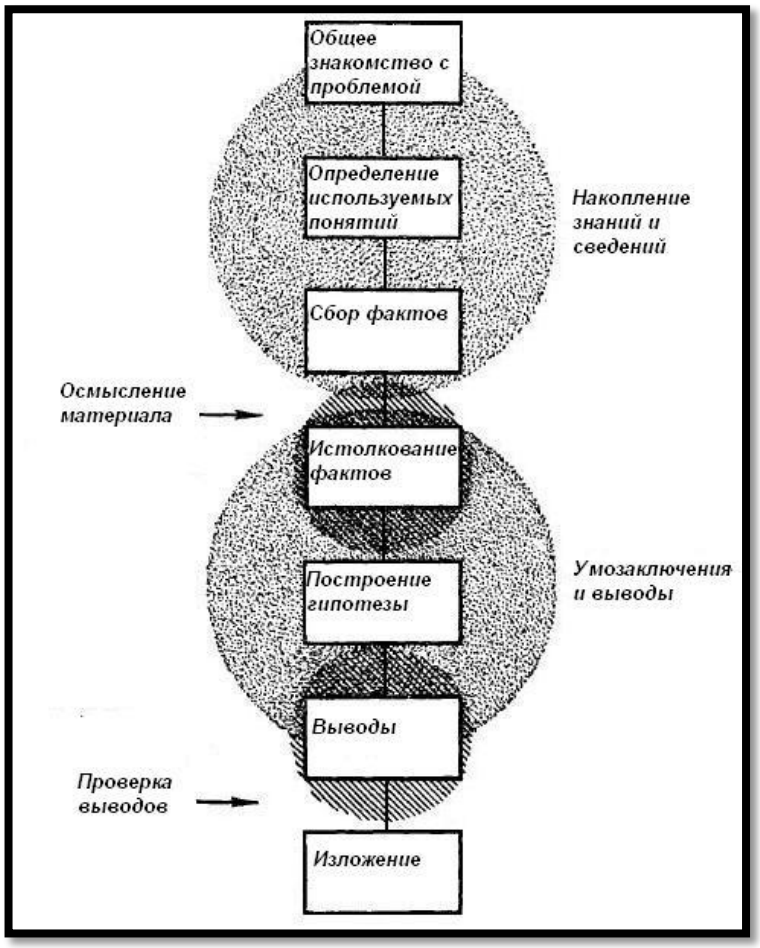

Рисунок 14 - Четыре стадии творческого мышления во взаимосвязи с семью этапами информационной работы [58]

Аналитики спецслужб активно использовали в своей деятельности научный подход к информационной работе, который со временем трансформировался в «разведывательный цикл», который бывшие сотрудники спецслужб и привнесли в практику КР. В общем виде разведывательный цикл состоит из пяти последовательно реализуемых этапов: планирование и выбор направления, сбор данных, обработка, анализ и составление отчёта, распространение. [89]

Планирование и выбор направления.

Планирование действий и определение направления, в котором мы должны двигаться, чтобы сделать работу, перечисляя то, что мы знаем о проблеме и что мы должны узнать. Обсуждение способов сбора необходимой информации и требующейся аналитики.

Сбор данных.

Непосредственно сбор данных из всех доступных нам источников. В случае с государственной разведкой, эти источники могут быть как открытыми (газеты, телевидение, радио), так и скрытыми (скрытые видеокамеры, подслушивающие устройства, агентура).

Обработка.

Вся собранная информация обрабатывается и помещается в сводку, это может быть что угодно, от переведённого документа, до расшифровки спутниковой фотографии.

Анализ и составление отчёта.

На основе обработанных данных мы составляем аналитический отчёт. Отталкиваясь от первоначальных задач, мы оцениваем то, что происходит, почему это происходит, что могло бы произойти затем, и как это затрагивает наши интересы.

Распространение.

Составленный отчёт доставляется заинтересованным лицам, ставившим задачи. После изучения отчёта задачи уточняются, либо появляются новые и весь цикл повторяется.

Эффективное применение КР возможно только при наличии чётко определённых направлений разведывательной деятельности, которые соотносятся со стратегическими целями компании. Определение приоритетов одна из важных составляющих разведывательного цикла.

Для продуктивной работы на этом этапе Ян Херринг предлагает использовать систему под названием «ключевые темы разведки» (key intelligence topics). Изначально данная модель была адаптирована для корпоративного уровня из системы «темы национальной разведки» (national intelligence topics) используемой в Американских спецслужбах. Суть системы ключевых тем разведки (КТР) заключается в систематическом диалоге с первыми лицами компании, принимающими решения. В результате обсуждения определяются основные направления для эффективных разведывательных операций и одновременно уточняется, какие именно

ресурсы потребуются для удовлетворения информационных потребностей компании.

Рисунок 15 - Место КТР в разведывательном цикле [49, 89]

Для лучшей систематизации КТР обычно делят на три основных блока: *Стратегические решения и действия.*

– Формулирование и реализация стратегических планов;

– Капитальные затраты, влияющие на конкурентные позиции;

– Создание стратегических альянсов, приобретения и продажи активов.

Темы разведывательной информации «раннего предупреждения».

– Возможности, которые компанию интересуют, прежде всего;

– Различные угрозы, включая новых конкурентов и новые товары субституты;

– Значительные изменения в промышленности, правительстве, технологиях.

Описание основных и новых игроков рынка.

– Более глубокое понимание своих возможностей относительно участников рынка;

– Понимание и предвидение относительно их действий;

– Мониторинг их деятельности на постоянной основе.

Процесс ТКР является практическим механизмом для определения потребностей менеджмента в разведывательной информации, но эта информация должна обновляться на постоянной основе. Потребность в получении и обновлении информации обусловлена несколькими факторами: 1) в большинстве отраслей конкурентная ситуация изменяется с течением времени; 2) приход новых менеджеров на место старых изменяет характер потребностей в информации; 3) с течением времени изменяется сама структура компании, а вместе с этим изменяется и потребность в информации.

Так же существует проблема того, что потребности в информации менеджеров высшего уровня, которые принимают стратегические решения, коренным образом отличаются от потребностей менеджеров среднего уровня, принимающих тактические решения. Например, топ-менеджерам необходимо понять динамику развития отрасли и оценить будущий потенциал для получения прибыли, а сотрудникам отдела продаж - заключить совершенно конкретные сделки. Перекос в сторону какой то из потребностей способен значительно снизить потенциал КР. Мири и Прескотт предлагают следующие механизмы, при помощи которых лучшие корпорации определяют конкретные характеристики необходимой стратегической и тактической информации (система TAP-IN™). Ее элементы:

– Формирование «команд», информационные технологии и обучение.

– Определение того, какой персонал отвечает за сбор стратегической, а какой — тактической информации.

– Планирование. Каким образом КР интегрирована в процесс планирования (на предприятии)?

– Диалоговое взаимодействие с клиентами, использующими данные КР.

– Позиция группы КР в сети коммуникаций организации [49].

С развитием компьютерных систем и IT, роль информационно-аналитических систем (ИАС) неуклонно росла. На современном этапе развития КР, использование подобного рода систем стало стандартом. Подобные системы способны автоматизировать процессы сбора, хранения и анализа информации, благодаря чему руководитель имеет возможность принимать управленческие решения не на интуитивном уровне, а основываясь на конкретных фактах. Примеры информационно-аналитических систем приведены в приложении Г.

ИАС позволяют собирать, накапливать и обрабатывать доступную информацию как из внутренних, так и из внешних источников. При организации КР в сети интернет, широкое распространение получило направление науки, возникшего на стыке искусственного интеллекта, статистики и теории баз данных, как Knowledge Discovery (обнаружение знаний), использующего концепции Data Mining (добыча знаний в формализованных базах данных) и Text Mining (добыча знаний в неструктурированных текстах) [25].

Технологии Data Mining и Text Mining помогают выявлять неочевидные закономерности в данных или текстах, так называемые скрытые знания. Эти технологии также помогают обнаружить в "информационном сырье" ранее неизвестные данные, полезные знания. Системы этого класса способны осуществлять анализ больших массивов документов и формировать предметные указатели понятий и тем, освещенных в этих документах. Одной из задач конкурентной разведки, которую можно реализовать в системах Text Mining, это нахождение исключений, то есть поиск объектов, которые своими характеристиками сильно выделяются из

общей массы. Ещё один класс важных задач, решаемых в рамках технологии Text Mining, это моделирование данных, ситуационный и сценарный анализ, а также прогноз [19].

В функционале ИАС выделяют три больших функциональных блока: Сбор и хранение, обмен данными, инструменты аналитики.

Сбор и хранение. В условиях постоянно увеличивающегося объёма информации этот вопрос остро встаёт перед современными отделами КР. Ведь всю собранную и обработанную информацию нужно где то хранить и иметь возможность оперативного доступа к ней. Для этих целей используют различные решения для создания баз данных (БД), баз знаний, экспертных систем.

В России БД определяется как представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и т. д.), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ), Статья 1260 ГК РФ.

По международным стандартам БД определяется как совокупность данных, организованных в соответствии с концептуальной структурой, описывающей характеристики этих данных и взаимоотношения между ними, причём такое собрание данных, которое поддерживает одну или более областей применения [82].

Дальнейшее развитие баз данных привело к появлению хранилищ данных (ХД) — предметно ориентированного, неизменяемого и поддерживающего хронологию набора данных. ХД используются для формирования решений. В отличие от баз данных, которые предназначены для обслуживания повседневной деятельности предприятия, ХД ориентированы на многолетний, оперативный, многомерный анализ данных, результаты которого могут быть использованы для принятия решений.

Моделью данных в ХД служат гиперкубы, т.е. многомерные базы данных, в ячейках которых находятся анализируемые данные. По осям

многомерного куба указываются измерители объекта с различных точек зрения.

На пересечении осей измерения находятся данные, количественно характеризующие события, факты, процессы Оси измерения позволяют создавать многомерную модель данных (гиперкуб), над которым можно выполнять следующие операции:

– срез;
– вращение;
– консолидация или детализация.

БД и ХД связаны с такими этапами разведывательного цикла как, процесс сбора и процесс обработки информации. На основе полученных знаний формируется база знаний (БЗ) компании.

БЗ – это совокупность знаний, относящихся к некоторой предметной области и формально представленных таким образом, чтобы на их основе можно было осуществлять рассуждения. [68, с. 10, 11]

Под БЗ понимается совокупность фактов и правил вывода, допускающих логический вывод и осмысленную обработку информация. Наиболее важным свойством информации, хранящейся в БЗ, является достоверность конкретных и обобщенных сведений в БД и релевантности информации, получаемой с использованием правил вывода, заложенных в БЗ.

В зависимости от особенностей используемых данных организация выбирает подходящую для себя модель БД, например:

– деревья (вывода, целей);
– семантические сети (ассоциативные сети);
– фреймы;
– нечёткие множества.

Ниже, на рисунке 16 представлено концептуальное отличие БД от БЗ в виде семантической сети.

Рисунок 16 - Отличия базы данных от базы знаний в виде семантической сети [65, с. 4]

Структуру БЗ по типам источников можно представить в виде трёх основных блоков:

– Публично доступная и опубликованная информация.
– Знания полученные от людей и экспертных групп.
– Знания полученные на основе анализа и синтеза знаний.

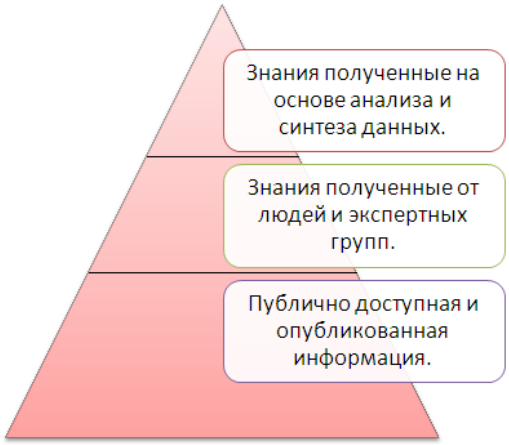

Рисунок 17 - Структура базы знаний [81]

База знаний связана с такими этапами разведывательного цикла как, процесс обработки информации и анализ данных. БЗ это по сути структурированный результат слаженной деятельности всех этапов

разведывательного цикла и представляет из себя большую интеллектуальную ценность. В связи с чем, работа с БЗ должна быть строго регламентирована, а для каждого пользователя должен быть установлен свой уровень доступа.

Обмен данными. Корпоративная система обмена данными так же имеет большое значение для КР. И речь идёт не о системах электронного документооборота или программах для внутрикорпоративного общения, хотя их использование способствует внутренней коммуникации. Речь идёт, в первую очередь, о построении системы взаимоотношений между службой КР и другими отделами внутри компании. Потому что одним из ключевых источников для получения конкурентной информации является сама компания. По сути дела, внутренние источники являются без преувеличения лучшими источниками конкурентной разведки. Например:

– Торговые представители изо дня в день контактируют с покупателями и слышат, что делают конкуренты;
– Отделы развития и аналитики могут обнаружить новые патенты или прочитать новые исследования в газетах, относящиеся к развитию конкурента;
– Отдел закупа может узнать что-то от поставщика, который обслуживает не только вас, но и вашего конкурента;
– Отдел маркетинга может на основе обратной связи составить прогноз покупательских предпочтений.

Регулярное отслеживание этих видов информации является гарантией успешной работы системы конкурентной разведки. [15]

Но здесь возникает несколько моментов, требующих особого внимания. Во-первых, необходимо, что бы сотрудники захотели делиться с вами информацией и добывать для вас информацию. Во-вторых, сотрудников необходимо научить, как это делать (на что обращать внимание, как общаться, как не привлекать внимания и не настораживать и т.п.). В-третьих, сотрудникам должно быть удобно, передавать вам информацию – должен быть простой и эффективный механизм обмена информацией.

Первичная задача при создании такой информационной сети в компании состоит в том, чтобы определить, кто в вашей организации обладает информацией по интересующим вас вопросам. И сделать так, чтобы сотрудники сами захотели поделиться с вами имеющимися у них данными [54, с. 62].

С внедрением современных платформ обмена данными активность взаимодействия между различными кластерами людей становится очень высокой, что в свою очередь приводит к возникновению таких явлений как «коллективный разум» и совместная аналитика. Разумное применение таких инструментов способно повысить эффективность КР.

Инструменты аналитики. Конкурентная разведка появилась на стыке: экономики, маркетинга, военной теории, информатики и стратегического управления [86]. И поскольку КР является междисциплинарным предметом, то список используемых инструментов достаточно обширный. Это могут быть и инструменты, которые традиционно использовались в маркетинге SWOT, PESTLE, ADL матрицы. И различные решения по визуализации данных и нейронные сети, которые сейчас активно используются в IT решениях. И стратегические «шахматные доски» и «военные игры», пришедшие из стратегического управления и военной теории. Например на сайте компании Competia приведён список из 46 техник анализа, которые используются в КР.

В связи с бурным ростом IT сферы, аналитические инструменты всё чаще реализуются в виде различного прикладного программного обеспечения, в связке с современными средствами визуализации связей активно применяются на этапе анализа разведывательного цикла.

Как мы видим, в основе КР лежат современные теории и практика разведывательных служб. В своём стремлении повысить свою эффективность, КР вобрала в себя множество инструментов из смежных дисциплин, а так же адаптировала передовые информационные технологии для своих нужд.

2.3 МЕСТО КОНКУРЕНТНОЙ РАЗВЕДКИ В СТРУКТУРЕ КОМПАНИИ.

Перед тем как перейти непосредственно к рассмотрению структуры и моделям отдела КР, мы должны рассмотреть основополагающие принципы заложенные в её основу (рисунок 18). Этих принципов девять и они универсальны вне зависимости от конкретной формы организации отдела КР.

