БИЗНЕС-РАЗВЕДКА

№ 63

Оглавление

Геннадий Перминов
OSINT: не нужно быть хакером, чтобы узнать о цели все

OSINT (Open Source Intelligence) – это способ получения информации, основанный на поиске в общедоступных источниках. Объем рынка OSINT *превысил* 5,24 миллиарда долларов США в 2023 году и, по прогнозам, достигнет 38,48 миллиарда долларов США к концу 2025 года. Чем вызван интерес к этому сегменту и почему популярность подобных техник будет расти, в данной статье разберет **Геннадий Перминов**, ведущий консультант по кибербезопасности технического Департамента компании RTM Group.

В основе OSINT лежит искусная работа с общедоступной информацией. Эксперты используют такие ресурсы, как социальные сети, новости, видео, блоги, данные, которые стали общедоступны в результате различных утечек. Ключевой особенностью OSINT является то, что профессионал деловой разведки не взаимодействует с исследуемой информационной системой или человеком и поэтому никак не выдает свою деятельность.

OSINT — это гибкий инструмент, который продолжает развиваться вместе с технологиями и ростом объемов публичной информации. Ожидается, что среднегодовой темп роста (CAGR) услуги *составит* почти 25% в период с 2023 по 2032 год.

Среди основных сфер применения OSINT:

- Маркетинговые исследования: анализ репутации бренда, товара, прогнозирование потребительских трендов
- Оценка финансовых рисков: мониторинг рынков, выявление потенциальных угроз для инвестиций, оценка рисков, связанных с партнерами или потенциальными слияниями и поглощениями
- Конкурентная разведка: анализ действий конкурентов, их новых продуктов, маркетинговых стратегий
- Проверка потенциальных кандидатов
- Военная и государственная безопасность: отслеживание международной обстановки, анализ активности потенциальных противников, изучение новостей и социальных сетей в целях предотвращения угроз
- Журналистика: проверка фактов, проверка источников, установление хронологии событий
- Противодействие терроризму: отслеживание активности террористических групп, выявление угроз и предотвращение атак через анализ в социальных сетях, на форумах и других онлайн-ресурсах
- Мониторинг инцидентов безопасности: анализ утечек данных из открытых баз позволяет оперативно реагировать на инциденты
- Правоохранительная деятельность: раскрытие преступлений, поиск подозреваемых, поиск пропавших людей.

Основные источники данных для OSINT

Основные источники OSINT, как правило, известны многим из нас. Когда мы собираем информацию о товаре для покупки или пытаемся найти сведения о бывших одноклассниках, чтобы связаться с ними, мы просматриваем множество ресурсов, используем поисковые системы и/или социальные сети.

Среди основных способов получения данных:

- Официальные реестры, включая базы юридических лиц и патентные БД
- Социальные сети. Являются богатым источником данных о поведении, предпочтениях и связях пользователей. Например, анализ их активности помогает определить рамки рабочего времени или распорядок сна, а фотографии на странице могут рассказать о месте жительства, посещаемых местах, семье и так далее
- Тематические форумы и сообщества. Используются для мониторинга специфических групп интересов, например, связанных с технологиями или кибербезопасностью
- Видеохостинги помогают анализировать контент для получения визуальной информации о событиях, продуктах или местах
- Подкасты и аудиозаписи. Используются для извлечения данных о мнениях, анализе обсуждаемых тем или ключевых персон
- Сервисы карт. Цифровые карты предоставляют данные о местоположении, маршрутах и инфраструктуре искомого объекта.

Инструменты и методы OSINT

У каждого специалиста по OSINT свой набор инструментов, который ему привычен. Одни сервисы абсолютно бесплатны, а для других требуется платная подписка или разовая оплата доступа. Вот некоторые популярные методы для поиска информации:

- Поисковые системы. Такие платформы, как Google и другие «поисковики», являются базовыми инструментами для OSINT. Их возможности не трудно расширить за счёт применения специальных операторов (дорков), например: "site:", "filetype:", "intitle:" и других. Они позволяют уточнять запросы, находить документы определённого типа или ограничивать поиск конкретным сайтом. Например, оператор "cache:" позволяет просматривать сохранённые версии страниц, а "inurl:" — находить URL с определёнными словами.
- Веб-скрапинг — метод автоматического извлечения данных с веб-страниц. Он используется для сбора больших объёмов информации, недоступной через обычные поисковые запросы. Есть, к примеру, Beautiful Soup — библиотека Python для парсинга HTML и XML-документов.
- Программы анализа, такие как Hootsuite и Brandwatch, предоставляют возможности для бизнес-анализа брендов.
- Методы определения местоположения. Современные приложения, такие как Google Earth, позволяют проводить детальный анализ местности. Кроме того, сервисы геолокации могут использовать метаданные из фотографий и видеозаписей для точного определения местоположения.
- Сбор данных из публичных профилей в соцсетях (например, Facebook, Instagram, Twitter, LinkedIn). Использование специализированных инструментов для анализа активности пользователей и создания графов взаимодействий (например, Maltego, Social Search).
- Слежение за изменениями на веб-страницах с применением автоматических инструментов (например, Visualping, Distill.io).
- Поиск утечек данных в открытых базах данных или на ресурсах, связанных с хакерской активностью (например, HaveIBeenPwned).
- Поиск в публичных реестрах (например, торговых и корпоративных регистрах, налоговых и судебных БД). Изучение документов, доступных через официальные сайты госорганов или в открытых библиотеках (например, научные статьи, правовые документы).
- Использование инструментов для анализа доменов (например, Whois) и IP-адресов для выяснения их принадлежности и связей с другими ресурсами.
- Изучение видео и изображений на платформах вроде YouTube, Vimeo, Instagram для поиска информации, которая может помочь в расследовании.
- Использование специальных OSINT-инструментов, включая Maltego, Recon-ng, SpiderFoot и другие, которые помогают автоматизировать процесс сбора информации и анализировать ее.

