



УТВЕРЖДЕНО
Протоколом Внеочередного Общего собрания участников
Товарищества с ограниченной ответственностью
«Микрофинансовая организация «Kredit Seven Kazakhstan
(Кредит Себен-Казахстан)»
№31-03-2026 от «31» марта 2026 г.

**ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ОТ
НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПРИ ОКАЗАНИИ
МИКРОФИНАНСОВЫХ УСЛУГ ЭЛЕКТРОННЫМ СПОСОБОМ
ТОВАРИЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«МИКРОФИНАНСОВАЯ ОРГАНИЗАЦИЯ «KREDIT SEVEN KAZAKHSTAN
(КРЕДИТ СЕВЕН КАЗАХСТАН)»**



г. Алматы 2026 г.

Содержание

1. Общие положения	
2. Архитектура и защита инфраструктуры	3
3. Защита данных и передача информации	3
4. Идентификация и аутентификация клиентов	3
5. Заключение договора	3
6. Защита от несанкционированного доступа	4
7. Управление инцидентами	5
8. Заключительные положения	5
	5

1. Общие положения

1. Настоящий Порядок обеспечения безопасности и защиты информации от несанкционированного доступа при оказании микрофинансовых услуг электронным способом (далее по тексту – Порядок), определяет организационные и программно-технические меры по обеспечению безопасности и защиты информации от несанкционированного доступа при оказании микрофинансовых услуг электронным способом в Товариществе с ограниченной ответственностью «Микрофинансовая организация «Kredit Seven Kazakhstan (Кредит Сеवन Казахстан)», Порядок разработан на основании нормативных правовых актов Агентства Республики Казахстан по регулированию и развитию финансового рынка и в соответствии с требованиями законодательства Республики Казахстан, нормативно-правовых актов Республики Казахстан и внутренних нормативных документов Товарищества с ограниченной ответственностью «Микрофинансовая организация «Kredit Seven Kazakhstan (Кредит Сеवन Казахстан)» (далее по тексту – Компания, МФО).
2. Порядок распространяется на:
 - интернет-ресурс Компании <https://creditplus.kz>;
 - информационные системы, обеспечивающие оказание услуг.
3. Целью Порядка является:
 - защита персональных данных и информации, составляющей тайну предоставления микрокредита;
 - предотвращение несанкционированного доступа к данным;
 - обеспечение целостности, конфиденциальности и доступности информации.
4. Порядок является внутренним нормативным документом Компании и обязателен для исполнения всеми работниками.

2. Архитектура и защита инфраструктуры

1. Информационная система Компании построена с учетом принципов сегментации и изоляции.
2. Серверы, содержащие конфиденциальную информацию (включая базы данных и ключевые сервисы), размещаются в защищенном сегменте сети, недоступном из глобальной сети Интернет.
3. Публичный доступ осуществляется только к отдельному серверу (веб-уровень), не содержащему конфиденциальных данных.
4. Программно-технический комплекс интернет-ресурса <https://creditplus.kz> размещается в отдельной защищенной подсети.

3. Защита данных и передача информации

1. Передача данных между клиентом и сервером осуществляется с использованием защищенных протоколов (HTTPS).
2. Для защиты информации применяется:
 - шифрование трафика (SSL/TLS)
 - механизмы контроля целостности данных (хеширование)
3. Компания обеспечивает защиту от:
 - подмены сервера
 - перехвата данных
 - несанкционированного изменения информации
4. При выявлении несоответствий в процессе обмена данными транзакция блокируется.

4. Идентификация и аутентификация клиентов

1. Для регистрации в личном кабинете клиент — физическое лицо вводит

(прикрепляет) следующие данные:

- фамилию, имя, отчество (при его наличии), указанные в документе, удостоверяющем личность, за исключением свидетельства о рождении;
 - индивидуальный идентификационный номер;
 - номер и срок действия документа, удостоверяющего личность, за исключением свидетельства о рождении;
 - абонентский номер устройства сотовой связи;
 - фотография лица в анфас на светлом фоне, с нейтральным выражением лица и закрытым ртом.
2. При регистрации клиента применяется биометрическая идентификация посредством использования услуг ЦОИД или иных средств, предусмотренных законодательством Республики Казахстан, и электронная цифровая подпись клиента физического лица, представленная аккредитованным удостоверяющим центром Республики Казахстан.
 3. Последующий доступ клиента к личному кабинету осуществляется путем ввода логина и пароля либо с использованием дополнительных аутентификационных признаков (одноразовые пароли, токены и иные средства).
 4. Логин в системе Интернет - ресурса <https://creditplus.kz> является номер мобильного телефона, который Клиент указывает при прохождении процедуры регистрации.
 5. Для обеспечения защиты от несанкционированного доступа к информации, составляющей тайну предоставления микрокредита, Компания применяет автоматическую проверку правильности указания Клиентом логина и пароля при входе в личный кабинет.
 6. Клиент проходит идентификацию и аутентификацию в порядке, установленном законодательством Республики Казахстан.
 7. При вводе пароля допускается не более 3 попыток ввода пароля, после чего доступ блокируется на 15 минут.
 8. При отсутствии активности более 10 минут, после входа Клиентом в личный кабинет, осуществляется автоматическое завершение сессии.
 9. В целях безопасности сохранение логина и пароля Клиента для упрощения процедуры входа в личный кабинет не предусматривается.
 10. Внесение изменений в данные об абонентском номере устройства сотовой связи клиента или реквизитов банковского счета (за исключением предоставления микрокредитов посредством терминалов), осуществляется в личном кабинете клиента с применением биометрической идентификации посредством использования услуг ЦОИД или иных средств, предусмотренных законодательством Республики Казахстан, а также электронная цифровая подпись клиента.
 11. В личном кабинете не подлежат изменению данные об индивидуальном идентификационном номере клиента.

5. Заключение договора

1. Заключение договора о предоставлении микрокредита осуществляется в электронной форме.
2. Подписание договора, а также внесение изменений и дополнения в условия договора осуществляется с использованием:
 - биометрической идентификации посредством использования услуг ЦОИД;
 - электронной цифровой подписи, выданной аккредитованным удостоверяющим центром Республики Казахстан.
3. Предоставление микрокредита осуществляется путем перевода денежных средств с банковского счета Компании на банковский счет (платежную карточку) клиента при условии подтверждения их принадлежности клиенту, а также иными способами, предусмотренными законодательством Республики Казахстан.
4. В случае невозможности идентификации принадлежности банковского счета или платежной карты клиенту перевод денег не осуществляется.

5. В случаях, предусмотренных законодательством Республики Казахстан, выдача микрокредита электронным способом осуществляется не ранее чем через 24 часа после заключения договора и получения дополнительного согласия клиента.

6. Защита от несанкционированного доступа

1. В целях обеспечения защиты информации Компания применяет:
 - автоматическую проверку учетных данных;
 - контроль доступа к информационным системам;
 - ограничение доступа к конфиденциальной информации;
 - мониторинг действий пользователей.
 - регистрацию и хранение событий информационной безопасности, включая попытки несанкционированного доступа и действия пользователей;
 - предоставление доступа к информационным системам на основании принципа минимально необходимого доступа с учетом ролей и должностных обязанностей работников;
 - антифрод-систему, обеспечивающую выявление подозрительных операций, автоматическую проверку клиентов, возможность приостановления операций, а также интеграцию и передачу данных в антифрод-центр Национального Банка Республики Казахстан в соответствии с требованиями законодательства Республики Казахстан, а также регулярный анализ, тестирование и актуализацию ее параметров;
 - процедуры управления рисками мошенничества, включающие идентификацию и оценку рисков, определение индикаторов раннего выявления, ведение реестра рисков, рассмотрение обращений клиентов, проведение внутренних расследований, разработку и мониторинг мер по минимизации рисков, а также сбор и хранение информации о реализованных рисках мошенничества.
2. Доступ к информации, составляющей тайну предоставления микрокредита, предоставляется только в случаях предусмотренных законодательством Республики Казахстан
3. Компания вправе в одностороннем порядке осуществлять мероприятия в сторону улучшения для Клиента, касающиеся усиления процедур безопасности от мошеннических действий, разглашения конфиденциальной информации, или иных противоправных действий в рамках выявления и предотвращения потенциальных угроз и рисков информационной безопасности.

7. Управление инцидентами

1. Компания обеспечивает регистрацию и хранение событий информационной безопасности, включая попытки несанкционированного доступа и действия пользователей в информационных системах.
2. В случае выявления:
 - несанкционированного доступа;
 - несанкционированного изменения информации;
 - мошеннических действийКомпания незамедлительно принимает меры по устранению причин и последствий.
3. Компания уведомляет уполномоченный орган в сроки, установленные законодательством Республики Казахстан (не позднее 1 рабочего дня).

8. Заключительные положения

1. Компания осуществляет регулярный пересмотр и совершенствование мер информационной безопасности.
2. Порядок подлежит пересмотру не реже одного раза в год, а также при изменении законодательства или технологических процессов.
3. Актуальная версия Порядка размещается на интернет-ресурсе Компании.
4. Порядок утверждается и вводится в действие Протоколом внеочередного общего собрания участников МФО.