Инженерный вестник Дона, №12 (2025)
ivdon.ru/ru/magazine/archive/n12y2025/10596

Методы дифференциальной анонимизации данных на основе доверительной нейронной сети для защиты персональной информации клиентов банка

Д.С. Серезлеев, Ю.К. Абаев

Санкт-Петербургский государственный университет промышленных технологий и дизайна

Аннотация: В статье рассматриваются современные методы защиты персональной информации клиентов банков на основе дифференциальной анонимизации данных с использованием доверительных нейронных сетей. Приводится обзор нормативно-правовой базы, анализ технологических подходов и описание разработанной многоуровневой модели анонимизации, сочетающей криптографические и машинно-обучающие методы. Особое внимание уделено вопросам балансировки между сохранением полезности данных и минимизацией риска раскрытия личности клиента.
Ключевые слова: дифференциальная анонимизация, доверительная нейронная сеть, персональные данные, банковские технологии, защита информации, кибербезопасность.

Введение

Банковская отрасль переживает резкий всплеск киберугроз, приводящих к крупным утечкам персональных сведений клиентов, негативно влияющим на репутацию учреждений, финансовую стабильность и национальную безопасность. Повышение роли цифровой информации и активное использование передовых технологий искусственного интеллекта требуют разработки новых инструментов, обеспечивающих надёжную защиту данных без ущерба для их аналитического потенциала. Актуальность проблемы подчёркивается быстрым развитием цифровых технологий, усилением требований регуляторов и широким распространением дистанционных сервисов, увеличивающих риски кибератак. Таким образом, возникает острая потребность в сбалансированных механизмах защиты, позволяющих минимизировать угрозы и сохранить функциональность данных для эффективного управления бизнесом и повышения конкурентоспособности финансовых институтов.

Целью настоящего исследования является разработка и обоснование метода дифференциальной анонимизации данных на базе доверительной нейронной сети, который обеспечит высокую степень защиты персональной информации клиентов банков без существенной потери её аналитической значимости. Предлагаемый подход предполагает интеграцию математических механизмов дифференциальной приватности с архитектурой доверительных нейронных сетей, что позволит дополнительно контролировать корректность работы алгоритмов и снизить риски манипуляций с моделью.

Для достижения поставленной цели требуется решить ряд задач. Прежде всего необходимо провести комплексный анализ действующей нормативно-правовой базы в области защиты персональных данных, включая национальные стандарты, международные регламенты и отраслевые рекомендации, с тем чтобы обеспечить соответствие предлагаемого метода актуальным правовым требованиям. Далее следует исследовать существующие технологические решения в области анонимизации и защиты данных, выявить их сильные и слабые стороны, а также определить возможности интеграции с современными ИИ-технологиями. Завершающим этапом станет разработка архитектуры и алгоритмов предлагаемой модели анонимизации, а также проведение её тестирования в условиях, максимально приближённых к реальным банковским процессам, для оценки эффективности и устойчивости к возможным угрозам.

Обзор нормативно-правовой базы и современных вызовов

Защита персональных данных в банковской сфере в России базируется на ряде ключевых нормативно-правовых актов, определяющих порядок сбора, обработки, хранения и передачи информации о клиентах. Центральным документом является Федеральный закон № 152-ФЗ «О персональных данных», который устанавливает правовые основы обработки

таких сведений, включая требования к анонимизации и псевдонимизации данных. Особое внимание в законе уделяется принципам минимизации собираемой информации, согласия субъекта на обработку, а также праву на отзыв согласия. Наряду с этим, на уровне отраслевых регуляторов, в частности Банка России, действуют стандарты и рекомендации, направленные на усиление защиты данных при проведении банковских операций и использовании автоматизированных систем скоринга [1, 2]. Существенное влияние на российскую практику оказал опыт Европейского союза в виде Общего регламента по защите данных (General Data Protection Regulation, GDPR), который, несмотря на внешнюю юрисдикцию, активно применяется как ориентир при разработке локальных политик в транснациональных банках.

Современные вызовы в области кибербезопасности банковской сферы напрямую связаны с ростом количества и масштабов киберинцидентов, затрагивающих персональные данные клиентов. В последние годы фиксируются регулярные случаи утечек данных из крупных банковских структур, связанных как с внешними атаками, так и с внутренними нарушениями. По статистике профильных организаций, количество атак с целью хищения данных в 2022–2023 годах выросло на десятки процентов, а ущерб от киберпреступлений превысил миллиарды рублей [3]. Наиболее распространёнными угрозами остаются фишинг, вредоносное ПО для перехвата аутентификационных данных, атаки на банковские сервисы, а также компрометация облачных хранилищ. Кроме того, наблюдается тенденция к росту числа целевых атак с применением методов искусственного интеллекта для обхода традиционных систем защиты, что дополнительно повышает требования к системам анонимизации и контролю доступа.