Перечень инструментов и методов, применяемых в OSINT, безграничен и зависит от конкретных задач.

Пример OSINT на основе анализа закупок

В качестве примера применения OSINT в нашей работе приведу результаты исследования, в рамках которого был проведен анализ закупок одной из компаний за несколько лет. В результате удалось собрать большой объем аналитической информации не только об отдельных компонентах внутренней инфраструктуры компании, открытых непосредственно в закупках, но и об особенностях бизнес-процессов организации, ее приоритетах.

Так, в результате анализа закупок было обнаружено:

1. Аналитическое и бизнес-аналитическое ПО

SAS Analytics Pro, QlikView: эти программные продукты указывают на наличие развитой аналитической системы в организации. Программное обеспечение SAS используется для продвинутого анализа данных, а QlikView — для бизнес-анализа и создания отчетности.

2. Интеграция и обмен данными

SAS/ACCESS Interface to ODBC, SAS/ACCESS Interface to PC File Formats: эти компоненты говорят о необходимости интеграции различных систем и баз данных. Это может свидетельствовать о том, что организация работает с различными источниками данных, включая базы данных и файлы из разных форматов, требующие универсальных интерфейсов для их обработки.

3. Системы управления и безопасности данных

Symantec Endpoint Protection, Kaspersky Security for Mail Server, TrendMicro: это программное обеспечение подтверждает наличие системы защиты данных и почтового трафика. Организация явно уделяет внимание безопасности конечных точек и почтовых серверов.

HPE Arcsight Express: платформа для централизованного мониторинга событий безопасности — это свидетельствует о наличии системы для отслеживания и анализа событий информационной безопасности.

Falcongaze SecureTower: этот продукт, вероятно, используется для мониторинга активности пользователей, предотвращения утечек данных и управления правами доступа.

4. Информационные системы для документооборота и юридических вопросов

Система электронного документооборота TESSA: это решение свидетельствует о наличии автоматизированной системы для обработки и управления документами внутри компании.

КонсультантПлюс, Casebook: эти программные инструменты связаны с правовыми вопросами — автоматизацией юридической работы и мониторингом судебных дел. Также это указывает на важность соблюдения законодательства и управления правовой информацией.

5. Инструменты для мониторинга и управления

Backup Exec: программное обеспечение для резервного копирования и восстановления данных. Это решение подтверждает, что организация уделяет внимание обеспечению резервных копий для защиты от потери данных.

InfoWatch Traffic Monitor Advanced: это ПО используется для мониторинга трафика, что указывает на внимание к безопасности сети и предотвращению утечек информации.

Система для мониторинга судебных дел: это решение также указывает на важность контроля правовых аспектов бизнеса и связи с внешними контрагентами.

6. Системы для обучения и управления

Система для дистанционного обучения WebTutor: указание на системы для онлайн-обучения и управления обучением в компании. Это может означать наличие программ, которые повышают осведомленность и квалификацию сотрудников или клиентов компании.

7. Оборудование для хранения данных

Ленточные носители HP Ultrium LTO-5 RW для долговременного хранения данных или резервного копирования информации. Это решение важно для архивирования данных на долгосрочной основе.

8. Интеграция с мобильными решениями

AirWatch, NitroDesk Touchdown: эти решения позволяют управлять мобильными устройствами сотрудников, что может быть связано с управлением мобильной инфраструктурой и поддержкой мобильных сотрудников.

9. СКЗИ и криптография

СКЗИ «КриптоПро CSP» и Мастерчейн: наличие этих инструментов говорит о применении системы криптографической защиты информации, что также указывает на высокие требования к безопасности данных и защиты информации на уровне законодательных норм.

Таким образом, можно сделать некоторые выводы об информационной инфраструктуре:

- Информационная безопасность: системы защиты (антивирусы, системы мониторинга безопасности, криптография) играют важную роль в инфраструктуре, что указывает на высокий уровень внимания к защите данных.
- Аналитика и управление данными: использование аналитических инструментов и систем для интеграции и обработки данных свидетельствует о развитой инфраструктуре для работы с большими объемами данных.
- Автоматизация и документооборот: наличие решений для автоматизации юридических процессов и документооборота говорит о стремлении к оптимизации внутренних процессов.
- Дистанционное обучение и управление мобильными устройствами: это решение может указывать на стратегию по обеспечению гибкости работы сотрудников.
- Резервное копирование и хранение данных: применение инструментов для резервного копирования данных и архивирования говорит о планировании защиты информации на долгосрочной основе.

В целом, организация имеет развитую информационную инфраструктуру с акцентом на безопасность данных, защиту конфиденциальной информации, аналитические решения и эффективное управление документами и процессами.

Заключение

Мы коснулись лишь малой части того, что представляет собой искусство OSINT. Узнать подробнее можно здесь.

Об авторе: Геннадий Перминов, ведущий консультант по информационной безопасности консалтинговой компании в области информационной безопасности, судебной экспертизы и

ИТ-права RTM Group. Профессиональный опыт в сфере информационных технологий и информационной безопасности с 2008 года.

Образ мышления мошенника. Некоторые аспекты психологического анализа

Поведение мошенника невозможно понять, не изучив, что сам преступник думает о своих криминальных схемах. Познав, как образ мышления злоумышленника проявляет себя, мы получаем возможность точнее определить возможные последствия хода мыслей, соответствующего поведения и адекватно на них реагировать.