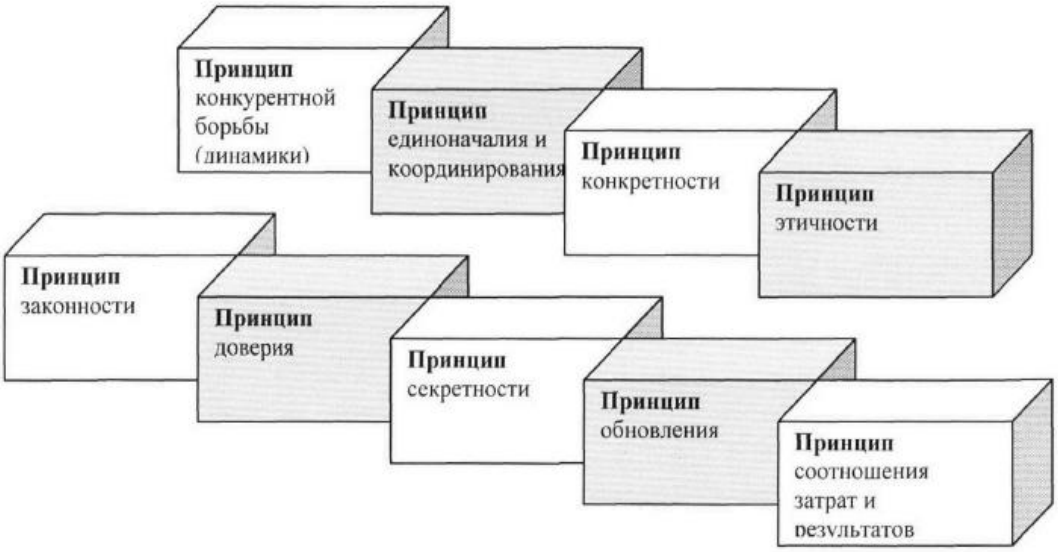

Рисунок 18 - Методические принципы функционирования службы КР на предприятии [34, с. 95]

Принцип конкурентной борьбы (динамики). В условиях конкурентной борьбы внешняя среда предприятия постоянно претерпевает динамические изменения. Своевременное и точное определение факторов её изменения и сбор информации о них является одной из ключевых потребностей современной организации. Именно эти потребности и удовлетворяет КР.

Принцип законности. Деятельность службы КР должна вестись строго в рамках закона, в противном случае предприятие могут обвинить в промышленном шпионаже со всеми вытекающими судебными и репутационными издержками.

Принцип единоналичия и координирования. Этот принцип – необходимое условие эффективной работы службы КР. Она должна подчиняться непосредственно первому лицу, несмотря на то, что заказчиками информации могут выступать и другие отделы предприятия.

Принцип конкретности. Результат деятельности КР который ложится на стол к высшему руководству должен содержать конкретные выводы и рекомендации, а не сухие цифры и факты. Они должны служить достаточным основанием для принятия решения.

Принцип доверия. При выполнении поставленных задач, деятельность службы КР сопряжена с большой долей самостоятельности и без доверия со стороны руководства её эффективная работа затруднительна. Выстраивание доверительных отношений с другими отделами так же является немаловажной задачей, ведь большая часть необходимой КР информации уже находится внутри компании.

Принцип этичности. Этика в конкурентной разведке – это способность строить свою работу так, чтобы не вызывать возмущения общественности. Именно поэтому этика – не личное дело специалиста и не находится внутри него. Это именно эмоциональная оценка обществом его поступков [70]. Проблема в том, что этика в разных обществах понимается по-разному. То, что неприемлемо в одной стране или профессиональной группе, может быть нормой жизни для другой, именно по этому к данному вопросу нужно относится с большой осторожностью. Например в американском сообществе профессионалов конкурентной разведки (SCIP) существует кодекс этики содержащий следующие пункты:

- постоянно старайся увеличить уважение и признание к этой профессии на всех государственных уровнях;
- выполняй свои служебные обязанности с рвением и прилежанием, поддерживай самый высокий уровень профессионального мастерства и избегай всех неэтичных поступков;
- оставайся верным политике компании, ее целям и общему курсу и выполняй обещания, данные своей компании;
- выполняй все действующие законы;
- во время делового свидания предоставляй всю относящуюся к делу информацию, включая принадлежность к организации;

– соблюдай правила работы с конфиденциальной информацией;
– действуй в полном соответствии с этими этическими стандартами при работе внутри компании, при ведении переговоров и во всех ситуациях, когда придется работать по специальности [88].

Принцип обновления. Работа по обновлению КТР должна вестись на регулярной основе. Вся информация по ключевым направлениям должна систематически обновляться. Используемые источники и инструменты так же должны регулярно обновляться.

Принцип секретности. При выполнении своих функций служба КР должна отталкиваться от принципа должной секретности. Российские специалисты сходятся во мнении, что это подразделение должно быть залегендировано в структуре предприятия. Связано это с тем, что в глазах всего остального рыночного окружения в случае обнаружения этим окружением вашей разведывательной активности ваша компания будет заниматься не чем иным, как противозаконным промышленным шпионажем. Кроме того, если по тем или иным признакам, вашим внешним конкурентным окружением – будут вскрыты непосредственные объекты разведывательного интереса вашей компании – это означает, что вы раскрываете перед своими конкурентами – как и какими конкретными методами, стратегиями, технологиями – вы собираетесь действовать на рынке в ближайшей и более отдаленной перспективе. На какие рынки и потребителей – будет нацелен бизнес вашей компании. Какие виды товаров или услуг вы будете развивать и в каком направлении. Какие технологии и бизнес-процессы развивать и использовать [43].

Принцип соотношения затрат и результатов. Очень важно, чтобы затраты на сбор и обработку информации были многократно меньше того положительного эффекта, который вы собираетесь получить от ее использования.

Одной из распространённых в России точек зрения заключается в том, что служба КР должна быть включена в СБ. Мы не согласны с такой узкой

точкой зрения, например Лемке Г. Э. так описывает эту ситуацию: «Отнесение функций конкурентной разведки к компетенции службы безопасности правомерно, когда конкурент пытается осуществить прямое физическое подавление бизнес-структуры, представляющее собой преступные посягательства на имущество, жизнь и здоровье персонала предприятия, и является ошибочной, когда речь идёт о конкурентном влиянии или стандартной конкурентной борьбе не некриминальными методами.» [42, с. 58] Другими словами, задачи СБ лежат преимущественно в области минимизации рисков предприятия от криминальных факторов. В то время как задачи КР заключаются в работе с факторами конкурентоспособности бизнеса. Подчинение руководителю СБ будет определять те цели и задачи которые будет решать подразделение КР в структуре предприятия и заточенность под нужды безопасности конечно будет сказываться на конечном результате. Кроме того, включение информационных потоков генерируемых КР в контур информационной системы СБ накладывает определённые искажения обусловленные функционалом этой службы. Однако в отдельных случаях, подходы КР могут использоваться и специалистами СБ.

Международные специалисты по КР, так же как и Российские коллеги, сходятся во мнении, что разведывательная деятельность в отношении конкурентов гораздо ближе к маркетингу, нежели к функциям, которые выполняет исключительно СБ предприятия. У специалиста в области коммерции больше шансов увидеть «слабые сигналы» свидетельствующие об изменении конъюнктуры рынка и сделать правильные выводы [14, с. 28].

Одной из точек зрения является то, что подразделение КР должно подчиняться напрямую первому лицу компании или органу ответственному за принятие управленческих решений. На практике же подчинённость КР и её структура очень сильно зависят от структуры самой организации в которой она внедряется, что может в разной степени влиять на её эффективность.

Один из вариантов функциональной структуры службы КР в крупной компании можно представить в виде четырех подразделений взаимодействующих между собой (рисунок 19). Это координационное подразделение, добывающее подразделение, обрабатывающее подразделение, подразделение обеспечения.

Рисунок 19 - Линейная схема службы конкурентной разведки с горизонтальными каналами обмена информацией [54]

Координационное подразделение берет на себя задачи общего управления:

- стратегическое планирование работ;
- оперативно-тактическое планирование;
- координация действий участников работ.

Добывающее подразделение выполняет работы по получению доступа к нужной информации:

- определения мест нахождения искомой информации;
- определение вариантов доступа к этой информации;
- получение доступа к этой информации;
- предоставление информации отделу КР.

Обрабатывающее подразделение осуществляет работы с полученной информацией:

- накопление и хранение собранной информации;
- анализ информации;
- составление результирующих документов;
- презентация результата заказчику.

Подразделение обеспечение выполняет вспомогательные функции:

- содержание технических средств в надлежащем состоянии;
- поддержка работоспособности ЛВС;
- разработка вспомогательного софта;

Несмотря на наличие линейной структуры, служба конкурентной разведки имеет скорее проектный характер. Выражается это в том, что под каждый крупный проект создается своя рабочая группа в составе координатора, аналитика, сотрудника добывающего подразделения и чаще всего консультанта из соответствующего подразделения компании. В результате получаются группы сотрудников, работающих над своими проектами (проблемами). Такая схема гораздо эффективнее, чем работать по принципу все делают все [54, с. 10].

3 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, КАК СОВРЕМЕННЫЙ ИНСТРУМЕНТАРИЙ КОНКУРЕНТНОЙ РАЗВЕДКИ И СЛУЖБЫ БЕЗОПАСНОСТИ, ВОЗМОЖНОСТИ ВЗАИМОДЕЙСТВИЯ

3.1 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, КАК ИНСТРУМЕНТАРИЙ КОНКУРЕНТНОЙ РАЗВЕДКИ

В данной главе рассмотрены конкретные инструменты применяемые специалистами КР и СБ. А именно, программные продукты и интернет как наиболее часто применяемые инструменты в работе современных специалистов.

Рассмотренные в 1 и 2 главе особенности работы подразделений КР и СБ, отражены здесь в виде информационных технологий с соответствующим функционалом позволяющим решать конкретные рутинные задачи. Именно автоматизация решения таких задач позволяет специалистам правильно распределять рабочую нагрузку и концентрироваться на наиболее критичных вопросах.

Кроме того в данной главе разработаны различные варианты взаимодействия КР и СБ. Показаны их сильные и слабые стороны, а так же показана та выгода для международной компании, которую способно дать такое взаимодействие.

Отталкиваясь от методологии КР описанной во второй главе, в этом параграфе рассмотрены основные практические инструменты используемые специалистами. Способы и особенности поиска информации в интернете, способы анонимизации, методы сбора и мониторинга все эти задачи могут решаться при помощи соответствующего программного обеспечения.

Поскольку конкурентная разведка это явление междисциплинарное, то и её инструментарий по большей части состоит из приёмов, пришедших в неё из смежных дисциплин. Но утверждать, что в её арсенале нет инструментов свойственных только ей, тоже не совсем верно. Охватить весь спектр

приёмов используемых в КР не представляется возможным ввиду ограничений, которые накладывает на нас формат данной работы. В связи с чем, целесообразней всего будет сконцентрироваться на методах получивших наибольшее распространение в последнее время, а именно на использовании цифровых технологий и сети Интернет.

Интернет с каждым днём всё глубже проникает в нашу жизнь и сфера КР не является исключением, то обстоятельство, что огромное количество информации сконцентрированной в сети делает этот источник очень привлекательным. Возможности программ работающих с интернет ресурсами растут невероятными темпами, и в этой главе мы коснёмся основных тенденций в этом направлении. Но для того что бы уметь пользоваться такими инструментами мы должны понимать как интернет устроен.

Наиболее часто для поиска информации в сети пользователи используют поисковые машины типа Yandex или Google, для многих они напрямую ассоциируются с интернетом. Существует распространённое заблуждение, что то чего поисковик не нашёл, не существует в интернете. Это связано с тем, что многие пользователи не знакомы с особенностями работы поисковиков. Частота и глубина индексирования страниц зависит от алгоритмов поискового робота, у разных поисковых машин они разные. Индексация представляет собой процесс добавления сведений о сайте роботом поисковой машины в базу данных поисковика, которая в дальнейшем является основой для полнотекстового поиска информации на проиндексированных сайтах. При переводе основного смыслового содержания сайта или документа с естественного языка на информационно-поисковый, происходит формирование поискового образа, который состоит из ключевых слов и метаданных. К метаданным можно отнести информацию, например о дате создания страницы или её географической привязке.

Таблица 3 - Краткая история развития сети Интернет [63]

Год	Число хостов	Событие
1965	2	Соединение первых двух хостов
1967		Дуг Енжельбард создаёт ARPAnet NIC (Network Information Center)
1970	4	В рамках проекта ARPANET объединены 4 компьютера
1971		Пегги Карп вводит понятие «host mnemonics» – Интернет-имена (RFC 226), появление файла hosts.txt
1972		hosts.txt Сендфордского исследовательского института – центральное хранилище имен. Появление электронной почты
1973		Разработан стек протоколов TCP/IP
1975	100	ARPANET переведена из разряда экспериментальной сети в рабочую сеть
1980	200	Первые мысли Тима Бернерса Ли о World Wide Web
1981		Дэвид Миллс – концепция одноуровневых доменов для адресов электронной почты (RFC-799)
1982		Джон Постель и Зау-Зинг Су. Концепция иерархического пространства доменных имен (RFC-819)
1983		Пол Макапетрис – современная система DNS (RFC-882,883), стек протоколов TCP/IP
1985	2000	TCP/IP – базовый стек NSFNET, зарегистрировано первое доменное имя Symbolic.com
1986	5000	В США на основе ARPANET была создана сеть Национального научного фонда
1987	10000	Профессор Цянь Тяньбай впервые отправил email из Китая
1989	100000	Тим Бернерс Ли «World Wide Web» для Церна
1990	200000	NSFNET заменяет ARPANET, первые серверы http
1992		Домен SU
1993	2700000	Появление Web Browser Mosaic. Впервые выделено адресное пространство для работы в России
1994	5800000	Появление WebCrawler
1995	14000000	Появление AltaVista. Появление первых метапоисковых машин
1996	22000000	Создание архива Интернета Archive.org
1997	30000000	Создание Yandex
1998	43000000	Создание Google. Создание почтового сервиса Mail.ru
1999	72000000	Появление вирусов способных массово заражать компьютеры
2000	104000000	Пузырь доткомов. Количество интернет поисковиков исчисляется десятками.

Краткую историю развития интернета можно увидеть в таблице 3. Ту часть интернета, которая не проиндексирована, обычно называют невидимый (глубокий, скрытый) веб. Появление таких скрытых зон происходит по следующим причинам:

– страницы, динамически создаваемые по запросам пользователей не индексируются;
– базы данных имеющие собственный поисковый интерфейс не индексируются;
– поисковые роботы индексируют страницы переходя по ссылкам, если на страницу не ведёт ни одна ссылка или её не внесли в очередь на индексирование вручную, то она не может быть найдена поисковиком;
– доступ к странице ограничен её владельцем, например требуется пароль;
– некоторые форматы веб страниц или файлов не индексируются (javascript, flash);
– страница может быть не проиндексирована, потому что алгоритм поисковика не счёл нужным её индексировать или она заблокирована.

По мнению разных авторов к видимому интернету относится порядка 20-30% содержимого сети. Самые смелые источники называют цифру не более 50%. Таким образом, можно утверждать, что невидимый интернет – это основная часть ресурсов, доступных онлайн [69].

И это не говоря о таком явлении как тёмный веб - это сетевые ресурсы напрямую не доступные из сети Интернет. Их работа может обеспечиваться тремя способами:

1) Построение своего интернета – Netsukuku project [72];
2) Децентрализация – BitTorrent [61];
3) Оверлейные системы - I2P [10], Tor [20], Freenet [30].

К наиболее популярным в России поисковым движкам относятся Yandex, Google, Mail.ru. В Америке так же популярны Yahoo и Bing. В Китае лидером является Baidu. Большинству обывателей этого количества вполне достаточно, хотя многие пользователи вообще ограничиваются одним поисковиком, к которому привыкли. В большинстве случаев, процесс поиска

происходит путём введения вопроса «как он есть» в поисковую строку, с последующим пролистыванием поисковой выдачи. Во всех современных поисковых системах уже внедрены элементы семантического поиска, что значительно облегчает обработку таких запросов. Но для более точных результатов, необходимо использовать форму расширенного поиска и применять язык поисковых запросов, это способно значительно улучшить результаты. Стандартный список документированных операторов можно посмотреть на сайтах поисковиков в разделе справки, список же недокументированных операторов приведён в приложении Д [46].

Нужно так же отметить что поисковая выдача, например на yandex.ru и yandex.com может отличаться в зависимости от запроса. Яндекс из доменной зоны *ru* будет выдавать результаты больше ориентированные на российскую аудиторию, в то время как Яндекс из доменной зоны *com* будет в большей степени ориентирован на международную аудиторию, это же справедливо и для других поисковиков. Например, при поиске информации о компании из другого региона, для получения более широкого спектра информации необходимо использовать в том числе и локальные поисковые машины других стран. Список поисковых машин разных стран мира [119].

