"Бизнес-разведка" № 22

ОГЛАВЛЕНИЕ

"Бизнес-разведка"

В.Егоров

Анализ СМИ как важнейшее направление конкурентной разведки

Одной из главных проблем для службы конкурентной разведки является выяснение того, какие виды информации необходимо собирать, анализировать и накапливать в базах данных. Особенно, если компания имеет достаточно широкую филиальную сеть (или группы аффилированных компаний с соответствующими долями участия головной компании). На этапах сбора стратегически важной информации целесообразно наличие соответствующих структур в регионах присутствия компании, осуществляющих сбор, анализ и представление информации по критериям, утвержденным службой конкурентной разведки головной компании. Периодичность экспресс-оценок материалов СМИ, отражающих ситуацию в регионе присутствия согласовывается заинтересованной службой заранее и осуществляется непрерывно.

Следует учитывать и то, что крупные компании обладают развитой экономической и политической разведкой, имеют свои издания и «своих» журналистов. Журналистика и вопросы экономической разведки и контрразведки, формирование имиджа, престижа и рейтинговых оценок чрезвычайно тесно связаны.

Работа со СМИ предполагает прежде всего анализ статей по экономической и криминальной тематике – там обычно встречается компромат, можно выловить утечки информации. Эта работа может проводиться с привлечением интегрированных аналитических систем, развитие которых в настоящее время приобрело массовый характер.

В процессе изучения доступных следует обратить внимание на такие моменты:
- количество публикаций позитивного и негативного характера о самой компании и основных конкурентах;
- в какой степени монополизированы темы (закрепление определенных аспектов за теми или иными изданиями);
- круг авторов (закрепление определенных аспектов за теми или иными журналистами);
- связь между рекламными объявлениями и заказными статьями;
- наличие сбалансированных оценок.

Основной метод, применяемый для подготовки значимых оценок с использованием прессы, это сопоставление фактов, намеков, слухов, мнений, версий, фамилий, т.е. разнородной информации по ключевому слову, фамилии, факту, событию (в зависимости от задачи) из:
- отечественных открытых источников информации;
- зарубежных открытых и платных источников;
- промышленных и коммерческих отчетов;
- коммерческих изданий.

В качестве базового знания может выступать информация о близости органа массовой информации конкретному коммерческому образованию. В ряде случаев задача информационного плана считается достигнутой, когда аналитик объективно приходит к смысловому совпадению сведений из независимых источников.

Аналитическая работа требует терпения, настойчивости, дотошливости. На примере одной специализированной организации могу сказать, что ежедневная сводка объемом не более страницы составляется на основе переработки материала объемом примерно в 7 млн. слов.

По каким признакам статьи или иные материалы могут попасть в сферу интересов аналитического подразделения? Близость к экономическому профилю компании, происходит организованная утечка конфиденциальных сведений, заметно чересчур эмоциональное изложение сведений, очевидное намерение автора навязать определенную точку зрения.

Аналитику в ходе просмотра и отбора статей важно обращать внимание на степень угрозы, которую демонстрирует лицо, пишущее на темы близкие интересам компании. Индикаторы угрозы - слова или существенные элементы информации, указывающие на то, что может случиться. Эти индикаторы в контексте статьи могут служить признаком вероятности наступления событий, замаскированной угрозы или предупреждения.

Примеры:
- «это столкновение интересов может повлечь...»;
- «коммерческая организация будет отстаивать интересы с применением всех средств, даже не опираясь на силу закона...»;
- «между этими лицами существуют неразрешимые противоречия»;
- «мы ориентируемся на экономические интересы всей страны, что затрагивает права большого количества лиц и влиятельных организации, и не потерпим....».
Кстати, подобные примеры скрытой угрозы предшествовали ряду известных заказных убийств.

Сведения, как правило, оценивают по надежности источника, достоверности информации, направленности информации и др.

1. НАДЕЖНОСТЬ ИСТОЧНИКА:
- совершенно надежный;
- обычно надежный;
- довольно надежный;
- не всегда надежный;
- ненадежный;
- надежность не может быть определена.

2. ДОСТОВЕРНОСТЬ ИНФОРМАЦИИ:
- достоверность подтверждена;
- вероятно правдивая;
- возможно правдивая;
- сомнительная;
- неправдоподобная;
- достоверность не может быть определена.

3. НАПРАВЛЕННОСТЬ ИНФОРМАЦИИ:
- обзорные, апологетические статьи;
- статьи дискредитационного плана;
- заказные рекламные статьи;
- статьи, разглашающие коммерческую тайну.

Для облегчения этой работы ее надо систематизировать, введя:
- указатель имен;
- указатель связей объектов;
- картотеку рекламы;
- анкету статьи, организации, лица, включающую сведения об источнике информации, заказчиках, финансировании, маршрутах поездок и контактов, а также сопутствующие материалы.

Индикаторы приобретают реальную значимость в свете базовых данных о явлениях, а также оценки фактов с помощью других источников, в частности, таких как: перечень фирм и рекламных агентств, размещающих рекламу в завуалированной форме или на основе долгосрочных контрактов, список авторов, пишущих в интересах этих организаций (прямое рекламирование и отстаивание интересов иными способами).

Индикаторы в данном случае априори указывают на:
- необъективность;
- лживость (усеченная, неполная информация);
- принадлежность к преступному формированию и пр.

Основные процедуры важнейшего метода исследования - контент-анализа, сводится к:
- выявлению смысловых единиц - понятий и терминов;
- установлению частоты применения понятий, связанных с критикой объекта;
- установлению, в какой мере источник информации ориентирован на те или иные позиции

и осведомлен о них, что является признаком, указывающим на необходимость установления источника утечки конфиденциальной информации;
- анализу тематики, т.е. определению содержания, показательных сюжетов, свидетельствующих об определенной направленности взглядов, интересов, ценностной ориентации журналистов, пишущих по проблемам, затрагивающим интересы компании;
- выяснению частоты употребления определенных имен, ссылок на авторитетных в той или иной области специалистов, свидетельствующих о влиянии отдельных лиц или представляемых ими организаций на журналиста, а также частоты упоминания организаций.

Об авторе: Егоров Валерий Игоревич
Консультант по информационно-аналитическому сопровождению бизнес-процессов, помощник Председателя Клуба сотрудников информационных служб (г. Москва).
e-mail: valeriyegorov@yahoo.com

"Бизнес-разведка"

И. Дудатьев

Некоторые особенности сбора информации о зарубежных конкурентах

Сбор информации о зарубежных рынках и конкурентах осуществляется активными (полевыми) и пассивными методами. При этом для сотрудников КР, осуществляющих сбор информации в другой стране, важно знание культуры, языка, особенностей деловой жизни.

