



Обезличивание персональных данных в банковской сфере: анализ методов и выбор стратегии внедрения

Е.К. Баранова, Я.В. Лебедкина

Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

АННОТАЦИЯ

В статье рассматривается актуальная проблема обезличивания персональных данных в кредитно-финансовых организациях (КФО) в контексте ужесточения регуляторных требований, в частности Приказа Роскомнадзора № 140. Проведен анализ классических и современных методов обезличивания (маскирование, псевдонимизация, генерация синтетических данных и др.) с точки зрения их применимости в банковской среде, где критически важны сохранение формата данных, референциальная целостность и высокая производительность. Дана сравнительная оценка трех современных отечественных решений: DataMask, «Гарда Data Masking» и N1 AI. Выявлены их системные ограничения, включая потенциальное несоответствие новым нормативным актам, недостаточную гибкость для уникальных банковских сущностей и высокую стоимость владения. На основе проведенного анализа обосновывается стратегическая целесообразность разработки специализированного внутрикорпоративного инструмента обезличивания, который гарантирует полное соответствие регулированию, максимальную адаптивность к бизнес-процессам банка и долгосрочную экономическую эффективность. Для кредитно-финансовой организации характерна обработка обширного массива структурированных персональных данных (ПДн), совмещающих признаки общих, иных данных и сведений, составляющих банковскую тайну. Данные сведения, как правило, хранятся в реляционных базах данных в формализованном виде (отдельные поля для номера паспорта, телефона, счета и т.д.), что, с одной стороны, упрощает их автоматизированный поиск, а с другой — требует применения строгих мер защиты, к которым относится и безопасное обезличивание для использования в непроизводственных средах. Это определяет ключевые требования к рассматриваемой системе: необходимость точного обнаружения полей различных категорий финансово-идентифицирующей информации и применение алгоритмов маскировки, обеспечивающих необратимость преобразования при сохранении структурной целостности и формата данных для корректной работы тестовых систем.

Ключевые слова: обезличивание персональных данных; псевдонимизация; маскирование данных; банковские информационные системы; информационная безопасность; защита информации

Для цитирования: Баранова Е.К., Лебедкина Я.В. Обезличивание персональных данных в банковской сфере: анализ методов и выбор стратегии внедрения. *Цифровые решения и технологии искусственного интеллекта*. 2026;2(3):26-33. DOI: 10.26794/3030-7097-2026-2-3-26-33

ORIGINAL PAPER

Depersonalization of Personal Data in the Banking Sector: Analysis of Methods and Selection of an Implementation Strategy

Е.К. Baranova, Ya.V. Lebedkina

Financial University under the Government of the Russian Federation, Moscow, Russian Federation

ABSTRACT

This article examines the pressing issue of personal data anonymization in credit and financial institutions (CFIs) in the context of tightening regulatory requirements, in particular, Roskomnadzor Order No. 140. It analyzes classic and modern anonymization methods (masking, pseudonymization, synthetic data generation, etc.) for their applicability in a banking environment where preserving data formats, referential integrity, and high performance are critical. A comparative assessment of three modern domestic solutions is provided: DataMask, Garda Data Masking, and N1 AI. Their systemic limitations are identified, including potential non-compliance with new regulations, insufficient flexibility for unique banking entities, and high cost of ownership. Based on this analysis, the strategic feasibility of developing a specialized internal anonymization tool is substantiated. This tool guarantees full regulatory compliance, maximum adaptability to the bank's business processes, and long-term economic efficiency. A credit and financial institution is characterized by processing an extensive array of structured personal data (PD), which combines the features of general, other data, and information that

constitutes bank secrecy. This information is typically stored in relational databases in a formalized format (separate fields for passport number, phone number, account number, etc.), which, on the one hand, simplifies their automated search, but on the other hand, requires strict protection measures, including secure anonymization for use in non-production environments. This determines the key requirements for the system under consideration: the need to accurately detect fields of various categories of financial and identifying information, and the use of masking algorithms that ensure irreversible conversion while preserving the structural integrity and data format for the correct operation of test systems.

