УДК 004.451.5
DOI: 10.36979/1694-500X-2026-26-8-24-32

ТЕХНОЛОГИЧЕСКИЕ СИСТЕМЫ ИНТЕГРАЦИИ ДАННЫХ (НА ПРИМЕРЕ PALANTIR TECHNOLOGIES): АНАЛИЗ ВОЗМОЖНОСТЕЙ И РИСКОВ ВНЕМЕДИЙНОЙ СЕНСАЦИОНАЛИЗАЦИИ

А.И. Евтушенко

Аннотация. Рассматриваются технологические возможности, ограничения и риски современных систем интеграции и аналитической обработки разнородных данных на примере платформ класса Palantir. Анализируются основные элементы их архитектуры, включая интеграцию данных, онтологическое и графовое представление, машинное обучение и поддержку принятия решений. Особое внимание уделяется эффекту эмерджентности интегрированных данных, позволяющему получать новое знание посредством объединения разрозненных информационных массивов. Рассматриваются технологические ограничения, риски профилирования, концентрации информационной власти и автоматизации решений. Показано различие между реальными возможностями интеграционных платформ и их медийным образом «цифрового всеведения», сформулированы основные условия их ответственного применения.

Ключевые слова: интеграция данных; Palantir; большие данные; онтология; графовый анализ; машинное обучение; искусственный интеллект; поддержка принятия решений; информационная безопасность; профилирование; аудит данных; human-in-the-loop.

МААЛЫМАТТАРДЫ ИНТЕГРАЦИЯЛООНУН ТЕХНОЛОГИЯЛЫК СИСТЕМАЛАРЫ (PALANTIR TECHNOLOGIES МИСАЛЫНДА): МЕДИА СЕНСАЦИЯДАН ТЫШКАРКЫ МҮМКҮНЧҮЛҮКТӨРДҮ ЖАНА ТОБОКЕЛДИКТЕРДИ ТАЛДОО

А.И. Евтушенко

Аннотация. Макалада Palantir тибиндеги платформалардын мисалында ар тектүү маалыматтарды интеграциялоонун жана аналитикалык иштеп чыгуунун заманбап системаларынын технологиялык мүмкүнчүлүктөрү, чектөөлөрү жана тобокелдиктери каралат. Алардын архитектурасынын негизги элементтери, анын ичинде маалыматтарды интеграциялоо, онтологиялык жана графтык чагылдыруу, машиналык үйрөтүү жана чечим кабыл алууну колдоо талданат. Маалыматтардын ар башка массивдерин бириктирүү аркылуу жаңы билимдерди алууга мүмкүндүк берген интеграцияланган маалыматтардын жаңы сапаттык касиеттердин пайда болуу эффектисине өзгөчө көңүл бурулат. Технологиялык чектөөлөр, мүнөздөмө түзүү, маалыматтык бийликтин топтолушу жана чечимдерди автоматташтыруу тобокелдиктери каралат. Интеграциялык платформалардын реалдуу мүмкүнчүлүктөрү менен алардын медиадагы «санариптик бардыгын билүүчүлүк» образынын ортосундагы айырмачылык көрсөтүлүп, аларды жоопкерчиликтүү колдонуунун негизги шарттары иштелип чыккан.

Түйүндүү сөздөр: маалыматтарды интеграциялоо; Palantir; чоң маалыматтар; онтология; графтык талдоо; машиналык үйрөтүү; жасалма интеллект; чечим кабыл алууну колдоо; маалыматтык коопсуздук; профилдөө; маалыматтардын аудити; human-in-the-loop.

