ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК004.056.5
DOI: 10.22213/2410-9304-2026-1-4-12

Методическая основа архитектуры анонимизации данных для задач машинного обучения

Э. М. Дюкина, студент, МИРЭА – Российский технологический университет, Москва, Россия
Ю. В. Силаев, МИРЭА – Российский технологический университет, Москва, Россия
О. М. Перминова, кандидат экономических наук, доцент, МИРЭА –
Российский технологический университет, Москва, Россия

Работа посвящена методическому каркасу архитектуры системы анонимизации табличных данных, встроенной в жизненный цикл проектов машинного обучения в корпоративном контуре подготовки данных. Предлагается процессно-этапный подход к проектированию конвейера анонимизации, который задает единый понятийный аппарат, требования и ограничения и формализует профили правил псевдонимизации, обобщения, маскирования и подавления для различных классов атрибутов: прямых идентификаторов, квазиидентификаторов и чувствительных признаков. На базе моделей k-анонимности, l-разнообразия и t-близости вводятся «контрольные точки приватности», в которых оценивается достижение целевых значений метрик, доля подавлений и уровень обобщения. В каждой точке формируется отчет о приватности с фактическими k, l, t, предупреждениями и комментариями, позволяющий принимать решение о допуске набора в ML-контур. Показано, как проводить предварительную проверку профилей и параметров на репрезентативных обезличенных сэмплах без обращения к фактическим производственным датасетам, что снижает риски раскрытия на ранних этапах согласования. Каркас включает распределение ролей и зон ответственности (владелец данных, инженер по данным, аналитик/дата-сайентист, ML-инженер, специалист по информационной безопасности, администратор системы) и трехслойную архитектуру ИС с веб-интерфейсом и API для интеграции в оркестраторы пайплайнов. Управление профилями правил как версионируемыми артефактами, совместно с версионированием наборов данных и параметров запусков, хранением метаданных, журналированием операций и регулярным аудитом, обеспечивает воспроизводимость подготовки обучающих выборок и прослеживаемость влияния анонимизации на качество моделей. Каркас может использоваться как референсная модель для пилотной реализации и последующего расширения на другие классы данных и практики управления приватностью в ML-проектах.

Ключевые слова: анонимизация, приватность, архитектура, обезличивание, безопасность, k-анонимность.

Введение

Масштабное внедрение систем машинного обучения в корпоративной практике сопровождается ростом объемов персональных данных и ужесточением требований регуляторов к их защите. Организации вынуждены одновременно поддерживать высокое качество моделей и снижать риск раскрытия конфиденциальной информации при передаче данных на этапы подготовки признаков обучения и эксплуатации. На практике решения по анонимизации часто принимаются ситуативно: используются разовые скрипты, частичные шаблоны преобразований и неформальные договоренности между командами разработки и информационной безопасности.

В такой организации процесса правила анонимизации редко формализуются и версионируются, слабо связываются с моделями приватности (k-анонимность, l-разнообразие, t-близость) и мало учитывают специфику жизненного цикла ML-систем. Поэтому одна и та же исходная информация

может по-разному обезличиваться в разных проектах [1], а воспроизведение обучающих выборок и оценка влияния анонимизации на качество моделей затруднены [2]. Ситуацию дополнительно осложняют требования импортозамещения и ориентация на отечественную инфраструктуру хранения и обработки данных.

В этих условиях актуально разработать методический каркас, который связывает модели приватности, роли участников, архитектуру информационной системы и процессы подготовки данных для ML-проектов в единую, воспроизводимую и пригодную к аудиту рамку. Цель работы – описать такой каркас на примере корпоративной ИС анонимизации данных, интегрированной с конвейером машинного обучения, и показать, как профили правил анонимизации и формализованный жизненный цикл их изменений повышают управляемость и воспроизводимость решений по приватности в ML-проектах.