Keywords: anonymization of personal data; pseudonymization; data masking; banking information systems; information security; information protection

For citation: Baranova E.K., Lebedkina Ya.V. Depersonalization of personal data in the banking sector: Analysis of methods and selection of an implementation strategy. *Digital Solutions and Artificial Intelligence Technologies*. 2026;2(3):26-33. DOI: 10.26794/3030-7097-2026-2-3-26-33

ВВЕДЕНИЕ

В современной цифровой экономике данные стали ключевым активом, а их защита — одним из главных приоритетов, особенно для кредитно-финансовых организаций. Обработывая огромные массивы персональных данных (ПДн), банки несут строгую юридическую ответственность за их конфиденциальность. Федеральный закон «О персональных данных»¹ устанавливает базовые принципы обработки ПДн, а обезличивание признается одним из основных методов приведения их в соответствие с законом. Согласно статье 3 Федерального закона «О персональных данных», обезличивание — это действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту.

Однако на практике перед ИТ-специалистами и архитекторами банков встает сложный комплекс задач. С одной стороны, необходимо безусловно выполнять регуляторные требования, которые постоянно ужесточаются (яркий пример — детализированный Приказ Роскомнадзора № 140², введенный с 01.09.2025 г.). С другой — обезличенные данные должны сохранять свою прикладную ценность для тестирования программного обеспечения, анализа бизнес-процессов и работы с данными в производственных средах. Традиционное решение — покупка готового коммерческого продукта — все чаще наталкивается на специфику высоко динамичной и сложно устроенной банковской ИТ-инфраструктуры.

Цель данной статьи — проанализировать существующие методы и рыночные решения для

обезличивания данных, оценить их применимость в условиях конкретных требований банковского сектора и обосновать выбор стратегии внедрения. Работа построена на сопоставлении функциональных возможностей, нормативного соответствия и экономических аспектов, что позволит сформировать объективный взгляд на проблему и предложить прагматичный путь ее решения.

КЛАССИФИКАЦИЯ МЕТОДОВ ОБЕЗЛИЧИВАНИЯ

Современные подходы и нормативные акты, такие как Приказ Роскомнадзора № 140, позволяют систематизировать методы обезличивания по их принципу действия и области применения (см. рисунок).

Наибольшее распространение на практике получили статические методы. Данные методы предполагают необратимое преобразование данных в рамках отдельного набора, например, копии производственной базы, с созданием нового, обезличенного массива информации. К ним относятся:

- **Маскирование.** Этот метод заключается в частичном или полном сокрытии оригинального значения путем замены символов на статические или динамические шаблоны. Различают несколько видов:

- а) маскирование по формату: замена части символов на фиксированные знаки (например, «*» или «X»). Например, номер паспорта «4012 123456» преобразуется в «XXXX XXXXX6». Данный метод прост в реализации, но может снизить полезность данных для тестирования бизнес-логики, зависящей от формата;

- б) детерминированное маскирование: замена исходного значения на одно и то же псевдонимизированное значение во всех системах и наборах данных. Например, ФИО «Иванов Сергей» всегда преобразуется в «Петров Андрей». Это критически важно для сохранения референциальной целостности между связанными таблицами базы данных;

- в) случайное маскирование: замена на случайное, но правдоподобное значение из заданного домена (словаря). Например, замена реального имени на случайное из списка распространенных имен.