Так же на результаты поиска будет оказывать влияние ваш ip адрес и компьютер с которого вы заходите. Так ip адрес как минимум будет указывать на географическую зону из которой вы заходите на сайт, что соответствующим образом отразится на поисковой выдаче. А использование файлов cookies позволит сайту идентифицировать ваш компьютер при следующих сессиях и запоминать вашу поисковую историю. Обычно компании ссылаются на то, что это позволяет им улучшить качество поисковой выдачи, но в первую очередь это позволяет лучше нацеливать рекламу исходя из ваших поисковых запросов. Персонализация результатов поиска возможно и идёт на пользу простым пользователям, но в сфере КР она приводит к обратному эффекту, так как создаёт «поисковый пузырь» вокруг пользователя, ограничивая его выдачу исходя из собственных

алгоритмов. Например Google учитывает какие сайты вы посещали, что искали до этого, какие ленты читаете и многое другое, к 2014г. он использует около 57 видов персонализации (индивидуализации) – ваших параметров, которые обработает поисковик. Так же не стоит забывать, что в ноябре 2014 года, суд города Сан Франциско вынес решение, по которому компания Google может управлять своей поисковой выдачей без ограничений, что означает что результаты автоматического алгоритма ранжирования могут быть изменены принудительно по усмотрению компании и это как минимум скажется на местах, которые будут занимать сервисы конкурентов в поисковой выдаче. В этом вопросе Поиск@Mail.Ru пошёл ещё дальше и позволил веб мастерам самим влиять на процесс ранжирования их сайтов.

Для обеспечения минимального уровня защиты от персонализации необходимо отключить сохранение истории в браузере, а так же включить опцию «не отслеживать меня», кроме того существует множество плагинов способных усилить вашу анонимность [26]. Можно использовать поисковики которые не отслеживают пользователей, такие как: DuckDuckGo, Ixquick, Privatelee. Ну а для максимального эффекта лучше использовать VPN (Virtual Private Network) [18]. Что в прочем не гарантирует полной анонимности, так как весь трафик пишется на стороне провайдера государственными системами технических средств, предназначенных для обеспечения функций оперативно-розыскных мероприятий. Согласно Приказу № 130 от 25.07.2000 г. Министерство Российской Федерации по Связи и Информатизации, для проведения оперативно-розыскных мероприятий на электронных телефонных станциях, центрах коммутации систем подвижной и беспроводной связи, а также системах персонального радиовызова общего пользования, находящихся в эксплуатации и вводимых в эксплуатацию, на сетях электросвязи, входящих в состав взаимоувязанной сети связи Российской Федерации, независимо от форм собственности и ведомственной принадлежности, должны устанавливаться технические средства для обеспечения оперативно-розыскных мероприятий. Кроме того, премьер-

министр Дмитрий Медведев подписал 31 июля 2014г. постановление правительства №743, уточняющее закон о блогерах. В нём говорится о взаимодействии спецслужб и «организаторов распространения информации» — так в законе называют социальные сети, форумы и любые сайты для общения, доступные всем пользователям интернета. Согласно постановлению, сайты должны подключать оборудование и программное обеспечение для силовиков согласно плану мероприятий, разработанных ФСБ. Это постановление запрещает сайтам раскрывать «организационные и технические приемы проведения оперативно-розыскных мероприятий».

Помимо привычных для нас поисковых машин, таких как Google и Yandex, существует много других поисковиков созданных под различные цели. Некоторые из них специализируются на соц. сетях, другие на поиске по патентам, третьи на научных данных, направлений огромное множество. И несмотря на то, что ведущие поисковики используют технологическую базу в сотни раз мощнее, знать и уметь пользоваться «малыми поисковиками» необходимо. Под этим термином понимаются не только узкоспециализированные поисковые машины с собственной поисковой технологией и индексом, но и различные модификации популярных поисковиков, а в некоторых случаях они могут представлять собой закрытые каталоги, а содержащаяся в них информация, в принципе не попадает в обычные поисковики, ввиду их технологических особенностей. В качестве примера можно привести поисковую систему по химическому кластеру ChemIndustry [109] или ресурс корпоративной сети библиотек Урала «CONSENSUS OMNIUM» [112]. Мы не будем описывать все возможности разных поисковых машин, тем более что на данный момент в мире существует более 1700 различных поисковиков [39] и перечислить их все в данной работе не представляется возможным. Помимо классических поисковиков с постраничной выдачей, наибольшее распространение по способу обработки и представления результатов получили визуально ориентированные кластерные поисковики, а по способу получения и

обработки информации, метапоисковые машины и системы федеративного поиска.

Кластерные поисковые машины отличаются от обычных поисковиков тем, что результаты поиска выдаются не стандартным списком, а проходят предварительную обработку с последующей группировкой. Система проводит анализ подобранных ресурсов и находит на них дополнительные ключевые слова, встречающиеся вместе с терминами из поступившего запроса. Полученные в результате такого анализа подмножества страниц с большой долей вероятности связаны тематически и относятся к разным аспектам темы запроса. Далее происходит определение релевантности ссылок и их позиции в результатах поиска. Кластерная машина проделывает эту операцию отдельно для каждого кластера. При этом ссылки со страниц одного кластера, то есть аналогичной или похожей тематики, ценятся выше, чем ссылки с посторонних, пусть даже очень популярных ресурсов. Таким образом, позиция сайта прошедшего кластеризацию более точно отражает его полезность для пользователя и позволяет вытащить релевантные, но не оптимизированные ресурсы наверх. Визуально ориентированные поисковики обычно представляют собой по сути те же кластерные поисковые машины, но с упором на визуальное представление результатов. Как например поисковик Quintura [118].

Метапоисковые машины обычно не занимаются самостоятельным сбором информации, а отсылают ваш запрос сразу на несколько поисковых серверов, объединяют результаты поиска, производят их дополнительную обработку и выдают обобщенный ответ. В некоторых случаях это способно улучшить результативность поиска за счет охвата различных баз данных и сэкономить время, которое пришлось бы потратить на личное обращение ко всем нужным серверам. Примеры метапоисковых машин можно увидеть по ссылке [48]. Проблема сортировки и дополнительной обработки результатов метапоиска стоит даже более остро, чем в случае отдельного поисковика. Неудивительно, что интерес к кластерным технологиям пришел и в эту

сферу. Идея "скрестить" две технологии — метапоиск по интернет-ресурсам и механизмы кластеризации результатов, оказалась достаточно удачной. Во-первых, сохраняются преимущества метапоисковиков в части широты охвата ресурсов. Во-вторых, возрастает роль кластерной сортировки результатов такого поиска — ведь именно в такой ситуации проявляются сильные стороны данной технологии, которая нивелирует главные недостатки метапоиска для конечного пользователя — перегрузка информацией, проблемы ранжирования результатов и скудные возможности уточнения запроса. В качестве примера кластерной метапоисковой машины можно привести российскую систему Нигма [97].

Технология федеративного поиска сложнее чем у классических поисковых машин работающих на принципе индексирования (рисунок 20). Поисковые машины федеративного поиска включают в себя программное обеспечение, позволяющее алгоритмически заполнять все веб-формы, с которыми они сталкиваются. В отличие от стандартных поисковых машин, которые имеют общий подход сканирования ссылок с любого веб сайта, федеративные поисковые системы запрограммированы так, чтобы распознавать каждую конкретную форму поиска на конкретном сайте. При этом специализированное программное обеспечение не только позволяет заполнять формы и имитировать нажатие кнопки «Поиск» на сайте, но и получать выдачу поисковых результатов (рисунок 21).

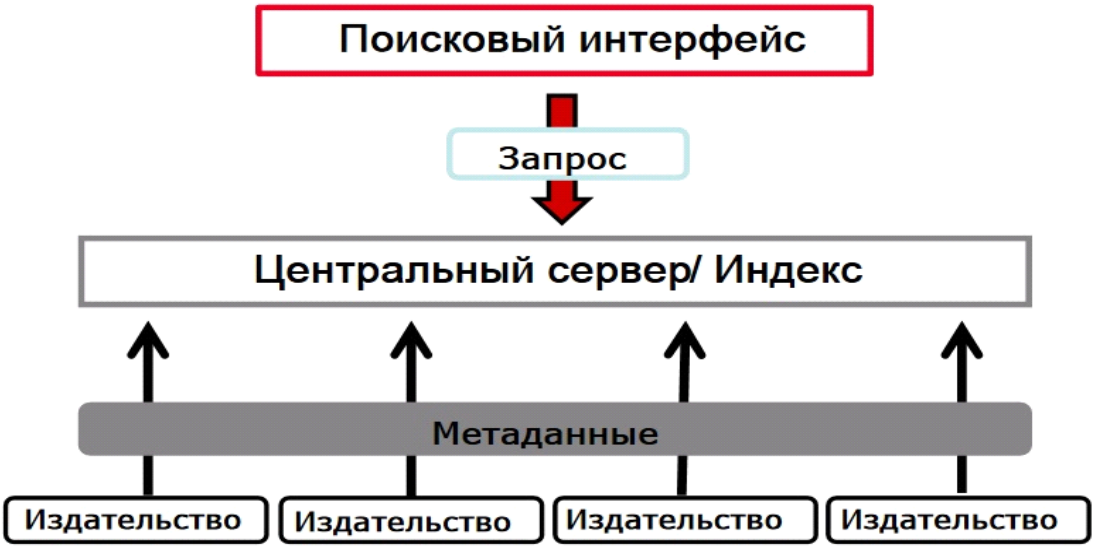

Рисунок 20 - Схема работы индексного поиска [38]

Существенные преимущества федеративного поиска для пользователей включают эффективность, качество поисковых результатов, их актуальность и релевантность контента. Технологии федеративного поиска показывают наилучшие результаты при поиске по обширным базам, таким, как ресурсы исследовательских центров, библиотек, корпораций и государственных ресурсов.

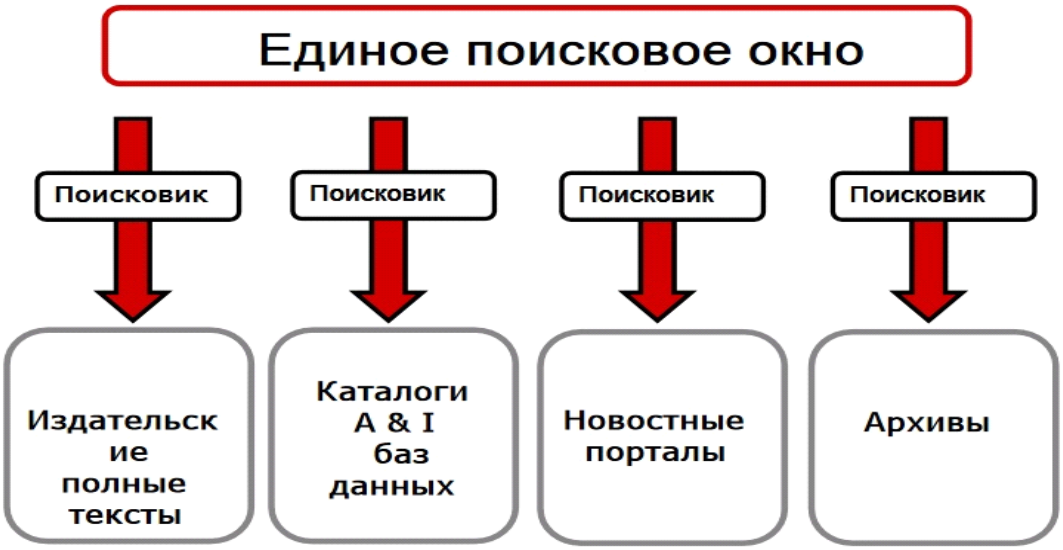

Рисунок 21 - Схема работы федеративного поиска [38]

Основное различие между федеративной поисковой системой и стандартной поисковой машиной типа Google заключается в том, что пользователь федеративной поисковой машины сам выбирает источники для поиска. Почти в каждом случае источник будет максимально авторитетным.

Именно авторитет источника и является основным критерием попадания его в список баз, с которым работает федеративный поиск. Еще одним важным преимуществом федеративного поиска является то, что он ищет контент в режиме реального времени. Данные в реальном времени имеют большое значение для тех исследователей, которые ищут информацию о предмете или событии, которое подвержено частным изменениям. [40]

Отдельно стоит упомянуть о том, что представляет из себя пользовательский поиск. Этот функционал есть у Google [116], а так же был у отечественной системы Flexum, которая к сожалению была закрыта 1 июля 2014 года. Системами пользовательского поиска называются сервисы, которые позволяют самостоятельно определять набор сайтов которые попадают в поисковый индекс. Такие системы особенно эффективны для построения тематических поисковиков и организации поиска по конкретным сайтам. Этот простой функционал позволяет избавиться от главного недостатка простых поисковиков, а именно мусора в поисковой выдаче. Но не стоит забывать, что поиск будет происходить по вашему списку сайтов и будет ограничен ими, хотя при желании в пользовательском поиске Google можно включить функцию - искать во всем Интернете, предпочитая включенные сайты. Так же нужно отметить, что в пользовательском поиске Google используется его индекс, который на данный момент является крупнейшем в мире, но не единственным. Исходя из этого, этот инструмент стоит применять в областях, где интересующий вас вопрос полностью изучен и список релевантных сайтов сформирован.

Ещё одной технологией прочно вошедшей в обиход специалистов по мониторингу и КР является семейство XML-форматов. Изначально эта технология была разработана для описания лент новостей, анонсов статей, изменений в блогах и т. п. Самыми популярными на сегодня XML стандартами являются RSS и Atom, они описывают потоки родственной информации, так же называемые - фиды (feed). Фиды состоят из нескольких элементов, каждый с определённым набором метаданных, условно фид

можно разделить на две значимых части, первая относится к описанию фида, представлению информации о самом канале, а вторая часть состоит из списка статей, новостей или любой другой информации представленной на сайте. Пионером в области внедрения RSS стала компания Netscape в конце 90-х, она использовала её для наполнения информационных каналов своего портала Netcenter. В ходе развития RSS появилось несколько его основных форматов:

- Rich Site Summary (RSS 0.9x) — обогащённая сводка сайта;
- RDF Site Summary (RSS 0.9 и 1.0) — сводка сайта с применением инфраструктуры описания ресурсов;
- Really Simple Syndication (RSS 2.x) — очень простой сбор сводной информации.

В 2006 г. появился Atom, основной конкурент формата RSS, являясь более продвинутым форматом, он учёл многие из недостатков своего предшественника. Atom активно продвигался крупными технологическими компаниями, в том числе и Google, который позже разработал собственный формат GData. Удобство и простота RSS и Atom позволила им быстро набрать популярность среди ведущих новостных сайтов. А с появлением программ агрегаторов (программы-сборщики), появилась возможность собирать все интересующие публикации вместе, а так же одновременно следить за появлением новых материалов на всех профильных сайтах сразу и читать их краткое содержание, не посещая каждый из этих сайтов по отдельности, разумеется если эти сайты поддерживают RSS. В случае если сайт не имеет собственного RSS потока, эту проблему можно попробовать решить при помощи сервисов наподобие Скиур [12]. Агрегаторы условно подразделяются на три группы: онлайновые, встроенные и программные. Задачи у них одинаковые, получение обновлений из интересующих пользователя RSS-потоков.

Онлайн агрегаторы предоставляют доступ к своим сервисам посредством веб интерфейса и расположены на каком-либо сервере в

Интернете. Популярные в России онлайновые сборщики связаны с поисковыми системами Yandex - Яндекс.Лента и Google - Google Reader (сервис закрыт). Одной из особенностей сервиса Яндекс, является то, что пользователь имеет возможность создавать потоки по интересующим его поисковым запросам, что очень удобно при регулярном мониторинге интересующей темы. Отдельно стоит упомянуть о сервисах предоставляющих графический пользовательский веб интерфейс, позволяющий обрабатывать и накладывать всевозможные фильтры на ленты новостей, на выходе получая совершенно иной, информационный продукт. Одним из известных сервисов, предоставляющих подобный функционал, является Yahoo! Pipes [121].

Встроенные агрегаторы представляют из себя встроенный в другую программу функционал по работе с RSS потоками. Например, практически во всех современных браузерах уже есть встроенные RSS агрегаторы, при желании эти возможности могут быть расширены при помощи соответствующих плагинов. Так же во многих современных почтовых клиентах есть подобный функционал.

Программы агрегаторы представляют собой программный продукт, специально написанный для работы с RSS потоками, этот софт требует полноценной установки на компьютер пользователя. Обычно такие программы предлагают более широкие возможности по управлению и фильтрации RSS потоками.

Задача мониторинга сайтов на самом деле шире, чем это может показаться на первый взгляд. Конечно, использование RSS способно помочь в этом, но только отчасти и причин тому может быть несколько. Во-первых, не вся интересующая нас информация попадет в RSS потоки. Во-вторых, не на всех сайтах в принципе есть RSS или Atom. В-третьих, часть информации может находиться на скрытых сегментах сайта. Использование RSS занимает небольшую долю в инструментарии специалистов КР ввиду ограничений накладываемых самой технологией.

