БИЗНЕС-РАЗВЕДКА

№62, 2024

Оглавление

Главная тема

Бизнес-разведка в 2025 году

Бизнес-разведка являет собой краеугольный камень корпоративной стратегии. Выявляя новые тенденции, возможности, угрозы и риски через анализ массивов данных, она обеспечивает конкурентные преимущества, а, следовательно, эффективность, прибыльность бизнеса.

Перспективы развития бизнес-разведки в 2025 году и последующие несколько лет будут определяться в первую очередь революционными технологическими инновациями в работе с Большим Данными. Не случайно издание Analytics Insight, специализирующееся на исследованиях и публикациях в области аналитики Больших Данных, искусственного интеллекта, блокчейна и криптовалюты, в статье о главных тенденциях эволюции бизнес-разведки на первое место ставит интеграцию искусственного интеллекта и машинного обучения как непременное условие совершенствования прогностической аналитики. Автоматизация и роботизация будут освобождать специалистов от рутинной работы по сбору и обработке данных в пользу концентрации человеческого внимания на принятии решений.

Дополненная технологиями ИИ, машинного обучения, обработки естественного языка так называемая «расширенная аналитика» (Augmented Analytics) не только ускорит и сделает более точным принятие бизнес решений, но и расширит круг людей, не обладающих опытом и специальными техническими знаниями, но способными управлять сложными аналитическими системами и получать результаты.

Эксперты прогнозируют рост бизнес-аналитики с самообслуживанием (Self-Service BI), что означает возможность сосредоточиться на аналитике, не возлагая большой нагрузки на ИТ-отдел и профессиональных информационных работников. Сотрудники компании получают в свои руки инструменты аналитики, могут самостоятельно принимать обоснованные решения, причем, намного быстрее, чем при использовании традиционных моделей BI. Снижение нагрузки на ИТ-отдел повышает их производительность, а, в конечном счете, эффективность бизнеса.

Управление данными при соблюдении требований прайвиси станет важным приоритетом и фундаментальным элементом стратегии бизнес-разведки в 2025 году. Следование жестким правилам регуляторов в этой сфере укрепит доверие потребителей продуктов и услуг к бизнесу, особенно к финансовым организациям.

Стремление к быстрым и точным решениям требует усиления внимания к аналитике в режиме реального времени. Способность компаний к быстрому анализу данных по мере их появления и немедленным решениям – непременное условие успешной конкуренции.

Критически важным компонентом бизнес-разведки в ближайшие годы будет визуализация данных, делающая их более понятными и действенными. Наглядное представление результатов обработки данных с помощью графиков, диаграмм, сводных таблиц, блок-схем, инфографики и так далее упрощает восприятие больших массивов данных со сложной структурой, иллюстрирует корреляции и связи, помогает сравнивать и находить различия, выявлять тренды и аномалии, акцентирует внимание на приоритетных аспектах.

Эксперты прогнозируют дальнейший рост популярности облачных решений бизнес-разведки, помогающих справиться с обработкой и анализом с каждым годом возрастающей массы данных, работать дистанционно, экономить средства. Правда, многие специалисты предупреждают и о рисках передачи функций бизнес-разведки в облака, имея в виду утечки информации. Об этом нельзя забывать.

В 2025 году значительная часть программных бизнес-решений, предлагаемых рынком, будет иметь встроенную аналитику. Интегрированные в корпоративное программное обеспечение и веб-приложения аналитические возможности позволяют автоматизировать мониторинг, управление и развертывание аналитики.

Быстрые темпы цифровизации бизнеса требуют от неспециалистов повышения уровня грамотности в работе с данными. Речь идет о способности понимать и использовать данные с максимальной пользой для дела. Организации неизбежно будут более заинтересованными в инвестициях в «дата-грамотность», в развитие у работников аналитического потенциала.

Наряду с прогрессом аналитики и искусственного интеллекта растет значение этических аспектов, требований ответственного подхода к работе с данными, что

предполагает прозрачность и в то же время надежную защиту данных от утечек. Этому направлению в развитии бизнес-разведки будет уделяться первостепенное внимание со стороны регуляторов и руководителей бизнеса.

Банковская безопасность и финансовая разведка

Расследование внутрикорпоративного мошенничества: основные этапы

В последние годы российские организации стали чаще сталкиваться с инцидентами внутрикорпоративного мошенничества, показало проведенное в 2024 году исследование компании «Технологии доверия». О преступлениях внутри компании сообщили 70% опрошенных представителей бизнеса. В 2018 году по итогам аналогичного опроса этот показатель оценивается в 46%.