По данным исследования «Внутрикорпоративные преступления в 2024 году», проведенного ассоциацией экспертов по вопросам мошенничества (Association of Certified Fraud Examiners - ACFE), 87% виновных в совершении внутрикорпоративного мошенничества никогда ранее не были замечены в правонарушениях. Во всех инцидентах, изученных в ходе данного исследования, только 5% были так или иначе вовлечены в криминал до прихода в компанию, что было не замечено или проигнорировано в процессе приема на работу.

Сэм Антар, организатор мошеннической схемы 80-х годов в должности финансового директора сети магазинов Crazy Eddie (осужденный на тюремное заключение и крупный штраф – (подробности по ссылке https://www.nytimes.com/1993/07/21/business/crazy-eddie-founder-guilty-of-fraud.html) писал позднее в одной из своих публикаций по беловоротничковой преступности, что склонный к криминалу человек рассматривает окружающий мир с точки зрения возможностей незаконного обогащения. При этом такие ценности как гуманизм, этика, мораль, доброе расположение интерпретирует исключительно как возможности для эксплуатации (см. данную статью https://whitecollarfraud.com/a-convicted-felons-view-of-white-collar-crime/).

Преступники редко афишируют свои намерения в легкодоступной для понимания окружающими манере. Но, изучая образ мыслей и поведение пойманных за руку мошенников, мы вооружаемся знаниями, которые помогают обнаруживать даже слабые сигналы потенциального преступления. Многие эксперты считают, что нет большой разницы в образе мышления и поведении между теми, кто готовит ограбление банка, и теми, кто способен манипулировать финансовой отчетностью. И те и другие, отмечал Стэнтон Сеймнау в статье журнала Psychology Today, July 7, 2012, «стремятся заполучить контроль и влияние за счет других. Оба способны продолжительное время полностью игнорировать резоны рассудка, не думать о последствиях, уверенно шагая к намеченной цели».

Франк Перри, адвокат из Иллинойса, специалист по беловоротничковой преступности, собрал из разных источников основные проявления преступного образа мыслей и действий, по которым можно выявить потенциального злоумышленника. Для распознавания криминального мышления, пишет он в публикации онлайнового издания Fraud Magazine, «необходимо понимать и отличать мышление антисоциальное». Оба типа мышления можно рассматривать как искаженное восприятие действительности, допускающее и оправдывающее правонарушение. Признаки антисоциального мышления – лживость, третирование, агрессивность.

Другие проявления:

Эксплуатация слабостей. Криминальное мышление расценивает слабость, уязвимость как «правомерный» инструмент достижения цели. В одном из исследований преступности

приводится такой пример: приговоренный к тюремному заключению бухгалтер-мошенник искренне считал и не скрывал своего мнения, «что если клиент не способен самостоятельно заботиться о своих деньгах, то почему бы ни наказать его за это».

Игнорирование правил, законов, кодексов этики. Бернард Эбберс, бывший генеральный директор телефонной связи WorldCom, осужденный в 2005 году за манипуляции бухгалтерского учёта, объяснял отсутствие в компании кодекса корпоративной этики его «абсолютной ненужностью», «колоссальной и пустой тратой времени».

Воспрепятствование (как форма вмешательства) работе законопослушных работников компании. Здесь имеется в виду преследование, несправедливое наказание подчиненных, несогласных следовать незаконным или неэтичным указаниям начальства. Занимавший пост финансового директора HealthSouth Corporation (сеть реабилитационных больниц в США) Уильям Оувенс упорно преследовал своего заместителя Диану Хенз, которая отказалась подписывать подозрительный финансовый отчет, гневно заявив ей: «Вы наглядно продемонстрировали, что не собираетесь выполнять наши указания».

Демонстрация власти методами травли, запугивания, несправедливых наказаний. В компании Livent Corporation (производитель литиевых соединений) топ-менеджеры, позднее осужденные за финансовые преступления, шантажировали работников бухгалтерии, принуждая их игнорировать требования внешних аудиторов. Свое поведение объясняли просто: «никому нет дела до того, как мы управляем компанией».

Претенциозность на особое положение и поведение безотносительно последствий для окружающих. Один из пойманных за руку мошенников объяснял свое поведение «сознанием собственной исключительности, восприятием компании как своей личной, поскольку долго и много на нее работал».

Рационалистическое объяснение мошеннических действий. Звучит следующим образом: «все успешные бизнесмены вынуждены соприкасаться и работать в серой зоне, и даже понимая противозаконность некоторых шагов, бывает трудно отказаться от попытки преступить правила».

Ложное ощущение иммунитета. Возникает под влиянием переоценки собственных способностей и ума. Разоблаченный инсайдер одной брокерской фирмы заявил следователю, что он нисколько не боялся возможных расследований со стороны представителей Комиссии по ценным бумагам и биржам, поскольку считал себя умнее: «Будь они умнее, то не работали бы в казенной конторе за гроши, а ворочали бы миллионами на Уолл-Стрите».

Нарочитая сентиментальность, выражаемая часто в благотворительных акциях с целью формирования образа респектабельного, честного и щедрого бизнесмена.

Чувство удовольствия и восторга преступными деяниями. М. Рапп, отправленный под суд за банковские аферы, признавал, что наслаждался разработкой и осуществлением мошеннических схем, приносивших быстрые и легкие деньги.

Как проводить опрос в ходе расследования финансового мошенничества

Вопросы, адресуемые подозреваемым и свидетелям финансовых преступлений, обычно оттачиваются с годами, по мере накопления практического опыта расследований. У каждого расследователя нарабатывается собственный стиль, но есть и общие исходные принципы,

доступные и полезные всем специалистам. Эксперт по расследованию финансовых преступлений Тим Болл предлагает следующие рекомендации.

