# Руководство пользователя для ПО “SMARTDNS”

# Оглавление

[**Оглавление 1**](#_9ai9hu7tst8a)

[**Введение 2**](#_8igme75xxytn)

[**Глоссарий терминов 4**](#_smqcwb5qkkrh)

[**Landing page – страница угрозы 6**](#_65wu2vtcm8q6)

[**Авторизация 7**](#_2qxl3yjm211t)

[**Просмотр устройств 9**](#_vqf5h8elpm2n)

[Внешний вид страницы 9](#_wfnazmlncpfy)

[Содержимое страницы 10](#_x42z3r1r1vcj)

[**Добавление устройств 11**](#_hjghbdvb6xgh)

[**Просмотр информации о устройстве 13**](#_omv8rcm516xq)

[**Просмотр статистики 14**](#_gs8c5nuph76k)

[Где найти статистику 14](#_lhabspwi2ofj)

[Описание элементов 14](#_mp5at3qb6ux0)

[1. За какой период выводится статистика 15](#_409flgil081d)

[2. Переключение между видами статистики 15](#_6ymo57kd939z)

[3. Переключение между таблицами и графиками 16](#_hhk0vixtwdvu)

[4. Угрозы 16](#_1rxeucm89wva)

[5. Количество данных 17](#_b2pckltcg0qh)

[6. Период 17](#_hq5k2tai7z35)

[7. Данные 17](#_dtaw5thfkteb)

[Всего запросов проверено 17](#_a3arf4aldq0v)

[История предотвращенных угроз 18](#_xbyxdbutfcjo)

[Данные отсутствуют 19](#_6jw6edycduhw)

[**Интерфейс просмотра и изменения зон 20**](#_nqszrvq1fc95)

[**Редактирование устройств 22**](#_6w09ika8j5fw)

[**Удаление 24**](#_h56tt22txflm)

# 

# Введение

Настоящее руководство пользователя предназначено для знакомства с системой защиты от посещения вредоносных сайтов. Данная система разработана с целью обеспечения безопасности пользователей путем автоматического перенаправления их на безопасную лендинг страницу в случае попытки доступа к нежелательным или запрещенным веб-ресурсам(см. Глоссарий терминов). Это решение не только минимизирует риски, связанные с посещением опасных сайтов, но и предоставляет пользователям удобные инструменты для управления и мониторинга своей интернет-безопасности.

В рамках данного руководства пользователи получат детальное описание функциональных возможностей системы, включая:

1. Ограничение доступа к вредоносным сайтам. При попадании на вредоносный сайт происходит перенаправление пользователя на сайт с предупреждением и описанием угрозы.
2. Включение и выключение зон(см. Глоссарий терминов). Возможность самостоятельного управления уровнями защиты путем активации или деактивации определенных зон безопасности.
3. Просмотр зон. Доступ к интерфейсу, позволяющему ознакомиться с различными категориями сайтов и соответствующими им зонами защиты.
4. Просмотр количества предотвращенных угроз. Предоставление информации о количестве потенциальных угроз, заблокированных системой, что позволяет оценить эффективность применяемых мер защиты.
5. Просмотр количества проверенных сайтов. Данные о количестве сайтов, подвергшихся проверке системой, что способствует информированности пользователя о своей интернет-активности.  
   Следование инструкциям, изложенным в данном руководстве, позволит пользователям эффективно эксплуатировать систему, обеспечивая высокий уровень безопасности и комфорта при использовании интернет-ресурсов.

# Глоссарий терминов

**Глосса́рий** (лат. glossarium «собрание глосс») — словарь узкоспециализированных терминов в какой-либо отрасли знаний с толкованием, иногда переводом на другой язык, комментариями и примерами.

**Глоссарий**

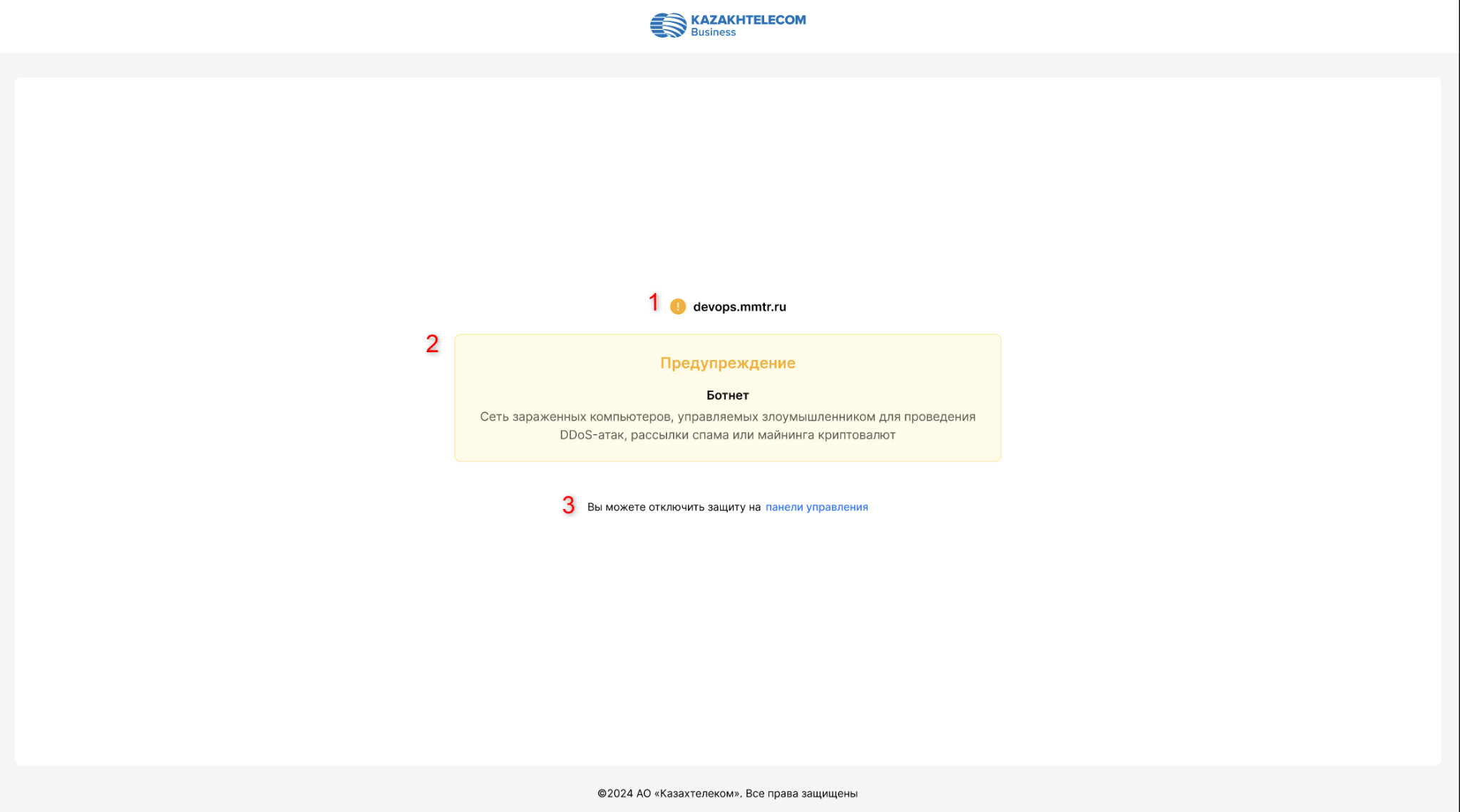
Таблица 1

| **Термин или сокращение** | **Значение** |
| --- | --- |
| Веб-ресурсы | Это информационные материалы, доступные в сети интернет. К ним относятся веб-сайты, блоги, форумы, онлайн-магазины, социальные сети, онлайн-платформы для образования, развлечений и других целей. |
| Доменное имя | Это уникальное название сайта или другого ресурса в Сети. Именно доменное имя люди печатают в адресной строке браузера, чтобы открыть конкретный интернет-портал или страницу. |
| Зона | Это совокупность доменных имен (сайтов) принадлежащих одной угрозе |
| Киберугроза | Незаконное проникновение или угроза вредоносного проникновения на компьютер |
| Подвал сайта | Это нижняя область веб-страницы, которая обычно повторяется на всех страницах сайта. Он размещается в самом низу страницы и служит для предоставления дополнительной информации и навигационных элементов пользователям |
| Landing Page | Это интернет-страница, которая оповещает пользователя о угрозе |

# Landing page – страница угрозы

Если пользователь попадает на вредоносный сайт, он увидит специальную страницу — Landing page (см. Глоссарий терминов; см. Рис.1). Эта страница предупреждает о потенциальной опасности и помогает пользователю избежать взаимодействия с опасным ресурсом.