DATA INTEGRATION TECHNOLOGY SYSTEMS (THE CASE OF PALANTIR TECHNOLOGIES): AN ANALYSIS OF CAPABILITIES AND RISKS BEYOND MEDIA SENSATIONALISM

A.I. Evtushenko

Abstract. The article examines the technological capabilities, limitations, and risks of modern heterogeneous data integration and analytics systems, using Palantir-class platforms as a representative example. It analyzes key architectural elements, including data integration, ontological and graph-based representation, machine learning, and decision support. Particular attention is paid to the emergent effect of integrated data, which enables the generation of new knowledge by combining disparate information arrays. The article discusses technological limitations and the risks of profiling, concentration of informational power, and automated decision-making. It distinguishes the actual capabilities of integration platforms from the media image of «digital omniscience» and outlines key requirements for their responsible use.

Keywords: data integration; Palantir; big data; ontology; graph analytics; machine learning; artificial intelligence; decision support; information security; profiling; data auditing; human-in-the-loop.

Введение. Быстрый рост объемов разнородных данных показал недостаточность традиционных способов их анализа. Как следствие, появились платформы, объединяющие данные из разных источников и позволяющие анализировать не только отдельные записи, а извлекать из них связи между сущностями (например: люди, организации, устройства, счета и др.) и событиями. Наиболее известным представителем этого класса систем стала Palantir Technologies. Упоминание этой компании все чаще можно встретить в современных средствах массовой информации. Ее описывают как мощную и одновременно спорную платформу для анализа больших данных и ИИ. СМИ называют ее «всевидящим оком» из-за тесного сотрудничества компании со спецслужбами, армией и полицией разных стран, что вызывает постоянные споры между сторонниками технологической безопасности и защитниками прав человека.

Цель данной статьи – рассмотреть технологическую архитектуру и принципиальные возможности систем класса Palantir, а также связанные с этим ограничения и риски, отделив их от медийных преувеличений.

Архитектура Palantir: от интеграции разнородных данных к операционной модели предметной области.

Интеграция гетерогенных источников – базы данных (SQL, NoSQL), распределенные хранилища (Hadoop, S3/подобные), сенсоры (дроны, спутники), документы, PDF, видео/изображения, логи систем, иногда – потоковые данные (streaming). Palantir подключает их через коннекторы и в зависимости от источников и сценариев данные могут загружаться напрямую в платформу, а могут синхронизироваться с внешними системами через шлюзы и/или использоваться без полной централизации. Принципиальным является то, что над физическим уровнем хранения формируется единое логическое представление данных. При этом данные объединяются с сохранением их контекста и истории происхождения (data lineage) [1].

Очистка и нормализация данных. Очистка (data cleaning) заключается в обнаружении и исправлении ошибок, пропусков, дубликатов и противоречий в исходных данных. Подход Palantir заключается в том, чтобы не чистить данные «до идеала», а работать с неопределенностью как частью модели. Каждому факту сопоставляются степень доверия, источник, время. Система учитывает, что данные могут быть неравны по качеству достоверности. В работе с противоречиями Palantir может хранить несколько конкурирующих версий с указанием источников, что важно для разведки – истина может быть неочевидной. В итоге Palantir работает с вероятностной моделью мира, превращая «грязность» в управляемую характеристику системы.

Нормализация состоит в приведении различных представлений данных одного типа к общему стандарту. Здесь используются справочники, классификаторы и mapping rules – правила соответствия между схемами различных источников [1].

Entity resolution (сведение сущностей) – установление того, что записи из разных источников относятся к одному объекту. Могут использоваться совпадения атрибутов, вероятностные модели, графовые связи. Объединение записей сопровождается оценкой вероятности совпадений.

Онтологическая модель. На основе предыдущих этапов формируется онтологический слой, представляющий данные в терминах сущностей предметной области и связей между ними. В онтологии задаются типы объектов: человек, счет, устройство, IP-адрес, организация, транзакция и так далее, и определяется, какие отношения между ними допустимы.

Визуальная аналитика, графовое представление связей. Принципиальное отличие Palantir от традиционных СУБД состоит в том, что поверх табличных и иных представлений данных создается граф объектов и отношений, что позволяет получить семантическую модель реальности. Аналитик работает не с записями и таблицами, а с объектами и сценариями, где граф является узлом управления.