Начните с бэкграундных вопросов

Любой опрос надо начинать как простой разговор, цель которого – собрать основную, «фоновую» информацию. Это, к примеру, такие вопросы:

- Как долго работаете в компании?
- Какие должности занимали, какие функции осуществляли, каков сегодняшний должностной статус в компании?
- Как выглядит ваш средний, нормальный рабочий день (неделя, месяц)?

Далее можно перейти к более подробным вопросам:

- Как организуете рабочее время? Какие главные задачи решаете?
- Кто ваш непосредственный начальник? Как контролирует вашу работу?
- Кто вас замещает на время отсутствия?
- С кем чаще всего контактируете в течение рабочего дня?
- Кто помогает с данными, документацией для выполнения заданий?

Важной задачей начального этапа интервью является создание атмосферы доверия и взаимопонимания с опрашиваемым лицом. Основная задача: определить позицию и роль собеседника в компании, его отношение к коллегам и рабочим процессам.

Не стесняйтесь повторять вопросы

Крупным недостатком следует считать нежелание вторично задавать одни и те же вопросы. Может быть, это обусловлено боязнью создать о себе впечатление как о туповатом дознавателе, до которого «не сразу доходит». Между тем, повторные вопросы могут иметь и нередко имеют решающее значение. Обращаясь к одному и тому же предмету, вы не только его лучше проясняете, но и можете уловить несоответствия, противоречия в ответах. Надо вновь и вновь обращаться к деталям тех или иных процедур и процессов с такими, например, вопросами как:

- Я не понимаю до конца, в чем заключается задача главного бухгалтера? Объясните еще раз подробно.
- Мне не понятно, почему чеки выписываются без подтверждающих документов. Давайте еще раз пройдемся по всей цепочке финансовой процедуры.

Внимание на проблемах, беспокоящих опрашиваемых лиц

После того, как прояснилась картина обязанностей опрашиваемого, важно сосредоточить внимание на том, что его беспокоит, выглядит рискованным, угрожающим. Уместно спросить:

- Что вас беспокоит больше всего?
- Бывает ли, что от вас требуют делать то, что не входит в должностные обязанности или к чему вы профессионально не подготовлены?
- Получаете ли адекватную оценку и поддержку со стороны руководителей?
- Расцениваете ли те или иные действия коллег как слишком рискованные для организации?

Большинство людей испытывают тревогу, как минимум, по одной из проблем, связанных с их работой. Очень часто это нормальное волнение по поводу сроков сдачи проекта, риска

увольнения, недовольства карьерой. Углубление в причины нервозности может помочь обнаружить недостаточный контроль за соблюдением финансовой дисциплины, корпоративных политик и инструкций, что открывает путь к злоупотреблениям и мошенничеству.

Спрашивайте напрямую о мошенничестве в компании

Не все любят касаться этой темы по разным причинам. Независимо от того, думали опрашиваемые лица об этом или нет, они, как правило, имеют неплохое представление о слабых сторонах, недостатках своей организации, коллег. Поэтому представляют собой ценный источник информации для расследователя. Вопросы могут формулироваться следующим образом:

- Где и в чем вы видите наибольшие риски мошенничества?
- Какие процедуры контроля нарушаются больше всего?
- Если решиться на кражу, то как лучше ее осуществить?

Такого рода вопросы нередко ведут к обнаружению серьезных рисков мошенничества.

Проявляйте настойчивость в ходе опроса

По мере продвижения интервью расследователь чувствует все большую уверенность в необходимости поднимать и задавать трудные, прямые вопросы о возможной вовлеченности собеседника в преступления:

- Вам приходилось участвовать или быть свидетелем преступных или, по крайней мере, сомнительных действий и поступков в компании?
- Кто-нибудь когда-нибудь привлекал вас к мошенническим операциям или просил закрыть на них глаза?
- Назовите происходящие в компании вещи, которые считаете нечестными/мошенническими/уголовно наказуемыми/аморальными?

В начале разговора опрашиваемое лицо обычно проявляет желание рассказывать то, что от него/нее хотят услышать. По мере углубления в детали выплывают недоговоренности, нестыковки, осознанное или непредумышленное умолчание о нарушениях и злоупотреблениях в компании, прочие вещи, ведущие к раскрытию преступления.

Искусственный интеллект в финансовом секторе: возможности и риски

Рынок технологий искусственного интеллекта в финансовом секторе экономики ежегодно прирастает более чем на 30%. Согласно данным лондонской исследовательской компании Sapio Research, две трети финансовых организаций (западных) активно используют ИИ для широчайшего спектра задач (365finance.co.uk). В том числе, такие задачи как:

Автоматическая обработка кредитных заявок и финансовая отчетность. Обрабатывая огромные массивы данных, алгоритмы ИИ существенно экономят время и ресурсы организаций.

Минимизация рисков путем обнаружения аномалий в потоках финансовых данных, в частности, в процессах оценки кредитоспособности потенциальных заемщиков. В Великобритании более 90% финансовых институтов используют предиктивную аналитику для борьбы с мошенничеством и иных операций (ukfinance.org.uk).

Рыночные исследования, опирающиеся на обработку и анализ данных из открытых источников, включая СМИ и социальные сети.

Обслуживание клиентов. Например, в форме роботов-ответчиков, способных не только реагировать на обычные вопросы, но и обеспечивать индивидуальный образовательный контент, включая рекомендации для эффективных инвестиций.

Как известно, идеальных, безупречных технологических инструментов в реальности не существует. То же самое можно сказать и об искусственном интеллекте в банковской сфере. Эксперты выделяют как преимущества, так и уязвимые аспекты применения ИИ финансовыми организациями.

