**Настройка web-интерфейса 3G/4G USB модема Huawei E3372h**
**в роутерах Kroks**

**СОДЕРЖАНИЕ**

В роутерах Kroks установлен высокоскоростной модем Huawei E3372h, позволяющий принимать данные на скорости до 100 Мбит/с при работе в сетях LTE. Модем является мультистандартным устройством – при отсутствии покрытия 4G модем автоматически перейдет на работу в сети 3G (HSPA+) или 2G (EDGE, GPRS).

Модем Huawei E3372h имеет веб-интерфейс, а управление соединением с мобильной сетью ведется средствами операционной системы, встроенной в модем. Модем устанавливает соединение с сетью Интернет автоматически, а для управления настройками модема есть web-интерфейс.

**Внимание! Модем полностью настроен и готов к работе с использованием SIM-карт любого оператора сотовой связи (Билайн, МТС, Мегафон, Tele2, Ростелеком). Просто установите SIM-карту в слот модема и затем, подключите модем к USB порту вашего ПК, ноутбука или роутера.**

## 1. АВТОРИЗАЦИЯ В WEB-ИНТЕРФЕЙСЕ МОДЕМА

1.1. Подключите ваш роутер с установленным USB модемом к ПК.

1.2. Для настройки модема, откройте обозреватель интернета (браузер), *например, Google Chrome*.

1.3. В адресной строке браузера наберите IP-адрес вашего модема: http://192.168.8.1 и нажмите клавишу **Enter (Ввод данных)**, (Рисунок А1).

1.4. На главной странице web-интерфейса модема отображается уровень сигнала, оператор сотовой связи, стандарт связи и параметры текущего соединения.

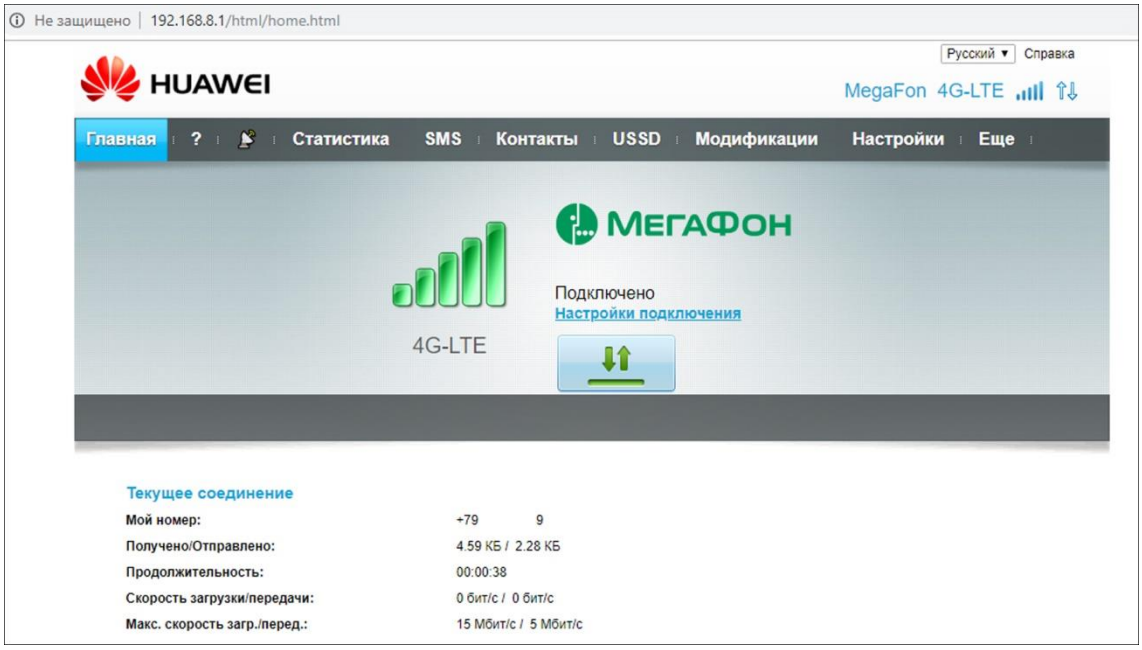


Рисунок А1 – Интерфейс USB модема

## 2. НАСТРОЙКА WEB ИНТЕРФЕЙСА МОДЕМА

### 2.1. Настройка мобильного соединения

2.1.1. Войдите в меню **Настройки** и выберите раздел **«Коммутируемое соединение»**. Во вкладке **«Мобильное соединение»** (Рисунок А2)

2.1.2. Установите параметры и режимы соединения, выбрав:

- **режим подключения** (автоматический или ручной);
- если нет необходимости в использовании **мобильной передачи данных**, отключите сетевое соединение, нажав кнопку **«Выключить»**. Последующее подсоединение к мобильной сети необходимо будет произвести вручную, нажав кнопку **«Включить»**;
- установите запрет или разрешение на **передачу данных в роуминге**
- **интервал автоматического отключения** модема при отсутствии сети или сетевого трафика.

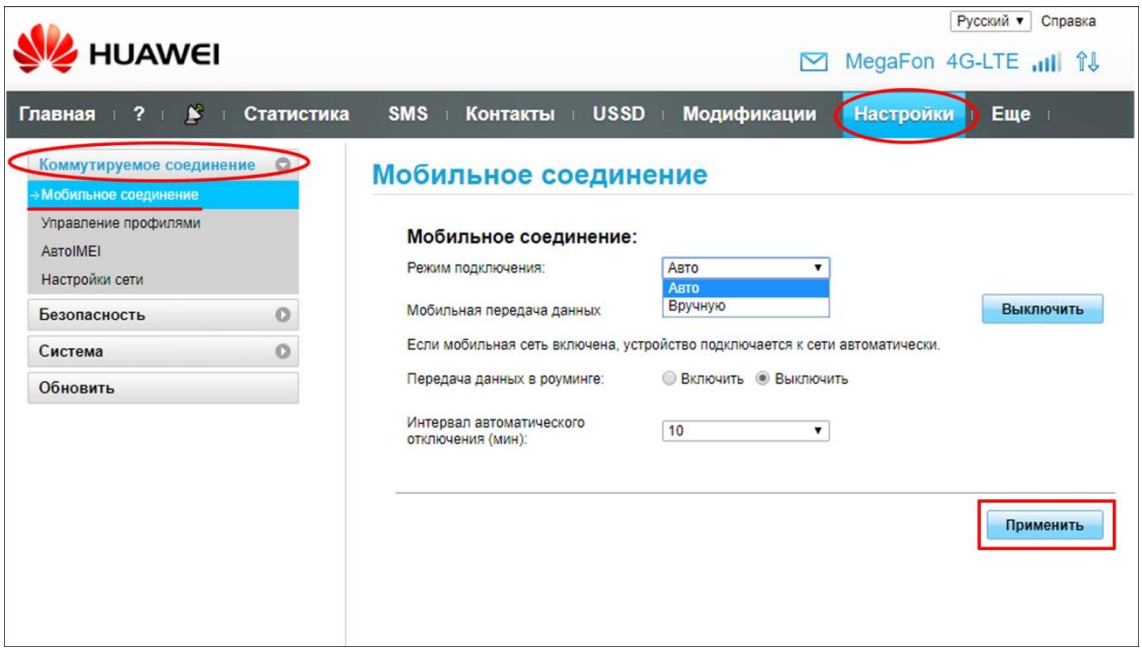


Рисунок А2 – Настройка параметров соединения

2.1.2. Настроив мобильное соединение, нажмите кнопку **Применить**, чтобы настройки были сохранены и вступили в силу.

### 2.2. Управление профилями

В большинстве случаев, настройки профиля загружаются провайдером, и соединение с сетью Интернет происходит автоматически. В редких случаях, для выхода в сеть Интернет необходимо настроить профиль вашего Интернет-соединения.

2.2.1. Войдите в меню **Настройки** и выберите вкладку **«Управление профилями»** в разделе **«Коммутируемое соединение»** (Рисунок А3).

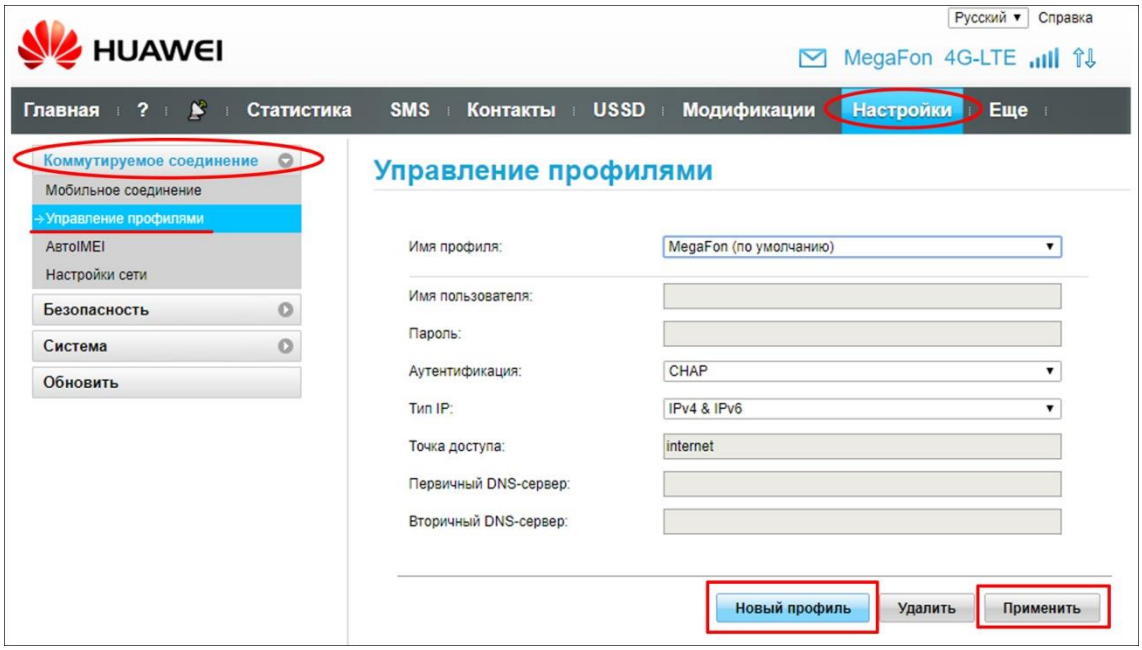


Рисунок А3 – Управление профилями

2.2.2. Создайте или выберите из выпадающего меню **имя профиля**. Затем введите **имя пользователя** и **пароль**, имя **точки доступа** и IP- адреса **DNS-серверов** указанные в договоре на оказание услуг провайдером.