Временной и пространственный анализ. Временной анализ (temporal analysis) – система фиксирует последовательности событий, интервалы, динамику объектов, изменение связей во времени.

Пространственный анализ (geospatial analysis) – системой отслеживаются координаты объектов, их маршруты, зоны, пространственные отношения и перемещения.

Машинное обучение (ML, LLM/AI интерфейсы). Наряду с традиционной аналитикой – статистикой, графовыми алгоритмами, оптимизацией, поиском аномалий – в платформу можно встраивать и современные модели на основе машинного обучения – модели прогнозирования, классификации, оценки рисков, автоматического выявления паттернов. Причем эти модели могут быть как нейросетевые, так и не нейросетевые. Можно подключать и генеративный ИИ/LLM (GPT, Claude, Gemini) – нейросетевой слой для работы с естественным языком, документацией, запросами к данным, агентными сценариями. И здесь можно провести границу: Palantir-подобная система не является одной гигантской нейросетью, которая «знает всё». Её сила возникает прежде всего из интеграции большого объема разнородных данных и возможности выявлять неочевидные закономерности и связи.

Операционный слой и поддержка принятия решений. Palantir не просто показывает данные, а позволяет действовать через систему: запустить расследование, изменить логистическую цепочку, отправить команду в поле, задать автоматическое правило.

Сквозное управление доступом к интегрированным данным. Платформа объединяет данные с разными исходными режимами доступа. При этом права должны сохраняться после преобразования данных и при представлении их в онтологии. Palantir поддерживает ограничения на уровне объектов/строк, свойств/столбцов и их комбинации вплоть до отдельных ячеек. Если главное преимущество Palantir-подобных систем состоит в снятии информационных барьеров между разрозненными источниками, то одна из главных технических задач состоит в том, чтобы интеграция данных не означала автоматического снятия законных барьеров доступа к ним [1, 2].

Ключевые возможности систем класса Palantir. Их можно разделить на четыре уровня:

Первый – интеграционный. Позволяет собирать сведения об одном объекте, распределённые между десятками информационных систем.

Второй – аналитический. Это способность обнаруживать закономерности, аномалии, группы и цепочки связей, которые трудно увидеть при раздельном анализе баз данных.

Третий – прогностический. Этот уровень говорит об умении системы рассчитывать риски и вероятности мошенничества, отказа оборудования, дефицита ресурсов, определённого поведения объекта и т. д.

Четвёртый – управленческий уровень – позволяет использовать результаты анализа непосредственно в процессе принятия решений.

Продукты компании Palantir Technologies (платформы Gotham, Foundry и Apollo, а также ИИ-платформа AIP) успешно применяются в таких сферах, как государственная безопасность, военное дело, крупный бизнес, медицина и гуманитарные проекты.

Оборона и разведка (Palantir Gotham).

Военная аналитика: создание единых карт поля боя, интеграция данных с дронов, спутников и радиоперехватов.

Оптимизация ударов: планирование и расчет логистики боевых операций

Спецслужбы и правопорядок: борьба с терроризмом прогнозирование преступлений и расследования для ЦРУ, ФБР и полиции [3].

Коммерческий сектор и промышленность (Palantir Foundry).

Финансовый мониторинг: выявление мошенничества и анализ рисков в крупных банках (например, JP Morgan Chase).

Производство и логистика: управление цепочками поставок на заводах автомобильных и авиационных компаний.

Энергетика: прогнозирование нагрузок на энергосистемы, поиск слабых мест и защита инфраструктуры.

Здравоохранение и гуманитарная сфера.

Медицина: анализ больничных данных, оптимизация распределения ресурсов и вакцин. Palantir Foundry успешно использовалась для отслеживания вакцинации в период пандемии COVID-19.

Разминирование: обработка исторических данных о боевых действиях и типах почв для безопасной очистки территорий.