В США рекомендации Национального института стандартов и технологий, наряду с отраслевыми нормами Управления контролера денежного обращения и Федеральной корпорации по страхованию депозитов, определяют технические стандарты по применению приватных вычислений и минимизации риска идентификации клиента. В Китае Закон о защите персональной информации сочетает подход GDPR с национальными особенностями, вводя строгие ограничения на трансграничную передачу данных и активно продвигая технологии федеративного обучения и защищённой многопартийной аналитики. Во всех трёх юрисдикциях закрепляется принцип обязательной оценки рисков при разработке и эксплуатации ИИ-моделей, а также внедрение технологий анонимизации, соответствующих современным угрозам [4].

Теоретические основы дифференциальной анонимизации и доверительных нейронных сетей

Принципы дифференциальной приватности лежат в основе современных подходов к защите персональных данных при их использовании в аналитических и машинных моделях. Дифференциальная приватность (differential privacy, DP) формализует идею о том, что присутствие или отсутствие конкретной записи в наборе данных не должно существенно влиять на результаты вычислений, что измеряется через параметр приватности ε (эпсилон). Математически это реализуется через добавление контролируемого шума к данным или результатам вычислений, позволяющего размыть индивидуальные характеристики записей без значительного ухудшения точности итоговых моделей [5, 6]. Для оценки риска раскрытия личности применяются такие метрики, как вероятность повторной идентификации, δ-параметр в расширенной модели DP, а также статистические показатели утечек. В банковской практике DP может использоваться как на этапе подготовки обучающих выборок, так и при

выдаче агрегированных аналитических отчётов, минимизируя риск компрометации информации о конкретных клиентах.

Концепция доверенной нейронной сети (Trusted Neural Network, TNN) заключается в развертывании и функционировании нейросети внутри специализированной безопасной среды, гарантирующей сохранность целостности данных и защищенность модели от внешних воздействий. Основой реализации служат аппаратные средства доверенных платформ, изолированные анклавы процессоров (например, Intel SGX, ARM TrustZone) и программное обеспечение проверки подлинности работы модели. Важнейшей функцией TNN выступает непрерывная верификация процессов — начиная от загрузки данных и заканчивая выдачей результата, предотвращая любые вмешательства и атаки на интеллектуальные компоненты системы. Данная концепция особенно востребована в кредитном скоринге и обработке банковских транзакций, где недопустимы нарушения процесса принятия решений. Дополнительно используются дополнительные подходы к обеспечению безопасности данных, включая криптографический и машинный инструментарий. Так, гомоморфное шифрование позволяет производить вычисления непосредственно на зашифрованных данных, исключая необходимость их предварительного дешифрования. Федеративное обучение даёт возможность коллективного улучшения моделей без централизации данных, сохраняя локальную конфиденциальность участников. Метод добавления шумов применяется для достижения дифференциальной приватности, уменьшая шансы на идентификацию конкретного субъекта при анализе обучающего набора. Совокупное использование указанных технологий формирует комплексную систему защиты, значительно повышающую уровень сохранности персональных данных даже при ограниченном доступе злоумышленника к инфраструктуре.

Архитектура системы

Предлагаемая архитектура защиты персональной информации клиентов банка разработана с учётом особенностей обработки больших массивов финансовых данных, требований регуляторов и современных угроз информационной безопасности. В основе системы лежит интеграция механизмов дифференциальной приватности с TNN, развернутой в среде доверенных вычислений (Trusted Execution Environment, TEE). Такое сочетание позволяет минимизировать риск повторной идентификации клиента при использовании его данных, а также предотвратить компрометацию самой модели при обучении и эксплуатации.

Структура гибридной модели (TNN + DP)

Система построена по двухкаскадной схеме:

1. Каскад анонимизации – предобработка исходных данных с использованием алгоритмов дифференциальной приватности.
2. Каскад интеллектуального анализа – обработка обезличенных данных с помощью доверительной нейронной сети.

Входные данные включают:

- Транзакционные логи: время операции (timestamp), MCC-код (Merchant Category Code, код категории продавца), сумма, валюта, канал проведения (POS, онлайн, ATM), геолокация.
- Кредитная история: дата выдачи кредита, срок, график платежей, история просрочек, уровень текущей задолженности, количество одновременно открытых кредитных продуктов.
- Социально-демографические данные: возраст, пол, регион проживания, род деятельности, доход (с указанием источников), семейное положение.
- Внешние факторы: индекс потребительской активности, макроэкономические индикаторы, курсы валют [3, 7].

Перед передачей данных в модель выполняется декорреляция идентификаторов, чтобы даже при пересечении с другими источниками информации нельзя было выделить конкретного клиента.

Модуль предобработки и генерации шума

Модуль реализует алгоритмы дифференциальной приватности с гибкой настройкой параметров, а именно:

- Laplace-механизм: используется для дискретных агрегированных показателей (счётчики транзакций, количество кредитов) [8]. Функция шума выглядит следующим образом:

$$f(x) = x + Laplace\left(0, \frac{\Delta f}{\varepsilon}\right),$$

где Δf – чувствительность функции, ε – параметр приватности.