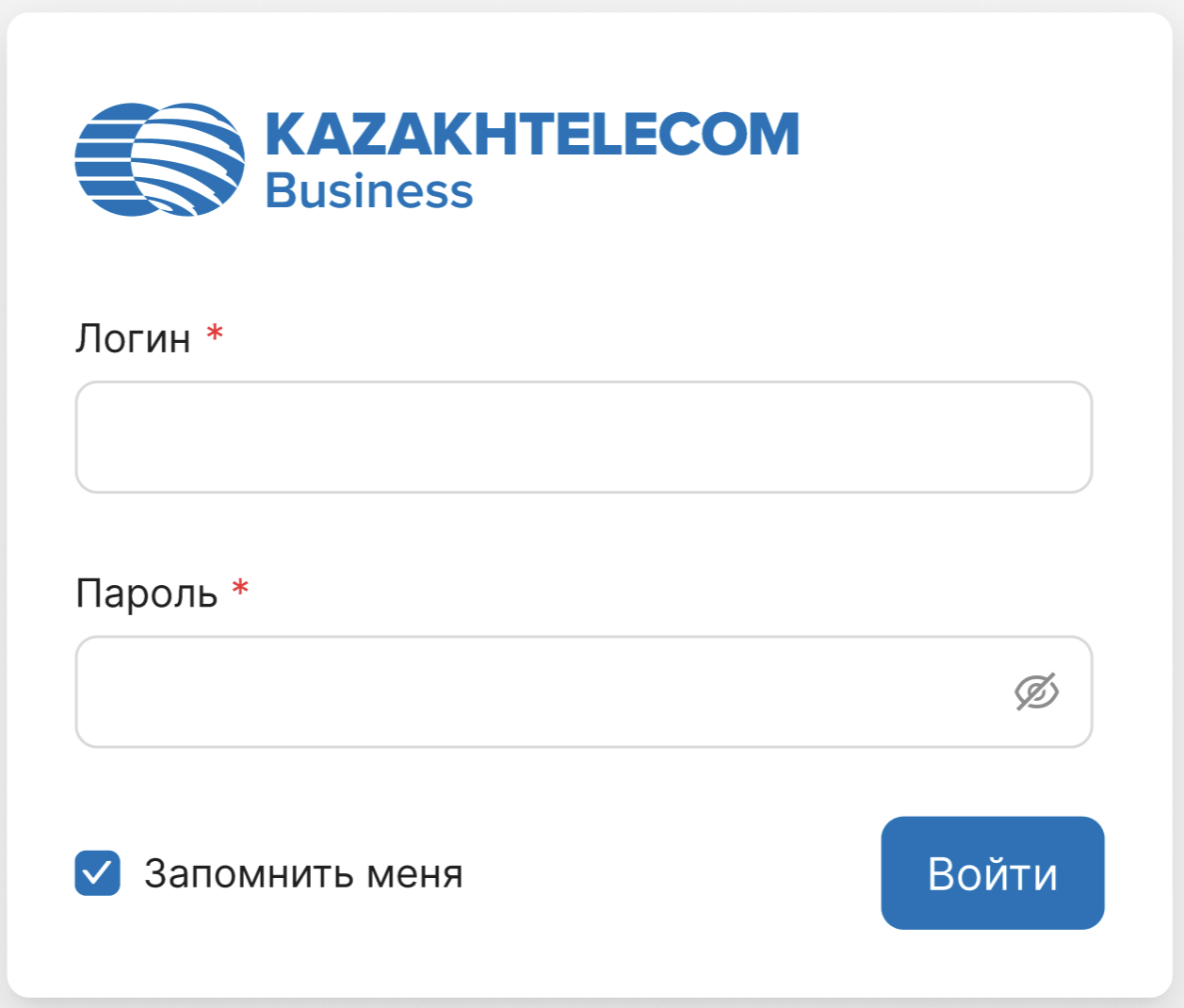
Разберем на данном примере за что отвечают отдельные блоки на этой странице.

  
Рис. 1. Пример Landing page.

1. Вредоносный адрес сайта, на который пытался попасть пользователь.
2. Информационное поле с оповещением о попытке зайти на вредоносный сайт и указанием типа угрозы. Ссылка на страницу личного кабинета, где "панели управления" является ссылкой на личный кабинет абонента.

# Авторизация

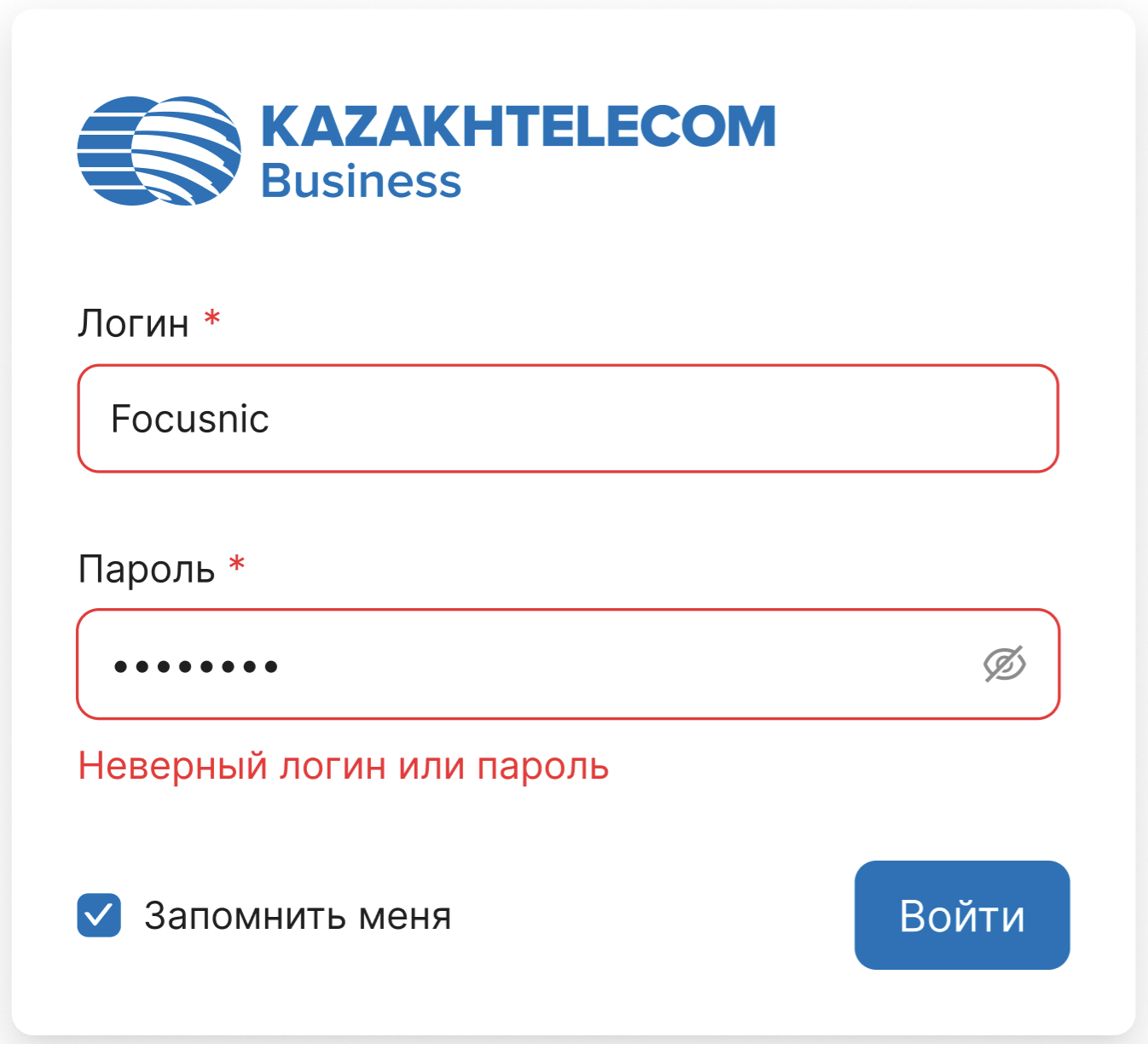
Чтобы получить доступ к личному кабинету, необходимо пройти авторизацию (см. Рис.2). Если авторизация ещё не пройдена, на экране появится окно, в котором потребуется ввести данные вашей учётной записи, а именно логин и пароль. Если авторизация уже пройдена, вы сразу окажетесь в личном кабинете.

