УДК 004.62 https://doi.org/10.26160/2309-8864-2025-19-80-86

ТЕГИРОВАНИЯ ДАННЫХ ДЛЯ СОВРЕМЕННЫХ МОДЕЛЕЙ ИНФОРМАЦИОННОГО УПРАВЛЕНИЯ НА МАШИНОСТРОИТЕЛЬНОМ ПРЕДПРИЯТИИ

Ерохин В.В.[1,2], Буторин Д.А.[2]

[1]Московский государственный институт международных отношений (университет) Министерства иностранных дел РФ, Москва;
[2]Московский государственный технический университет имени Н.Э. Баумана, Москва

Ключевые слова: управление данными, защита данных, обработка данных, тегирование данных, цифровая фиксация обязательств, автоматизированная проверка соблюдения правил.
Аннотация. Современная парадигма, характеризующаяся тотальным сбором, многоаспектным использованием и трансграничной циркуляцией данных, демонстрирует несостоятельность традиционных систем управления и защиты информации. Поскольку организации оперируют данными из гетерогенных источников и в разнородных целях, на них распространяется сложный комплекс зачастую противоречивых нормативных требований. В ответ на эту проблему авторы концептуализируют модель управления, в которой нормативные предписания и коммерческие обязательства инкапсулируются в сами данные. Ключевым технологическим решением, обеспечивающим практическую реализацию данного подхода, выступает метод тегирования информации.

DATA TAGGING FOR MODERN INFORMATION MANAGEMENT MODELS IN A MACHINE-BUILDING ENTERPRISE

Erokhin V.V.[1,2], Butorin D.A.[2]

[1]Moscow state institute of international relations (university), Ministry of Foreign Affairs of the Russian Federation, Moscow;
[2]Bauman Moscow State Technical University, Moscow

Keywords: data management, data protection, data processing, data tagging, digital recording of obligations, automated verification of compliance with rules.
Abstract. The modern paradigm, characterized by the total collection, multidimensional use and cross-border circulation of data, demonstrates the failure of traditional information management and protection systems. Because organizations use data from heterogeneous sources and for diverse purposes, they are subject to a complex set of often contradictory regulatory requirements. In response to this problem, the authors conceptualize a management model in which regulatory prescriptions and commercial obligations are encapsulated in the data itself. The key technological solution that ensures the practical implementation of this approach is the information tagging method.

1. Введение

Повсеместный сбор, использование и передача данных усложняют системы защиты и управления ими. Производственные и организационные структуры предприятия машиностроения извлекают данные из множества источников и применяют их в различных целях, что приводит к различиям в правилах: например, для внутренних задач (проектирование изделия, изготовление изделия, бухгалтерия) или передачи партнёрам на другие предприятия.

Географические границы не ограничивают поток данных, но устанавливают разные требования к обработке, например, персональных данных, создавая сложности для соблюдения прав на конфиденциальность, или параметров изделия, создавая сложности защиты интеллектуальных прав.

В этой динамичной среде управление данными требует привязки правил к самим данным, независимо от их местоположения, сбора или обработки. Для этого предлагается "помечать" данные информацией, помогающей пользователям и получателям понимать свои обязательства по надлежащему использованию и защите.

Модель защиты конфиденциальности, основанная на "уведомлении и выборе", подвергается критике как непрактичная и неэффективная. В ней потребители данных в машиностроительном производстве получают информацию о сборе, использовании и передаче их данных и решают, разрешать ли это. Однако в эпоху мгновенного анализа и повсеместного сбора данных (через интернет, камеры, мобильные устройства, датчики) персонал предприятия сталкивается с бесконечными сложными уведомлениями, не дающими реального выбора – он часто иллюзорен или ограничен.

Представители научного сообщества в области управления данными призывают к альтернативам. Например, Фред Х. Кейт предлагает специализированную защиту с ключевыми ограничениями на обработку данных для предотвращения вреда [1], а научные деятели Академии наук России – более всеобъемлющую версию добросовестной информационной практики, включающую принципы за рамками уведомления и выбора.

Новые модели защиты информации и конфиденциальности адаптированы к реалиям XXI века: сбору, анализу, использованию и хранению данных. Они реалистично определяют, где эффективно уведомление, а где уместен индивидуальный выбор и контроль. Эти подходы учитывают роль данных как ключевого бизнес-актива и сложности управления ими в структурах машиностроительного предприятия. Они включают подотчётность; добросовестные информационные практики, ориентированные на использование данных (а не их сбор); и комплексную систему стратегического управления информацией.