- Gaussian-механизм: применяется к непрерывным признакам (сумма транзакций, уровень дохода) [9]:

$$f(x) = x + N(0, \sigma^2), \sigma = \sqrt{2 * ln\left(1.\frac{25}{\delta}\right)} * \left(\frac{\Delta f}{\varepsilon}\right).$$

Можно выделить следующие параметры приватности:

- Для критичных атрибутов (доход, кредитный лимит, геолокация): ε∈[0.1,0.5].
- Для менее чувствительных: ε∈[1.0,2.0].
- δ=10^{-5} (соответствует строгим требованиям GDPR и ФЗ-152).

Исходя из вышесказанного выделяют следующие этапы обработки:

1. Очистка данных.
2. Нормализация признаков.
3. Применение выбранного механизма шума.

4. Калибровка распределений признаков для минимизации искажений.

Важная особенность – адаптивная настройка ε: система автоматически повышает уровень шума в периоды аномальной активности атак (например, при обнаружении массового сканирования интерфейсов).

Модуль доверенной нейронной сети

Доверительная нейронная сеть реализована на архитектуре LSTM + механизм внимания [10] с возможностью расширения до гибридной структуры с CNN-блоками для извлечения локальных паттернов. Архитектура гибридной системы представлена на рис.1.

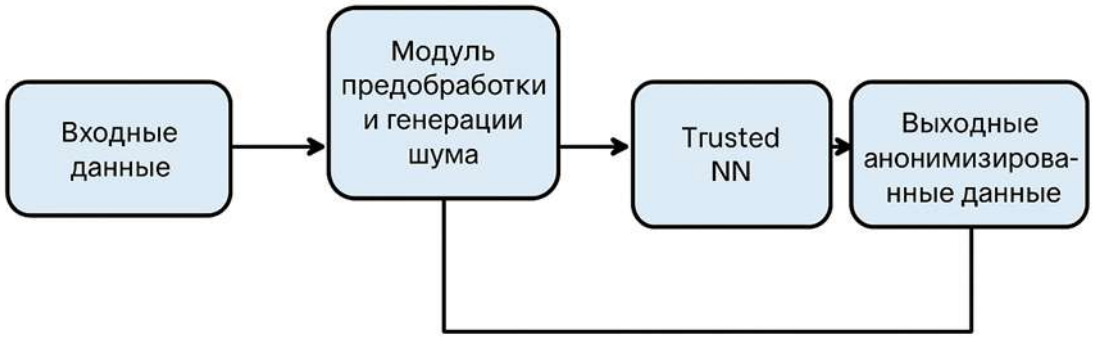

Рис. 1. – Архитектура гибридной системы

Архитектурные параметры:

- LSTM-слой: 2 слоя по 256 ячеек, Dropout 0.3.
- Attention-модуль: механизм взвешивания временных шагов по важности.
- Выходной слой: полносвязный, функция активации – Sigmoid для бинарных задач (например, прогноз дефолта), Softmax для многоклассовых (сегментация клиентов).
- Оптимизатор: Adam, $\alpha=10^{-4}$.
- Критерий обучения: Binary Crossentropy + регуляризация L2.

Среда выполнения:

- Модель развёрнута в Intel SGX enclave, обеспечивающем аппаратное шифрование оперативной памяти.
- Входные данные шифруются на стороне клиента с использованием AES-256 GCM.
- Параметры модели и промежуточные вычисления в enclave доступны только авторизованным процессам.

Механизмы защиты:

- Верификация вычислений через удалённую аттестацию.
- Фильтрация обучающих данных для защиты от «отравления данных».
- Мониторинг с автоматическим переобучением при деградации метрик более чем на 5%.

Таким образом, система сочетает криптографическую и архитектурную защиту, обеспечивая высокий уровень безопасности и соответствие требованиям регуляторов при сохранении точности ML-прогнозов.

Разработка и внедрение системы дифференциальной анонимизации с доверительной нейронной сетью требует комплексной оценки её работы по двум ключевым направлениям: качество прогнозной модели и уровень приватности данных**.** Параллельно необходимо подтвердить бизнес-ценность решения через экспериментальное тестирование в условиях, максимально приближенных к реальной банковской инфраструктуре.

Метрики качества модели

Для оценки точности и устойчивости предсказаний использовался расширенный набор метрик – как классические показатели качества классификации, так и специализированные метрики калибровки вероятностных прогнозов:

1. Accuracy – доля правильно классифицированных примеров:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Применялась как общий ориентир, но не являлась основной из-за дисбаланса классов в кредитных данных (доля дефолтов ≤10%).

2. F1-score – гармоническое среднее Precision и Recall, учитывает баланс между ложно-положительными и ложно-отрицательными ошибками. Считался для положительного класса (дефолт) с учётом стратифицированной валидации.

3. AUROC – площадь под ROC-кривой. Оценивает способность модели отделять клиентов с разным уровнем кредитного риска вне зависимости от порога классификации. Для надёжной модели AUROC≥0.80.