  
Рис. 2. Пример окна авторизации.

Логин и пароль предоставляются провайдером. Пользователь может проверить введенный пароль, нажав на значок в поле ввода пароля.

Если вы нажмете на флажок «Запомнить меня», при повторном входе в систему вам не придется вводить данные повторно.

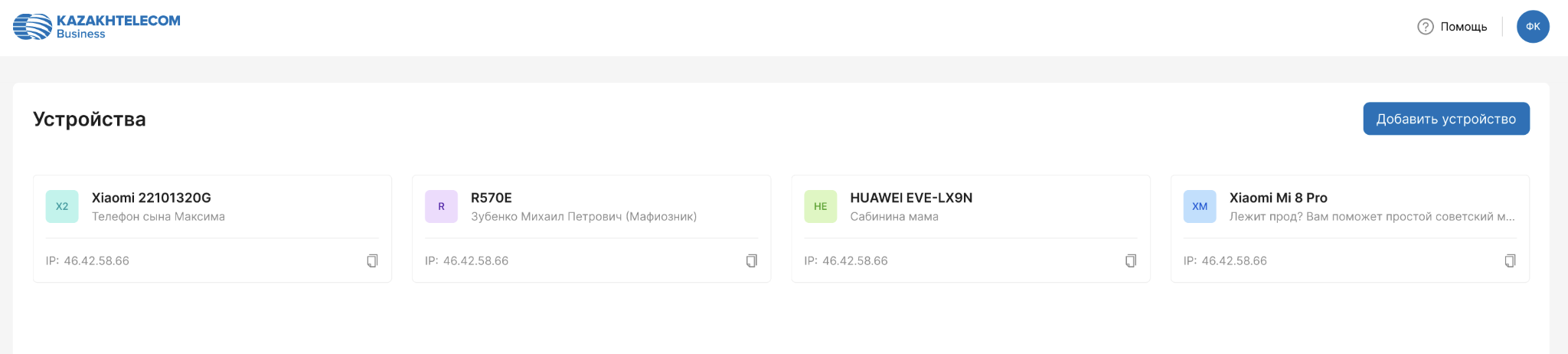
В случае возникновения ошибки при авторизации поля, оставшиеся незаполненными или заполненные некорректно, будут выделены красным цветом, а также будет выведен текст, описывающий характер ошибки (см. Рис.3).

  
Рис. 3. Пример ошибки заполнения окна авторизации.

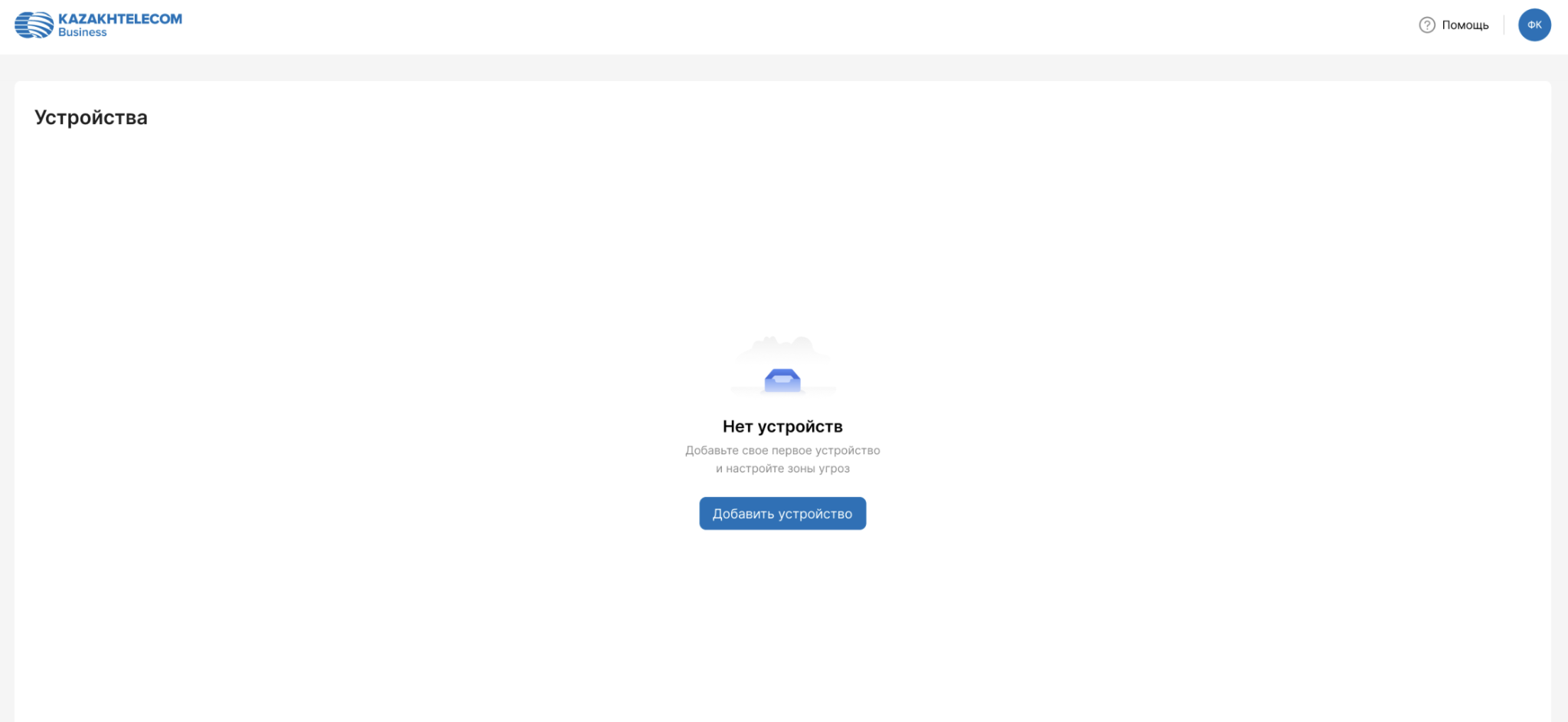
# Просмотр устройств

## **Внешний вид страницы**

При входе в личный кабинет пользователь попадает на страницу с выбором устройств (см. Рис.4), для которых он имеет возможность настроить статистику.

  
Рис. 4. Пример списка устройств.

В случае если нет устройств привязанных к аккаунту, то пользователь видит следующую страницу (см. Рис.5).

  
Рис. 5. Пример отсутствия устройств.

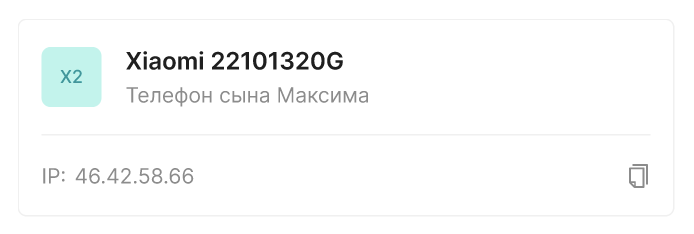
В центральной части окна находится информация о возможности создания новых устройств и кнопка “Добавить устройства”, которая была описана выше.

## 

## **Содержимое страницы**

1. Для каждого существующего устройства выводится следующая информация (см. Рис.6):

* Имя устройства, заданное пользователем.
* Краткое описание.
* IP-адрес.