Преимущества

- Демократизация финансовых данных. Генеративный потенциал ИИ можно эффективно использовать для трансформации данных (например, сложных финансовых документов, протоколов совещаний и презентаций) в действенные инсайты, на основе которых принимаются решения.
- Рост эффективности, экономия ресурсов. Автоматизация и роботизация благодаря ИИ технологиям повышают продуктивность финансовых организаций в среднем на 14% (данные исследования Массачусетского технологического института, подробнее см. на сайте nber.org/papers/w31161).
- Контроль за соответствием требованиям регуляторов. Речь идет об автоматической проверке банковских процессов и операций на предмет их соответствия постоянно меняющимся законам, нормам и правилам, что избавляет от необходимости нанимать комплаенс-специалистов, снижает риски возможных нарушений.
- Повышение инновационных компетенций. Оптимизация финансовых процессов позволяет сосредоточить основное внимание на развитии инновационных банковских решений. К примеру, многие ИИ платформы предлагают низкокодовые и даже безкодовые инструменты (No-code и Low-code — технологии разработки сайтов, мобильных приложений, блогов, баз данных и других продуктов без погружения в код. Работа с этими инструментами не требует знания языков программирования и навыков в разработке ПО).
- Аналитические решения на основе ИИ могут также прогнозировать рыночные тенденции, потенциальные риски и угрозы.

Риски и уязвимости:

- Проблемы сохранения и защиты персональных данных. Технологиями ИИ обрабатываются, анализируются мощные массивы финансовых и персональных данных. И это вызывает обеспокоенность многих банкиров и бизнесменов (43% опрошенных Sapio Research), вынуждая их обращаться к дорогостоящим решениям с усиленной защитой от краж и злоупотреблений данными.
- Результативные неточности, ошибки. При определенных обстоятельствах, считают некоторые эксперты, генеративный искусственный интеллект может предпочитать новизну, уникальность, своеобразие фактическому положению вещей. Поскольку финансовая индустрия как, может быть, ни одна другая нуждается в точной и объективной информации для принятия решения, без дополнительного контроля и проверки специалистами пока еще трудно обойтись.
- Отсутствие осмысленной объяснимости. Сложная структура Большой Языковой Модели затрудняет понимание пользователями, как эта технология достигает предлагаемое ею то или иное финансовое решение. Еще труднее объяснить данное решение клиентам и инвесторам финансовой организации. Впрочем, сегодня уже можно найти на рынке модели «объяснимого искусственного интеллекта» (Explainable AI, XAI),

запрограммированного на описание цели, обоснование и процесс принятия решений таким образом, чтобы его мог понять обычный человек (подробнее см. веб-сайт websoftshop.ru).

- Этический аспект. Искусственный интеллект надежен настолько, насколько надежны обрабатываемые и анализируемые им данные. Пользователи должны помнить об этом и не допускать предвзятость, ангажированность, необъективность в выборе источников информации, чреватые искажением конечных результатов.
- Сокращение рабочих мест. Недавнее исследование компании CFOtech (cfotech.co.uk) обнаружило, что сегодня внедренная в финансовый сектор автоматизация с помощью ИИ освобождает от человеческого труда 38 рабочих дней в году. Но бить тревогу относительно безработицы пока рано. При современном технологическом уровне применения ИИ человеческая профессиональная экспертиза будет востребована еще очень и очень долго.

SWOT анализ для финансовых организаций

SWOT анализ не является экзотикой для компаний в финансовой сфере. Он применяется в конкурентной разведке для измерения и сравнения рыночных позиций своей компании с другими по каждому из четырех компонентов: сильные и слабые стороны (strengths, weaknesses), возможности и угрозы (opportunities and threats). SWOT анализ помогает с большой точностью определить реальное место, занимаемое вашей организацией (и конкурентов) на финансовом рынке, возможности роста и потенциальные риски.

Если «сильные и слабые стороны» следует рассматривать как внутренние, свойственные каждой организации факторы развития, то «возможности и угрозы» требуют тщательного изучения позитивного и негативного воздействия на бизнес конкурентной среды.

Рассмотрим каждый из четырех факторов отдельно.

Сильные стороны

Собственно речь о конкурентных преимуществах. Применительно к финансовым организациям они представляют собой:

- Уникальность продуктов/услуг (например, оптимизация налогообложения, льготное кредитование, большой кэшбэк).

- Прочная репутация бренда и высокий уровень лояльности клиентов.

- Устойчивая траектория роста.

- Стратегия или модель инвестирования из собственных средств.

Анализ сильных сторон позволяет понять, где вы опережаете своих конкурентов.

Слабые стороны

Для финансовых организаций ими могут быть:

- Отставание с выходом инновационных продуктов/услуг.

- Слабый географический охват.

- Недостаточно активное привлечение новых клиентов и удержание имеющихся.

- Проблемы с выполнением требований регуляторов.

- Высокая текучка кадров.

- Недостаточный собственный капитал.

- Слабая операционная эффективность.

Определив свои уязвимости, слабые стороны, необходимо составить план и не мешкая приступить к их устранению.

Возможности

Это в первую очередь внешние обстоятельства, позитивные тенденции рынка, требующие учета и использования:

- Перспективы расширения клиентской базы, в частности, за счет новой волны переступивших порог совершеннолетия клиентов.

- Инновационные финтехнические продукты (в том числе, на основе искусственного интеллекта).

- Изменения в законодательстве и предписаниях регуляторов, открывающие новые возможности роста.

- Экономические тенденции, требующие инновационных финансовых продуктов/услуг.