Используемые подходы

При проектировании архитектуры анонимизации данных ключевую роль играют синтаксические модели приватности, задающие формальные критерии допустимого риска реидентификации. Базой для их применения служит разбиение атрибутов на три группы: прямые идентификаторы (ФИО, номер паспорта, телефон), квазиидентификаторы (дата рождения, регион, должность, характеристики договора) и чувствительные атрибуты (доход, состояние здоровья, результаты обследований, категории риска и т. п.). Прямые идентификаторы подлежат псевдонимизации или удалению, квази-идентификаторы – обобщению и подавлению, чувствительные атрибуты – контролю распределений и устойчивости к восстановлению.

Модель k-анонимности [3] требует, чтобы каждая комбинация значений квазиидентификаторов встречалась не менее чем у k записей. Интуитивно это означает, что отдельный субъект «растворён» в группе из k похожих субъектов, а злоумышленник не может сузить поиск до единичной записи, используя внешнюю информацию. Достижение k-анонимности обеспечивается обобщением (укрупнение категорий, округление чисел) и подавлением (частичное или полное удаление значений).

Однако k-анонимность не защищает от атак, связанных с однородностью чувствительных атрибутов внутри кластера. Модель l-разнообразия [4] вводит требование по разнообразию значений чувствительного атрибута для каждой к-анонимной группы: внутри группы должно быть как минимум l «существенно различных» значений или распределение не должно быть сконцентрировано на одном значении.

Модель t-близости [5] дополняет этот подход, ограничивая расстояние между распределением чувствительного атрибута внутри группы и его глобальным распределением по набору. Чем меньше параметр t, тем ближе локальное распределение к глобальному и тем меньше информации о смещении вероятностей получает злоумышленник. Совместное использование k-анонимности, l-разнообразия и t-близости позволяет задать формальные критерии приватности, которые затем связываются с профилями правил и контрольными точками в архитектуре системы.

В корпоративной практике жизненный цикл систем машинного обучения включает извлечение данных из прикладных систем, очистку и приведение к единому формату, построение признаков, обучение и верификацию моделей, их развертывание и последующий мониторинг качества. Подготовка наборов данных для экспериментов, как правило, реализуется через скрипты и пайплайны в инфраструктуре хранения и оркестрации, которыми управляют инженеры по данным, аналитики и специалисты в области машинного обучения.

Анонимизация в таком контуре обычно воспринимается как вспомогательный шаг перед загрузкой данных в ML-среду: используются разовые скрипты, простые шаблоны замены значений и ручная фильтрация записей [6]. Правила при этом редко формализуются и версионируются, практически не связываются с моделями k-анонимности, l-разнообразия и t-близости, поэтому одно и то же исходное множество данных может быть анонимизировано по-разному, а точное воспроизведение использованных при

обучении выборок впоследствии затруднительно [7].

Существующие программные решения по анонимизации данных представлены отдельными библиотеками и пакетами для обработки табличных наборов специализированными инструментами статистической анонимизации и оценки рисков, а также встроенными модулями в составе СУБД, ETL-платформ и крупных зарубежных облачных сервисов [8]. Для сценариев, где обезличивание должно быть встроено в подготовку данных для ML, описаны фреймворки поддержки принятия решений по выбору преобразований и оценке их влияния на процесс обучения [9]. При этом в современных обзорах подчеркивается, что анонимизация не является «идеальной» процедурой и всегда остается компромиссом между полезностью данных и риском раскрытия [10]. В отечественной практике дополнительно развиваются процедурные артефакты управления публикацией и использованием данных, включая паспорта наборов данных [11]. Также предлагаются форматы протоколов анонимизации как отдельного управляемого документа жизненного цикла набора [12]. Подходы на основе имитационного моделирования формализуют оценку состояния и базовые положения применения обезличивания в прикладных сценариях [13]. В развитие этого направления предлагаются алгоритмы обезличивания методом синтеза как вариант построения преобразований данных [14]. Однако перенос подобных подходов в корпоративный контур часто упирается в необходимость учитывать инфраструктурные ограничения, регуляторные требования и условия импортозамещения, характерные для эргасистем [15].

Материалы и методы

Рассматриваемый корпоративный контекст включает множество прикладных информационных систем с собственными хранилищами и журналами событий (операционные базы данных, CRM, системы учета обращений, специализированные реестры и сервисы отчетности).