Эти подходы предполагают, что обязательства по защите и безопасности данных привязаны к самим данным и должны соблюдаться независимо от места их хранения или обработки. Они опираются на маркировку данных информацией об этих обязательствах, чтобы все стороны могли их понимать и выполнять. Обязательства могут основываться на законах, нормативных актах, принципах саморегулирования, передовой практике и обещаниях организаций людям.

Например, ERP-система предприятия собирает данные клиентов для выполнения заказов, доставки, внутренних процессов (выставление счетов, бухгалтерия) и обслуживания. Этот сбор регулируется законами, принципами и обещаниями, которые ERP-система обязуется выполнять. При передаче данных внешнему поставщику (для обработки счетов или запросов) обязательства сохраняются, и поставщик также должен их соблюдать.

Если клиент ERP-системы меняет свой юридический адрес, то ERP-система фиксирует переезд и обновляет адрес в базе данных. Это означает смену юрисдикции и применимых законов к данным клиента. ERP-система должна определить, применяются ли правила новой или старой юрисдикции к ранее собранным данным, после чего предприятие и его поставщики должны внедрить правильные правила в своих системах и обеспечить их соблюдение у бизнес-партнёров.

Машиностроительные предприятия всё больше ценят данные как ключевой бизнес-актив и применяют комплексный подход к их защите, обеспечивая не только конфиденциальность, но и целостность, доступность для внутренних нужд. Например, ERP-система может использовать обновлённый адрес клиента для таргетированного продвижения товаров (полуфабрикатов, изделий), а партнёры по кобрендингу или поставкам – для своих целей. Данные также должны быть доступны по процессуальным запросам, что усложняется противоречивыми требованиями в разных юрисдикциях [2]. Так, представитель менеджмента предприятия может проверить адрес для верификации личности звонящего или соответствия доставки изделия (полуфабрикатов, сырья и т.д.).

Новые подходы к защите данных на машиностроительном предприятии включают установление правил доступа, использования, хранения и сохранения, с обеспечением их соблюдения сотрудниками при передаче данных внутри организации [3]. Обязательства по защите привязаны к данным и передаются вместе с ними. Сотрудники предприятия полагаются на законы, передовые практики и заявления менеджмента предприятия о работе с данными, независимо от обработчиков. Пользователи и хранители данных должны понимать и соблюдать правила: кто, как, когда и для чего использует данные. Сторонние обработчики знают требования и спецификации. Это обеспечивает защиту в децентрализованной среде обработки и хранения данных, где сотрудники предприятия не контролируют обработку своей информации [4].

2. Применение модели подотчетности данных на машиностроительном предприятии

Принцип подотчётности данных заложен как в раннем международном документе о конфиденциальности – Руководстве по конфиденциальности Организации экономического сотрудничества и развития (ОЭСР), так и в последнем – Рамках конфиденциальности Азиатско-Тихоокеанского экономического сотрудничества (АТЭС). Оба требуют от владельца информации или контролера данных ответственности за соблюдение мер, обеспечивающих добросовестную информационную практику, описанную в этих документах.

Сейчас предприятия машиностроения определяют границы подотчётности данных и изучают условия, которые организационные структуры предприятия должны продемонстрировать, а регуляторы (государственные институты власти) – измерить для её подтверждения. Политики, органы и эксперты описывают подотчётную организацию как ту, что устанавливает цели по защите конфиденциальности на основе внешних критериев (закона, саморегулирования, передовых практик) и наделяет себя полномочиями определять эффективные меры для их достижения. Учитывая сложность сбора данных, бизнес-моделей,

поставщиков и технологий, превышающую способность индивидов к активному выбору, подотчётность требует от организаций дисциплинированных решений об использовании данных даже без традиционного согласия.

Подотчётность данных строится на приверженности принципам и внутренним политикам, соответствующим внешним требованиям; реализации политик конфиденциальности с использованием инструментов и обучения; постоянном внутреннем и внешнем надзоре, проверках и внешней верификации; прозрачности и участии граждан; и эффективных мерах устранения нарушений и принуждения.

ERP-система может разработать внутреннюю политику конфиденциальности и управления данными, соответствующую местным законам и обязательствам перед пользователями. В рамках подотчётности будут внедрены механизмы соблюдения сотрудниками, а также процессы оценки рисков, надзора и гарантий. Эти системы регулируют внутреннюю обработку данных. Предприятие машиностроения может привлечь внешнего поставщика для обслуживания клиентов и обработки полуфабрикатов, при этом применяются правила обработки данных к любому партнеру. ERP-система обязуется обеспечить приверженность и способность поставщика соблюдать эти требования.