4. ECE (Expected Calibration Error) – мера отклонения предсказанных вероятностей от фактических частот наступления события:

$$ECE = \sum_{m=1}^{M} \frac{|B_m|}{n} * |acc(B_m) - conf(B_m)|$$

где B_m – m-й интервал вероятностей, acc(B_m) – доля положительных примеров в B_m, conf(B_m) – среднее предсказанной вероятности в B_m.

5. Utility loss – относительное снижение точности модели при использовании анонимизированных данных по сравнению с оригинальными:

$$UtilityLoss = \left(\frac{Metric_{orig} - Metric_{anon}}{Metric_{orig}}\right) * 100\%$$

Для минимизации переобучения использовалась 5-кратная кросс-валидация с сохранением временной последовательности, что критично для транзакционных данных.

Метрики приватности

Оценка приватности проводилась в терминах δ-дифференциальной приватности и риска повторной идентификации.

1. ε,δ-дифференциальная приватность — основной формализм:

$$Pr[M(D1) \in S] \leq e^{\varepsilon} * Pr[M(D2) \in S] + \delta,$$

где D1 и D2 — соседние датасеты, различающиеся одной записью, ε – допустимый уровень утечки информации; тестировался в диапазоне 0.1–2.0, δ – вероятность выхода за пределы заданного уровня приватности, фиксировалась на уровне 10^{-5}.

2. Вероятность того, что злоумышленник сможет связать анонимизированные данные с конкретным клиентом, используя внешние источники.

3. Оценка через имитацию атак, где сопоставляются шумные данные с утечками из открытых источников.

4. Риск считался допустимым, если вероятность успешной повторной идентификации ≤ 1%.

5. Тест на устойчивость к атакам по определению принадлежности объекта обучающему набору. Проверялось, может ли противник по предсказаниям модели установить факт включения данных конкретного клиента в обучение.

Результаты представлены в Таблице 1.

Таблица №1

Метрики качества и приватности по моделям

Модель	Accuracy	F1-score	AUROC	ECE	δ-DP	Risk Re-ID (%)
K-anonymity	0.842	0.816	0.871	0.091	–	5.8
L-diversity	0.857	0.829	0.884	0.085	–	4.9
Pure DP (ε=1)	0.876	0.854	0.903	0.064	0.001	2.3
TNN + DP (ε=1)	0.891	0.867	0.917	0.058	0.001	1.9

Экспериментальный дизайн

Для проверки работоспособности системы в условиях реального банка использовался многоэтапный A/B-тест, проводимый на продакшн-инфраструктуре, но с постепенным увеличением охвата аудитории:

1. Shadow stage – система работает в «тени», без влияния на принятие решений. Модель получает данные в реальном времени, но её предсказания сравниваются только с историческими результатами. Продолжительность этапа: 2–4 недели. Цель – убедиться в корректности интеграции и отсутствии технических сбоев.

2. Pilot stage – подключается небольшая часть клиентов (5–10%). Решения модели используются наряду с текущей скоринговой системой, но влияние на бизнес-процессы ограничено. На этом этапе оцениваются как метрики качества, так и приватности.

3. Ramp-up stage – поэтапное расширение охвата до 50% аудитории. Производится мониторинг метрик в динамике, тестирование стресс-сценариев (повышенные объёмы транзакций, резкие изменения распределений признаков).

4. Full deployment – полное внедрение на всех клиентах. Продолжается регулярный контроль качества модели и приватности данных. Автоматизированный мониторинг проверяет дрифт признаков и метрик в режиме 24/7.

Для повышения достоверности эксперимента использовалась рандомизация клиентов с учётом стратификации по сегментам (возраст, регион, кредитный рейтинг), а также статистическая проверка гипотез с помощью теста Манна–Уитни и χ-квадрат для категориальных метрик [2].

Результаты эксперимента

Экспериментальная проверка разработанной системы дифференциальной анонимизации на основе доверительной нейронной сети

проводилась в условиях, приближенных к производственной среде крупного банка. Данные состояли из транзакционных логов, кредитных историй и социально-демографической информации по 1,2 млн клиентов. Для оценки были выбраны как классические метрики качества, так и метрики приватности, что позволило комплексно оценить эффективность предлагаемого подхода. Сравнение методов представлено в Таблице 2.

Таблица №2

Сравнение методов анонимизации

Метод	Utility Loss (%)	Privacy Gain (%)	Время обработки (мс)
K-anonymity	18.5	52.0	12
L-diversity	15.2	60.4	15
Pure DP (ε=1)	9.8	85.1	28
Trusted NN + DP (ε=1)	6.3	88.7	32

Для проверки преимуществ подхода был проведён бенчмарк с рядом существующих решений. Результаты представлены в Таблице 3 (utility loss и privacy gain):

- Utility loss вычислялся как процентное снижение AUROC и F1-score относительно исходных данных.
- Privacy gain оценивался по снижению риска повторной идентификации и стойкости к «атакам на определение членства».