¹ Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.02.2025) «О персональных данных». URL: <http://www.kremlin.ru/acts/bank/24154>

² Приказ Роскомнадзора от 19.06.2025 № 140 «Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных, за исключением случаев, указанных в п. 9.1 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»». URL: <http://publication.pravo.gov.ru/document/0001202508010002>

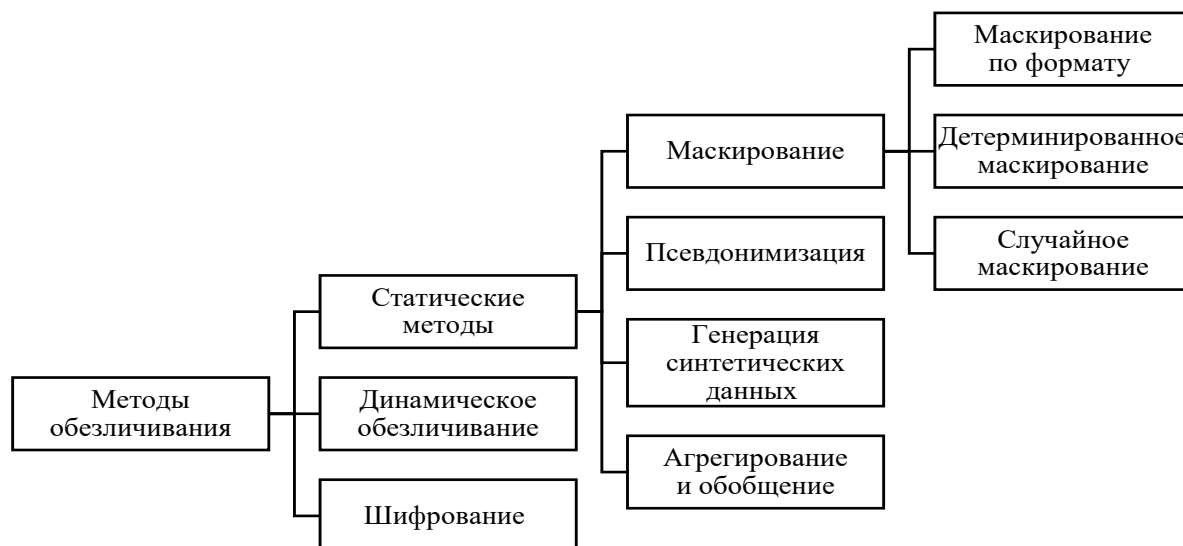
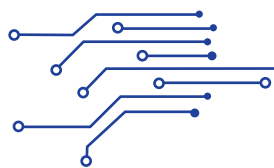


Рис. / Fig. Классификация методов обезличивания / Classification of Depersonalization Methods

Источник / Source: составлено авторами / Compiled by the authors.

- **Псевдонимизация.** В отличие от простого маскирования, псевдонимизация часто предполагает использование алгоритмов шифрования или хеширования с ключом («солью») для замены прямого идентификатора на устойчивый псевдоним. Исходные данные могут быть восстановлены только при наличии ключа, хранящегося отдельно. Это основной метод, соответствующий концепции GDPR (General Data Protection Regulation). Пример: замена e-mail «client@domain.com» на детерминированный хеш «a1b2c3d4e5».

- **Генерация синтетических данных** предполагает создание полностью искусственного, но статистически похожего на реальный набор данных с помощью специальных алгоритмов. Синтетические данные не содержат реальной информации о клиентах, что полностью исключает риски, однако их создание, адекватно отражающее все сложности и аномалии реальных данных, является нетривиальной задачей.

- **Агрегирование и обобщение.** Данные заменяются на обобщенные категории или статистические показатели. Например, точный возраст заменяется на возрастную группу «25–35 лет», а конкретная сумма транзакции — на диапазон «от 10 000 до 50 000 руб.». Метод эффективен для аналитических целей, но бесполезен для функционального тестирования приложений.

Динамическое обезличивание предполагает маскировку данных «на лету» в момент выполнения запроса к базе данных, без изменения самих хранимых данных. Правила маскирования применяются на уровне СУБД или промежуточного программного слоя в зависимости от прав доступа пользователя. Например, оператор колл-центра ви-

дит только последние четыре цифры номера карты, в то время как сотрудник бэк-офиса имеет доступ к полному номеру. Этот метод оптимален для разграничения доступа в производственных системах, но не подходит для создания обезличенных копий для тестирования.