ERP-система может по возможности избегать выполнения кросс‑юрисдикционных правовых требований и создать внутреннюю политику, ограничивающую сбор клиентских данных за пределами каждой юрисдикции. Эта политика частично реализуется за счёт механизмов, определяющих источник запроса (IP‑адрес, код города) и направляющих его в соответствующую юрисдикцию к своему представителю поддержки. Предприятие машиностроения затем публикует подтверждаемую отчётность о деятельности, например, долю сотрудников, прошедших обучение, или число запросов, обработанных согласно политике. Центральную роль играет непрерывная оценка рисков и снижение рисков по использованию информации. При маршрутизации запросов клиенту в нужную юрисдикцию владелец хранилища данных фиксирует и анализирует случаи, не соответствующие политике, и за счёт этого ищет изменения в практиках или технологиях для повышения эффективности в будущем.

3. Применение модели использования и обязательств данных на машиностроительном предприятии

Модель использования и обязательств данных считает использование данных главным фактором обязанностей по защите информации, а не сам факт их сбора. Сбор и согласие обычно не порождают обязательств, за исключением ситуаций, когда сбор используется для идентификации клиента или доставки груза и т.д. Модель предлагает структуру добросовестной информационной практики XXI века: прозрачность, уведомление, выбор, доступ и исправление, ограничение сбора, минимизацию использования, качество данных, хранение, безопасность и подотчетность.

Модель использования и обязательств охватывает все виды использования данных, необходимые для удовлетворения потребностей потребителя и соответствия закону. Она налагает на структуры предприятия обязательства по

пяти категориям использования: 1) установление и поддержание отношений с клиентом; 2) внутренние бизнес-операции; 3) маркетинг; 4) предотвращение мошенничества и аутентификация; 5) требования национальной безопасности и правовые требования. Пример: проверить личность клиента (категория 4) и отправить сообщение в подразделение предприятия (категория 1). Обязательства действуют даже при передаче данных третьим лицам.

4. Применение модели стратегического управления информацией на машиностроительном предприятии

Стратегическое управление информацией – это комплексный подход к управлению данными на уровне всей компании, направленный на защиту всех информационных активов, минимизацию рисков и обеспечение юридической соответствия. Оно рассматривает информацию как важный бизнес-ресурс и обеспечивает доступность данных нужным сотрудникам, а также стимулирует их безопасное и творческое использование для повышения ценности организации и клиентов.

Предприятие машиностроения может внедрить систему управления доступом на основе политик для защиты ресурсов, ограничивая доступ к данным по заранее определённым правилам. Это включает правила для защиты коммерческой тайны (например, в ERP-системе доступ к данным поставщиков ограничен переговорщиками и получателями товаров в транспортной компании); соблюдения законодательства о конфиденциальности (запрет бухгалтерии на доступ к клиентским данным, кроме сотрудников, обрабатывающих жалобы); и выполнения фидуциарных обязанностей (централизованный доступ к налоговым данным только для назначенных сотрудников и аудиторов). Все правила следуют общей структуре: доступ к конкретным данным предоставляется лицам с определённой ответственностью для конкретной цели.

5. Практическое обсуждение моделей

Представленные модели регулируют обработку данных по принципу: кто (субъект), что (данные), как (действие) и при каких условиях. Эти правила (разрешить, обязать, запретить) теперь требуют автоматической проверки системами, так как вручную это делать невозможно из-за объёмов данных. Для этого данные и действия должны быть помечены специальными тегами, чтобы системы могли их распознавать и автоматически применять политики.

Гарантировать соблюдение правил обработки данных (кто, что и как может делать с информацией) в современных условиях можно только с помощью автоматизированных систем. Для этого данные должны быть соответствующим образом размечены, так как ручная проверка непрактична из-за огромных объёмов информации и транзакций.

Соблюдение политик обработки данных зависит от возможности идентифицировать взаимосвязь между субъектом, данными, действием и контекстом в рамках установленных правил. Примеры таких политик:

– разрешение на использование адреса клиента службой поддержки для верификации;

– требование к системам направлять запросы локальным представителям поддержки;

– запрет на отправку товаров на непроверенные адреса.

Ручной контроль таких операций стал неэффективен из-за масштабов данных. Единственное решение – автоматизированная проверка, которая возможна только при наличии аннотаций и тегов у всех элементов данных и транзакций.

