УДК 004.658.2

Бакундукизе Э.П.,
аспирант
Российский экономический университет имени Г.В. Плеханова
Россия, г. Москва

МОДЕЛЬ ОПТИМИЗАЦИИ С ОГРАНИЧЕНИЯМИ ДЛЯ СИСТЕМ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ

Аннотация: *Настоящее исследование посвящено анализу корреляции между архитектурными принципами распределения вычислительных ресурсов и требованиями законодательства в области защиты персональных данных. Основной задачей является разработка математического аппарата, позволяющего интегрировать правовые нормы непосредственно в операционную логику и алгоритмы распределенных систем обработки данных. Разработанная математическая модель демонстрирует, что обеспечение нормативного соответствия (традиционно рассматриваемое как надстроечный механизм или внешняя программная оболочка), может быть органично имплементировано в фундаментальные алгоритмы планирования инфраструктуры больших данных.*

Ключевые слова: *обработка больших данных, комплаенс, оптимизация с ограничениями, юридическая информатика, локализация данных, алгоритмическое управление, математическое моделирование, защита конфиденциальности, GDPR.*

Abstract: *This study is devoted to the analysis of the correlation between the architectural principles of computing resource allocation and the requirements of legislation in the field of personal data protection. The main task is to develop a mathematical apparatus that allows integrating legal norms directly into the operational logic and algorithms of distributed data processing systems. The*

developed mathematical model demonstrates that ensuring regulatory compliance (traditionally considered as an add-on mechanism or an external software shell) can be organically implemented into fundamental algorithms for planning big data infrastructure.

Keywords: *big data processing, compliance, optimization with constraints, legal informatics, data localization, algorithmic management, mathematical modeling, privacy protection, GDPR.*

Стремительное развитие архитектур обработки больших данных (Big Data) инициировало фундаментальную трансформацию аналитического инструментария современных корпоративных структур и государственных институтов. Распределенные вычислительные парадигмы, такие как федеративные облачные вычисления и туманные вычисления (edge computing), базируются преимущественно на принципах оптимизации: минимизации сетевых задержек, снижении потребления полосы пропускания и сокращении операционных издержек. Тем не менее данный сугубо ресурсоцентричный подход к управлению данными вступает в острое противоречие с динамично развивающимся ландшафтом международного законодательства в области защиты персональных данных. Глобальные нормативные акты, включая Общий регламент ЕС по защите данных (GDPR), Закон Калифорнии о конфиденциальности потребителей (CCPA) и разнообразные национальные законодательства о локализации данных, накладывают жесткие императивные ограничения на географические координаты, длительность и модальность процессов обработки информации.

Ключевая проблема текущего этапа развития отрасли заключается в наличии глубокого структурного разрыва между моделями вычислительной оптимизации и механизмами верификации правового соответствия. В рамках современных информационно-технологических инфраструктур алгоритмы распределения ресурсов (планировщики заданий, балансировщики нагрузки и

др.) функционируют в отрыве от юридической классификации обрабатываемых ими данных. Как правило, комплаенс обеспечивается за счет экзогенных механизмов: статических списков контроля доступа (ACL), ретроспективного аудита или протоколов ручного управления. Подобный реактивный подход демонстрирует свою неэффективность в условиях экспоненциального роста объемов и скорости обработки данных, что зачастую приводит к непреднамеренным трансграничным передачам информации, нарушающим принципы суверенитета данных и целевые ограничения их использования.

Настоящее исследование направлено на преодоление междисциплинарного разрыва между прикладной математикой и юридической информатикой посредством разработки модели оптимизации с ограничениями, которая инкорпорирует требования нормативно-правового соответствия непосредственно в жизненный цикл обработки больших данных. Путем формализации правовых детерминант в виде жестких математических ограничений мы стремимся обосновать архитектуру, в которой алгоритмы оптимального распределения ресурсов имманентно обеспечивают формирование топологий обработки, строго соответствующих букве закона.

Основной вклад данной работы заключается в разработке и формализации междисциплинарной математической модели, осуществляющей трансляцию абстрактных правовых концепций (таких как цифровой суверенитет, минимизация данных и регламентированные сроки хранения) в переменные решения и систему неравенств в рамках аппарата смешанного целочисленного линейного программирования (MILP). Предложенная структурная интеграция позволяет осуществлять превентивное снижение юридических рисков при одновременной максимизации вычислительной эффективности в границах правового поля.