2.2.3. Из выпадающего списка выберите тип протокола соединения (**Тип IP**) при необходимости.

2.2.4. По окончании настройки профиля нажмите кнопку **Применить**.

2.2.5. Чтобы создать новый профиль, нажмите кнопку **Новый профиль** (Рисунок А3).

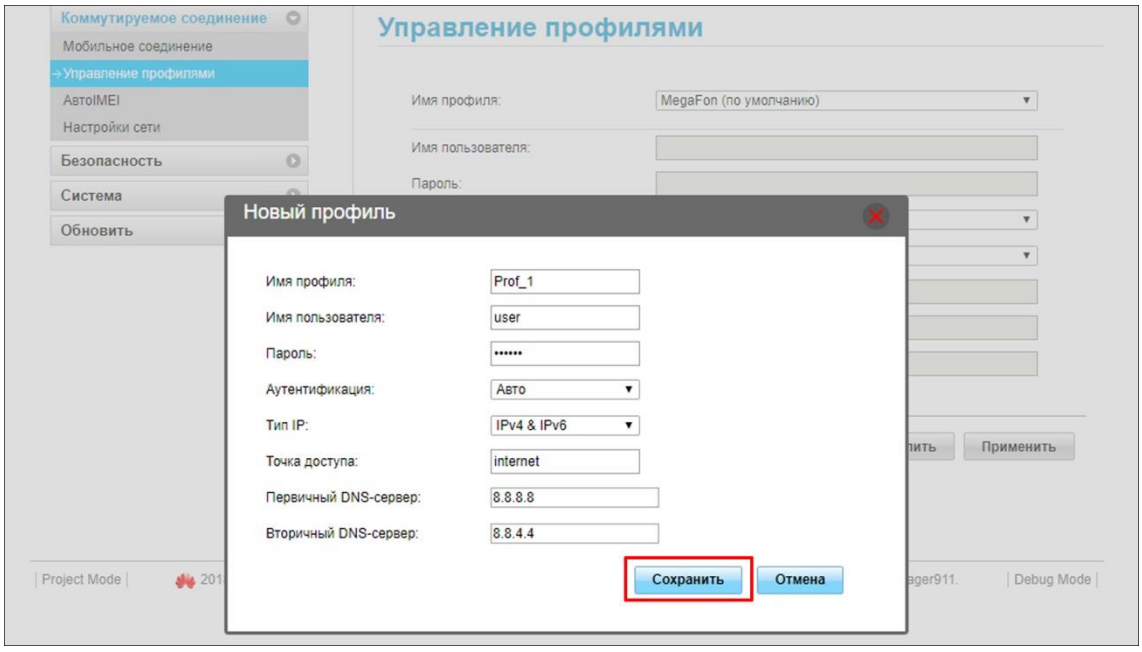


Рисунок А4 – Создание нового профиля

2.2.6. В открывшемся окне, заполните строки, введя имя профиля, имя пользователя, пароль. Имя точки доступа и IP-адреса DNS-серверов. В выпадающем списке выберите тип аутентификации, и тип протокола IP-соединения (Рисунок А4). Затем, нажмите кнопку **Сохранить**.

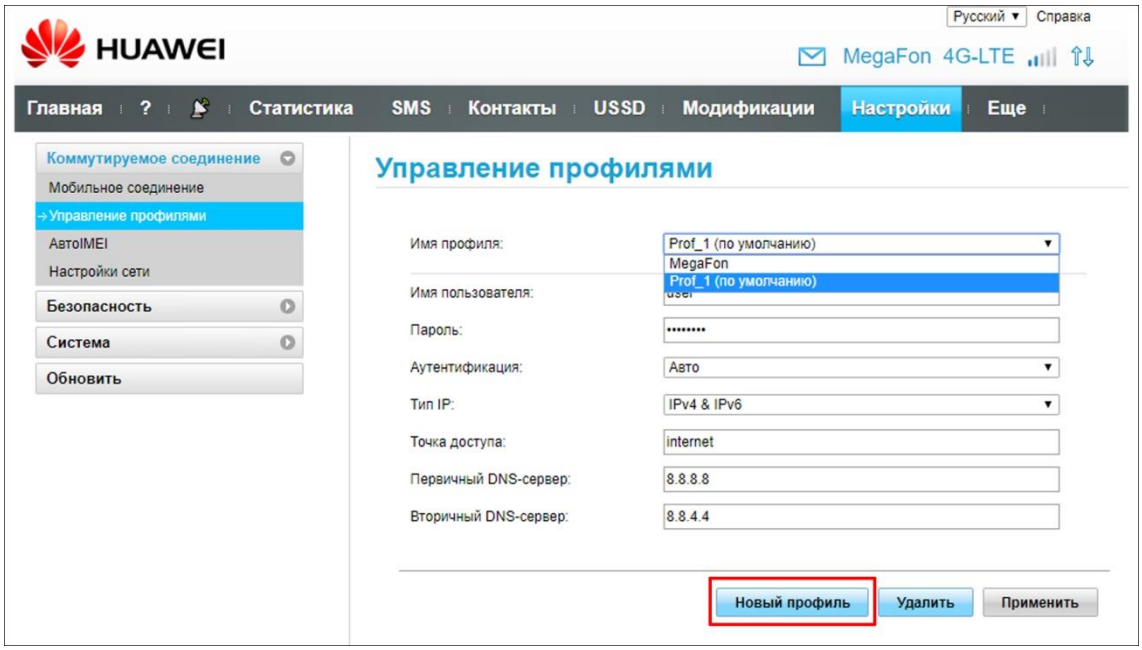


Рисунок А5 – Новый профиль создан и используется по умолчанию

2.2.7. Из выпадающего списка выберите профиль Интернет соединения и нажмите **Применить** (Рисунок А5). Кнопка **Удалить** удаляет выбранный из выпадающего списка профиль.

### 2.3. Изменение IMEI

Web - интерфейс модема Huawei E3372h позволяет изменять международный идентификатор мобильного оборудования (IMEI). В ряде случаев, изменение или смена IMEI может привести к невозможности идентификации оборудования оператором сотой связи. В таком случае, модем не сможет подключиться к мобильной сети и доступ в Интернет будет невозможен.

**Все неисправности модема Huawei E3372h возникшие после смены или изменения IMEI считаются не гарантийными. В некоторых странах изменение IMEI является уголовно наказуемым деянием! Прежде чем производить изменение или смену IMEI ознакомьтесь с законодательством своего государства!**

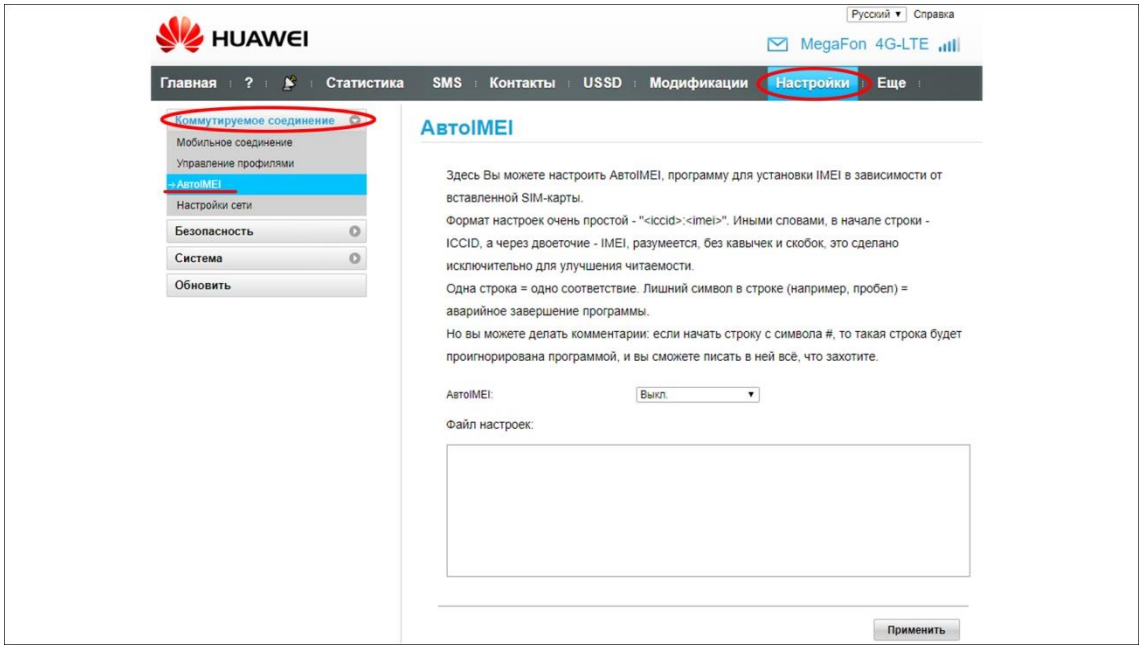


Рисунок А6 – Окно настройки программы АвтоIMEI

2.3.1. Войдите в меню **Настройки** и выберите вкладку **«АвтоIMEI»** в разделе **«Коммутируемое соединение»** (Рисунок А6). Здесь производится настройка программы АвтоIMEI, которая устанавливает IMEI в зависимости от установленной SIM-карты.