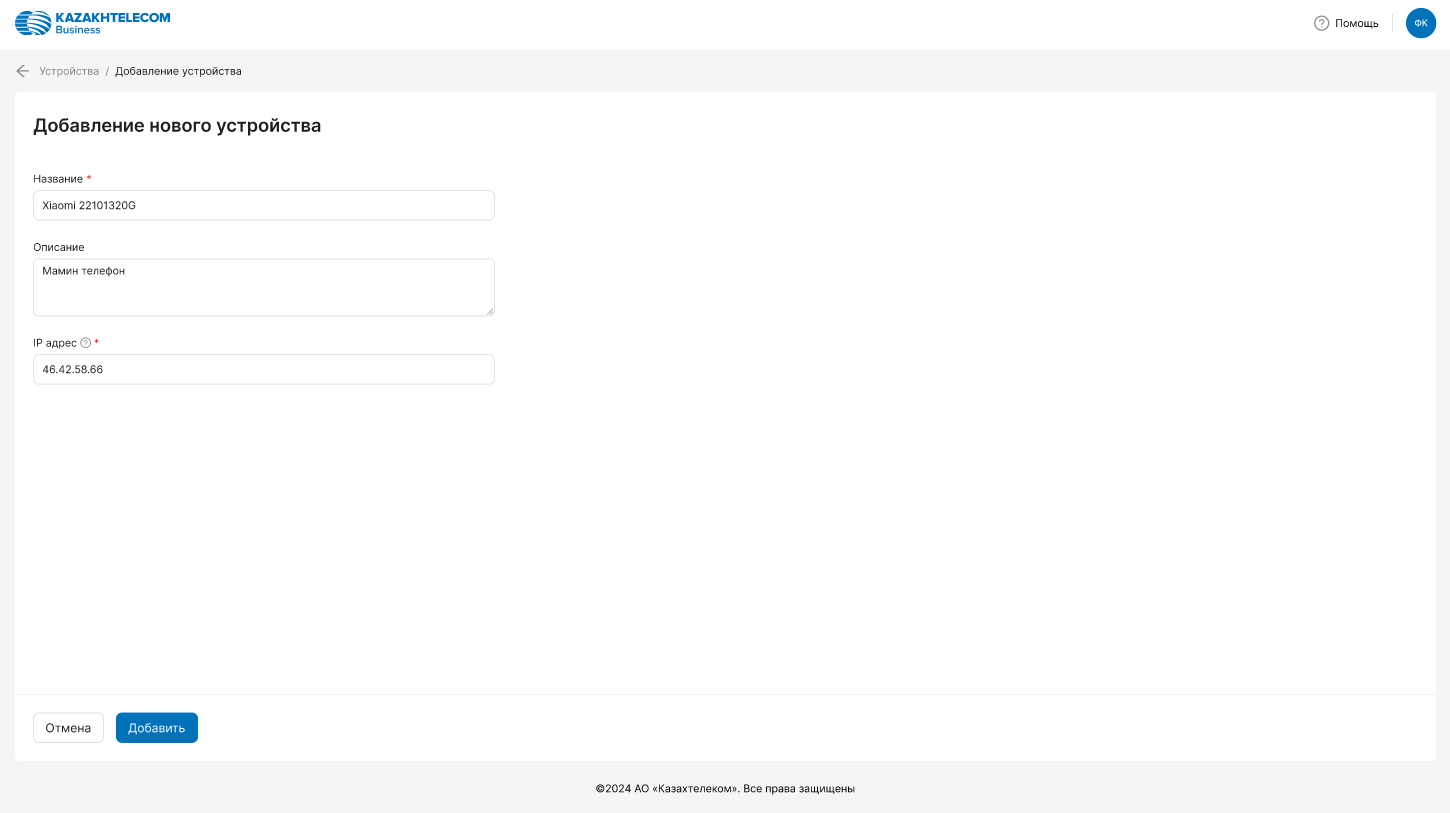
  
Рис. 6. Пример карточки устройства.

Рядом с IP-адресом находится кнопка для его копирования. При нажатии на нее IP-адрес будет сохранен в буфере обмена.

1. При нажатии на кнопку “добавить устройство” будет осуществляться переход на страницу добавления устройства.

# Добавление устройств

При нажатии на кнопку «Добавить устройство» вы перейдете на страницу «Добавление нового устройства» (см. Рис.7).

  
Рис. 7. Пример страницы добавления устройства.

Для добавления нового устройства необходимо заполнить следующую информацию:

* Имя устройства - Человекочитаемое название устройства.
* Описание - Короткое описание устройства до 255 символов.
* IP-адрес — IP-адрес устройства, которое нужно добавить. Формат IP-адреса выглядит следующим образом:
  + Четыре числовых блока, каждый из которых может принимать значения от 0 до 255.
  + Записывается в формате десятичной системы счисления.
  + Используются цифры от 0 до 9.

Примеры IP-адреса: 192.168.1.34; 8.8.8.8; 34.67.212.23

Рядом с IP-адресом находится указание, которое описывает его внешний вид и указывает, где его можно найти.

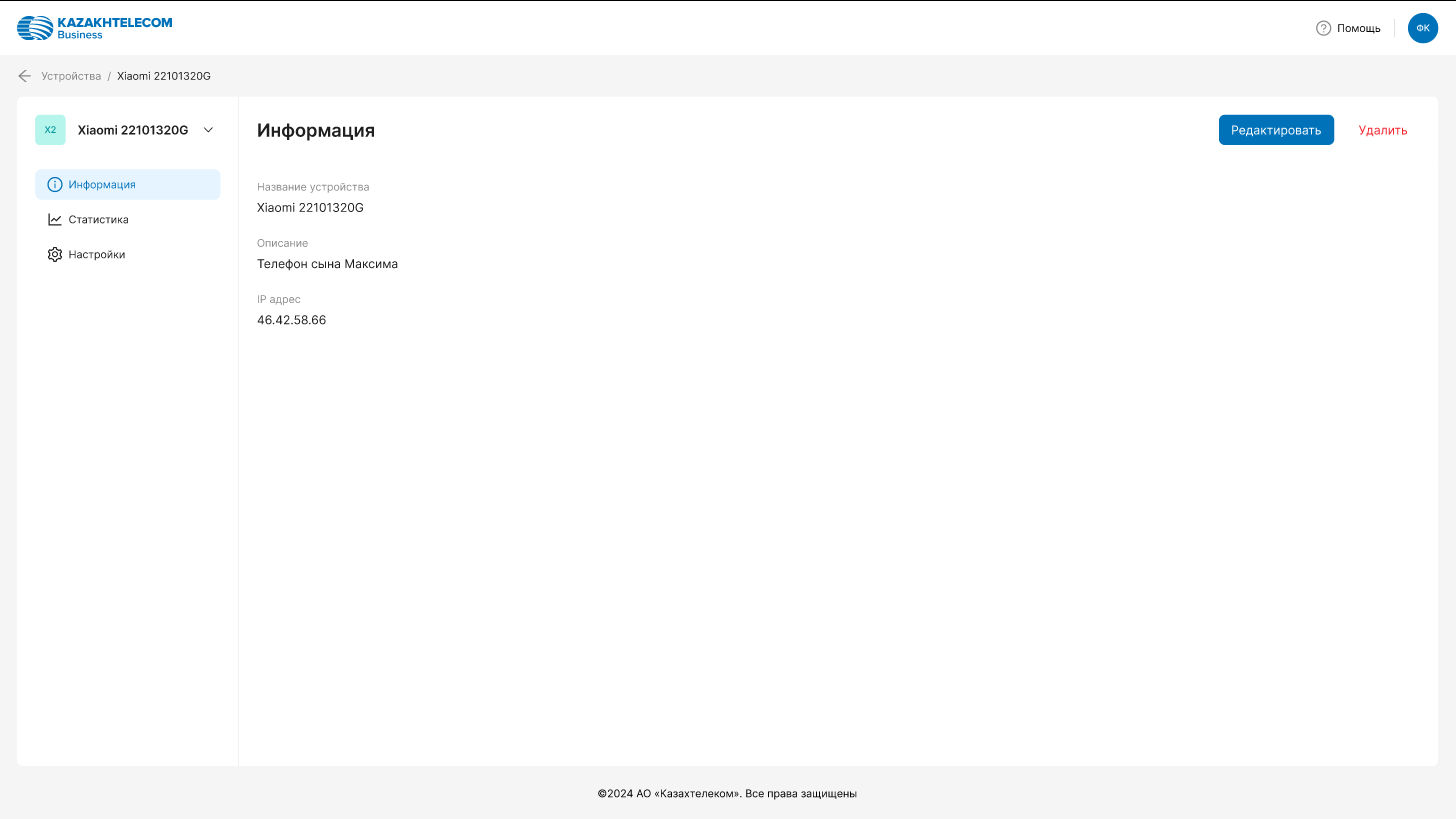
После заполнения данных необходимо сохранить изменения. Если все заполнено правильно и ошибок нет, то в правом верхнем углу появится уведомление об успешном добавлении устройства.