Важно знать, например, что американцы общительны, китайцы на переговорах любят обсуждать не более одного-двух вопросов, японцы не любят рукопожатий и т.д. При проведении интервью с иностранными гражданами сотрудники КР должны учитывать специфику страны. Для этого необходимо:

- в порядке подготовке к беседе усвоить правильное произношение фамилий, стран, городов и т.д., которые придется упоминать в беседе;

- избегать использования профессионального и регионального жаргона, не воспринимаемого на других языках;

- не спешить с установлением доверительных отношений, которые могут смутить и насторожить собеседника, особенно из стран с иной культурой общения;

- проявлять терпение и вежливость, не забывая, например, спросить, располагает ли собеседник временем и т.п.;

- сдерживать свой темп речи, облегчая ее восприятие иностранцем;

- заблаговременно установить должностное положение собеседника, поскольку должности и звания существенно различаются в разных странах;

- прибегать к различной формулировке вопросов, добиваясь их правильного понимания;

- относиться с уважением к возрасту и званию собеседника.

Прежде чем собранная информация будет анализироваться, она проходит предварительный анализ – КР должна удостовериться, что полученная информация качественная, соответствует установленным критериям.

Сопоставительный анализ («кросс-анализ») - наиболее распространенный и надежный метод проверки полученной информации. Суть метода в сопоставлении ответов на один и тот же вопрос из разных источников информации. Если информация подтвердилась всеми источниками, то ее можно считать качественной и в дальнейшем использовать для анализа. Если информация не подтвердилась всеми источниками (или, что еще хуже, носит противоречивый характер), то КР должна поставить под сомнение не только данную информацию из первоначального источника, но и всю информацию, полученную из него.

При проведении кросс-анализа необходимо обратить внимание на выборку источников информации, которая используется для проверки первоначального источника. Возможен вариант, когда источник сообщает «лояльную» для КР информацию, исходя из каких-то своих соображений.

.

Другой метод - метод поиска противоречий. Если КР в процессе сбора информации получила два противоречивых факта, то это серьезное основание для того, чтобы признать полученную информацию некачественной и непригодной для решений. Обычно такие противоречия и нестыковки выглядят достаточно безобидными и незначительными. Но КР, помня, что «маленькая ложь рождает большое недоверие», должна самым тщательным образом расследовать любые информационные натяжки. Пусть лучше это окажется профессиональной перестраховкой, нежели ошибкой при принятии стратегического решения о выходе предприятия на рынок новой страны.

"Бизнес-разведка"

От информации к действиям – как сократить дистанцию

Сердцевиной активной бизнес-разведки является не просто информация, но «информация действенная» (actionable), которая реализуется в конкретных решениях и практических шагах, утверждает президент американской консалтинговой компании Bolder Technology, Inc. Ричард Хакертон. Звучит, может быть, банально, но каждый знает массу примеров, когда получаемая информация, нужная, важная, по разным причинам не находит практического применения. Специалист по информационным ресурсам, автор ряда книг Хакертон размышляет на тему эффективности деловой разведки, которая зависит от многих факторов, и не в последнюю очередь от той временной дистанции, которая пролегает между получением данных и их реализацией в практических делах (SCIP.online, Issue 46).

Есть два способа сократить эту дистанцию, пишет американский эксперт.

Первый – поставить в центр работы совершенствование системы управления информацией. Это традиционный подход, предполагающий прежде всего поиск ответов на такие вопросы как «Какой информацией мы располагаем?», «Как управлять этой информацией?», «Можем ли мы анализировать информацию, чтобы она служила практическим задачам?».

Второй путь – подчинить систему управления информацией задачам управления бизнесом, выбрать такую последовательность вопросов:

• Какие процессы нашего бизнеса требуют корректировки, улучшения?
• Кто персонально несет ответственность за эти процессы?
• Какие шаги нужно предпринять для решения задач?
• Какая информация необходима для решения задач?
• Где и как можно получить и изучить такую информацию?

Второй подход, считает Хакертон, предпочтительнее, если мы хотим сделать бизнес-разведку действенной, эффективной. Чтобы проделать путь от определения задач по улучшению бизнеса до поиска нужной информации, ее анализа и оценки, и далее – ее реализации в практических действиях, требуется время, подчас немалое. Как сократить эту дистанцию?

Автор предъявляет три главных требования к системе управления информацией.

Во-первых, она должна предупреждать – своевременно обнаруживать риски и угрозы (например, начавшиеся у банка-кредитора проблемы).

Во-вторых, анализировать, помогая быстро и правильно оценить складывающуюся ситуацию.

В-третьих, ориентировать на верные решения и шаги по исправлению, улучшению ситуации.

"Бизнес-разведка"

Информационные совещания – когда они полезны?

В нашем журнале мы регулярно печатаем материалы, посвященные вопросам взаимодействия информационщика/аналитика с различными отделами внутри компании с целью регулярного обмена информацией. Помимо создания и использования для этого внутрикорпоративного Интранета, многие эксперты настойчиво советуют чаще встречаться с коллегами по организации, участвовать в различных совещаниях и производственных встречах, самим устраивать такие встречи и обсуждения на регулярной основе. Между тем, увлечение частыми совещаниями чревато обернуться негативной стороной – количественным переизбытком информации в ущерб ее качеству, малополезной тратой рабочего времени.

Кстати, любовь к заседаниям, совещаниям, обсуждениям – свойство не только государственной бюрократии. Этой слабости подвержены и частные компании. Причем, не только в России. Эпидемия необязательных, малоэффективных совещаний давно охватила многие крупные организации за рубежом, в частности, в США. Как отмечает американский исследователь Дж.Уолтерс в книге “Big Vision, Small Business”, «побудьте в любой конторе, особенно в крупной компании, и вы увидите, как служащие ходят с одного совещания на другое, тратя часы на то, что требует в реальности 20-30 минут».

Уолтерс выделяет пять ключевых факторов, отличающих хорошее совещание от плохого (см. SCIP.online, Issue 46):

1. Прежде всего, ясно понимаемая задача, оправдывающая организацию совещания.

2. Четко разработанная программа, отвечающая задаче совещания.

3. Определение лимита времени, отведенного для совещания, строгое следование регламенту.

4. Требование от участников быть подготовленными, что предполагает, что они заблаговременно ознакомлены с темой и задачей совещания, знают, что от них ждут.

5. Достаточно искусное руководство ходом обсуждений, не позволяющее отвлекаться на второстепенные вещи.