Исторически они развивались независимо, поэтому схемы данных и форматы представления информации различаются, а централизованное озеро данных либо отсутствует, либо охватывает лишь часть источников; подготовка наборов для аналитики и машинного обучения выполняется отдельными командами через скрипты и пайплайны. В as-is-процессе обезличивание данных встроено фрагментарно: используются локальные шаблоны псевдонимизации и фильтрации, отдельные механизмы СУБД и ETL-инструментов, при этом нет единых профилей правил и централизованной точки управления анонимизацией. Решения по выбору атрибутов и степени обобщения принимаются на уровне пайплайнов и не всегда документируются, из-за чего близкие по назначению наборы обрабатываются поразному, а воспроизводимость экспериментов и повторное использование согласованных решений по анонимизации ограничены. Этот контекст далее используется как отправная точка для проектирования целевого решения (рис. 1).

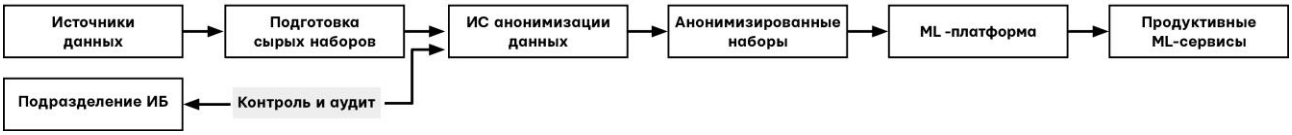

Рис. 1. Контекст системы анонимизации данных в жизненном цикле проекта машинного обучения

Fig. 1. Context of the data anonymization system in the machine learning project lifecycle

Разработка целевой архитектуры системы анонимизации данных опирается на подход инженерии артефактов («design science»), в рамках которого ключевым результатом является спроектированное решение, адаптированное к конкретному классу практических задач. Исходной точкой служит анализ существующего процесса подготовки данных и ограничений инфраструктуры (используемые СУБД, средства оркестрации, стек разработки ML-

моделей). На этой основе формулируются требования к системе: поддержка моделей приватности (k-анонимность, l-разнообразие, t-близость), интеграция с ML-пайплайнами, воспроизводимость и аудит действий по анонимизации, технологическая реализуемость в заданном контуре. Далее строится методический каркас с ролями и зонами ответственности, целевым процессом подготовки данных с контрольными точками приватности и многослойной архитектурой информационной системы, рассматриваемый как референсная модель, пригодная для адаптации под конкретные проекты.

Методический каркас архитектуры системы анонимизации данных

Целевая архитектура информационной системы анонимизации данных (ИСАД) опирается на четкое разделение ролей. Ключевые участники: владелец продукта или бизнес-заказчик, формулирующий ML-задачу; владелец данных; инженер по данным и аналитик/дата-сайентист, готовящие выборки и признаки; ML-инженер, внедряющий модель; специалист по информационной безопасности; администратор и разработчик ИСАД.

Основные объекты управления: источники данных и их схемы; сырые и анонимизированные наборы; профили правил анонимизации с целевыми k, l, t и перечнем преобразований для типов атрибутов; отчеты о приватности с фактическими метриками и комментариями ИБ; контрольные точки приватности в процессе подготовки данных; журналы операций с фиксацией применения профилей и результатов проверок.

Зоны ответственности организованы так, чтобы минимизировать конфликт интересов и обеспечить воспроизводимость. Бизнес-заказчик и владелец данных задают цель использования и допустимые ограничения по бизнес-содержанию. Инженер по данным и аналитик формируют выборки и инициируют применение профилей, не изменяя утвержденные параметры приватности. Специалист ИБ и владелец профилей разрабатывают, рецензируют и утверждают правила, а также интерпретируют отчеты о приватности. Администратор ИСАД поддерживает работоспособность, управление версиями и журналирование. ML-инженер использует уже анонимизированные наборы и отчеты как формальные артефакты, связывающие конкретную модель с примененными правилами анонимизации.

Целевой процесс подготовки данных встраивает анонимизацию в жизненный цикл ML-проекта и задает фиксированные контрольные точки приватности. Общая схема целевого процесса подготовки данных с выделением контрольных точек приватности приведена на рис. 2.