Если в процессе сохранения данных произошла ошибка (не удалось сохранить данные или IP-адрес уже существует), то в правом верхнем углу появляется уведомление об ошибке при добавлении устройства.

# Просмотр информации о устройстве

При выборе пользователем устройства осуществляется переход на его карточку (см. Рис.8). На главной странице находится следующая информация об устройстве:

* Название устройства.
* Описание.
* IP адрес устройства.

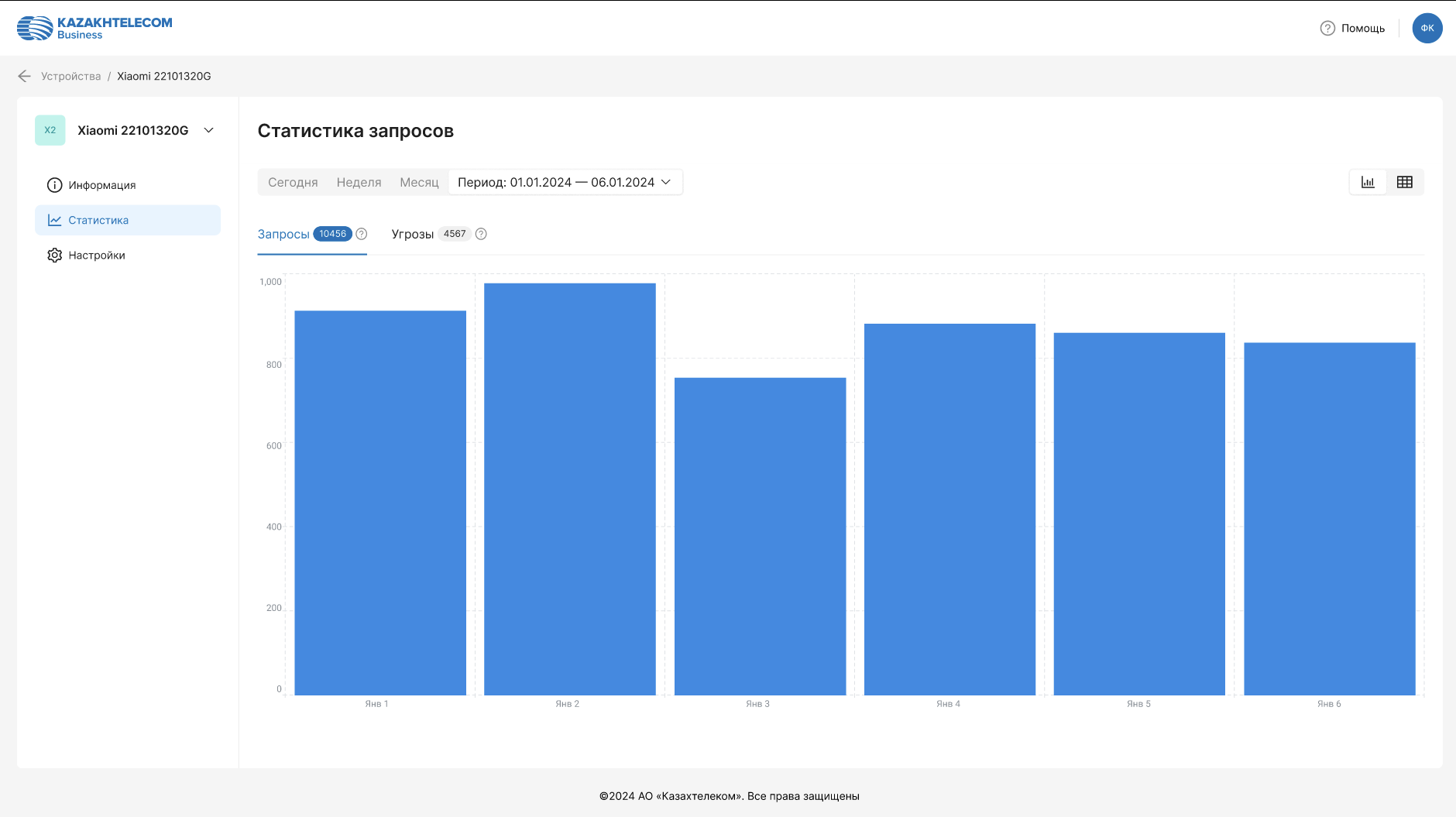
  
Рис. 8. Пример страницы с информацией о устройстве.

# Просмотр статистики

Система предоставляет пользователю инструменты для анализа статистики за выбранный период времени. В рамках анализа рассматриваются два ключевых параметра: количество предотвращенных угроз и количество проверенных веб-ресурсов.

## **Где найти статистику**

Чтобы просмотреть статистику, перейдите на вкладку «Статистика запросов» (см. Рис.9). На ней пользователю будут представлены два графика: «Всего запросов проверено» и «Предотвращено угроз».

  
Рис. 9. Пример статистики количества запросов.

## 

## **Описание элементов**

Диаграммы статистики (см. Рис.10) представляют собой совокупность следующих элементов:

****Рис. 10. Описание элементов страницы.

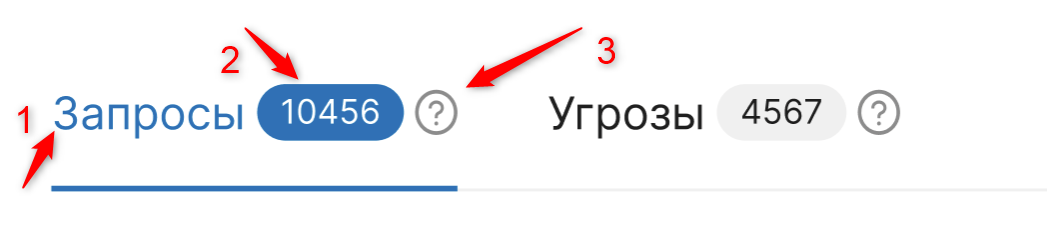
### 1. За какой период выводится статистика

Статистика может выводится за определенный промежуток времени:

* Сегодня (с 00:00 до 23:59)
* Неделя (с 00:00 понедельника до 23:59 воскресенья)
* Месяц (с первого по последнее число)
* День/Период(Задается интервал времени, минимальная)

### 2. Переключение между видами статистики

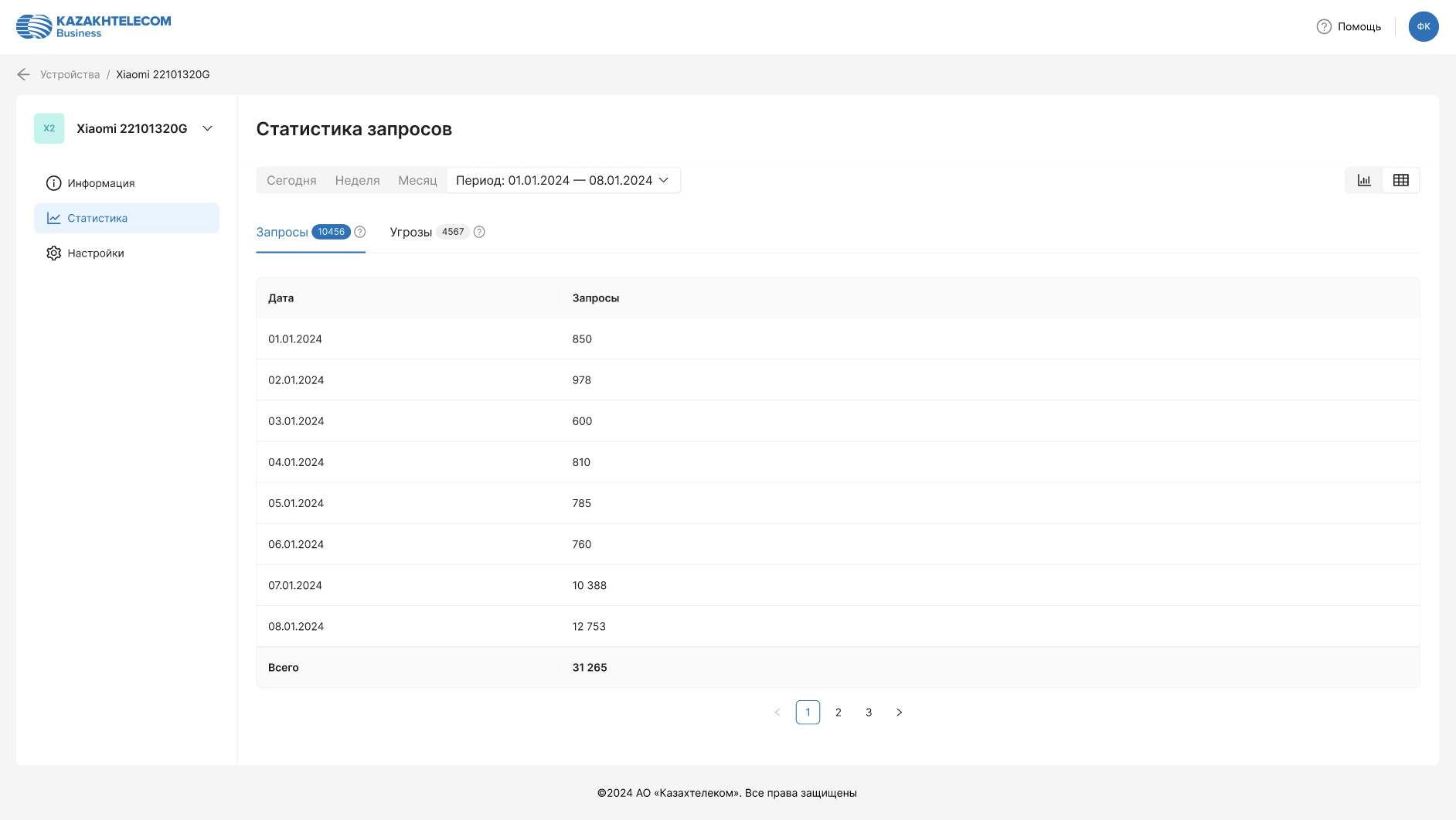
Данный блок содержит следующие элементы (см. Рис.11):