Отслеживать в ручном режиме изменения на небольшом количестве сайтов в принципе реально, но если их количество и интенсивность изменений начинает расти, то эффективность подобного метода работы становится под вопросом. В связи с чем, возникает логичная потребность в автоматизации подобных рутинных задач. Если количество интересующих сайтов не очень большое, то проблему мониторинга изменений вполне можно решить при помощи специальных плагинов для браузеров. Примерами таких плагинов для браузера FireFox могут являться UpdateScanner или SiteDelta. Но если у вас большое количество сайтов, которые необходимо отслеживать, то для более системной работы необходимо использовать полноценные программы, способные отслеживать и рубрицировать все изменения на интересующих сайтах. Примером таких программ могут выступать Check&Get или Web Site Watcher.

Но наибольший интерес представляют комплексные программные продукты, способные решать широкий спектр задач по автоматизации поиска и рубрикации информации, а так же способные дать дополнительные инструменты для её анализа. Наиболее продвинутыми на российском рынке являются такие программы как СайтСпутник [100], Аваланч [92], Семантический архив [101]. Каждая из этих программ как стандартный функционал встречающийся у конкурентов, так и свои специфические возможности.

Предназначение и функционал программы "СайтСпутник" (SiteSputnik). Основное предназначение этой программы заключается в метапоиске с последующим устранением дублей и мониторинге интересующих вас объектов в сети интернет. Конечно возможности СайтСпутник будут зависеть от версии программы (Pro, Objects, News, Comments, WebSpider, Station, Invisible, Contacts, Corp). Основной функционал представляет из себя следующие функциональные блоки:

Поисковые возможности и обработка результатов.

Метапоиск - выполнение поискового запроса одновременно на нескольких источниках на заданную глубину поиска для каждого из них. Возможен метапоиск как по встроенным поисковикам (Яндекс, Google, Yahoo, Bing, Поиск@Mail.Ru, блоги Яндекса и Google), так и по подключенным вами средствам поиска.

Работа с несколькими поисковиками происходит с использованием единой формы. Простые запросы на универсальном языке СайтСпутник транслируются на языки запросов встроенных поисковиков.

Дубли найденных ссылок удаляются. Есть функция аналитического объединения результатов поиска, что позволяет объединить результаты различных поисков в единую выдачу, причем первыми ссылками в выдаче будут те ссылки, которые были найдены большим количеством поисков. Аналитическое вычитание позволяет из результатов одного поиска убрать результаты другого поиска.

Кроме того программа способна выполнять метапоиск по заданному сайту, а так же в офисных документах и кэш-копиях ссылок.

Имеется функция глубокого поиск для Яндекса, Google, что позволяет объединить в один список все ссылки из обычного поиска и все ссылки из разделов "Еще с сайта", "Дополнительные результаты с сайта" и "Искать на сайте (Всего ...)".

Поиск в невидимом интернете. Этот функционал реализуется при помощи нескольких методов:

- поиск невидимых ссылок при помощи спайдера (поискового робота),
- поиск невидимых ссылок в окрестности видимой ссылки или папки по "образу и подобию",
- специальный поиск открытых папок,
- поиск невидимых ссылок и папок со стандартными именами с использованием специальных словарей.

Мониторинг и рубрикация потоков информации.

Мониторинг на предмет появления в интернете новых ссылок по заданной теме. Мониторить появление новых ссылок можно при помощи целых пакетов запросов, в которых задействованы любые упомянутые выше методы поиска.

Мониторинг новостных потоков, формирование собственных новостных лент. Это происходит в два этапа: синтез и анализ информационного потока. Синтез потока, содержащего части нужной информации, осуществляется не только из имеющихся на сайтах RSS-потоков, но и из встроенных в сайты поисков и с эмулированных RSS-потоков с произвольных веб-страниц. Анализ сформированного потока осуществляется при помощи рубрикатора, который обеспечивает автоматическое раскладывание контента новостей по темам и формирование полнотекстовых тематических новостных лент.

Мониторинг комментариев позволяет сформировать и рубрицировать потоки комментариев к сообщениям из новостных потоков, описанных в предыдущем абзаце.

Мониторинг изменений на сайтах наблюдает за обновлениями уже существующих страниц, а именно, за появлением на них новой информации, удовлетворяющей запросам, заданным Пользователем (рубрикация обновлений).

Клиентские папки. Их применение позволяет сотрудникам предприятия разных подразделений по одному клику мышки получать новую информацию по своей специализации по факту её появления в открытых источниках интернета. Реализована автоматическая e-mail рассылка тематических новостных лент, отправка их в локальные папки компьютера и папки сайта.

Мониторинг на веб-страницах на предмет обнаружения изменений в их контенте. Найденные изменения выделяются цветом и специальными знаками.

Функции анализа информации.

Правила попадания в рубрики позволяют указывать ключевые слова и расстояние между ними, задавать логические "И", "ИЛИ" и "НЕ", применять одноуровневую скобочную структуру и словари (файлы-вставки), к которым можно применять логические операции.

ВФ-технология - практически произвольное расширение возможности рубрикации материалов посредством реализации внешних функций. Могут быть реализованы программистом самостоятельно без участия автора программы.

Анализ заполняемости Рубрик, установка сигнализации и оповещение о наступлении значимых событий посредством выделения цветом Рубрик и/или отправки по e-mail отчета о срабатывании сигнализации.

Фактическая релевантность. Существует возможность упорядочить ссылки в порядке близком со значимостью этих ссылок по отношению к решаемой задаче, воздействие SEO приёмов значительно снижается. Это достигается на основе анализа результатов выполнения нескольких "разноплановых" запросов на заданную тему. Вычисляются, в прямом смысле этого слова, ссылки, содержащие максимум искомой информации.

Вычисление связей объектов - поиск ссылок, ресурсов (площадок), папок и доменов, на которых одновременно упоминаются объекты. Для поиска связей могут быть задействованы все упомянутые выше средства программы СайтСпутник, что значительно повышает эффективность работы. Операция может выполняться над любым количеством объектов.

Формирование, объединение и пересечение потоков информации на самые различные темы, сопоставление потоков.

Построение веб-карт сайтов, ресурсов, папок и искомых объектов на основе найденных в интернете при помощи поисковых ссылок, принадлежащих сайту. Это позволяет определить какая информация видна из интернета на их сайтах, а также исследовать на этот предмет сайты конкурентов. Веб-карта сайта - это материализация видимого интернета.

Поиск контактной информации предприятий в открытых источниках. Список предприятий может быть любой длины. Контактная информация: адрес, номера телефонов и факсов, e-mail.

Поиск новых источников информации на заданную тему, которые затем можно применить для отслеживания появления новой нужной информации.

Сервисные функции.

Планировщик задач (Scheduler) обеспечивает работу по расписанию, выполняет в заданное время заданные функции программы.

Инструктор проектов - это помощник при создании и сопровождении проектов по поиску, сбору, мониторингу и анализу информации (рубрикации и сигнализации).

Автоматическая архивация. В базах данных автоматически запоминаются все результаты работы, а именно: запросы, пакеты запросов, протоколы поиска и мониторинга, любые другие вышеперечисленные функции и результаты их выполнения. Можно структурировать работу по темам и подтемам.

База данных включает сортировки, простой поиск и произвольный поиск по SQL-запросу. Для последнего имеется мастер составления SQL-запросов. Используя эти средства, можно найти и ознакомиться с той работой, которую делали вчера, в прошлом месяце, год назад, определить в качестве критерия поиска тему или задать другой критерий поиска по содержанию базы данных.

Технические ограничения поисковиков. Некоторые ограничения, связанные, например, с длиной строки запроса, могут быть преодолены. Обеспечивается выполнение не одного, а нескольких запросов с объединением результатов поиска или раздельно. Для одного слова или одной фразы, взятой в кавычки, реализован поиск в поисковиках с учетом регистра, в частности, поиск по аббревиатуре. Имеется инструмент для сравнительного анализа выдачи поисковиков.

Встроенный браузер. Навигатор по страницам. Многоцветный маркер для выделения ключевых и произвольных слов. Билистинг и N-листинг из сформированных документов.

Выгрузка новостных лент в табличное представление, ориентированное на импорт в Excel, MySQL, Access, Кронос и другие приложения.

Коллективная обработка информации. Создание корпоративной или профессиональной сети для коллективного сбора, мониторинга и анализа информации. Участниками и создателями такой сети являются сотрудники корпорации, члены профессионального сообщества или группы по интересам. Географическое расположение участников не имеет значение.

Мониторинг на нескольких компьютерах. Круглосуточный мониторинг источников информации (сайтов) с использованием нескольких компьютеров.

Предназначение и функционал программы "Аваланч" (Avalanche). Основное предназначение этой программы заключается в мониторинге сети интернет, на предмет интересующих вас объектов, с последующим распределением найденной информации по "умным папкам". Функциональность программы будет меняться в зависимости от версии программы. В настоящее время существует несколько основных версий программы, это версии 2.5 и 2.7 и SaaS (soft as a service) версия технологии Avalanche под названием «Лавина-Пульс» [95]. Если говорить про версии 2.5 и 2.7, то основной функционал у них будет выглядеть следующим образом:

Поисковые возможности и обработка результатов.

Использование поискового агента - специальной программы, способной в автоматическом режиме самостоятельно перемещаться по гиперссылкам в интернет пространстве и собирать документы.

Использование специальных алгоритмов анализа документов на предмет их соответствия области (тематике) поиска.

Осуществление поиска по «невидимому» интернету (то есть поиск страниц, которые не видны для ИПС).

Возможность задания регламента обхода источников, а так же возможность настройки авто регламент.

Быстрый полнотекстовый поиск по базе.

Автоматическое скрытие нечетких дублей новостей.

Программа обладает гибкими настройками параметров поиска, что позволяет осуществлять накопление информации и хранить ее в форме информационных карточек.

Предоставление возможности ведения и внесения изменений в карточки (досье) для объектов мониторинга.

Мониторинг и рубрикация потоков информации.

Автоматизированный мониторинг различных внешних информационных ресурсов, в том числе RSS лент, форумов и поисковых систем (Google, Yandex, Mail, Yahoo, Bing).

Автоматизированный мониторинг социальных сетей (Вконтакте, Фейсбук, Твиттер, Одноклассники, Livejournal, LiveInternet, Мой мир, Яндекс.Блоги)

Сбор, рубрикацию, хранение в централизованной базе данных, подготовку и представление для анализа больших объемов текстовой информации о любых заданных объектах поиска.

Автоматизированный сбор данных из социальной сети «ВКонтакте» в карточки объектов мониторинга.

Быстрый полнотекстовый поиск по объектам мониторинга.

Возможность прикрепления различных документов (файлов) к конкретному объекту мониторинга.

Расширяемый набор типов объектов мониторинга.

Функции анализа информации.

В комплексе реализован механизм автоматизированного нахождения связей между объектами, субъектами и т.п. и графическая визуализация диаграмм и связей.

Предоставление собранной информации в разрезе источников, в разрезе рубрик (предметов или объектов исследования), а также в контексте объектов мониторинга в виде карточек персоны, организации, события и т.д.

Возможность фильтрации рубрицированных новостей по тематике, источнику и дате, а также возможность подсветки ключевых слов.

Возможность построения связей между объектами мониторинга с графической реализацией.

Генерации готовых отчетов по объектам мониторинга.

Технология Avalanche позволяет не только собирать HTML-документы, но и выявлять в них смысловой контент (т.е. текст самого сообщения - из HTML-документа удаляется все, что не относится к смыслу документа: баннеры, меню, ссылки на другие материалы…) и некоторые атрибуты (например, заголовок документа, дата и время его публикации).

Сервисные функции.

Программные решения Avalanche имеют открытую архитектуру, что позволяет в достаточно короткие сроки оснащать дополнительными инструментами вашу систему. В зависимости от потребностей пользователя система может развиваться в том или ином направлении, позволяя дополнять новыми сервисами и возможности.

Работа по заранее заданному расписанию.

Возможность экспорта/импорта настройки источников на(с) диск(а), между проектами.

Возможность многопользовательской работы, и разграничение прав доступа к проектам.

Предназначение и функционал программы "Семантический архив" (Semantic Archive). Основное предназначение этой программы заключается поиске информации в сети, мониторинге интернет ресурсов и составлении семантической базы. Актуальной на текущий момент является версия 4.5, а SaaS версия находится в стадии бета-тестирования. Основной функционал можно представить в следующем виде:

Поисковые возможности и обработка результатов.

Обширный список поисковых роботов настроенных как для работы с классическими поисковиками, так и с социальными сетями и отдельными гос. сайтами.

Эмуляция действий реальных пользователей в поисковых формах онлайн баз и извлечение найденных результатов в базу данных «Семантического архива».

Сквозной поиск. Поиск объектов интереса – компаний/персон с учетом синонимов, сокращений, аббревиатур одновременно в большом количестве сайтов, онлайн базах, поисковиках, социальных сетях в режиме реального времени.

Возможность делать поисковые запросы через шлюзы, в такие системы как СПАРК и Интегрум.

Широкие возможности по подключению дополнительных источников информации.

Сквозной поиск по внутренним базам.

Мониторинг и рубрикация потоков информации.

Широкие возможности по настройке мониторинга новостных сайтов, блогов, форумов, а так же любых других типов сайтов. Сбор новостей с использованием RSS-каналов, так и без них.

Автоматическое извлечение данных с веб-сайтов и сохранение их в удобном виде в базу системы «Семантический архив». Парсинг сайтов, таблиц, форм, данных документов на сайтах.

Постановка интересующих вас объектов на мониторинг, с последующим автоматическим добавлением выявленных объектов, фактов и связей между ними.

Использование фильтров для отбора новостей по ключевым словам. Подсветка искомых фраз прямо в модуле.

Возможность оперативного ручного добавления объектов и фактов, а так же источников в систему при помощи модуля УДОФ.

Функции анализа информации.

Возможность автоматического извлечения объектов и фактов из документов.

Существует возможность увидеть события и объекты в привязке к географическим координатам. Полученное изображение может быть сохранено.

Автоматическое выделение реквизитов документа (источник, URL, авторы и т.д.).

Настраиваемая онтологическая модель.

Визуализация семантической сети в виде: стратегической семантической сети, дерева, графа, последовательности фактов, поиска цепочки связей, стратегической сети по различным срезам, использование слоёв данных и др. Возможность быстрой выгрузки в Visio для последующей доработки.

В основе работы с семантическими сетями лежит один из известных методов анализа - Визуальный Анализ Данных (VAD - Visual Analysis Data).

Построение графиков упоминания объекта в СМИ и блогах.

Генерация аналитических отчётов с использованием большого количества шаблонов в формате doc, pdf, rtf, html и др.

Создание дайджеста статей.

Сервисные функции.

Имеет модуль подключения дополнительных компонентов SDK (software development kit), что позволяет силами собственных программистов расширять функционал программы.

Программа позволяет хранить информацию портированную из различных реляционных баз данных.

Возможность настроить мониторинг интернет источников по расписанию. Много поточность выполняемых задач.

Возможность обмена настроенными заданиями на новостные или поисковые сайты между пользователями.

Сохранение в системе всех поисковых задач. Всегда можно проследить, как работал пользователь, что искал и какие результаты были найдены в конкретной поисковой сессии.

Сохранение результатов в виде файлов на жесткий диск или базу SQL или в базу ИАС "Семантический архив".

Есть возможность подключения автоматической антикапчи.

Как видно из приведённого в этом параграфе инструментария, он может быть использован различными службами и не является чем то уникальным, присущим только подразделениям КР. Но специалист с продолжительной практикой использования, знанием нюансов работы и глубоким пониманием сути исследуемого вопроса, способен сделать компьютерную программу или простой поисковик, настоящим инструментом КР. Так же без способности анализировать и строить гипотезы, собранная информация представляет из себя лишь разрозненный набор событий, фактов, слухов и т.д. При нестандартном подходе, инструментом КР может стать и не предназначенный для этого на первый взгляд сервис. Например babo.com представляющий из себя платформу для взаимодействия новостных агентств и очевидцев события, при определённых условиях может стать интересным источником информации.

3.2 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, КАК ИНСТРУМЕНТАРИЙ СЛУЖБЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Инструментарий применяемый СБ в своей работе достаточно обширен, он включает в себя как оперативные, так и аналитические методы. Мы же сконцентрируем наше внимание в этой главе на информационных технологиях, развитие которых помогло автоматизации некоторых направлений деятельности СБ. В большей степени это относится к проверке контрагентов и физических лиц, что в свою очередь хорошо отражает разницу в подходах работы между СБ и КР.