Финансовый ущерб от мошенничеств растет. Треть опрошенных оценили его в более чем 100 млн руб., 10% — в 25–100 млн руб., 54% — в 1–25 млн руб. Помимо непосредственного ущерба компании несут определенные затраты в ходе расследования, в частности, на привлечение юристов и консультантов (в 13% случаев превысили 100 млн руб.). Косвенные потери — ухудшение морального климата в коллективе, потеря сотрудников и рост недоверия к руководству.

Финансовое расследование является одним из действенных инструментов минимизации рисков мошенничества. Оно проводится, когда у руководителей организации возникают подозрения о манипуляции бухгалтерской отчетностью, нарушаются правила внутреннего контроля или появляются иные предположения о финансовых махинациях со стороны сотрудников организации. Финансовым расследованием могут заниматься не только правоохранительные органы, но собственные службы безопасности, либо приглашенные частные расследователи.

Аналитики Hudson Intelligence, частного агентства, специализирующегося на расследовании финансовых преступлений, представили план действий, который может служить базовой моделью для профессионалов в этой сфере.

1. Консультации

Прежде чем приступить к работе, расследователь проводит консультации с руководством организации для уточнения сложившейся ситуации, согласования вопросов оказания расследованию поддержки и помощи. С приглашенным экспертом подписывается договор, отражающий объем, график и стоимость предстоящей работы.

2. Сбор материалов (улик)

Сначала проверяется наличие документальных свидетельств, подтверждающих факт финансового мошенничества. В отдельных случаях возникает необходимость в привлечении узкого специалиста, к примеру, эксперта по отслеживанию

криптовалютных трансакций. Уточняются и документируются детали мошеннической схемы, размер нанесенного урона. Если преступная схема продолжает действовать, отрабатываются и реализуются соответствующие контрмеры.

3. Идентификация мошенников

Когда основные фрагменты информационной мозаики собраны в более-менее понятную картину, основные усилия направляются на установление ее организаторов. Допрашиваются свидетели и подозреваемые. Их показания перепроверяются, если они противоречат собранной доказательной базе и между собой. Сложные расследования, такие как взяточничество и коррупция, могут потребовать серии повторных допросов. Допрос главного подозреваемого целесообразно отложить на финальную стадию расследования.

4. Бэкграундная проверка

Речь идет о серьезной персональной, профессиональной и финансовой проверке всех охваченных расследованием людей, в первую очередь, тех, на кого пало подозрение. Особое внимание - к поиску документальных подтверждений о причастности в прошлом к мошенническим схемам. Используются доступные источники информации об уголовных и гражданских делах в судах, архивы полиции. Выявить мотивы преступления поможет поиск данных о банкротстве, кредитной задолженности, залоговом имуществе и его изъятии с потерей права выкупа, налоговой задолженности. Также изучаются личные расходы подозреваемых сравнительно с их легальными доходами.

5. Определение источников возврата материальных и денежных средств

Находятся и документируются банковские счета, инвестиции, движимое и недвижимое имущество подозреваемых и их ближайших родственников.

6. Юридические действия

Если установленные в ходе расследования лица, ответственные за мошенничество, отказываются возместить нанесенный ими ущерб, может понадобиться обращение в органы правопорядка. Собранные в процессе расследования материалы, экспертные заключения пригодятся для последующего использования в суде.

Почему многие компании бессильны в отношении платежного мошенничества

Платежное мошенничество представляет собой разновидность финансовых преступлений, когда злоумышленники подделывают или крадут платежную информацию для совершения нелегальных трансакций. Для достижения преступных целей применяются разные способы:

Социальная инженерия, в частности, фишинг и дипфейки, играющие на доверчивости людей.

Скимминг – установка на терминалы оплаты сканирующих устройств, которые считывают данные банковских карт.

Мошенничество с поддельными доказательствами оплаты, к примеру, фальсифицированными скриншотами банковских переводов.

Мошенничество с возвратом платежей. Чтобы инициировать отмену платежа, мошенники заявляют, что транзакция была «мошеннической» или «ошибочной».

Мошенничество с Card Not Present (CNP) транзакциями - когда данными кредитной карты пользуются без физического присутствия карты (по телефону или в интернете).

Мошенничество с помощью SMS. Преступники используют SMS сообщения, выдавая себя за банки или приложения, имитируя реальные уведомления.

И это еще не полный список мошенничества, который охватывает также аферы с криптовалютой.

Страдают люди. Несут ощутимые потери банки и компании. При этом бизнес не демонстрирует способность эффективно противостоять платежному мошенничеству. Об этом, в частности, свидетельствует опрос, проведенный летом 2024 года в США компанией Trustmi (решения для безопасных платежей), в котором участвовали 516 специалистов финансовой сферы.

48% респондентов, в том числе финансовых директоров, бухгалтеров, кассиров, признались, что понятия не имеют о том, сколько раз они становились жертвами платежного мошенничества за последние 12 месяцев.

51% заявили, что не знают, какое количество денег потеряли банки и компании в результате платежного мошенничества.