****Рис. 11. Переключение между видами статистики.

1. Тип графика. То, какую информацию отображает график. Количество проверенных запросов — «Запросы», количество предотвращенных угроз — «Угрозы»
2. Количество запросов. Количество запросов, проверенных или предотвращенных, в зависимости от выбранного графика.
3. Подсказка. Подсказка содержит в себе информацию о вкладке

### 3. Переключение между таблицами и графиками

В этой системе информация может быть представлена в двух форматах: в виде графика или в виде таблицы. Если вы выберете значок с изображением таблицы, данные будут представлены в виде таблицы (см. Рис.12). Если вы выберете значок с изображением графика, данные будут представлены в виде графика. Пример отображения данных в виде таблицы:

  
Рис. 12. Пример таблицы с данными по попыткам попадания на вредоносный сайт.

### 4. Угрозы

В этом разделе представлен перечень угроз, каждой из которых соответствует определённый цвет.

### 5. Количество данных

Шкала представляет собой количественную меру данных.

### 6. Период

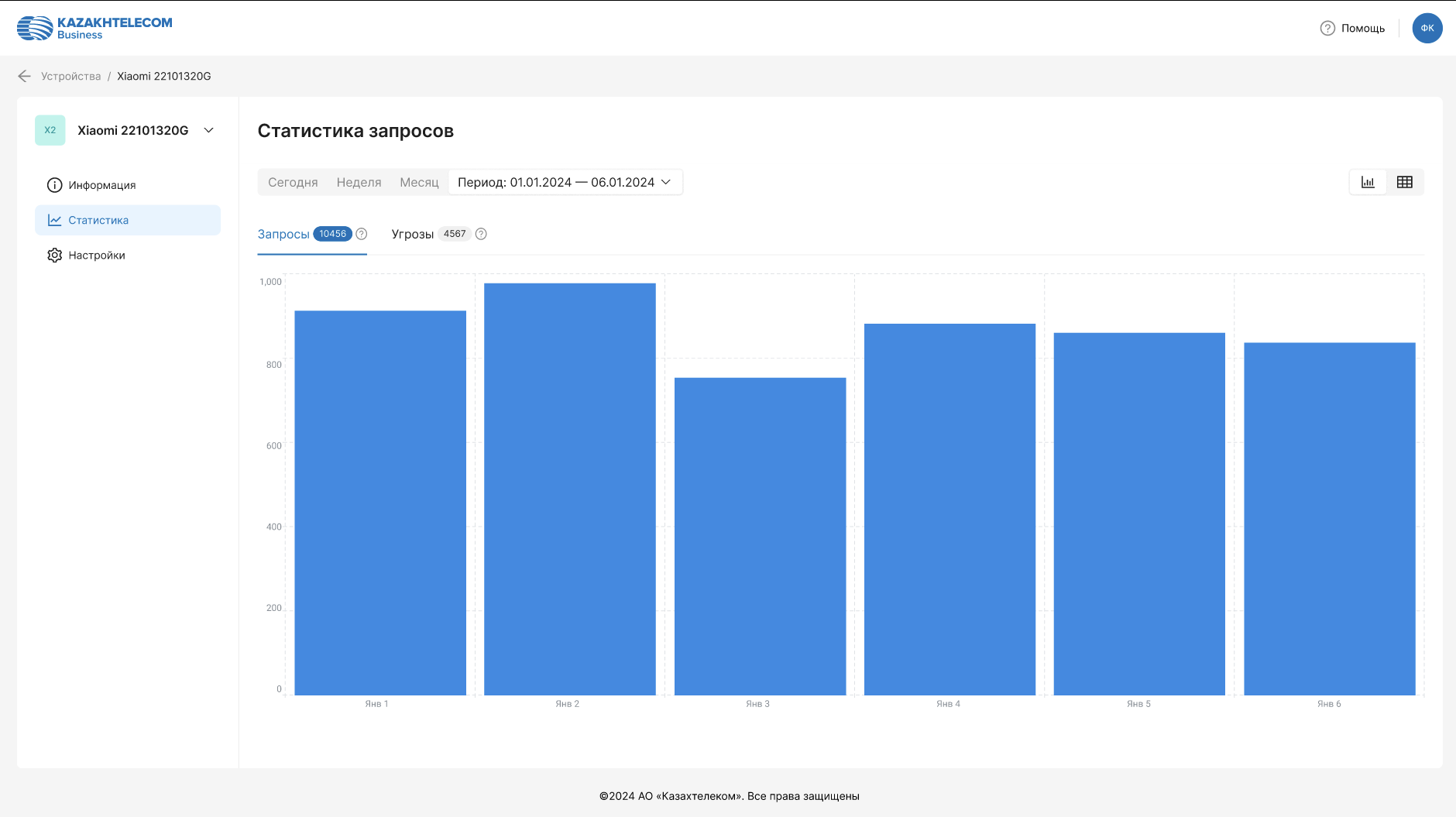
Шкала представляет собой временной отрезок, в течение которого осуществляется сбор данных.

### 7. Данные

Данные представлены в виде столбчатой диаграммы, где каждый цвет соответствует отдельной угрозе. Высота зоны с определённым цветом пропорциональна количеству данных по соответствующей угрозе. Если цвет на диаграмме не представлен, это означает, что за указанный период времени данная угроза не была обнаружена.

