



ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

и порядок безопасной передачи платёжных данных IT Cody

Редакция от 07.10.2026 г.

1. Общие положения

1.1. Настоящий документ определяет меры **информационной безопасности** сервисов **IT Cody** и **порядок безопасной передачи платёжных данных** при оплате на сайте <https://itcody.ru> (далее — **Сайт**).

1.2. Оператор: индивидуальный предприниматель **Новиков Владимир Игоревич**, бренд **IT Cody** (далее — **Оператор, мы**).

1.3. Документ разработан в соответствии с законодательством Российской Федерации, в том числе:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платёжной системе»;
- требованиями платёжных сервисов и банков-эквайеров при приёме оплаты через интернет.

1.4. Документ применяется совместно с **Политикой конфиденциальности**, **Публичной офертой**, **Политикой обработки файлов cookie** и иными документами IT Cody, размещёнными на Сайте.

1.5. Настоящая Политика распространяется на:

- Сайт **itcody.ru** и его поддомены;
- сервис «**Disk**»;
- **IT-услуги** (разработка сайтов, программ и иных решений);
- инфраструктуру и системы, используемые для их функционирования.

Часть I. Политика информационной безопасности

2. Цели и принципы

2.1. Цели:

- обеспечение **конфиденциальности**, **целостности** и **доступности** информации пользователей и данных IT Cody;
- защита от несанкционированного доступа, модификации, уничтожения и утечки данных;

- минимизация рисков при обработке информации в Сервисах IT Cody.

2.2. Принципы:

- **минимизация данных** — собираем и храним только необходимое;
- **разграничение доступа** — доступ к системам имеют только уполномоченные лица;
- **шифрование и защищённые каналы** — где это технически необходимо;
- **регулярное обновление** программного обеспечения и мониторинг инцидентов.

3. Объекты защиты

3.1. IT Cody защищает:

Объект	Примеры
Персональные данные	e-mail, данные профиля, идентификаторы OAuth
Учётные записи	логины, хеши паролей, сессии
Данные Сервисов	файлы в «Disk», метаданные
Платёжная информация	факт оплаты, идентификатор транзакции — не полные реквизиты карты
Техническая инфраструктура	серверы, базы данных, резервные копии, журналы

3.2. Подробности обработки персональных данных — в **Политике конфиденциальности**.

4. Организационные меры

4.1. Оператор:

- назначает ответственное лицо за обработку обращений по безопасности — **support@itcody.ru**;
- ограничивает доступ к административным панелям, серверам и базам данных;
- использует **корпоративную почту** IT Cody (@itcody.ru) для деловой переписки;
- при привлечении подрядчиков (хостинг, разработка) требует соблюдения конфиденциальности в объёме, необходимом для проекта.

4.2. Сотрудники и подрядчики, имеющие доступ к данным, обязаны:

- не передавать пароли и ключи доступа третьим лицам;
 - не копировать пользовательские данные без служебной необходимости;
 - сообщать о подозрительных инцидентах на **support@itcody.ru**.
-

5. Технические меры

5.1. Сайт и Сервисы IT Cody:

- передача данных между браузером пользователя и Сайтом осуществляется по протоколу **HTTPS (TLS)**;
- пароли пользователей хранятся в виде **криптографических хешей**, а не в открытом виде;
- применяются механизмы защиты от CSRF, brute force и иных типовых атак;
- ведутся **журналы** событий безопасности (вход, подозрительная активность).

5.2. Сервис «Disk»:

- доступ к файлам — только через **авторизованную учётную запись** и в рамках тарифа;
- резервное копирование критичной инфраструктуры выполняется в объёме, необходимом для работоспособности Сервиса.

5.3. Авторизация:

- вход через e-mail/пароль или OAuth (**Яндекс ID, VK ID**) — без получения пароля от стороннего сервиса.

5.4. Обновления:

- программное обеспечение серверов и приложений **регулярно обновляется** для устранения известных уязвимостей.

6. Действия пользователя

Пользователь обязан:

- хранить пароль и данные доступа к учётной записи **в тайне**;
- использовать актуальную версию браузера с поддержкой HTTPS;
- сообщать о подозрении на взлом аккаунта на **support@itcody.ru**.