Интенсивный, постоянный мониторинг изменений в экономической среде – необходимое условие для опережающего реагирования, получения т.н. «преимущества первопроходца».

Угрозы

Среди негативно влияющих факторов на бизнес в финансовой сфере можно выделить:

- Появление новых сильных конкурентов, особенно отличающихся нестандартными действиями.

- Экономическая рецессия.

- Ужесточение законодательных или регуляторных требований, ведущих к росту расходов.

- Риски утечек персональных данных, конфиденциальной финансовой информации.

- Дефицит талантливых профессионалов (к примеру, в сфере банковской кибербезопасности).

Постоянный глубокий анализ потенциальных рисков и угроз позволит вам своевременно принимать действенные меры по минимизации последствий и их предупреждению.

(по материалам веб-сайта lexisnexis.com)

10 шагов успешного конкурентного анализа

Президент лондонской компании Studio Noel (https://studionoel.co.uk), автор ряда публикаций по бизнес стратегии Мишель Ноель формулирует и комментирует последовательность действий, необходимых, по ее мнению, для успешного осуществления конкурентной разведки:

1. Определение целевого рынка

Важно понять, что собой представляет клиентская база конкурентов (равно как и своя). В этом смысле интерес представляют веб-сайты конкурентов, социальные медиа, маркетинговые кампании и любые иные источники информации об изучаемой аудитории. Особое внимание следует уделять высказываниям пользователей соцсетей на темы качества продуктов/услуг, которые помогают понять, в чем конкуренты преуспевают, а в чем терпят неудачу. Такое исследование способно обозначить «идеальный профиль» целевой аудитории, под которую оттачивается рыночная стратегия.

2. Идентификация прямых конкурентов

Завершив составление списка конкурентов, разделите его на две группы (прямые и не прямые конкуренты). Обе группы важны и требуют постоянного изучения, вне зависимости от того, давно они присутствуют на рынке или только готовятся на него выйти. Разница между прямыми и непрямыми конкурентами заключается в том, что первые предлагают *аналогичные* вашему бизнесу продукты и/или услуги, а вторые – *отличные*, но ориентируются на общую с вами клиентскую базу. Основной фокус внимания – на первой группе конкурентов, но важно не забывать и о второй.

3. Идентификация потенциальных конкурентов

Это практически третья группа конкурентов, которые, по мысли Ноель, работают в том сегменте рынка, в который вы еще только планируете войти. Здесь уместен сравнительный анализ (benchmarking), помогающий выявить лучшие практики, которые можно использовать для завоевания новых позиций.

4. Изучение вербальных и визуальных характеристик идентичности конкурентных брендов

Детальной оценке подлежат:

- Лого и имиджевый слоган. Демонстрируются по всем платформам и каналам?
- Цветовая палитра. Везде одинаковая?
- Оформление. Как оно отражает персональные особенности конкурента?
- Имиджевый стиль. Используют ли профессионального фотографа? Рисунки, иконки, иллюстрации?
- Стиль изложения. Каков тон – доверительный, шутливый, заигрывающий или другой?

5. Необходим SWOT анализ

Подробно об этом инструменте конкурентной разведки смотри материал в этом же выпуске журнала «Бизнес-разведка» («SWOT анализ для финансовых организаций»).

6. Весьма полезен и PEST анализ

Он охватывает политические, экономические, социальные и технологический сферы, то есть внешние объективные факторы, воздействующие на бизнес. Можно осуществлять в тандеме с SWOT анализом.

7. Исследование маркетинговой и ценовой стратегии конкурентов

Такое исследование многое расскажет о конкурентах, главное, что у них работает, а что нет. Особого внимания требует мониторинг социальных сетей: как они используются конкурентами для рекламных, маркетинговых и прочих мероприятий по продвижению продуктов/услуг. Поставьте и постарайтесь ответить на такие вопросы:

- Насколько активны конкуренты в социальных сетях, какие именно используются?
- Как часто публикуют свой контент?
- Что чаще используют - видео или фото/картинки?
- Выпускают ли пресс-релизы?
- Имеются ли в арсенале средств подкасты, вебинары, кейсы?
- На чем концентрируют внимание в рекламных кампаниях?
- Занимаются ли рассылкой реклам по электронной почте?
- Акцент – на цифровом маркетинге или оффлайновом?
- Какими приемами привлекают внимание аудитории, повышают уровень узнаваемости бренда?

8. Изучение ценовой политики

Ценовая политика дает довольно точное представление о привлекательности продукта или услуги для пользователей. В сфере услуг может оказаться, что конкурент делает упор не на привлекательную цену как таковую, но на важность, значение услуги для клиента в смысле наилучшей опции удовлетворения его/ее потребности.

9. Активное использование онлайновых аналитических инструментов

Сегодня на рынке имеется множество интернет технологий, предназначенных, в том числе, и для проведения конкурентного анализа. Автор предлагает два: BuzzSumo и SEMRush.

10. Поддерживать конкурентную разведку в актуальном состоянии

Регулярно заниматься конкурентным анализом. Удерживая в фокусе внимания прямых и непрямых конкурентов, вносить необходимые коррективы в стратегическое планирование, практические действия на рынке, направленные на получение и усиление своих преимуществ.

Метрики эффективности бизнес-разведки

В современной бизнес среде деловая разведка уже давно не роскошь, а необходимость. Организации опираются на нее как на важный инструмент изучения конкурентных рынков, своевременного реагирования на зарождающиеся тенденции, как на основу принятия стратегических решений.

Построить и запустить бизнес-разведку полдела. Не менее важно научиться измерять ее эффективность. Для этого необходимо понимать, что может служить метриками.

