БИЗНЕС-РАЗВЕДКА

№ 64

Оглавление

Управление данными: приоритетные тенденции в 2025 и на ближайшие годы

Дисциплина «управление данными» (data management) окончательно освободилась от ярлыка «второстепенности» для бизнеса и экономики. Сегодня это ключевой фактор успешного развития бизнеса, его эффективности.

Я. Мехта, автор статей в ведущих западных изданиях по проблемам анализа данных, Интернета вещей, информационных инновационных технологий, в публикации онлайн издания Chief Information Officer, Jan 30, 2025, отмечает и характеризует наиболее актуальные и приоритетные направления развития науки и практики управления данными.

Интеграция с искусственным интеллектом и машинным обучением

Искусственный интеллект и машинное обучение полностью преобразили процессы управления данными, автоматизировав и оптимизировав такие процессы работы с информацией как:

- metadata tagging **(**процесс добавления описательной информации о данных для улучшения удобства их использования);

- schema creation (организация объектов базы данных, оптимизация и улучшение общей структуры базы данных);

- data lineage mapping (процесс понимания, документирования и визуализации данных от момента их возникновения до момента использования).

Новые возможности позволили минимизировать ошибки, обусловленные человеческим фактором, гигантски ускорить процессы обработки данных. К примеру, искусственный интеллект анализирует качество информации, сигнализируя об аномалиях, несоответствиях, оптимизируя процесс запросов к базе данных.

Маскировка данных

Маскировка (обфускация) данных — это способ защиты конфиденциальной информации от несанкционированного доступа путём замены исходных данных фиктивными данными или произвольными символами. При этом замаскированная информация выглядит реалистично и непротиворечиво и может использоваться в процессе тестирования программного обеспечения. В большинстве случаев маскировка применяется для защиты персональных данных, закрытой служебной информации.

В 2025 году маскировка данных приобретает стратегическое значение. С ускоренным расширением гибридной и мульти-облачной среды, бизнес как никогда ранее критически нуждается в надежной защите своих данных, обрабатываемых разными системами. Инновационные специальные решения (IBM, K2view, Oracle, Informatica и некоторые другие) предлагают масштабируемые, учитывающие контекст методы маскировки данных в режиме реального времени. В отличие от традиционных способов, такие решения обеспечивают полную доступность тестирования, анализа, развития данных без малейшего для их качества урона. При этом сохраняется унифицированный подход к управлению данными, разбросанными в изолированных хранилищах.

Интеграция данных в режиме реального времени с поддержкой масштабирования

Интеграция данных в режиме реального времени имеет ключевое значение, особенно для финансовой сферы, где высокая скорость операций критически необходима. Уже в самом близком будущем такие технологии, как, например, «change data capture» - отслеживание изменений в базах данных (вставки, обновления и удаления записей) и передача в целевые системы в режиме реального времени – обеспечат синхронизацию в управлении бескрайними массивами данных с минимальным лагом.

Стратегия «cloud-first data»

Cloud-first data — стратегия, подразумевающая миграцию большей части IT-инфраструктуры организации на облачную платформу, что дает компании преимущество в вопросах экономичности, надежности, улучшения возможностей восстановления и другие выгоды.

Стратегия «cloud-native data lakes» («облачные озера данных»)

Речь идет о централизованных облачных хранилищах для сырых, структурированных, полуструктурированных и неструктурированных данных**.** **Они** позволяют компаниям осуществлять продвинутую аналитику и обработку данных без значительных инвестиций в инфраструктуру, выполнять сложные преобразования данных, исследовательский анализ и решать задачи машинного обучения прямо на «озере данных». Аналитика структурированных и неструктурированных данным существенно облегчается.

Соблюдение этических норм в управлении данными с помощью искусственного интеллекта

По мере внедрения искусственного интеллекта в процессы принятия решений на основе управления данными все более остро встает вопрос о соблюдении правил этики. Этика искусственного интеллекта необходима, чтобы оперировать объективными метриками, избегать влияния предвзятостей и предубеждений на принимаемые решения, контролировать процессы, быть уверенными в надежности и точности результатов.

Концепции этической ответственности в ИИ разрабатываются и внедряются во многих странах. Даже создаются специальные организации, как, например, Европейская комиссия по этике в области искусственного интеллекта. Среди принципов этической ответственности:

- принцип благодеяния (ИИ должен приносить людям и обществу пользу, а не вред);

- принцип справедливости и не дискриминации;

- принцип прозрачности и неподотчетности;

- принцип уважения автономии человека;

- принцип конфиденциальности и защиты данных.

ИИ этика – сфера ответственности разработчиков, производителей и пользователей системами искусственного интеллекта.

В России ведется работа по разработке этических норм. В 2021 году был принят «Кодекс этики в сфере ИИ». Необходимость выработки этических стандартов закреплена в «Национальной стратегии развития искусственного интеллекта на период до 2030 года» (http://www.kremlin.ru/acts/bank/44731).

Forensic Accounting как инструмент выявления и предупреждения финансовых преступлений

Forensic Accounting (далее FA) обычно переводится на русский как судебная или судебно-бухгалтерская экспертиза. Такая формулировка заведомо ограничивает ее задачи уголовными делами, которые связаны с хищениями и другими экономическими преступлениями, налоговыми, таможенными и прочими корпоративными спорами.

Между тем, большинство экспертов трактуют FA в расширительном смысле как, прежде всего, дисциплину, которая активно используется бизнесом (а не только судебными органами) для обнаружения и предупреждения внутрикорпоративных финансовых преступлений.