Эффект «цифрового всеведения». Впечатление «всевидящего ока» возникает не потому, что система обладает какими-то фантастическими данными, но благодаря объединению обычных данных, образуется принципиально новое качество в понимании происходящих событий. Например, сами по себе:

- банковский счёт;
- IP-адрес, устройство, геолокация;
- событие входа, банковская транзакция;
- дают сравнительно мало информации.

Но цепочка «пользователь → устройство → IP → событие входа → счёт → транзакция → другой счёт → другое устройство», позволяет реконструировать значительно больше и может способствовать выявлению мошеннических схем.

Здесь стоит ввести понятие эмерджентности интегрированных данных: совокупность данных оказывается существенно информативнее простой суммы отдельных источников. Главный технологический эффект систем класса Palantir состоит не просто в накоплении большого количества данных, а в появлении нового знания вследствие их интеграции, контекстуализации и установления связей.

Именно это часто воспринимается на публичном уровне как существование некого «всевидящего ока» [3].

Принципиальные технологические ограничения. Система знает не реальность, а то, что может быть смоделировано из доступных системе данных.

Отсюда вытекают ограничения:

- ***Неполнота данных.*** Этот фактор связан с тем, что разные ведомства не хотят делиться данными, существуют разные стандарты и интересы, а также юридические ограничения. В итоге система получает неполную картину и «слепые зоны» становятся структурными.
- ***Ошибки исходных источников – «грязные данные».*** Подход «работаем с неопределённостью» не снимает фундаментальной проблемы: при высокой доле шума граф начинает «связывать всё со всем» и система теряет различимость структур.
- ***Устаревшие данные*** – мир меняется быстрее модели. Онтология и связи требуют настройки и обновляются не мгновенно. Если среда высокодинамична (конфликты, рынки, социальные процессы), то модель **запаздывает**, активными остаются вчерашние связи – система просчитывает «вчерашний день».

- ***Ошибочное сопоставление сущностей.*** Любая онтология – это выбор категорий и отношений. Отсюда возможен риск онтологической предвзятости (как назвали сущности и связи, так система и «видит» мир). Сложные явления (мотивы, намерения, культурные смыслы) редуцируются к суррогатам, и система теряет точность там, где смысл не сводится к наблюдаемым признакам. В итоге качество решений ограничено качеством выбранной онтологии, а не только данными или алгоритмами.
- ***Вычислительный предел: комбинаторный взрыв.*** Такие операции на графах как поиск путей, анализ центральности, многослойные зависимости, являются вычислительно трудоёмкими. Как следствие, приходится вводить эвристики и отсечения**,** анализ становится приближённым, «полная картина» заменяется локальной проекцией**.** Система неизбежно «не видит всё», даже если данные есть.
- ***Ложные корреляции.*** Palantir умеет хорошо работать с корреляциями, паттернами, ассоциациями. Но причинность (почему это происходит) не всегда является прямым следствием корреляции. Типичная ошибка – «связано» → «значит влияет» → «значит нужно действовать». Это системный риск для любых decision-driven (основанных на решениях) платформ.
- ***Проблема интерпретируемости моделей – человек не успевает за системой.*** В Palantir реализован принцип human-in-the-loop («человек в контуре») – интерактивное взаимодействие с системой. И в этом случае объём сигналов может превышать когнитивные возможности оператора. Как следствие, возникает automation bias (склонность доверять системе). Решения принимаются по «рекомендациям», а не по пониманию.
- ***Предел глубины и значимости смысла.*** Есть такие сущности в нашем мире, которые принципиально плохо формализуются. Это – мотивации людей, культурные контексты, религиозные и экзистенциальные решения. Здесь нет устойчивых признаков и стабильных связей, нет воспроизводимых паттернов, т. е. существует область реальности, где системы, подобные Palantir, не просто ошибаются, а методологически неприменимы**.**

