Меры по обеспечению безопасности проведения операций с использованием реквизитов карт

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

1. Общие положения

Настоящий документ определяет комплекс мер по обеспечению безопасности операций с использованием реквизитов банковских карт при приёме платежей в электронной коммерции (интернет-эквайринг).

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

2. Нормативно-правовая база

При реализации мер безопасности организация руководствуется:

- Федеральным законом № 152-ФЗ «О персональных данных»;
- требованиями Банка России;
- стандартом PCI DSS (Payment Card Industry Data Security Standard);
- правилами международных платёжных систем (Visa, MasterCard, «Мир»);
- внутренними регламентами организации.

3. Технические меры безопасности

3.1. Шифрование данных:

- применение протокола TLS версии не ниже 1.2 для передачи данных между браузером клиента и платёжным шлюзом;
- использование 256-битного шифрования для защиты конфиденциальной информации.

3.2. Токенизация:

- замена реальных данных карты (номер, CVV) на уникальный токен, не имеющий ценности для злоумышленников;
- хранение токенов вместо фактических реквизитов карт.

3.3. Многофакторная аутентификация:

- внедрение технологии 3D Secure (Verified by Visa, MasterCard SecureCode, Mir Accept) с подтверждением операций через SMS-код или push-уведомление.

3.4. Антифрод-системы:

- автоматический анализ транзакций на признаки мошенничества (проверка IP-адреса, геолокации, истории покупок);
- установка лимитов на сумму и количество операций с одной карты за определённый период;
- ведение «чёрных» и «белых» списков клиентов.

3.5. Защита инфраструктуры:

- использование межсетевых экранов (файрволов) для защиты корпоративных сете й;
- регулярное обновление антивирусного ПО и установка патчей безопасности;
- защита от DDoS-атак платёжного шлюза.

3.6. Веб-безопасность:

- работа сайта по протоколу HTTPS с действительным SSL-сертификатом;
- проверка URL-адреса на наличие префикса https:// и значка замка в браузере.

4. Организационные меры

4.1. Контроль доступа:

- ограничение доступа к платёжному модулю и административной панели сайта тол ько для уполномоченных сотрудников;
- применение сложных паролей и двухфакторной аутентификации для входа в сист емы.

4.2. Обработка и хранение данных:

- отсутствие хранения реквизитов карт на серверах организации (данные обрабаты ваются и хранятся на стороне сертифицированного платёжного агрегатора/банка);
- шифрование баз данных с персональными данными клиентов (ФИО, e-mail, телеф он);
- резервное копирование информации для быстрого восстановления после инциден тов.

4.3. Обучение персонала:

- регулярные тренинги по кибербезопасности и распознаванию мошеннических схе м;
- ознакомление сотрудников с процедурами реагирования на инциденты.

5. Процедурные меры

5.1. Мониторинг и аудит:

- непрерывный мониторинг транзакций с использованием SIEM-систем;
- логирование всех операций с возможностью ретроспективного анализа;
- проведение регулярных тестов на проникновение (пентестов) и сканирование уязв имостей.

5.2. Реагирование на инциденты:

- немедленная блокировка подозрительных транзакций;
- уведомление банка и платёжных систем о выявленных нарушениях;
- информирование затронутых клиентов (при необходимости);
- внутреннее расследование и устранение причин инцидента.

5.3. Документация:

- актуализация политик информационной безопасности;

- ведение журнала учёта инцидентов и мер по их устранению.

6. Дополнительные рекомендации

6.1. Для клиентов:

- подключение SMS- и push-уведомлений о транзакциях;
- использование виртуальных карт для онлайн-платежей с ограниченным лимитом;
- избегание публичных Wi-Fi сетей при проведении платежей (или использование V PN).

6.2. Для организации:

- работа только с сертифицированными платёжными агрегаторами и банками;
- внедрение капчи для защиты от автоматических атак;
- ограничение количества попыток ввода пароля для защиты от брутфорс-атак.

7. Ответственность и контроль

7.1. Ответственность:

- сотрудники, нарушившие требования безопасности, несут дисциплинарную, матер иальную или иную ответственность в соответствии с законодательством РФ и вну тренними регламентами.

7.2. Контроль:

- ежегодный аудит соответствия требованиям PCI DSS;
- периодические проверки системы безопасности внутренними и внешними специал истами.

8. Контактная информация

По вопросам безопасности платежей и обработки данных обращайтесь:

- Телефон: 74957885806
- E-mail: info@institutbeauty.ru
- Форма обратной связи на сайте: через форму обратной связи на сайте https://institutbeauty.ru/

Примечание: настоящий документ является обязательным для исполнения всеми подразделениями организации, участвующими в обработке платёжных данных. И зменения в меры безопасности вносятся приказом руководителя организации.