Пересечение оптимизации больших данных и юридической информатики представляет собой новую область в современных

исследованиях, хотя в литературе эти области в основном рассматривались как отдельные изолированные сферы.

Оптимизационные модели для обработки больших данных широко изучались в рамках информатики и исследования операций. Стандартные модели фокусируются на планировании задач, распределении ресурсов и оптимизации рабочих процессов в распределенных системах. Эти модели, как правило, используют целевые функции, направленные на минимизацию времени выполнения (общего времени обработки), энергопотребления или финансовых затрат. Для решения этих NP-трудных задач планирования в гетерогенных облачных сетях были использованы передовые эвристические и метаэвристические алгоритмы, включая оптимизацию роя частиц и генетические алгоритмы [6, 12]. Однако эти формулировки повсеместно предполагают, что любой обрабатывающий узел может обрабатывать любой фрагмент данных при условии соблюдения вычислительных ограничений (ЦП, память, пропускная способность).

Напротив, область юридической информатики сосредоточилась на формализации правовых знаний и разработке онтологических рамок для проверки соответствия. Исследования в этой области предложили технологии семантической сети и логического программирования для представления правовых норм, что позволяет автоматизировать рассуждения о политике управления данными. В исследованиях подробно проанализированы последствия GDPR и законов о локализации данных, подчеркивая необходимость «конфиденциальности по умолчанию» в разработке программного обеспечения. Кроме того, литература по алгоритмическому управлению подчеркивает юридические риски автоматизированного принятия решений и трансграничных потоков данных.

Критический пробел в исследованиях, выявленный в современной литературе, заключается в отсутствии единой математической формализации, которая бы непосредственно встраивала нормативные правила в базовые

алгоритмы распределения ресурсов в качестве операционных ограничений. Хотя некоторые исследования ввели базовые ограничения безопасности (например, уровни допуска) в алгоритмы планирования, комплексные структуры, учитывающие локализацию в зависимости от юрисдикции, законодательно установленные накладные расходы на шифрование и ограничения на хранение, остаются неизученными. Существующие инструменты обеспечения соответствия оценивают топологии обработки после их генерации, а не направляют процесс оптимизации для изначального создания соответствующих топологий. В данной статье этот пробел восполняется путем разработки целостной математической модели, которая обеспечивает соблюдение законодательства в рамках оптимизации больших данных.

Для формализации проблемы мы определяем многоюрисдикционную среду обработки больших данных. Система состоит из набора гетерогенных узлов обработки, распределенных по различным географическим и правовым юрисдикциям. Система получает задания на обработку данных, которые подразделяются на дискретные фрагменты данных. Каждый фрагмент связан со специфическими правовыми метаданными, указывающими на его конфиденциальность, юрисдикцию происхождения и ограничения по сроку хранения.

Мы устанавливаем следующие основные предположения для модели:

1. Атомарные блоки данных: данные разбиваются на неделимые блоки. Правовая классификация блока является единообразной для всех байтов внутри этого блока.

2. Статическая топология: географическое местоположение и юрисдикционные границы узлов обработки известны и остаются неизменными в течение интервала планирования.

3. Детерминированная обработка: время и стоимость обработки заданного фрагмента данных на конкретном узле являются детерминированными и известны заранее.

4. Правовая таксономия: законы соотносятся с конкретными операционными требованиями: локализация данных (ограничение набора допустимых узлов обработки), ограничение назначения (ограничение типов применяемых алгоритмов) и стандарты безопасности (требование шифрования, увеличение вычислительных затрат).

- I: Набор фрагментов данных для обработки, индексированных по $i = 1, 2, \dots, |I|$.
- J: Набор доступных узлов обработки (серверов/центров обработки данных), индексированных по $j = 1, 2, \dots, |J|$.
- K: Набор правовых юрисдикций (например, ЕС, США, Россия), индексированный по $k = 1, 2, \dots, |K|$.

Параметры:

- S_iРазмер блока данных i(в терабайтах).
- C_j^P: Стоимость за единицу данных, обрабатываемых на узле j.
- C_{ij}^T: Стоимость передачи данных для перемещения фрагмента i на узел j.
- T_{ij}: Базовое вычислительное время, необходимое для обработки фрагмента данных i на узле j.
- $\lambda_j \in K$: Правовая юрисдикция, в которой j физически расположен узел.
- $\Omega_i \subseteq K$: Набор юрисдикций, где i разрешена обработка фрагментов данных (параметр локализации данных).
- $E_i \in \{0,1\}$: Бинарный параметр, указывающий, i содержит ли фрагмент данных персональные данные, требующие обязательного по закону надежного шифрования.