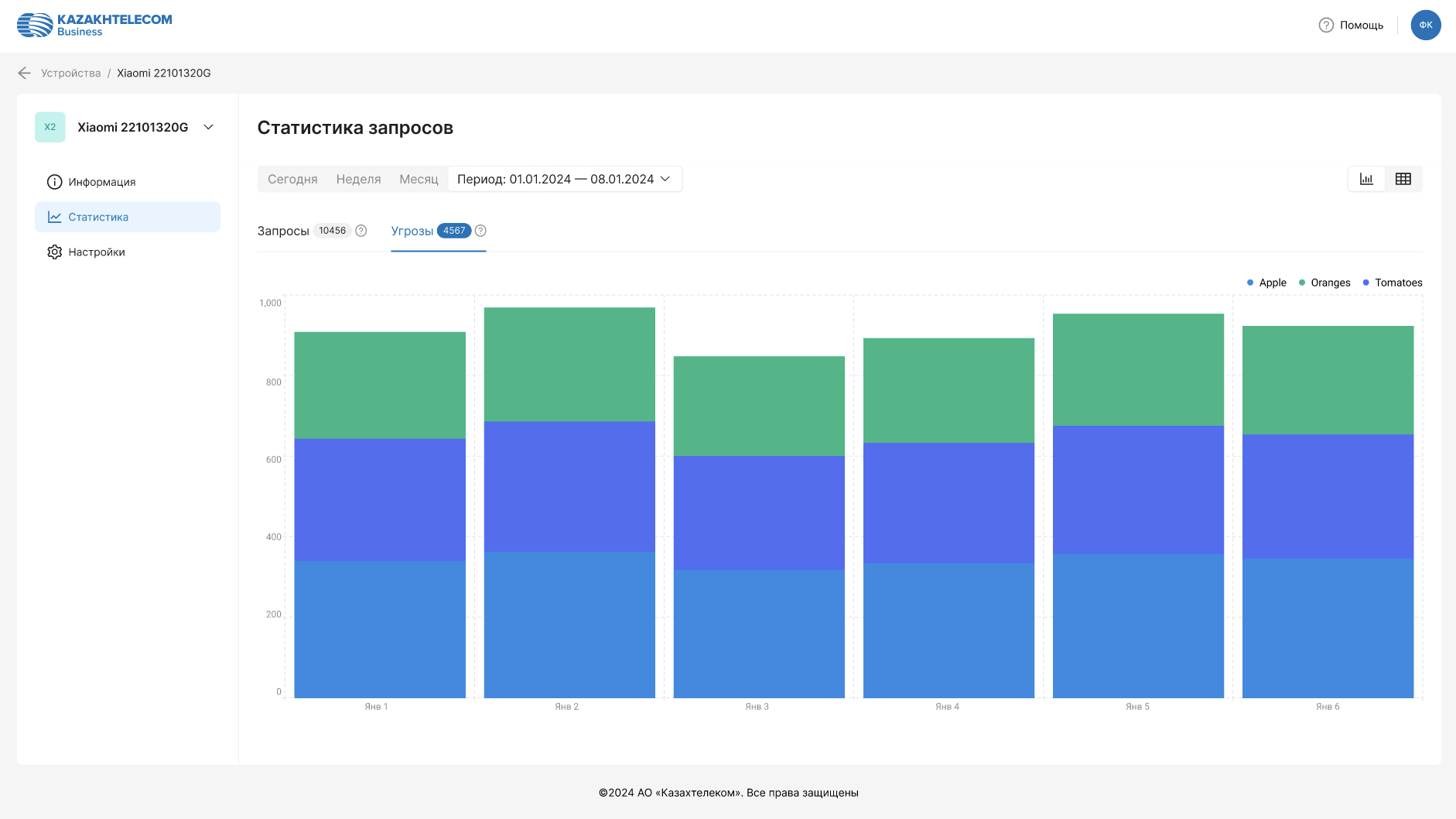
## **Всего запросов проверено**

На этой диаграмме представлена информация о количестве проверенных сайтов, то есть о числе веб-ресурсов, которые подверглись анализу (см. Рис.13). Подсказка к заголовку «Статистика по количеству предотвращенных угроз» — «Количество запросов, отправленных в DNS».

  
Рис. 13. Переключение между видами статистики.

## **История предотвращенных угроз**

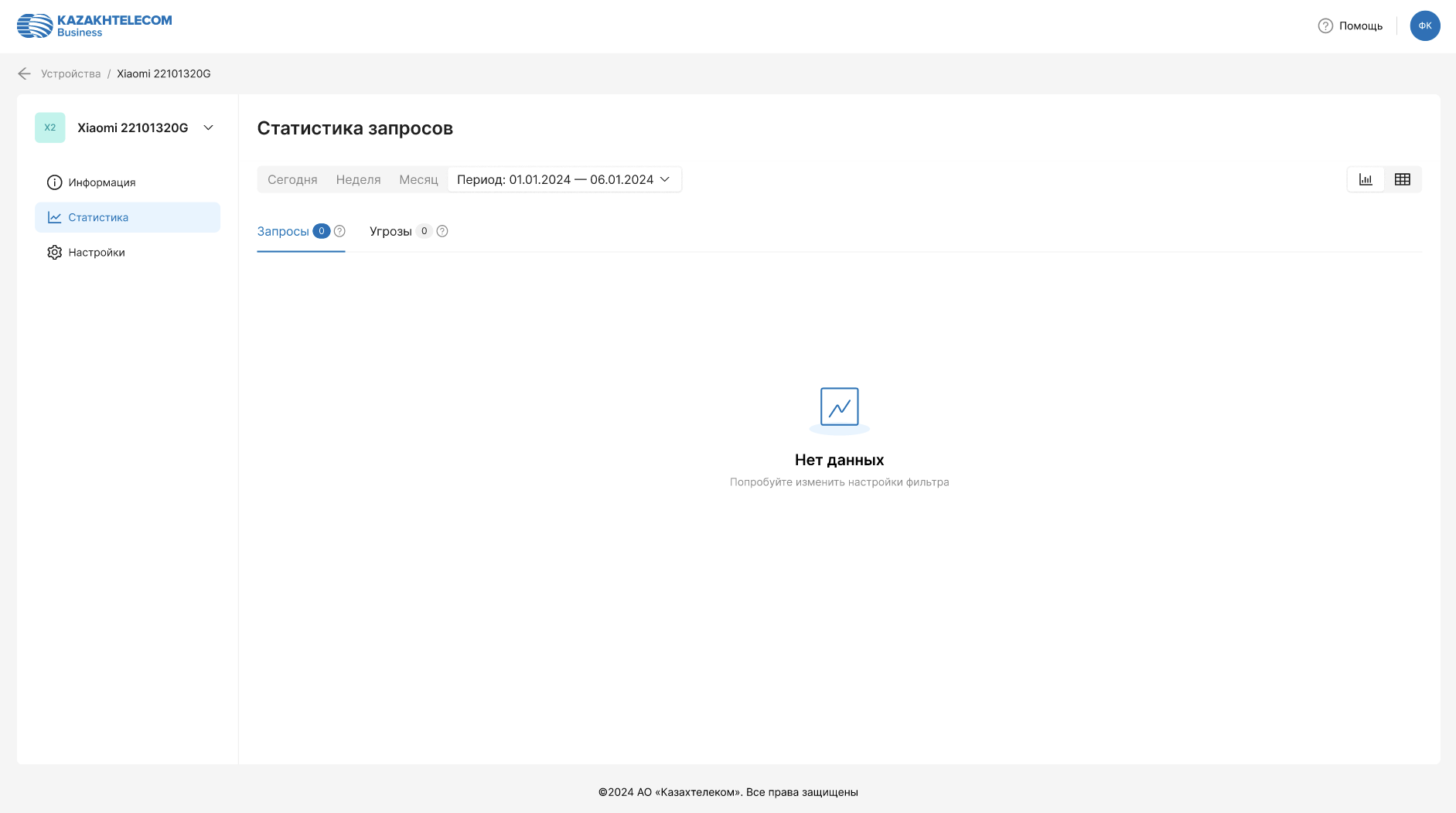
На этой диаграмме представлена информация о количестве предотвращения угроз (см. Рис.14), то есть о количестве веб-ресурсов, которые были определены как вредоносные и доступ к которым был запрещён.

  
Рис. 14. Пример статистики предотвращенных угроз.

Эта диаграмма иллюстрирует статистику предотвращения угроз. Она не только показывает общее количество выявленных угроз, но и предоставляет подробную информацию по каждой из них в отдельности.

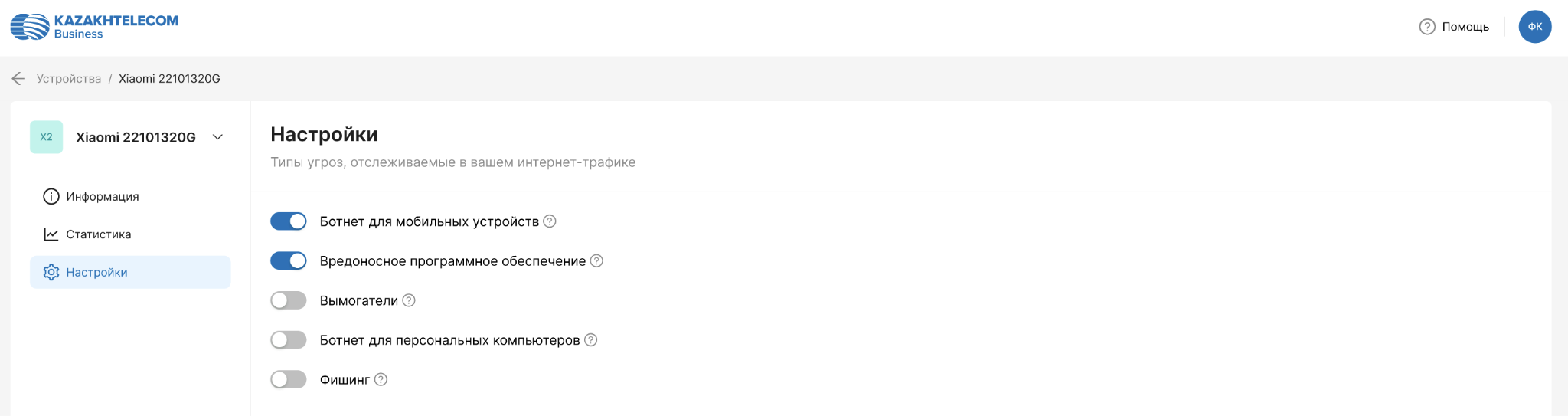
## **Данные отсутствуют**

Если сведения за указанный период ещё не были собраны, на экране пользователя отобразится следующая страница (см. Рис.15).