С другой стороны, экспертиза FA не укладывается в рамки стандартной бухгалтерской практики. Ее практика требует специальных знаний, включая владение методологией финансовой отчетности, аудита и расследований. Специалистов FA можно идентифицировать как своего рода «финансовых детективов» или «финансовых криминалистов». Их отличает умение работать с данными по следующим направлениям:

Анализ данных. Использование методов анализа данных для выявления признаков аномалий в финансовой активности, возможно, указывающих на мошенничество.

Анализ финансовой отчетности для обнаружения расхождений, несоответствий в финансовой документации. Детальному изучению подлежат бухгалтерские отчеты, транзакции, иные имеющие и не имеющие прямого к финансам отношения информационные ресурсы (например, электронная почта) на предмет фиксации признаков манипулирования и недостоверности.

Расследование хищений. В случае подозрений на мошенничество специалисты FA проводят тщательное расследование, собирая свидетельства и улики путем опросов и реконструкции финансовых транзакций. При наличии судебной перспективы привлекаются юристы, собственные и/или привлеченные извне независимые консультанты.

В арсенале финансовых криминалистов – богатое разнообразие технических средств и технологических инструментов. В их числе эксперты выделяют:

Анализ финансовых коэффициентов (Financial ratio analysis). К ним относятся доходность, кредитоспособность, ликвидность. Сравнение коэффициентов компании со среднестатистическими показателями по отрасли или аналогичных по размеру других организаций помогает идентифицировать отклонения, аномалии как возможные признаки мошенничества. К примеру, резкое и беспричинное, на первый взгляд, падение чистого валового дохода может послужить основанием для специального расследования.

Технологии аналитики данных. Машинное обучение, искусственный интеллект, средства автоматизации все шире используются для решения задач FA, таких, в частности, как вскрытие фактов манипуляции финансами, злоупотребления схемами материального стимулирования, взяточничества, других видов коррупции.

Анализ Закона Бенфорда. Это статистический инструмент для наблюдения за распределением ведущих цифр в реальных наборах данных. Согласно этому закону ведущие числа не равномерно распределены в наборе данных, но следуют предсказуемому шаблону. Анализ Закона Бенфорда используется для обнаружения несоответствий или мошенничества в данных**.** Значительные отклонения от ожидаемого распределения могут указывать на ошибки, манипуляцию или неточную отчётность. Расследователи выискивают неестественное распределение ведущих чисел в финансовой отчетности. Для них эта картина служит красным флажком, указывающим на потенциальное финансовое злоупотребление.

Мониторинг транзакций. Финансовые криминалисты тщательно отслеживают финансовые потоки между системами и подразделениями компании в попытке обнаружить мошенничество.

Интервью. Одна из ключевых компетенций специалиста FA – умение проводить опросы свидетелей, допросы подозреваемых для сбора данных, воссоздания последовательности и хронологии событий, исследования причин обнаруженных финансовых нестыковок и противоречий.

Ни одна организация не обладает иммунитетом от рисков мошенничества. Для стимулирования полноценных процессов выявления и предотвращения финансовых преступлений эксперты рекомендуют не упускать из виду следующие профилактические меры и шаги:

Приоритетное отношение к тренингам и программам ознакомления персонала с рисками и угрозами. Их надо проводить регулярно, обучая работников умению распознавать признаки мошенничества, своевременно информировать начальство о замеченной подозрительной активности.

Постоянно действующая система оценки и анализа рисков, призванная своевременно вскрывать уязвимости организации, играющие на руку мошенникам и расхитителям.

Модернизация финансовых инструментов в соответствии с требованиями дня. В частности, внедрение автоматизации в процессы авторизации транзакций, сверки счетов, финансовой отчетности.

На заре квантовой конкурентной разведки

Сегодня на каждом шагу слышишь и читаешь, что человечество вошло в новую технологическую эпоху, знаменательную искусственным интеллектом, машинном обучением, робототехникой и так далее. Между тем, внедрение этих технологий требует колоссальных вычислительных ресурсов. На пороге – квантовые вычисления. Их поминают реже, но именно они, по мнению большинства ученых, полностью изменят облик окружающего мира уже в обозримом будущем. На смену нынешним компьютерам идут квантовые.

Алексей Федоров, научный руководитель группы «Квантовые информационные технологии» Российского квантового центра, пишет: «ограничения многих традиционных способов работы с данными можно будет преодолеть при помощи высокопроизводительных квантовых компьютеров…. Квантовые компьютеры сейчас динамично развиваются, их построением занимаются такие гиганты, как Google, IBM, Microsoft и Intel. Россия вошла в число стран, которые приняли долгосрочные программы развития — квантовые «дорожные карты» (подробнее: https://trends.rbc.ru/trends/industry/64ef1f429a7947cead947763?from=copy).

Одна из многих сфер практического применения квантовых компьютеров – конкурентная разведка. Эксперты из Стратегического консорциума профессионалов конкурентной разведки уверены, что применяемые в разведке квантовые технологии смогут «обрабатывать гигантские массивы данных с беспрецедентной быстротой, открыв возможности таких решений и инсайтов, которые пока еще недоступны в настоящее время» (scip.org).

Квантовая разведка преобразит следующие процессы КР:

Анализ данных. Обработка квантовыми алгоритмами информации позволит бизнесу анализировать тенденции, системы, аномалии намного быстрее, чем это делают нынешние компьютеры.