При этом каждый пятый опрошенный подтвердил, что как минимум один раз в год компания или ее руководитель подвергался атаке с применением искусственного интеллекта (дипфейк).

Комментируя полученные в ходе опроса результаты, аналитики Trustmi объясняют их двумя основными причинами. Первая – разрозненная инфраструктура (siloed operations). Вторая – устаревшие системы безопасности.

Особую озабоченность экспертов вызывает тот факт, что респонденты не смогли количественно оценить убытки от платежного мошенничества.

И это не удивительно, если учесть, что каждый четвертый из опрошенных специалистов не смог даже сказать, сколько и какие технологические решения для выявления и предотвращения финансового мошенничества имеются в наличии в их организациях. Более того, 14% признались, что вообще не имеют таких технологий. И только треть респондентов заявили, что пользуются 3 – 5 решениями.

Опрос показал, что платежные операции автоматизированы в 70% организаций. Всего 5% компаний пользуются полностью автоматизированными платежными процессами. А 26% осуществляют их вручную или почти вручную.

Лучшие практики по безопасности платежей предусматривают надежное хранение данных, их шифрование, строгую аутентификацию и контроль доступа, разработку безопасного кода, мониторинг сетевой и системной активности, регулярные проверки, аудит и тестирование систем безопасности.

Компании смогут эффективно защитить свои платежные процессы, восприняв передовые методы, взяв на вооружение современные инструменты и технологии, в том числе:

- безопасные платежные шлюзы и хостинг;

- токенизацию данных (процесс замены данных, к примеру, банковских карт, на уникальный цифровой индентификатор);

- системы обнаружения мошенничества;

- уровни защиты данных - сертификаты SSL/TLS).

Подробнее об этом см. appmaster.io/ru/blog/bezopasnost-platezhei-v-elektronnoi-kommertsii.

По каким «красным флажкам» и признакам можно обнаружить внутрикорпоративное мошенничество

Financial Crime Academy – организация, осуществляющая образовательные программы в онлайне по противодействию финансовым преступлениям и управлению корпоративными рисками – опубликовала в октябре 2024 года на своем сайте financialcrimeacademy.org перечень «красных флажков» и признаков, позволяющих подозревать внутрикорпоративное мошенничество.

«Красные флажки» в контексте финансового мошенничества

- Преступление «по возможности» (opportunistic crime), то есть деяние, совершаемое без преднамеренности, когда злоумышленник действует экспромтом, пользуясь подвернувшимся случаем совершить кражу или другое правонарушение. Специалисты по безопасности должны находить и изучать условия, возможности, при которых может быть совершено преступление.
- Прием на работу заведомых мошенников. Криминальные элементы нередко преднамеренно пытаются устроиться на работу в конкретную организацию с целью воровства. Если им это удается, то возникают вопросы к кадровикам, чья работа должна быть подвергнута серьезному расследованию.
- Подкуп и шантаж персонала. Известный способ организованной преступности вовлечь работников организации в финансовые махинации в обмен на хороший «приработок». Угрозы и шантаж в случае отказа.
- Слишком высокая текучесть кадров.

Работники своим поведением вызывают подозрения о возможных финансовых преступлениях, когда они:

- Постоянно задерживаются на работе без видимых на то оснований
- Отказываются от отпусков и выходных
- Демонстрируют необоснованную скрытность, секретность в своих служебных делах
- Находятся в стрессе из-за семейных проблем
- Неожиданно и радикально меняют стиль жизни, социальное поведение
- Проявляют беспокойство и тревогу без видимых причин
- Ведут себя агрессивно в контактах с некоторыми коллегами
- Регулярно нарушают установленные в организации правила работы и поведения
- Вызывают рост жалоб на свое поведение
- Задерживают предоставление информации о результатах своей работы
- Тянут или отказываются предоставлять данные, требуемые внутренними аудиторами. Либо предоставляют искаженные, поддельные данные
- Резко меняют отношение к коллегам и руководителям в негативную сторону
- Чрезмерно любопытствуют о деталях предстоящего аудита

К этому следует добавить рекомендации ряда российских экспертов, выступающих по данной проблеме в разных онлайн изданиях:

- персонал нарушает правила заполнения документов: просит поставить подпись на пустом бланке, не указывает дату на документах или заверяет их задним числом
- у работника нет доверия к другим сотрудникам: он не желает передавать коллегам дела при уходе в отпуск и неохотно занимается совместным проектами
- отчётность часто корректируется
- тесные контакты с работниками иных отделов без служебной необходимости
- регулярное появление недостачи
- рост числа претензий к качеству товара, услуг, работ
- конфликт внутри компании, в том числе между её владельцем и топ-менеджером.
  (kontur-.ru)

  А также:

- Закупка все большего количества товара при неизменных объемах производства
- Обнаружение на складах при случайных проверках контрафактной или некачественной продукции
- Снижение объемов продаж
- Систематические жалобы клиентов на качество продукции/услуг
- Резкое увеличение продаж при снижении стоимости товара
- Несоответствие расходов сотрудника его доходам. Например, если менеджер среднего звена приезжает на работу на Ferrari
- Резкое увеличение представительских расходов у персонала и т.п.
  (advgazeta.ru)

Конкурентная разведка в финансовых организациях

Банки и другие финансовые компании, по образному выражению Мэдисона Бласка (crayon.co/blog), «мгновенно взлетели на поезд цифровой информации». В результате сегодня каждые несколько минут на рынке появляется новое приложение финансовых услуг.