Генеральный директор

ООО «Институт пластической хирургии» _____ Я.Э.Макарова

Меры по обеспечению безопасности проведения операций с использованием реквизитов карт

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

1. Общие положения

Настоящий документ определяет комплекс мер по обеспечению безопасности операций с использованием реквизитов банковских карт при приёме платежей в электронной коммерции (интернет-эквайринг).

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

2. Нормативно-правовая база

При реализации мер безопасности организация руководствуется:

- Федеральным законом № 152-ФЗ «О персональных данных»;
- требованиями Банка России;
- стандартом PCI DSS (Payment Card Industry Data Security Standard);
- правилами международных платёжных систем (Visa, MasterCard, «Мир»);
- внутренними регламентами организации.

3. Технические меры безопасности

3.1. Шифрование данных:

- применение протокола TLS версии не ниже 1.2 для передачи данных между браузером клиента и платёжным шлюзом;
- использование 256-битного шифрования для защиты конфиденциальной информации.

3.2. Токенизация:

- замена реальных данных карты (номер, CVV) на уникальный токен, не имеющий ценности для злоумышленников;
- хранение токенов вместо фактических реквизитов карт.

3.3. Многофакторная аутентификация:

- внедрение технологии 3D Secure (Verified by Visa, MasterCard SecureCode, Mir Accept) с подтверждением операций через SMS-код или push-уведомление.

3.4. Антифрод-системы:

- автоматический анализ транзакций на признаки мошенничества (проверка IP-адреса, геолокации, истории покупок);
- установка лимитов на сумму и количество операций с одной карты за определённый период;
- ведение «чёрных» и «белых» списков клиентов.

3.5. Защита инфраструктуры:

- использование межсетевых экранов (файрволов) для защиты корпоративных сетей;
- регулярное обновление антивирусного ПО и установка патчей безопасности;
- защита от DDoS-атак платёжного шлюза.

3.6. Веб-безопасность:

- работа сайта по протоколу HTTPS с действительным SSL-сертификатом;
- проверка URL-адреса на наличие префикса https:// и значка замка в браузере.

4. Организационные меры

4.1. Контроль доступа:

- ограничение доступа к платёжному модулю и административной панели сайта только для уполномоченных сотрудников;
- применение сложных паролей и двухфакторной аутентификации для входа в системы.

4.2. Обработка и хранение данных:

- отсутствие хранения реквизитов карт на серверах организации (данные обрабатываются и хранятся на стороне сертифицированного платёжного агрегатора/банка);
- шифрование баз данных с персональными данными клиентов (ФИО, e-mail, телефон);
- резервное копирование информации для быстрого восстановления после инцидентов.

4.3. Обучение персонала:

- регулярные тренинги по кибербезопасности и распознаванию мошеннических схем;
- ознакомление сотрудников с процедурами реагирования на инциденты.

5. Процедурные меры

5.1. Мониторинг и аудит:

- непрерывный мониторинг транзакций с использованием SIEM-систем;
- логирование всех операций с возможностью ретроспективного анализа;
- проведение регулярных тестов на проникновение (пентестов) и сканирование уязвимостей.

5.2. Реагирование на инциденты:

- немедленная блокировка подозрительных транзакций;
- уведомление банка и платёжных систем о выявленных нарушениях;
- информирование затронутых клиентов (при необходимости);
- внутреннее расследование и устранение причин инцидента.

5.3. Документация:

- актуализация политик информационной безопасности;

- ведение журнала учёта инцидентов и мер по их устранению.

6. Дополнительные рекомендации

6.1. Для клиентов:

- подключение SMS- и push-уведомлений о транзакциях;
- использование виртуальных карт для онлайн-платежей с ограниченным лимитом;
- избегание публичных Wi-Fi сетей при проведении платежей (или использование V PN).

6.2. Для организации:

- работа только с сертифицированными платёжными агрегаторами и банками;
- внедрение капчи для защиты от автоматических атак;
- ограничение количества попыток ввода пароля для защиты от брутфорс-атак.

7. Ответственность и контроль

7.1. Ответственность:

- сотрудники, нарушившие требования безопасности, несут дисциплинарную, матер иальную или иную ответственность в соответствии с законодательством РФ и вну тренними регламентами.

7.2. Контроль:

- ежегодный аудит соответствия требованиям PCI DSS;
- периодические проверки системы безопасности внутренними и внешними специал истами.

8. Контактная информация

По вопросам безопасности платежей и обработки данных обращайтесь:

- Телефон: 74957883524
- E-mail: info@nomosclinic.ru
- Форма обратной связи на сайте: через форму обратной связи на сайте https://nomosclinic.ru/

Примечание: настоящий документ является обязательным для исполнения всеми подразделениями организации, участвующими в обработке платёжных данных. И зменения в меры безопасности вносятся приказом руководителя организации.

