

## **Разъяснение о политике информационной безопасности для интернет-эквайринга**

**Компания:** Общество с ограниченной ответственностью "ИНСТИТУТ ПЛАСТИЧЕСКОЙ ХИРУРГИИ" (ООО "ИНСТИТУТ ПЛАСТИЧЕСКОЙ ХИРУРГИИ" )  
**Дата утверждения:** 15.01.2010

### **1. Общие положения**

Настоящее разъяснение описывает меры по обеспечению информационной безопасности при приеме онлайн-платежей с использованием банковских карт (интернет-эквайринг).

Цель политики —

защита персональных данных и реквизитов платёжных карт клиентов, предотвращение несанкционированного доступа к информации, соблюдение требований законодательства и международных стандартов.

### **2. Применяемые стандарты безопасности**

Компания обеспечивает соответствие требованиям:

- **PCI DSS** (Payment Card Industry Data Security Standard) — международный стандарт безопасности данных платёжных карт.
- **ФЗ-152 «О персональных данных»** — законодательство РФ о защите персональных данных.
- Требования платёжных систем: Visa, MasterCard, «Мир».

### **3. Технические меры защиты**

Для обеспечения безопасности платежей применяются:

- **Шифрование данных** по протоколу TLS версии не ниже 1.2 при передаче данных между браузером клиента и платёжным шлюзом.
- **Токенизация** — замена реальных данных карты на уникальный токен, не имеющий ценности для злоумышленников.
- **Технология 3D Secure** (Verified by Visa, MasterCard SecureCode, Mir Accept) — дополнительная аутентификация держателя карты через SMS-код или push-уведомление.

- **Антифрод-системы** — автоматический анализ транзакций на признаки мошенничества (проверка IP-адреса, лимиты на сумму и частоту операций и др.).
- **Защищённое соединение HTTPS** на всех страницах, связанных с оплатой.

#### **4. Обработка и хранение данных**

- Реквизиты банковских карт **не хранятся** на серверах компании. Обработка и хранение данных осуществляются на стороне сертифицированного платёжного агрегатора/банка.
- Персональные данные клиентов (ФИО, e-mail, телефон) обрабатываются только в целях выполнения договорных обязательств и хранятся в защищённых базах данных.
- Доступ к конфиденциальной информации ограничен и предоставляется только уполномоченным сотрудникам.

#### **5. Обязанности компании**

Компания обязуется:

- Обеспечивать защиту информационных ресурсов от внешних и внутренних угроз.
- Немедленно уведомлять банк и клиентов о случаях нарушения конфиденциальности (при наличии оснований).
- Регулярно обновлять программное обеспечение и антивирусную защиту.
- Проводить аудит безопасности и тестирование на проникновение.
- Обучать сотрудников правилам информационной безопасности.

#### **6. Обязанности клиента**

При проведении платежей клиент обязан:

- Использовать только личные и легитимные платёжные инструменты.
- Не передавать реквизиты карты третьим лицам.
- Незамедлительно сообщать банку о подозрительных операциях.

#### **7. Порядок реагирования на инциденты**

В случае выявления нарушения безопасности:

1. Блокировка подозрительных транзакций.
2. Уведомление банка и платёжных систем.
3. Информирование затронутых клиентов (при необходимости).
4. Проведение внутреннего расследования и устранение причин инцидента.

## 8. Контактная информация

По вопросам безопасности платежей и обработки данных обращайтесь:

- Телефон: 74957885806
- E-mail: [info@institutbeauty.ru](mailto:info@institutbeauty.ru)
- Форма обратной связи на сайте: через форму обратной связи на сайте <https://institutbeauty.ru/>

---

**Примечание:** Настоящее разъяснение является частью публичной оферты компании и подлежит размещению на сайте в разделе «Безопасность платежей» или «Политика конфиденциальности».