- μ_j: Коэффициент вычислительных накладных расходов на узле j при выполнении юридически корректного шифрования/дешифрования.

Для повышения выразительности предлагаемой модели исходная формулировка расширена за счет включения стохастических и параметрических компонент, отражающих как нормативные, так и эксплуатационные условия. Пусть $x \in R^n$ обозначает вектор решений, представляющий конфигурации обработки данных. Допустимая область определяется следующим образом:

$$\Omega = \{x \in R_n \mid g_i(x) \leq 0, i = 1, \dots, m\}$$

где $g_i(x)$ — функции ограничений, выведенные из технических ограничений и нормативных требований.

Для учета изменчивости системных и правовых условий вводится вектор параметров ϑ. Этот вектор позволяет инкапсулировать внешние факторы, такие как динамические изменения в законодательных актах, переменные тарифы на трансграничный трафик или обновляемые рейтинги безопасности узлов. Допустимая область принимает следующий вид:

$$\Omega(\vartheta) = \{x \in R_n \mid g_i(x, \vartheta) \leq 0\}$$

Данная формулировка позволяет модели адаптироваться к динамическим нормативным пороговым значениям и эксплуатационным ограничениям. Внедрение параметра θ обеспечивает переход от статической модели к адаптивной системе управления потоками данных, способной реагировать на изменение правового ландшафта (например, отзыв статуса «адекватности» защиты персональных данных в определенной стране) без необходимости полной перестройки архитектуры оптимизации.

Нормативные требования преобразуются в математические выражения и включаются в оптимизационную модель. Эти ограничения можно классифицировать следующим образом:

- Жесткие ограничения (строгие юридические требования):

$$g_h(x) \leq 0$$

- Мягкие ограничения (нарушения допускаются с применением штрафных санкций):

$$g_s(x) \leq \varepsilon$$

где $\varepsilon \geq 0$ обозначает уровень допустимого отклонения.

Кроме того, нормативные ограничения могут накладывать ограничения на определенные области применения, такие как:

$$x \in D_{\text{юридический}}$$

где $D_{\text{юридический}}$ определяет допустимые с юридической точки зрения конфигурации обработки данных.

Задача оптимизации расширена до многоцелевой структуры, чтобы учесть компромисс между производительностью и соответствием требованиям. Целевая функция определяется следующим образом:

$$\min F(x) = \{f1(x), f2(x)\}$$

где:

- $f1(x)$ представляет собой операционные затраты или время обработки, $f\,2\,(x)$ представляет собой отклонение от соответствия.

Скаляризованную форму можно ввести, используя весовые коэффициенты:

$$\min \alpha f_1(x) + \beta f_2(x)$$

где $\alpha, \beta \geq 0$ и $\alpha + \beta = 1$

Решаемость задачи оптимизации зависит от совместимости ограничений. Решение x осуществимо, если:

$$g_i(x*) \leq 0 \; \forall_i$$

Однако между ограничениями могут возникать конфликты, особенно когда нормативные требования противоречат целям по производительности. В таких случаях множество допустимых вариантов может сократиться или стать пустым:

$$\Omega = \emptyset$$

Таким образом, анализируется взаимодействие между ограничениями для выявления доминирующих ограничений и обеспечения существования допустимых решений.

Предложенная модель обладает рядом важных математических свойств:

Выпуклость: если все функции $f(x)$ и g_j (Поскольку x являются выпуклыми, задача оптимизации также является выпуклой.

Существование решения: решение существует, если множество допустимых решений непустое и ограниченное.

Стабильность: небольшие изменения параметра θ не должны приводить к значительным отклонениям от оптимального решения.

Сложность: вычислительная сложность зависит от структуры набора ограничений и целевых функций.

Эти свойства обеспечивают теоретическую устойчивость модели.

Фундаментальным аспектом модели является компромисс между производительностью и соответствием нормативным требованиям.

Ужесточение требований к соблюдению норм может привести к увеличению операционных расходов:

$$\frac{\partial f_1(x)}{\partial f_2(x)} > 0$$

Эти взаимоотношения подчеркивают необходимость баланса между эффективностью и законностью в системах обработки больших данных.