Оптимизация бизнес-решений. Квантовая разведка способна одновременно моделировать огромное множество сценариев и их последствий, помогая компаниям своевременно оценивать действия конкурентов, рыночные сдвиги, или, к примеру, потенциальные сбои в цепочках поставок и адекватно на них реагировать.

Предиктивная аналитика. Квантовая разведка существенно улучшит процесс прогнозирования клиентских предпочтений, стратегии конкурентов, в целом динамики развития рынков с небывалой ранее точностью.

Усиление кибербезопасности. Квантовая технология позволит не только улучшить идентификацию уязвимостей в системе кибербезопасности, но и выработать действенные меры защиты против квантовых кибератак.

Для бизнеса квантовая разведка означает широчайшие возможности для определения и оценки в режиме реального времени зарождающихся новых возможностей, впрочем, как и угроз, более точного и глубокого понимания конкурентных стратегий, прогнозирования и минимизации потенциальных рисков для цепочек поставок на волатильных рынках.

При всем огромном потенциале квантовой разведки, предупреждают эксперты, в ее практической реализации просматриваются немалые проблемы и трудности. Во-первых, развитие и внедрение квантовых технологий требует больших инвестиций в инфраструктуру. Во-вторых, для такой сравнительно узкой сферы как бизнес-разведка будет нелегко найти специалистов по квантовым вычислениям. В-третьих, ускоренное внедрение и распространение квантовых алгоритмов неизбежно породит опасения относительно защиты информации, прозрачности операций, а также этических аспектов конкурентной разведки.

К приходу квантовой эпохи надо готовиться сегодня. Стратегический консорциум профессионалов конкурентной разведки призывает бизнес и специалистов активно действовать по следующим направлениям:

- Развивать грамотность и осведомленность о квантовых технологиях и их практическом применении.

- Инвестировать в подготовку специалистов по квантовым вычислениям и искусственному интеллекту.

- Налаживать партнерские связи с провайдерами квантовых технологий, научно-исследовательскими центрами в вопросах разработки и использования соответствующих программных решений.

Хотя кантовые технологии находятся еще в начале своего развития, их трансформирующее влияние на конкурентную разведку с каждым годом возрастает.

Опросы и допросы в расследовании корпоративных финансовых преступлений

Продолжаем начатую в предыдущем (№63) выпуске журнала серию статей о корпоративном расследовании финансовых преступлений.

Чем различаются между собой опросы и допросы?

Задача интервью со свидетелем (опроса) - собрать факты и мнения. Причем мнение свидетелей может быть существеннее сообщенных им сведений и фактов. В ходе интервью важно уловить настроение собеседника, его/ее желание идти на откровенный контакт. Доверие и понимание необходимо создать как можно быстрее, уже в самом начале беседы.

Следует иметь в виду, что свидетели могут давать показания под тяжелым психологическим грузом, если речь идет о действиях начальников и коллег. К тому же со временем их показания могут «выгорать», то есть меняться или противоречить высказываниям других свидетелей. Поэтому необходимо держать всю документацию расследования в полном порядке. Документы помогают не только освежить чью-то память, но и содействовать приведению к общему знаменателю противоречивых данных.

У ведущего расследование в процессе работы постепенно складывается собственное мнение о том, что произошло. Свидетели едва ли будут с вами откровенны, если по характеру задаваемых им вопросов, по тону поймут, что у вас уже сложилось определенная точка зрения и решение принято. Некоторые участники даже побоятся в этом случае высказывать нечто, что может противоречить вашему мнению. В худшем случае они подумают, что с ними ведут нечестную игру, вынуждая к определенным показаниям. Поэтому нужно хранить молчание, не снимая до завершения расследования маски объективности и беспристрастности.

Давшего показания свидетеля необходимо уверить в том, что расследование ведется компетентными профессионалами, которые во всем разберутся, но до завершения расследования ни одна сторона не имеет права раскрывать содержание интервью. Более того, результаты расследования, равно как и принимаемые по его результатам меры, также могут сохранять конфиденциальность. Наилучшим завершением беседы была бы просьба к свидетелю восстановить контакт, если он/она вспомнит что-то дополнительное и важное.

В отличие от опроса допрос преследует следующие цели:

- Подтверждение уже собранных фактов и доказательств
- Воссоздание реальной картины преступления в структурированном виде
- Признание вины подозреваемым

Интервью с подозреваемым (допрос) проводится обычно тогда, когда его/ее вина в преступлении уже обоснована рядом фактов и свидетельств. Такие беседы более сложны по сравнению с опросами свидетелей и требуют тщательной подготовки, серьезного предварительного обдумывания. Вопросы носят обвинительный характер, принуждающий собеседника сознаться в содеянном и предоставить точную, критически важную информацию о преступлении.

Допрос по сравнению с опросом обычно более интенсивный и структурированный. Он предполагает конфронтационный подход, включая элементы психологической манипуляции. Расследователь выкладывает собеседнику факты и свидетельства, разрушающие его/ее попытки оправдаться. В то же время он не должен выходить за рамки закона и правил, нарушающих права обвиняемого, оперируя информацией, которая, возможно, будет использована в судебном заседании.

Эксперты рекомендуют соблюдать особую осторожность в работе с документами. Оригиналы не могут подвергаться каким-либо корректировкам или видоизменениям. Такой подход позволяет избежать риск признания документа не действительным.