7. Инциденты безопасности

7.1. **Инцидент** — событие, которое может привести или привело к утечке, утрате, несанкционированному доступу к данным пользователей или нарушению работы Сервисов.

7.2. О подозрении на инцидент сообщайте: **support@itcody.ru** (тема: «Безопасность»).

7.3. Оператор:

- рассматривает обращение в разумный срок;
 - принимает меры по блокировке компрометированного доступа, устранению уязвимости, восстановлению работы;
 - при необходимости уведомляет пользователей и уполномоченные органы в порядке, установленном законом.
-

Часть II. Порядок безопасной передачи платёжных данных

8. Общие положения об оплате

8.1. Оплата платных услуг и подписок IT Cody принимается следующими способами:

Способ	Описание
Система быстрых платежей	на защищённой странице оплаты
Банковские карты	на защищённой странице оплаты
По реквизитам	банковский перевод по реквизитам Исполнителя

8.2. Оплата **по реквизитам** возможна **после согласования** заказа с Оператором (см. Публичную оферту и Порядок оформления заказов).

8.3. IT Cody не принимает, не обрабатывает и не хранит на своих серверах:

- полный номер банковской карты (PAN);
- CVV/CVC-код;
- PIN-код;
- иные данные, позволяющие совершить операцию без участия платёжного сервиса и банка.

9. Как проходит оплата на Сайте

9.1. Пошагово:

1. Пользователь выбирает тариф или услугу на **itcody.ru**.
2. Нажимает «Оплатить» и перенаправляется на **защищённую страницу оплаты**.
3. Вводит платёжные данные **на стороне платёжного сервиса и банка**, а не на серверах IT Cody.
4. Платёжный сервис подтверждает результат транзакции.
5. IT Cody получает **уведомление об успешной или неуспешной оплате** (статус, сумма, идентификатор операции) — **без** полных данных карты.

9.2. Передача платёжных данных от Пользователя к банку осуществляется по **защищённым каналам связи** (HTTPS/TLS) **силами платёжного сервиса** в соответствии с требованиями национальной платёжной системы и стандартами индустрии.

9.3. IT Cody использует полученный **статус оплаты** исключительно для:

- активации подписки «Disk»;
 - подтверждения заказа IT-услуг;
 - формирования учётных записей о платеже.
-

10. Хранение информации о платежах

10.1. IT Cody может хранить **не чувствительные** сведения о транзакции:

- дата и время;
- сумма;
- способ оплаты (Система быстрых платежей / банковские карты / по реквизитам);
- идентификатор операции в платёжном сервисе;
- e-mail учётной записи.

10.2. Указанные данные используются для исполнения договора, возвратов и ответов на обращения пользователей (см. **Политику возврата, Порядок рассмотрения претензий**).

10.3. Срок хранения — в соответствии с **Политикой конфиденциальности** и требованиями налогового законодательства РФ.

11. Ответственность сторон

11.1. IT Cody обеспечивает безопасность **своей инфраструктуры** и корректную интеграцию с платёжным сервисом.

11.2. **Платёжный сервис и банк-эквайер** несут ответственность за безопасность обработки платёжных данных **на этапе ввода карты и проведения транзакции** в рамках их правил и договоров.

11.3. IT Cody **не несёт ответственности** за перебои в работе платёжного сервиса, банков или операторов связи, если они не вызваны виной Оператора.

12. Изменение Политики

12.1. Оператор вправе обновлять настоящий документ. Актуальная версия публикуется на Сайте с указанием даты редакции.

12.2. Продолжение использования Сайта и оплаты услуг после публикации новой редакции означает согласие с обновлёнными условиями в части, не требующей отдельного согласия по закону.

13. Контакты и реквизиты

По вопросам информационной безопасности и оплаты:

- **E-mail:** support@itcody.ru
- **Сайт:** <https://itcody.ru>

Наименование	Индивидуальный предприниматель Новиков Владимир Игоревич
Бренд	IT Cody
ИНН	234401764206
ОГРНИП	325237500092343
Город	г. Краснодар
Адрес для корреспонденции	г. Краснодар, ул. Московская, д. 140А
E-mail	support@itcody.ru
Сайт	https://itcody.ru