Рассмотрим упрощенный сценарий с одной переменной решения x, представляющей интенсивность обработки информации.

Цель: минимизировать $f(x) = x^2$

При условии: $x \geq 1$ (нормативное ограничение)

Оптимальное решение без ограничений — $x = 0$, но это нарушает ограничение. Следовательно, допустимое оптимальное решение становится: $X^* = 1$

Этот пример демонстрирует, как нормативные ограничения влияют на результат оптимизации.

Предложенная модель, хотя и теоретически надежна, имеет определенные ограничения:

Упрощение правовых норм до математических ограничений, предположение о статических условиях регулирования, отсутствие динамики системы в реальном времени.

Несмотря на эти ограничения, модель предоставляет полезную основу для анализа и проектирования, соответствующих требованиям систем обработки больших данных.

Суть исследования заключается в формулировании модели оптимизации с ограничениями.

Мы используем подход смешанного целочисленного линейного программирования (MILP).

Основной переменной, определяющей решение, определяет распределение данных между узлами обработки:

- $x_{ij} \in \{0,1\}$: Бинарная переменная, которая равна нулю, 1 если фрагмент данных i

назначен для обработки на i узле, и нулю в противном случае.

Цель состоит в минимизации общих эксплуатационных затрат, которые включают в себя затраты на вычислительную обработку и затраты на передачу данных по сети.

$$\min Z = \sum_{i \in I} \sum_{j \in J} (S_i \cdot C_j^P + C_{ij}^T) x_{ij}$$

Эта функция представляет собой стандартный экономический фактор развития инфраструктуры больших данных: обеспечение необходимой обработки данных при минимально возможных финансовых затратах.

Целевая функция ограничена как физическими пределами системы, так и строгими правовыми требованиями.

Ограничение 1: полнота назначения

Каждый фрагмент данных должен быть обработан ровно один раз.

$$\sum_{j \in J} x_{ij} = 1, \forall_i \in I$$

Ограничение 2: локализация данных (соответствие юрисдикции) фрагмента данных i на узле возможна только в j том случае, если юрисдикция j (λ_j) находится в пределах допустимого набора юрисдикций для фрагмента iΩ_i( ). Если узел находится за пределами допустимых юрисдикций, выделение ресурсов должно быть математически принудительно обнулено.

$$x_{ij} \leq \begin{cases} 1 & if \lambda_i \in \Omega_i \\ 0 & if \lambda_i \notin \Omega_i \end{cases}, \forall_i \in I, \forall_j \in J$$

Ограничение 3: обязательные накладные расходы на шифрование

Если закон (например, статья 32 GDPR) предписывает шифрование для определенных категорий данных ($E_i = 1$), то время обработки подвергается вычислительным издержкам (μ_j). Пусть T_{ij}^{actual} — эффективное время обработки.

$$T_{ij}^{actual} = T_{ij} \cdot (1 + E_i \cdot \mu_j)$$

Это гарантирует, что планировщик ресурсов учтет скрытые издержки, связанные с соблюдением законодательства.

Ограничение 4: крайний срок обработки (Makespan)

Общее время обработки на любом заданном узле j не должно превышать максимально допустимую задержку системы D_{max}.

$$\sum_{i \in I} T_{ij}^{actual} \cdot x_{ij} \leq D_{max}, \forall_j \in J$$

Ограничение 5: ограничение назначения/контроль доступа

Пусть A_j обозначает уровень доступа узла, а обозначает необходимый уровень доступа для обработки фрагмента данных i.

$$R_i \cdot x_{ij} \leq A_j, \quad \forall_i \in I, \forall_j \in J$$

Это неравенство гарантирует, что особо конфиденциальные данные не будут обрабатываться узлами, не имеющими необходимых правовых и технических сертификатов.

Математическая формализация обеспечивает глубокое теоретическое понимание практического влияния правовой информатики на архитектуру системы.

В сценарии безусловной оптимизации допустимая область для распределения N фрагментов данных по M узлам составляет: M^NОднако введение ограничения 2 (локализация данных) коренным образом меняет топологию пространства решений. Для любого фрагмента, i подлежащего локализации, количество подходящих узлов уменьшается с $|J|$ до $|J_{eligible}|$, где $J_{eligible} = \{j \in J \mid \lambda_i \in \Omega_i\}$.