Криптографическое преобразование данных является надежным методом защиты. Для целей обезличивания может применяться форматированное шифрование, которое позволяет сохранить исходный формат и тип данных (например, шифрует номер кредитной карты, оставляя валидный с точки зрения контрольной суммы номер). Восстановление данных возможно только при наличии ключа дешифрования.

При разработке системы обезличивания для кредитно-финансовых организаций (КФО) необходимо учитывать специфические требования [1–3].

1. Сохранение формата и валидности: обезличенные номера паспортов, ИНН, банковских карт должны сохранять контрольные суммы и структуру для успешного прохождения валидации в тестовых контурах.

2. Обеспечение референциальной целостности: связи между таблицами (например, «client_id» в таблицах «clients» и «accounts») не должны быть разорваны после обезличивания.

3. Детерминированность: при необходимости проведения согласованного тестирования одинаковые исходные данные должны маскироваться в одинаковые значения при каждом запуске процесса.

4. Необратимость: в соответствии с Приказом № 140 процесс должен исключать возможность восстановления ПДн без специальных средств, хранящихся отдельно.



5. Производительность: алгоритмы должны эффективно обрабатывать большие объемы данных, характерные для КФО.

Таким образом, для реализации скрипта обезличивания — наиболее целесообразным представляется применение комбинации статических методов, соответствующих Приказу Роскомнадзора № 140. Ядро системы будет составлять маскирование по формату или псевдонимизацию по словарям для атрибутов, требующих сохранения правдоподобия (ФИО, адреса, номера документов)³ [4]. Такой подход позволит обеспечить баланс между требованиями безопасности, функциональной полезности обезличенных данных и производительности.

АНАЛИЗ СУЩЕСТВУЮЩИХ РЕШЕНИЙ И ИХ ПРИМЕНИМОСТЬ В БАНКЕ

В условиях ужесточения регуляторных требований и роста угроз информационной безопасности рынок предлагает КФО ряд готовых решений для обезличивания персональных данных. Выбор стратегии — внедрение коммерческого продукта или разработка собственного инструмента — требует тщательного анализа существующих предложений [5–7], а именно — анализ трех актуальных отечественных решений: DataMask (Secret Technologies)⁴, «Гарда Data Masking» (Гарда Технологии)⁵ и N1 AI (ООО «Умные решения»)⁶. Целью анализа является оценка их функциональной полноты, соответствия специфическим требованиям банковского сектора и обоснование экономической и технической целесообразности разработки специализированного внутрикорпоративного решения.

Современный рынок решений для защиты данных [8–10] можно условно разделить на два класса: системы, ориентированные на работу со структурированными данными в СУБД, и платформы, использующие искусственный интеллект (ИИ) для обработки неструктурированной информации.

1. DataMask (Secret Technologies)

Решение позиционируется как универсальный инструмент для автоматического обнаружения и маскирования более 30 типов чувствительных данных в реляционных базах данных. К его декларируемым преимуществам относятся:

- автоматизация, т.е. сквозной процесс обнаружения и маскирования;
- обеспечение референциальной целостности данных между связанными таблицами;
- поддержка различных СУБД (PostgreSQL, Oracle, MS SQL) и возможность встраивания в конвейеры CI/CD через API;
- реалистичность, однородность, необратимость.

2. «Гарда Data Masking» (Гарда Технологии)

Более зрелый продукт, представленный как отраслевой стандарт для безопасной передачи данных третьим лицам. Его отличительные черты:

- автоматическое выявление обширного спектра данных: от персональных (ФИО, паспорт) до финансовых (номера счетов, карт) и юридических (реквизиты организаций);
- заявленное соответствие широкому кругу стандартов, включая Федеральный закон «О персональных данных» GDPR, PCI DSS, СТО БР ИББС;
- поддержка пользовательских алгоритмов маскирования и ролевой модели доступа.