Риски, специфичные для систем класса Palantir. Интеграция больших объемов данных приводит к рискам, связанным с концентрацией информационной власти. Разрозненные базы данных ограничивают возможности наблюдения естественным образом. Их объединение снимает эти ограничения. Отсюда:

- ***Возможность масштабного профилирования.*** Интеграция разрозненных массивов информации позволяет строить детальные цифровые портреты людей, предсказывать их поведение, решения и скрытые особенности без их ведома и согласия. Сбор данных из соцсетей, геолокаций и покупок раскрывает интимные стороны жизни человека, что является непосредственной угрозой приватности нашей жизни. Люди теряют контроль над тем, как их воспринимают государственные системы и организации.
- ***Вторичное использование данных вне первоначальной цели их сбора.*** Точечное таргетирование влияет на политические выборы и потребительские привычки через персонализированную рекламу и пропаганду.
- ***Автоматизированная категоризация людей.*** Приводит к возможности политического или административного злоупотребления. Алгоритмы могут отказывать в кредитах, работе или страховании на основе предвзятых или скрытых профилей.
- ***Утечка безопасности.*** Накопление огромных баз данных делает их лакомой целью для хакеров, что ставит под угрозу сохранность личных данных.
- ***Зависимость принимающего решение человека от рекомендаций системы – automation bias.*** Получается парадокс – система создана для усиления человека, но может вытеснять его из реального анализа**.**

Можно сделать следующий вывод: опасность таких платформ определяется не только тем, какие данные государство или организация собирает, но и тем, какие новые знания становятся возможными после их объединения [3].

Медийный образ Palantir: мифы и реальность.

«Palantir следит за всеми и знает всё о человеке». Тезис СМИ о том, что система Palantir лично следит за всеми, является медийным преувеличением, так как компания не собирает персональные данные самостоятельно, а выступает только разработчиком софта для их анализа. Программное обеспечение компании объединяет разрозненные архивы и базы данных, которые спецслужбы, полиция или корпорации уже имеют на руках, а не является самостоятельным источником глобальной слежки. Платформы вроде Palantir Gotham или Foundry – это инструменты-агрегаторы. Они связывают воедино банковские транзакции, телефонные биллинги, камеры, соцсети и госархивы заказчика.

За слежку отвечают конкретные ведомства, например, полиция или разведка, которые покупают софт и загружают туда свои легальные или собранные оперативные материалы. Сама компания не владеет сервером, где хранится досье на каждого человека в мире и не использует базы данных в личных целях.

Почему возник этот миф? Название компании взято из «Властелина колец» – всевидящие камни Палантиры, а ее руководство активно поддерживает ореол технологической мистики и всемогущества. Продукты компании действительно использовались американскими миграционными службами и полицией для громких расследований и депортаций, что вызывало этические вопросы о приватности. Работа с Пентагоном и разведкой создает образ «цифрового Большого брата», который контролирует всё происходящее на поле боя или в городах [4].

«ИИ сам выбирает цели и алгоритм принимает решение вместо человека». Алгоритмы Palantir Technologies не принимают самостоятельных решений, так как программное обеспечение компании спроектировано по принципу второго пилота – copilot, или системы поддержки принятия решений, где окончательное решение, юридическая и моральная ответственность остаются за человеком.

Как складывается миф об автономном разуме? Из-за работы с армией, разведкой и крупными госструктурами деятельность компании часто обрастает конспирологическими слухами о создании цифрового авторитарного мозга или терминаторов [5, 6] Внедрение передовых языковых моделей и AI-агентов через Palantir AIP создает иллюзию того, что система действует сама, хотя она лишь генерирует сценарии и варианты действий.

Human-in-the-loop – архитектура платформ технически и логически завязана на обязательные шлюзы человеческого контроля. Алгоритм может составить карту угроз, предложить логистический маршрут или выделить аномалию, но запуск критического, тем более силового процесса требует подтверждения оператором. Продукты компании работают на базе Palantir Ontology – модели реального мира, которая связывает разрозненные данные в понятные объекты: люди, счета, техника. Она структурирует хаос для аналитиков, ускоряя его работу, но не заменяет суждение.