Сталкиваясь с растущей конкуренцией, многие банки проявляют интерес к инструментарию конкурентной разведки, рассчитывая сохранить и приумножить свои преимущества. Конечная цель КР – помочь сформировать верные стратегические решения, которые учитывают преимущества и недостатки конкурентов, делают акцент на том, что отличает вашу компанию от других, действующих в том же рыночном сегменте.

Мэдисон Бласк перечисляет и кратко характеризует главные сферы применения КР в финансовой сфере:

Выявление ключевых отличий от конкурентов

Финансовым организациям свойственно стремление к расширению. В условиях жесткого соперничества даже небольшое на первый взгляд отличие, своего рода «изюминка», может при правильном ее использовании дать ощутимое преимущество. Это может быть предложение льготной корпоративной банковской карты. Или личное финансовое приложение подобное приложению Venmo, разработанному для Android и мобильной операционной системы iOS, которое позволяет осуществлять быстрые, простые переводы между строго ограниченным числом физических лиц (например, родственниками).

Отслеживая обновление конкурентного продукта/услуги, как реагируют пользователи, вы находите отличие от своих продуктов/услуг, и решаете, стоит ли тратить время и ресурсы на погоню за конкурентом, если его инновация действительно дает ему какое-либо преимущество.

Коррекция маркетинговой стратегии

Быстрое развитие и распространение новейших технологий превращает многие инновации в общепринятые отраслевые стандарты. Важно поспевать их отслеживать, брать на вооружение, стараясь опередить конкурентов.

Придание бизнесу устойчивости, стабильности

По мнению Бласка, современное понимание устойчивости бизнеса заключается в следовании принципам ESG (экология, социальная политика, корпоративное управление), которые обещают успех в конкурентной борьбе при их воплощении «во все свои операции».

Кадровая стратегия

Этому аспекту уделено особое внимание. Поиск способных перспективных специалистов «еще никогда не стоял так остро для индустрии финансовых услуг, как сегодня». Опросы показывают, что менее половины работающих по найму в этой сфере довольны своей работой и не планируют никуда переходить. Джон Бухевер из Eagle Hill Consulting предупреждает: «Финансовые компании сталкиваются с серьезными конкурентными вызовами, в то время как их сотрудники чувствуют себя разочарованными, а число добровольных увольнений в банках растет небывалыми темпами». Конкурентная разведка держит в фокусе внимания размещение конкурентами объявлений о вакансиях, их кадровую политику, что крайне важно для корректировки и обновления собственной стратегии в этом вопросе.

Соблюдение требований регуляторов

Казалось бы, причем здесь конкурентная разведка? Ведь правила и нормы обязательны для всех. Дело в том, что на практике, сталкиваясь с новыми требованиями (а они появляются в финансовой сфере чаще, чем в других отраслях), организации реагируют разными путями. Одни переписывают внутренние политики и инструкции. Другие переносят выполнение новых норм на партнера/партнеров. Третьи присоединяют компанию, уже практикующую новые правила, как поступила, например, в 2016 году Visa, поглотившая CardinalCommerce с передовой технологией аутентификации.

Способ имплементации сигнализирует о стратегических планах компании. Так упомянутая сделка между Visa и CardinalCommerce продемонстрировала желание и готовность первой из них к серьезной экспансии в сегменте цифровой торговли. Конечно, данный случай не рядовой. Но он показывает, что правильно налаженная конкурентная разведка помогает найти нестандартные пути и способы опередить конкурентов.

«Социальное прослушивание» для финансовой сферы

Социальное прослушивание (social listening) это процесс мониторинга и анализа разговоров, обсуждений, отзывов и упоминаний о бренде, продукте или услуге в социальных медиа и на других онлайн-платформах. По данным интернет издания Social Media Today и онлайн сервиса Meltwater, около 60% американских компаний считают, что внедрили social listening в свою бизнес стратегию.

Социальное прослушивание находит широкое применение. Например, в конкурентной разведке важно следить за множеством событий: контрактами, слияниями и поглощениями, движением капитала, кадровыми назначениями, инновациями, финансовыми результатами, развитием партнерств, фандрейзингом, выставками и конференциями, выпуском новых конкурентных продуктов/услуг, публикациями отраслевой прессы, включая издания, которые принадлежат исследовательским компаниям (например, Gartner, Forrester), и так далее.