3. N1 AI (ООО «Умные решения»)

Данное решение представляет собой принципиально иной подход, основанный на технологиях искусственного интеллекта и машинного обучения, сфокусированный на обработке текстовых данных. Основные особенности:

- фокус на неструктурированные данные: предназначен для обезличивания текстов, документов (PDF, Word), датасетов, что актуально для сканов договоров, корреспонденции, расшифровок переговоров;
- использование NLP-моделей (Natural Language Processing), обученных на русском языке, с заявленной точностью распознавания сущностей свыше 99%, включая обработку опечаток;
- предлагает как полное замещение, так и псевдонимизацию с идентификаторами, а также детектирование позиций ПДн;
- предоставление REST API для обезличивания в реальном времени и возможность дообучения модели на данных заказчика.

Для системной оценки необходимо провести сравнение решений по ключевым критериям [11, 12], критически важным для банка. Результаты представлены в *таблице*.

Проведенный анализ выявляет ряд системных ограничений готовых решений в контексте высокоспециализированной среды КФО:

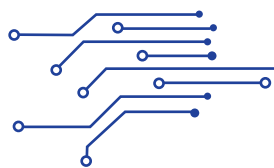
1. Проблема гарантированного соответствия актуальному регулированию. Приказ Роскомнадзора № 140 устанавливает детализированные, юридически обязательные требования к методам и необратимости обезличивания. Большинство

³ Шаблинский И.Г. Правовое регулирование информационных отношений в сфере обработки персональных данных. Учебное пособие для вузов. М.: Издательство Юрайт; 2024.

⁴ Диджитал Маскинг. URL: <https://d-mask.ru>

⁵ Garda.ai. Маскирование данных. URL: <https://garda.ai/products/data-protection/datamasking>

⁶ Портал о технологиях больших данных N1.AI. URL: <https://n1ai.ru/bigdata>



Сравнительный анализ решений для обезличивания данных /
Comparative Analysis of Solutions for Data Anonymization

Критерий анализа / The Criterion of Analysis	DataMask	«Гарда Data Masking»	N1 AI	Ключевые требования для банка / Key Requirements for the Bank
Основной объект обработки	Структурированные данные в СУБД		Неструктурированные/ текстовые данные (документы, текст)	Структурированные данные в СУБД
Ключевая технология	Детерминированные алгоритмы, словари, правила	Детерминированные алгоритмы, шаблоны	Модели искусственного интеллекта (NLP)	Детерминированные алгоритмы, словари, правила, шаблоны
Соответствие Приказу РКН № 140	Не заявляется производителем. Требуется валидации		Требуется глубокой валидации. Объяснимость и необратимость ИИ- методов — сложная задача	Гарантированное и документально подтвержденное соответствие Приказу Роскомнадзора № 140
Покрывание специфических банковских сущностей	Ограничено предустановленными шаблонами. Расширение возможно через вендора	Широкий, но фиксированный набор. Пользовательские правила требуют настройки	Возможно через дообучение модели, что требует экспертизы Data Science	Полное и адаптивное. Необходима возможность мгновенного добавления правил для новых продуктов
Гибкость и скорость адаптации	Зависит от вендора. Обновление правил — часть процесса поддержки	Настройка параметров доступна, изменение ядра — у вендора	Высокая за счет дообучения, но требует данных и вычислительных ресурсов	Максимальная независимость от цикла разработки вендора. Возможность изменений силами команды банка
Экономическая модель	Высокие CAPEX (лицензии) и OPEX (ежегодная поддержка, обновления)	Индивидуальный расчет, масштабируемая стоимость	Лицензирование/ подписка, возможны затраты на дообучение и инфраструктуру для ИИ	Первоначальные инвестиции в разработку с последующей минимальной стоимостью владения

Источник / Source: составлено авторами / Compiled by the authors.

коммерческих решений были разработаны до его выхода. Их адаптация под новые требования носит для банка характер «черного ящика» и требует дополнительных затрат на валидацию. Для ИИ-решений, подобных N1 AI, доказательство необратимости и объяснимости алгоритмов представляет отдельную научно-практическую проблему.

2. Бизнес-процессы банка порождают уникальные категории конфиденциальных данных, не входящие в стандартные шаблоны:

- номера внутренних кредитных договоров, заявок, депозитных счетов со сложной структурой;

- коды валютных операций, признаки бенефициарного владения;
- структурированные описания залогового имущества.