  
Рис. 15. Данные по статистике отсутствуют

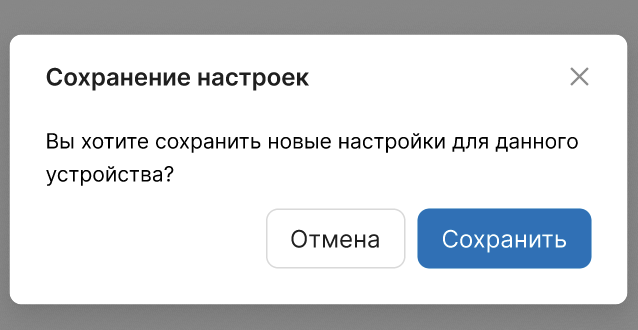
# Интерфейс просмотра и изменения зон

При выборе вкладки «Настройки» (см. Рис.16) пользователь может выбирать между различными защитными функциями, так называемыми зонами (см. Глоссарий терминов), отдавая предпочтение тем, которые кажутся ему наиболее важными, и исключая те, которые не представляют для него интереса.

  
Рис. 16. Переключение между видами статистики.

Каждая зона имеет собственный переключатель, с помощью которого можно настроить ее состояние. Выключенная зона означает отсутствие защиты, а включенная — что защита для пользователя настроена. Рядом с названием зоны находится элемент управления зоной. Значок, который предназначен для просмотра ее назначения.

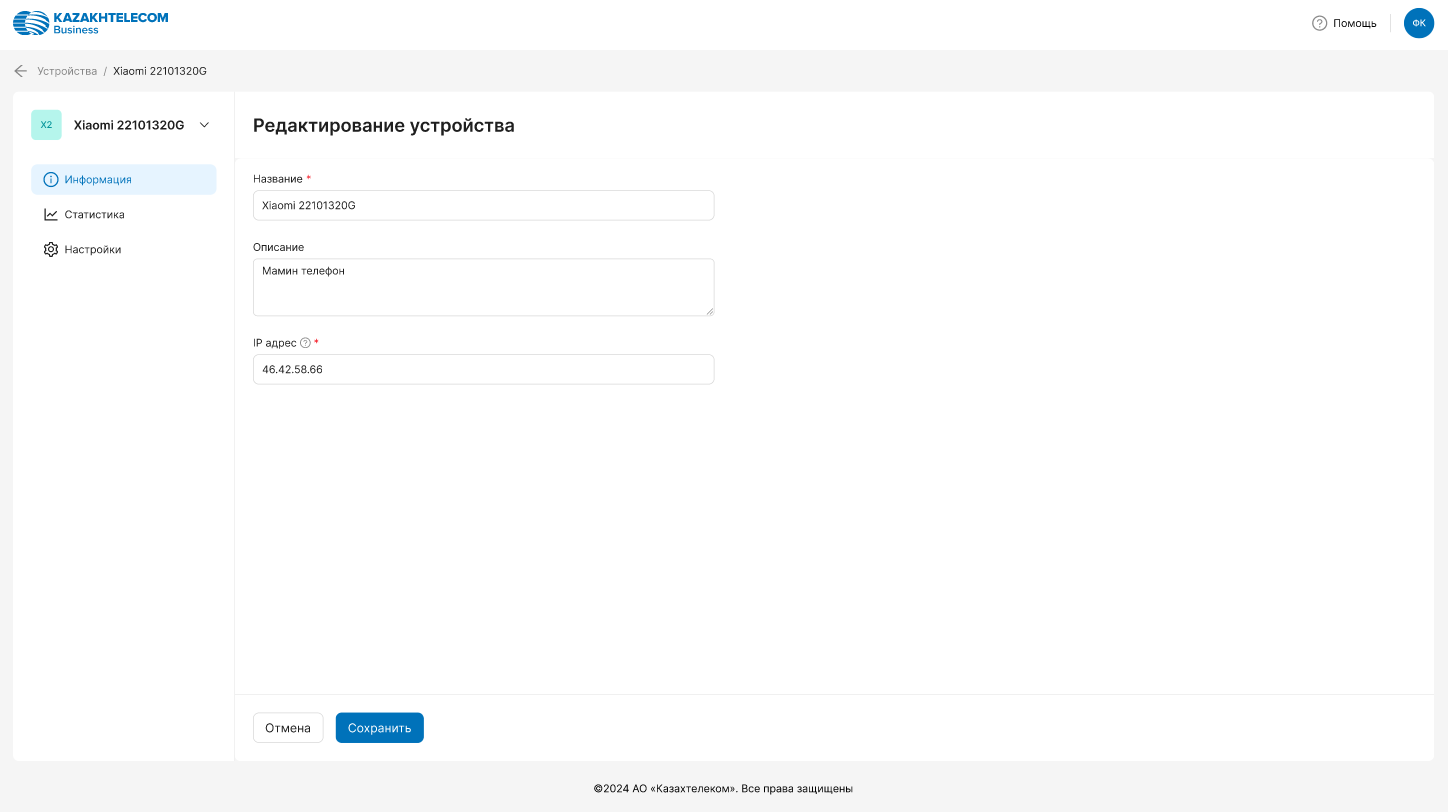
После завершения настройки параметров пользователю необходимо нажать кнопку «Сохранить», чтобы внесенные изменения вступили в силу. После этого на экране появится окно с подтверждением действий (см. Рис.7), в котором необходимо подтвердить намерение создать новую зону или отменить его.

  
Рис. 17. Модальное окно с подтверждением сохранения настроек.

# Редактирование устройств

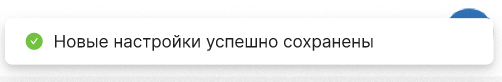
Вкладка «Редактирование» (см. Рис.18) предназначена для изменения данных об устройстве. Вы можете изменить такие данные, как:

* IP-адрес.
* Имя устройства.
* Описание устройства.

  
Рис. 18. Переключение между видами статистики.

Когда все необходимые изменения будут внесены, нажмите кнопку «Сохранить» в нижней части страницы. Если вы хотите отменить изменения, нажмите кнопку «Отмена».

Если редактирование устройства прошло успешно (см. Рис.19), то пользователь увидит следующее уведомление:

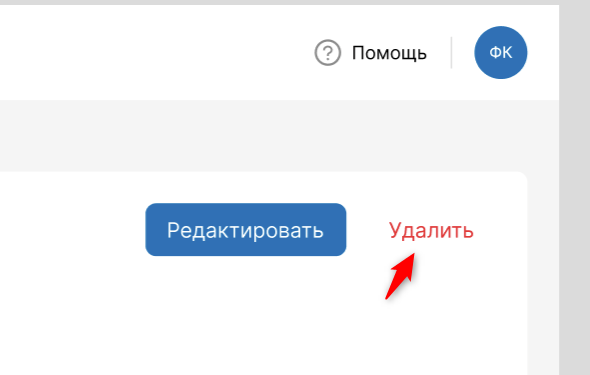
  
Рис. 19. Сообщение об успешно выполненном действии.

Если при редактировании устройства прошла ошибка (см. Рис.20), то пользователь увидит следующее уведомление

  
Рис. 20. Сообщение о не выполненном действии.

# Удаление

Чтобы удалить существующее устройство, необходимо на странице «Информация» нажать «Удалить» (см. Рис.21) в правом верхнем углу

  
Рис. 21. Кнопка удаления устройства.

После этого появится модальное окно с запросом на подтверждение удаления устройства.