Тщательно записывайте показания, включая дату, время, место интервью, данные о свидетеле, всех при этом присутствующих. Включайте в протокол все без исключения факты и прочие данные, сообщаемые или опровергаемые свидетелем, используя его/ее собственные слова и

обороты речи, не ограничиваясь одними лишь заключениями. Столь скрупулезная фиксация показаний поможет впоследствии, в ходе принятия решения, точно воспроизвести то, что было сказано во время интервью. Подробные, детальные документы также пригодятся для обоснования и защиты вашей позиции во время судебного процесса, если до него дойдет дело.

Предвзятость как этическая и практическая проблема в расследовании финансовых преступлений

Предвзятость (предубеждение, пристрастность, в общем, необъективность) – неотъемлемая черта человеческого характера. Проявляется в отношении других людей иногда сознательно, но чаще всего неосознанно. Охватывает широкий круг социальных стереотипов, имеющих отношение к полу и расе человека, его возрасту, социальному положению, религиозным убеждениям и так далее.

Ученые из Института Кирвана, исследовательского центра при Университете штата Огайо в Колумбусе, штат Огайо, так охарактеризовали неосознанную предвзятость: «набор определенных стереотипов, автоматически воздействующих на восприятия и убеждения, на поведение и поступки. Она (предвзятость) может быть позитивна или негативна, но в любом случае возникает и влияет вне осознания, желания и контроля со стороны человека». Подробнее смотри: (https://kirwaninstitute.osu.edu/research/state-science-introduction-implicit-bias-review-2018-2020).

Расследователи финансовых преступлений, естественно, не составляют исключения. Свойственные им, как всем людям, пристрастия и предубеждения могут сказаться в процессе работы, отразиться на выводах и принимаемых решениях. Если расследователи не осознают свои предубеждения и предвзятости, то привносят риск недооценки или, напротив, переоценки потенциальных угроз, подозрительной активности, ошибок в анализе исследуемых объектов, процессов и их участников.

Авторы статьи на сайте консалтинговой компании Crowe LLP (финансовые аудиты) Х. Хоксуорт и К. Саксе, обращают внимание на такую человеческую особенность, как зависимость от накопленной в прошлом информации, которая довлеет при каждом новом расследовании и нередко мешает восприятию специфики конкретной ситуации в реальном времени.

Имея в виду потенциальные последствия некорректного, ошибочного или неполного расследования, особенное значение приобретает способность расследователей понимать и преодолевать собственные предвзятости. Но как это делать?

Хоксуорт и Саксе предлагают три следующие действия:

Распознать и признать наличие у себя определенных пристрастий и предубеждений

Этим шагом расследователи сознательно настраивают себя на объективный и беспристрастный анализ, на соблюдение норм профессиональной этики. Расследователю финансового преступления, подобно судье или ученому, необходимо фокусировать внимание строго на имеющихся у него/нее фактах, делать выводы на основе объективного анализа, а не на субъективных предубеждениях.

Осуществлять стандартные процедуры и участвовать в регулярных тренингах

Чтобы обеспечить корректное и эффективное расследование, его организаторы должны неукоснительно придерживаться стандартизированных процедур, инструкций, шаблонов. Это необходимые инструменты для структурированного, упорядоченного расследования. Кроме того, важно предусмотреть специальные занятия, в ходе которых участники обучаются методам идентификации и нейтрализации своих предвзятостей. Проводить такие тренинги надо регулярно, не реже раза в год.

Разработать и внедрить систему контроля качества расследования

Система контроля качества (quality control frameworks) организуется и осуществляется независимыми экспертами, не входящими в команду расследователей. Она включает инструменты для мониторинга и проверки процессов, в данном случае – процессов расследования (чек-листы, диаграммы Парето и прочие), которые помогают обнаруживать возможные предубеждения, предупреждать их воздействие на результаты работы, проверять объективность, справедливость анализа ситуации. Выбирается модель, которая учитывает и опирается на методологию управления рисками, позволяющую определить проблемы и области, потенциально наиболее подверженные влиянию предубеждений.

Помимо этого эксперты рекомендуют практиковать обратную связь, сбор мнений участников свидетельских опросов о проведенных в рамках расследования процедурах и процессах. Эти мнения, особенно критического характера, помогут обнаружить влияние субъективных факторов и вовремя принять меры к их устранению, минимизировать воздействие на результаты расследования.

В чем опасность информационных перегрузок для бизнес-разведки

Относительно деловой разведки все еще бытует устаревшее мнение, что чем больше данных , тем лучше для результатов анализа.

Между тем, стремление искать и собирать все, что может пригодиться, чревато возникновением немалых проблем, в первую очередь, перенасыщенностью информацией.

Доступные сегодня массивы данных поражают воображение. Как подсчитали эксперты, в 2025 году ожидается, что генерация данных в мире составит 175 зеттабайтов (ZB). Чтобы представить себе объем одного зеттабайта, сошлемся на публикацию на сайте nag.ru. Для хранения одного ZB требуется около 83 миллионов жестких дисков емкостью 12 терабайт. Другое сравнение: один ZB равен памяти 34,4 миллиарда смартфонов каждый с емкостью 32 гигабайта.

В практической жизни сбор и обработка «монблана» информации нередко оборачивается напрасной тратой времени и ресурсов. При этом надо иметь в виду, что использование искусственного интеллекта в управлении данными многократно умножает объем собираемой информации, что соответственно увеличивает нагрузку на аналитиков, без активного участия которых точные, глубокие инсайты недоступны. Идти же по пути численного увеличения специалистов по работе с информацией – не самый лучший вариант.

Правы те, кто утверждает, что силы и время, потраченные на добывание и анализ масс данных, часто не стоят полученных результатов.