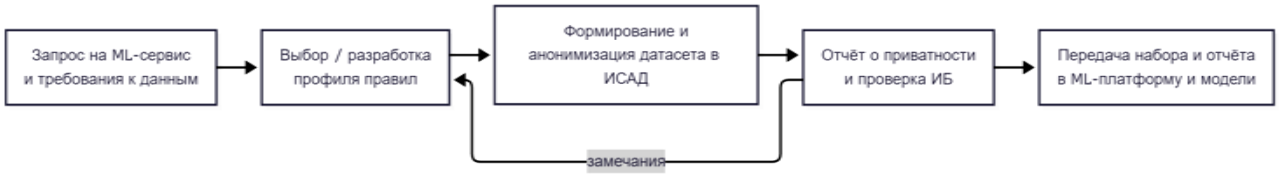

Рис. 2. Целевой процесс подготовки данных с контрольными точками приватности

Fig. 2. Target data preparation process with privacy control points

Сначала бизнес-заказчик и владелец продукта формулируют запрос на ML-сервис, цель использования данных и ограничения.

Инженер по данным и аналитик уточняют требования к набору: список атрибутов, объем, источники, допустимую задержку обновления, формируя пространство потенциальных квазиидентификаторов и чувствительных атрибутов.

Далее выбирается или создается профиль правил анонимизации. При наличии типового профиля он адаптируется под задачу (квазиидентификаторы, целевые k, l, t). Если подходящего профиля нет, инициируется разработка нового с последующим рецензированием и утверждением.

После выбора профиля инженер по данным формирует исходный датасет из производственных источников и регистрирует его

в ИСАД. Применение профиля образует первую контрольную точку: фиксируются версии профиля, параметры запуска и исходного набора.

Затем ИСАД выполняет анонимизацию и расчет метрик приватности, формируя отчёт с достигнутыми значениями k-анонимности, l-разнообразия и t-близости, а также сведениями о подавлениях и обобщениях. Специалист по ИБ и владелец профиля анализируют отчет и принимают решение: допускается ли набор к использованию или требуется корректировка профиля/состава признаков. Это вторая контрольная точка приватности.

Только после успешного прохождения этих шагов анонимизированный набор и отчет передаются в ML-платформу для обучения и валидации моделей. Каждая версия модели опирается на формально описанный и проверенный набор, а история изменений правил и параметров приватности сохраняется для воспроизводимости и аудита.

Целевая архитектура ИСАД реализуется как трехслойная система. Верхний уровень – слой представления: веб-интерфейс для специалистов по данным, ИБ и владельцев продуктов, а также внешние API для интеграции с оркестраторами пайплайнов. Через этот слой инициируются операции регистрации наборов, выбора и применения профилей, расчета метрик приватности и формирования отчетов (рис. 3).