Эффективное и оперативное управление правилами для таких сущностей в рамках «коробочного» продукта затруднено.

3. Инфраструктура банка — сложный организм с унаследованными системами, строгими регламентами переноса данных между изолированными контурами (Prod/Dev/Test). Интеграция стороннего продукта, даже с API, часто превращается в длительный и дорогой проект



по адаптации банка под логику работы вендора, а не наоборот.

Учитывая выявленные системные ограничения коммерческих продуктов, разработка собственной автоматизированной системы обезличивания представляется для банка не только целесообразной, но и стратегически необходимой.

ВЫВОДЫ

Проведенное исследование позволяет сделать ряд значимых выводов относительно обезличивания данных в банковской сфере. Современные нормативные требования, особенно Приказ Роскомнадзора № 140, задают высокую планку для методов обезличивания, делая акцент на их необратимости и доказательной базе. Ни один из рассмотренных классических методов (маскирование, псевдонимизация, агрегирование) не является универсальным; их эффективное применение требует комбинированного подхода, тщательно настроенного под типы обрабатываемых данных и целевые сценарии использования.

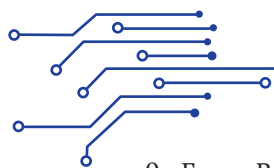
Сравнительный анализ ведущих отечественных коммерческих решений (DataMask, «Гарда Data Masking», N1 AI) демонстрирует, что, несмо-

тря на заявленную функциональность, они в полной мере не отвечают уникальным запросам крупного банка. Ключевыми проблемами остаются негибкость в адаптации под специфические банковские сущности, сложности с гарантированным соответствием последним редакциям нормативных актов, а также высокие совокупные затраты на интеграцию и владение [13, 14].

Таким образом, для кредитно-финансовой организации, обладающей развитой ИТ-экспертизой, наиболее рациональным и перспективным путем представляется разработка собственной автоматизированной системы обезличивания. Такой подход обеспечит не просто выполнение формальных требований регулятора, но и создаст стратегическое конкурентное преимущество. Он даст банку полный контроль над алгоритмами, позволит мгновенно реагировать на изменения в продуктовой линейке и регулировании, а в долгосрочной перспективе окажется экономически более выгодным, чем зависимость от внешних вендоров. Реализация подобного проекта требует значимых первоначальных инвестиций, но формирует устойчивую основу для безопасной и эффективной работы с данными во всех контурах информационной системы.

СПИСОК ИСТОЧНИКОВ

1. Альмухаметова Э.И., Шаймарданов И.Ф. Актуальность и методы обезличивания персональных данных. В сб.: Передовые инженерные решения в нефтепереработке и нефтехимии. Салават: Уфимский государственный нефтяной технический университет; 2025:261-263. URL: <https://elibrary.ru/ffypro>
2. Алексеев Д.В., Тумбинская М.В. Современные методы обезличивания персональных данных: анализ эффективности и направления развития. В сб.: Цифровые системы и модели: теория и практика проектирования, разработки и использования. Казань: Казанский государственный энергетический университет; 2025:2036-2039. URL: <https://elibrary.ru/wldthv>
3. Колбасов В.В. Персональные данные: обезличивание персональных данных, обрабатываемых в информационных системах персональных данных. *Некоммерческие организации в России*. 2017;1:59-62. URL: <https://elibrary.ru/zegwvv>
4. Кучин И.Ю. Защита конфиденциальности персональных данных с помощью обезличивания. *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*. 2010;2:158-162. URL: <https://elibrary.ru/muyqhf>
5. Полуянова Е.В. Актуальные вопросы, связанные с обезличиванием персональных данных в Российской Федерации. *Тенденции развития науки и образования*. 2024;114-6:36-38. URL: <https://doi.org/10.18411/trnio-10-2024-243>
6. Чепик П.И. Обезличивание персональных данных как способ повышения их защиты при обработке в информационных системах. В сб.: Безопасные информационные технологии. М.: Московский государственный технический университет им. Н.Э. Баумана; 2023:150-153. URL: <https://elibrary.ru/tktuem>
7. Алексеев Д.В., Тумбинская М.В. Современные методы обезличивания персональных данных: анализ эффективности и направления развития. В сб.: Цифровые системы и модели: теория и практика проектирования, разработки и использования. Казань; 2025:2036-2039. URL: <https://elibrary.ru/wldthv>
8. Борисов А.В. Применение имитационного компьютерного моделирования к задаче обезличивания персональных данных. Оценка состояния и Основные положения. *Программирование*. 2023;4:58-74. URL: <https://doi.org/10.31857/S0132347423040040>



