

**Руководство пользователя по  
эксплуатации  
программного обеспечения  
«Интегрированная платформа предупреждения мошенни-  
чества (ИППМ)» (далее – ИППМ)**

для расширения коммерциализации «Платформы цифрового доверия»

**Москва  
2024 г.**

**Оглавление**

1. Общие сведения.....	3
2. Работа с ИППМ.....	3
3. Демонстрационное веб-приложение .....	3
4. Примерный сценарий работы с демонстрационным веб-приложением .....	7

## **1. Общие сведения**

Программное обеспечение «Интегрированная платформа предупреждения мошенничества» (далее – ИППМ) представляет собой программное обеспечение, разработанное ООО «Системы управления идентификацией» (ИНН 7709982222) в 2023 году и предназначенное для предупреждения мошеннических действий в интернет-среде.

## **2. Работа с ИППМ**

Для установки ИППМ необходимо следовать инструкции «Руководство по установке программного обеспечения». Для работы с ИППМ необходимо следовать инструкции, описанной в настоящем документе. Пользователи с нарушением зрения должны также владеть навыками работы со специальными программами экранного доступа.

Перед началом работы с ИППМ, потребителю системы необходимо также произвести интеграцию его информационной системы с ИППМ, используя API клиентской библиотеки и ядра, описанные в документе «Функциональные и технические характеристики ИППМ». Интеграция выполняется потребителем в непосредственном контакте с разработчиком ИППМ, так как требует выделения идентификаторов и выполнения настроек, необходимых для реализации конкретных, индивидуальных задач потребителя по защите его веб-приложения.

Пример результата такой интеграции описан в разделе «3. Демонстрационное веб-приложение» данного документа.

Примерный сценарий работы с демонстрационным веб-приложением описан в разделе «4. Примерный сценарий работы с демонстрационным веб-приложением».

## **3. Демонстрационное веб-приложение**

Для демонстрации работы ИППМ реализовано веб-приложение «Демо-банк». В демонстрационном приложении реализовано 2 роли пользователей: администратор и клиент. На рисунке 3.1 представлено стартовая страница демонстрационного веб-приложения.

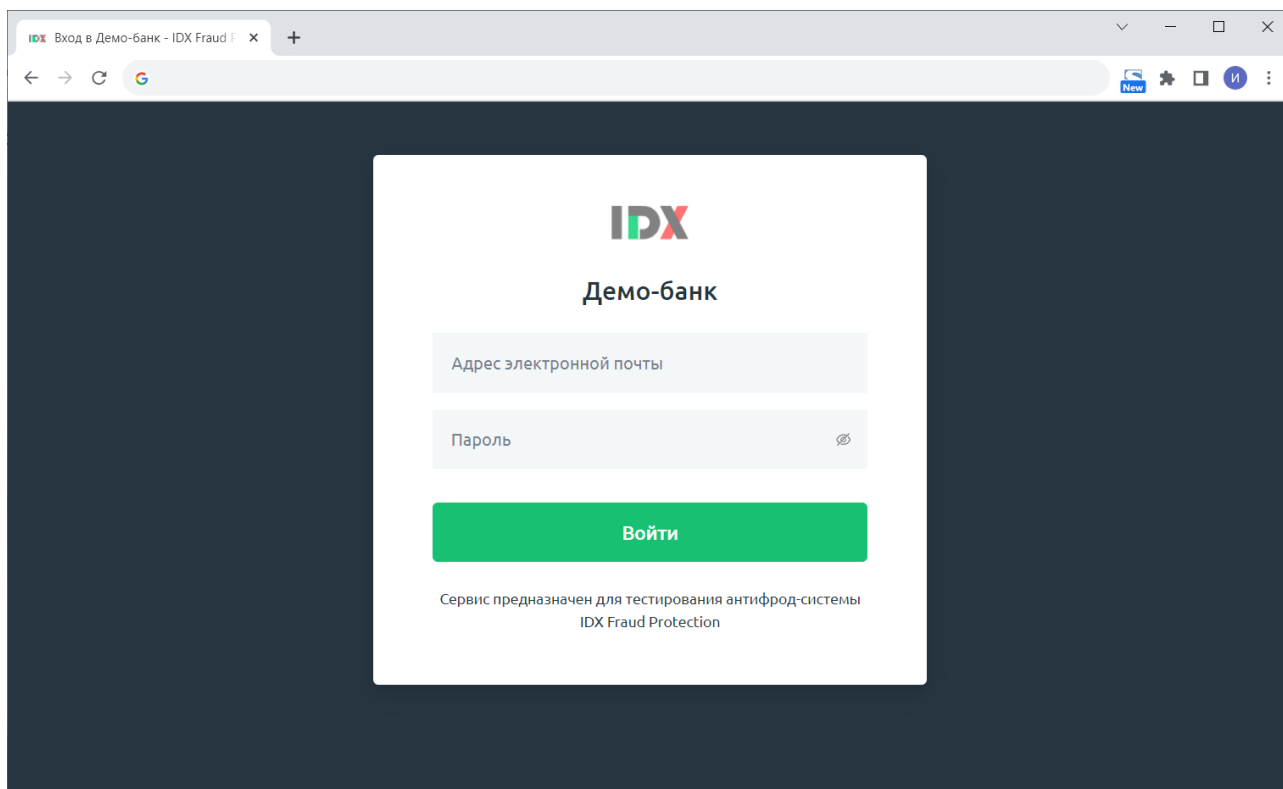


Рисунок 3.1 – Стартовая страница демонстрационного веб-приложения

В демонстрационное веб-приложение встроена клиентская библиотека ИППМ. При входе с ролью «Клиент» в демонстрационном веб-приложении отображаются результаты работы вызовов API клиентской библиотеки и ядра (например, методы установки начала и окончания сессии). Фрагмент веб-приложения при авторизации с ролью «Клиент» представлен на рисунке 3.2.