Генеральный директор

ООО «Институт пластической хирургии»



Я.Э.Макарова

## Разъяснение о политике информационной безопасности для интернет-эквайринга

**Компания:** Общество с ограниченной ответственностью "ИНСТИТУТ ПЛАСТИЧЕСКОЙ ХИРУРГИИ" (ООО "ИНСТИТУТ ПЛАСТИЧЕСКОЙ ХИРУРГИИ" )

**Дата утверждения:** 15.01.2010

### 1. Общие положения

Настоящее разъяснение описывает меры по обеспечению информационной безопасности при приёме онлайн-платежей с использованием банковских карт (интернет-эквайринг).

Цель политики —

защита персональных данных и реквизитов платёжных карт клиентов, предотвращение несанкционированного доступа к информации, соблюдение требований законодательства и международных стандартов.

### 2. Применяемые стандарты безопасности

Компания обеспечивает соответствие требованиям:

- **PCI DSS** (Payment Card Industry Data Security Standard) — международный стандарт безопасности данных платёжных карт.
- **ФЗ-152 «О персональных данных»** — законодательство РФ о защите персональных данных.
- Требований платёжных систем: Visa, MasterCard, «Мир».

### 3. Технические меры защиты

Для обеспечения безопасности платежей применяются:

- **Шифрование данных** по протоколу TLS версии не ниже 1.2 при передаче данных между браузером клиента и платёжным шлюзом.
- **Токенизация** — замена реальных данных карты на уникальный токен, не имеющий ценности для злоумышленников.
- **Технология 3D Secure** (Verified by Visa, MasterCard SecureCode, Mir Accept) — дополнительная аутентификация держателя карты через SMS-код или push-уведомление.
- **Антифрод-системы** — автоматический анализ транзакций на признаки мошенничества (проверка IP-адреса, лимиты на сумму и частоту операций и др.).
- **Защищённое соединение HTTPS** на всех страницах, связанных с оплатой.

### 4. Обработка и хранение данных

- Реквизиты банковских карт **не хранятся** на серверах компании. Обработка и хранение данных осуществляются на стороне сертифицированного платёжного агрегатора/банка.
- Персональные данные клиентов (ФИО, e-mail, телефон) обрабатываются только в целях выполнения договорных обязательств и хранятся в защищённых базах данных.

- Доступ к конфиденциальной информации ограничен и предоставляется только уполномоченным сотрудникам.

#### **5. Обязанности компании**

Компания обязуется:

- Обеспечивать защиту информационных ресурсов от внешних и внутренних угроз.
- Немедленно уведомлять банк и клиентов о случаях нарушения конфиденциальности (при наличии оснований).
- Регулярно обновлять программное обеспечение и антивирусную защиту.
- Проводить аудит безопасности и тестирование на проникновение.
- Обучать сотрудников правилам информационной безопасности.

#### **6. Обязанности клиента**

При проведении платежей клиент обязан:

- Использовать только личные и легитимные платёжные инструменты.
- Не передавать реквизиты карты третьим лицам.
- Незамедлительно сообщать банку о подозрительных операциях.

#### **7. Порядок реагирования на инциденты**

В случае выявления нарушения безопасности:

1. Блокировка подозрительных транзакций.
2. Уведомление банка и платёжных систем.
3. Информирование затронутых клиентов (при необходимости).
4. Проведение внутреннего расследования и устранение причин инцидента.

#### **8. Контактная информация**

По вопросам безопасности платежей и обработки данных обращайтесь:

- Телефон: 74957883593
- E-mail: [nfo@doktorvolos.ru](mailto:nfo@doktorvolos.ru)
- Форма обратной связи на сайте: через форму обратной связи на сайте <https://doktorvolos.ru/>

**Примечание:** Настоящее разъяснение является частью публичной оферты компании и подлежит размещению на сайте в разделе «Безопасность платежей» или «Политика конфиденциальности».