Эксперты, регулярно выступающие на сайте сообщества профессионалов конкурентной разведки (skip.org), предлагают такие рекомендации:

Влияние на принятие стратегических решений

Изначально центральная роль деловой разведки – обеспечивать наилучшие бизнес решения. Именно в этом и проявляется ее главная эффективность. Организации могут измерять влияние, отслеживая, как часто отчеты, рекомендации, инсайты профессионалов бизнес-разведки инкорпорируются в принимаемые первыми лицами решения. Об этом нелишне регулярно интересоваться у акционеров и топ-менеджеров.

Проактивная идентификация возможностей и угроз

Успешная разведка это в первую очередь своевременный прогноз. Число ранних предупреждений о близкой дестабилизации рынка, зарождающихся тенденциях, вероятных действиях конкурентов позволяет оценивать и измерять проактивность разведки.

Своевременность отчетов

В условиях быстро меняющегося бизнес ландшафта время стоит как никогда ранее дорого. Способность бизнес-разведки заблаговременно предупреждать о новых тенденциях является ключевым индикатором ее эффективности. Конкретными метриками могут служить как время, затрачиваемое на подготовку и выпуск отчета, так и скорость обнаружения и информирования о новых рисках и угрозах. Специальная панель с доступом к отчетам, к внутреннему бюллетеню и другим документам службы бизнес-разведки ускорит процесс ознакомления с результатами работы, если автоматизировать процессы поиска, обработки и анализа данных в режиме реального времени.

Охват и полнота обрабатываемых данных

Сильная сторона бизнес-разведки заключается в ее способности синтезировать исчерпывающую информацию. Измерение ширины и глубины обрабатываемых данных осуществляется путем оценки разнообразия, географического охвата, полноты источников информации относительно рыночных тенденций, покупательских предпочтений, конкурентного анализа. Недостаточное внимание к этим параметрам чревато упущенными преимуществами и провороненными рисками.

Сотрудничество по обмену информацией

Здесь метрикой может служить число кросс-функциональных совещаний и совместных проектов между разными подразделениями организации. Также показательно количество посещений раздела внутрикорпоративной платформы, касающегося бизнес-разведки.

Реальная отдача от инвестиций (ROI) в бизнес-разведку

Одно из важнейших, ключевых измерений эффективности. На эту тему немало публикаций в отраслевой прессе. Показателями служат снижение затрат, рост доходов, минимизация рисков. Все это – как результат эффективной деловой разведки. В числе конкретных метрик – подсчет финансовой выгоды от своевременного и правильного реагирования на появление нового сильного конкурента, о чем заранее предупредила бизнес-разведка.

Высокий рейтинг использования развединформации

Отслеживание откликов на отчеты бизнес-разведки со стороны менеджмента и акционеров – надежный индикатор оценки работы.

Итак, измерение эффективности бизнес-разведки подразумевает использование определенного набора количественных и качественных метрик – от реального влияния на принятие важных решений до подсчета практической (финансовой) отдачи. Умелое оперирование метриками внушает доверие к бизнес-разведке как к одной из краеугольных основ бизнес стратегии.

Как собирать конкурентную информацию внутри своей организации

Профессионалы конкурентной разведки тратят много времени и сил на прочесывание интернета, социальных сетей, веб-сайтов конкурентов и так далее, часто недооценивая информацию, которой обладают коллеги по работе, прежде всего менеджеры по продажам товаров/услуг, занимающие первую линию борьбы за клиентов. А эта информация порой бывает более полезной с практической точки зрения, чем разрозненные данные, добываемые на бескрайних просторах интернета.

Адам МакКуин, блогер на сайте klue.com, рекомендует начать с определения группы менеджеров для подробного интервью по темам конкурентной разведки. Собеседники подбираются с учетом опыта работы, выполняемой функции, близости к источникам информации в лице клиентов, партнеров, поставщиков. Нелишне проверить, не работали ли у конкурентов ваши потенциальные собеседники в прошлом.

Прежде чем приступить к интервью, следует хорошенько подготовиться. Собрать солидную первичную информацию о компаниях, которых планируете изучать (продукты, целевой рынок, ключевые сферы конкуренции). Еще раз просмотреть имеющиеся в компании отчеты по работе, связанной с управлением рисками, чтобы уяснить, какие темы, вопросы конкурентной борьбы отразились в них недостаточно. А то и вообще не нашли своего места.

Чтобы «разговорить» коллег, раскройте цель интервью, подчеркнув, что конечные результаты помогут им лучше ориентироваться в своей работе, добиваться большей эффективности. Объясните, что вы рассматриваете их как ценных экспертов, обладающих знаниями и опытом, весьма востребованными для конкурентного анализа. Избегайте формальных, письменных форм общения. Доверительный разговор – наилучший путь получить требуемую информацию. По завершении интервью обязательно доведите до сведения их начальства благодарность за участие в сборе и анализе информации.

Рекомендуемые экспертами общие вопросы для интервью:

- Как часто вам приходится сталкиваться с проявлениями конкуренции?
- Каких новых конкурентов вы заметили в последние месяцы?
- С кем состязаться всего сложнее? И почему?
- В чем заключаются отличительные особенности поведения конкурентов на рынке?
- Характерные для них приемы продвижения продуктов/услуг?
- Как они себя позиционируют?
- Что слышали о стратегии конкурента?
- Что говорят конкуренты о нашей компании с целью дискредитации? Что легче опровергнуть, а что труднее?
- Что известно о ценовой стратегии конкурентов?

- Как конкуренты структурируют ценовую политику (ценовые сегменты, разные упаковки)?
- Как часто и охотно используют скидки?