Стандартная технология проверки контрагентов включает в себя сбор и анализ информации по контрагенту на предмет возможных рисков, которые можно разбить на 4 основные группы:

- Работа с контрагентами созданными в мошеннических целях.
- Работа с контрагентами несущими налоговые риски.
- Работа с контрагентами с неустойчивым финансовым положением.
- Работа с контрагентами аффилированными с работниками компании.

Каждая из обозначенных групп требует проверки и анализа своего блока информации, большая часть которой доступна в открытых источниках. С появлением интернета, онлайн доступ к официальным источникам информации значительно облегчил и ускорил процесс проверки контрагентов. Активное развитие централизованных сервисов ФНС, ФССП, Арбитражного суда, помогло значительно сократить время сбора необходимой информации для СБ. Но вместе с тем, эти сервисы до сих пор не лишены и своих недостатков, основными из которых являются:

- сбои в работе ресурса;
- временные задержки при публикации информации;
- неполная или неточная информация.

Так например в картотеке арбитражных дел, для более полного результата необходимо провести поиск по 3 атрибутам: ИНН, ОГРН, название юр. лица. Связано это в первую очередь с качеством введения первичной информации в систему в самих арбитражных судах. Кроме того треть судебных решений по гражданским делам публикуются на сайтах районных судов с опозданием, около 20% не публикуются вообще. Публикуется около 93% от общего количества решений по уголовным делам, с опозданием — 23%. Мировые судьи публикуют чуть 56% своих решений по гражданским делам и 67% актов по делам об административных правонарушениях. Таковы результаты обобщения практики исполнения судами в 2013 г. и первом полугодии 2014 г. требований федерального закона

об обеспечении доступа к информации о деятельности судов, следует из справки Судебного департамента [36].

Ещё в качестве примера можно привести сайт ФМС и их сервис по "проверке паспорта" [98]. В марте 2014 года, ЦБ и Росфинмониторинг ввели требование по проверке паспортов клиентов банков на сайте ФМС, внеся изменения в положение «Об идентификации кредитными организациями клиентов и выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма». Банки должны проверять на подлинность паспорт при идентификации клиентов в рамках любых операций, включая открытие вклада, выдачу кредита, обмен валюты и денежные переводы (по двум последним операциям — на сумму свыше 15 тыс. рублей). За неисполнение требований регулятора предусмотрены штрафы: сотрудники банков могут быть оштрафованы на 10–30 тыс. рублей, а сам банк — на 50–100 тыс. рублей. За время действия этого положения, каждый 10-й клиент кредитных организаций получал отказ в обслуживании по вине сервиса, из-за того что данных его паспорта ошибочно нет на сайте ФМС [8].

Для банковской сферы так же будут особо актуальны кредитные истории потенциальных заёмщиков. Сами кредитные истории аккумулируются в бюро кредитных историй (БКИ). В реестре БКИ, который ведет Центробанк, значится 26 бюро [92]. Большая часть кредитных историй сосредоточена у трёх крупнейших БКИ, это — Национальное бюро кредитных историй (НБКИ), «Эквифакс» (Equifax) и Объединенное кредитное бюро (ОКБ). Кроме того у некоторых банков есть прямой доступ к информации из пенсионного фонда России (ПФР), что позволяет определить официальное место работы потенциального заёмщика, речь идёт о Сбербанке, банке «Уралсиб», Газпромбанке, Банке Москвы и ВТБ24 [7].

Помимо работы с юр. лицами большой пласт работы направлен на проверку физических лиц как при приёме на работу, так и как

потенциальных контрагентов. В большинстве случаев, эту задачу можно разбить на три основных блока:

- Поиск информации о человеке по открытым источникам. Сюда можно отнести официальные гос. ресурсы, а так же результаты, полученные с использованием поисковых движков.
- Поиск профилей человека в социальных сетях. Поиск может производиться с использованием встроенных поисковых возможностей самих соц. сетей. В случае, если необходимы более широкие возможности для анализа, можно использовать специализированные сервисы которых сейчас достаточное количество на рынке, широкий список инструментов можно посмотреть на ресурсе Кена Бербари [108].
- Использование закрытых криминальных баз и сообществ. Хотя использование баз, содержащих информацию о судимостях и прочих правонарушениях в России законодательно ограничено, применение подобных источников информации происходит регулярно. Во многих компаниях применение подобных источников для проверки персонала прямо интегрировано в рабочий процесс. В основном, они представляют из себя разной степени наполненности базы под различными программными оболочками: "Экар", "Марафон", "Фимида" , "Эксперт", "Эгида", "Феникс", "Спрут", "Дофин", "Ариадна", "ИнфоЛоджик", "Проф". Подобная практика так же существует и в западных странах, но она будет сильно зависеть от законодательства отдельно взятой страны. Например в Америке ограничений значительно меньше и получать подобную информацию можно на легальной основе используя такие сервисы как TLOxp, CLEAR, FirstSearch, CollectionAdvantage.

Отдельно стоит упомянут о сообществах СБ которые существуют во многих регионах. Обычно они организованы по типу закрытых клубов, куда можно попасть только по рекомендации после определённой проверки.

Обмен профильной информацией в них происходит по неформальным каналам, что бы защитить себя от лишнего внимания. Современные технологии позволили организовать этот процесс на базе так называемого web 2.0, другими словами это разновидности закрытых социальных сетей профессиональной направленности. Ярким примером такой платформы является система Искра [94]. Подобные сообщества конечно существуют и на иностранных ресурсах, они делают больший упор на образование и аккумулирование опыта, в качестве примера можно привести крупное сообщество Global Risk Community [115] в котором более 19 000 членов.

Ещё одной ступенью развития инструментария СБ является переход от ручного сбора данных из официальных источников к информационно-аналитическим системам работающим по принципу одного окна. В настоящее время выбор таких систем на российском рынке достаточно обширен, но к наиболее популярным можно отнести: СПАРК, Интегрум, Глобас-i, Контур-Фокус, ДельтаБезопасность . Каждая из этих систем имеет как свои плюсы, так и свои минусы. Так же большинство подобных систем генерируют индексы, оценивающие риски работы с конкретной компанией. На первый взгляд подобные инструменты способны ускорить проверку контрагентов, но здесь есть свои подводные камни. В большинстве случаев при формировании подобных индексов используется 2 подхода:

Скоринговый расчёт исходя из некоторой рисковой модели.

У этого подхода есть очевидный плюс, в нем есть простая логика, особенно если можно менять вес коэффициентов. Но в то же время есть и существенные недостатки, например:

– Автоматически достоверно определить количество судебных исков практически нельзя. Не всегда иск определяется номером, часто нужно искать по имени. В этом случае при расширении области поиска до региона, при отсутствии уникального наименования, даёт большое количество совпадений.

– Вопрос массовости адреса регистрации решить автоматически тоже сложно. По одному адресу могут находиться компании холдинга или компании одного владельца в силу особенностей бизнеса. Та же проблема возникает, когда речь заходит о бизнес центрах.
– Иногда источники возвращают некорректную и устаревшую информацию.

При таких исходных данных, даже самая правильная формула может дать неверные результаты. Ровно поэтому, тот кто смотрит на этот интегральный показатель, должен понимать, как он получился и какие существуют ограничения при его расчете.

Расчёт индекса по совокупности схожих факторов.

Эти индексы рассчитываются, не как сумма каких-то показателей, а как степень похожести на хорошую или плохую компанию. Степень похожести определяет не человек, а некая математическая модель распознавания, которая основана на выделенных особенностях фирм, признанных "однодневками" [6] по суду. То есть увидеть индекс можно, но нельзя понять почему он получился именно такой, а не какой-то иной.

Если же говорить о международном рынке, то наиболее крупными и продвинутыми справочными системами здесь являются: LexisNexis, Dun and Bradstreet, Bureau van Dijk, Factiva.

Инструменты применяемые СБ так же обусловлены теми задачами которые приходится решать. Каждодневная работа с показанными выше источниками, позволяет вырабатывать оптимальные алгоритмы проверки с учётом особенностей самих ресурсов. И только совокупность этих инструментов позволяют решать в достаточной мере задачи по проверке контрагентов, что является неотъемлемой частью системы экономической безопасности любой компании. Логика такой работы будет похожей на любом международном рынке, но конечно будет иметь свою специфику.

3.3 Ф ОРМЫ ВЗАИМОДЕЙСТВИЯ КОНКУРЕНТНОЙ РАЗВЕДКИ И СЛУЖБЫ БЕЗОПАСНОСТИ В МЕЖДУНАРОДНОЙ КОМПАНИИ

В предыдущих главах мы показали различия в подходах и задачах решаемых КР и СБ. А так же рассмотрели конкретные прикладные инструменты используемые ими наиболее часто. Как видно из всего выше перечисленного, конкурентная разведка и обеспечение экономической безопасности, это отдельные виды деятельности в структуре компании. В этом параграфе будет проанализирована проблема взаимодействия КР и СБ и рассмотрены различные варианты её решения. Мы попытаемся найти наиболее универсальные подходы, которые могут использовать компании в международном бизнесе.

И КР и СБ в ходе своей работы генерируют значительные потоки информации, которые в дальнейшем оседают в сетевых папках и базах данных компании. Структура и содержание этой информации может быть абсолютно различной, что приводит к тому, что даже руководители служб не всегда представляют реальные объёмы накопленной информации, а отдельно взятый специалист хорошо ориентируется только в кластерах информации сформированных им самим. И если в небольшой компании эта проблема легко решается через простое общение тет-а-тет, то в транснациональной корпорации такой подход слабо применим и нужны какие то системные решения на базе информационных технологий.

Организация служебной базы данных не представляет особой сложности в наше время, на рынке предостаточно соответствующих решений. Но проблема выбора конкретной базы данных, это не только проблема выбора технологического решения. Проблема ещё в том, что даже самая изощрённая база данных не способна в полной мере отразить всё многообразие процессов и взаимоотношений реального мира. Другими словами, перед тем как попасть в базу данных, информация форматируется соответствующим образом, зачастую от неё отсекается всё, что не

вписывается в существующую структуру базы. И получается, что только специалист, занимавшийся каким-то конкретным вопросом сможет полностью восстановить картину, простому же пользователю системы это будет уже недоступно. Другими словами ведение совместной базы данных, может быть использован как вариант взаимодействия КР и СБ, но он несёт в себе определённые недостатки показанные выше. Более прогрессивный подход заключается в использовании не баз данных, а баз знаний и экспертных систем об особенностях работы которых мы писали в предыдущих главах. Например, новое поколение экспертных систем, таких как IBM Watson, уже вполне успешно проводят консультации врачей в области онкологии. Кроме того, есть информация, что система готовится к использованию департаментом внутренней безопасности АНБ и ФБР. Что касается ФБР, то, как заявил, правительственный чиновник Шон Маккарти: «Watson является великолепной аналитической платформой. Детальный скрупулезный анализ огромных массивов данных он может выполнить лучше наших специалистов. Он не будет принимать решения, он будет делать выводы. А конечные решения будут принимать, естественно, люди. Первой областью, где мы собираемся задействовать Watson – это расследование случаев мошенничества» [41]. В настоящее время Watson стал доступен для использования сторонним организациям. Другой вопрос, что далеко не все компании готовы доверять такую чувствительную информацию как разведданные и отчёты по внутренним расследованиям, посторонней организации.

Если же говорить про корпоративные хранилища документов, в которых могут храниться служебные записки, отчёты, доклады подразделений КР и СБ, то поиск в массиве таких документов решается при помощи соответствующего программного обеспечения. Но здесь возникает другая проблема, в любой крупной организации со временем таких документов будет накапливаться огромное количество, что значительно усложнит как сам поиск, так и последующую их обработку человеком.

Другими словами здесь возникнет 3 большие проблемы. Первая, это проблема релевантного поиска нужных документов. Вторая, это большое количество времени необходимое на прочтение и анализ соответствующих документов. Третья, как найти то, о чём ты ещё не знаешь?

Конечно, современные программы для локального поиска значительно продвинулись вперёд и по своему функционалу мало чем отличаются от интернет поисковиков, точнее сказать базовые принципы работы у них те же, и основаны на индексировании. Но проблема в том, что современные поисковые системы не понимают текст, а только анализируют его статистически, опираясь на огромный массив данных. Чтобы добиться понимания, машина должна располагать аналитической моделью, по сложности сопоставимой с моделью самого языка. То есть должна не только различать слова и значения грамматических показателей, но и анализировать синтаксис и, главное, понимать смысл высказывания, накладывая его на культурную модель мира, принятую в конкретном языке [9].

Другими словами проблему релевантного поиска в огромном количестве разнородных документов не решить при помощи старых подходов. При стандартном запросе она просто будет выдавать большое количество документов, что повлечёт за собой дополнительную работу по ручному отсеиванию. Но это не единственная проблема, которую должны решить системы корпоративного поиска нового поколения. Такие программные решения должны обладать целым рядом новых функций:

Интеллектуальный поиск

Переход от морфологии к семантике. При выборе наиболее релевантных ответов на запрос, система должна учитывать не только все формы слов, но и их значения, смысловые связи между словами и контекст употребления.

Извлечение сущностей

Извлечение объектов, событий и связей между ними. Наполнение корпоративной базы знаний.

Классификация документов.

Автоматическое определение типа документа, основываясь на его структуре и содержании.

Выявление дублей.

Отсечение полных дублей документов в выдаче, а так же увязывание частичных дублей друг с другом.

Анализ тональности.

Система должна понимать тональность высказываний содержащихся в документе и маркировать их соответствующих образом.

Многоязычный поиск.

Автоматический сквозной поиск на нескольких языках. То есть при вводе запроса на родном языке, система переводит его на другие языки и так же производит поиск.

Но работа с базами данных или хранилищами документов, это работа со свершившимися фактами, зачастую без контекста. Как оптимально организовать совместную работу КР и СБ так, что бы взаимодействие специалистов было более "живым". Отчасти решить эту проблему помогают технологии Web 2.0 или социального интернета, как его ещё называют. В нашем случае, они должны представлять собой закрытые площадки для совместного общения и обмена информацией в реальном времени, с возможностями обработки и хранения данных. Именно эти возможности, в своё время, привели к бурному росту популярности соц. сетей и бизнес сообщество тоже не осталось в стороне. Ярким примером тому является LinkedIn или более узкоспециализированная соц. сеть [111], созданная на базе Ning. На первый взгляд может показаться что все эти технологии социальных сетей и wiki-справочников несут в себе мало полезного для КР и СБ, но это не так. Именно богатые возможности по созданию контента и взаимодействию и привлекли в своё время американские спецслужбы. Это послужило толчком для создания целой плеяды соответствующих проектов: Intellipedia, Intellipublia, Bureaupedia, DoDTechpedia, Diplopedia, A-Space. По

большей части они представляют собой вики-системы с возможностями по созданию статей, блогов, дискуссионных площадок и вложением различных документов, но не только.

Для частных компаний существует множество решений, которые позволяют организовать внутрифирменное взаимодействие между работниками. Это могут быть как корпоративные порталы созданные на базе MS SharePoint или Liferay, так и более простые и узкоспециализированные продукты вроде Hontza [117]. Но выбор конкретного программного продукта здесь не главное, он будет продиктован структурой и возможностями самой компании. Основные критические моменты, которые будут влиять на эффективность этого инструмента, это взаимное доверие специалистов и контроль доступа к информации. Без взаимного доверия, система не будет наполняться нужной информацией или имеющаяся информация не будет использоваться в работе. Так же должна быть разработана гибкая система получения доступа к нужной информации, которая с одной стороны не будет особо ограничивать, с другой будет чётно контролировать действия пользователя системы. Разные подходы и источники информации объединённые на одной площадке (рисунок 22), способны дать положительный синергетический эффект для компании.