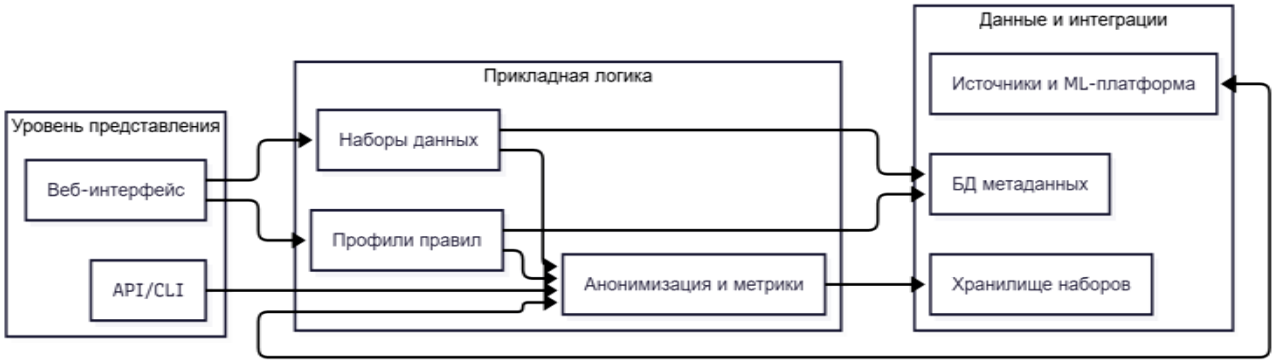

Рис. 3. Многослойная архитектура информационной системы анонимизации данных

Fig. 3. Multilayer architecture of the data anonymization information system

Средний уровень образует слой прикладной логики: движок анонимизации, реализующий преобразования атрибутов по профилю; сервис вычисления метрик приватности и потерь качества; компоненты управления ролями и журналирования. Нижний уровень – хранилища сырых и анонимизированных наборов, профилей правил и метаданных, а также коннекторы к корпоративным источникам и ML-платформе.

Интеграция с ML-конвейером реализуется через API ИСАД: конвейер регистрирует сырые выборки, выбирает или получает утвержденный профиль, инициирует анонимизацию и получает анонимизированный набор с отчетом о приватности. Идентификаторы версий профиля, набора и параметров запуска фиксируются в системах управления конфигурацией и журналирования, что обеспечивает воспроизводимость экспериментов и позволяет прослеживать влияние изменений правил на качество моделей и риск раскрытия.

Профиль правил анонимизации – формализованный набор параметров и преобразований для класса наборов данных или типовой аналитической задачи. В него входят перечни прямых идентификаторов с методами удаления или псевдонимизации, квазиидентификаторы с допустимыми схемами обобщения и подавления, целевые значения k, l, t для различных сегментов, ограничения на искажения (долю подавлений, степень укрупнения категорий) и дополнительные правила (запретные комбинации атрибутов).

Профиль связывается с ML-задачами и типами источников, обеспечивая повторное использование согласованных правил и единый подход к приватности. Разработка

нового профиля требуется при появлении новых классов данных или ужесточении требований ИБ. Жизненный цикл профиля (рис. 4) включает инициирование, разработку, согласование, апробацию и эксплуатацию.

Рис. 4. Жизненный цикл профиля правил анонимизации данных

Fig. 4. Lifecycle of the data anonymization rule profile

На этапе инициирования формулируется потребность в новом профиле или корректировке существующего. Затем подготавливается проект: описываются атрибуты, целевые k, l, t и планируемые преобразования. Проект проходит внутреннее рецензирование у специалистов по данным и ИБ, после чего профиль проверяется на репрезентативной выборке обезличенных сэмплов с оценкой метрик приватности и потерь качества. По результатам апробации профиль дорабатывается или утверждается и переводится в эксплуатацию. В эксплуатации ведутся журнал применения и периодический аудит; при выявлении проблем или изменении требований запускается новый цикл, при этом предыдущие версии сохраняются для воспроизводимости и ретроспективного анализа.

Воспроизводимость решений по анонимизации – ключевое требование к ИСАД. Каждая операция анонимизации однозначно связывается с версией исходного набора, профиля и параметров запуска; соответствующие идентификаторы сохраняются в метаданных и конфигурации ML-экспериментов. Журналирование фиксирует, кто и когда применял профиль, к какому набору, какие значения k, l, t достигнуты, а также предупреждения и ошибки, дополняя записи ссылками на отчеты о приватности и результаты аудита.

Аудит включает регулярный анализ журналов, выборочные проверки отчетов и сопоставление достигнутых метрик с целевыми значениями профилей и актуальными требованиями регуляторов. При обнаружении отклонений или новых рисков инициируется пересмотр профилей и корректировка процесса. Совместное использование версионирования, журналирования и аудита обеспечивает прослеживаемость решений и снижает вероятность незаметного нарушения политик анонимизации.

Предложенный методический каркас отличается от типичных решений тем, что объединяет модели приватности, архитектуру ИС и процессы подготовки данных для ML-проектов в единую рамку. Вместо того чтобы оставлять выбор преобразований на усмотрение разработчиков и фиксировать его фрагментарно, профили правил выступают централизованным объектом управления, формально связанным с атрибутами наборов, целевыми k, l, t и метриками потерь качества [5].