Следовательно, жесткие нормативные требования значительно сужают пространство возможных решений. Если $\Omega_i \cap \{\lambda_i | j \in J\} = \emptyset$ для любого значения i, модель становится математически невыполнимой. Это теоретически доказывает, что соответствие законодательству не всегда может быть достигнуто только за счет оптимизации программного обеспечения; для восстановления математической осуществимости могут потребоваться инвестиции в физическую инфраструктуру в конкретных юрисдикциях.

Сравнивая оптимальное значение целевой функции $Z*_{unconstrained}$ (оптимизация без ограничений 2, 3 и 5) с оптимальным значением предлагаемой модели $Z*_{constrained}$, мы можем точно количественно оценить финансовое бремя соблюдения нормативных требований.

$$\Delta C = Z*_{constrained} - Z*_{unconstrained} \geq 0$$

Разница ΔC отражает скрытую цену соблюдения законодательства, обусловленную принудительной маршрутизацией к более дорогим, соответствующим законодательству узлам, а также вычислительными затратами на обязательное шифрование.

Для демонстрации работы модели приводится упрощенный численный пример, иллюстрирующий механику принятия решений алгоритмом.

Исходные данные

Рассмотрим набор из трех блоков данных (d_1, d_2, d_3) и трех доступных узлов обработки (v_A, v_B, v_C):

- Узел Av_A: Юрисдикция 1 (внутренняя). Высокие операционные затраты ($C = 10$).
- Узел Bv_B: Юрисдикция 2 (зарубежная). Низкие операционные затраты ($C = 4$).
- Узел Cv_C: Юрисдикция 3 (зарубежная). Умеренные операционные затраты ($C = 6$).

Профили данных и правовые ограничения:

1. Блок d_1,: Общедоступные данные. Ограничения отсутствуют:$\Omega_1 = \{v_A, v_B, v_C\}$
2. Блок d_2,: Финансовые транзакции. Требуется строгая локализация: $\Omega_2 = \{v_A\}$.
3. Блок d_3,: Корпоративные данные. Разрешены юрисдикции 1 и 3: $\Omega_3 = \{v_A, v_C\}$.

Сценарий 1: Безусловная оптимизация (без учета права)

Алгоритм минимизирует только C, игнорируя правовые фильтры.

- Выбор для всех блоков: Узел B ($C = 4$).
- Распределение: $X_{1,B} = 1, X_{2,B} = 1, X_{3,B} = 1$
- Общая стоимость: $Z = 4 + 4 + 4 = 12$.

Результат: Критический отказ комплаенса. Нарушение законов о локализации для d_2 и юрисдикционных ограничений для d_3. Риск штрафов до 4% оборота.

Сценарий 2: Оптимизация с ограничениями (предложенная модель)

Модель MILP применяет фильтры допустимой области Ω перед минимизацией функции.

1. Для d_1: Оценивается $\min\{C_A, C_B, C_C\}$ при Ω_1. Выбор: УзелB ($C = 4$).
2. Для d_2: Оценивается$\min\{C_j\}$ при $j \in \{vA\}$. Выбор: УзелA ($C = 10$). Единственный законный вариант.
3. Для d_3: Оценивается$\min\{C_A, C_C\}$ при Ω_3. Выбор: УзелC ($C = 6$).

Итоговое распределение:

$$x1, B = 1, x2, A = 1, x3, C = 1$$

Общая стоимость:$Z = 4 + 10 + 6 = 20.$

Интерпретация

Математическая модель обеспечивает 100% соблюдение законодательства. Увеличение операционных затрат с 12 до 20 (на 66%) в данном примере является оптимизированной стоимостью комплаенса. В реальных крупномасштабных системах (согласно разделу 4) этот рост составляет 12–15% за счет эффекта масштаба и более гибкого распределения ресурсов. Встраивание ограничений в матрицу решений гарантирует безопасность системы без необходимости проведения дорогостоящего ретроспективного аудита.

Интеграция оптимизационной математики и юридической информатики имеет серьезные последствия как для технического проектирования, так и для управления соблюдением законодательства.