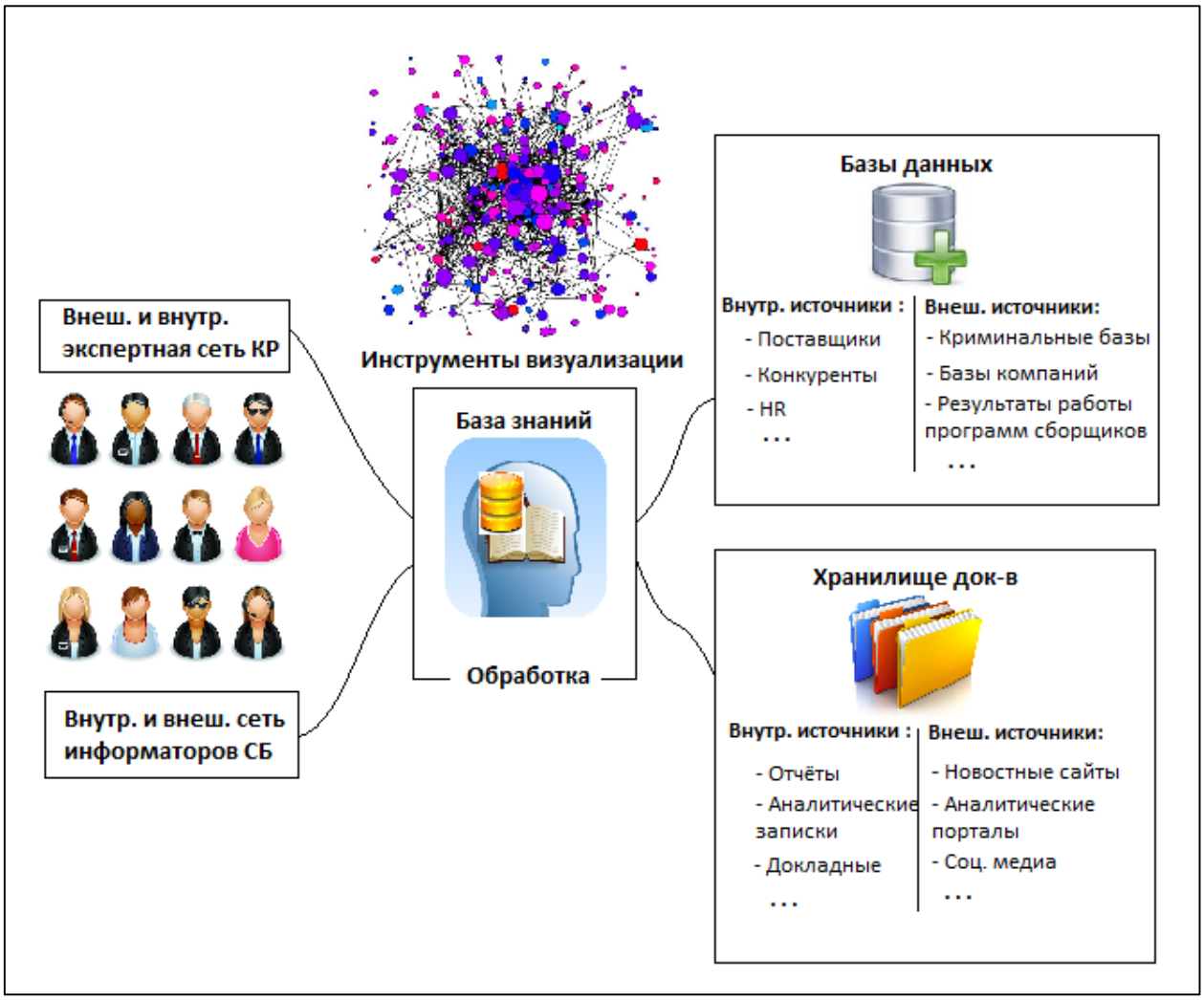

Рисунок 22 - Структура источников информации в рамках взаимодействия КР и СБ [9, 25, 65]

Большую долю работы как в КР, так и СБ составляет работа с людьми или напрямую, или опосредованно. И поэтому невозможно взаимодействие исключительно дистанционное, нужно и личное взаимодействие. Хотя технологии - от Вики до Скайпа практически стирают грань между личным присутствием и дистанционным. Они дают возможность свести живое общение к минимуму (скажем, на совещаниях или конференциях) и ограничить их только тем критическим кругом вопросов, который в силу обширности или конфиденциальности не может быть передан по существующим каналам коммуникации.

Как мы видим у различных подходов на которых может быть основано взаимодействие КР и СБ есть как свои плюсы, так и свои минусы и только одновременное использование всех описанных выше подходов, способно

дать наибольший эффект. Но даже если культура компании не предполагает взаимодействие КР и СБ на уровне обмена массивами знаний, совместная работа на оперативном уровне должна осуществляться в любом случае. Как можно заметить, все инструменты, описанные в конце параграфа 3.1, имеют функции совместной работы в той или иной степени. Наличие подобного функционала входит в современный стандарт специализированного программного обеспечения, что говорит о несомненной пользе подходов основанных на взаимодействии различных специалистов.

ЗАКЛЮЧЕНИЕ

Не смотря на то что иногда КР и СБ могут использовать в своей работе похожие инструменты, это два разных направления деятельности, решающие разные задачи в рамках международного бизнеса. Их увязывание между собой, было обусловлено особенностями развития этих двух направлений в 90х годах прошлого века у нас в стране. В международной же практике, такие тенденции были минимальными. И связано это было с первоочередными задачами, которые решал бизнес у нас в стране и за рубежом. А рост интереса к КР в России в последние годы, обусловлен как раз сменой приоритетов бизнеса и попытками продвижения на внешние рынки. И если подходы СБ привнесённые бывшими работниками силовых ведомств и оправдывают себя на внутреннем рынке, то когда речь заходит о международном бизнесе, то тут им уже предложить особо нечего. Ведь даже сама структура рисков на внешних рынках значительно меняется в зависимости от региона и требует уже иных подходов, связанных с более плотной работой с другими отделами компании.

Крупные корпорации, особенно с гос. участием, при разработке планов по выходу на новый иностранный рынок привлекают к работе отставных офицеров разведслужб, с аналитическим опытом работы в интересующих регионах. Эта практика распространена во всех развитых странах. И именно подобное взаимодействие, в своё время и дало толчок к развитию современной КР. В настоящее время КР прошла процесс институционализации в западных странах и представляет собой полноценное направление, наравне с маркетингом, стратегическим планированием и бенчмаркингом. В нашей стране этот процесс ещё только набирает обороты и его развитие неизбежно, потому что для конкуренции с западными компаниями потребуются использовать все современные подходы.

Конечно противопоставлять КР и СБ нельзя ни в коем случае, эти две структуры должны работать помогая друг другу. И в первую очередь, это взаимодействие должно выражаться в информационном обмене. Ведь в

процессе работы имея разный фокус и спектр источников информации как подразделение КР, так и СБ может получить информацию имеющую минимальную пользу для собственного отдела и большой приоритет для коллег.

Большой скачок в развитии информационных технологий, позволил вывезти работу международных компаний на новый уровень. Обилие программных продуктов позволяет в значительной степени облегчить и автоматизировать работу подразделений КР и СБ. А их взаимодействие в рамках международной компании стало значительно проще реализовать. Сама же архитектура подобного взаимодействия будет зависеть от структуры подразделений КР и СБ, а так же от специфики бизнеса самой организации. Основные же варианты такого взаимодействия рассмотрены в данной работе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об акционерных обществах [Электронный ресурс]: Федеральный закон РФ от 26 декабря 1995 г. №208-ФЗ – Доступ из справочно-правовой системы «КонсультантПлюс». Режим доступа: http://www.consultant.ru

2. О государственной регистрации прав на недвижимое имущество и сделок с ним [Электронный ресурс]: Федеральный закон РФ от 21 июля 1997 г. №122-ФЗ – Доступ из справочно-правовой системы «КонсультантПлюс». Режим доступа: http://www.consultant.ru

3. О государственной регистрации юридических лиц и индивидуальных предпринимателей [Электронный ресурс]: Федеральный закон РФ от 8 августа 2001 г. №129-ФЗ – Доступ из справочно-правовой системы «КонсультантПлюс». Режим доступа: http://www.consultant.ru

4. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: Федеральный закон от 8 июля 2006 г. №149-ФЗ – Доступ из справочно-правовой системы «КонсультантПлюс». Режим доступа: http://www.consultant.ru

5. Публикация сведений о выдаче патента на изобретение, полезную модель, промышленный образец [Электронный ресурс]: Статья 1394 ГК РФ – Доступ из справочно-правовой системы «КонсультантПлюс». Режим доступа: http://www.consultant.ru

6. О подтверждении добросовестности контрагента налогоплательщика. (Письмо Минфина России от 17.12.2014 N 03-02-07/1/65228) [Электронный ресурс]. - Правовая система «КонсультантПлюс». Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=QUEST;n=51790

7. Алексеевских, А. Все банки могут получить доступ к пенсионным данным россиян [Электронный ресурс]. - Газета «Известия», 2014. Режим доступа: http://izvestia.ru/news/574665

8. Алексеевских, А. Банкам разрешили не проверять паспорта клиентов на сайте ФМС [Электронный ресурс]. - Газета «Известия», 2015. Режим доступа: http://izvestia.ru/news/581470

9. Андреева, О. Машина с языком и смыслом [Электронный ресурс]. - журнал "Кот Шрёдингера" №2 (02), 2014. Режим доступа: http://kot.sh/statya/66/mashina-s-yazykom-i-smyslom

10. Анонимная оверлейная сеть I2P [Электронный ресурс]. - Режим доступа: https://geti2p.net/ru/

11. Баяндин, Н.И. Технологии безопасности бизнеса: введение в конкурентную разведку [Текст]// – М.: Юристъ, 2002. – 320 с.

12. Бегтин, И. Анализ веб-страниц, выявление новостей и не только [Электронный ресурс]. - Режим доступа: http://ivan.begtin.name/2010/02/17/webpage-analysis

13. Берд, К. Модель OSINT [Электронный ресурс]/ Компьютерра №22, 2007. Режим доступа: http://old.computerra.ru/2007/690/322686/

14. Берсенёв, В.Л. Ющук, Е.Л. Феномен конкурентной разведки: основы теоретического анализа [Препринт] Екатеринбург: Институт экнономики УрО РАН 2009. – 52 с.

15. Вайс, А. Краткое руководство по конкурентной разведке: как собирать и использовать информацию о конкурентах [Электронный ресурс]/ перевод Е.Л. Ющук, 2006. - Режим доступа: http://ci-razvedka.ru/Arthur_Weiss_Brief_Guide_CI.html

16. Ващекин, Н.П. Дзлиев, М.И. Урсул, А.Д. Безопасность предпринимательской деятельности Б[Текст]/ Учеб. пособие //М.: Экономика, 2002. – 336 с.

17. Взятки не гладки [Электронный ресурс]// Деловой еженедельник «Компания», Выпуск №20, 2008 - Режим доступа: http://ko.ru/articles/18913

18. Виртуальная частная сеть VPN [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/VPN

19. Воротников, А.А. Информационно-аналитические системы для конкурентной разведки [Электронный ресурс]. - Режим доступа: http://www.amulet-group.ru/print.htm?id=742&str=5

20. Гибридная анонимная сеть Tor [Электронный ресурс]. - Режим доступа: http://ru.wikipedia.org/wiki/Tor

21. Горбовцов, С.Г. Требования регулирующих органов к годовому отчету: опыт западных стран и российские стандарты [Электронный ресурс]/ Материалы практической конференции «Годовой отчет: опыт лидеров и новые стандарты», 2005 - Режим доступа: http://www.annual-report.ru/conference/materials/

22. Грусов, С. Противодействие внутрикорпоративному мошенничеству и хищениям [Текст]// М.: Технологии безопасности бизнеса №25, 2011. – С. 9

23. Денисов, Р.В. Менсеф, М. Методы деловой разведки как антикризисный инструмент ординарного управления [Электронный ресурс]/ I Международная научно-практическая конференция "Новые подходы в антикризисном управлении", 2011. – С. 3-4, 6. Режим доступа: http://econf.rae.ru/article/6138

24. Джилад, Б. Конкурентная разведка. Как распознать внешние риски и управлять ситуацией [Текст]/ перевод Н. Черенкова, В. Черенков// СПб.: Питер, 2010. – 320 с.

25. Додонов, А.Г. Ландэ, Д.В. Прищепа, В.В. Путяти, В.Г. Конкурентная разведка в компьютерных сетях [Текст] К.: ИПРИ НАН Украины 2013. – 248 с.

26. Дополнения браузера Firefox, связанные с безопасностью [Электронный ресурс]. - Режим доступа: http://forum.razved.info/index.php?t=1893

27. Доронин А.И., Бизнес-разведка. 2-е изд., перераб. и доп. [Текст] М.: Ось-89, 2003. – 384 с.

28. Ермак, С. Бизнес с интеллектом [Электронный ресурс]/ Эксперт-Урал №12, 2013. Режим доступа: http://www.expert-ural.com/archive/12-549/biznes-s-intellektom.html

29. Закон Великобритании «О борьбе со взяточничеством» (основные положения) [Электронный ресурс]/ Ernst & Young и White & Case - Режим доступа: http://www.itechnopark.ru/File/

30. Закрытая децентрализованная сеть Freenet [Электронный ресурс]. - Режим доступа: https://freenetproject.org

31. Исследование рисков безопасности бизнеса в Российских компаниях [Электронный ресурс]/ ACFE Russia, 2011. Режим доступа: http://www.acfe-rus.org/

32. Исследование. Оценка рисков хищений как актуальное направление в безопасности бизнеса [Электронный ресурс]/ ACFE Russia, 2013. Режим доступа: http://www.acfe-rus.org/

33. Как противостоять внутреннему мошенничеству [Электронный ресурс]. - Режим доступа: http://www.nsbural.ru/Documents/Detail/12367

34. Кирьянов, А.Е. Конкурентная разведка на предприятии в условиях глобализации экономики: организационно-методическое обеспечение [Текст]/ дис. канд. экон. наук: Кострома, 2006. – 177 с.

35. Комаров, А. Оценка комплаенс-рисков: вопросы практического применения [Электронный ресурс]. - Режим доступа: http://www.lexisnexis.ru/

36. Корня, А. Российские суды нарушают закон, обязывающий их публиковать свои решения [Электронный ресурс]. - Газета «Ведомости», 2014. Режим доступа: http://www.vedomosti.ru/politics/news/36995911/nepechatnyj-prigovor

37. Кришталюк, А. Н. Управление безопасностью бизнеса [Электронный ресурс] Учебное пособие, МАБИВ, 2011. Режим доступа: http://www.mabiv.ru/

38. Кулешова, Т.В. Тимофеева, О.В. Федеративный поиск, его достоинства и недостатки в сравнении с индексным поиском [Электронный ресурс]. - Режим доступа: http://www.nlr.ru/tus/20130325/prezent/Federated_Search.pps

39. Ларина, Е. Поисковики [Электронный ресурс]. - Режим доступа: http://hrazvedka.ru/category/poisk

40. Ларина, Е. Федеративный поиск или что не может Google [Электронный ресурс]. - Режим доступа: http://hrazvedka.ru/programm/federativnyj-poisk-ili-chto-ne-mozhet-google-chast-pervaya.html

41. Ларина, Е. IBM Watson: путь к когнитивно-вычислительному бизнесу [Электронный ресурс]. - Режим доступа: http://therunet.com/articles/2211-ibm-watson-put-k-kognitivno-vychislitelnomu-biznesu

42. Лемке, Г.Э. Конкурентная война. Нелинейные методы и стратегемы [Текст]// М.: Ось-89, 2007. – 464 с.

43. Лемке Г. Основы коммерческой разведки [Электронный ресурс]. - Краткие тезисы вебинара. Режим доступа: http://webschool-r.nethouse.ua/

44. Лемке, Г.Э. Секреты коммерческой разведки [Текст]// М.: Ось-89, 2008. – 416 с.

45. Лемке, Г.Э Три вида коммерческой разведки [Электронный ресурс]. - Режим доступа: http://komrazvedka.blogspot.ru/2011/04/blog-post_27.html

46. Людкевич, С. Сеанс поисковой магии. Недокументированные операторы языка запросов Яндекса [Электронный ресурс]. - Режим доступа: http://www.searchengines.ru/articles/seans_poiskovoy.html

47. Марцынковский, Д. Обзор основных аспектов риск-менеджмента [Электронный ресурс]. - Режим доступа: http://www.cfin.ru/finanalysis/risk/main_meths.shtml

48. Метапоисковые системы [Электронный ресурс]. - Институт катализа СО РАН. Режим доступа: http://catalysis.ru/link/index.php?ID=12&SECTION_ID=54

49. Миллер, С.Х. Прескотт, Д.Е. Конкурентная разведка. Уроки из окопов [Текст] М.: Альпина Бизнес Букс, 2004. – 336 с.

50. Митрофанов, А.А. Экономическая безопасность коммерческих предприятий и деловая разведка [Электронный ресурс]/ 2004. – Режим доступа: http://www.bre.ru/security/22843.html

51. Морковкина, Е. Комплаенс-функция в кредитных организациях [Электронный ресурс]/ Бухгалтерия и банки, №12, 2005 - Режим доступа: http://www.pbu.ru/bib

52. Морозов, И.В. Проверка добросовестности Due Diligence компании: цели и задачи [Электронный ресурс]. - Режим доступа: http://www.maonline.ru

53. Нежданов, И.Ю. Аналитическая разведка для бизнеса [Текст]//М.: Ось-89, 2008. – 336 с.