9. Бесов В.В., Данилова Э.З., Мекуриа Д.В. Методы обезличивания пользовательских данных: анализ применимости в условиях современных требований к приватности. *Телекоммуникации и информационные технологии*. 2025;12(1):84-89. URL: <https://elibrary.ru/xjkqtn>
10. Мищенко Е.Ю., Соколов А.Н. Алгоритмы реализации методов обезличивания персональных данных в распределенных информационных системах. *Доклады Томского государственного университета систем управления и радиоэлектроники*. 2019;22(1):66-70. URL: <https://doi.org/10.21293/1818-0442-2019-22-1-7-66-70>
11. Малявко А.А., Реутов В.В., Коротких И.В., Шперлинг В.К. Алгоритмы, методы и подходы к обезличиванию и обогащению данных, в том числе персональных. *Безопасность цифровых технологий*. 2022;4(107):9-26. URL: <https://doi.org/10.17212/2782-2230-2022-4-9-26>
12. Гусева Т.М., Карабанова А.Н., Блимготов Т.К. Защита персональных данных путем их обезличивания. В сб.: *Теория и практика применения новых информационных технологий*. Ставрополь: Издательство «АГРУС»; 2020:103-106. URL: <https://elibrary.ru/jssuvn>
13. Маршалко Г.Б., Дали Ф.А., Савиных А.Н. Сравнительный анализ методов обезличивания персональных данных. В сб.: *Методы и технические средства обеспечения безопасности информации*. СПб.; 2022:161-163. URL: <https://elibrary.ru/wppbj>
14. Учаева Е.С., Фот Ю.Д. Исследование методов обезличивания персональных данных. В сб.: *Актуальные вопросы обеспечения комплексной безопасности*. Оренбург; 2025:1570-1574. URL: <https://elibrary.ru/eevaeh>