**2.4. Сетевые настройки модема**

Пользователь может самостоятельно установить предпочтительные диапазоны и стандарты, в которых будет работать его USB модем более стабильно.

2.4.1. Войдите в меню **Настройки** и выберите вкладку **«Настройка сети»** в разделе **«Коммутируемое соединение»** (Рисунок А7).

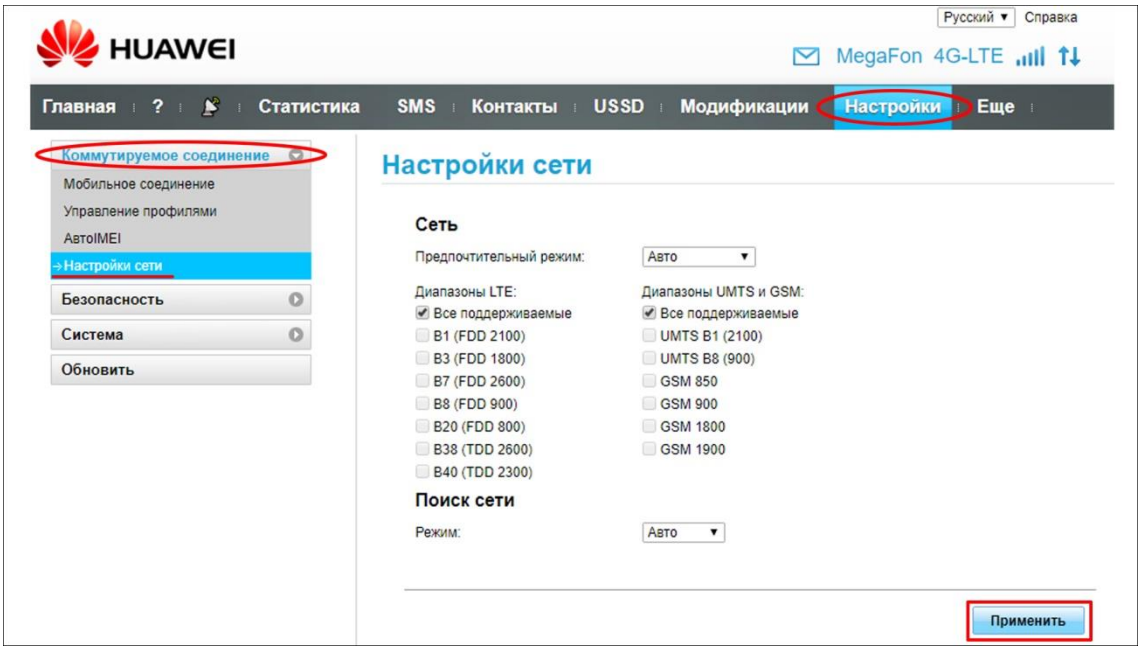


Рисунок А7 – Меню сетевых настроек модема

2.4.2. Из выпадающего списка выберите предпочтительный стандарт сигнала, с которым будет работать модем (Рисунок А8):

- (**Авто**) - автоматический выбор стандарта;
- (**Только GSM**) - работа только в стандарте GSM;
- (**Только UMTS**) - работа только в стандарте UMTS;
- (**Только LTE**) - работа только в стандарте;
- (**LTE->UMTS**) - работа в сети стандарта LTE, а при её отсутствии переключаться в стандарт UMTS:
- (**LTE->GSM**) - работа в сети стандарта LTE, а при её отсутствии переключаться в стандарт GSM;
- (**UMTS->GSM**) - работа в сети стандарта UMTS, а при её отсутствии переключаться на стандарт GSM.

2.4.3. Опционально выберите предпочтительные частотные диапазоны LTE с методом разделения каналов FDD (частотное разделение) или TDD (временное разделение) поддерживаемые вашим оператором.

2.4.4. Аналогично выберите рабочие частоты оператора в диапазонах UMTS и GSM.

2.4.5. Пользователь может установить режим поиска сети. Поиск сети будет произведен автоматически или вручную.

2.4.6. Для сохранения настроек и вступления их в силу, нажмите кнопку **Применить**.

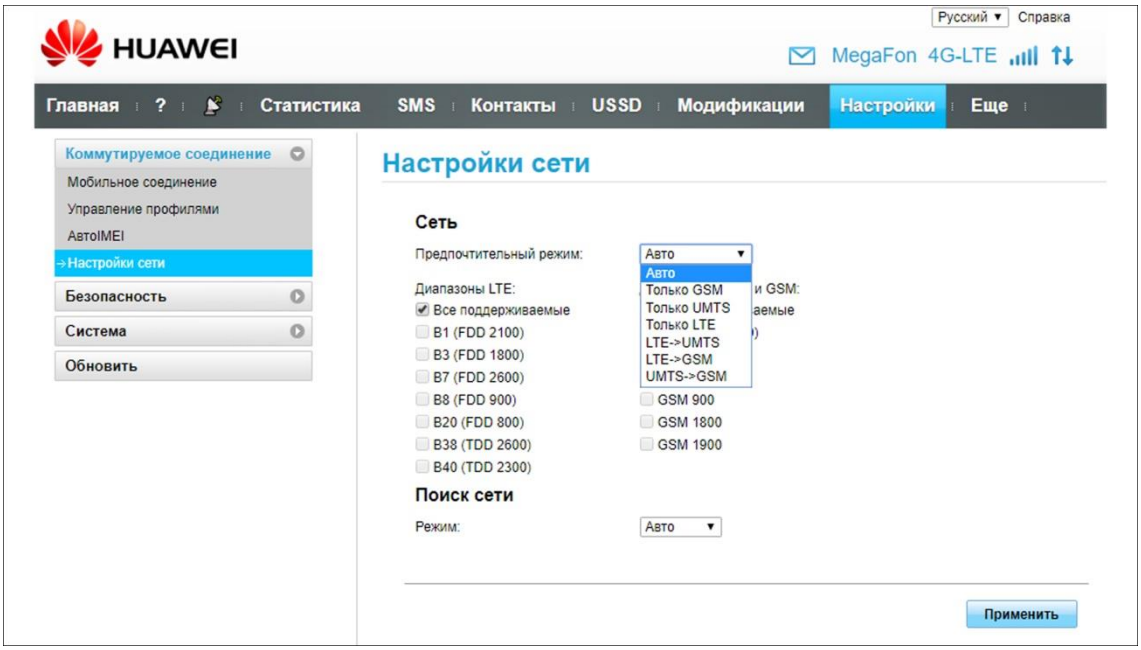


Рисунок А8 – Выбор предпочтительного стандарта мобильного сигнала

## 3. НАСТРОЙКИ БЕЗОПАСНОСТИ

### 3.1. Защита PIN-кодом от несанкционированного выхода в сеть

Для защиты от несанкционированного выхода в сеть Интернет, необходимо использовать PIN-код. С его помощью производится авторизация владельца SIM-карты. PIN-код предоставляется оператором сотовой связи владельцу SIM-карты при её продаже.

3.1.1. Войдите в меню **Настройки** и выберите вкладку **«Защита PIN-кодом»** в разделе **«Безопасность»** (Рисунок А9).

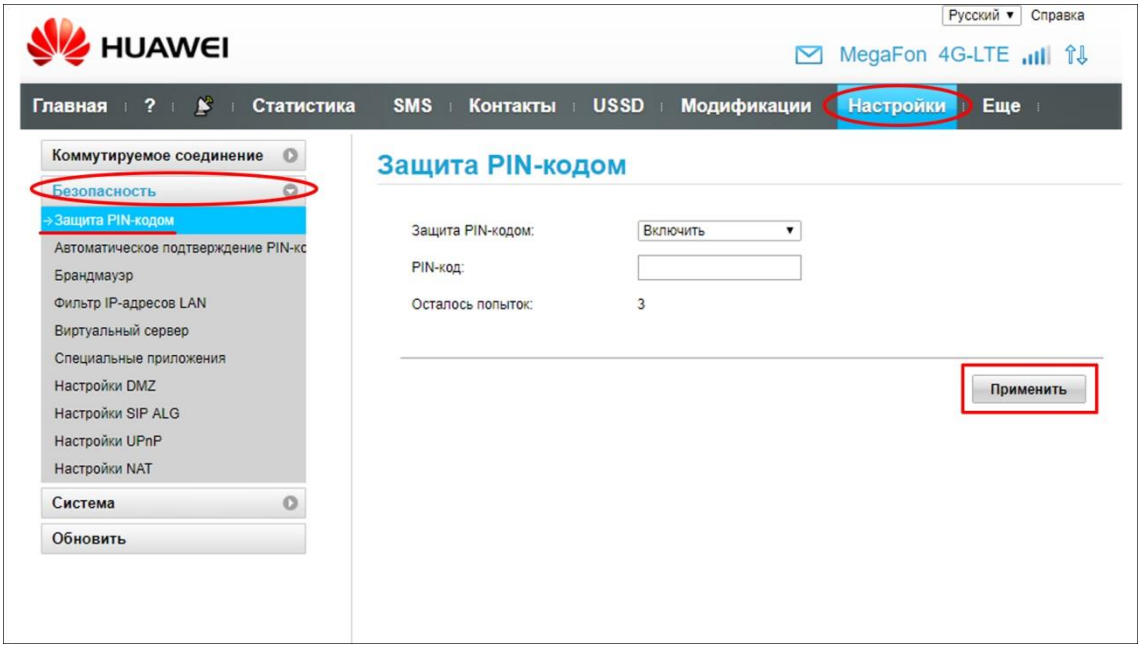


Рисунок А9 – Включение защиты PIN-кодом

3.1.2. Из выпадающего списка выберите **Включить** защиту PIN-кодом. Введите PIN-код в соответствующее поле и нажмите кнопку **Применить**.

3.1.3. Все последующие соединения с оператором будут происходить только после ввода корректного PIN-кода.

