ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

Дата публикации: 07 марта 2026 г.

Настоящая Политика конфиденциальности (далее — «Политика») описывает, какие сведения обрабатываются при использовании сервиса «Итого» (далее — «Сервис»), каким образом они защищены, а также какие права имеет лицо, использующее Сервис (далее — «Пользователь»).

Политика составлена в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Используя Сервис, Вы подтверждаете согласие с условиями настоящей Политики. Если Вы не согласны с каким-либо из положений — пожалуйста, воздержитесь от использования Сервиса.

---

1. Оператор

Оператором обработки данных является:

Индивидуальный предприниматель Лукьянов Павел Андреевич

- ОГРНИП: 321784700108333
- ИНН: 780159889217
- Адрес: 199004, г. Санкт-Петербург, Василеостровский р-н, линия 2-я В.О., д. 35 литера Б, кв. 20
- Электронная почта: support@itogo.app

---

2. Принцип минимизации данных

Сервис спроектирован с применением принципа минимизации данных и архитектуры zero-knowledge. Это означает, что Оператор целенаправленно ограничивает объём обрабатываемой информации до технического минимума, необходимого для функционирования Сервиса.

---

3. Данные, которые мы НЕ собираем

В отличие от большинства онлайн-сервисов, Оператор **не собирает и не обрабатывает** следующие категории персональных данных:

- **фамилия, имя, отчество** — при регистрации не запрашиваются;
- **адрес электронной почты** — для входа в Сервис email не используется;
- **номер телефона** — не запрашивается;
- **финансовые данные в открытом виде** — все финансовые сведения шифруются на стороне Пользователя до передачи на сервер (подробнее — раздел 5);
- **файлы банковских выписок** — импорт и обработка (парсинг) файлов выписок происходят полностью на устройстве Пользователя; файлы не передаются на сервер и не сохраняются Оператором;
- **данные банковских карт** — обработка платежей осуществляется исключительно платёжными провайдерами (Prodamus и/или Robokassa); Оператор не получает, не обрабатывает и не хранит реквизиты платёжных карт;
- **персональные данные из платёжного колбэка** — при успешной оплате платёжный провайдер направляет на сервер Оператора уведомление (колбэк), которое может содержать персональные данные Пользователя (ФИО, адрес электронной почты, номер телефона и иные данные, указанные Пользователем при оплате). Сервер Оператора обрабатывает колбэк исключительно для подтверждения факта оплаты и активации Подписки. Персональные данные из колбэка **не сохраняются** на сервере Оператора и удаляются из оперативной памяти сразу после обработки.

---

4. Данные, которые мы обрабатываем

Оператор обрабатывает следующие категории сведений:

4.1. Данные учётной записи

При создании учётной записи на сервере сохраняются:

- **идентификатор пользователя** (user_id) — криптографический хеш (SHA-256), вычисляемый из Ключа доступа на стороне клиента;
- **хеш токена аутентификации** (auth_token_hash) — используется для проверки подлинности запросов;
- **криптографическая соль** (salt) — случайно сгенерированная последовательность для деривации ключа шифрования.

Указанные данные являются криптографическими производными и **не позволяют идентифицировать Пользователя** как физическое лицо. Они не относятся к персональным данным в смысле Федерального закона от 27.07.2006 № 152-ФЗ.

4.2. Финансовые данные

Основная часть финансовых данных (наименования операций, описания, балансы, правила и прочие детали) шифруется на устройстве Пользователя с использованием алгоритма **AES-256-GCM** и ключа, производного от Ключа доступа посредством PBKDF2 (600 000 итераций). На сервере хранятся исключительно зашифрованные массивы данных (blob-ы). Оператор не имеет технической возможности расшифровать эти данные.

Исключение: категория операции и сумма операции хранятся на сервере в незашифрованном виде. Это необходимо для работы функций машинного обучения (прогнозирование, аналитика по категориям, выявление аномалий), которые выполняются на стороне сервера. Указанные данные (категория и сумма) привязаны исключительно к криптографическому идентификатору пользователя и **не позволяют установить личность Пользователя** или определить, в каком банке, магазине или учреждении была совершена операция.

4.3. Техническая информация

При взаимодействии с Сервисом автоматически фиксируются:

- **IP-адрес** — в журналах (логах) веб-сервера;
- **тип и версия браузера** (User-Agent) — в журналах веб-сервера;
- **дата и время обращения** к Сервису.

Журналы веб-сервера хранятся в течение 90 (девяноста) дней и затем удаляются.

4.4. Аналитические данные об использовании

Сервис собирает обезличенные события использования (например, факт перехода между разделами, использование функций) для целей улучшения качества Сервиса. Аналитические данные привязаны к идентификатору пользователя (криптографическому хешу) и **не содержат персональных данных**.