Список таких вопросов неисчерпаем. Но особенно важно в ходе интервью провести сравнительный анализ конкурентных преимуществ и слабостей.

О своих преимуществах:

- В чем мы опережаем их? Причины?
- Как конкретно используем свои преимущества?

О преимуществах конкурентов:

- В чем сила конкурентов?
- В чем конкретно мы уступаем? И почему?
- С какими внешними вызовами сталкиваетесь, продвигая продукцию? И как преодолеваете эти вызовы?
- Что больше всего беспокоит, когда сталкиваетесь с конкурентами?
- Самый болезненный провал в борьбе с конкурентами?
- Что известно о ключевых клиентах конкурентов?

В процессе ряда интервью вы отмечаете общие оценочные моменты, которые лягут в основу аналитического отчета.

Как нотариусы могут противодействовать отмыванию доходов

С первого декабря 2024 года в работе российских нотариусов произошли изменения, знаменующие повышение их роли в борьбе с отмыванием доходов и другими финансовыми преступлениями.

Так, нотариусы обязаны теперь досконально проверять достоверность представленных для совершения сделки документов и реальность принимаемых сторонами или стороной обязательств. Например, запросить банк подтвердить подлинность документа о передаче денежных средств заемщику, что исключит использование нотариальных услуг для легализации незаконных доходов.

Нотариусы также получили право отказать в совершении нотариальных действий, если у них возникнут обоснованные подозрения, что сделка направлена на отмывание денег. "Таким образом, нотариусы становятся частью системы раннего предупреждения и выявления подозрительных операций", отмечал председатель Комитета Госдумы по вопросам собственности, земельным и имущественным отношениям Сергей Гаврилов в интервью «Российской газете» (30 ноября 2024). В сделках с крупными денежными суммами нотариусы обязаны идентифицировать клиентов, собирая подробную информацию о физических и юридических лицах (паспортные данные, налоговые номеров и других сведения). Другая прямая их обязанность - замораживание денежных средств или ценных бумаг клиента, если есть основания полагать, что они связаны с подозрительными действиями.

О потенциальном вкладе института нотариата в борьбу с мошенниками рассуждает Аманда Фарелл, обладатель диплома по психологии криминальных расследований Ливерпульского

университета. Анализируя разнообразный инструментарий мошенничества, в первую очередь подделку документов и приемы социальной инженерии, она советует нотариусам следовать следующим мерам выявления криминала:

1. Скрупулезно изучать идентифицирующий личность документ, обращая особое внимание на дату рождения, подпись владельца, гладкость краев, ровность ламинации там, где помещено фото (или дата рождения), ясность и четкость текста, отсутствие частичного наложения и других признаков подделки.

2. Овладеть методикой анализа поведенческих характеристик. Повышенное внимание должны вызвать такие сигналы в поведении клиента как:

- Попытка навязать разговор на отвлеченные темы
- Нервозность, неуверенность
- Поторапливание
- Заигрывание
- Давление (должностным авторитетом, социальным положением)

Фарелл приводит пример из реальной жизни, когда женщина, обратившаяся к помощнику нотариуса за доверенностью от мужа, предъявила подписанный мужем документ. Сославшись на болезнь супруга, который, по ее словам, лежит в постели, она протянула его водительское удостоверение. Хотя закон США требует, чтобы заявитель присутствовал лично, либо с использованием видео и аудио технологии, помощник удовлетворился тем, что женщина позвонила «мужу для подтверждения его согласия». Как потом выяснилось, звонила она своему любовнику, выдавая его за супруга, который, естественно, ни о чем не подозревал. Когда афера вскрылась, то помощник нотариуса понес справедливое наказание, потеряв патент на юридические услуги и полностью возместив жертве обмана материальный ущерб (подробнее см. prologix.com/blog).

Сегодня на помощь нотариусам пришли нейросетевые технологии. Ведущий российский разработчик в области систем распознавания документов на основе искусственного интеллекта компания Smart Engines разработала технологию небиометрической сверки лица. Алгоритмы ИИ не выделяют биометрические признаки, но обучены сравнивать лица и давать оценку, насколько изображения лиц совпадают друг с другом. Этот процесс сильно напоминает «традиционную» сверку лиц «на глаз» с той лишь разницей, что это делает не человек, а машина.

Нотариусу для использования новой опции достаточно обычного ПК и веб-камеры: посетителя фотографируют, после чего программа сравнивает два изображения и выдает оценку их совпадения, выраженную в процентах менее чем за секунду. Результаты: программа показывает совпадение в 90–95% случаев, даже если с момента выдачи паспорта прошло 10–20 лет *(по материалам газеты «Известия» и других российских СМИ)*.

Рецензия
Business Intelligence *(Reprint Edition 2025)* by Stacia Misner, S.Vitt

Это ориентированное на профессионалов издание позволяет понять, что такое бизнес-разведка, как она работает, где и почему используется. Все освещаемые темы и проблемы иллюстрированы реальными фактами и историями. Авторы показывают, как с помощью инструментария бизнес-разведки, превращая горы данных в полезную информацию, организации способны быстро принимать адекватные бизнес решения.

Основные тематические разделы включают:

- Парадигмы бизнес-разведки. Фундаментальные основы, характеристики, компоненты, общая архитектура бизнес-разведки.
- Аргументы в пользу бизнес-разведки. Как лидеры бизнеса в сфере финансов, промышленности и торговли успешно применяют бизнес-разведку и каких позитивных результатов добиваются с ее помощью.
- Практика бизнес-разведки. Как определить возможности и перспективы бизнес-разведки для вашей организации, какие решения требуются для ее запуска в действие, как сохранить динамику процессов обработки и анализа всех собираемых данных.