Пытаясь объять всё, вы рискуете упустить из виду то, что имеет ключевое значение для анализа. К примеру, вы тратите время на изучение недавно появившегося в сегменте рынка нового, но не самого опасного конкурента, в то время как другой, более крупный и серьезный игрок приступил к выпуску инновационного продукта. За всем и всеми усмотреть сложно. Без расстановки приоритетов вы рискуете потерять время на менее важных вещах, упустив более значимые для конкурентной борьбы события и тенденции.

Формирование системы приоритетов предполагает перенос фокуса внимания на следующие факторы:

Прямые конкуренты. То есть компании, предлагающие аналогичные вашим продукты и/или услуги для одной с вами клиентской аудитории.

Возникающие непосредственные угрозы. Это могут быть стартапы или уникальные инновационные предложения конкурентов.

Потенциальные угрозы. Например, компании, действующие на смежных рынках, но способные осуществить экспансию в ваш сегмент.

Конечно, важно держать в поле зрения всех конкурентов, но уделять им не одинаковое внимание. Профессионалы конкурентной разведки рекомендуют создать нечто вроде пирамиды, разместив на верхушке 2-3 наиболее сильных игроков, остальных разместить по бокам и внизу в зависимости от их веса и роли. При этом, замечают эксперты, ни в коем случае не игнорировать тех, кто занимает низший ряд. Время от времени, скажем, раз в месяц, проверять, продолжают ли они действовать как прежде: не поглощены, ничего нового не придумали, не демонстрируют намерения к расширению и выходу на другие рынки, и так далее…

Информационные перегрузки чреваты ложным представлением о прямой зависимости результатов от количества данных. Не стоит забывать, что сама по себе информация вне контекста или правильной интерпретации весьма обманчива, предвзята, отвлекает внимание на ложные тенденции.

Время и усилия, потраченные на поиск и обработку информации, украдены у более важной задачи – разработки и осуществления конкурентной стратегии. Отслеживание каждой рыночной метрики, каждого движения конкурентов неизбежно ведет к информационному перегоранию.

Чтобы этого избежать, следует начать с четкого определения вашей стратегии в работе с данными. На какие наиболее важные вопросы вы должны получить ответы? Вместо попытки мониторить всё и всех подряд, эксперты рекомендуют сосредоточить конкурентный анализ на трех вопросах конкурентной разведки: ценовая политика конкурентов, их тактика по удержанию клиентов, развитие ими своих продуктов/услуг.

Что такое Data LakeHouse

Data LakeHouse (**«**дом на озере данных») представляет собой гибридную архитектуру управления данными, которая в одном решении сочетает лучшие характеристики традиционных хранилищ данных (Data Warehouses) и «озер данных» (Data Lakes).

Разница между последними двумя репозиториями заключается в том, что хранилища содержат структурированные данные, а озера – неструктурированные данные в большом объеме из разных ресурсов и источников в сыром формате. Естественно, что работа с данными ведется в каждом из репозиториев отдельно.

Как указывает основатель Школы прикладного бизнес-анализа BABOK School Анна Вичугова, «отсутствие согласованности и изоляции, делало практически невозможным смешивание операций добавления и чтения, а также пакетных и потоковых заданий» ((www.eweek.com/big-data-and-analytics/data-lakehouse/). Что, конечно, создавало немалые трудности для специалиста по управлению данными.

Data LakeHouse, новая модель гибридной архитектуры, появившаяся несколько лет назад, устраняет этот недостаток, объединив в себе гибкость, масштабируемость и сравнительно низкую стоимость озер с требованиями ACID («Атомарность, Согласованность , Изолированность, Надежность»), обеспечивающими сохранность данных (в том числе и после транзакций).

Таким образом, впервые появилась возможность управления всеми данными на одной, общей платформе.

Амин Абдуллахи, автор книги и ряда статей по проблематике технологий B2B в финансовой сфере, называет области практического применения Data LakeHouse:

Аналитики данных используют Data LakeHouse для машинного обучения, бизнес-разведки, SQL аналитики (язык структурированных запросов), управления данными.

Аналитики бизнеса – для обработки и анализа данных из разных источников в целях бизнеса.

Менеджеры по продукту, маркетологи, управленческий персонал – для мониторинга ключевых индикаторов деятельности компании, для анализа рыночных тенденций (www.eweek.com/big-data-and-analytics/data-lakehouse/).

Анна Вичугова называет следующие особенности Data LakeHouse:

- *поддержка транзакций* — конвейеры данных способны одновременно считывать и записывать данные.
- *принудительное применение и управление схемой,* включая поддержку классических моделей Data Warehouse с обеспечением целостности и полноты данных, а также надежные механизмы управления и аудита.
- *совместимость с бизнес-разведкой* — Lakehouse позволяет использовать инструменты бизнес-аналитики непосредственно в исходных данных, повышая их актуальность, а также уменьшая задержку и затраты.
- *изоляция хранения от вычислений* по разным кластерам, что облегчает масштабирование для большего количества одновременных пользователей и объемов данных.
- *открытость стандартизованных форматов хранения данных*, которые предоставляют API (application programming interface, программный интерфейс приложений), поэтому различные инструменты и механизмы могут эффективно обращаться к данным напрямую.
- *многообразие различных типов данных.* Lakehouse можно использовать для хранения, уточнения, анализа и доступа к разным типам данных, включая изображения, видео, аудио, JSON-структуры и текст.
- *поддержка разнообразных рабочих нагрузок*, от алгоритмов машинного обучения до SQL-запросов и распределенных вычислений.
- *сквозная потоковая передача событий* в режиме реального времени.