Сказанное относится и к финансовой сфере. Автор статей на сайте awario.com А. Горбач считает, что банки стали активно использовать социальное прослушивание несколько позже других отраслей экономики и бизнеса. Отчасти по причине распространенного заблуждения, что такие солидные организации как банки не нуждаются в социальных сетях. Им вполне хватает Гугла, чтобы получать, когда надо, нужную информацию.

Статистика опросов подвергает сомнению такой подход. Согласно одному из недавних отчетов компании SproutSocial (исследования социальных сетей и консалтинг), в чатах и на форумах люди говорят не только о своих финансовых проблемах, но и высказывают оценочные суждения о банках. Примерно половина упоминаний о финансах (46.6%) требует реагирования, разъяснительного ответа от банков, но только 13.4% в реальности его получает.

Социальное прослушивание помогает определить место организации на рынке, географию популярности, лучше понимать целевую аудиторию, осуществлять конкурентный анализ, сравнивая сильные и слабые стороны своей и конкурирующих организаций.

Наконец, выявить и предупредить потенциальные риски для бренда, игнорирование которых может привести к кризису. Ежедневный или недельный мониторинг негативных высказываний обнаружит проблему, а своевременно реагирование не допустит перерастания локального недовольства в громкий скандал.

Как отмечает журнал Risk Management Magazine (rmmagazine.com), злоумышленники активно пользуются скоростью, широтой охвата социальных медиа, доступностью к миллионам пользователей для реализации имитационных схем мошенничества, чреватых финансовыми и репутационными рисками компаний.

Бруно Фарнелли, старший директор по операциям и аналитике компании ClearSale (услуги по борьбе с мошенничеством и защите от возвратных платежей), в частности, пишет: «Социальное прослушивание должно стать неотъемлемой частью программы управления рисками. Оно предполагает мониторинг упоминаний вашей организации, акционеров и топ-менеджеров, наиболее популярных продуктов/услуг. Своевременный анализ этих упоминаний позволяет обнаруживать попытки мошенничества еще до их применения» (rmmagazine.com).

Ведение мониторинга не должно ограничиваться специалистами. Это также обязанность тех банковских работников, кто работает непосредственно с клиентами. Им проще первыми заметить признаки мошеннических аккаунтов, схем и информировать руководство.

При обнаружении мошеннической уловки Фарнелли рекомендует сразу же документировать скриншотом и предавать огласке подменную рекламу или пост, вредоносный вымысел, фейковый веб-сайт.

Обмен информацией как ключевой фактор борьбы с мошенничеством и отмыванием денег

Цифровизация финансовой сферы, с одной стороны, гигантски ускорила и облегчила банковские операции, но с другой – дала злоумышленникам широкие возможности для финансового мошенничества, что отразилось на криминальной статистике.

Так, поток жалоб на аферы и жульничество в Валютное управление Гонконга (HKMA), осуществляющее практически функции центрального банка, возрос в 2023 году вдвое по сравнению с предыдущим годом. Это соотносится с ростом на 50% случаев мошенничества, зафиксированных полицией Гонконга за тот же период.

Волна криминализации финансового сектора заставила Валютное управление Гонконга с удвоенной энергией заняться налаживанием системы быстрого обмена данными между разными организациями для эффективного реагирования на действия преступников. Эта система, существующая уже несколько лет, представляет собой оперативную группу разведки инцидентов мошенничества и отмывания денег (FMLIT) в составе: а) упомянутого Валютного управления, б) соответствующего подразделения полиции по борьбе с мошенничеством, 3) около 30 ведущих банков.

В распоряжении группы - механизм блокировки подозрительных переводов, система банковского мониторинга финансового трафика. Тесное партнерство государственных и частных организаций принесло свои плоды. За последние годы удалось своевременно отреагировать и вернуть похищенное на сумму более миллиарда гонконгских долларов. Заблокировано переводов на сумму более 12 миллиардов гонконских долларов.

Вместе с тем, банковское сообщество и власти Гонконга посчитали предпринятые меры «недостаточно эффективными». Проблема - пробелы в организации обмена данными, который происходит, как правило, по факту совершенного преступления. Благодаря временному лагу между обнаружением жертвой факта мошенничества, сообщением в полицию, началом расследования преступники успевают перевести деньги на мул-счета (**m**ule account - банковский счёт, используемый для отмывания денег и мошеннических транзакций).