### 3.2. Автоматическое подтверждение PIN-кода

В мобильных тарифах операторов сотовой связи, интернет-сессия может быть ограничена по времени. В зависимости от условий договора и формы оплаты, оператором устанавливается максимальная длительность интернет-сессии. По достижении максимальной длительности интернет-сессии, происходит кратковременное отсоединение абонента от сети Интернет.

В дальнейшем, в зависимости от настроек мобильного соединения (п.2.1. настоящего Приложения), ваш модем либо восстанавливает Интернет-соединение автоматически, либо пользователь подключается к сети Интернет вручную.

В случае автоматического восстановления соединения модемом и включенной защите PIN-кодом, пользователь должен вводить PIN-код для авторизации. В случае неустойчивого Интернет-соединения и частых разрывов, установите автоматическое подтверждение PIN-кода.

3.2.1. Войдите в меню **Настройки** и выберите вкладку **«Автоматическое подтверждение PIN-кода»** в разделе **«Безопасность»** (Рисунок А10).

3.2.2. Включите или выключите автоматическое подтверждение PIN-кода, затем введите PIN-код в соответствующее поле и нажмите кнопку **Применить**. Текущий статус подтверждения PIN-кода будет изменен.

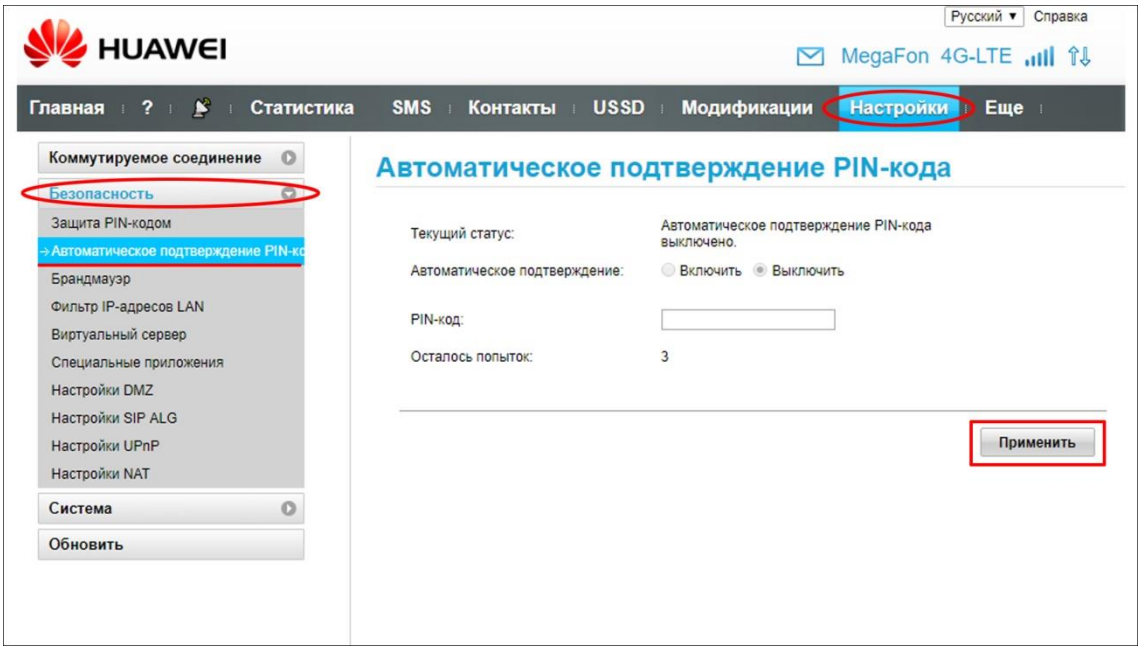


Рисунок А10 – Автоматическое подтверждение PIN-кода

### 3.3. Настройка межсетевого экрана (брандмауэра)

Межсетевой экран (брандмауэр) это программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Основной задачей межсетевого экрана является защита сегментов сети или отдельных хостов от несанкционированного доступа.

3.3.1. Войдите в меню **Настройки** и выберите вкладку **«Брандмауэр»** в разделе **«Безопасность»** (Рисунок А11).

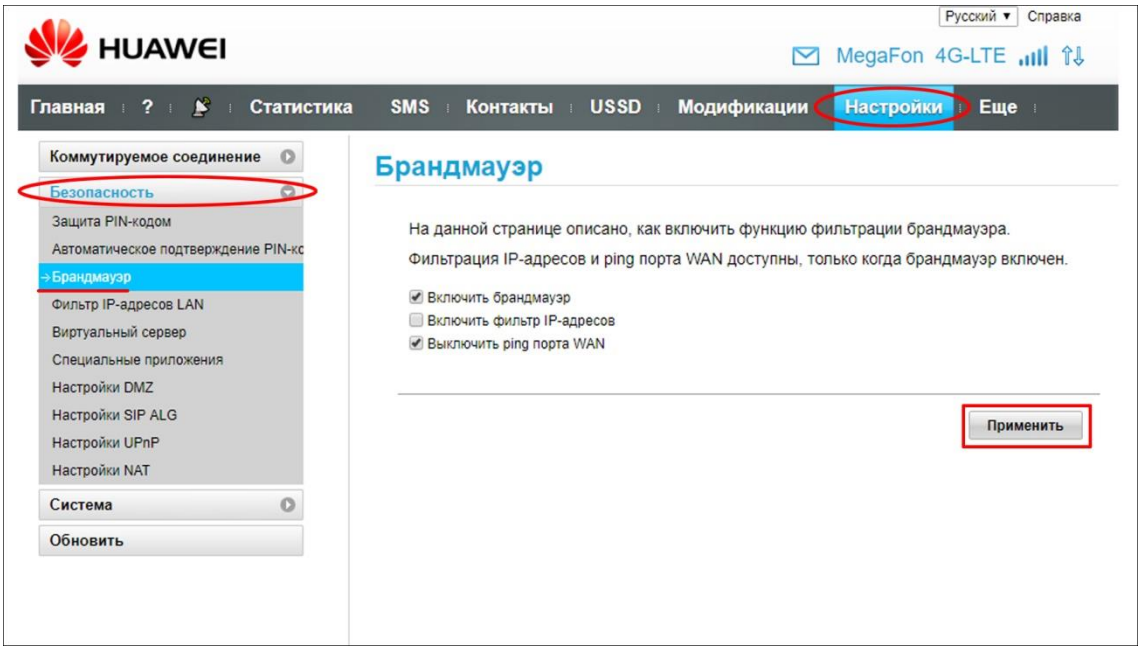


Рисунок А11 – Включение межсетевого экрана

3.3.2. В данной вкладке пользователь может **включить межсетевой экран (брандмауэр)**. Если планируете производить фильтрацию пакетов по IP-адресу и протоколу, **включите фильтр IP-адресов**. При отсутствии проводного Интернет подключения от Интернет-провайдера, **выключите ping порта WAN.**

3.3.3. Настроив межсетевой экран (брандмауэр) нажмите кнопку **Применить**, чтобы настройки были сохранены и вступили в силу.

### 3.4. Фильтрация IP-адресов локальной сети

Функция фильтрации IP-адресов локальной сети (LAN) применяется для ограничения доступа к определенным сервисам сети Интернет для определенных клиентов локальной сети. Убедитесь, что функция фильтрации IP-адресов включена.

Примечание. Включите функцию фильтрации IP-адресов, как указано в п. 3.3. настоящего Приложения.

3.4.1. Войдите в меню **Настройки** и выберите вкладку **«Фильтр IP-адресов LAN»** в разделе **«Безопасность»** (Рисунок А12).

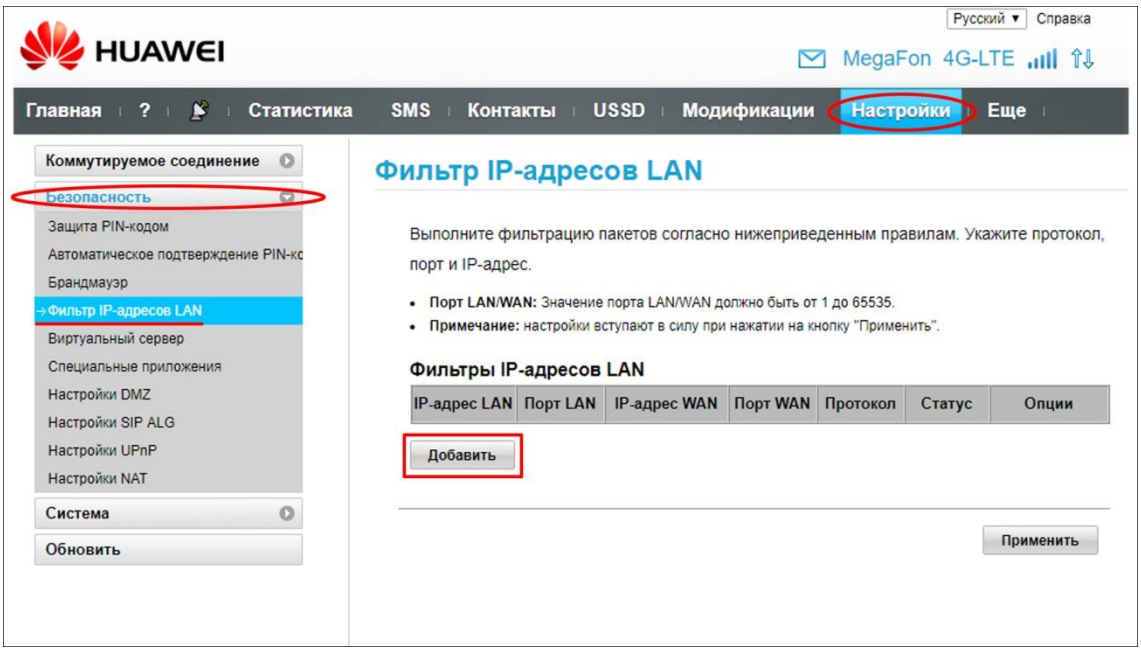


Рисунок А12 – Фильтр IP-адресов LAN

3.4.2. Нажмите кнопку **Добавить** и введите в таблицу значения IP-адресов и номера портов локальной (LAN) и глобальной (WAN) сети (Рисунок А13).