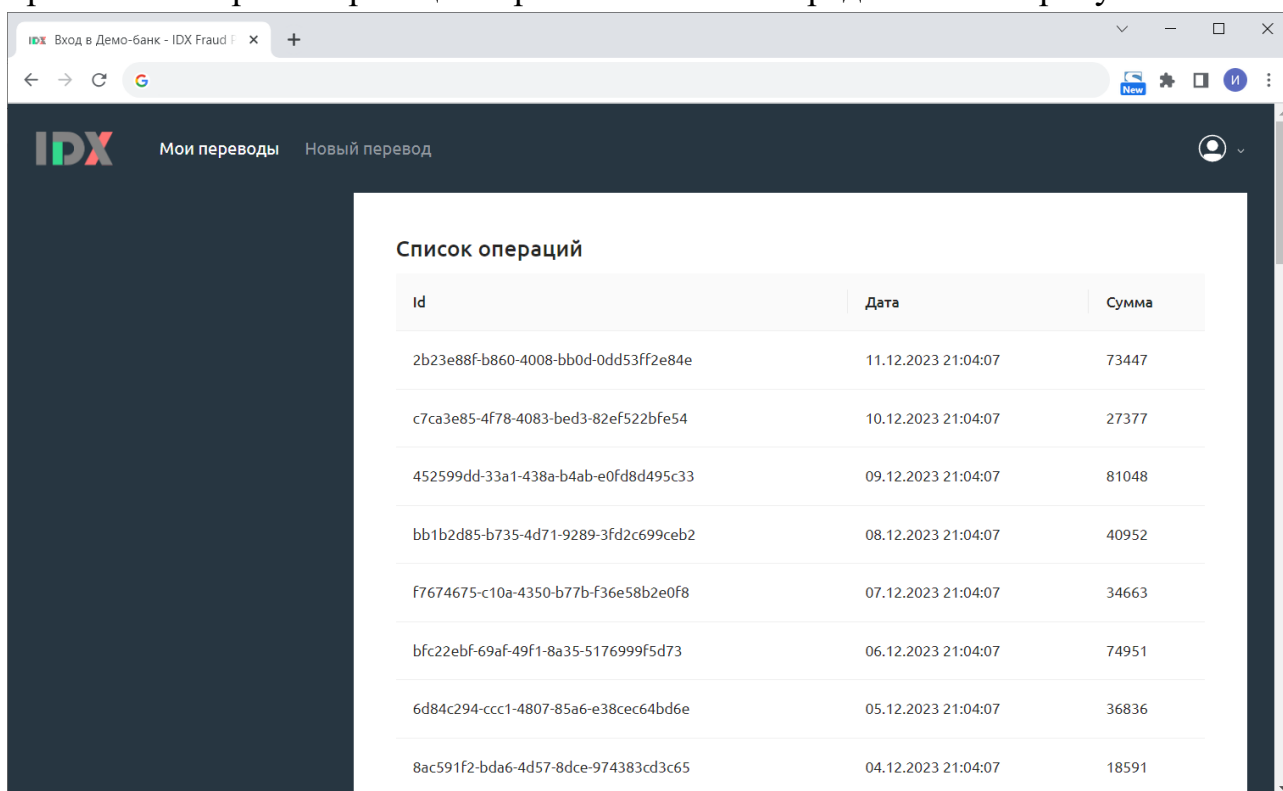


Рисунок 3.2 – Фрагмент веб-приложения при авторизации с ролью «Клиент»

При авторизации с ролью «Администратор» имеется возможность просматривать список всех клиентов и их сессий, добавлять новых клиентов, отправлять в ядро обратную связь по репутации сессии, вызывать методы получения списка инцидентов и списка атрибутов сессии. Интерфейс включает три вкладки: Пользователи, Проверка сессии и Моя сессия. На рисунке 3.3 представлен фрагмент веб-страницы вкладки «Пользователи».

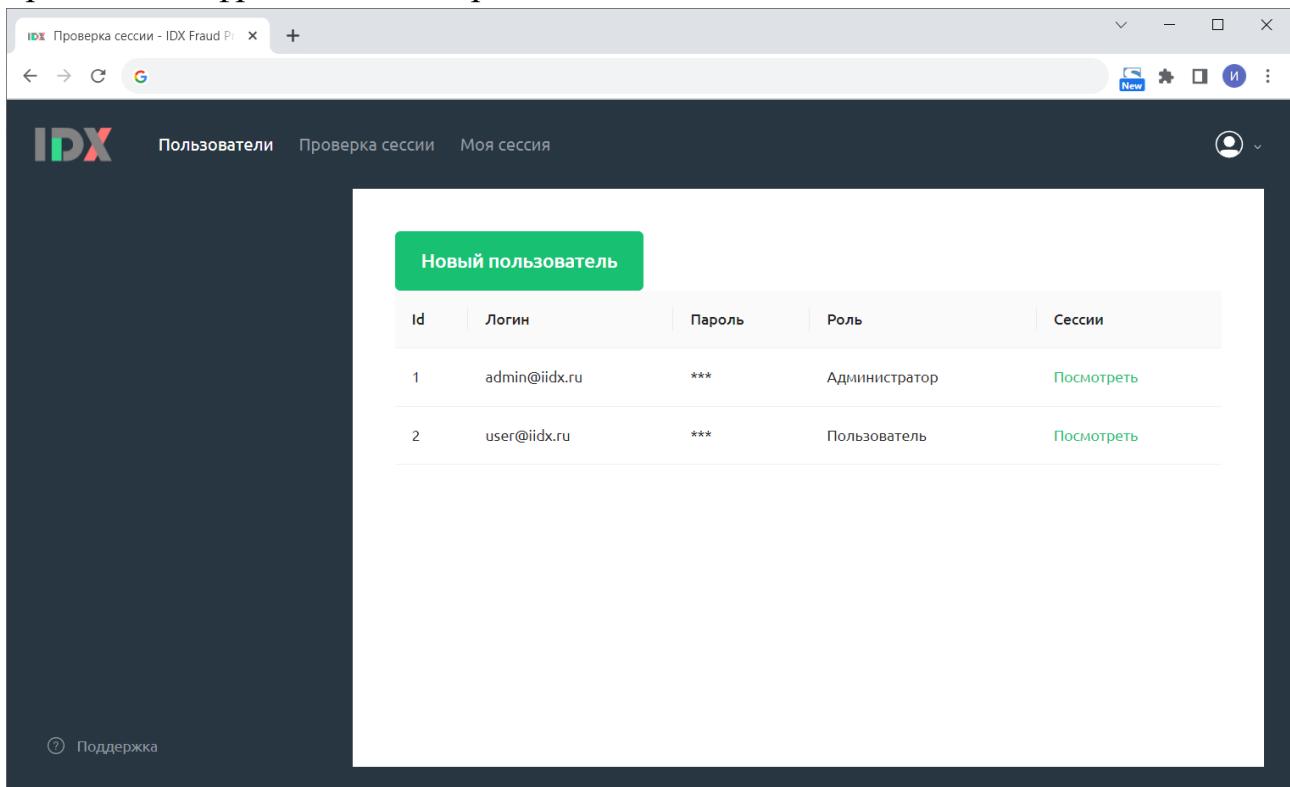


Рисунок 3.3 – Фрагмент веб-приложения на вкладке «Пользователи»

При переходе к клиенту (кнопка «Посмотреть») отображается таблица со списком последних сессий и есть возможность отправить обратную связь по репутации сессии (кнопка «Отметить инцидент»). На рисунке 3.4 представлен фрагмент веб-страницы со списком сессий клиента.