"Бизнес-разведка"

В. Борисов

Криминальный спам – угроза личности и бизнесу

Десять лет назад, когда спам только заявлял о себе, его рассматривали, в том числе и в правовом отношении, как агрессивную коммерческую рекламу, несанкционированно вторгающуюся в сферу privacy. Как считают авторы исследования, проведенного американскими университетами во Флориде и Кэмбридже (www.prog.rif.ru/generateEvent), такое понимание спама с появлением в последние годы фишинга и других разновидностей мошенничества с использованием электронной почты, устарело. Требуется серьезная корректировка, отражающая серьезную криминализацию этого явления.

Спам ныне угрожает не только неприкосновенности частных прав. Он превращается в серьезную проблему для безопасности бизнеса, нанося ежегодный урон в десятки и сотни миллионов долларов, причем проблему международного характера.

Если поначалу большинство инициаторов спама концентрировались в США, то с принятием в этой стране жестких мер преследования и наказания спамеров последние расползлись по всему миру, проявляя особую активность там, где местное законодательство в этом смысле

довольно либерально. К ним относится и Россия. Опрос, организованный Лабораторией Касперского и информационным порталом SecurityLab в конце 2005 года, дал такие результаты:

- 30% пользователей e-mail не получают спам вовсе;
- 38% получают менее 5 спам-писем в год;
- 14% - от 6 до 10 спамерских сообщений ежедневно;
- 18% - более 10;

Таким образом, проблема спама затрагивает двух из трех пользователей электронной почты. Миллионы людей. При этом надо учитывать, как подчеркивают авторы российского исследования, что в нашей стране все больше пользователей используют Интернет для совершения покупок, банковских операций – потенциально половина российской интернет-аудитории. Но примерно каждый второй не знает, что такое фишинг.

Между тем, фишинг остается самым распространенным способом онлайнового мошенничества, нацеленного на кражу паролей, номеров банковских счетов, иной конфиденциальной личной информации, с помощью которой совершаются финансовые хищения. Обычно получаемые на персональные электронные адреса сообщения от имени «вашего банка» или иной «финансовой или торговой организации» выглядят с первого взгляда солидно, убедительно, нередко используется реальный логотип. Содержание такого послания, изложенная в нем просьба также звучит невинно, искусно копируя переписку реальных финансово-кредитных организаций со своими коллегами. Но достаточно вам ответить на запрос, и вы в ловушке. Используя предложенные в фальшивке линки, вы оказываетесь на сайте, очень похожим на настоящий. Главное для мошенников – получить доступ к финансовой информации.

Но этим далеко не исчерпывается криминализация спама. По-прежнему, в ходу такие испытанные приемы как «письма нигерийских вдов», заманивающих посулами огромных комиссионных за скромную помощь в «переводе средств», онлайновые «лотереи» и «сетевые пирамиды», фальшивые «наследства». Не говоря уже о примитивных попытках всучить вам по Интернету негодный, а то и отсутствующий в реальности товар. В последнее время в спамерской торговле растет доля контрабандных, контрафактных товаров, предложений наркотиков и других видов криминального бизнеса.

Антивирусные и антиспамовые программы помогают минимизировать риски, но стопроцентную безопасность не гарантируют. Несмотря на широкое применение этих программ криминальные спам-атаки продолжают наносит урон как отдельным гражданам, так и российской экономике в целом. По мнению координатора Проекта «Антиспам» Евгения Альтовского, цифра в 30 миллионов долларов – отправная точка в подсчете ущерба, наносимого спамерами экономике России. Для точного подсчета не хватает данных, с которыми «итоговая цифра, вероятно, возрастет на порядок» (crime-research.ru, 13.05.2006). Помимо чисто материальных потерь спам имеет и иные, не всегда выраженные в цифрах негативные последствия – затраты рабочего времени (и денег на оплату Интернета), дополнительные нагрузки на трафик в сетях.

В российском парламенте готовится антиспамовое законодательство, позволяющее надеяться, что борьба с этим явлением примет более широкие и эффективные масштабы. Но самой надежной гарантией были и остаются элементарная бдительность и внимательность. Эксперт по спаму А.Ларсон (“ExpertLaw”, June, 2004) предлагает две понятные, простые рекомендации:

1. Получив по e-mail сообщение от кредитно-финансовой или торговой компании, требующее раскрытие финансовой и/или личной информации, не торопитесь использовать содержащиеся в нем линки. Минуя послание, зайдите прямо на сайт настоящего банка (организации) и проверьте путем запроса, не их ли полученное вами послание. Нелишне заодно проверить и свой банковский счет – нет ли каких проблем, которые можно было бы своевременно решить. Эти проверочные процедуры требуют времени, но такие затраты не дороже денег, которыми вы рискуете.

2. Совсем просто, но зато наиболее надежно – проявлять повышенную осторожность в передаче своего электронного адреса помимо постоянных и проверенных корреспондентов.

И, конечно, нельзя пренебрегать установкой антивирусных программ, антиспамовых фильтров.

"Бизнес-разведка"

Аналитический отчет – преодолеваем психологический барьер

Конечный продукт, итог работы специалиста КР – отчет. Как правило, письменный. Короткий или длинный, обзорный или аналитический, констатирующий или заключающий выводы и предложения – отчет всегда требует серьезных интеллектуальных усилий.

Многие считают, что для написания аналитического отчета требуется особый талант, сочетающий способность к анализу и литературный дар. На самом деле это не так. Кто способен отбирать, систематизировать, осмысливать факты, полученные данные, тому вполне по силам толково изложить материал в виде информационного, аналитического отчета (за очень редким исключением). Поэтому рассуждения на тему «я не могу и не люблю писать отчеты» скорее обусловлены психологически негативным настроем, самовнушением, нежели отсутствием к этому способностей.

О том, как преодолеть такой психологический барьер, говорится в материале, размещенном на сайте MarketingProfs.com, 5 сентября 2006 г. (Daphne Gray-Grant, Five Negative Thoughts That Can Sabotage Your Writing).

Итак, рекомендации, как справиться с некоторыми распространенными самовнушениями.

«Я безнадежен, абсолютно нет писательских талантов». Мы все рождаемся «безнадежными», однако учимся и приобретаем необходимые навыки. Для этого надо три вещи:
- читать хорошие тексты и стараться им подражать;
- пытаться как можно больше писать, тренироваться;
- тратить на редактирование своего текста вдвое больше времени, чем на написание.