*В нашем примере мы ограничиваем доступ клиенту локальной сети (LAN) с IP-адресом 192.168.1.101 к ресурсу глобальной сети (WAN) имеющему IP-адрес 217.20.147.1.*

3.4.3. Из выпадающего списка выберите протокол. Если вы не знаете протокол подключения, выберите **TCP/UDP**. Модем автоматически выберет нужный протокол. Измените статус фильтра IP-адресов на включено (**Вкл.**) или выключено (**Выкл.**). Для сохранения созданного фильтра нажмите кнопку **ОК** в колонке Опции. Для удаления фильтра IP-адресов, нажмите кнопку **Отмена** в колонке Опции.

3.4.4. Завершив настройки фильтра IP-адресов, для сохранения и вступления в силу созданной конфигурации нажмите кнопку **Применить**.

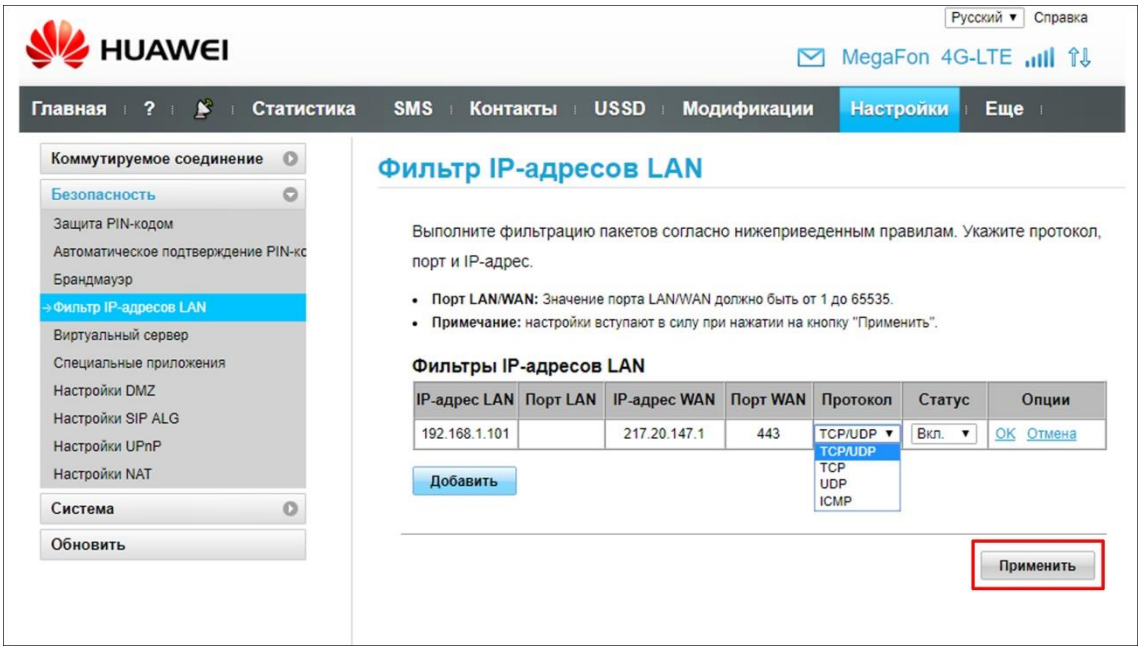


Рисунок А13 – Ввод значений IP-адресов и портов

### 3.5. Открытие портов для доступа к своим устройствам из сети Интернет

В рамках виртуального сервера пользователь может настроить параметры маршрутизации, для получения доступа к своим устройствам из сети Интернет. Роутер перенаправляет получаемый на один из портов трафик, на выбранные пользователем порты и устройства.

3.5.1. Войдите в меню **Настройки** и выберите вкладку **«Виртуальный сервер»** в разделе **«Безопасность»** (Рисунок А14).

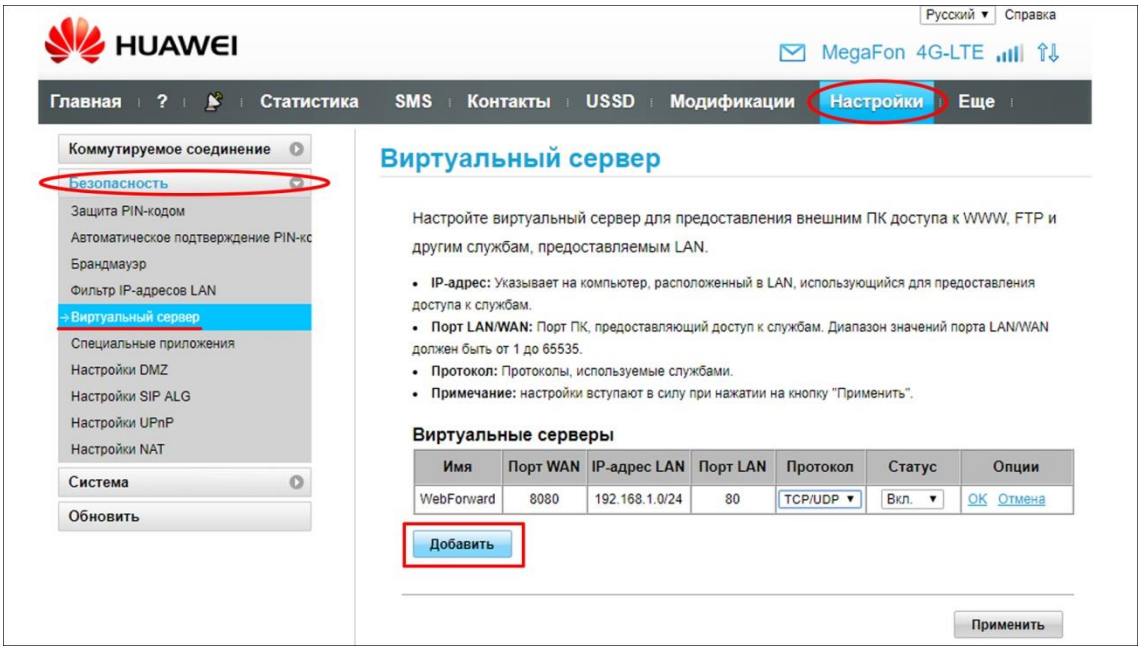


Рисунок А14 – Перенаправление портов в рамках виртуального сервера

3.5.2. Нажмите кнопку **Добавить** и введите в таблицу:

- имя перенаправления;
- номер внешнего порта (WAN), с которого будет перенаправляться траффик;
- IP-адрес локального устройства;
- номер порта локального устройства, на которое перенаправляется трафик.

3.5.3. Из выпадающего списка выберите протокол. Если вы не знаете протокол подключения, выберите **TCP/UDP**. Модем автоматически выберет нужный протокол. Измените статус нового

перенаправления портов на включено (**Вкл.**) или выключено (**Выкл.**). Для сохранения созданного перенаправления портов, нажмите кнопку **ОК** в колонке Опции. Для удаления созданного или имеющегося перенаправления портов, нажмите кнопку **Отмена** в колонке Опции.

3.5.4. Для сохранения и применения настроек нажмите кнопку **Применить**.

### 3.6. Специальные приложения

Существует ряд специальных программ, которые предназначены для организации общения и эффективного взаимодействия между пользователями локальной сети. Например, программа для организации голосовой связи в локальной сети, различные чаты с общими и закрытыми каналами и т.п.

3.6.1. Войдите в меню **Настройки** и выберите вкладку **«Специальные приложения»** в разделе **«Безопасность»** (Рисунок А15).

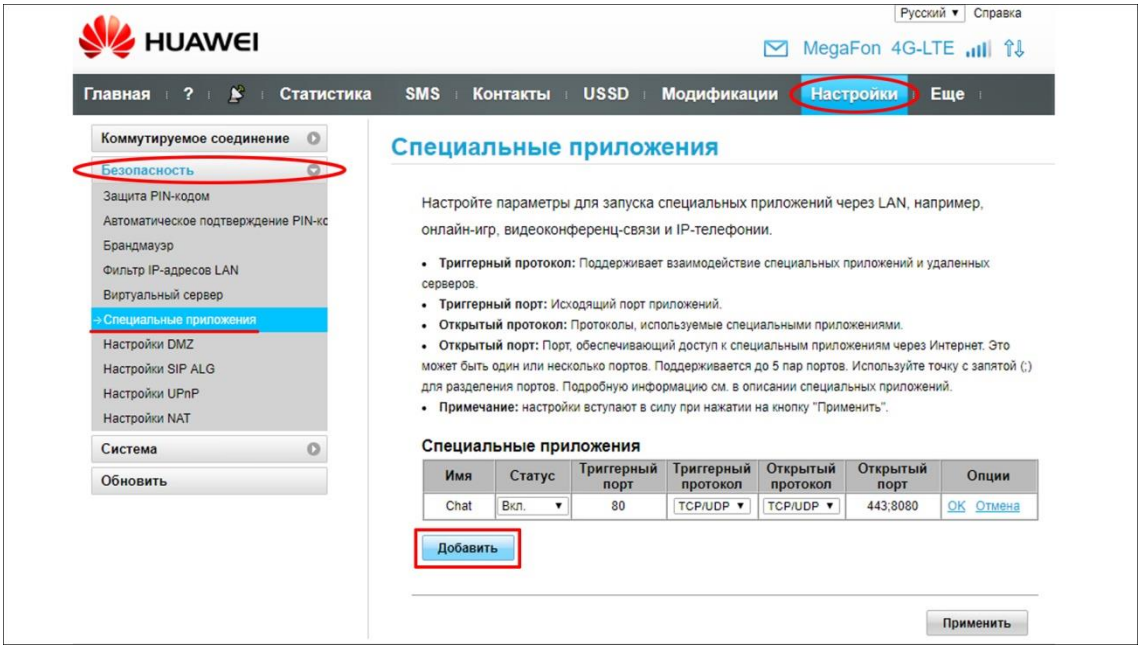


Рисунок А15 – Настройка параметров для специальных приложений

3.6.2. Нажмите кнопку **Добавить** и введите в таблицу:

- имя специального приложения;
- номер триггерного порта (исходящий порт приложения):
- номера открытых портов (порты обеспечивающие доступ к специальным приложениям через Интернет);

3.6.3. Из выпадающих списков выберите **триггерный** и **открытый протоколы**. Если вы не знаете, какие протоколы следует установить, выберите **TCP/UDP**. Модем автоматически выберет нужный протокол. Измените статус специального приложения на включено (**Вкл.**) или выключено (**Выкл.**). Для сохранения созданной настройки для специального приложения, нажмите кнопку **ОК** в колонке Опции. Для удаления созданной или имеющейся настройки для специального приложения, нажмите кнопку **Отмена** в колонке Опции.