Поэтому летом 2023 года Ассоциация гонконгских банков **(**The Hong Kong Association of Banks) совместно с Валютным управлением (HKMA) и полицией инициировала проект электронной платформы FINEST (Financial Intelligence Evaluation Sharing Tool). На базе платформы пяти крупнейших банков Гонконга осуществляется обмен данными, указывающими на возможную преступную активность в сфере инвестиций, онлайн коммерции, любовных афер (romance scams).

Новый инструмент борьбы с мошенничеством позволяет идентифицировать прежде не фиксируемые подозрительные счета и трансакции, начинать немедленно по ним расследование. Из соображений прайвеси FINEST пока отслеживает только корпоративный сегмент, хотя, как замечает Эдди Юэ, глава Валютного управления Гонконга, большинство мул-счетов индивидуальны. В его планах - распространить контроль и мониторинг на лицевые счета (hkma.gov.hk).

Другое не менее важное перспективное направление – охват системой обмена информацией (FINEST) всех лицензированных банков Гонконга (на начало 2024 г.

лицензированных банка плюс 8 виртуальных банков, занимающихся коммерческим кредитованием и личными банковскими услугами). Это предложение обсуждалось банковским сообществом в течение первой половины 2024 года. С принятыми поправками проект документа будет внесен парламент Гонконга в 2025 году.

Проект предусматривает определенные ограничения в распространении информации. Во-первых, она должна касаться исключительно задач обнаружения и предотвращения мошенничества и других видов финансовых преступлений. Во-вторых, каналы обмена будут максимально защищены от несанкционированных вторжений. И даже после отправки сообщения о подозрительной активности банк должен будет держать эту информацию строго конфиденциально.

Валютное управление согласно проекту документа будет надзирать за соблюдением банками всех правил и ограничений. Оно планирует выпустить письменное руководство, где пропишут условия, приемлемые и допустимые для предоставления информации, требования к ее хранению.

В России Центральный банк и МВД РФ ведут систематический онлайн-обмен информацией для противодействия кибермошенникам с 21 октября 2023 года, когда вступил в силу Федеральный закон № 408-ФЗ "О внесении изменений в статью 26 Федерального закона "О банках и банковской деятельности" и статью 27 Федерального закона "О национальной платежной системе". По нему МВД России оперативно получает данные о финансовых операциях из автоматизированной системы Банка России ФинЦЕРТ (Центр взаимодействия и реагирования Департамента информационной безопасности). Согласие клиента для этого не требуется.

Получив обращение жертвы сотрудники МВД могут запрашивать у регулятора данные о мошеннической операции и получателе похищенных средств. Если сведения отсутствуют в базе ФинЦЕРТ, регулятор обратится непосредственно в банк. Как только информация от полиции поступит в базу, банк может сразу остановить подозреваемому в мошенничестве все операции, заморозить деньги на его счетах на время следствия и суда.

С июля 2024 года все финансовые организации России обязаны блокировать счета и карты людей, которые появляются в базе мошеннических переводов.

Технологии, методологии

Data-driven разведка во времена кризиса и неопределенности

«Data-driven разведка» (или любая иная деятельность) — это подход, при котором решения принимаются с преобладающей опорой на данные, и переводится как «управляемая данными разведка». Иногда data-driven подход противопоставляют принятию решений на основе интуиции, опыта или мнения руководства. Еще, случается, противопоставляют лучшим практикам, общепринятым стандартам отрасли.

Вадим Шестаков, руководитель отдела аналитики маркетингового агентства Adventum, уверен, что data-driven подход эффективнее, так как минимизирует риск ошибок в отличие от решений, принимаемых интуитивно или по шаблону (scillbox.ru).

Методики data-driven проникли и в финансовую сферу. Центральный банк России использует их для принятия решений в сложных условиях. Еще в 2022 году специалисты и руководители ЦБ прошли интенсивные тренинги по «управлению на основе данных» (data-driven management) у ведущих экспертов из Института бизнес-аналитики и компании Visiology. "Экспертиза data-driven позволяет выстроить в любой организации новый уровень культуры принятия решений, обеспечивая возможность эффективного управления в условиях постоянно нарастающего объема данных", — рассказал в ходе тренингов Иван Вахмянин, руководитель и со-основатель Visiology, эксперт по анализу и визуализации данных, преподаватель Университета Иннополис (comnews.ru).

Ключевым фактором работы банка в парадигме data-driven директор департамента развития технологий искусственного интеллекта и машинного обучения Сбербанка Максим Еременко называет количество решений, принимаемых на основе анализа данных. При этом делает акцент на культурном аспекте: «Иногда надо убедить себя, что аналитика данных дает более консистентный, более достоверный результат, чем эксперт, который сидит в этом направлении уже 25 лет, но может не знать чего-то, что показывают данные» (futurebanking.ru).

В современном мире бизнеса, полном непредсказуемости и глобальных кризисов, data-driven разведка приобретает ключевое значение для кризисного управления, позволяя преодолевать сложности быстрым и точным определением тенденций, рисков и угроз, выявлением причин трудностей, своевременным и адекватным реагированием.