«У меня нет времени на писанину», Старайтесь писать быстро. По кусочкам. По 10 минут. Через какое-то время возвращаться и добавлять еще абзац, несколько предложений. А вот на редактуру времени жалеть не надо.

«Боюсь плохим отчетом испортить свою репутацию». Если такая мысль мешает приступить к делу, попробуйте от нее избавиться, полностью сосредоточившись на теме отчета. Пусть мысль о том, какое впечатление, хорошее или плохое, произведет ваш отчет на начальство и коллег, свербит во время редактуры, шлифовки теста, а не во время написания.

«Творить текст – неимоверно трудное занятие». Это как любая работа. Времена она кажется более трудной. Временами – менее. Главное, внушить себе, что писать отчет – очень даже приятное занятие. Это не таскать кирпичи под дождем или снегом. Напротив, комфортно сидеть в сухом, теплом помещении, у компьютера в удобном кресле (на стуле), рядом чашечка чая или кофе. А главное, очень хочется поделиться с коллегами своими мыслями и соображениями!

"Бизнес-разведка"

Как не надо управлять информационной службой
(по материалам журнала Information Management Journal)

Опросы сотрудников корпоративных библиотек, информационных служб компаний указывают на серьезные проблемы в отношениях между руководителями таких служб и рядовыми работниками, что негативно отражается на результатах работы.

Наиболее распространенные жалобы подчиненных на своих непосредственных

руководителей:

1. *Подавление инициативы.* «Он/она не позволяет и шагу сделать без разрешения и постоянного надзора». Самая распространенная жалоба. Так считают 25% опрошенных. Руководители, которые подавляют стремление своих подчиненных расти, совершенствоваться, проявлять самостоятельность и инициативу, всегда рискуют растерять хорошие кадры, а, следовательно, упускают возможность добиваться лучших результатов.

2. *Отсутствие коммуникабельности*. «Я не получаю необходимую для работы информацию. Я не знаю, что начальник ожидает от моей работы». Руководители проявляют некоммуникабельность в отношениях с подчиненными часто по причине уверенности, что последние уже знают, что от них требуется. Иногда не желают высказывать замечания. Тем самым, теряют управление, в котором нуждается коллектив.

3. *Искусственное разделение коллектива*. «Меня не уважают, мои способности и заслуги игнорируют. Меня не приглашают к обсуждению проблем». Разделение коллектива на «достойных и не совсем», т.н. фаворитизм, нередко проявляется у менеджера подсознательно, но четко улавливается подчиненными, воспринимающими это как несправедливое отношение к себе.

4. *Высокомерие*. «Этот человек всех нас считает идиотами, нисколько не считается с нашим мнением, нередко прилюдно оскорбляет». Менеджеры иногда чересчур агрессивно реагируют на ошибки подчиненных, не задумываясь о том, какое впечатление их поведение производит и к каким отрицательным последствиям оно может привести.

5. *Неумение слушать*. «Он/она совершенно не слушает меня, обрывает на полуслове и принимает решение, совершенно не считаясь с моим мнением», Такое поведение – проявление упоминавшегося выше «фаворитизма», отсутствие гибкости, чреватое грубыми просчетами.

6. *Бегство от конфликтов*. Одна из самых тяжелых ошибок – игнорировать возникающие в коллективе проблемы, позволять им разрастаться. Если сотрудники видят, что их начальник бежит от проблем – производственных или персонально-конфликтных, то они, естественно, будут его держать в неведении. Неведение – прямой путь к провалам.

7. *Кража идей и инициатив*. «Он/она сегодня говорит «нет» на мое предложение, а завтра выдает за свое». Довольно распространенная практика отношений в коллективе. Подрывает доверие, а главное, убивает любую творческую инициативу.

"Бизнес-разведка"

Ищем работу – как опередить конкурентов

В прошлом мы публиковали статьи и переводы о минимизации рисков компании при найме новых работников. Продолжая освещать важную проблему использования методов конкурентной разведки для обеспечения безопасности бизнеса предлагаем читателям несколько иной материал - о том, как быстрее и лучше найти работу в условиях высокой конкуренции на рынке труда. Своими соображениями делится эксперт по проблемам трудоустройства и профессиональной карьеры Дебора Уолкер (SCIP.online, Issue 49)

Нередко у хороших, востребованных на рынке, но не обладающих обширными связями, специалистов возникают немалые трудности в поиске достойной работы. Это особенно касается тех сегментов рынка, где идет острая конкуренция за приличные вакансии, высокооплачиваемые рабочие должности и места. Как помочь в разумные сроки найти то, что ищешь, и, самое главное, убедить работодателей в вашем превосходстве над другими соискателями?

Прежде всего, советует Д. Уолкер, надо разработать стратегический план, предусматривающий ряд важных моментов.

Резюме – самое важное в первых верхних строчках
Те, кому предназначено ваше резюме, начинают чтение с первых строк, но далеко не всегда просматривают до конца. Поэтому очень важно в этих, верхних строчках дать самую главную, самую интересную и привлекательную информацию о себе, сразу же заинтересовав потенциального работодателя.

Одно резюме – хорошо, несколько – лучше
Опыт эксперта показывает, что резюме отвергается, если оно не сфокусировано на конкретной цели, к которой стремится автор резюме. Если в одном резюме выражена готовность к разным видам деятельности, к различным должностным позициям, следует ожидать негативную реакцию. Поэтому, если вы действительно готовы и хотите пробовать себя в разных амплуа, лучше всего иметь несколько резюме, каждое – по конкретной позиции.

Сопроводиловка к резюме – не пустая формальность
Это факт, что от сопроводительного письма часто зависит, прочитают ли вообще ваше резюме. Чтобы быть в этом уверенным, сопроводиловка должна содержать нечто, что заставит адресат раскрыть и просмотреть ваше резюме. При этом необходимо помнить, что для искомой компании прежде всего важна квалификация, отвечающая требованиям менеджмента, а для кадрового агентства – характеристики, которые можно продать. Все это желательно кратко отразить в сопроводиловке.

Несколько советов по собеседованию
Готовясь к собеседованию с потенциальными работодателями, надо иметь в виду три основных этапа:
в начале интервью - задать вопросы, проясняющие, кто именно нужен компании;
быть готовым отвечать на вопросы, вытекающие из задач беседующего с вами менджера/кадровика;
в конце интервью – задать вопросы, которые помогут получить предложение о работе.

"Бизнес-разведка"

Т. Тимкова

К вам нагрянула проверка. Как себя вести?