3.6.4. Для сохранения и применения настроек нажмите кнопку **Применить**.

### 3.7. Настройка Демилитаризованной Зоны на модеме

Демилитаризованная Зона (DMZ) это специальный сегмент локальной сети, в который выводятся сервисы и устройства, к которым должен быть открыт доступ, как из локальной, так и из внешней сети.

В ряде случаев возникает необходимость открытия доступа к оборудованию, например, регистратору камер видеонаблюдения из внешней сети. Можно столкнуться с тем, что порты устройств заняты, и перенаправить их не удается. Тогда, для открытия доступа, необходимо добавить IP-адрес оборудования в специальную DMZ зону на модеме, тем самым сделав из него DMZ-хост. При этом локальная сеть по-прежнему будет закрыта, а DMZ-хост теперь полностью

доступен из сети Интернет и обеспечивает свою безопасность сам, например установленным паролем.

3.7.1. Войдите в меню **Настройки** и выберите вкладку **«Настройки DMZ»** в разделе **«Безопасность»** (Рисунок А16).

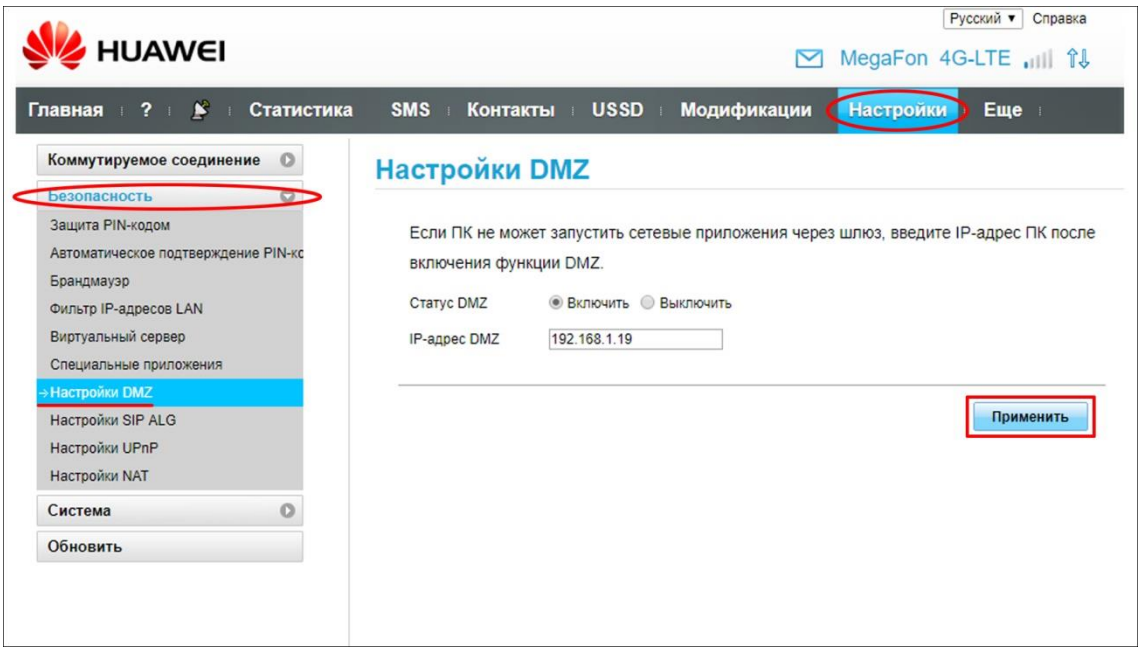


Рисунок А16 – Вывод оборудования в Демилитаризованную Зону модема

3.7.2. Для вывода оборудования в Демилитаризованную Зону (DMZ), измените **статус DMZ** на «**Включить**» и введите IP- адрес оборудования в специальной строке. Затем нажмите кнопку **Применить**, чтобы настройки вступили в силу и были сохранены.

### 3.8. Настройка порта SIP ALG

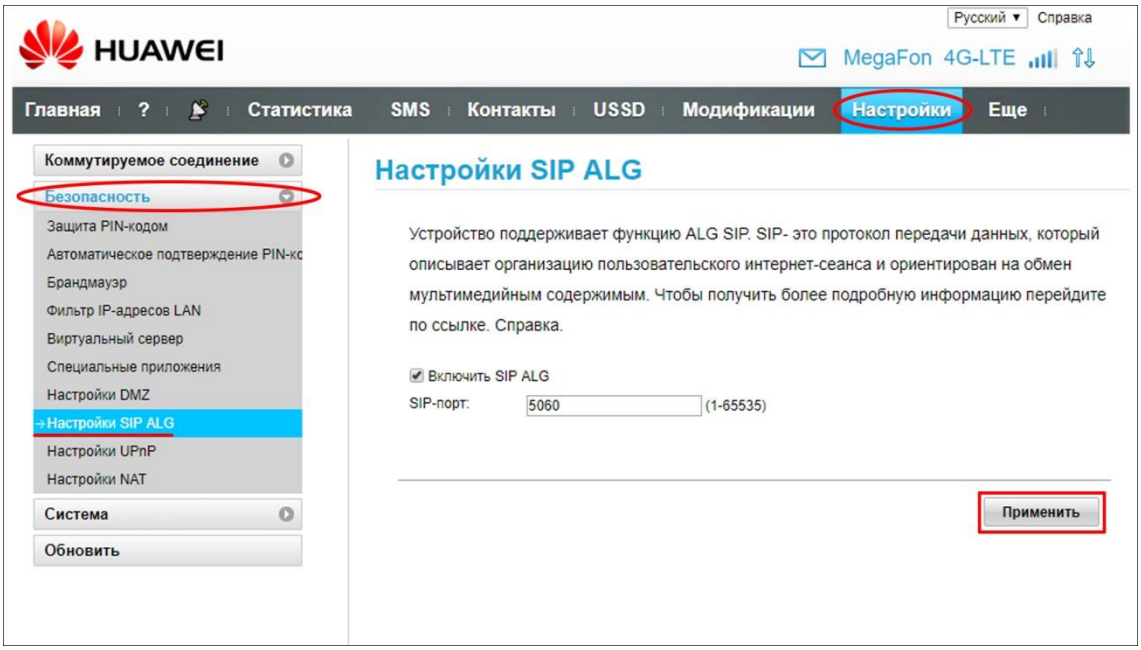


Рисунок А17 – Настройка шлюза прикладного уровня

«Шлюз прикладного уровня» (ALG) — это программный компонент, управляющий конкретными протоколами приложения, такими как SIP и FTP. ALG используется как посредник между Интернетом и сервером приложений, который понимает прикладной протокол. ALG выступает в

качестве сервера конечной точки и может разрешать или запрещать трафик к серверу приложений. Для этого ALG перехватывает и анализирует указанный трафик, распределяет ресурсы и определяет динамические политики, которые разрешают трафик, проходящий через шлюз.

3.8.1. Войдите в меню **Настройки** и выберите вкладку **«Настройки SIP ALG»** в разделе **«Безопасность»** (Рисунок А17).

3.8.2. Для включения программного компонента установите разрешающую «галочку» в строке **Включить SIP ALG** и введите номер SIP-порта в соответствующее поле. Затем нажмите кнопку **Применить**, чтобы настройки были сохранены и вступили в силу.

### 3.9. Включение «умного соединения» устройств UPnP

UPnP (Universal Plug and Play) — это архитектура многоранговых соединений между персональными компьютерами и интеллектуальными устройствами обеспечивающая автоматическое подключение подобных устройств друг к другу и их совместную работу.

Технология UPnP обеспечивает обмен данными между любыми двумя устройствами, находящимися под контролем какого-либо управляющего устройства сети. Технология UPnP действует независимо от используемой операционной системы, физической среды передачи данных или языка программирования. В результате использования технологии UPnP настройка локальной сети становится легкой для настройки большому числу пользователей.

3.9.1. Войдите в меню **Настройки** и выберите вкладку **«Настройки UPnP»** в разделе **«Безопасность»** (Рисунок А18).