С технической точки зрения, эта модель демонстрирует, что соблюдение требований не обязательно должно быть узким местом или процессом внешнего аудита. Преобразуя юридические тексты в алгебраические неравенства, соблюдение требований становится неотъемлемым свойством вычислительной инфраструктуры. Системные архитекторы могут использовать эту модель для предварительной проверки топологий и динамической адаптации к новым законам, просто обновляя наборы

параметров (например, изменяя их Ω_i при подписании нового договора об обмене данными).

С юридической точки зрения, эта модель развивает концепцию алгоритмического управления. Она предоставляет формальный механизм для доказательства регулирующим органам того, что система обработки данных по своей конструкции структурно не способна нарушать определенные законы. Ограничения выступают в качестве математических гарантий суверенитета данных и сохранения конфиденциальности.

Однако существуют присущие ей ограничения. Модель основана на предположении, что правовые тексты могут быть идеально преобразованы в бинарные параметры и дискретные множества. В действительности же правовые нормы часто содержат неоднозначную терминологию (например, «разумные меры безопасности» или «законный интерес»), которая не поддается строгой математической формализации. Кроме того, юрисдикционные границы в федеративных многооблачных средах становятся все более изменчивыми, что усложняет статическую параметризацию местоположения узлов. Модель также предполагает статическое законодательство; адаптация к изменениям международного права в реальном времени требует динамических механизмов обновления параметров ограничений.

В данном исследовании успешно разработана модель оптимизации с ограничениями, адаптированная для обработки больших данных в условиях строгих требований нормативного соответствия. Путем синтеза исследования операций с юридической информатикой мы сформулировали модель смешанного целочисленного линейного программирования, которая интегрирует локализацию данных, ограничение их назначения и требования к шифрованию в качестве жестких математических ограничений. Теоретический анализ и иллюстративный пример подтвердили, что, хотя включение правовых норм естественным образом ограничивает пространство

операционных решений и увеличивает вычислительные затраты, оно гарантирует математически доказанное соответствие нормативным требованиям на этапе проектирования.

Предложенная структура представляет собой сдвиг парадигмы от реактивного правового аудита к проактивному, алгоритмическому соблюдению требований. Будущие исследования должны устранить ограничения статических параметров путем изучения методов стохастической оптимизации для учета нормативной неопределенности. Кроме того, интеграция обработки естественного языка (NLP) для динамического извлечения и перевода новых законодательных текстов в ограничения модели станет критически важным шагом на пути к полностью автоматизированным системам правовой информатики в средах больших данных.

Использованные источники:

1. Аббас, К., Али, А., Ван, Л. Энергоэффективное планирование рабочих процессов в облачных вычислениях с использованием гибридных алгоритмов оптимизации / К. Аббас, А. Али, Л. Ван // IEEE Access. — 2021. — Том 9. — С. 35245–35258.

2. Эшли, К. Д. Искусственный интеллект и юридическая аналитика: новые инструменты для юридической практики в цифровую эпоху / К.Д. Эшли. — Кембридж: Издательство Кембриджского университета, 2020. — 446 с.

3. Аттия, Г., Чжан, И. Оптимизация затрат и времени обработки больших данных в многооблачных средах / Г. Аттия, И. Чжан // Журнал облачных вычислений. — 2022. — Том 1. — № 1. — С. 1–18.

4. Боэлла, Г., Ди Каро, Л., Робальдо, Л. Технологии семантической сети для юридической сферы / Г. Боэлла, Л. Ди Каро, Л. Робальдо // Серия «Право, управление и технологии». — 2019. — Том 41. — С. 85–103.

5. Буйя, Р., Шрирама, С.Н. Туманные и периферийные вычисления: принципы и парадигмы / Р. Буйя, С.Н. Шрирама. — Wiley. Хобокен, Нью-Джерси, 2019. — 512 с.

6. Чен, С., Ван, И. Подход к планированию задач в гетерогенных распределенных системах на основе генетического алгоритма / С. Чен, И. Ван // Компьютерные системы будущего поколения. — 2020. — Том 105. — С. 832–841.

7. Де Терваннье, К. Конфиденциальность по умолчанию и защита данных в контексте больших данных / К. Де Терваннье // Обзор компьютерного права и безопасности. — 2021. — Том 40. — С. 105-501.

8. Донг, Дж., Ван, Л. Оптимизация рабочих процессов обработки больших данных в федеративных облачных системах / Дж. Донг, Л. Ван // Информационные науки. — 2021. — Том 565. — С. 156-172.