В собственной этической и технической документации Palantir по ИИ-этике подчеркивается, что алгоритмы – это лишь математические и статистические формализмы, не способные обладать пониманием или выносить моральные суждения.

Противоположный миф – «это всего лишь красивая визуализация обычных баз данных». Palantir – это не просто визуализация баз данных, а полноценная операционная система для интеграции, моделирования и принятия решений на уровне крупных корпораций и спецслужб. Платформы класса Palantir не заменяют базы данных или хранилища, а надстраиваются поверх них, превращая хаос из разрозненных таблиц в единую смысловую структуру. Программа не просто рисует графы. Она строит цифровой двойник бизнеса или организации, связывая абстрактные строки в базах данных с реальными объектами: клиент, самолет, банковский перевод, детали на заводе и событиями между ними.

Обычные BI-системы визуализации только читают данные и показывают графики. Palantir позволяет операторам совершать действия прямо из интерфейса, например, изменить логистический маршрут или подтвердить закупку, и эти решения записываются обратно в исходные транзакционные системы. Система управляет потоками данных, сохраняя контекст безопасности и контроля доступа на всех этапах трансформации от сырого файла до готового решения на базе искусственного интеллекта.

Внутри платформы работают мощные движки обработки данных, например Apache Spark, которые автоматизируют сложные инженерные процессы и экономят недели ручной работы по сведению отчетов [1].

Где проходит реальная граница опасности. Рассмотрим, что говорят о системе Palantir сами ее создатели.

Политическую линию компании представляет ее основатель, американский предприниматель и технологический инвестор Питер Тилль. Он исходит из идеи, что Запад теряет способность к координации и действию. По мнению Тилля, проблема состоит в том, что данных становится слишком много, понимания слишком мало, и решения принимаются слишком медленно. Поэтому необходимо создать систему, которая восстановит зрение государству.

Алекс Карп – сооснователь и генеральный директор компании – философ по образованию. Его позиция состоит в том, что технологии не бывают нейтральными – они усиливают либо либеральные демократии, либо их противников. Мир становится алгоритмическим полем боя, где ключевым фактором является скорость принятия решений – выигрывает тот, кто быстрее интерпретирует данные.

Главная идея основателей Palantir – миром будут управлять те, кто лучше структурирует его сложную реальность.

Почему это воспринимается как опасность?

Система дает превосходство в знании – управляет тот, кто больше видит.

Централизация знаний усиливает возможности контроля. Поведение любого человека можно анализировать, предсказывать и направлять.

Palantir – это не просто технология, это попытка решить фундаментальную проблему управления сложным миром через тотальную структуризацию данных и ускорение принятия решений [2–4].

Реальная опасность состоит в том, что одна и та же технологическая архитектура может использоваться как для обнаружения мошенничества, оптимизации производства, поиска преступников так и для политического контроля. Опасность находится не в алгоритме, а в способах его применения.

Можно предложить такую модель расчета риска – «технологические возможности × объём доступных данных × полномочия оператора × непрозрачность применения».

Условия ответственного применения. В предыдущих разделах были рассмотрены технологические аспекты системы Palantir и дана некоторая диагностика ее возможностей и связанных с ними рисков. Далее логично перейти к требованиям ответственного применения интеграционных платформ подобного класса.

Принципы работы с данными.