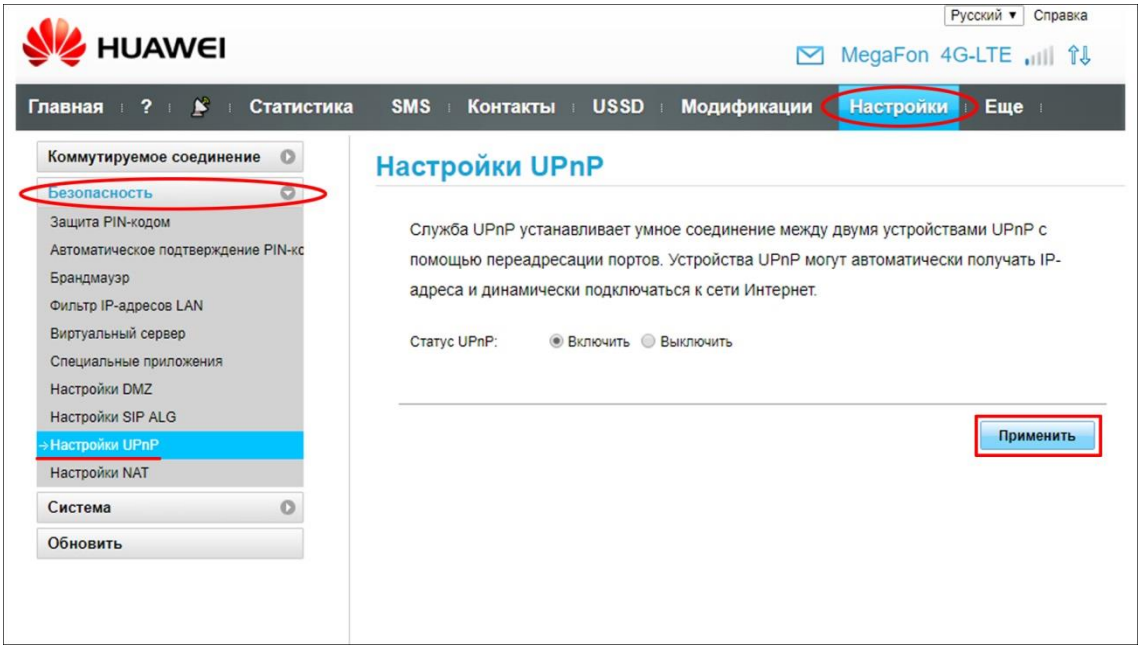


Рисунок А18 – включение «умного соединения» устройств

3.9.2. Включите «умное соединение» UPnP установив маркер напротив обозначения «**Включить**». Нажмите кнопку **Применить** для сохранения настроек и активации включенного режима.

### 3.10. Выбор механизмов преобразования сетевых адресов NAT

NAT (Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

Применение технологии NAT позволяет:

а) сэкономить IP-адреса, транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних).

б) Позволяет предотвратить или ограничить обращение снаружи к внутренним хостам, оставляя возможность обращения из внутренней сети к внешней.

в) Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов.

3.10.1. Войдите в меню **Настройки** и выберите вкладку **«Настройки NAT»** в разделе **«Безопасность»** (Рисунок А19).

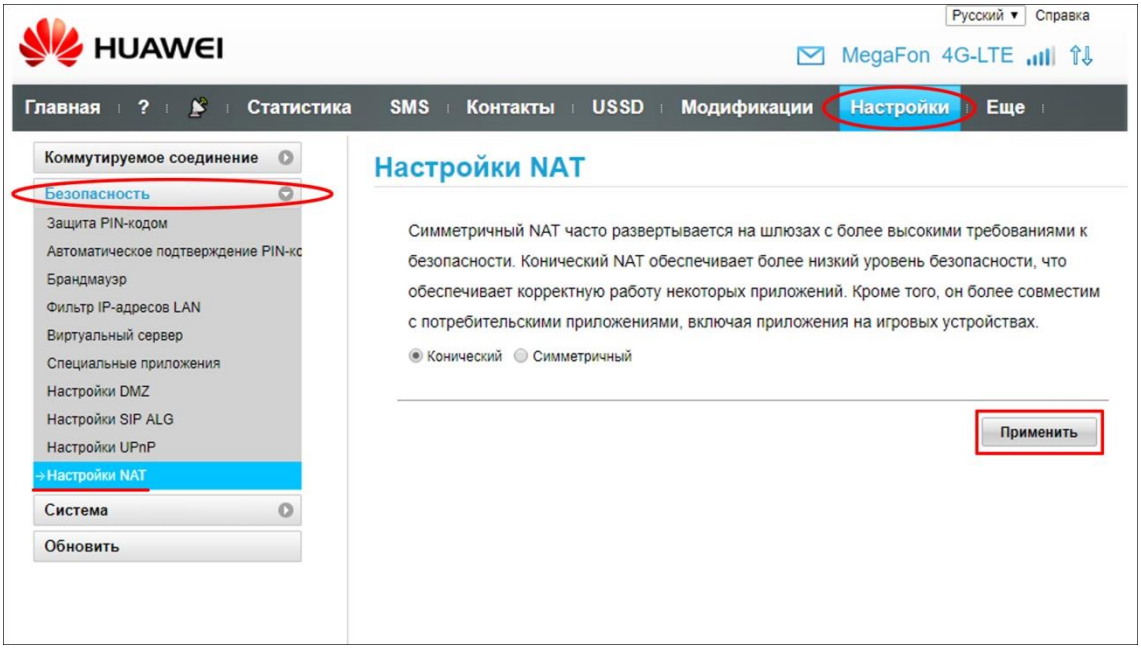


Рисунок А19 – Выбор механизмов взаимодействия локальной сети с внешней сетью

3.10.2. Включите **Конический** или **Симметричный** механизм взаимодействия локальной сети с внешней сетью, установив маркер напротив соответствующего обозначения. Нажмите кнопку **Применить** для сохранения настроек и активации включенного механизма.

## 4. НАСТРОЙКИ СИСТЕМЫ

### 4.1. Сводная информация об устройстве

4.1.1. Для получения информации о модеме войдите в меню **Настройки** и выберите вкладку **«Информация об устройстве»** в разделе **«Система»** (Рисунок А20).

Примечание. Для быстрого перехода во вкладку **«Информация об устройстве»** нажмите изображение вопросительного знака в главном меню.

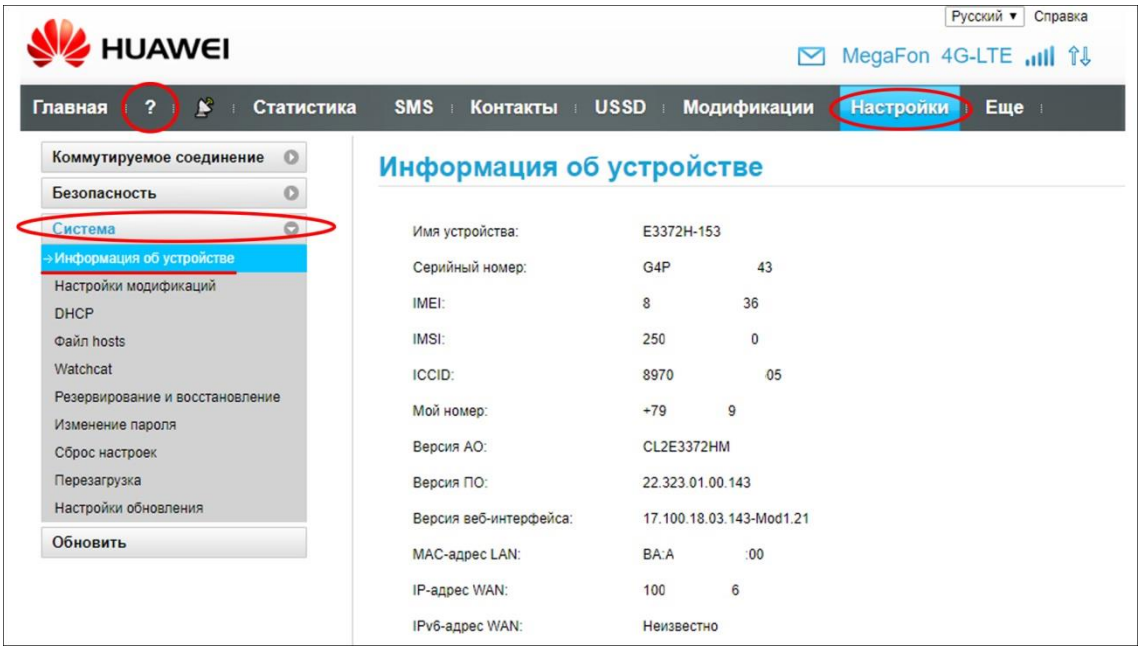


Рисунок А20 – Информация об устройстве

### 4.2. Настройка модификаций устройства

В данном разделе настроек системы, пользователь может модифицировать настройки модема для его оптимального функционирования. Внесение модификаций в системные настройки модема (такие как изменение или смена серийного номера, IMEI) пользователем приведет к потере гарантии на устройство!

4.2.1. Войдите в меню **Настройки** и выберите вкладку **«Настройки модификаций»** в разделе **«Система»** (Рисунок А21).

4.2.2. В этом пункте рассмотрим опцию изменения TTL.

**Фиксация TTL**. Число TTL обозначает время жизни пакетов трафика и определяет число участков («прыжков») между маршрутизаторами. Наличие этого параметра не позволяет пакету бесконечно ходить по сети. Каждый маршрутизатор при маршрутизации (при каждом транзитном «прыжке») должен уменьшать значение TTL на единицу. Максимальное значение TTL=255. Для Linux, Android, iOS обычное начальное значение TTL=64, для Windows TTL=128. Контроль TTL часто используются операторами сотовой связи для обнаружения использования SIM-карт в устройствах отличных от смартфона (при использовании абонентом смартфонных тарифов).

Для обхода контроля TTL, измените значение TTL.

4.2.3. Настроив модификации, для вступления в силу и сохранения изменений нажмите кнопку **Применить** внизу страницы.