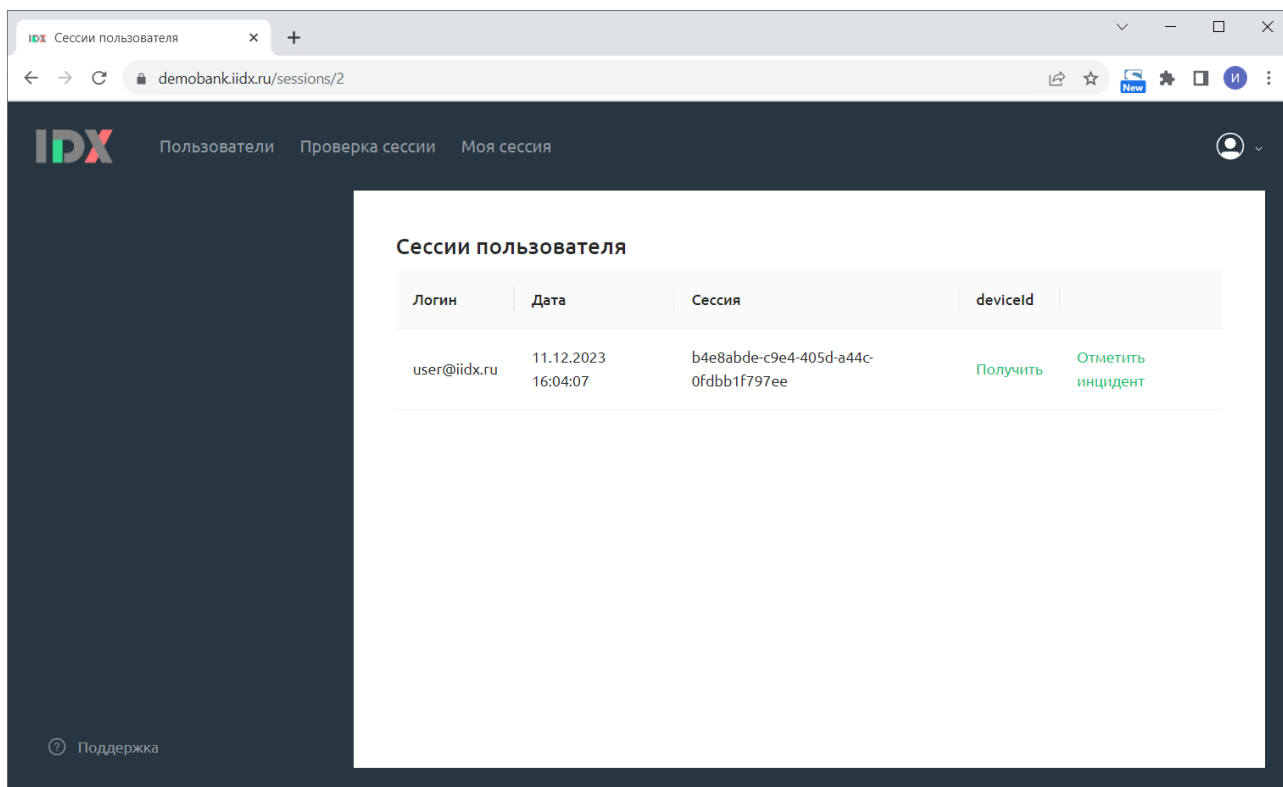


Рисунок 3.4 – Фрагмент веб-приложения со списком сессий клиента

В таблице со списком сессий клиента в колонке «Сессия» указывается идентификатор сессии, которую можно проверить на вкладке «Проверка сессии». Страница «Проверка сессии» включает форму с вводом идентификатора сессии. При отправке формы вызываются методы API ядра для получения списка инцидентов и списка атрибутов сессии. На рисунке 3.5 представлен фрагмент веб-страницы с информацией о сессии.