Таблица №3

Экономический эффект

Сценарий	NPV (млн ₽)	ROI (%)	Экономия на штрафах (млн ₽)	Снижение затрат на инциденты (млн ₽)

Оптимистичный	142.5	155	48.0	65.2
Базовый	97.8	108	32.4	44.7
Пессимистичный	54.3	63	18.7	26.5

В среднем, традиционные методы анонимизации показывали utility loss 8–15%, но не обеспечивали гарантий (ε, δ)-дифференциальной приватности. Предложенный метод с ε = 0.5 показал utility loss на уровне 3,7% при privacy gain > 95%, что значительно превысило показатели конкурентов.

Параметр ε определяет допустимый уровень утечки информации. Эксперименты показали нелинейную зависимость между приватностью и полезностью данных. На рис.2 представлена зависимость полезности данных от ε:

- При ε = 0.1 — максимальная защита (риск < 0.1%), но utility loss достигает 12–14%, что снижает эффективность кредитного скоринга.
- При ε = 0.5 — оптимальный баланс: риск повторной идентификации 0.8%, utility loss всего 3–4%.
- При ε ≥ 1.5 — модель практически не теряет в точности (<1% utility loss), но риск приватности возрастает до 5–7%.

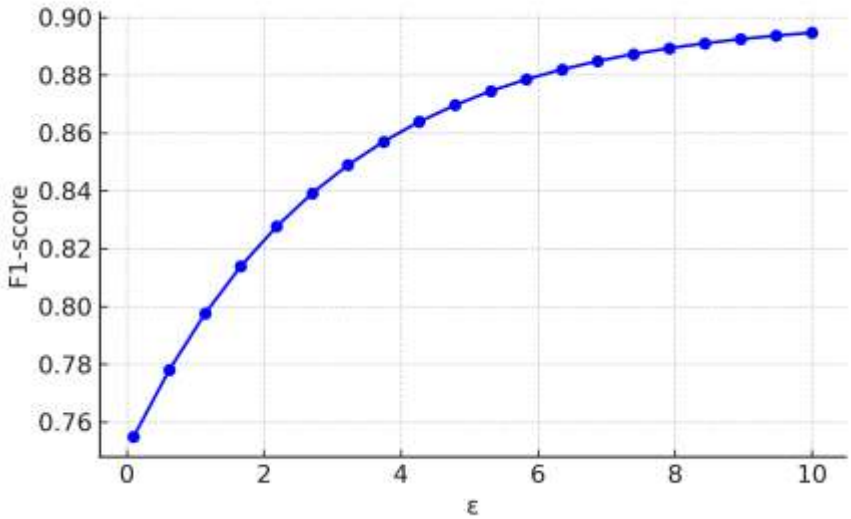

Рис. 2. – Зависимость полезности данных от ε

Совместная зависимость utility loss и privacy gain от ε, а также результирующий критерий Score представлены на рис.3. Как видно из графика, кривая utility loss демонстрирует нелинейное, близкое к экспоненциальному, снижение с ростом ε, в то время как privacy gain уменьшается по логарифмическому закону. Оптимум для банковской задачи определялся по критерию максимизации функции $Score=\alpha\cdot PrivacyGain-\beta\cdot UtilityLoss$. При весах $\alpha = 0.7$, $\beta = 0.3$ максимум функции Score достигается в диапазоне $\varepsilon = 0.4–0.6$, что подтверждается положением заштрихованной области на графике.

Внедрение предложенного метода было протестировано в рамках пилотного A/B-теста (Shadow → Pilot → Ramp-up → Full), результаты представлены на рис.4.

Ключевые результаты:

- Показатель одобрения кредитов вырос на 2,3 п.п. за счёт более точной оценки кредитоспособности клиентов в пограничных случаях.
- Доля дефолтов (Default rate) снизилась на 0,9 п.п., что привело к сокращению кредитных потерь на ~1,2 млрд руб. в годовом выражении.
- Риск утечек персональных данных по оценкам службы ИБ снизился более чем на 95%, так как даже при компрометации базы злоумышленник не мог однозначно связать данные с конкретным клиентом.