«Переход к гибридной архитектуре позволил унифицировать источники данных, включая хранилища и озера, в масштабе всей организации, обеспечивая получение непротиворечивой отчетности и аналитики для разных бизнес-вертикалей», заключает Вичагова (там же).

Некоторые эксперты находят не только преимущества, но и недостатки гибридной архитектуры Lakehouse. На них указывает блог пост на сайте hashdork.com/ru:

- *Монолитная конструкция* часто приводит к ухудшению обслуживания всех пользователей, может быть жесткой и сложной в обслуживании. Как правило, архитекторам и дизайнерам нравится более модульная архитектура, которую они могут настраивать для различных вариантов использования.
- *Технология еще не совсем там.* Конечная цель влечет за собой значительный объем машинного обучения и искусственного интеллекта. Прежде чем домики у озера смогут работать так, как предполагается, эти технологии должны развиваться дальше.
- *Незначительный прогресс по сравнению с существующими структурами.* До сих пор существует значительный скептицизм в отношении того, насколько большую ценность на самом деле принесут домики у озера. Некоторые недоброжелатели утверждают, что конструкция «озеро-склад» в сочетании с соответствующим автоматизированным оборудованием может обеспечить сопоставимую эффективность.

Безымянный автор (или авторы?) данной публикации считает, что метод «дома на озере данных» трудно внедрить из-за сложности составляющих его частей. Кроме того, из-за растущего внедрения озер данных предприятиям придется перемещать в них свои текущие хранилища данных, полагаясь только на обещание успеха без заведомо очевидной экономической выгоды.

Как изучать маркетинговую стратегию конкурентов

Эксперты Unrover, компании конкурентной разведки, широко использующей технологии искусственного интеллекта, опубликовали на своем сайте unkover.com краткое руководство по изучению маркетинговой стратегии конкурентов. Оно содержит 10 разделов.

1. Анализ содержания и стратегии продвижения веб-сайтов конкурентов

Собственно, с изучения веб-сайтов и должен начинаться анализ стратегии конкурентов. Какие формы контента превалируют – блоги, видематериалы, инфографика, кейсы? Старайтесь выделить специфические темы, узкие места, ключевые слова, свидетельствующие о приоритетах в продвижении сайта. Как используются внутренние ссылки и линки, мета-описания (теги, описывающие содержание страницы). Полученная информация позволит уяснить, как конкуренты привлекают и удерживают аудиторию.

2. Мониторинг активности в социальных сетях

Начните с платформ, где конкуренты особенно активны. Обращайте внимание на частоту появления и виды контента (тексты, видео, картинки), как позиционируют свой бренд. Не менее важно отслеживать, как реагирует аудитория: лайки, комментарии, участие в обсуждениях.

3. Платные рекламные кампании

Какие платформы предпочитают для своей рекламы. Каков формат реклам. На чем делают акцент – на ценовых скидках, акциях, бесплатном опробовании или на чём-то другом. Это позволит лучше понимать целевую аудиторию.

4. Позиционирование и рекламное обращение продукта/услуги

Каковы тон, язык рекламы, подчеркиваемые характеристики продуктов. На чём упирают – на качестве, доступности, эксклюзивности, инновационности. Как выделяют и отличают свою продукцию от конкурентной. Внимательный анализ рекламного обращения позволяет выявить как сильные, так и слабые стороны кампании.

5. Участие конкурентов в отраслевых выставках и мероприятиях, включая вебинары

Следите, как они презентуют свои продукты/услуги настоящим и потенциальным клиентам. Особое внимание – темам выступлений, выбору спикеров, стилю участия в мероприятиях.

6. Партнерства и коллаборация

Изучение данного аспекта поможет лучше определить цели конкурентного бизнеса, его авторитет и имидж на рынке. Отдельного внимания заслуживают задачи совместных с другими фирмами рекламных кампаний: выпуск нового продукта, совместное продвижение, или экспансия в социальных сетях?

7. Обратная связь: отклики и комментарии клиентов

Как пользователи оценивают их продукты, услуги, бренды. Анализируйте как позитивные, так и негативные мнения. Так легче понять, где сильные, а где слабые стороны. Не менее важно отслеживать реакцию конкурентов на жалобы со стороны покупателей/клиентов. Активно взаимодействуют, предлагают решение проблем, улучшают качество продуктов/услуг?

8. Email-маркетинг

Email-маркетинг или продвижение бренда и работа с клиентами через электронные почтовые рассылки входит в базовый инструментарий интернет-маркетологов. Начните с подписки на рассылки. Они периодичны или рассылаются только в рамках рекламных разовых кампаний? Внимание контенту: выпуск нового продукта, образовательная цель, или предложения по скидкам? Каков дизайн, стиль, язык, тон email сообщений? Их визуальное оформление?

9. Метрики рекламного трафика

Частота и средняя продолжительность рекламных сообщений, показатель «ненужных просмотров» (после перехода по рекламной ссылке страница закрывается пользователем), географическое расположение аудитории, наиболее и наименее посещаемые страницы. Эти и другие подобные метрики требуют привлечения высоко технологичных инструментов поиска и анализа.

10. Контент-анализ маркетинговой стратегии

Контент-анализу подвергаются блог посты, видеоматериалы, практические кейсы, электронные издания, подкасты. Важно фиксировать, как часто, периодично или нет, появляется новый контент. Все это надо делать, чтобы понять ключевые темы, которые конкуренты адресуют

аудитории. Важно обращать внимание и на явные белые пятна контента, которые вы можете заполнить уже собственными материалами.