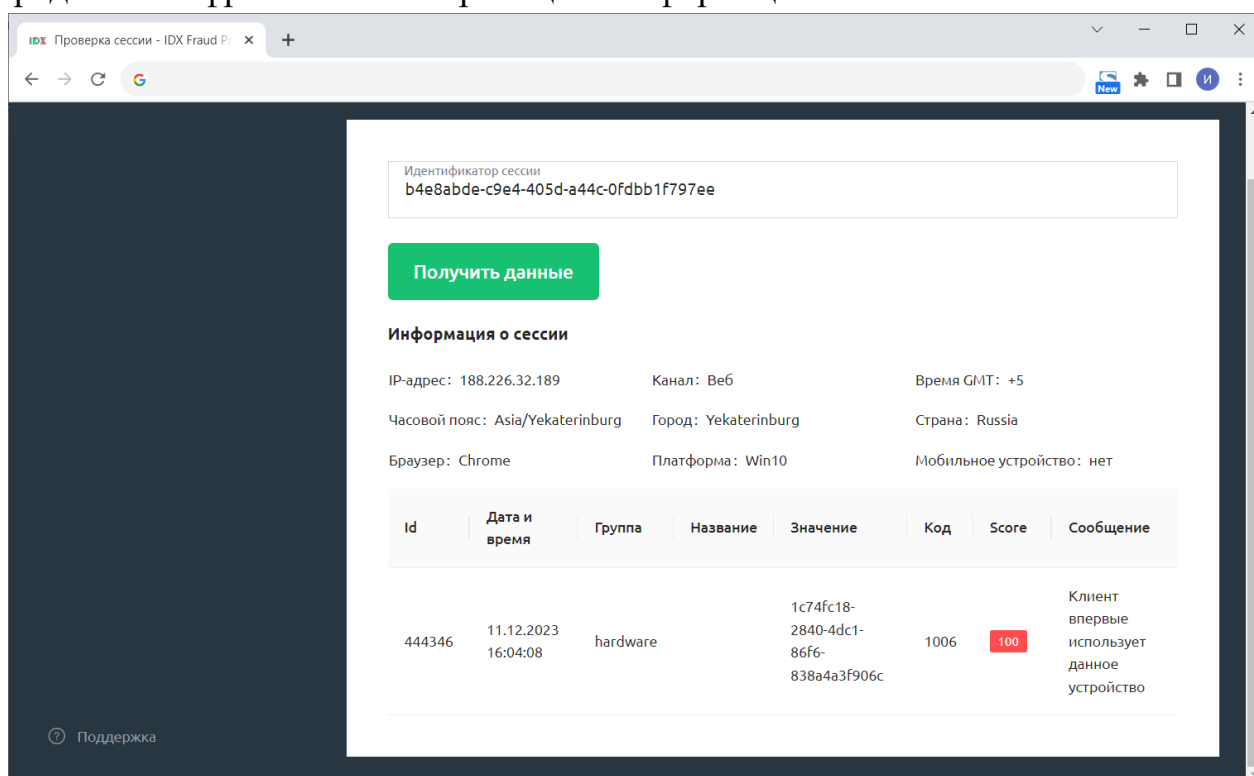


Рисунок 3.5 – Фрагмент веб-приложения с информацией о сессии

На вкладке «Моя сессия» продемонстрирована работа API клиентской библиотеки при вызове метода получения идентификатора сессии. На рисунке 3.6 представлен фрагмент веб-страницы со вкладки «Моя сессия».

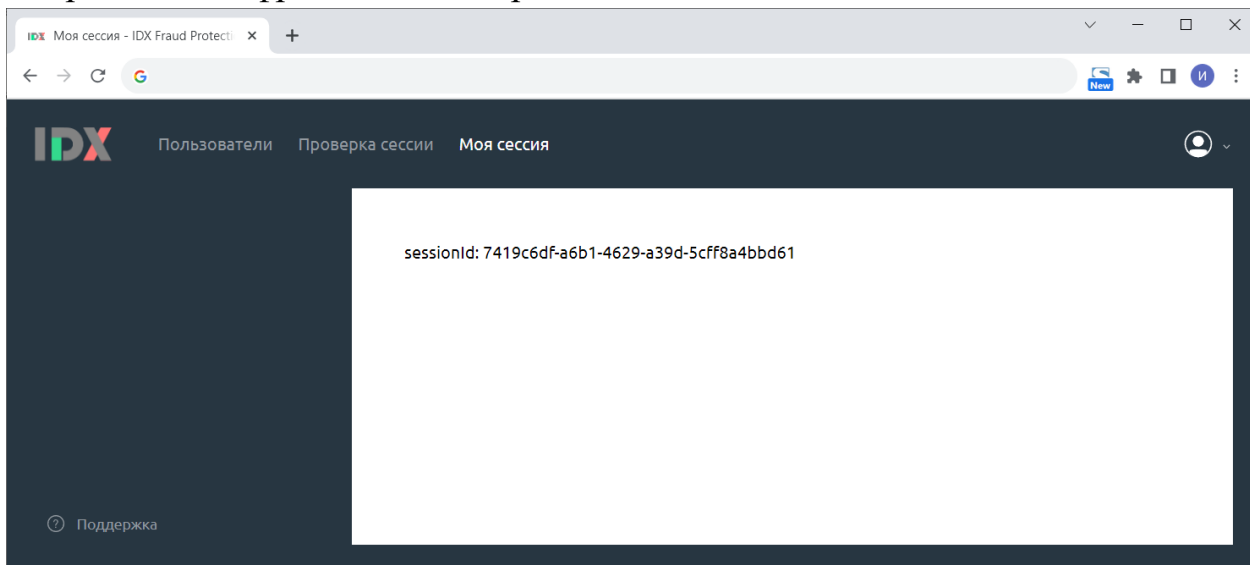


Рисунок 3.5 – Фрагмент веб-приложения со вкладки «Моя сессия»

#### 4. Примерный сценарий работы с демонстрационным веб-приложением

Для проверки различных сценариев работы с демонстрационным веб-приложением используется одна учетная запись с ролью «Администратор» (адрес электронной почты для входа - [admin@iidx.ru](mailto:admin@iidx.ru)) и две учетные записи с ролью «Клиент» (адреса электронной почты - [user1@iidx.ru](mailto:user1@iidx.ru), [user2@iidx.ru](mailto:user2@iidx.ru)). Пароли для входа в любую из этих учетных записей – iidx.

Т.к. сессии пользователей в демонстрационном веб-приложении привязываются с помощью Cookie, то при проверке сценариев для одновременного входа в разные учетные записи необходимо использовать разные браузеры или разные устройства.

Выполнение сценария осуществляется с помощью учетных записей с ролью «Клиент», а проверка сгенерированных инцидентов – в учетной записи с ролью «Администратор». Для проверки сгенерированных инцидентов необходимо в интерфейсе роли «Администратор» выбрать в списке учетную запись, с помощью которой выполнялся сценарий, скопировать последний идентификатор сессии (рисунок 4.1) и вставить его в соответствующее поле на странице «Проверка сессии» интерфейса роли «Администратор».