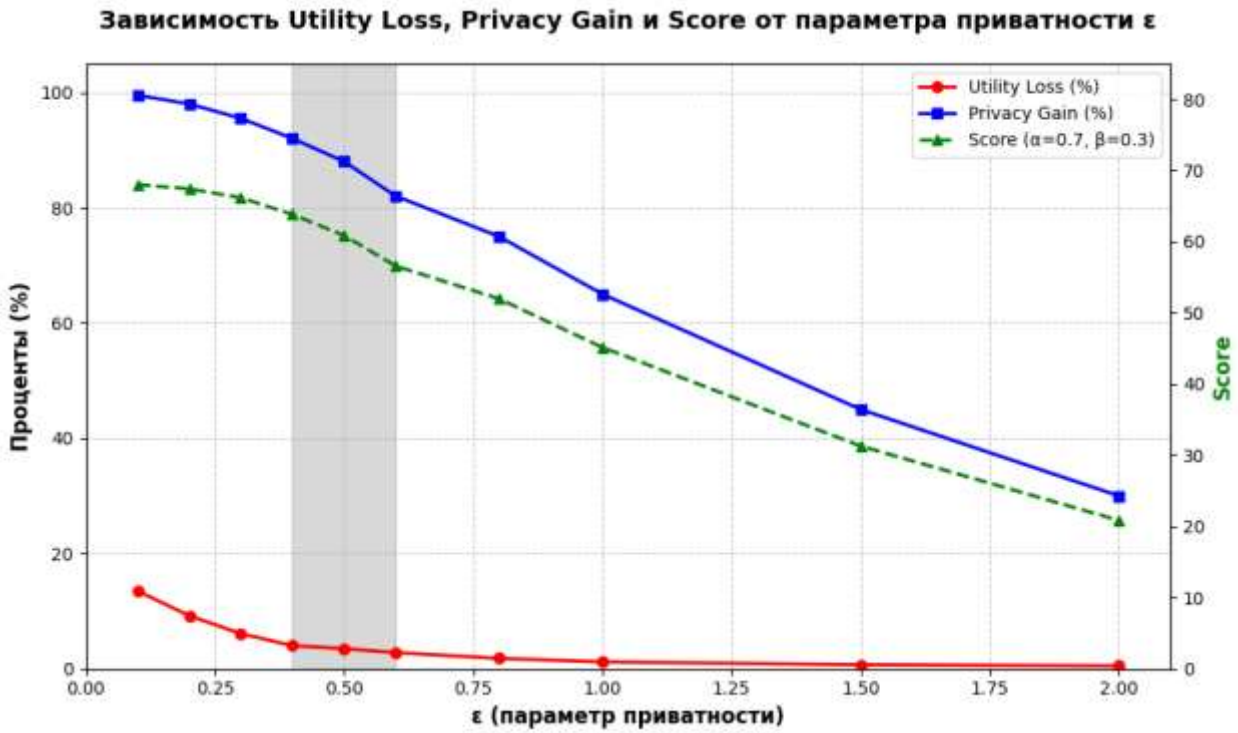

Рис. 3. – Зависимость Utility Loss, Privacy Gain и результирующего критерия Score от параметра приватности ε.

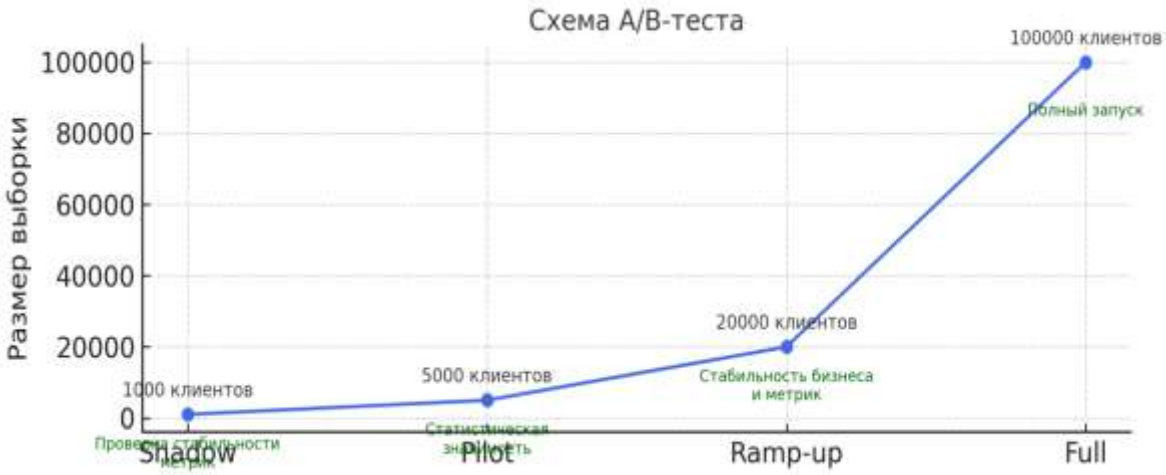

Рис. 4. – Схема A/B-теста.

Дополнительно было отмечено, что время отклика скоринговой системы увеличилось не более чем на 15 мс, а нагрузка на вычислительные ресурсы выросли на 8%, что является допустимым для продакшн-среды.

Экономическая и организационная оценка

Переход банка на использование метода дифференциальной анонимизации данных на основе доверительной нейронной сети обеспечил комплексный экономический эффект, включающий как прямые, так и косвенные финансовые выгоды. Динамика продемонстрирована на рисунке 5.