4.5. Данные о подписке

Информация о статусе подписки (тариф, дата начала и окончания периода) хранится на сервере для обеспечения контроля доступа к функционалу Сервиса.

---

5. Архитектура zero-knowledge

5.1. Сервис применяет архитектуру zero-knowledge («нулевого знания»), которая означает, что Оператор не обладает доступом к содержимому данных Пользователя.

5.2. Механизм работы:

- при регистрации Пользователь получает уникальный **Ключ доступа**, который генерируется локально на его устройстве;
- из Ключа доступа на стороне клиента вычисляются: идентификатор пользователя, токен аутентификации и ключ шифрования;
- основная часть финансовых данных шифруется ключом шифрования (**AES-256-GCM**) до отправки на сервер;
- категория и сумма операций хранятся в незашифрованном виде для обеспечения работы ML-аналитики на стороне сервера;
- сервер хранит зашифрованные данные, криптографические хеши, а также незашифрованные категории и суммы;
- расшифровка данных возможна исключительно на устройстве Пользователя при наличии Ключа доступа.

5.3. Следствием архитектуры zero-knowledge является невозможность восстановления данных при утрате Ключа доступа. Оператор не может восстановить ни Ключ доступа, ни зашифрованные данные.

---

6. Цели обработки данных

Обработка указанных в разделе 4 сведений осуществляется в следующих целях:

- обеспечение функционирования Сервиса и аутентификации Пользователя;
- контроль доступа к платному функционалу;
- обеспечение информационной безопасности;
- улучшение качества Сервиса на основе обезличенной аналитики использования;
- исполнение требований законодательства Российской Федерации.

---

7. Правовые основания обработки

Обработка данных осуществляется на следующих основаниях:

- исполнение договора (Пользовательского соглашения) между Оператором и Пользователем — п. 5 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ;
- законные интересы Оператора по обеспечению работоспособности и безопасности Сервиса — п. 7 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ.

---

8. Передача данных третьим лицам

8.1. Оператор может передавать данные следующим категориям третьих лиц:

- **Платёжные провайдеры** — Prodamus (https://prodamus.ru) и/или Robokassa (https://robokassa.ru), обрабатывающие платежи за Подписку. Платёжный провайдер получает платёжные данные непосредственно от Пользователя. При успешной оплате провайдер направляет на сервер Оператора уведомление (колбэк), которое может содержать персональные данные Пользователя. Оператор использует колбэк только для подтверждения оплаты и не сохраняет персональные данные из него;
- **хостинг-провайдер** — для размещения серверной инфраструктуры Сервиса. Хостинг-провайдер обеспечивает хранение зашифрованных данных и не имеет возможности их расшифровать;
- **государственные органы** — в случаях, прямо предусмотренных законодательством Российской Федерации.

8.2. Оператор не продаёт, не обменивает и не передаёт данные Пользователя третьим лицам в маркетинговых или рекламных целях.

---

9. Хранение данных

9.1. Данные учётной записи и зашифрованные финансовые данные хранятся на территории Российской Федерации на протяжении всего периода использования Сервиса Пользователем.

9.2. При удалении учётной записи все связанные данные (идентификаторы, зашифрованные данные, аналитические события) удаляются в течение 30 (тридцати) календарных дней.

9.3. Журналы веб-сервера хранятся не более 90 (девяноста) дней.

---

10. Права Пользователя

Пользователь имеет право:

- запросить информацию о том, какие данные обрабатываются в отношении его учётной записи;
- потребовать удаления учётной записи и всех связанных данных;
- отозвать согласие на обработку данных путём удаления учётной записи;
- обратиться с жалобой в Роскомнадзор (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций).

Для реализации указанных прав Пользователь может направить обращение на электронную почту Оператора: support@itogo.app.

---

11. Меры безопасности

Оператор принимает следующие организационные и технические меры для защиты данных:

- end-to-end шифрование финансовых данных (AES-256-GCM);
- передача данных по защищённым каналам (HTTPS/TLS);
- хранение аутентификационных данных исключительно в виде криптографических хешей;
- ограничение доступа к серверной инфраструктуре;
- регулярное обновление программного обеспечения.

---

12. Изменение Политики

12.1. Оператор вправе в одностороннем порядке вносить изменения в настоящую Политику. Актуальная редакция Политики размещается на Сайте.

12.2. Продолжение использования Сервиса после публикации изменений означает согласие Пользователя с обновлённой редакцией Политики.

12.3. Пользователь обязуется самостоятельно отслеживать изменения Политики.

---

13. Контактная информация

По всем вопросам, связанным с обработкой данных, Пользователь может обращаться:

- Электронная почта: support@itogo.app
- Адрес для корреспонденции: 199004, г. Санкт-Петербург, Василеостровский р-н, линия 2-я В.О., д. 35 литера Б, кв. 20