Специализированные инструменты статистической анонимизации и оценки риска раскрытия, как правило, ориентированы на разовые сценарии публикации для внешних потребителей [5] и лишь частично учитывают жизненный цикл ML-моделей. Подходы, ориентированные на поддержку машинного обучения [9], фокусируются на алгоритмах и инфраструктуре экспериментов, но менее подробно рассматривают организацию ролей, жизненный цикл профилей и требования к журналированию. В отечественных работах по паспортам наборов данных [11] и протоколам анонимизации [12] основной акцент делается на нормативных и процедурных аспектах [13]; предлагаемый каркас дополняет их архитектурными и технологическими механизмами интеграции с ML-конвейером и применимости в условиях ограниченных, преимущественно отечественных инфраструктур [15].

Выводы

В работе предложен методический каркас архитектуры системы анонимизации данных,

изначально встроенной в жизненный цикл проектов машинного обучения в корпоративном контуре. Каркас опирается на синтаксические модели приватности (k-анонимность, l-разнообразие, t-близость) и разбиение атрибутов на прямые идентификаторы, квазиидентификаторы и чувствительные атрибуты, что позволяет задать формальные критерии допустимого риска реидентификации.

Сформулированы роли и зоны ответственности участников процесса, описан целевой процесс подготовки данных с фиксированными контрольными точками приватности, а также многослойная архитектура ИС анонимизации данных, интегрированная с ML-конвейером. Введено понятие профиля правил анонимизации и описан его жизненный цикл: инициирование, рецензирование, апробация на обезличенных сэмплах, утверждение, эксплуатация и аудит.

Сопоставление с существующими решениями демонстрирует, что предложенный подход смещает фокус с разовой обработки выгрузок на долговременное управление правилами приватности в составе промышленного ML-цикла и может быть реализован в отечественных технологических стэках. Практическая значимость состоит в возможности проектировать и оценивать решения по анонимизации на уровне процессов и архитектуры, не обращаясь к реальным данным, а также в создании основы для последующей пилотной реализации и расширения на другие классы данных и модели приватности.

Библиографические ссылки

1. Slijepčević D., Henzl M., Klausner L.D., Dam T., Kieseberg P., Zeppelzauer M. k-Anonymity in Practice: How Generalisation and Suppression Affect Machine Learning Classifiers // Computers & Security. 2021. Vol. 111. Art. 102488. DOI: 10.1016/j.cose.2021.102488.

2. Ni C., Cang L.S., Gope P., Min G. Data Anonymization Evaluation for Big Data and IoT Environment // Information Sciences. 2022. Vol. 605. P. 381–392. DOI: 10.1016/j.ins.2022.05.040.

3. Sweeney L. k-Anonymity: A Model for Protecting Privacy // International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems. 2002. Vol. 10, No. 5. P. 557–570. DOI: 10.1142/S0218488502001648.

4. Machanavajjhala A., Kifer D., Gehrke J., Venkitasubramaniam M. ℓ-Diversity: Privacy Beyond k-Anonymity // ACM Transactions on Knowledge Discovery from Data. 2007. Vol. 1, No. 3. Art. 3.DOI: 10.1145/1217299.1217302.

5. Li N., Li T., Venkatasubramanian S. t-Closeness: Privacy Beyond k-Anonymity and ℓ-Diversity // Proceedings of the 23rd IEEE International Conference on Data Engineering. 2007. P. 106–115.DOI: 10.1109/ICDE.2007.367856.

6. Majeed A., Lee S. Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey // IEEE Access. 2021. Vol. 9. P. 8512–8545. DOI: 10.1109/ACCESS.2020.3045700.

7. El Mestari S.Z., Lenzini G., Demirci H. Preserving Data Privacy in Machine Learning Systems // Computers & Security. 2024. Vol. 137. Art. 103605.DOI: 10.1016/j.cose.2023.103605.

8. Domingo-Ferrer J., Mateo-Sanz J.M. Practical Data-Oriented Microaggregation for Statistical Disclosure Control // IEEE Transactions on Knowledge and Data Engineering. 2002. Vol. 14, No. 1. P. 189–201.DOI: 10.1109/69.979982.