Наиболее распространенные ошибки конкурентного анализа

При изучении рыночной, конкурентной среды ошибки практически неизбежны. Некоторые обнаруживаются и исправляются быстро. Другие, малозаметные, раз за разом повторяются, искажая реальную картину конкуренции, затрудняя выбор правильной, адекватной рыночной стратегии. Эксперты компании Octopus, специализирующейся в области маркетинга и конкурентной разведки, выделили наиболее часто повторяющиеся заблуждения и просчеты в конкурентном анализе.

Чрезмерное внимание поверхностным показателям и параметрам

Нередко аналитики придают незаслуженно большое значение легко доступным, лежащим на поверхности данным об изменениях и тенденциях. К примеру, конкурент выпустил продукт с новыми характеристиками. О чем это говорит? Возможно, о том, что он опережает вас в инновациях. Или о том, что стремится занять лидирующую позицию в рыночном сегменте. Такие выводы сделать нетрудно. Но они могут быть и ошибочными, если вы не поставите и не проработаете достаточно глубоко следующие вопросы:

- Какова настоящая задача новой характеристики конкурентного продукта/услуги?
- Стремится ли конкурент выделиться от других игроков?
- Или хочет усилить лояльность клиентов?
- Или все дело в давлении со стороны инвесторов и акционеров?

Не доверяйте внешним измерениям, старайтесь выявить действительные, не всегда видимые намерения конкурентов.

Пропуск ранних сигналов

Если вы ждете, когда зарождающиеся сдвиги и тенденции станут очевидными, неоспоримыми, то велик риск проиграть конкуренцию. Даже малейшие изменения могут указывать на начало стратегических подвижек. Важными, достойными внимания сигналами могут быть:

- Размещение конкурентом объявлений о вакансиях в новом регионе или с новыми должностными функциями
- Патентная заявка
- Технологическое партнерство
- Изменения в контексте, языке, стиле корпоративного веб-сайта и рекламы

Такие, на первый взгляд, несущественные моменты могут сигнализировать о важных изменениях.

Уверенность, что конкуренты действуют рационально и прагматично

Нельзя исходить из предположения, что другие игроки всегда принимают рациональные, взвешенные решения. В реальности часто происходит наоборот. В конце концов, людям

свойственно ошибаться, их решения далеко не всегда логичны и закономерны. Ошибки и просчеты могут проистекать вследствие таких факторов как:

- Внутренние политики
- Чрезмерная самоуверенность
- Давление со стороны акционеров

Неспособность различать первичные и вторичные факторы

При изучении рыночной динамики в глаза бросаются изменения, обещающие прямое и немедленное воздействия на процессы. Это, к примеру, выпуск конкурентом нового продукта/услуги, движение в ценах, новое партнерство и так далее. Все эти моменты важно рассматривать и анализировать не в изоляции друг от друга, но в контексте с другими факторами, системно. Каждое конкурентное движение вызывает круги на поверхности. И здесь следует разобраться, какое влияние оно оказывает на рынок – краткосрочное, среднесрочное, долгосрочное. Даже легкая зыбь может предвещать серьезное волнение в скором будущем.

Чрезмерная уверенность в собственной правоте

Не дайте самоуверенности взять верх надо собой. Постоянно подвергайте сомнению свои суждения и заключения. По отношению к себе примите роль адвоката дьявола. Терзайте себя вопросом «а вдруг я ошибаюсь?».

Слишком острое, горячее реагирование на действия конкурентов

Конкурент принял смелое решение. Это может быть новая мощная рекламная кампания. Или его появление на новом рынке. Первая реакция на это – желание немедленно реагировать, действовать. Однако, надо помнить, что далеко не каждое движение в конкурентной среде требует реагирования. Иногда наилучшее решение – вообще ничего не делать. К примеру, конкурент снизил цены. Не спешите с ответом. Может быть, он это сделал без серьезной проработки, а как отчаянную попытку удержать клиентов. В этом случае было бы ошибкой начинать с ним ценовую войну. Так что прежде чем реагировать на изменения, тщательно проанализируйте их причины и возможные последствия

Игнорирование или недооценка предпочтений и ожиданий клиентов

Чрезмерная концентрация аналитической работы на конкурентах может ослабить внимание на клиентах. Поэтому каждый шаг со стороны конкурентов необходимо рассматривать и изучать через призму борьбы за клиентов. В конце концов, именно они определяют ваш успех (или неуспех) в конкурентной борьбе.

Поведенческий анализ в разведке киберугроз

По определению Лаборатории Касперского система поведенческого анализа User and Entity Behavior Analytics (UEBA) анализирует поведение пользователей и сущностей (устройств, аккаунтов, процессов) для выявления аномалий и угроз, невидимых для традиционных систем защиты, таких как антивирусы и SIEM (Security Information and Event Management).

Сегодня UEBA — это неотъемлемая часть кибербезопасности. Она помогает организациям отслеживать изменения в поведении пользователей, устройств, учетных записей и обнаруживать такие угрозы, как утечки данных, мошенничество, атаки на внутренние ресурсы, компрометация учетных записей и др. (подробнее см. https://www.securitylab.ru/blog/personal/paragraph/354252.php?ysclid=m77hutduzf670048999).