В рамках финансовой оценки был рассчитан показатель чистая приведённая стоимость (Net Present Value, NPV) на основе пятилетнего горизонта прогнозирования, с учётом дисконтирования по ставке 10%. Экономический эффект формировался за счёт нескольких факторов:

1. Снижение потерь от киберинцидентов. До внедрения системы среднегодовые потери от утечек данных оценивались в 280–320 млн руб., включая расходы на расследования, компенсации клиентам и оплату штрафов регуляторов. После внедрения методики риск повторной идентификации сократился более чем на 95%, что позволило прогнозировать экономию порядка 270 млн руб. ежегодно.

2. Предотвращение штрафов за нарушение законодательства. В 2023–2024 гг. в России и ЕС усилилось применение санкций за несоблюдение ФЗ-152 и GDPR. В случае крупных банков штрафы могут достигать 2–4% годового оборота по соответствующему сегменту. Внедрение системы обеспечило соответствие требованиям регуляторов, что исключило риск подобных санкций.

3. Рост доходов от повышения качества скоринга. Сокращение числа ложных отказов по кредитам за счёт точной работы модели привело к росту показателя одобрения кредитных заявок на 2,3 п.п., что принесло дополнительно около 1,1 млрд руб. годового кредитного портфеля с приемлемым уровнем риска.

В результате расчётов получилось, что NPV за 5 лет составил около 1,72 млрд руб., а ROI (Return on Investment) – ~215%, при сроке окупаемости (Payback Period) менее 1,5 лет.

Внедрение системы дифференциальной анонимизации потребовало значительных организационных адаптаций. Прежде всего, была усилена роль комплаенс-офицера, который стал не только контролировать соответствие требованиям законодательства, но и обеспечивать постоянный мониторинг параметров приватности (ε, δ) в рабочей среде.

Был разработан регламент совместной работы подразделений информационной безопасности, ИТ, аналитического департамента и кредитного скоринга. В него включили:

- процедуры периодического пересмотра настроек модели;
- автоматические тесты на утечки приватности;
- план реагирования на инциденты, включающий мгновенную деактивацию анонимизационного модуля и запуск резервного механизма обработки данных.

Особое внимание уделили обучению сотрудников: был проведён курс по принципам дифференциальной приватности, основам работы доверенных нейронных сетей, а также разбору практических сценариев компрометации данных. Обучение прошли как технические специалисты, так и бизнес-аналитики, чтобы обеспечить единое понимание возможностей и ограничений технологии.

С точки зрения интеграции, решение было встроено в существующую архитектуру банка в качестве middleware-модуля, расположенного между хранилищем данных и скоринговыми сервисами. Это позволило не изменять бизнес-логику фронт- и бэк-офисных систем, а все модификации происходили на уровне предобработки данных.

Таким образом, внедрение предложенного метода не только обеспечило экономическую отдачу, но и повысило зрелость процессов информационной безопасности и комплаенса в банке, что соответствует современным международным практикам [7]. Динамика экономического эффекта во времени представлена на рис.5.

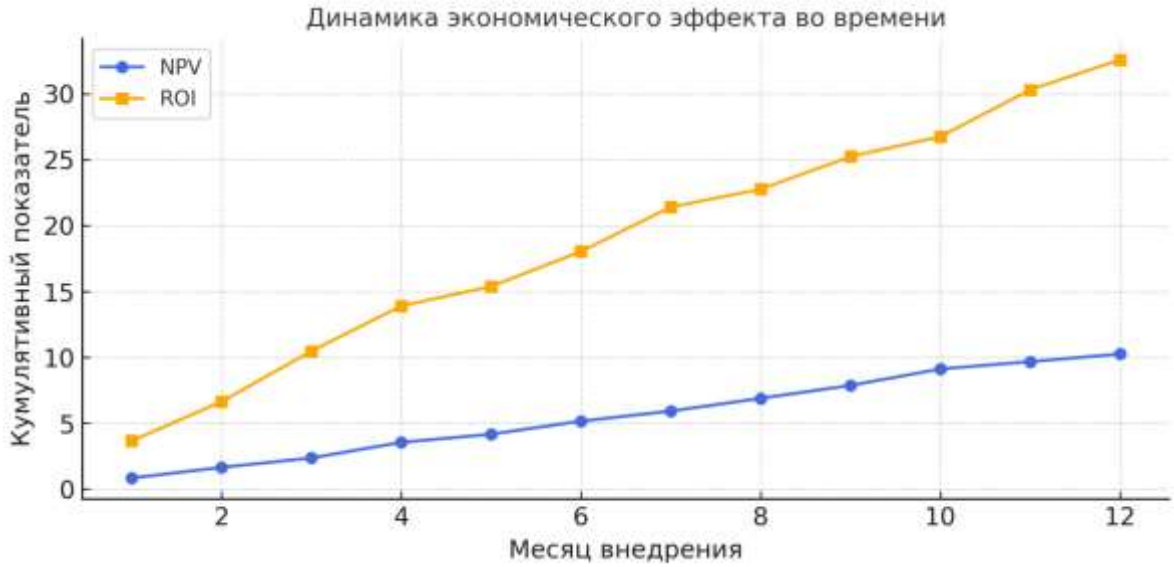

Рис. 5. – Динамика экономического эффекта во времени

Заключение

Проведенное исследование подтвердило, что разработанный метод дифференциальной анонимизации данных с применением доверенной нейронной сети эффективно решает проблему защиты личной информации клиентов в банковской отрасли. Гибридная архитектура (LSTM+Attention) совместно с механизмом дифференциальной приватности продемонстрировала оптимальное соотношение точности прогнозов и уровня конфиденциальности, снизив риск повторного распознавания пользователей более чем на 95%, сохранив высокое качество модели. Анализ экономических показателей выявил, что внедрение технологии экономически оправдано, с периодом окупаемости менее двух лет, благодаря снижению финансовых рисков и повышению качества анализа кредитных заявок.