9. Caruccio L., Desiato D., Polese G., Tortora G., Zannone N. A Decision-Support Framework for Data Anonymization with Application to Machine Learning Processes // Information Sciences. 2022. Vol. 613. P. 1–32. DOI: 10.1016/j.ins.2022.09.004.

10. Gadotti A., Rocher L., Houssiau F., Creţu A.-M., de Montjoye Y.-A. Anonymization: The Imperfect Science of Using Data While Preserving Privacy // Science Advances. 2024. Vol. 10, No. 29. Art. eadn7053.DOI: 10.1126/sciadv.adn7053.

11. *Борисов Р. С., Ефименко А. А.* Паспорт наборов данных и результатов исследований для публикации в открытых источниках // Правовая информатика. 2022. № 2. С. 66–79.DOI: 10.21681/1994-1404-2022-2-66-79.

12. *Борисов Р. С., Ефименко А. А*. Протокол анонимизации наборов данных для публикации в открытых источниках // Правовая информатика. 2023. № 2. С. 54–66.DOI: 10.21681/1994-1404-2023-2-54-66.

13. *Борисов С. А., Босов А. А., Иванов Д. Е.* Применение имитационного компьютерного моделирования к задаче обезличивания персональных данных. Оценка состояния и основные положения // Программирование. 2023. № 4. С. 58–74.DOI: 10.31857/S0132347423040040.

14. *Борисов С. А., Босов А. А., Иванов Д. Е.* Применение имитационного компьютерного моделирования к задаче обезличивания персональных данных. Модель и алгоритм обезличи-

вания методом синтеза // Программирование. 2023. № 5. С. 19–34.DOI: 10.31857/S0132347423050023.

15. *Ловцов Д. А.* Теория защищенности информации в эргасистемах: монография. М. : РГУП, 2021. 276 с.

References

1. Slijepčević D., Henzl M., Klausner L.D., Dam T., Kieseberg P., Zeppelzauer M. k-Anonymity in Practice: How Generalisation and Suppression Affect Machine Learning Classifiers // Computers & Security. 2021. Vol. 111. Art. 102488. DOI: 10.1016/j.cose.2021.102488.

2. Ni C., Cang L.S., Gope P., Min G. Data Anonymization Evaluation for Big Data and IoT Environment // Information Sciences. 2022. Vol. 605. P. 381–392. DOI: 10.1016/j.ins.2022.05.040.

3. Sweeney L. k-Anonymity: A Model for Protecting Privacy // International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems. 2002. Vol. 10, No. 5. P. 557–570. DOI: 10.1142/S0218488502001648.

4. Machanavajjhala A., Kifer D., Gehrke J., Venkitasubramaniam M. ℓ-Diversity: Privacy Beyond k-Anonymity // ACM Transactions on Knowledge Discovery from Data. 2007. Vol. 1, No. 3. Art. 3.DOI: 10.1145/1217299.1217302.

5. Li N., Li T., Venkatasubramanian S. t-Closeness: Privacy Beyond k-Anonymity and ℓ-Diversity // Proceedings of the 23rd IEEE International Conference on Data Engineering. 2007. P. 106–115.DOI: 10.1109/ICDE.2007.367856.

6. Majeed A., Lee S. Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey // IEEE Access. 2021. Vol. 9. P. 8512–8545. DOI: 10.1109/ACCESS.2020.3045700.

7. El Mestari S.Z., Lenzini G., Demirci H. Preserving Data Privacy in Machine Learning Systems. Computers & Security. 2024;137:103605. DOI: 10.1016/j.cose.2023.103605.

8. Domingo-Ferrer J., Mateo-Sanz J.M. Practical Data-Oriented Microaggregation for Statistical Disclosure Control. IEEE Transactions on Knowledge and Data Engineering. 2002;14(1):189–201.DOI: 10.1109/69.979982.

9. Caruccio L., Desiato D., Polese G., Tortora G., Zannone N. A Decision-Support Framework for Data Anonymization with Application to Machine Learning Processes. Information Sciences. 2022;613:1–32. DOI: 10.1016/j.ins.2022.09.004.