(советы психолога)

Проверка – это всегда неприятно, но не смертельно. Как подготовиться к правильному общению с сотрудниками контрольно-надзорных органов? Как вести себя с ними? Каких ошибок следует избегать при таком общении? На эти и другие вопросы помогают ответить рекомендации психологов. Рассмотрим основные проблемы, возникающие в процессе общения с представителями контролирующих органов и пути их разрешения.

Процесс общения начинается с «вешалки»: с входа в помещение, знакомства и проверки документов: на фирме должен быть внедрен «кризисный план», где разработаны все схемы поведения и действия каждого сотрудника в случае прихода проверяющих. Поэтому в критических ситуациях проще тому руководителю, который произносит «ключевое слово» - и команда срабатывает так, как нужно...

Первыми в контакт с представителями проверяющих органов обычно входят представители службы безопасности (СБ) фирмы, от вежливости и тактической грамотности которых может зависеть настроение проверяющих. От СБ во многом зависит и скорость проникновения проверяющих на фирму в случае, если проверка внеплановая (проверка документов может занимать долгое время...);

В это время руководителю необходимо успокоиться, дать необходимые инструкции и психологически подготовить персонал. Как успокоиться самому и успокоить других? Необходимо знать, что для нормального человека существует три типичные реакции в экстремальных ситуациях:
- Резкое понижение организованности поведения (дезорганизация, «предстартовая

лихорадка»). Дезорганизация поведения может проявляться в неожиданной утрате ранее приобретенных навыков. Может произойти резкое снижение надежности действий, движения приобретают импульсивный, неорганизованный характер, появляется суетливость, сумбурность. Нарушается логичность мышления.
- Резкое торможение активных действий (предстартовая апатия), состояние ступора, оцепенения.
- Повышение эффективности действий (психологическая готовность). Выражается в мобилизации всех ресурсов психики человека на преодоление неблагоприятной для него ситуации. Здесь наблюдается мобилизация сознания, повышенный самоконтроль, четкость восприятия и оценки происходящего, совершение адекватных ситуации действий и поступков.

Зная возможную реакцию сотрудников на экстремальную ситуацию (агрессия, истерия, паника и т.д.), руководителю легче прогнозировать и держать под контролем складывающуюся ситуацию. Людей, переживший травматический опыт в прошлом, склонных к неадекватным реакциям, необходимо психологически готовить или в период проверки отправить с фирмы по каким-либо делам.

Лучше, если Вы знаете своего проверяющего. Но если Вы не знакомы, то Вам придется обучиться методике не только быстро оценивать своего оппонента, но и мгновенно вызывать к себе симпатию, а также – технике эффективного знакомства:

Необходимо учитывать, что контакт устанавливается невербальными (неречевыми) средствами – это взгляд, улыбка, жесты доверия. Нежелательно отводить глаза в сторону или смотреть под ноги, лучше использовать тактику «глаза – в глаза». Все внимание должно быть направлено на этого человека. Необходимо определить дистанцию комфортного общения. Желательно сразу использовать приемы подстройки под собеседника – садясь в ту же позу, «отзеркаливая» жесты собеседника, наблюдая за его мимикой и т.п. Ваша речь не должна отличаться от речи собеседника ритмом, громкостью, лексикой, профессиональным жаргоном. Это быстро создаст ауру взаимной симпатии и доверия.

Если Вы испытываете страх, чувство зажатости, самое верное дело – заранее иметь в запасе ряд проверенных в действии речевых или поведенческих заготовок. Например:
• представьте, что человек, с которым Вам предстоит познакомиться – Ваш лучший друг детства…;
• можно рассказать свежий анекдот или достойную внимания притчу;
• рассказать какую-либо свежую интригующую информацию;
• сделать скрытый комплимент (фальшь и лесть всегда улавливаются);
• эффективным может быть и постепенное вхождение в контакт, когда Вы активно слушаете и расспрашиваете собеседника, задавая открытые вопросы типа «А что Вы думаете по этому поводу?»;
• чаще называйте собеседника по имени, так как для многих нет ничего слаще звучания собственного имени;
• проявите к проверяющему неподдельный интерес, дайте почувствовать человеку его значимость;
• используйте приемы «землячества», «родственные души», «общие знакомые», «служба в армии», ведь всегда находится что-то общее…;
• идите на совместные действия, даже «чайная церемония», хождение по офису может укрепить Ваш контакт с проверяющим (параллельные действия укрепляют подстройку под клиента);
• продемонстрируйте позитивный настрой и открытость, желательно ни о ком не говорить плохо;
• используйте юмор. Помните, что человек, обладающий чувством юмора, всегда выглядит привлекательным и симпатичным;
• выразите уверенность в плодотворности дальнейших действий и контактов.

К моменту окончания знакомства, у Вас должно сложиться мнение о проверяющем, его психологический портрет и представление о его предполагаемых слабостях, психологических комплексах. В завершении знакомства необходимо подвести итоги, еще раз выразить готовность к дальнейшему сотрудничеству. Последняя фраза должна строиться по принципу: «Жалко с вами расставаться (очень приятно было пообщаться, надеюсь, это не последняя наша встреча)»…

При предъявлении документов – откровенно признавайте мелкие недостатки, не ожидая претензий со стороны собеседника. Воздействуйте на психологические комплексы великодушия и превосходства. Держите ситуацию под контролем; следует ссылаться на весомое одобрительное мнение авторитетных людей о вашей работе (положительными отзывами о предыдущих работах и благодарственными письмами полезно «украсить» кабинет).

Навязывайте проверяющему выгодную Вам модель эксперта. Поставьте оппонента в ситуацию «выбор – без выбора». Например: «Я могу дать Вам подробное заключение по этому вопросу. Мне приходилось этим заниматься и раньше. Мне самому этим заняться или мы поработаем вместе? Окончательное решение принимать Вам» и др.

Не указывайте проверяющим на их ошибки, когда они готовят документ об административном правонарушении. В дальнейшем все эти ошибки будут толковаться в Вашу пользу, предоставляя Вам возможность обвинить сотрудника контролирующего органа в нарушении действующего законодательства. Как сказал величайший китайский полководец Сунь-Цзы: «Непобедимость заключена в самом себе, а возможность победы заключена в противнике».

"Бизнес-разведка"

Т. Маркевич

Как минимизировать потери в области потребительского кредитования коммерческого банка

Риск и бизнес - это два неразделимых понятия, избежать кредитного риска нельзя, его можно только минимизировать. Только благодаря комплексному подходу к решению проблем безопасности и правильному сочетанию различных ее составляющих, можно чувствовать себя уверено. Для достижения минимизации кредитных рисков используется большой арсенал методов, включающий формальные, полуформальные и неформальные процедуры оценки кредитных рисков.