54. Нежданов, И.Ю. Технологии конкурентной разведки [Электронный ресурс]/ 2011. – 243 с. Режим доступа: http://forum.razved.info/pdfs/Igor-Nezhdanov-Tekhnologii-Razvedki.pdf

55. Новиков, В. Статья по безопасности [Электронный ресурс]/ Форум СПКР, 2013. Режим доступа: http://forum.razved.info/

56. Обрезков, О. Разведка, конкурентная борьба и охота на мамонтов. [Текст]/ КЦ «ЛЕКС», Сборник статей Выпуск №1, 1998. – 84 с.

57. Пименов, Н.А. Борьба преступлениями против собственности хозяйствующих субъектов [Текст]// М.: Библиотечка российской газеты, выпуск №8, 2008. – 176 с.

58. Плэтт, В. Информационная работа стратегической разведки. Основные принципы [Текст]/ перевод с англ. Е.В. Пескова, ред. А.Ф. Федорова// М.: Издательство иностранной литературы, 1958. – 342 с.

59. Портер, М. Конкурентная стратегия: Методика анализа отраслей и конкурентов [Текст]// М.: Альпина Бизнес Букс, 2007. – 454 с.

60. Прелебский, Ю. Деловая и конкурентная разведка в России. [Текст]/ КЦ «ЛЕКС», Сборник статей Выпуск №1, 1998. – 84 с.

61. Протокол BitTorrent [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/BitTorrent

62. Российский обзор экономических преступлений за 2014 г. На правильном пути [Электронный ресурс]/ PwC. Annual Global CEO Survey, 2014. – Режим доступа: www.pwc.ru/ceo-survey

63. Современные информационные технологии [Электронный ресурс]/ Кафедра "Информационные системы", МФПА. Режим доступа: http://inftis.narod.ru/it/n11.htm

64. Стандарты управления рисками [Электронный ресурс]// Федерация европейских ассоциаций риск менеджеров (FERMA), Русское общество управления рисками (РусРиск), 2003. – Режим доступа: http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-russian-version.pdf

65. Технология баз информации. Информационное обеспечение процессов управления в экономике [Электронный ресурс]/ Лекция, НОУ ИНТУИТ. – Режим доступа: http://www.intuit.ru/studies/courses/3735/977/lecture/14681

66. Черников, А. BI 2014: Трансформация представлений [Электронный ресурс]. - Режим доступа: http://ko.com.ua/bi_2014_transformaciya_predstavlenij_104501

67. Шевелев, А.Е. Бухгалтерский учет в системе экономической безопасности предприятия [Текст]// М.: Экономистъ, 2005. – 222 с.

68. Шауцукова, Л.З. Информатика [Текст]// М.: Просвещение, 2000. – 420 с.

69. Ющук, Е.Л. Интернет-разведка. Руководство к действию [Электронный ресурс]. - Режим доступа: http://ci-razvedka.com/Invisible_Web.html

70. Ющук, Е.Л. Кэйлоф, Д. Этика в конкурентной разведке [Электронный ресурс]: Комментарии Режим доступа: http://yushchuk.livejournal.com/194932.html

71. Ярочкин В.И., Бузанова Я.В., Корпоративная разведка (2-е изд., перераб. и доп.) [Текст] М.: Ось-89, 2005. – 304 с.

72. Netsukuku — свой собственный интернет [Электронный ресурс]. - Режим доступа: http://habrahabr.ru/post/86702

73. Albaum, G. Competitive Intelligence [Text]: Watertown, MA: C.I. Associates, 1959.

74. Anti-bribery management systems [Electronic resource]. - Access mode: https://www.standard.no/Global/PDF/Standardisering%20-%20nye%20prosjekter/CL_NWIP_Anti-bribery_management_system_Requirements.pdf

75. Competitive Intelligence: Information Espionage and Decision- Making [Text]: Special Report to Management by Students at the Harvard Business School. Watertown, MA: C.I. Associates, 1959.

76. Fleisher, C. Wright, S. Tindale, R. Dishman, P. Knip, V. Bibliographic listing of key competitive intelligence scholarship [Electronic resource]// Competitive intelligence: Marketing interface teaching and research initiative (CIMITRI), De Montfort University, UK Access mode: http://www.dmu.ac.uk/home.aspx

77. Fuld, L. Competitive intelligence dictionary [Electronic resource]. - Access mode: http://www.fuld.com/resource-center/dictionary

78. Fuld, L. What is Competitive Intelligence? [Electronic resource]. - Access mode: http://www.fuld.com/company/what-is-competitive-intelligence

79. Greene, R.M. Business Intelligence and Espionage [Text]: Dow Jones-Irwin Inc. 1966.

80. Havenga, J. Competitive intelligence: What should it offer? [Text]// Security conference. University of Pretoria, Republic of South Africa, 2003.

81. Herring, J.P. Defining your intelligence requirements [Electronic resource]// SLA Annual conference CI Divisions 1st Conference, 2005 - Access mode: http://units.sla.org/division/dci/Conf_Presentations/2005/Defining_Your_Intelligence_Requirements.pdf

82. ISO/IEC 2382-1:1993. Information technology, Vocabulary - Part 1: Fundamental terms [Electronic resource]. - Access mode: http://www.iso.org/iso/catalogue_detail.htm?csnumber=7229

83. ISO 19600:2014 Compliance management systems – Guidelines [Electronic resource]. - Access mode:

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62342

84. Kahaner L., Competitive Intelligence: How to Gather Analyze and Use Information to Move Your Business to the Top [Text] Simon & Shuster, 1997. – 304 с.

85. Luhn, H.P. A business intelligence system [Text]// IBM Journal of Research and Development, T. 2. – №. 4, 1958. – С. 314-319

86. Muller, M.L. Parts of competitive intelligence: competitor intelligence [Electronic resource]// South African Journal of Information Management, Vol 8, № 1, 2006. Access mode: http://www.sajim.co.za/index.php/SAJIM/issue/view/20

87. OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions [Electronic resource]. - Access mode: http://www.oecd.org/corruption/oecdantibriberyconvention.htm

88. SCIP Code of Ethics for CI Professionals [Electronic resource]. - Access mode: https://www.scip.org/CodeOfEthics.php

89. The Intelligence Cycle [Electronic resource]. - Access mode: https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html

90. Tricker, B. Corporate Governance - principles, policies and practices [Text]// Oxford University Press, Oxford, 2009. – 431 с.

91. Venter, P. A new look at marketing intelligence: contemporary views and directions for future research [Electronic resource]. - Graduate school of business leadership university of South Africa, 2009. – Access mode: http://uir.unisa.ac.za/bitstream/handle/10500/4983/Prof%20Peet%20Venter%20INAUGURAL_LECTURE__MARCH%202009%20FINAL.pdf

92. Аваланч: [Электронный ресурс]. - Режим доступа: http://interrussoft.com/avalanche

93. Информация для посетителей о бюро кредитных историй, прошедших государственную регистрацию (ЦБ РФ): [Электронный ресурс]. - Режим

доступа:
https://www.cbr.ru/ckki/print.aspx?file=list_BKI.htm&pid=restr&sid=ITM_23447
94. ИСКРА: [Электронный ресурс]. - Режим доступа: http://iskr-a.com
95. Лавина-Пульс: [Электронный ресурс]. - Режим доступа: https://start.avalancheonline.ru/information/about/
96. Национальная часть единого реестра зарегистрированных деклараций о соответствии, оформленных по единой форме: [Электронный ресурс]. - Режим доступа: http://188.254.71.82/rds_ts_pub/
97. Нигма: [Электронный ресурс]. - Режим доступа: http://нигма.рф/
98. Проверка по списку недействительных российских паспортов (ФМС): [Электронный ресурс]. - Режим доступа: http://services.fms.gov.ru/info-service.htm?sid=2000
99. Российское общество профессионалов конкурентной разведки: [Электронный ресурс]. - Режим доступа: http://www.rscip.ru
100. СайтСпутник: [Электронный ресурс]. - Режим доступа: http://www.sitesputnik.ru/
101. Семантический архив: [Электронный ресурс]. - Режим доступа: http://anbr.ru/products/semarchive/
102. Сообщество практиков конкурентной разведки: [Электронный ресурс]. - Режим доступа: http://razvedka-open.ru
103. Уральский государственный экономический университет: [Электронный ресурс]. - Режим доступа: http://www.usue.ru/
104. Харьковский национальный университет радиоэлектроники: [Электронный ресурс]. - Режим доступа: http://nure.ua/
105. Academy of Competitive Intelligence: [Electronic resource]. - Access mode: http://www.academyci.com
106. Amity Institute of Competitive Intelligence and Strategic Management: [Electronic resource]. - Access mode: http://amity.edu/aicism/default.aspx
107. Australian Institute of Professional Intelligence Officers: [Electronic resource]. - Access mode: http://www.aipio.asn.au

108. A Wiki of Social Media Monitoring Solutions: [Electronic resource]. - Access mode: http://wiki.kenburbary.com/

109. Chem Industry: [Electronic resource]. - Access mode: http://www.chemindustry.com/index.html

110. Competia: [Electronic resource]. - Access mode: http://competia.com

111. Competitive Intelligence Ning: [Electronic resource]. - Access mode: http://competitiveintelligence.ning.com/

112. CONSENSUS OMNIUM: [Electronic resource]. - Access mode: http://opac.urfu.ru/consensus/

113. Decision Intelligence: [Electronic resource]. - Access mode: http://decisionintel.org/intelligence-degrees-courses-and-certificates/

114. Ecole de Guerre Economique – EGE: [Electronic resource]. - Access mode: http://www.ege.fr

115. Global Risk Community: [Electronic resource]. - Access mode: http://globalriskcommunity.com/

116. Google Custom Search: [Electronic resource]. - Access mode: https://www.google.com/cse/

117. Hontza: [Electronic resource]. - Access mode: http://www.hontza.es/

118. Quintura: [Electronic resource]. - Access mode: http://www.quintura.ru/

119. Search Engines Index: [Electronic resource]. - Access mode: http://searchenginesindex.com/

120. The Institute for Competitive Intelligence: [Electronic resource]. - Access mode: http://www.institute-for-competitive-intelligence.com/

121. Yahoo! Pipes: [Electronic resource]. - Access mode: http://pipes.yahoo.com/pipes

ПРИЛОЖЕНИЕ А

Индекс цитирования Google Академия

Таблица А.1 - Сводная таблица определений КР [86, с. 16; 27, с. 43; 11, с. 8; 16, с. 177; 71, с. 8; 53, с. 11; 50]

Термин	Книга	Определение	Цит-ть
"Competitive intelligence"	Kahaner L. Competitive intelligence: how to gather analyze and use information to move your business to the top.	Конкурентная разведка является систематической программой для сбора и анализа информации о деятельности ваших конкурентов и общих тенденциях бизнеса для дальнейших целей вашей собственной компании.	678
"Бизнес разведка"	Доронин А. И. Бизнес-разведка.	Организационная структура, занимающаяся вопросами сбора, проверки (верификации), обработки, анализа и синтеза данных по различным аспектам хозяйственной деятельности предприятия с дальнейшим использованием полученной информации для решения конкретных задач его хозяйственной деятельности.	81
"Конкурентная разведка"	Баяндин Н. И. Технологии безопасности бизнеса: введение в конкурентную разведку.	Конкурентной разведкой называется деятельность негосударственной организации по добыванию сведений об имеющихся и потенциальных угрозах ее существованию и интересам при условии соблюдения существующих	34

		правовых норм.	
"Экономическая разведка"	Ващекин Н. П., Дзлиев М. И., Урсул А. Д. Безопасность предпринимательской деятельности.	Термин экономический, промышленный, коммерческий, научно-технический шпионаж (разведка) означает активные действия, направленные на сбор, хищение, накопление и обработку ценной информации, закрытой для доступа посторонних лиц, ведущиеся негосударственными организациями и частными лицами. Существует множество способов получения конфиденциальной информации о деятельности конкурентов. Условно их можно разделить на две большие группы: законные и незаконные методы, что, собственно, и подразумевает деление добывания информации на экономическую разведку и промышленный шпионаж.	29
"Корпоративная разведка"	Ярочкин В. И., Бузанова Я. В. Корпоративная разведка.	Корпоративная разведка - совокупность органов, сил и средств, осуществляющих сбор, анализ и обработку сведений о конкурентной ситуации на рынке, в интересах всей корпорации.	15
"Аналитическая разведка"	Нежданов И. Ю. Аналитическая разведка для бизнеса	Аналитическая разведка обозначает разведывание посредством анализа. Или, говоря расширенно, получение	8

		знаний (информации, сведений и т.п.) посредством аналитических операций. То есть получение новых сведений об объекте своего интереса посредством изучения имеющихся данных о нем и не прибегая к непосредственному контакту.	
«Деловая разведка»	Митрофанов А. А. Экономическая безопасность коммерческих предприятий и деловая разведка.	Деловая разведка (конкурентная разведка, competitive intelligence, business intelligence) — постоянный процесс сбора, накопления, структурирования, анализа данных о внутренней и внешней среде компании и выдачи высшему менеджменту компании информации, позволяющей ему предвидеть изменения в этой среде и принимать своевременные оптимальные решения по управлению рисками, внедрению изменений в компании и соответствующие меры, направленные на удовлетворение будущих запросов потребителей и поддержание прибыльности.	7

ПРИЛОЖЕНИЕ Б

Признаки хищений в организации

Таблица Б.1 - Индикаторы хищений [32, с. 10-15]

Индикатор	Пояснение
Утеря или уничтожение документов и электронных файлов, содержащих ключевую информацию о сомнительных операциях.	При проведении проверки (расследования) выяснилось, что ключевые документы или файлы отсутствуют – утеряны (например, вследствие сбоя в компьютерной системе) или уничтожены (по любым основаниям).
Отсутствие первичных подтверждающих документов.	При проведении проверки (расследования) выяснилось отсутствие первичных подтверждающих документов.
Стоимость личной собственности и образ жизни не соответствует доходам.	Расходы сотрудника значительно превышают его официально декларированные доходы.
Отсутствие наказаний за выявленные нарушения.	Виновные в нарушениях сотрудники не наказываются или наказываются формально (степень наказания не соответствует нанесённому компании ущербу).
Проведение сделок, по форме не соответствующих содержанию.	Например, заключается фиктивный договор на оказание аутсорсинговых услуг по предоставлению персонала, для компенсации якобы дополнительных расходов подрядчика.
Беспорядочная система хранения ТМЦ, документов и электронных файлов.	Отсутствие формально или неформально установленной системы хранения документов и файлов, невозможность найти документы и файлы без помощи конкретного сотрудника.
Необоснованное чрезмерное сосредоточение ключевых полномочий.	Все ключевые полномочия в бизнес-процессе сосредоточены у одного менеджера, необоснованно избегается делегирование полномочий.

