ПРИЛОЖЕНИЕ
к исх. 347-01.05-12/565 от 05.11.2026

Памятка (рекомендации) для пользователя портала ГИС ЭПД

Признаки мошеннических действий и иной нелегитимной активности выявляются на основе автоматизированного мониторинга (контроля) и поведенческого анализа посредством совокупности технических и организационных мер.

Основными механизмами автоматизированного мониторинга (контроля) и поведенческого анализа являются:

– фиксация технических параметров действий пользователя;

– скоринг, работающий как на уровне анализа технических параметров в рамках функций Портала ГИС ЭПД и анализа действий пользователя на Портале ГИС ЭПД, так и на уровне анализа цифрового следа пользователя и его устройства;

– анализ цифрового отпечатка (фингерпринтинг). В части фиксации цифрового следа пользователя используются идентификаторы пользователя, и его действий. В части фиксации цифрового следа устройства собирается информация об устройстве и браузере, плагинах браузера, наличии признаков вмешательства в трафик, геолокации, cookies.

Действия легитимного пользователя могут быть приняты за мошеннические или автоматизированные при наличии определенных признаков вмешательства в траффик и штатную работу портала. Чтобы легитимные пользователи не получали ошибки и не сталкивались с постоянными проверками и блокировками, необходимо соблюдать следующие рекомендации.

1. Сетевые настройки и подключение

- **Убедитесь, что корпоративные антивирусы, фаерволы или сетевые фильтры не подменяют SSL-сертификаты и не блокируют запросы, не используйте средства, вмешивающиеся в трафик (отключите VPN, анонимайзеры и прокси-серверы и используйте прямое подключение интернет провайдера).** Уровень доверия к трафику, поступающему из дата-центров, хостинговых подсетей, пулов VPN или иных узлов существенно понижается, также при подключении из таких узлов часто используется один внешний IP-адрес на сотни устройств и, если иное устройство в этой же сети спамит запросами или подменяет свой реальный IP-адрес адресом из иной страны (пункт пропуска – на границе РФ, страна из

которой поступил запрос, например – Мальта или Австралия), доступ может быть ограничен для всей подсети.

- **Следите за синхронизацией времени.** Расхождение между системным временем вашего устройства и реальным временем приводит к ошибкам при установлении соединения.

2. Настройки браузера и расширения

- **Разрешите выполнение JavaScript.** Система защиты проводит фоновые интерактивные проверки (JS-челленджи) для подтверждения того, что запросы отправляет реальный браузер. Если JavaScript отключен, доступ может быть ограничен.
- **Включите поддержку Cookies.** Служебные cookie-файлы необходимы для фиксации вашей легитимной сессии и пропуска последующих запросов без повторных проверок.
- **Не используйте антидетект- и приватные расширения.** При использовании плагинов, подменяющих параметры и заголовки устройства и браузера или эмулирующих фальшивые отпечатки (fingerprint), доступ может быть ограничен.
- **Отключите скрипты автообновления и автовыполнения запросов.** При использовании расширений браузера или иных средств, автоматически перезагружающих вкладки или отправляющих серии запросов к порталу, доступ может быть ограничен.
- **Устанавливайте браузер с официального сайта и регулярно обновляйте его.** Устаревшие версии браузеров имеют устаревший стек протоколов и механизмов, а также могут иметь встроенные вирусы и иные недокументированные средства, что снижает общую оценку безопасности сессии и может привести к фиксации подозрительной активности.

3. Поведение на портале

- **Не передавайте данные вашей учетной записи иным пользователям.** В случае наличия такого факта ранее – смените пароль, т.к. ваш личный кабинет может использоваться без вашего ведома для выполнения нелегитимных действий.
- **Не допускается одновременная работа в одном личном кабинете пользователя с нескольких устройств.** При организации такой работы доступ может быть ограничен.
- **Избегайте «сверхбыстрой» активности.** Открытие десятка вкладок портала за несколько секунд, многократные частые клики по кнопкам

отправки форм или спам-навигация вызывают срабатывание лимитов частоты запросов (rate limiting).

- **Не используйте самодельные макросы, скрипты и парсеры.** При автоматизации сбора информации или запросов через расширения или утилиты доступ может быть ограничен.
- **Не закрывайте страницу проверки сразу.** Если при входе на ресурс появилась промежуточная страница ожидания или капча, дождитесь завершения фоновой проверки и корректно пройдите подтверждение, не закрывая страницу преждевременно.