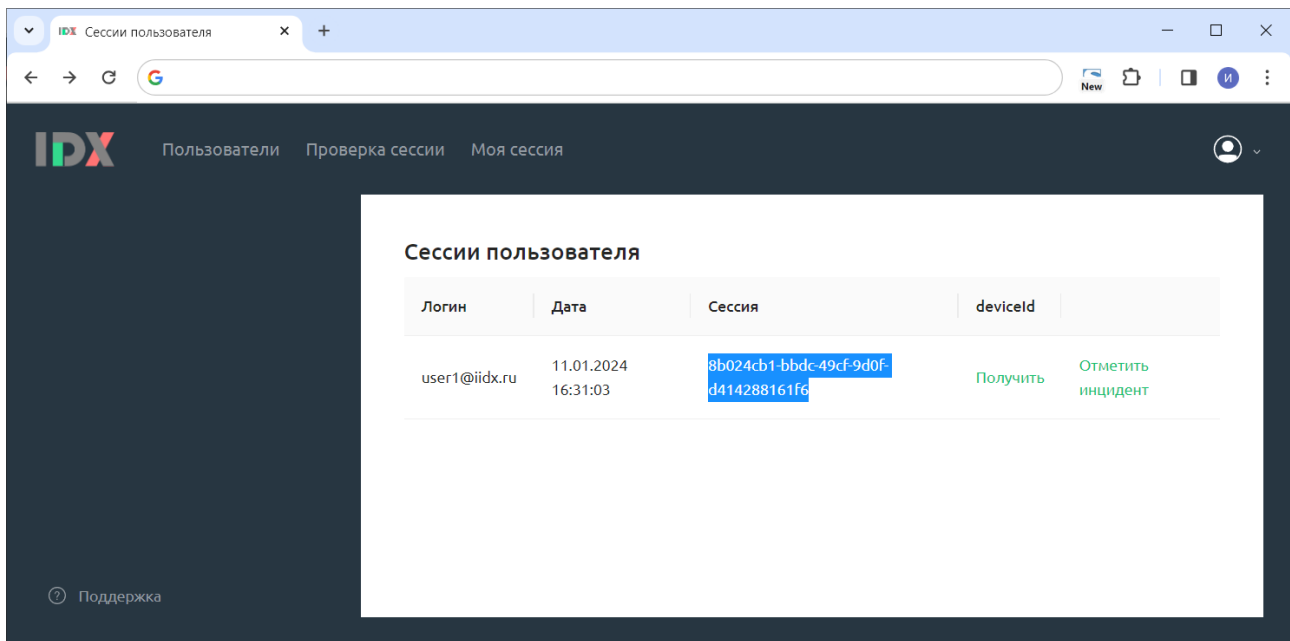


Рисунок 4.1 – Фрагмент веб-приложения со списком сессий клиента

При проверке каждого нового сценария в браузере, который ранее уже использовался для проверки предыдущего сценария, необходимо вначале выйти из учетной записи данного клиента (рисунок 4.2).

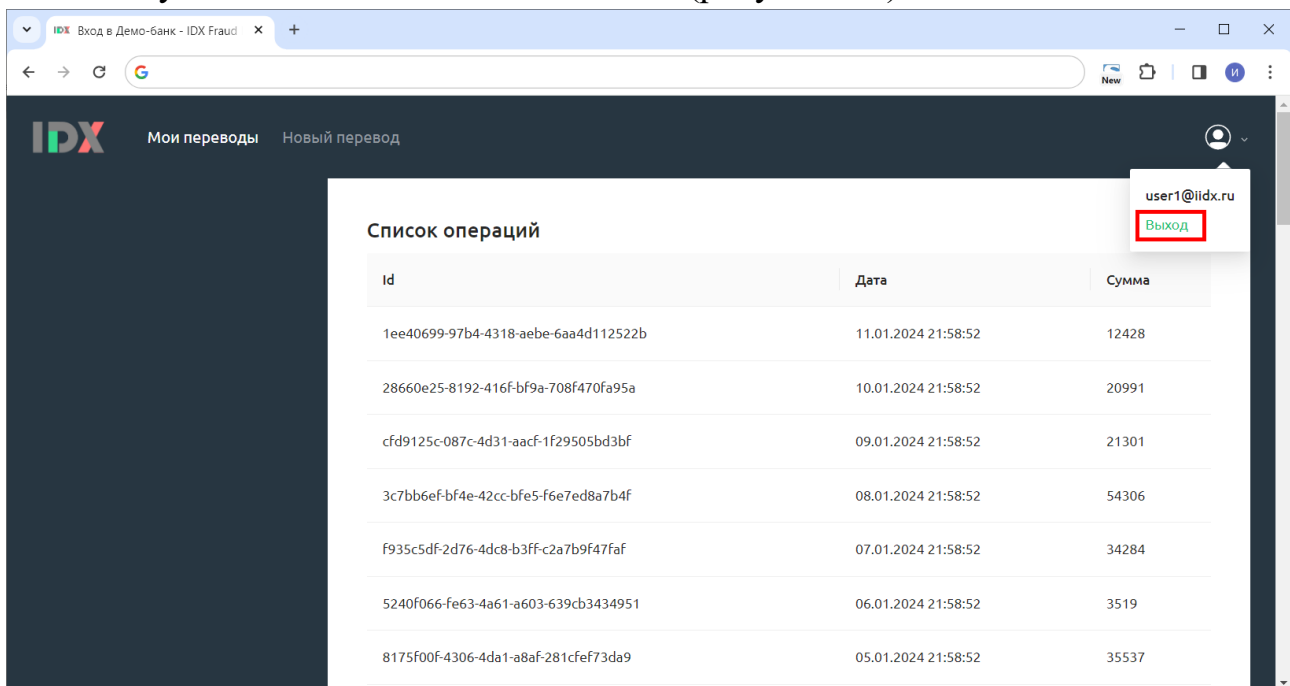


Рисунок 4.2 – Фрагмент веб-приложения со ссылкой выхода из системы

#### 4.1. Проверка сценария «Клиент впервые использует данное устройство»



Для проверки сценария необходимо выполнить вход в учетную запись [user1@iidx.ru](mailto:user1@iidx.ru) с нового устройства или из нового браузера. Ожидаемый результат проверки сессии для данного сценария представлен на рисунке 4.3.