10. Gadotti A., Rocher L., Houssiau F., Creţu A.-M., de Montjoye Y.-A. Anonymization: The Imperfect Science of Using Data While Preserving Privacy. Science Advances. 2024;10(29):eadn7053. doi:10.1126/sciadv.adn7053. DOI: 10.1126/sciadv.adn7053.

11. Borisov R.S., Efimenko A.A. [Data Set and Research Results Passport for Publication in Open Sources]. Legal Informatics. 2022; 2:66–79 (in Russ.). DOI: 10.21681/1994-1404-2022-2-66-79.

12. Borisov R.S., Efimenko A.A. [Data Set Anonymization Protocol for Publication in Open Sources]. Legal Informatics. 2023; 2:54–66 (in Russ.). DOI: 10.21681/1994-1404-2023-2-54-66.

13. Borisov S.A., Bosov A.A., Ivanov D.E. [Application of Simulation Computer Modelling to the Problem of Personal Data Depersonalization]: State-of-the-Art Assessment and Basic Provisions. Programming and Computer Software. 2023; 4:58–74 (in Russ.). DOI: 10.31857/S0132347423040040.

14. Borisov S.A., Bosov A.A., Ivanov D.E. [Application of Simulation Computer Modelling to the Problem of Personal Data Depersonalization]: Model and Synthesis-Based Depersonalization Algorithm. Programming and Computer Software. 2023; 5:19–34 (in Russ.). DOI: 10.31857/S0132347423050023.

15. Lovtsov D.A. [Theory of Information Security in Ergasystems]. Moscow: Russian State University of Justice; 2021. 276 p. (in Russ.).

* * *

Methodological Framework for the Architecture of Data Anonymization for Machine Learning Tasks

E. M. Dyukina, Student, MIREA – Russian Technological University, Moscow, Russia
Y. V. Silaev, Senior Lecturer, MIREA – Russian Technological University, Moscow, Russia
O. M. Perminova, PhD, Associate Professor, MIREA – Russian Technological University, Moscow, Russia

This paper presents a methodological framework for the architecture of a tabular-data anonymization system embedded into the lifecycle of corporate machine learning projects and data preparation workflows.

We propose a process- and stage-based approach to designing an anonymization pipeline that establishes a unified terminology, requirements, and constraints, and formalizes rule profiles for pseudonymization, generalization, masking, and suppression across different attribute classes: direct identifiers, quasi-identifiers, and sensitive attributes. Building on the k-anonymity, l-diversity, and t-closeness models, we introduce "privacy checkpoints" at which attainment of target metric values, suppression rates, and the level of generalization are evaluated. At each checkpoint, a privacy report is generated containing the observed k, l, and t values, warnings, and explanatory notes, enabling an informed decision on whether a dataset can be admitted into the ML pipeline. The paper also shows how to pre-validate profiles and parameters on representative anonymized samples without accessing actual production datasets, thereby reducing disclosure risks at early approval stages. The framework further specifies roles and responsibility boundaries (data owner, data engineer, analyst/data scientist, ML engineer, information security specialist, and system administrator) and a three-tier system architecture with a web interface and an API suitable for integration with pipeline orchestrators. Treating rule profiles as versioned artifacts—alongside dataset versions, run parameters, metadata storage, operation logging, and periodic auditing—ensures reproducibility of training data preparation and end-to-end traceability of anonymization impacts on model quality. The framework can serve as a reference model for an initial pilot implementation and subsequent expansion to other data classes and privacy governance practices in ML projects.

Keywords: anonymization, privacy, architecture, de-identification, security, k-anonymity.

Получено: 21.01.26

Образец цитирования

Дюкина Э. М., Силаев Ю. В., Перминова О. М. Методическая основа архитектуры анонимизации данных для задач машинного обучения // Интеллектуальные системы в производстве. 2026. Т. 24, № 1. С. 4–12. DOI: 10.22213/2410-9304-2026-1-4-12.

For Citation

Dyukina E.M., Silaev Y.V., Perminova O.M. [Methodological Framework for the Architecture of Data Anonymization for Machine Learning Tasks]. *Intellektual'nye sistemy v proizvodstve*. 2026, vol. 24, no. 1, pp. 4-12 (in Russ.). DOI: 10.22213/2410-9304-2026-1-4-12.