- ***Минимизация данных.*** Означает сбор и обработку ровно того объема информации, который необходим для выполнения конкретной аналитической или операционной задачи без избыточного накопления. Доступ к сырым и агрегированным данным жестко ограничивается на уровне ролей и контекста конкретного расследования или бизнес-задачи. Личные данные скрываются, хешируются или заменяются псевдонимами до момента, пока у аналитика не появятся подтвержденные полномочия на деанонимизацию.
- ***Целевое назначение данных.*** Принцип ограничения целей требует, чтобы персональные данные собирались только для конкретных, явно выраженных и законных целей. Цель сбора должна быть четко определена до начала сбора данных, а не сформулирована размыто. Субъект персональных данных должен точно понимать, на что он дает согласие. Цели обработки не должны нарушать действующее законодательство. Нельзя использовать собранную информацию для новых задач, которые противоречат или не связаны с первоначальной целью, без нового согласия или законного обоснования.
- ***Сроки хранения.*** Ограничение сроков хранения требует настройки автоматического удаления или архивации данных по истечении установленного законом или регламентом периода. Например, для невиновных лиц, свидетелей, ошибочно попавших в выборку объектов.

Разграничение доступа и прослеживаемость данных.

- Безопасность должна быть привязана к любой единице данных, где бы она ни находилась. Должно быть реализовано автоматическое наследование атрибута секретности и настроен мандатный контроль через ограничительные метки. Чтобы увидеть нужный объект, пользователь обязан обладать взаимосвязным допуском в своем профиле.
- Помимо жестких меток система должна уметь проверять условия в реальном времени: доступ по строкам и колонкам. Права доступа могут выдаваться на ограниченный период, например, на время проведения расследования или аудита. Для получения доступа к определенным данным целесообразно требовать обоснование, с какой целью данные запрашиваются.
- Сохранение происхождения данных (data lineage). Это фиксация полной истории информации от ее создания до текущего момента, включая все источники, изменения, перемещения. Сохранение происхождения помогает понять, можно ли доверять информации, упрощает нахождение места сбоя в расчетах или отчетах, подтверждает честность и прозрачность данных для регуляторов.
- Журналирование действий операторов. Обязательное журналирование или логирование – это непрерывная автоматическая фиксация всех входов, команд, изменений настроек и операций в информационных системах для расследования инцидентов и контроля безопасности. Обязательному учету подлежат аутентификация, управление конфигурацией, оперативные команды, экспорт и удаление данных. Должны быть реализованы все требования к хранению и защите логов: неизменяемость, синхронизация времени, сроки хранения.

Разделение фактов и алгоритмических выводов.

- Для реализации вышеобозначенного принципа необходима маркировка степени достоверности. Ее можно реализовать через механизм метаданных, сквозное отслеживание происхождения данных и возможной интеграцией со стандартами разведсообщества.

Оценка достоверности должна переноситься на уровень конвейеров данных. Таким образом метки безопасности, метаданные о надежности и секретности намертво привязываются к источнику данных. При объединении, фильтрации или трансформации данных эти метки автоматически наследуются нижестоящими наборами данных и объектами онтологии. Возможно использование больших языковых моделей LLM для автоматического назначения весов достоверности неструктурированному тексту.

Разделение фактов и алгоритмических предположений позволяет четко разграничивать объективную реальность от гипотез, сформированных ИИ или математическими моделями. В хорошей нормативной модели интеграционные платформы должны разделять всю поступающую и генерируемую информацию на несколько строго разграниченных слоев.

Слой фактов: сырые данные и онтология – это фундамент системы. Сюда относятся жесткие верифицированные данные из первоисточников: транзакции, логи звонков, регистры, GPS-треки, отчеты разведки.

Слой алгоритмических предположений. На этом слое работают аналитические модули и предиктивные алгоритмы. Они анализируют слой фактов и генерируют вероятностные сущности или гипотетические связи.

Слой пользовательских гипотез – пространство, где аналитик-человек вручную строит версии, проверяя алгоритмические предположения. Для того чтобы пользователь: военный, следователь, финансовый аналитик не перепутал факт с домыслом машины, используется маркировка происхождения, визуальное кодирование на графах и механизм песочницы.