Противоречия в объяснениях или смена одних объяснений другими.	Многократные изменения объяснений причин ущерба или нарушений в ходе проведения проверки или расследования ответственным лицом.
Внезапный отказ персонала от сотрудничества в процессе проверки.	В процессе проведения проверки происходит внезапный отказ ранее хорошо сотрудничавших с группой проверки сотрудников от дальнейшего сотрудничества, отношение меняется на недоброжелательное, начинают происходить задержки и отказы в предоставлении информации.
У операционного персонала существуют права доступа для изменения архивных файлов и записей о проведённых операциях.	Персонал, ответственный за проведение и учёт операции имеет права изменения данных об операциях за прошлый период (например, бухгалтер, работающий с программой 1С, имеет права редактировать данные за прошедшие периоды или задним числом менять какую-то информацию).
Ограничения в доступе проверяющих к персоналу организации.	В частности, требование направлять все запросы и получать информацию только от руководителя подразделения, запрет проведения интервью с исполнителями.
Уровень развития контрольных процедур.	Влияние на уровень хищений уровня развития контрольных процедур в компании. Чем больше внимания компания уделяет развитию и совершенствованию системы контрольных процедур, тем, в общем случае, ниже риск хищений.
Создание обособленных групп персонала менеджером.	Создание неформальных групп «особо доверенных» или «приближенных» к менеджеру сотрудников, которые обладают большой властью не в соответствии с организационной структурой компании, а в

	силу неформальных отношений с руководителем.
Определение расхода сырья обратным счётом.	Объем сырья и материалов, израсходованного на производство продукции, определяется расчётным способом от объёма выпущенной продукции, а не на основании замера фактически израсходованного объёма.
Производные таблицы не подтверждаются первичными документами.	Расхождения между первичными и производными документами.
Недостаточный уровень автоматизированного контроля операций.	Необоснованный отказ от внедрения повсеместно принятых средств автоматизированного учёта операций, например, ручное ведение бухгалтерского учёта, в то время как обычно в этих случаях используется программа 1С.
Неудовлетворённость персонала уровнем заработной платы.	Если персонал предприятия (отдела) выражает недовольство уровнем оплаты труда и использует это как объяснение (самооправдание) невыполнения контрольных процедур или халатности.
Нарушение установленного порядка исполнения операций, объясняемое благими целями, если в результате нарушения создаются благоприятные условия для хищения.	Такая ситуация создаётся, когда контрольная процедура нарушается персоналом, но прямые доказательства хищения отсутствуют, но из-за нарушения КП были созданы благоприятные условия для хищения.
Объем материальных ценностей в обороте.	Чем больше в обороте подразделения или бизнес-процесса материальных ценностей (денег, товаров и т.д.), тем выше риск хищений.
Отключение предусмотренных возможностей	По разным причинам контрольно-измерительные приборы и средства

контроля в автоматизированных системах.	автоматизации отключаются и не фиксируют результаты операций. Например, автомобильные весы сломаны большую часть времени, или файлы с записями результатов ежедневно уничтожаются.
Использование расчётных показателей при наличии автоматизированных учётных систем.	При наличии автоматизированных учётных систем их возможности не используются, либо они часто выходят из строя.
Наличие программы по противодействию хищениям.	Влияние на уровень хищений наличия в компании эффективно работающей программы по противодействию хищениям.
Удалённость производства от топ-менеджмента и контролирующих служб.	Географическая удалённость места проведения хозяйственной деятельности (производственных процессов) от высшего менеджмента и контролирующих подразделений.
Наличие персональных факторов давления (кредиты, зависимости и т.д.)	Зависимость от наркотических средств, алкоголизм, игровая зависимость, наличие близких родственных связей с людьми, ведущими асоциальный образ жизни, потребность в дорогостоящем лечении, привычка к расточительному образу жизни.
Отсутствие системы разделения прав и полномочий.	В контрольных процедурах отсутствует разделений полномочий по принятию решений и учёту результатов операций, оценке рисков.
Высокая текучесть кадров на уровне руководства/высшего менеджмента.	Частая сменяемость высшего менеджмента на ключевых позициях (директор, финансовый директор и т.д.).
Даты модификации файлов не соответствуют дате, когда они	Например, файл, который был создан год назад, имеет вчерашнюю дату

должны быть созданы.	модификации.
Низкая лояльность персонала.	Низкая лояльность персонала задачам и целям компании, отношение к компании как к временному месту работы, где интересы компании и сотрудников противоположны.
Необоснованные задержки в предоставлении запрошенной документации и доступа к электронным файлам.	При проведении проверки возникают необоснованные реальными обстоятельствами задержки в предоставлении документов и доступа к информационным системам.
Поведение менеджмента, демонстрирующее доминирование над внутренним аудитом и другими контрольными службами.	Типичные заявления: мы тут работаем, а вы (проверяющие) только мешаете.
Избирательный подход к выполнению контрольных процедур.	Отдельные контрольные процедуры не выполняются без обоснованных причин.
Чрезмерно высокие ожидаемые ключевые показатели работы менеджеров.	Когда ключевые показатели эффективности работы менеджмента нереальны для исполнения в существующих условиях.
Менеджмент демонстрирует недостаточное внимание к этическим ценностям, недостаток коммуникаций с сотрудниками по вопросам этики, недостаточно агрессивное отношение к проблеме хищений.	Менеджмент демонстрирует перед работниками пренебрежение к нормам закона и этики.
Значительные корректировки отчётности и бюджетов.	В течение отчётного периода осуществляются значительные корректировки отчётности (бюджетов).
Большое расхождение между бюджетными и фактическими данными.	Данные фактического исполнения бюджета значительно (более чем на 15-20%) отличаются от первоначально

	утвержденного бюджета.
Некриминальные объяснения нанесённого ущерба, если проверка объяснений невозможна.	Факт нанесения ущерба компании обнаружен, ответственное лицо предоставляет некриминальные объяснения причины ущерба (стихийные бедствия, происки конкурентов и т.д.), однако проверка правдивости этих объяснений невозможна.
Необоснованное невыполнение рекомендаций по устранению недостатков.	Менеджмент необоснованно не выполняет рекомендации и не предпринимает мер по устранению выявленных недостатков в организации системы внутреннего контроля.
Неспособность менеджмента продемонстрировать заинтересованность в установлении соответствующего уровня контроля.	Как правило, в таких случаях менеджмент заявляет, что противодействие хищениям – это работа службы безопасности, внутреннего аудита и т.д.
Наличие копий документов вместо оригиналов.	Копии документов первичных документов, например, счетов, счетов-фактур и т.д.
Длительная работа сотрудника на ключевой позиции без отпусков.	Длительная работа сотрудника на одной должности без отпусков и больничных, без временных замен другими сотрудниками.
Вид бизнес-процесса. Влияние типа бизнес-процесса на уровень хищений в нем.	К традиционно высоко рисковым для хищений процессам относятся закупки, капитальное строительство, инвестиции.
Нестабильность и кризисные явления. Влияние кризисных явлений на уровень хищений в компании.	К кризисным явлениям относятся: предстоящие реорганизации и сокращения, смена менеджмента – все, что создаёт у сотрудников ощущение нестабильности и неуверенности в завтрашнем дне.
Чрезмерное волнение и неадекватное поведение при	Типичные вербальные и невербальные признаки неадекватного

общении в процессе проверки.	волнения - слезы, истерики, гнев и т.д.
Периодичность оценки.	Влияние на уровень хищений частоты проверок и оценки рисков хищений в подразделении (предприятии): насколько часто контролирующие службы проводят аудиторские, ревизионные проверки на предприятии – например, раз в год или раз в три года.
Отсутствие системы анонимного информирования («горячей линии») в компании.	Отсутствие в компании «горячей линии» для приёма анонимных сообщений сотрудников о злоупотреблениях, отсутствия должной осведомленности сотрудников о результатах работы «горячей линии», отсутствие доверия сотрудников к желанию руководства компании рассматривать сообщения по существу.
Менеджмент демонстрирует повышенную склонность к риску, нежелание оценивать риски.	Типичный аргумент менеджера в таком случае: я принимаю решение и сам оцениваю риски, мне не нужен независимый и формализованный риск-менеджмент.
Отсутствие системы КПЭ у менеджмента.	Отсутствие ключевых показателей эффективности у менеджмента.
Низкий уровень корпоративной культуры.	Влияние на уровень хищений степени развитости корпоративной культуры в компании. Высокая корпоративная культура, приверженность персонала целям и ценностям компании является одним из факторов, снижающих уровень хищений.

ПРИЛОЖЕНИЕ В

Зоны комплаенс-риска для различных бизнес процессов

Таблица В.1 Зоны комплаенс-риска и необходимые меры контроля [35]

Зоны риска	Меры контроля
Проверка контрагента при заключении договора	
• Контрагенту (аффилированным с ним лицам) предъявлялись обвинения в коррупционной деятельности. • Контрагент находится в офшорной зоне. • Контрагент использует разные. юрисдикции (при отгрузках / платежах) • Контрагент отказывается раскрывать информацию о конечных бенефициарах либо акционеры контрагента находятся в офшорной зоне (информация о конечных бенефициарах не может быть подтверждена). • Контрагент находится под санкциями либо ведёт бизнес в странах, находящихся под санкциями. • В отношении контрагента выявлен конфликт интересов с сотрудниками компании. •Отсутствует прозрачное обоснование выбора контрагента (нет разумных пояснений об обстоятельствах, при которых было инициировано начало сотрудничества, отсутствие конкурсных процедур либо не прозрачные критерии выбора участников конкурса, либо недостаточно прозрачный процесс проведения конкурса).	• Проверка контрагента, основанная на оценке потенциальных рисков. • Особое внимание: - Контрагент является лицом, связанным с государством; - Контрагенты, которые представляют интересы либо выступают от имени компании (дилеры, агенты, юристы, консультанты и т.п.); - Контрагент привлекает третьих лиц к исполнению договора; -Посредники. • Анализ целесообразности и уровня вознаграждения: - Контрагентов, которые представляют интересы компании (агенты, юристы, консультанты и т.п.); - Посредников; - Лиц, связанных с государством. •Анализ обоснования причин (целесообразности) работы с контрагентом.
Сертификация дилеров, дистрибьюторов	
• Недостаточно прозрачные критерии сертификации дилеров либо не эффективный контроль за данными критериями. • Операции дилера с повышенным риском: - Сделки по ценам выше прейскуранта; - Продажи лицам, связанным с государством; - Продажи посредникам .	• Обязательное внедрение комплаенс-политик дилером. • Комплаенс-оговорка в дилерском соглашении. • Аудит процедуры сертификации дилеров. • Аудит дилеров на предмет внедрения комплаенс-мер с учётом оценки рисков. • Визит сотрудника комплаенс-подразделения и встреча с руководителями и собственниками дилеров с «красными флажками».
Открытие и закрытие банковских счетов	
• Наличие счетов, по которым. отсутствуют основания для их наличия • Счета в офшорных юрисдикциях.	• Мониторинг счетов. • Формализованная процедура открытия и закрытия счетов.

• Открытие и закрытие счетов для разовых сделок без достаточного обоснования. • Недостаточный контроль доступа к счетам компании либо наличие такого доступа у третьих лиц. • Выпуск неименных корпоративных карт.	
Благотворительность	
• Перечисление помощи третьим лицам, которые не оказывают услуги (не поставляют товары) благополучателю. • Финансирование политических партий. • Публикация информации о благотворительности несёт репутационные риски. • Отсутствует детальное обоснование направления и использования благотворительной помощи.	• Типовой договор, включающий обязанность: - Указания конечного получателя помощи; - Предоставления отчёта о расходах; - Предоставления информации для проверки целевого использования средств; - Публикации информации о благотворительности; - Возвратить имущество в случае их нецелевого использования; - Соблюдать требования антикоррупционного законодательства - Право на аудит. • Анализ фактического использования выделенной помощи. • Обязательная публичность информации о благотворительности.
Приём делегаций, подарки, представительские расходы	
• Подарки чиновникам свыше 3 тысяч рублей допустимы в ходе протокольных мероприятий – в обязанность чиновника входит передача такого подарка государству. При несоблюдении данного требования подарок может быть определён как взятка. • При подарках физическим лицам свыше 4 тысяч рублей в год необходимо уведомление налоговых органов. • Размер расходов по приёму делегации (представительским расходам) превышает установленный норматив либо отличается от нормативов компании для аналогичного уровня сотрудников. • Размер представительских расходов на человека в день более 15 тысяч рублей. • Мероприятие не связано с бизнес-целями либо время, использованное для	• Установление нормативов подарков и расходов по уровням сотрудников. • Определение критериев подарка. Он не должен противоречить законодательству и способствовать принятию незаконного решения. • Возмещение расходов на основе подтверждающих документов. • Запрет на финансирование определённого вида расходов / подарков.

обсуждения бизнес-вопросов менее 50%.	
Ценовая политика	
• Дополнительные скидки и отсрочки. • Скидки и отсрочки имеют отношение к ограниченному кругу контрагентов. • Цена превышает обычный уровень.	• Анализ причин возникновения обстоятельств, приводящих к необходимости предоставления дополнительных скидок, отсрочек. • Обоснование и мониторинг экономической целесообразности предоставления скидок, отсрочек. • Анализ причин предоставления индивидуальных преференций. • Анализ обстоятельств, связанных с ростом цены выше обычного уровня.
Взаимодействие с государственными органами	
• Наличие сотрудников (кандидатов), связанных с государством, либо ранее занимавших государственные должности. • Наличие сотрудников, чьи близкие родственники связанные с государством, могут принимать решения, приводящие к конфликтам интересов.	• Обязательное уведомление государственного органа, в котором работал сотрудник (кандидат). • Анализ всех обстоятельств и принятие мер по недопущению конфликта интересов.
Платежи	
• Платёж не одобрен в соответствии с внутренней процедурой. • Платежи контрагентам с комплаенс-рисками. • Платежи в иные юрисдикции (офшоры).	• Разделение обязанностей согласования, выпуска платёжного поручения, права первой и второй подписи, отражения в учёте. • Контроль соответствия платежа условиям договора. • Детальный учёт платежей по операциям с комплаенс-рисками. • Своевременное отражение платежей. • Периодический мониторинг платежей.
Закупки	
• Ценообразование не является прозрачным. • Использование посредников.	• Тендерные процедуры на прозрачной основе: - Отбор участников (включение лидеров рынка, исключение аффилированных участников); - Определение критериев выбора победителей; - Проведение переговоров по снижению цены . • Долгосрочные контракты с формулой цены.

	• Анализ целесообразности использования посредников.
Продажа непрофильного и излишнего имущества	
• Ценообразование не является прозрачным. • Использование посредников.	• Тендерные процедуры на прозрачной основе: - Отбор участников (обеспечение максимального участия возможных заинтересованных лиц, исключение аффилированных участников); - Определение критериев выбора победителей. • Анализ информации о победителях тендерных процедур. • Анализ целесообразности использования посредников.
Деятельность дочерних обществ совместных предприятий и зависимых обществ	
• Наличие процессов с комплаенс-риском в дочерних обществах. • Получение информации о нарушении комплаенс-процедур. • Совершение сделок с комплаенс-рисками.	• Назначение ответственных за комплаенс • Внедрение комплаенс-программ. • Получение и анализ сведений об операциях с комплаенс-рисками. • Сбор, обработка и анализ информации об операционной и финансовой деятельности дочерних обществ и совместных предприятий. • Проведение аудита.

ПРИЛОЖЕНИЕ Г

Информационно-аналитические системы на российском рынке

Таблица Г.1 - Примеры ИАС [19]

Название	Компания	Сайт
ИАС «Семантический архив»	Аналитические бизнес решения	www.anbr.ru
«Avalanch», «Лавина Пульс»	«Инфорус»	https://lavinapulse.ru
«Web-Observer»	Finport Technologies	http://www.webobserver.ru/
СИОИ «Айкумена Аналитика»	IQmen	http://iqmen.ru/
ИАС «Астарта»	Cognitive Technologies Ltd.	http://www.cognitive.ru/
RCO Fact Extractor Desktop, RCO Zoom	"ЭР СИ О"	http://www.rco.ru
«Аналитический курьер», «X-Files»	I-teco	http://i-teco.ru/
Программный комплекс «Intellectum.BIS»	«Информбюро»	www.informburo.net
ИАПК «Дипломат»	Разработано НИЦИ при МИД России	-
ИПК «Тренд», «Мониторинг», «Интернет-монитор»	ООО «Вербин и партнеры»	vipcompanys@infoline.su
«Галактика Zoom»	Корпорация Галактика	www.galaktika-zoom.ru

ИПС «Артефакт»	«Интегрум-Техно»	http://www.integrum.ru/
АИС «Монитор»	АРСИН	http://www.attskopin.ru/
Программный комплекс «Дофин», «СФН», «Апокриф», «Профиль»	«АР-Систем»	http://www.ar-system.ru
PolyAnalyst	Megaputer Intelligence	http://megaputer.ru

ПРИЛОЖЕНИЕ Д

Поисковые операторы Яндекса, не указанные на официальном сайте

Таблица Д.1 - Недокументированные операторы Яндекса [46]

Оператор	Описание
<<	Не ранжирующее логическое «И».
intext	Поиск только в текстах документов.
inlink	Поиск в ссылках на документы. Хотя бы одно слово запроса нужно вынести из-под данного оператора.
inpos	Специальное имя атрибута для указания точного диапазона позиций, в которых должен находиться предыдущий лист или скобка. Имеет синтаксис inpos:N1..N2, где N1 и N2 — целые положительные числа.
linkint	Поиск внутренних ссылок на определенный документ.
anchorint	Поиск по документам, содержащих ключевую фразу в текстах своих ссылок, ведущих на внутренние страницы того же сайта.
address	Поиск внутри текстов, заключенных в теге.
quote	Поиск внутри текстов, заключенных в теге.
image	Поиск по имени файлов изображений, используемых в документе.
anchormus	Ищет ссылки на музыкальные файлы, содержащие в анкоре поисковый запрос.
linkmus	Найти все страницы, ссылающиеся на определенный музыкальный файл.
idate	Ищет документы с заданной датой последней индексации.
style	Поиск по значению атрибута stylesheet тега link.
applet	Поиск по значению атрибута code тега applet.
script	Поиск по значению атрибута src тега script.
object	Поиск по содержимому атрибутов тега object.
action	Поиск по значению атрибута action тега form.
profile	Поиск по значению атрибута profile тега head.