Концепция обнаружения аномалий в сфере кибербезопасности была предложена еще в 1987 году математиком Дороти Деннинг в ее статье «Модель обнаружения несанкционированных вторжений» (https://ieeexplore.ieee.org/document/1702202/authors#authors).

«Обнаружение аномалий это Священный Грааль для кибербезопасности», говорит Брюс Поттер, основатель и руководитель аудиторской компании Turngate. Если вы все делаете правильно, то вам не обязательно априори знать об угрозах, которые вы ищете. Они сами заявят о себе, поскольку выглядят как «чужие», не так, как должны выглядеть нормальные вещи (онлайн издание CSO, 14 Feb 2025).

Аномалии представляют собой отклонения от обычной, нормальной, рутинной активности в сети или компьютерной системе, как, например, неожиданной скачок трафика, или необычно высокая активность в сервере, или нетипичный всплеск активности с IP адресов. Мэтт Шрайнер, Партнер IBM Consulting , считает правильным ассоциировать любые аномалии с возможными угрозами, но «не все аномалии заведомо плохи». Некоторые из них могут раскрывать возможности для оптимизации архитектуры или совершенствования бизнес стратегии, например, путем адаптации к сезонным изменениям в движении железнодорожного транспорта.

Среди наиболее значимых инструментов отлавливания аномалий эксперты называют:

Endpoint Detection & Response (EDR). Задача EDR - непрерывно отслеживать данные об угрозах на рабочих станциях и других конечных устройствах, выявлять бреши в защите в режиме реального времени и оперативно реагировать на потенциальные угрозы.

Межсетевой экран (firewall) предназначен для проверки и фильтрации сетевого трафика.

Security Information and Event Management (SIEM) – класс программных продуктов по управлению событиями и информацией о безопасности.

В принципе совокупность инструментов и методов обнаружения аномалий можно разделить на две части, полагает Поттер. Одна находит уже известные нам угрозы, другая показывает вещи, которые могут быть опасными. Известные угрозы – своего рода база сигнатур, опираясь на которую мы можем твердо сказать о замеченном нами явлении: это угроза. Большинство хакеров не занимаются изобретением колеса, стараясь не напрягаться для достижения своей цели, подчеркивает эксперт. Они предпочитают повторять один и тот же трюк 100 раз подряд. И если в 10 случаев у них получается, то это уже неплохой результат. О хорошо известных угрозах обычно сигнализируют основные инструменты кибербезопасности, например, межсетевые экраны. Но наиболее эффективными, по мнению Поттера, проявляют себя системы EDR.

Другой специалист, Эндрю Круг из компании DataDog (сервис наблюдения для облачных приложений) указывает на SIEM как на главный инструмент мониторинга аномалий в его компании: «Если у вас нет этого продукта, то вы можете «проворонить» нечто нехорошее».

Но и самые продвинутые технологии не могут на все 100% гарантировать защиту от атак, тем более уникальных, изощренных, не типичных. Компьютеры сложно натренировать на классификацию и определение любых аномалий. И здесь могут выручить интуиция, проницательность оператора в центре мониторинга информационной безопасности. Именно

человек, специалист, получив сигнал о некой аномалии, должен разобраться и сказать: да, это дурной знак. Работа в таком центре – одна из самых тяжелых, трудоемких. Сидящие за экранами мониторинга завалены сигналами и подчас не успевают разобраться, какие из них ложные, какие реальные.

Некоторые специалисты предупреждают не возлагать слишком больших ожиданий на человеческие способности. Эмилио Эскобар, руководитель информационной защиты в Datadog (американская компания, предоставляющая сервис наблюдаемости для облачных приложений), утверждает: «На фоне быстро меняющегося ландшафта угроз в сочетании с усложняющейся IT архитектурой мы, полагаясь на свои глаза и мозги, просто суждены играть с противником в кошки-мышки, следуя за ним по пятам, но не рядом и не впереди» (там же).

Проблема в том, что в прокрустово ложе сигнатур обнаружения типичных аномалий невозможно вогнать все аномалии, в том числе связанные с внутрикорпоративным инсайдерством, эксфильтрацией данных, скомпрометированными учетными данными, техникой «malware beaconing» (с помощью которой вредоносное ПО устанавливает скрытный канал связи между заражёнными системами и злоумышленниками).

Поэтому эксперты призывают брать на вооружение модели «bespoke anomaly detection» — индивидуальное решение для обнаружения аномалий**,** разработанное с учётом конкретных потребностей и задач каждой компании. Такое решение позволяет компаниям добавлять возможности обнаружения аномалий в собственные продукты и услуги.

Рецензия
Financial Intelligence for IT Professionals: What You Really Need to Know About the Numbers
by Karen Berman, Joe Knight, John Case

Монография представляет собой руководство по базовым вопросам финансовой разведки специально для IT-специалистов. Авторы не только объясняют основы финансового менеджмента, но предоставляют возможность попрактиковаться на конкретных примерах, иллюстрирующих получаемые во время чтения знания.

В книге подробно излагаются и характеризуются фундаментальные проблемы финансового менеджмента применительно к IT-специальности. В том числе:

- О чем говорят финансовые документы компании, такие как отчет о доходах и расходах, баланс счетов
- Как движутся денежные средства
- Как использовать коэффициенты и показатели для оценки финансового здоровья организации
- Как считывать рентабельность инвестиций в IT
- Как использовать финансовую информацию в целях улучшения эффективности работы службы IT и в целом бизнеса компании
- Как организовать и вести финансовую разведку силами айтишников в рамках их служебных обязанностей