REFERENCES

1. Almukhametova E.I., Shaimardanov I.F. Relevance and methods of depersonalization of personal data. In: *Advanced engineering solutions in oil refining and petrochemistry*. Salavat: Ufa State Petroleum Technical University; 2025:261-263. URL: <https://elibrary.ru/ffypno> (In Russ.).
2. Alekseev D.V., Tumbinskaya M.V. Modern methods of depersonalization of personal data: analysis of effectiveness and development directions. In: *Digital Systems and Models: theory and practice of design, development and use*. Kazan: Kazan State Power Engineering University; 2025:2036-2039. URL: <https://elibrary.ru/wldthv> (In Russ.).
3. Kolbasov V.V. Personal data: depersonalization of personal data processed in personal data information systems. *Non-profit organizations in Russia*. 2017;1:59-62. URL: <https://elibrary.ru/zegwvv> (In Russ.).
4. Kuchin I.Y. Protection of the confidentiality of personal data through depersonalization. *Bulletin of the Astrakhan State Technical University. Series: Management, Computer Engineering and Computer Science*. 2010;2:158-162. URL: <https://elibrary.ru/muyqhf> (In Russ.).
5. Poluyanov E.V. Topical issues related to depersonalization of personal data in the Russian Federation. *Trends in the Development of Science and Education*. 2024;114-6:36-38. (In Russ.). URL: <https://doi.org/10.18411/trnio-10-2024-243>
6. Chepik P.I. Depersonalization of personal data as a way to increase their protection during processing in information systems. In: *Secure Information technologies*. Moscow: Bauman Moscow State Technical University; 2023:150-153. URL: <https://elibrary.ru/tktuem> (In Russ.).
7. Alekseev D.V., Tumbinskaya M.V. Modern methods of depersonalization of personal data: analysis of effectiveness and development directions. In: *Digital Systems and Models: Theory and practice of design, development and use*. Kazan; 2025:2036-2039. URL: <https://elibrary.ru/wldthv> (In Russ.).
8. Borisov A.V. Application of simulation computer modeling to the problem of depersonalization of personal data. Assessment of the condition and the main provisions. *Programming*. 2023;4:58-74. (In Russ.). URL: <https://doi.org/10.31857/S0132347423040040>
9. Besov V.V., Danilova E.Z., Mekuria D.V. Methods of depersonalization of user data: an analysis of applicability in the context of modern privacy requirements. *Telecommunications and Information Technology*. 2025;12(1):84-89. URL: <https://elibrary.ru/xjkqtn> (In Russ.).
10. Mishchenko E.Yu., Sokolov A.N. Algorithms for implementing methods of depersonalization of personal data in distributed information systems. *Reports of Tomsk State University of Control Systems and Radio Electronics*. 2019;22(1):66-70. (In Russ.). URL: <https://doi.org/10.21293/1818-0442-2019-22-1-7-66-70>
11. Malyavko A.A., Reutov V.V., Korotkov I.V., Shperling V.K. Algorithms, methods and approaches to depersonalization and enrichment of data, including personal data. *Digital Technology Security*. 2022;4(107):9-26. (In Russ.). URL: <https://doi.org/10.17212/2782-2230-2022-4-9-26>

12. Guseva T.M., Karabanova A.N., Blimgotov T.K. Protection of personal data by depersonalization. In: Theory and practice of the application of new information technologies. Stavropol: AGRUS Publishing House; 2020:103-106. URL: <https://elibrary.ru/jssuvm> (In Russ.).
13. Marshalko G.B., Dali F.A., Savinykh A.N. Comparative analysis of methods of depersonalization of personal data. In: Methods and technical means of ensuring information security. St. Petersburg; 2022:161-163. URL: <https://elibrary.ru/wppbj> (In Russ.).
14. Uchaeva E.S., Fot Yu.D. Research of methods of depersonalization of personal data. In: Current issues of ensuring integrated security. Orenburg; 2025:1570-1574. URL: <https://elibrary.ru/eevae> (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Елена Константиновна Баранова — доцент кафедры информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

Elena K. Baranova — Assoc. Prof., Department of Information Security, Financial University under the Government of the Russian Federation, Moscow, Russian Federation

<http://orcid.org/0000-0003-4650-2623>

Автор для корреспонденции / Corresponding author:

ekbaranova@fa.ru

Яна Витальевна Лебедкина — студент бакалавриата кафедры информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

Yana V. Lebedkina — bachelor student, Department of Information Security, Financial University under the Government of the Russian Federation, Moscow, Russian Federation

<http://orcid.org/0000-0002-539-0457>

228958@edu.fa.ru

Заявленный вклад авторов:

Е.К. Баранова — разработка общей концепции статьи, обзор публикаций по заявленной теме.

Я.В. Лебедкина — классификация методов обезличивания ПДн; анализ существующих решений и их применимость в банке.

Authors' declared contributions:

E.K. Baranova — development of the general concept of the article, and review of publications on the stated topic.

Ya.V. Lebedkina — classification of methods for anonymizing personal data; analysis of existing solutions and their applicability in the bank.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Статья поступила 22.04.2026; после рецензирования 10.06.2026; принята к публикации 01.08.2026.

Авторы прочитали и одобрили окончательный вариант рукописи.

The article was submitted on 22.04.2026; revised on 10.06.2026; accepted for publication on 01.08.2026.

The authors read and approved the final version of the manuscript.