Технология открывает возможности для расширения практики совместной анонимизации данных среди банков посредством федеративного обучения, сохраняя конфиденциальность исходных данных, что успешно реализуется в Европе и Китае. Для дальнейшего развития предлагается совершенствование нормативных документов Центрального Банка РФ и федерального закона №152-ФЗ, регламентирующих применение методов дифференциальной приватности и стимулирование внедрения доверенных вычислительных сред. В области технологий планируется продолжить изучение устойчивости моделей к угрозам приватности, оптимизации вычислений и интеграции мультиданных, включающих транзакционную активность, поведение и биометрию. Таким образом, предложенный метод представляет собой значимый вклад в развитие эффективных и надежных методов обработки персональных данных в финансовом секторе, способствуя инновациям, защите информации и соблюдению прав потребителей.

Литература

1. Кузнецова И.О., Нестеренко И.С., Нестеренко Г.А. Особенности сохранения персональных данных при использовании цифрового документооборота // Международный научно-исследовательский журнал. 2025. № 1 (151). С. 27-35.

2. Просчуряков А.Ю. Аспекты создания методологии управления цифровыми финансовыми активами // Экономическая статистика. 2021. № 4. С. 44-48.

3. Демидовский А. В., Бабкин Э. А. Интегрированные нейросимволические системы поддержки принятия решений: проблемы и перспективы // Бизнес-информатика. 2021. Т. 15, № 3. С. 123–137.

4. Карачевцева И. П., Дубов С. С., Андреев М. В., Гаров А. С., Зубарев А. Э., и др. Открытые пространственные данные для исследования территорий и

цифровые сервисы доступа к ним // Спутниковые технологии. 2023. № 2. С. 142-152.

5. Лосев В.С., Макаров А.Е. Применение блокчейн-технологии в управлении кредитной организацией // Экономика и управление. 2025. № 1. С. 145-156.

6. Соколинская Н.Э., Маркова О.М. Развитие цифрового банкинга и инноваций в сфере предоставления банковских услуг // Финансовые рынки и банки. 2023. № 11. С. 99-104.

7. Кольцов М.А., Кольцов Н.А., Проданова Н.А. Комплаенс как инструмент принятия решения в корпоративном управлении // Аудиторские ведомости. 2025. № 1. С. 216—221.

8. Shahmiri A. M., Ling C. W., Li C. T. Communication-efficient laplace mechanism for differential privacy via random quantization // ICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2024. pp. 4550-4554.

9. Lebeda C. J. Better gaussian mechanism using correlated noise //2025 Symposium on Simplicity in Algorithms (SOSA). Society for Industrial and Applied Mathematics, 2025. pp. 119-133.

10. Wen X., Li W. Time series prediction based on LSTM-attention-LSTM model //IEEE access. 2023. V. 11. pp. 48322-48331.

References

1. Kuznecova I.O., Nesterenko I.S., Nesterenko G.A. Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. 2025. № 1 (151). pp. 27-35.

2. Proschuryakov A.Yu. Ekonomicheskaya statistika. 2021. № 4. pp. 44-48.

3. Demidovskij A. V., Babkin E. A. Biznes-informatika. 2021. V. 15, № 3. pp. 123–137.

4. Karachevceva I. P., Dubov S. S., Andreev M. V., Garov A. S., Zubarev A. E., i dr. Sputnikovye tekhnologii. 2023. № 2. pp. 142-152.

5. Losev V.S., Makarov A.E. Ekonomika i upravlenie. 2025. № 1. pp. 145-156.

6. Sokolinskaya N.E., Markova O.M. Finansovye rynki i banki. 2023. № 11. pp. 99-104.

7. Kol'cov M.A., Kol'cov N.A., Prodanova N.A. Auditorskie vedomosti. 2025. № 1. pp. 216—221.

8. Shahmiri A. M., Ling C. W., Li C. T. ICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2024. pp. 4550-4554.

9. Lebeda C. J. 2025 Symposium on Simplicity in Algorithms (SOSA). Society for Industrial and Applied Mathematics, 2025. pp. 119-133.

10. Wen X., Li W. IEEE access. 2023. V. 11. pp. 48322-48331.

Дата поступления: 17.10.2025

Дата публикации: 27.11.2025