Human-in-the-loop и аудит. Это архитектурный подход, при котором человек-эксперт обязательно включается в контур работы ИИ-системы для проверки, корректировки или финального одобрения рискованных операций. При этом ИИ обязан предоставлять полный контекст и логику решения, а не слепой числовой расчёт. Люди могут задействовать критическое мышление и понимать нюансы, недоступные алгоритму.

Без строгого контроля платформы класса Palantir несут высокие риски нарушения прав человека и конфиденциальности, потому что они агрегируют огромные массивы разнородных данных и используют алгоритмы искусственного интеллекта для выявления скрытых связей. К ключевым компонентам аудита больших интеграционных систем относится логирование действий, контроль цепочки передачи данных, проверка алгоритмической предвзятости. Последнее означает проверку того, что алгоритм принимает решение одинаково объективно для разных групп людей и не ущемляет никого по защищенным признакам: пол, раса, возраст, национальность и так далее.

К мерам аудита стоит отнести регулярный независимый надзор, привлечение внешних правозащитных, этических или государственных регуляторов для проверки работы системы.

Персональная и институциональная ответственность. Поскольку платформа лишь агрегирует, визуализирует и связывает данные, окончательное решение и действие всегда совершает человек. Аналитик или офицер принимает решение – запустить расследование, отправить оперативную группу или отказать в выдаче визы, руководствуясь собранными в системе данными. Ответственность за юридические и этические последствия этого шага лежит на нем. Человек отвечает за то, чтобы не доверять слепо автоматическим связям, которые построила система, а перепроверять источники данных.

Институциональная ответственность. Государственный орган, спецслужба или корпорация, внедрившая платформу-агрегатор, отвечает за системный контур работы, качество и законность данных. Институт несет ответственность за то, какие базы данных загружаются в систему. Институт должен настроить жесткие уровни доступа. Институт определяет, в каких сценариях допустимо использовать аналитику платформы, а в каких требуются альтернативные источники проверки. Необходимо соблюдать очень важный принцип: ответственность нельзя переносить с субъекта принятия решения на алгоритм.

Заключение. Системы класса Palantir не обладают мистическим «всеведением», приписываемым им частью медийного дискурса. Однако именно поэтому их реальные риски не следует недооценивать. Их мощь заключается не столько в отдельных алгоритмах искусственного интеллекта, сколько в способности объединять разрозненные данные, выявлять скрытые связи и непосредственно включать полученное знание в процесс принятия решений. Поэтому центральным вопросом становится не только «что может алгоритм?», но и «кто получает возможность использовать интегрированное знание, в отношении кого и с какими полномочиями?».

Поступила: 24.07.2026; рецензирована: 07.08.2026; принята: 08.08.2026.

Литература

1. Официальная документация Palantir Foundry. URL: https://www.palantir.com/docs/foundry/getting-started/foundry-platform-summary-llm/ (дата обращения: 05.08.2026).
2. *Хаскинс К.* Чем на самом деле занимается Palantir?/Wired/Бизнес/. URL: https://www.wired.com/story/palantir-what-the-company-does/ (дата обращения: 05.08.2026).
3. *Харрис М.Э.* Как секретная компания Питера Тилля по обработке данных проникла в полицейскую сферу?/Wired/Главная история/. URL: https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/ (дата обращения: 05.08.2026).
4. *Хаскинс К.* Все способы, которыми крупные технологические компании подпитывают ICE и CBP./Wired/Бизнес/. URL: https://www.wired.com/story/how-big-tech-is-powering-trumps-immigration-crackdown/ (дата обращения: 05.08.2026).
5. Доступ компании Palantir к персональным данным пациентов/ The Guardian/ Новости. URL: https://www.theguardian.com/society/2026/may/11/palantir-access-nhs-england-patient-data (дата обращения: 05.08.2026).
6. «Потенциальный риск для безопасности»: анализ проблем доверия в Великобритании к Palantir. Aljazeera/Новости/Здоровье/. URL: https://www.aljazeera.com/news/2026/5/12/palantir (дата обращения: 05.08.2026).