При оценке кредитных рисков большинство банков применяют скоринговые модели: специальные программы, которые, сопоставляя доходы и расходы заемщика, делают вывод о том, сколько он может платить. Клиент заполняет анкету, в которой указывает место работы, состав семьи, образование и проч. По каждому параметру он попадает в определенный диапазон, в соответствии с которым ему присваиваются баллы. Сумма баллов определяет «кредитоемкость» заемщика, т.е. сколько он может платить. На основе этого банк рассчитывает максимальную сумму кредита. Настройки скоринга у каждого банка индивидуальны: они нарабатываются с опытом, корректируются с учетом российской специфики. Одному и тому же заемщику в разных банках будут предложены совершенно разные условия.

Естественно, что со временем и при различных условиях требования скоринга постоянно изменяются. Этим, как правило, занимается отдел минимизации рисков, целью которого является предотвращение потерь на этапе, предшествующем самому факту выдачи кредита.

Мошенничество является неизбежным злом всяких товарно-денежных отношений. Искоренить его невозможно. Поэтому единственной возможностью избежать «мошеннического дефолта» являются превентивные меры против потенциальных угроз.

Такими угрозами могут быть:

- выдача кредита лицам, заведомо неплатежеспособным;

- выдача кредита по поддельным документам;

- выдача кредита по утерянным ранее документам;

- выдача кредита лицам, ведущим асоциальный образ жизни (бомжи, наркоманы, алкоголики);

- выдача кредита «криминальным элементам»;

- выдача кредита «собирателям кредитов».

Это то, что касается этапа общения «клиент – специалист банка в точке продаж», но, к сожалению «нечистыми на руку» бывают не только клиенты, но и специалисты по продажам банка и партнеры, привлекаемые в процессе ПК создают определенный спектр проблем, в их числе:

• Наем на работу банком в качестве специалиста по продажам человека, связанного с мошенническими ОПГ.

• Привлечение банком к сотрудничеству недобросовестного партнера (в данном случае - торговой точки, предоставляющей товары в кредит)

• Наем на работу торговым предприятием – партнером банка – в качестве специалиста, оформляющего заявки, человека, не имеющего мошеннических намерений, но добросовестно выполняющего указания руководства данной торговой точки по увеличению продаж товара в кредит любой ценой.

Для исключения вышеперечисленных угроз отделом минимизации угроз решаются следующие внешние задачи::

- Обеспечение кредитного конвейера необходимыми для верификации базами данных.

- Регулярный анализ и формирование «черных списков», выделение информации на автоматический «отказ», введение информации в систему скоринга.

- Обеспечение принятия решения по клиенту при возникновении затруднения на этапе верификации.

- Информационная проверка торговых предприятий – будущих партнеров Банка и их сотрудников в области ПК (в том числе и вновь принятых на предприятии – действующие параметры Банка) и формирование внутреннего архива.

- Аналитический мониторинг действующих торговых точек на предмет дефолтности, программное обеспечение работы подразделения.

- Оперативный мониторинг как действующих, так и вновь привлекаемых к сотрудничеству торговых точек (негласный выезд сотрудника группы оперативного контроля , с целью проведения наблюдения за ТТ и ее продавцами на предмет выявления мошеннических действий).

К сожалению, существует и внутренняя проблема – неподготовленность (неготовность) персонала к противодействию мошенничеству. Основная задача подразделения в данном направлении – работа с персоналом, который сталкивается с мошенниками в момент оформления кредитов и проведение проверки предоставляемых данных.

Персонал кредитных учреждений, работающий в торговых организациях - это, как правило, молодые люди и девушки в возрасте от 18 до 25 лет. Часто - это студенты, работающее по 12-ти часовому графику, не имеющие опыта работы с людьми, интуитивных навыков, и даже значительного жизненного опыта (не говоря уже об опыте выявления мошенников и противодействия им).

Вместе с тем, как показывает практика, мошенничество в данной сфере не отличается сверхвысоким уровнем эрудированности и изобретательности. Это тоже люди в среднем 20 - 35 лет. Действуют они по довольно наработанной схеме, основанной главным образом на невнимательности и неопытности в работе сотрудников банка, принимающих клиентов. Мошенники преследуют цель обмануть сотрудника банка, создав имидж респектабельного человека, действительно желающего приобрести товар в кредит за счет выбранного им банка, намеревающегося добросовестно производить выплаты. При предъявлении чужих (утраченных или похищенных) документов мошенники прибегают к маскировке,

гримированию, отвлечению сотрудника различными приемами и т.п. Они также допускают массу ошибок - часто «прокалываются». Мошенников такого рода можно отнести к средней группе распознаваемости. Их нельзя сравнивать с мошенниками «высшего пилотажа». Поэтому требования к персоналу в сфере потребительского кредитования, хотя и не настолько высоки, как, например, к персоналу в сфере автокредитования, но, тем не менее, сотрудникам отдела контроля кредитного процесса приходится акцентировать внимание на обучение принимаемых сотрудников способам противодействия мошенничеству.

Важное значение имеет стратегия подбора. После изучения подразделением по персоналу данные проверяются и анализируются службой безопасности, т.е. осуществляется более тщательная и глубокая проверка кандидатур с использованием возможностей подразделений безопасности.

Кроме проверки кандидатов на работу, контроля их работы и постоянного обучения разрабатываются и совершенствуются способы мотивации сотрудников (как материальной, так и нематериальной), которая напрямую связана с обеспечением безопасности и занимает важное место в ее обеспечении. Существует и всячески культивируется практика поощрения сотрудников, выявляющих мошенников. Это, как правило, выявление лиц, оформляющих кредиты по чужим (утраченным) документам, лиц, заполняющих анкеты под влиянием третьих лиц. При этом очень важно недопущение негативных последствия для бизнеса, т.к. возможны «перегибы» в проявлении «сверх бдительности».

Следует отметить, что нематериальной мотивацией сотрудников наряду с вынесением благодарностей руководству сотрудника со стороны руководства может являться и моральное удовлетворение от результатов профессионально выполненного долга. Как правило, сотрудники, выявившие и изобличившие мошенников, продолжают работать более активно в этом направлении. У них появляется «азарт сыщика», они начинают замечать то, на что раньше не обращали внимание и оценивать окружающую обстановку с точки зрения ее криминогенности, становясь, таким образом, активными помощниками в противодействии мошенникам.