Пол Сантилли, эксперт в области конкурентной разведки, одно время возглавлявший совет директоров SCIP (организации профессионалов конкурентной разведки), рассматривает роль data-driven разведки в кризисном менеджменте как три последовательных этапа.

Этап первый – подготовительный, характеризующийся изучением пока еще слабых сигналов раннего предупреждения о потенциальных угрозах. На этом этапе компании собирают и анализируют данные о рыночных аномалиях, изменениях в покупательских предпочтениях и так далее… Предиктивная аналитика и алгоритмы искусственного интеллекта позволяют выяснить характер предполагаемых рисков, будь то экономическая рецессия, перебои в цепочках поставок, киберугрозы или нечто другое. Тем самым компании выигрывают время для заблаговременной подготовки к кризису.

Этап второй - собственно ответ на кризис. На основе данных из разных источников, таких как внутрикорпоративные операции, социальные медиа, обмен мнениями покупателей/клиентов услуг и других, проводится глубокая оценка масштабов и потенциальных последствий кризиса, проверка и уточнение мер реагирования, гарантирующих их эффективность, адаптивность к быстро меняющимся условиям.

Этап третий – восстановление. Предполагается анализ данных с точки зрения того, что получилось в ходе управления кризисом, а что надо улучшать, внося коррективы в политики, инструкции, планы подготовки к будущим кризисам.

При этом важно иметь в виду использование метрик эффективности, которые могут выражаться цифрами сохраненной клиентуры, потраченного на восстановление времени, финансовых издержек. Правильные выводы и уроки помогают организации лучше готовиться к будущим кризисам и потрясениям.

Пол Сантилли уверен, что data-driven разведка значит «много больше, чем инструмент реагирования, поскольку представляет собой критически важный компонент конкурентной устойчивости» (scip.org). Ее проактивный характер позволяет не только преодолевать кризисные времена, но и принимать обращенные на перспективу стратегические решения.

Искусственный интеллект для конкурентной разведки: преимущества и ограничения

Влияние технологий на конкурентную разведку невозможно переоценить. Его можно сравнить с революцией, которую произвели в информационной работе первые персональные компьютеры и поисковые машины. Алгоритмы просеивают гигантские массивы данных, выявляя характерные особенности, тенденции, аномалии, то есть совершают за считанные минуты объем работы, на который человеку понадобились бы недели и месяцы.

Джеспер Мартелл, руководитель компании Comintelli (провайдер решений для деловой разведки), считает наиболее важным приобретением ИИ его способность автоматически и в режиме реального времени отслеживать веб-сайты конкурентов, фиксируя и анализируя всё новое, что там появляется, кто, когда, где и в каком контексте упоминает объект мониторинга (scip.org).

Другой эксперт, Алекс Уолтен, выделяет главные направления развития конкурентной разведки на основе технологий искусственного интеллекта:

1. Мониторинг рынка и конкурентов с использованием одновременно большого числа ресурсов – новостных сообщений, финансовых отчетов, социальных сетей, отраслевых изданий и т.д. Инструментарий ИИ позволяет отслеживать и анализировать присутствие конкурентов в интернет пространстве, вычленять в общем информационном потоке данные об изменениях в их развитии – появлении новых продуктов, отделений, расширении/сужении клиентской базы, тому подобное.
2. Анализ настроений клиентов у конкурентов в динамике.
3. Изучение изменений в рыночных тенденциях (продукты и цены).

Помогая решать эти задачи, искусственный интеллект освобождает специалистов от кропотливого и затратного с точки зрения времени и физических ресурсов труда по фильтрованию информационного шума, позволяя им сосредоточиться на интерпретации обработанных машинами данных, выводах и решениях.

В то же время надо помнить, даже самые совершенные технологии имеют ограничения. Искусственный интеллект тоже не свободен от недостатков. Он может

давать правильные ответы на вопросы «кто», «что», когда», «где», но лишен возможности (пока, во всяком случае) ответить на самый главный вопрос - «почему?».

Только человеческий мозг в состоянии понимать контекст проблемы, опираясь на отраслевые знания, профессиональный опыт, в не малой степени и на интуицию. Джеспер Мартелл считает, что при всех захватывающих дух перспективах искусственного интеллекта только человек-аналитик способен разглядеть в изменениях кадровой политики конкурента подготовку к серьезной коррекции рыночной стратегии. А машина может это пропустить.

Более того, человек руководствуется в своей работе определенными этическими принципами, например, имея дело с персональными данными. А искусственный интеллект этот момент может проигнорировать.