Генеральный директор

ООО «Институт пластической хирургии»



Я.Э.Макарова

## Разъяснение о политике информационной безопасности для интернет-эквайринга

**Компания:** Общество с ограниченной ответственностью "ИНСТИТУТ ПЛАСТИЧЕСКОЙ ХИРУРГИИ" (ООО "ИНСТИТУТ ПЛАСТИЧЕСКОЙ ХИРУРГИИ" )

**Дата утверждения:** 15.01.2010

### 1. Общие положения

Настоящее разъяснение описывает меры по обеспечению информационной безопасности при приёме онлайн-платежей с использованием банковских карт (интернет-эквайринг).

Цель политики —

защита персональных данных и реквизитов платёжных карт клиентов, предотвращение несанкционированного доступа к информации, соблюдение требований законодательства и международных стандартов.

### 2. Применяемые стандарты безопасности

Компания обеспечивает соответствие требованиям:

- **PCI DSS** (Payment Card Industry Data Security Standard) — международный стандарт безопасности данных платёжных карт.
- **ФЗ-152 «О персональных данных»** — законодательство РФ о защите персональных данных.
- Требования платёжных систем: Visa, MasterCard, «Мир».

### 3. Технические меры защиты

Для обеспечения безопасности платежей применяются:

- **Шифрование данных** по протоколу TLS версии не ниже 1.2 при передаче данных между браузером клиента и платёжным шлюзом.
- **Токенизация** — замена реальных данных карты на уникальный токен, не имеющий ценности для злоумышленников.
- **Технология 3D Secure** (Verified by Visa, MasterCard SecureCode, Mir Accept) — дополнительная аутентификация держателя карты через SMS-код или push-уведомление.
- **Антифрод-системы** — автоматический анализ транзакций на признаки мошенничества (проверка IP-адреса, лимиты на сумму и частоту операций и др.).
- **Защищённое соединение HTTPS** на всех страницах, связанных с оплатой.

### 4. Обработка и хранение данных

- Реквизиты банковских карт **не хранятся** на серверах компании. Обработка и хранение данных осуществляются на стороне сертифицированного платёжного агрегатора/банка.
- Персональные данные клиентов (ФИО, e-mail, телефон) обрабатываются только в целях выполнения договорных обязательств и хранятся в защищённых базах данных.

- Доступ к конфиденциальной информации ограничен и предоставляется только уполномоченным сотрудникам.

#### **5. Обязанности компании**

Компания обязуется:

- Обеспечивать защиту информационных ресурсов от внешних и внутренних угроз.
- Немедленно уведомлять банк и клиентов о случаях нарушения конфиденциальности (при наличии оснований).
- Регулярно обновлять программное обеспечение и антивирусную защиту.
- Проводить аудит безопасности и тестирование на проникновение.
- Обучать сотрудников правилам информационной безопасности.

#### **6. Обязанности клиента**

При проведении платежей клиент обязан:

- Использовать только личные и легитимные платёжные инструменты.
- Не передавать реквизиты карты третьим лицам.
- Незамедлительно сообщать банку о подозрительных операциях.

#### **7. Порядок реагирования на инциденты**

В случае выявления нарушения безопасности:

1. Блокировка подозрительных транзакций.
2. Уведомление банка и платёжных систем.
3. Информирование затронутых клиентов (при необходимости).
4. Проведение внутреннего расследования и устранение причин инцидента.

#### **8. Контактная информация**

По вопросам безопасности платежей и обработки данных обращайтесь:

- Телефон: 74957883524
- E-mail: [info@nomosclinic.ru](mailto:info@nomosclinic.ru)
- Форма обратной связи на сайте: через форму обратной связи на сайте <https://nomosclinic.ru/>

---

**Примечание:** Настоящее разъяснение является частью публичной оферты компании и подлежит размещению на сайте в разделе «Безопасность платежей» или «Политика конфиденциальности».

Генеральный директор

ООО «Институт пластической хирургии»



Я.Э.Макарова