Об авторе: Маркевич Татьяна Витальевна. Имеет высшее технологическое и юридическое образование. Десять лет проработала в МУРе. В настоящее время – начальник отдела «Альфа-Банка».
markevich@mosfirm.ru

"Бизнес-разведка"

Е. Кобелев

Анализ возможных угроз и рисков в системах электронных платежей и Интернет-трейдинга

Основной проблемой, возникающей при обеспечении информационной безопасности электронной коммерции, является проблема защиты информации в электронных платёжных системах. Решение этой проблемы связано с использованием smart-карт, криптографических методов и защищённых протоколов взаимодействия.

Четыре причины недоверия электронным платёжным системам.

1. Юридический статус всех известных электронных платежных систем до сих пор не определен, а кража электронной наличности (даже в особо крупных размерах) не является "кражей" в уголовно-процессуальном смысле и если преследуется, то не так строго, как кража бумажных денег. Отсюда естественный соблазн поживиться. Возникает целая армада воинствующих хакеров, специализирующихся на виртуальных кражах. Разработчики электронных платежных систем настаивают на том, что защитные механизмы несокрушимы, а во всех кражах (уже принявших массовый характер) виноваты пользователи, которые не поставили (или неправильно настроили) брандмауэр, вовремя не обновили антивирус, не скачали свежий сервис-пак и т.д.

2. Электронные кошельки, хранимые на жестких дисках или сменных носителях, в один миг

могут быть уничтожены энтропией (сбоем операционной системы, аппаратным отказом и т.д.). Восстановить электронный кошелек в большинстве случаев все-таки возможно, но сколько времени и денег уйдет на это. Бумажные деньги, по крайней мере, не исчезают вдруг и бесследно.

3. Единой платежной системы нет, а обмен деньгами между различными платежными системами до безобразия затруднен. Например, популярный на западе PayPal официально обслуживает только американцев, и оплата по PayPal из России вызывает большие проблемы. Перевести деньги с помощью нее, конечно, возможно, но вопрос в том, насколько это просто. В противном случае исчезает главное преимущество электронных денег - прозрачность и простота.

4. Далеко не все участники рынка принимают электронные деньги к оплате. Например, одна фирма переводит зарплату на электронный кошелек, другая - нет. Какой-то провайдер принимает электронные деньги к оплате, какой-то - нет. Так что наличие электронных денег - еще не гарантия того, что удастся воспользоваться ими.

5. Если при заказе наложенным платежом трехтомника Кнута вместо него получили кирпич, то можно не брать данное керамическое изделие, а дать им по голове курьеру. В данной ситуации продавцу просто не выгодно обманывать покупателей, но при оплате электронными деньгами жульничество встречается сплошь и рядом. Даже кирпича не пришлют - просто покажут палец. Существует железное оправдание: "«Кража электронной наличности - вообще-то не кража". Владельца магазина, который работает с электронной наличностью, отмажет любой адвокат. Документов, подтверждающих перевод (пригодных для суда), у потерпевшей стороны все равно нет, а отследить получателя платежа нереально.

Угрозы:

- угроза внедрения на клиентский компьютер хакерской программы, которая опустошает электронный кошелёк;

- угроза перехвата канала связи плательщика и получателя;

- угроза внедрения ложного эмитента. Во многих платёжных системах предусмотрена авторизация клиента сервером, но отсутствует авторизация сервера клиентом.

- угроза взлома самого эмитента.

При ведении деятельности на Internet-бирже можно столкнуться со следующими видами *рисков*:

- риск, связанный с влиянием внешней среды (государственных органов и структур РФ, мировых событий и иных факторов);

- риски, связанные с Internet-трейдингом. Осуществление операций с ценными бумагами с использованием Интернет-трейдинга приводит к возникновению рисков, связанных с недостаточно надёжной работой оборудования, программного обеспечения или каналов связи; в результате возможно возникновение ситуации, когда поручение трейдера исполняется не в соответствии с содержащимися в нём указаниями, либо не исполняется совсем.

- ценовой риск. Риск заключается в возможном изменении цен на акции таким образом, что убытки возникнут даже без ведения операций на фондовом рынке.

- риск уменьшения ликвидности. Возможное уменьшение инвестиционной привлекательности акций для участников фондового рынка, вплоть до полной потери ликвидности, связано, как правило, с тенденциями фондового рынка, а также инвестиционным и финансовым положением эмитентов, либо с приостановкой торгов по причинам резкого изменения цены инструмента как в сторону увеличения, так и в сторону уменьшения, либо с техническими неполадками самой торговой системы.

- риск маржинального кредитования. Работая с заёмными средствами брокера, трейдер рискует ошибиться в существующей на фондовом рынке ценовой тенденции и понести

убытки больше, нежели работая только со собственными средствами; при этом убытки будут тем больше, чем больше соотношение заёмных средств к его собственным средствам.

Так как в нашей стране не развита нормативно-правовая база, обеспечивающая безопасность работы с различными средствами электронного платежа, то не следует доверять этим системам. Использование подобных систем удобно для осуществления микроплатежей в Internet-магазинах, но не следует зачислять на свой Web-кошелёк значительные суммы денег, так как риск потерять их слишком велик, а возможности доказать пропажу и тем более вернуть свои средства нет. Такая незащищённость и отсутствие наказания за хищение электронных денег привлекает толпы хакеров желающих опустошить чужие Web-кошельки.

При крупных перечислениях через Internet безопаснее пользоваться кредитными и дебетовыми средствами платежа, так как при данных видах оплаты остаются документы, подтверждающие осуществление транзакций и есть стороны, отвечающие по своим обязательствам.

При осуществлении операций на Internet-бирже трейдер переводит свои средства на субсчёт брокера дебетовыми средствами платежей, а следовательно риск, связанный с переводом средств, сведён к минимуму. Но существуют риски, связанные с неопытностью и невнимательностью самого трейдера, и риски, связанные со своевременностью и достоверностью получаемой и передаваемой информации между трейдером и биржей, так как она проходит через брокера, который теоретически может нарушить её своевременность, достоверность, целостность. Риск нарушения достоверности и целостности тоже сведён к минимуму, так как это прописано в регламентах и установлена ответственность. А вот своевременность информации ничем не гарантирована. При нарушении своевременности информации у трейдера наступает риск потери части прибыли или даже всех своих собственных средств. Особенно опасна данная ситуация при совершении маржинальных сделок, поскольку брокер имеет право самостоятельно закрыть позиции трейдера при соответствующем движении рынка. Следовательно, риск нарушения своевременности информации о рынке ценных бумаг очень опасен для трейдера.

Об авторе: Кобелев Евгений Юрьевич
Студент шестого курса «Московского Энергетического Института (Технического Университета)», специальность «роботы и робототехнические системы», прошёл профессиональную переподготовку в «ЦПП Институт безопасности бизнеса и личности».