Вот перефразированный вариант с сохранением основной идеи и структуры, но более компактным и прямым:

Компьютерные системы не являются человеческими. Они не способны по порядку извлекать смысл из целых предложений или самостоятельно реализовывать сложную логику. Однако принципы конфиденциальности можно постепенно внедрять в цифровую среду, сводя текст к задаче алгебраической формы:

– Если сущность называется «Служба поддержки клиентов» и категория данных – «Адрес клиента» и цель использования – «Подтверждение личности», то разрешено.

– Если категория данных – «Адрес доставки» и она не та же самая, что «Адрес клиента», то запрещено.

Таким образом, разработчики создают инструкции, понятные компьютерам. Они задают категории информации, связанных с бизнес-деятельностью (например, «сущность», «категория данных» и «цель использования»). В зависимости от правила можно заранее определить элементы, которые подходят под категорию, или позволить другим людям или системам помещать в неё любые данные. Если данные в системе помечены для определения таких категорий, компьютер может определить необходимую информацию для реализации политик.

Ценность тегов становится очевидной, когда данные распределены. Если бы вся информация для соблюдения правил хранилась в единой базе, они не были бы так критичны. Вспомним бумажные досье: в папке с закладкой имени клиента лежали его имя, адрес и номер счёта. Но кто именно имел к ней доступ, с какой целью и что делал – не фиксировалось.

Однако даже простые правила требуют знания не только о самих данных, но и о контексте: кто их запрашивает и зачем. Реальные же законы и договоры обладают куда большей сложностью – с условиями, исключениями и вложенными оговорками. Для их выполнения необходимо понимать происхождение данных, время их получения, цепочку правил, которые к ним уже применялись, и множество других контекстных фактов. Ни бумажное досье, ни стандартный цифровой файл такую информацию обычно не содержат.

Именно здесь систематическая разметка данных – об их происхождении, транзакциях и связанных политиках – открывает новые возможности. Она позволяет организациям внедрять сложную автоматизированную проверку правил. Так можно управлять допустимым использованием данных, обеспечивать их защиту, прозрачность и подотчётность, а также отслеживать согласованность применения политик на всём жизненном цикле информации, даже при смене её владельца или формы.

6. Заключение

Современные методы управления данными на предприятии машиностроения – это ответ на вызовы новой цифровой реальности. Сегодня информация собирается зачастую без возможности получить традиционное согласие, анализируется и передаётся мгновенно и может обрабатываться в юрисдикции, отличной от места её сбора. В этих условиях маркировка данных становится практичным инструментом, позволяющим в цифровой форме закреплять правила работы с информацией и адаптироваться к новым моделям защиты.

Внедрение такой системы сталкивается с серьёзным финансовым барьером, особенно при модернизации устаревших инфраструктур. Хотя растущее предложение на рынке постепенно снижает затраты, ключевой задачей для политиков и компаний остается поиск оптимального баланса между издержками и долгосрочными преимуществами этого перспективного подхода, способного обеспечить надёжную защиту данных в XXI веке.

Список литературы

1. Hammond A.S., McConnell B.W., Nelson M., Obuchowski J., Rotenberg M., Cate F. H. Panel Two: Information Policy Making // Federal Communications Law Journal. 1995, vol. 48, iss. 1, p. 3.
2. Тараскин И.Д., Коныхов В.С., Тыренко Д.В., Дудкин А.С. Алгоритм маркировки базы данных с целью анализа и идентификации утечек персональных данных // Методы и технические средства обеспечения безопасности информации. – 2023. – № 32. – С. 98-99.
3. Garg T., Kagalwalla N., Puthran Sh, Churi P., Pawar A. A novel approach of privacy-preserving data sharing system through data-tagging with role-based access control / T. Garg, N. Kagalwalla, Sh. Puthran, P. Churi, A. Pawar // World Journal of Engineering. 2023, vol. 20, no. 1, pp. 12-28. DOI: 10.1108/wje-04-2021-0218.
4. Rimjhim, Dandapat S.K. Tagging multi-label categories to points of interest from check-in data // Transactions on Emerging Topics in Computational Intelligence. 2023, vol. 7, no. 4, pp. 1191-1204. DOI: 10.1109/tetci.2022.3229338.

Сведения об авторах:

Ерохин Виктор Викторович – д.т.н., доцент, профессор кафедры математических методов и бизнес-информатики МГИМО МИД РФ, профессор кафедры инновационного предпринимательства МГТУ им. Н.Э. Баумана;

Буторин Денис Андреевич – магистрант.