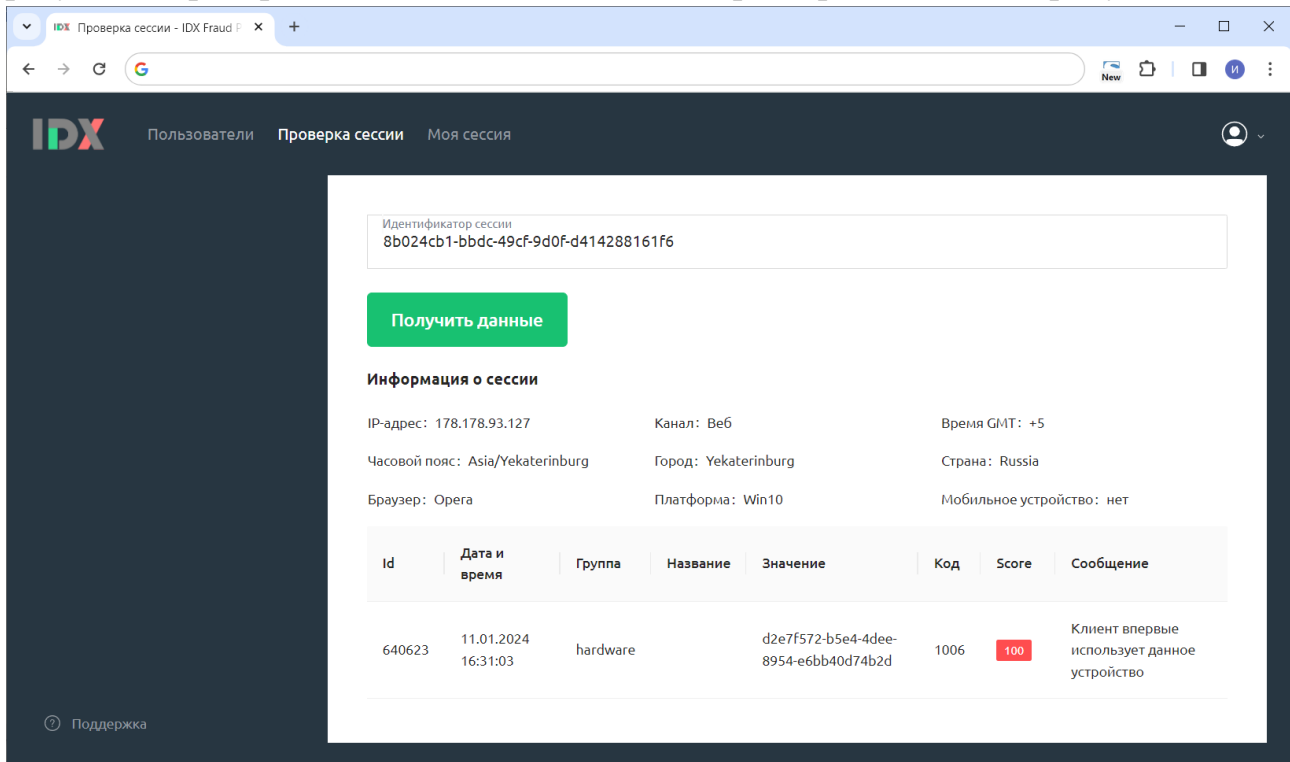


Рисунок 4.3 – Фрагмент веб-приложения с результатом проверки сессии по сценарию «Клиент впервые использует данное устройство»

#### 4.2. Проверка сценария «Клиент включил режим инкогнито»

Для проверки сценария необходимо выполнить вход в учетную запись [user1@iidx.ru](mailto:user1@iidx.ru) с включенным режимом «Инкогнито» в браузере. Ожидаемый результат проверки сессии для данного сценария представлен на рисунке 4.4.

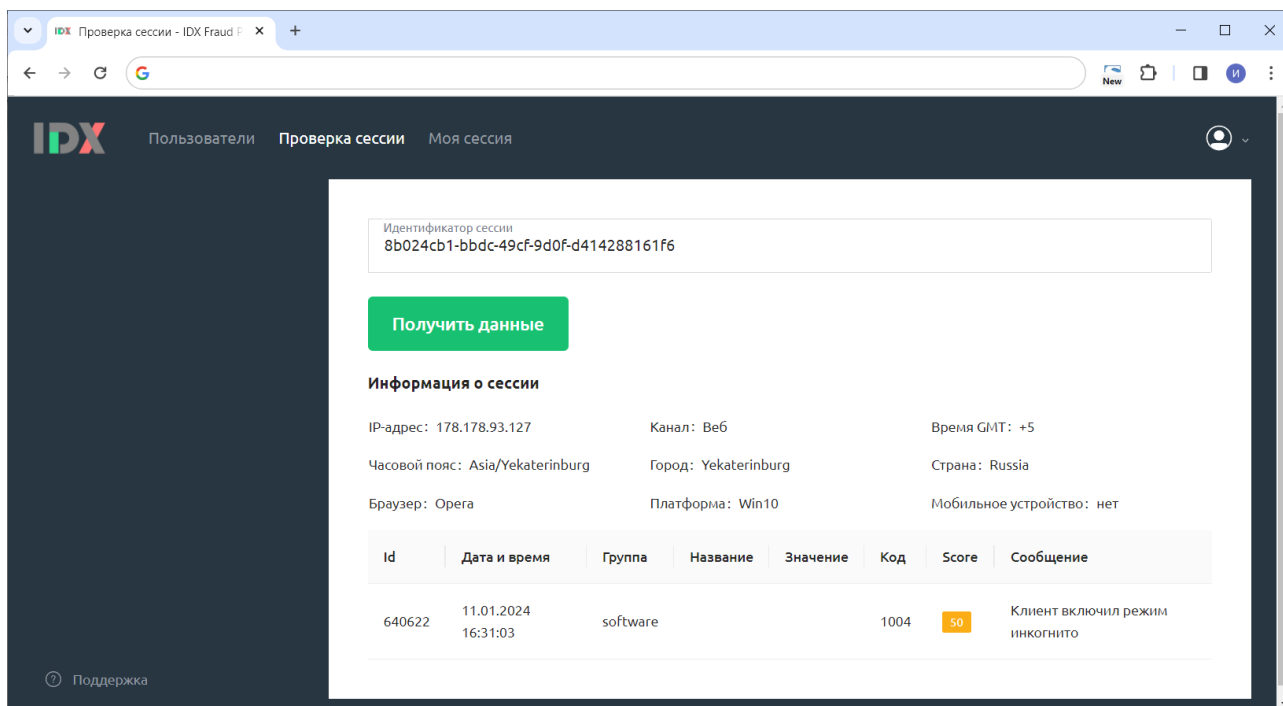


Рисунок 4.4 – Фрагмент веб-приложения с результатом проверки сессии по сценарию «Клиент включил режим инкогнито»

### 4.3. Проверка сценария «Клиент имеет более одной сессии одновременно»

Для проверки сценария необходимо выполнить вход в учетную запись [user1@iidx.ru](mailto:user1@iidx.ru) одновременно с двух разных браузеров или на двух разных устройствах. Ожидаемый результат проверки сессии для данного сценария представлен на рисунке 4.5.