ИИ даст ошибочную интерпретацию данных, если контекст изучаемой проблемы не вполне ясен, указывает В. Собусяк, топ-менеджер компании Proactive Worldwide (исследования, консалтинг). Пример с кадровой политикой. Резкий рост вакансий у конкурента искусственный интеллект может воспринимать как свидетельство к расширению производства/услуг. Аналитик же разберется, что наблюдаемый феномен связан с большим оттоком кадров, что может свидетельствовать о неполадках внутри компании.

Только человеку под силу учитывать в совокупности политические, культурные, психологические, другие важные аспекты в работе изучаемого объекта. Глубокое проникновение в контекст, подчеркивает Собусяк, особенно ценно применительно к таким отраслям экономики и бизнеса как здравоохранение, юриспруденция, международная торговля.

Искусственный интеллект помогает в обработке данных, но пока еще не обладает способностью понимать цели и задачи компании, его корпоративную культуру, стратегические приоритеты. Возможно, это дело недалекого будущего.

Кадры

10 главных компетенций аналитика деловой разведки

Веб-сайт scip.org международной организации профессионалов конкурентной разведки, последнее название которой – «Стратегический консорциум профессионалов разведки», опубликовал статью эксперта в этой области Мэтью Селла об основных профессиональных требованиях к специальности «insights analyst». Последнее определение трудно перевести на русский дословно. Допустимыми представляются варианты: аналитик данных или аналитик информации.

Автор рассматривает требуемые для аналитика знания и умения под углом зрения оценки компетенций кандидата на работу в качестве insights analyst. Итак, требуются следующие компетенции:

Пытливый ум. Аналитик постоянно формулирует для себя и коллег вопросы. Последние касаются не статичного состояния исследуемых объектов в данный конкретный момент, но как бы они (объекты) выглядели, если бы… Такой подход позволяет понять не только настоящее и прошлое изучаемого явления, но и возможную его эволюцию в будущем.

Постоянное накопление знаний. Аналитик должен непрерывно постигать новые для него/нее вещи и не останавливаться на достигнутом. Хороший специалист пытается заглянуть дальше происходящих и даже назревающих перемен.

Умение связывать разрозненные факты в единое целое. Практически не бывает полной и ясной картины, когда вы рассматриваете потенциальные возможности и перспективы. Какие-то фрагменты мозаики отыскать нельзя. От аналитика требуется умело оперировать имеющимися данными и по ним выстраивать адекватную информационную картину.

Мыслить нешаблонно, за рамками общепринятого. Речь идет о способности видеть «большую картину» с разных точек зрения. Особенно это качество важно в ходе т.н. «штабных игр», когда рассматриваются разные варианты развития рынка, ожидаемых действий конкурентов.

Обеспечивать контекст и знание. М. Селл имеет здесь в виду, что «знание рынка означает знание клиентов (их запросов), равно как и понимание бизнеса». Это необходимо для верного прогнозирования рыночных тенденций.

Специалист по работе с данными. Данные сами по себе ничто. Умение их интерпретировать, делать на их основе верные заключение и решения – ключевая компетенция аналитика.

Умение презентовать свои результаты убедительно и не скучно. Лучший способ убеждать – рассказать историю. Аналитик должен уметь конструировать отчет. Первая часть – ситуация как она выглядит. Вторая – в чем проблема или проблемы. Третья – способы и пути решения.

Отличная коммуникабельность. Особенно необходима в больших коллективах, где приходится постоянно контактировать с отделами продаж, маркетинга, инженерами и юристами.

Умение продвигать себя и свою команду в компании. Признание, узнаваемость, благодарность и вознаграждение за труды - все это не приходит автоматически. Многое зависит от умения подать свою работу. Вы можете быть незаменимым работником для организации, но если об этом мало кто в компании знает, то, значит, и не имеет значения.

Надежный, доверенный советчик. Вопрос вашей репутации, которая зависит от способности наладить хорошие отношения с акционерами и топ-менеджерами, другими словами, искусство межличностных отношений.

Рекрутинговый сайт velvetjobs.com сформулировал следующие квалификации для соискателей на работу в должности insights analyst:

- Минимум трехгодичный опыт аналитической работы в сфере продаж
- Большой интерес к маркетингу
- Степень бакалавра/магистра в данной отрасли бизнеса, включая знание маркетинга, покупательского поведения, статистики, математики, финансов, экономики
- Серьезный опыт анализа данных
- Владение инструментами Google Analytics, Moat (анализ медийной рекламы), MRI (маркетинговые исследования), comScore (анализ рынка интернет технологий), Tableau (программное обеспечение для интерактивной бизнес-аналитики и визуализации данных)
- Интерес к работе с цифрами
- Умение составлять отчеты по работе с данными
- Высокая степень самосознания и самоосмысления
- Умение презентовать результаты работы
- Продвинутое умение работать с приложениями Microsoft
- Технические знания программного обеспечения SAS и Oracle
- Опыт работы с коллегами в компании и внешними партнерами.