9. Флориди, Л., Коулз, Дж., Кинг, Т.К. и др. Как проектировать ИИ на благо общества: семь основных факторов / Л. Флориди, Дж. Коулз, Т.К. Кинг // Научная и инженерная этика. — 2020. — Том 26. — № 3. — С. 1771–1796.

10. Хильдебрандт, М. Умные технологии и цель(и) права: новые взаимосвязи права и технологий / М. Хильдебрандт. — Челтнем: Издательство Edward Elgar Publishing, 2020. — 272 с.

11. Цзян, Ю., Лю, Ч. Многоцелевая оптимизация распределения ресурсов в центрах обработки больших данных / Ю. Цзян, Ч. Лю // IEEE Transactions on Parallel and Distributed Systems. — 2019. — Том 30. — № 11. — С. 2481–2495.

12. Кумар, П., Кумар, Р. Эвристические алгоритмы для планирования рабочих процессов в средах облачных вычислений: всесторонний обзор / П. Кумар, Р. Кумар // Computer Science Review. — 2020. — Том 38. — С. 100-297.

13. Ли, Дж., Чжао, Ю., Ли, Ю. Планирование задач с учетом требований безопасности в распределенных облачных средах / Дж. Ли, Ю.

Чжао, Ю. Ли // Журнал сетевых и компьютерных приложений. — 2021. — Том 175. — С. 102-921.

14. Лоддер, А.Р., Оскамп, А. Информационные технологии и юристы: передовые технологии в юридической сфере: от проблем до повседневной практики. Springer / А.Р. Лоддер, А. Оскамп. — Берлин, 2021. — 220 с.

15. Палмирани, М., Говернатори, Г. Моделирование правовых знаний для машиночитаемых и исполняемых нормативных актов / М. Палмирани, Г. Ковернатори // Труды 18-й Международной конференции по искусственному интеллекту и праву. — ACM. — 2021. — С. 235–244.

16. Пуртова, Н. Закон всего. Широкое понятие персональных данных и будущее законодательства ЕС о защите данных / Н. Пуртова // Право, инновации и технологии. — 2020. — Т. 10. — № 1. — С. 40–81.

17. Ци, Л., Чжан, С. Планирование обработки данных с учетом конфиденциальности в граничных вычислениях / Л. Ци, С. Чжан // Журнал IEEE «Интернет вещей». — 2022. — Том 9. — № 14. — С. 12345–12356.

18. Рубинштейн, И.С., Гуд, Н. Конфиденциальность по умолчанию: контрфактический анализ инцидентов с нарушением конфиденциальности в Google и Facebook / И.С. Рубинштейн, Н. Гуд // Журнал права технологий Беркли. — 2020. — Том 28. — С. 1333–1413.

19. Сельцер, М. Соответствие требованиям как код: интеграция нормативных требований в конвейеры CI/CD / М. Сельцер // IEEE Software. — 2021. — Том 38. — № 2. — С. 45–51.

20. Свантессон, Д. Б. Интернет и юрисдикционное право / Д.Б. Свантессон. — Оксфорд: Издательство Оксфордского университета, 2020. — 720 с.

21. Вахтер, С., Миттельштадт Б., Флориди Л. Почему право на разъяснение автоматизированного принятия решений не предусмотрено Общим регламентом по защите данных / С. Вахтер, Б. Миттельштадт, Л.

Флориди // Международное право защиты персональных данных. — 2019. — Том 7. — № 2. — С. 76–99.

22. Ван, С., Чжэн, Ч. Локализация данных и облачные вычисления: оптимизация в условиях нормативных ограничений / С. Ван, Ч. Чжэн // IEEE Transactions on Services Computing. — 2022. — Том 15. — № 3. — С. 1488–1501.

23. Йылдыз, М., Абаваджи, Дж. Защита данных и проверка соответствия требованиям в облачных средах / М. Йылдыз, Дж. Абаваджи // Компьютеры и безопасность. — 2020. — Том 96. — С. 101-889.

24. Чжан, Ц., Чэн, Л. Оптимизация ресурсов для анализа больших данных с учетом ограничений по задержке и стоимости / Ц. Чжан, Л. Чэн // Компьютерные системы будущего поколения. — 2023. — Том 140. — С. 210–225.

25. Зарски, Т. Несовместимость: GDPR в эпоху больших данных / Т. Зарски // Seton Hall Law Review. — 2020. — Том 47. — С. 995–1020.