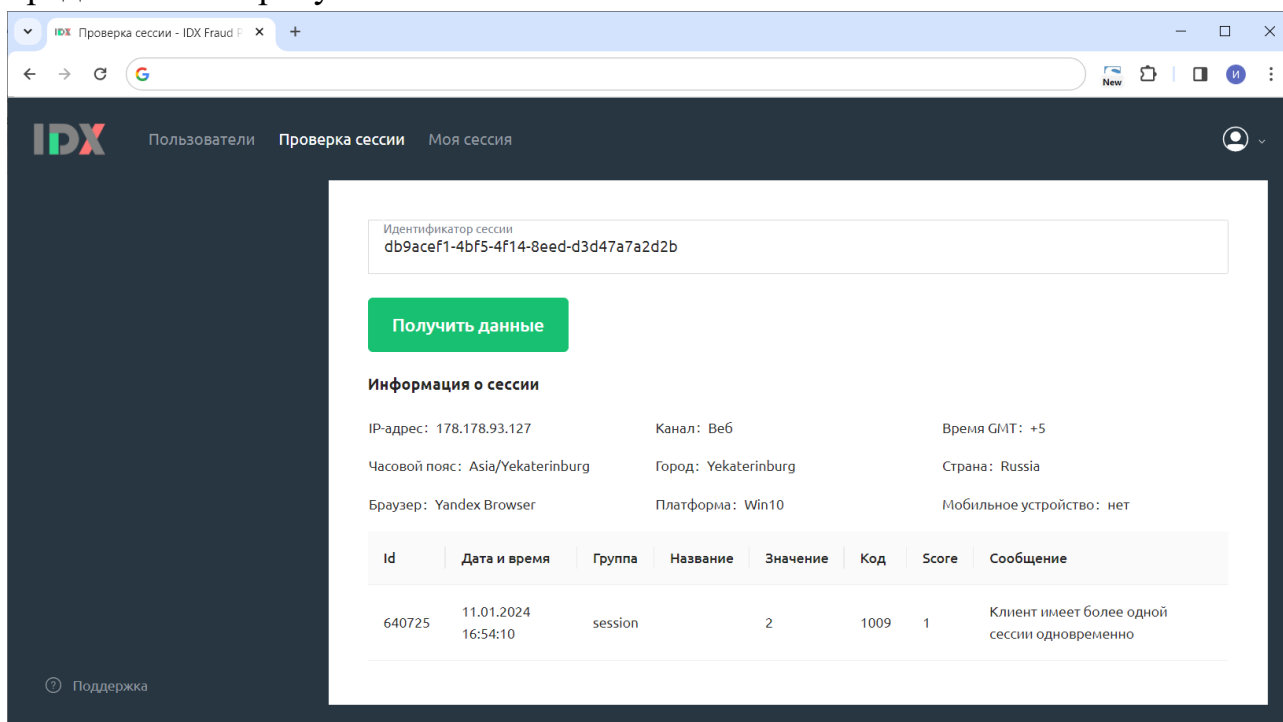


Рисунок 4.5 – Фрагмент веб-приложения с результатом проверки сессии по сценарию «Клиент имеет более одной сессии одновременно»

#### 4.4. Проверка сценария «Устройство было использовано более, чем одним клиентом»

Для проверки сценария необходимо выполнить вход в учетную запись [user1@iidx.ru](mailto:user1@iidx.ru), далее выйти из системы и на том же устройстве и в том же браузере выполнить вход в учетную запись [user2@iidx.ru](mailto:user2@iidx.ru). Для проверки сценария в интерфейсе роли «Администратор» нужно использовать идентификатор сессии пользователя [user2@iidx.ru](mailto:user2@iidx.ru). Ожидаемый результат проверки сессии для данного сценария представлен на рисунке 4.6.

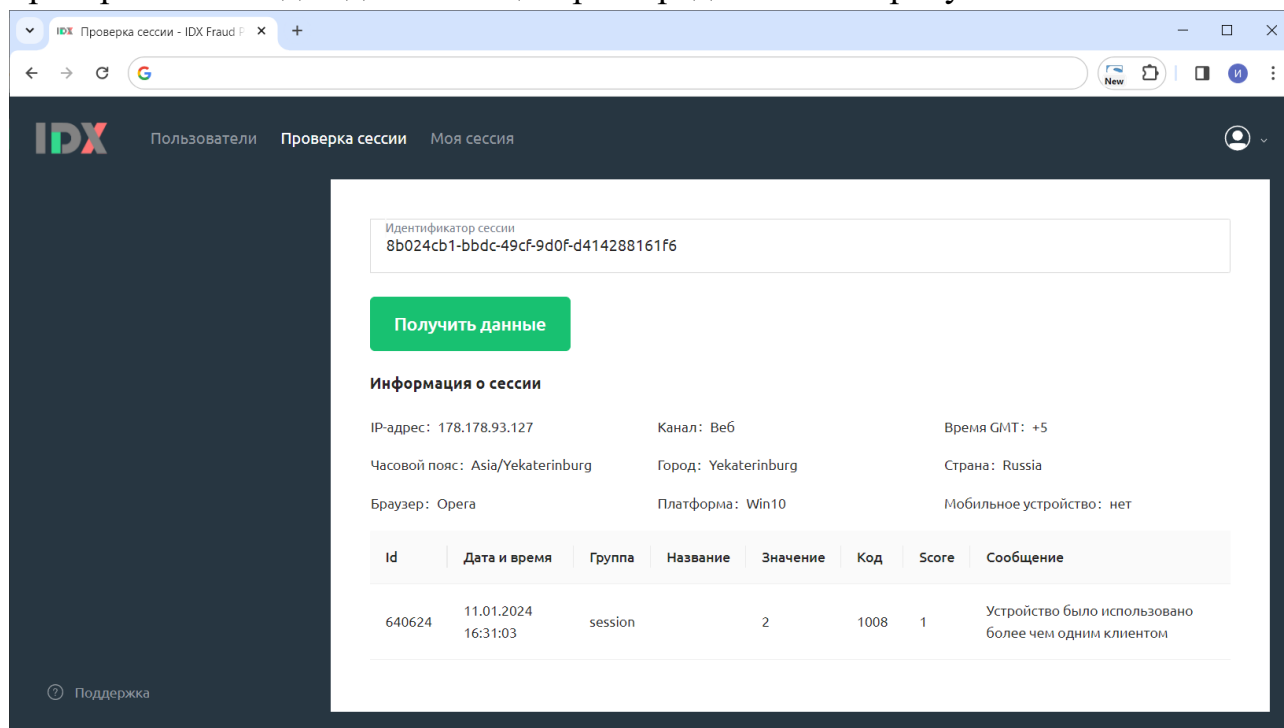


Рисунок 4.6 – Фрагмент веб-приложения с результатом проверки сессии по сценарию «Устройство было использовано более, чем одним клиентом»

#### 4.5. Проверка сценария «Клиент использует устройство с плохой репутацией»

Для проверки сценария необходимо выполнить вход в учетную запись [user1@iidx.ru](mailto:user1@iidx.ru).