Генеральный директор

ООО «Институт пластической хирургии» _____ Я.Э.Макарова

Меры по обеспечению безопасности проведения операций с использованием реквизитов карт

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

1. Общие положения

Настоящий документ определяет комплекс мер по обеспечению безопасности операций с использованием реквизитов банковских карт при приёме платежей в электронной коммерции (интернет-эквайринг).

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

2. Нормативно-правовая база

При реализации мер безопасности организация руководствуется:

- Федеральным законом № 152-ФЗ «О персональных данных»;
- требованиями Банка России;
- стандартом PCI DSS (Payment Card Industry Data Security Standard);
- правилами международных платёжных систем (Visa, MasterCard, «Мир»);
- внутренними регламентами организации.

3. Технические меры безопасности

3.1. Шифрование данных:

- применение протокола TLS версии не ниже 1.2 для передачи данных между браузером клиента и платёжным шлюзом;
- использование 256-битного шифрования для защиты конфиденциальной информации.

3.2. Токенизация:

- замена реальных данных карты (номер, CVV) на уникальный токен, не имеющий ценности для злоумышленников;
- хранение токенов вместо фактических реквизитов карт.

3.3. Многофакторная аутентификация:

- внедрение технологии 3D Secure (Verified by Visa, MasterCard SecureCode, Mir Accept) с подтверждением операций через SMS-код или push-уведомление.

3.4. Антифрод-системы:

- автоматический анализ транзакций на признаки мошенничества (проверка IP-адреса, геолокации, истории покупок);
- установка лимитов на сумму и количество операций с одной карты за определённый период;
- ведение «чёрных» и «белых» списков клиентов.

3.5. Защита инфраструктуры:

- использование межсетевых экранов (файрволов) для защиты корпоративных сете й;
- регулярное обновление антивирусного ПО и установка патчей безопасности;
- защита от DDoS-атак платёжного шлюза.

3.6. Веб-безопасность:

- работа сайта по протоколу HTTPS с действительным SSL-сертификатом;
- проверка URL-адреса на наличие префикса https:// и значка замка в браузере.

4. Организационные меры

4.1. Контроль доступа:

- ограничение доступа к платёжному модулю и административной панели сайта тол ько для уполномоченных сотрудников;
- применение сложных паролей и двухфакторной аутентификации для входа в сист емы.

4.2. Обработка и хранение данных:

- отсутствие хранения реквизитов карт на серверах организации (данные обрабаты ваются и хранятся на стороне сертифицированного платёжного агрегатора/банка);
- шифрование баз данных с персональными данными клиентов (ФИО, e-mail, телеф он);
- резервное копирование информации для быстрого восстановления после инциден тов.

4.3. Обучение персонала:

- регулярные тренинги по кибербезопасности и распознаванию мошеннических схе м;
- ознакомление сотрудников с процедурами реагирования на инциденты.

5. Процедурные меры

5.1. Мониторинг и аудит:

- непрерывный мониторинг транзакций с использованием SIEM-систем;
- логирование всех операций с возможностью ретроспективного анализа;
- проведение регулярных тестов на проникновение (пентестов) и сканирование уязв имостей.

5.2. Реагирование на инциденты:

- немедленная блокировка подозрительных транзакций;
- уведомление банка и платёжных систем о выявленных нарушениях;
- информирование затронутых клиентов (при необходимости);
- внутреннее расследование и устранение причин инцидента.

5.3. Документация:

- актуализация политик информационной безопасности;

- ведение журнала учёта инцидентов и мер по их устранению.

6. Дополнительные рекомендации

6.1. Для клиентов:

- подключение SMS- и push-уведомлений о транзакциях;
- использование виртуальных карт для онлайн-платежей с ограниченным лимитом;
- избегание публичных Wi-Fi сетей при проведении платежей (или использование V PN).

6.2. Для организации:

- работа только с сертифицированными платёжными агрегаторами и банками;
- внедрение капчи для защиты от автоматических атак;
- ограничение количества попыток ввода пароля для защиты от брутфорс-атак.

7. Ответственность и контроль

7.1. Ответственность:

- сотрудники, нарушившие требования безопасности, несут дисциплинарную, матер иальную или иную ответственность в соответствии с законодательством РФ и вну тренними регламентами.

7.2. Контроль:

- ежегодный аудит соответствия требованиям PCI DSS;
- периодические проверки системы безопасности внутренними и внешними специал истами.

8. Контактная информация

По вопросам безопасности платежей и обработки данных обращайтесь:

- Телефон: 74957883593
- E-mail: nfo@doktorvolos.ru
- Форма обратной связи на сайте: через форму обратной связи на сайте https://doktorvolos.ru/

Примечание: настоящий документ является обязательным для исполнения всеми подразделениями организации, участвующими в обработке платёжных данных. И зменения в меры безопасности вносятся приказом руководителя организации.

Генеральный директор

ООО «Институт пластической хирургии» _____ Я.Э.Макарова