

ПРИЛОЖЕНИЕ 2

ПОЛИТИКА БЕЗОПАСНОСТИ ПЛАТЕЖЕЙ и обработки данных банковских карт АНО «Кладовая добра»

г. Тимашевск

«17» августа 2026 г.

Настоящий документ определяет условия обеспечения безопасности онлайн-платежей, порядок совершения безналичных пожертвований и меры защиты конфиденциальной информации при совершении транзакций на сайте <https://kladovayadobra.ru> (далее - Сайт), принадлежащем Автономной некоммерческой организации помощи гражданам, оказавшимся в трудной жизненной ситуации «Кладовая добра» (далее - Организация).

1. ОБЩИЕ ПОЛОЖЕНИЯ И ПОРЯДОК ОПЛАТЫ В СЕТИ ИНТЕРНЕТ

1.1. Жертвователь может совершить добровольное благотворительное пожертвование на Сайте с помощью банковских карт (МИР, Visa, Mastercard) и иных электронных платежных сервисов, доступных в форме пожертвования.

1.2. Проведение платежей осуществляется через специализированный процессинговый центр ООО «Миксплат Процессинг» (далее - Платёжный сервис).

1.3. При совершении пожертвования Жертвователь перенаправляется на защищенную платежную страницу Платёжного сервиса, где производит ввод необходимых реквизитов.

1.4. После успешного проведения пожертвования Жертвователю на указанный им адрес электронной почты направляется электронный кассовый чек с детальной информацией о совершенной транзакции (в соответствии с требованиями Федерального закона № 54-ФЗ).

2. ГАРАНТИИ БЕЗОПАСНОСТИ И ТЕХНОЛОГИИ ЗАЩИТЫ

2.1. Безопасность обработки интернет-платежей через Платёжный сервис «Миксплат Процессинг» гарантируется международными сертификатами соответствия стандарту безопасности данных индустрии платежных карт PCI DSS (Payment Card Industry Data Security Standard) наивысшего уровня.

2.2. Надежность проведения транзакций обеспечивается многоуровневой системой интеллектуального антифрод-мониторинга мошеннических операций, а также применением современной технологии безопасности 3D-Secure (Verified by Visa, Mastercard Identity Check, MirAccept).

2.3. Ввод реквизитов банковской карты осуществляется исключительно на защищенной платежной странице Платёжного сервиса. Передача данных от Жертвователя в процессинговую компанию происходит с использованием криптографического протокола шифрования высокой стойкости (TLS / HTTPS).

2.4. Дальнейшая передача информации осуществляется по закрытым банковским сетям, имеющим максимальный уровень защиты от перехвата и несанкционированного доступа.

3. КОНФИДЕНЦИАЛЬНОСТЬ ПЛАТЕЖНЫХ ДАННЫХ

3.1. Организация не получает, не обрабатывает и не хранит на своих серверах конфиденциальные данные банковских карт Жертвователей (полный номер карты, срок её действия, CVV2/CVC2-код).

3.2. Платёжный сервис не передаёт платежные данные Жертвователя третьим лицам, за исключением случаев, строго предусмотренных законодательством Российской Федерации и правилами платежных систем.

3.3. Если банковская карта Жертвователя поддерживает технологию 3D-Secure, проведение платежа требует дополнительного подтверждения одноразовым SMS-кодом или паролем, направляемым банком-эмитентом, выпустившим карту.

4. ПРАВИЛА ВВОДА ДАННЫХ БАНКОВСКИХ КАРТ

4.1. Для корректного совершения платежа Жертвователь вводит следующие реквизиты банковской карты строго в соответствии с их написанием на пластиковой карте:

- номер карты (указан на лицевой стороне, состоит из 16-19 цифр);
- срок действия карты (месяц и год, до которого действительна карта);
- имя и фамилия держателя карты (латинскими буквами, если указаны на карте);
- код безопасности (CVV2/CVC2 - 3 цифры, указанные на обратной стороне карты на полосе для подписи).

5. ВОЗМОЖНЫЕ ПРИЧИНЫ ОТКАЗА В ПРОВЕДЕНИИ ТРАНЗАКЦИИ

5.1. Банк-эмитент или Платёжный сервис могут отклонить операцию по следующим основаниям:

- банковская карта не предназначена для проведения платежей в сети Интернет (определяется банком-эмитентом);
- неверно введены реквизиты карты (ошибка в номере, сроке действия или CVV/CVC-коде);
- истёк срок действия банковской карты;
- на счете банковской карты недостаточно средств для совершения пожертвования;
- превышен лимит однократных, суточных или месячных операций, установленный банком-эмитентом;
- система антифрод-мониторинга зафиксировала подозрительную активность по карте (например, неоднократные попытки совершения идентичных платежей за короткий промежуток времени).

6. СЛУЖБА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ ПЛАТЕЖЕЙ

6.1. По вопросам, связанным с прохождением онлайн-платежей, списанием средств или техническими ошибками при совершении пожертвования, Жертвователь может обратиться в круглосуточную службу поддержки ООО «Миксплат Процессинг»:

- электронная почта: support@mixplat.ru
- телефон горячей линии: +7 (495) 775-06-00 (режим работы 24/7).

6.2. По вопросам целевого использования пожертвований и работы Организации:

- электронная почта АНО «Кладовая добра»: kladovayadobra@yandex.ru
- официальный сайт: <https://kladovayadobra.ru>

7. РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ ДЛЯ ЖЕРТВОВАТЕЛЕЙ

7.1. Никогда не передавайте полный номер карты, секретный CVV/CVC-код или одноразовые пароли из SMS третьим лицам.

7.2. Убедитесь, что соединение с сайтом защищено: в адресной строке браузера перед адресом <https://kladovayadobra.ru> отображается значок «закрытого замка».

8. РЕКВИЗИТЫ ОРГАНИЗАЦИИ

Полное наименование: Автономная некоммерческая организация помощи гражданам, оказавшимся в трудной жизненной ситуации «Кладовая добра»

ИНН: 2369010274 / КПП: 236901001 / ОГРН: 1232300052192

Юридический адрес: 352700, Краснодарский край, Тимашевский район, г. Тимашевск, ул. Ленина, д. 165А

Расчётный счёт: 40703810230000001056 в Краснодарском отделении № 8619 ПАО Сбербанк

БИК: 040349602 / Корр. счёт: 30101810100000000602

E-mail: kladovayadobra@yandex.ru

Директор
АНО «Кладовая добра»



Т.И. Халина