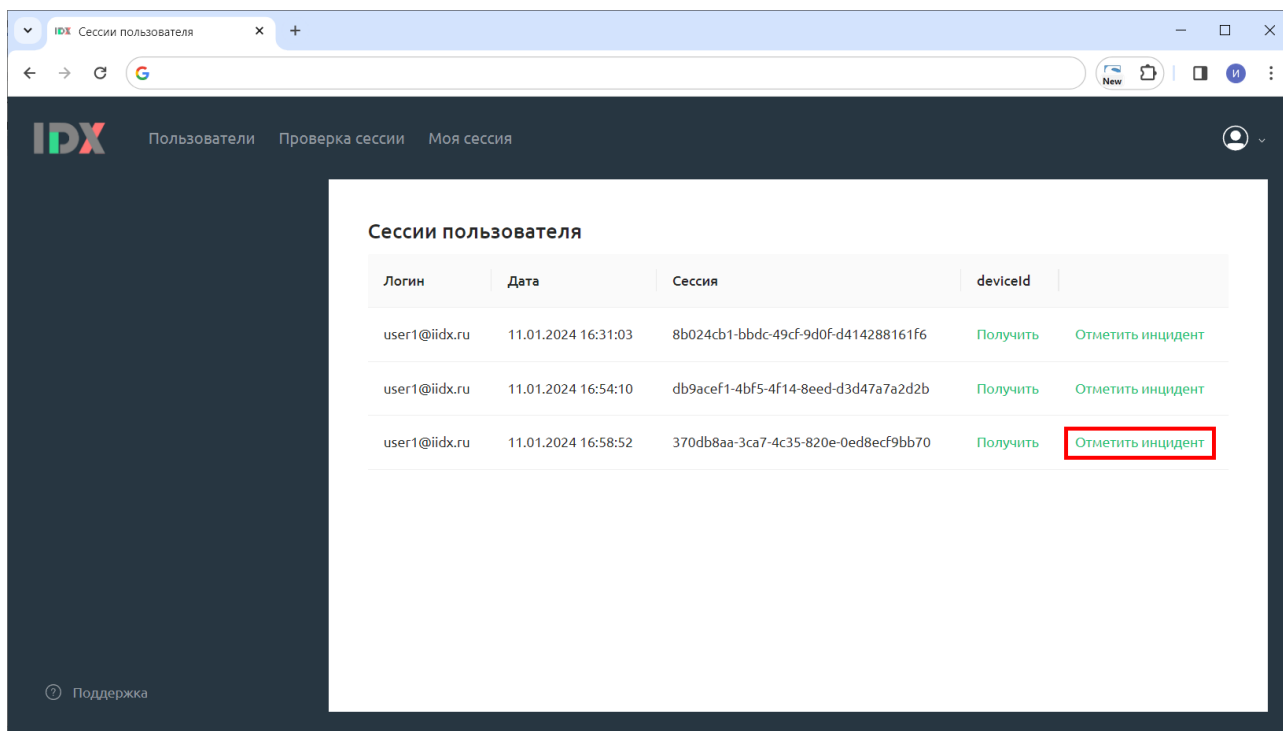


Рисунок 4.7 – Фрагмент веб-приложения со списком сессий пользователя

Затем на странице роли «Администратор» со списком сессий необходимо нажать ссылку «Отметить инцидент» для последней сессии клиента (рисунок 4.7); в результате этого будет вызвана функция API ядра ИППМ для регистрации обратной связи по репутации сессии, после чего её состояние изменится на «Инцидент отмечен».

Далее необходимо выйти из системы и выполнить вход в систему с того же устройства в том же браузере. Ожидаемый результат проверки сессии для данного сценария представлен на рисунке 4.8.

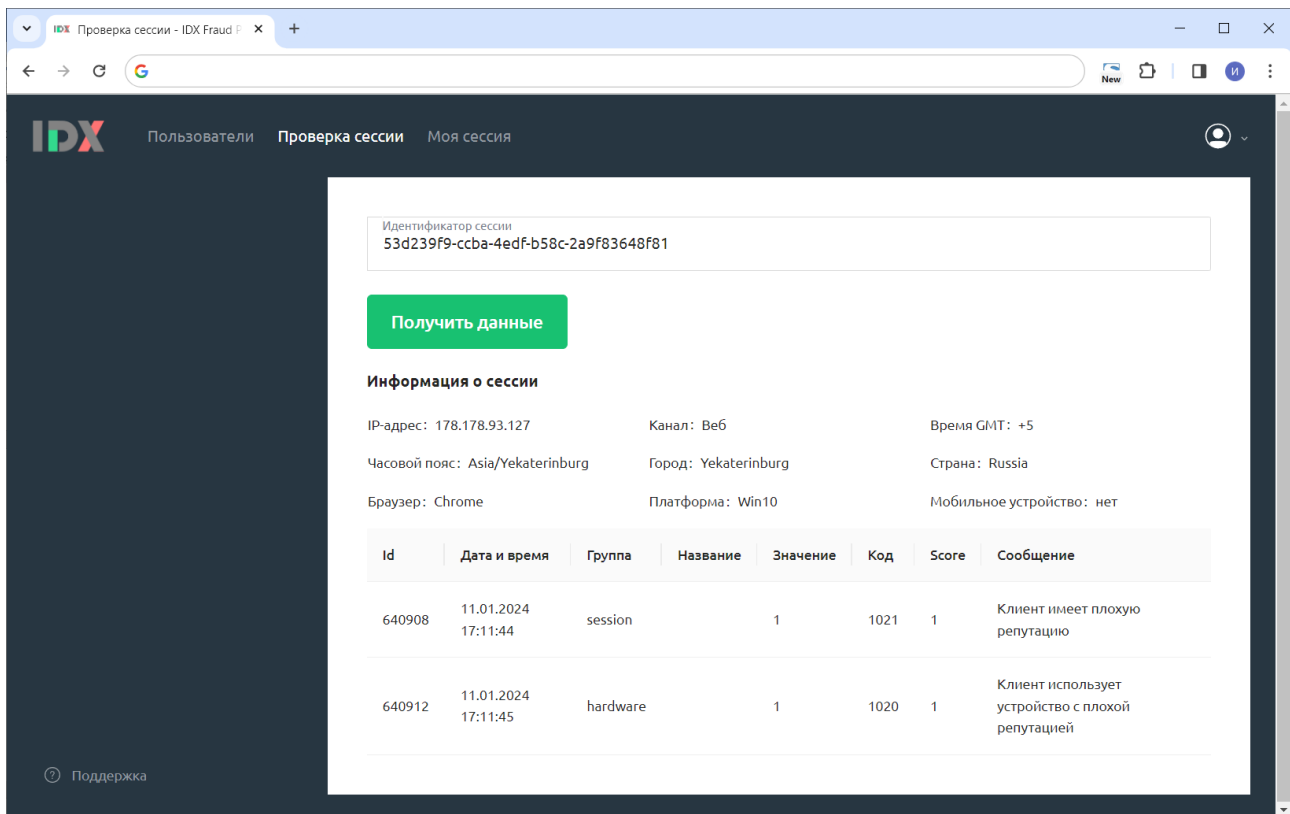


Рисунок 4.8 – Фрагмент веб-приложения с результатом проверки сессии по сценарию «Клиент использует устройство с плохой репутацией»