"Бизнес-разведка"

Еще раз о т.н. «вторичных источниках»

Мы продолжаем знакомить с публикациями Д.Карпе, посвященными «вторичным» ресурсам информации для КР, которые эксперт по интернет-ресурсам рассматривает не менее важными, чем «первичные» источники.

В частности, к числу недооцененных и мало используемых в конкурентной разведке интернет-ресурсов Д. Карпе относит кино, телевидение, аудио и видео файлы. Он обращает внимание на огромное число фильмов, художественных и документальных, сфокусированных на той или иной проблеме, теме. Советует посетить сайт www.imbd.com (Internet Movie Database), либо специализированные на документальном кино разделы таких известных коммерческих сайтов как Amazon.com, netflix.com. Там можно встретить интервью, комментарии, полезные ссылки на архивированные источники, онлайновые библиографии и т.п.

Определенный интерес могут представлять теле и радио – транскрипты (тексты теле и радио интервью, дискуссий, комментариев), которым уделяется в Интернете все больше внимания. Автор предлагает, в частности, просматривать в поисках профессионально интересного транскрипта сайт www.tveyes.com

Точно так же полезными могут оказаться аудио и видео-компоненты корпоративных

сайтов. Например, на сайте компании Sun Microsoft можно отыскать в архивах видеоклипы, презентации, интервью, содержащие массу потенциально полезной информации. В том же ряду стоят веб-семинары и конференции. Речь идет не только об архивных материалах. Карпе рекомендует профессионалам КР участвовать в такого рода онлайновых мероприятиях.

Он также советует не пренебрегать и фотографиями. К примеру, имеется задача подготовить справку о конкурирующей компании. В прессе или интернете вы встречает фотографию с деловой вечеринки или презентации, на которой изображены пять человек, представляющих топ-менеджмент компании-цели. Фотография с текстовкой и перечислением сфотографированных лиц. Это уже неплохая первичная информация о потенциальных ваших собеседниках, ведь кто-то из них, не исключено, пойдет на контакт. Некоторые сайты, в частности, принадлежащий Smithsonian Institute Research Information System сайт www.siris.si.edu, имеют отличный архив фотодокументов.

"Бизнес-разведка"

Проверка информационной системы – путь к эффективности и экономии

Автоматические информационные системы, позволяющие вести мониторинг интернета и СМИ в круглосуточном режиме, становятся все более популярными. К их достоинствам и недостаткам наш журнал обращался неоднократно. Собственно, главный их недостаток – довольно высокая стоимость, исчисляемая десятками и сотнями тысяч долларов. Тем не менее, спрос на них высок. Ведь, как говорят в мире бизнеса, «чтобы делать деньги, нужно тратить деньги». Вопрос в том, эффективно ли используются инвестиции в информационные технологии, каков баланс в формуле «затраты=реальная отдача».

Наиболее часто встречающиеся случаи несбалансированности, когда инвестиции в IT не дают ожидаемого результата, связаны с плохой корпоративной информационной инфраструктурой – слабая интеграция входящих в нее систем, отсутствие единого интерфейса, дублирование т.п. В результате идут сбои в получении информации, и сама информация нередко искаженно отражает реальную картину. А причины неудовлетворительного использования дорогостоящих автоматических систем, как правило, не лежат на поверхности, а требуют серьезной проверки и анализа по всей цепочке отбора и прохождения информации вплоть до ее появления на экранах компьютеров конечных пользователей.

Джейн Гриффитс, автор программ для деловой разведки, предлагает свою методологию обнаружения недостатков, слабостей информационной инфраструктуры (DM Review Magazine, May 2006 Issue). Методология включает четыре последовательных процесса:

1. Проверка системы поиска и отбора информации. Необходимо проанализировать работу таких компонентов как информационные ресурсы, подлежащие мониторингу, и фильтры, обеспечивающие отбор данных.

2. Второй процесс включает проверку системы подготовки отчета: репозитарий и хранилища данных, инструментарий выборки и систематизации данных, приложения, обеспечивающие формирование отчетов.

3. Затем следует проанализировать технологии, отвечающие за выход информации в форме готовых отчетов и их прохождение до адресатов (именно в этом звене наиболее часто встречается дублирование).

4. И, наконец, анализ того, как информация используется: кто потребляет информацию, сколько всего потребителей, и, главное, как они используют информацию в своей деятельности.

«Возможно проведенная проверка, - пишет в заключение Дж. Гриффитс, - вас неприятно удивит. Но зато теперь у вас в руках информация, с помощью которой вы можете избавиться от дублирования и других изъянов, повысить отдачу от информационной системы, а, значит, сберечь немало денег».

"Бизнес-разведка"

Мужчины и женщины в интернете: общее и различия

Эксперт по интернету Дебора Феллоу опубликовала ряд статей, посвященных особенностям использования Интернета мужчинами и женщинами (см. www.pewinternet.org). Предлагаем некоторые результаты и выводы ее исследований.

Мужчина по сравнению с прекрасным полом более интенсивно пользуются интернетом, тратя на это заметно больше времени. Он чаще используют возможности интернета для получения информации, причем по более широкому спектру проблем и тем. Мужчины больше женщин используют Интернет в целях отдыха и развлечений – просмотра онлайнового контента своего хобби, чтения для удовольствия, игр и пр. В то же время мужчины демонстрируют повышенную восприимчивость к новым интернет-технологиям, большую склонность к использованию новых поисковых систем.

Женщины же в отличие от мужчин проявляют себя в первую очередь как «онлайновые коммуникаторы», т.е. в большей степени используют электронную почту для поддержания контактов с друзьями и знакомыми. Среди тем онлайновой переписки доминируют – семейные, бытовые новости, договоренности о встречах, обмен шутками и анекдотами. Если мужчины больше используют e-mail для деловых целей, то женская онлайновая переписка характеризуется большим тематическим разнообразием.

Что объединяет тех и других – так это одинаково высокая оценка интернета с точки зрения практической эффективности – интернет облегчает работу и жизнь, помогает экономить время и деньги. В то же время их подход к интернету как источнику безбрежных информационных ресурсов различается. Мужчины «копают» глубже и шире – от финансовой информации до политических новостей. Они используют поисковые машины более агрессивно, интенсивно, с большей уверенностью, чем женщины.
Женщины «залезают» глубоко в информационные массивы по интересующим их вопросам, например, медицина и здоровье. Но все же в отличие от мужчин предпочитают интерактивное общение в онлайновом режиме.