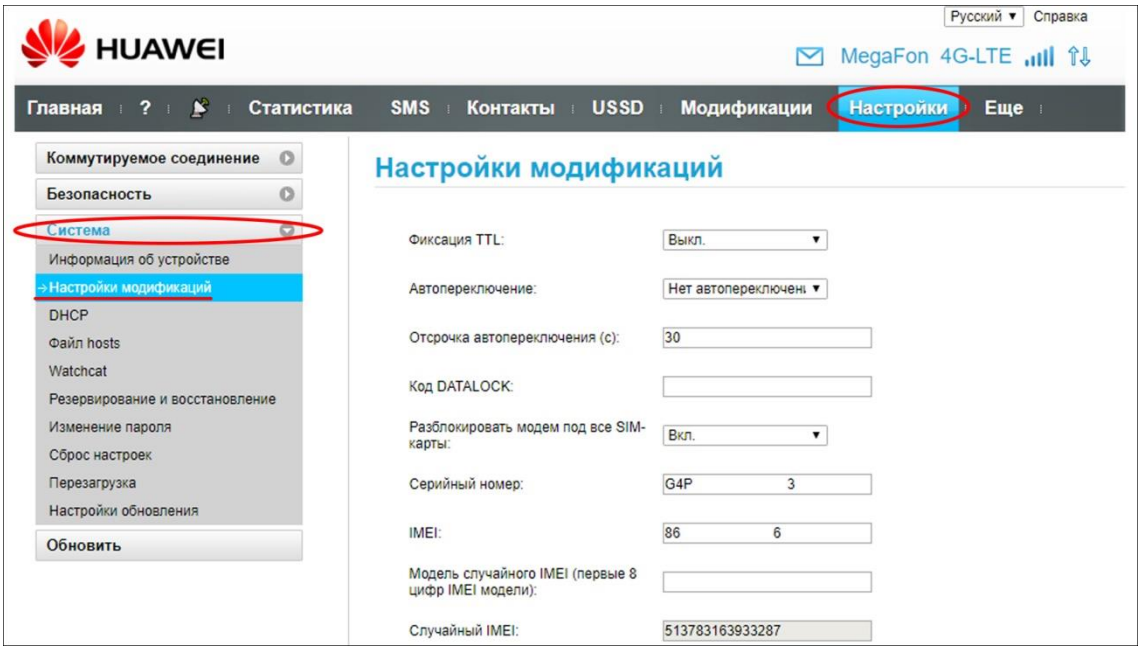


Рисунок А21 – Настройка модификаций устройства

### 4.3. Протокол динамической настройки узла DHCP

**DHCP** — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Администратор может задать диапазон адресов, распределяемых модемом среди компьютеров.

4.3.1. Войдите в меню **Настройки** и выберите вкладку **«DHCP»** в разделе **«Система»** (Рисунок А22).

4.3.2. На странице указан IP-адрес модема, который используется как DHCP сервер. Включение или выключение функции DHCP сервера в модеме производится установкой маркера напротив соответствующего значения. По умолчанию, задан диапазон 100 IP-адресов, которые будут распределены модемом между подключаемыми устройствами.

4.3.3. Введите IP-адрес первичного DNS-сервера и при необходимости вторичного DNS-сервера. Установите срок аренды DHCP в диапазоне 86400-804800 секунд.

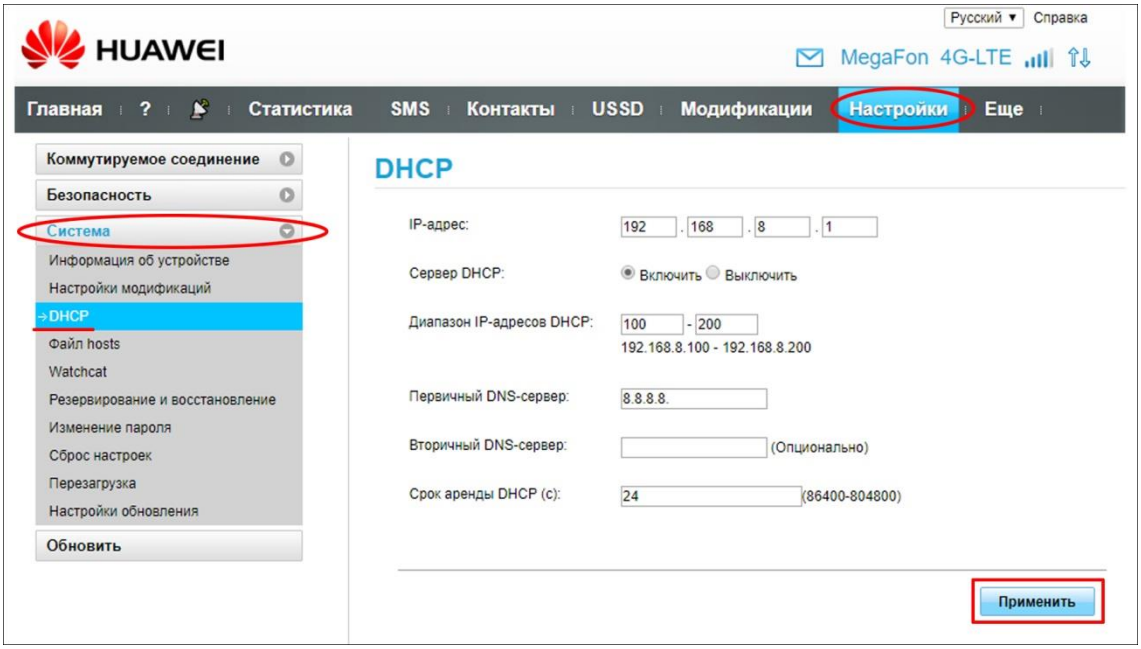


Рисунок А22 – настройка протокола динамической настройки

4.3.4. Чтобы изменения были сохранены и вступили в силу, нажмите кнопку **Применить**.

### 4.4. Файл hosts

**Hosts** – текстовый файл содержащий базу доменных имен и используемый при их трансляции в сетевые адреса узлов. Запрос к этому файлу имеет приоритет перед обращением к DNS-серверам. Содержимое файла задается администратором устройства.

Файл hosts служит:

- для ускорения загрузки (если IP-адрес запрашиваемого ресурса был найден в файле hosts, то обращения к внешнему DNS-серверу не происходит);
- для блокировки нежелательных сайтов (назначив против их имени либо локальный IP 127.0.0.1, либо IP какого-либо другого сайта);
- для блокировки доступа к определенным сайтам.

4.4.1. Войдите в меню **Настройки** и выберите вкладку **«Файл hosts»** в разделе **«Система»** (Рисунок А23).

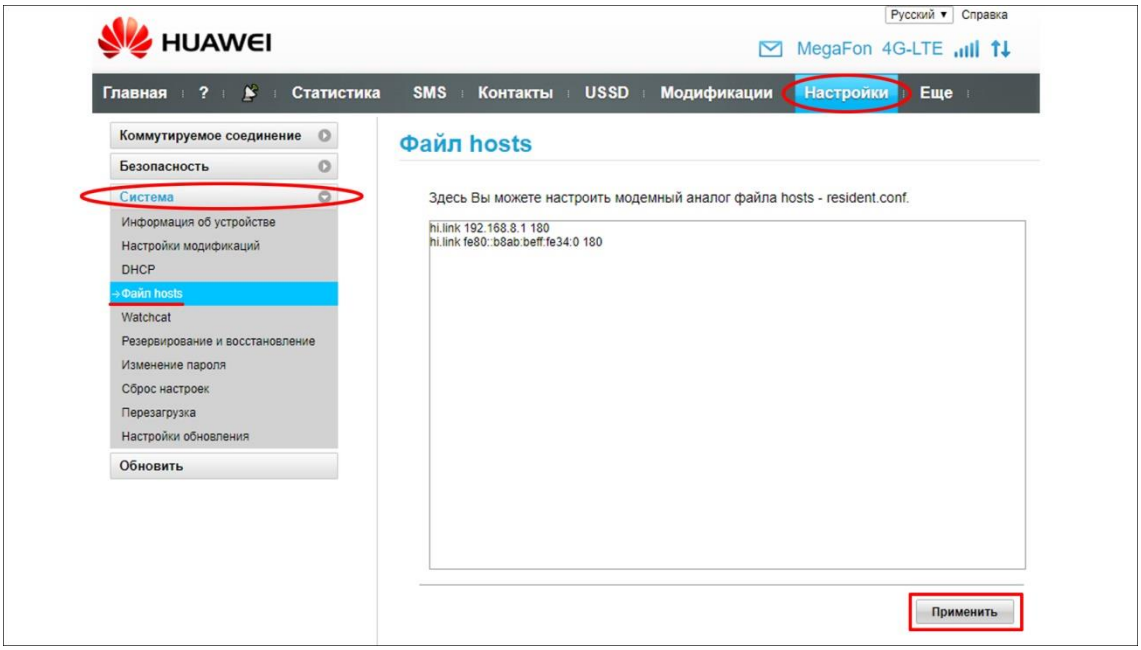


Рисунок А23 – Редактирование файла hosts

4.4.2. Закончив редактирование файла, нажмите кнопку **Применить**. Изменения будут сохранены и вступят в силу.

### 4.5. Перезагрузка модема по расписанию

Утилитой Watchcat пользователь настраивает периодическую перезагрузку модема или перезагрузку при потере Интернет-соединения на определенное (заданное пользователем) время.

4.5.1. Войдите в меню **Настройки** и выберите вкладку **«Watchcat»** в разделе **«Система»** (Рисунок А24).

4.5.2. Для включения программной перезагрузки модема, выберите из выпадающего списка статус включено (**Вкл.**). Установите режим работы утилиты:

- **Периодическая перезагрузка** – перезагрузка будет произведена через период, указанный пользователем в соответствующей графе. По умолчанию значения вводятся в секундах. Можно использовать суффиксы «m», «h» и «d» для указания минут, часов и дней.
- **Перезагрузка при потере Интернет-соединения**. Значением данной настройки определяется период времени без доступа в сеть Интернет, после которого модем перезагружается. По умолчанию значения вводятся в секундах. Можно использовать суффиксы «m», «h» и «d» для указания минут, часов и дней.

4.5.3. В случае необходимости перезагрузки системы модема, утилита Watchcat вызовет программную перезагрузку. Установив значение отличное от нуля, пользователь запланирует аппаратную перезагрузку устройства, в случае неудачной программной. Значение **задержки принудительной аппаратной перезагрузки** устанавливается в секундах. Установив значение

задержки принудительной перезагрузки равное нулю, пользователь запланирует только программную перезагрузку.

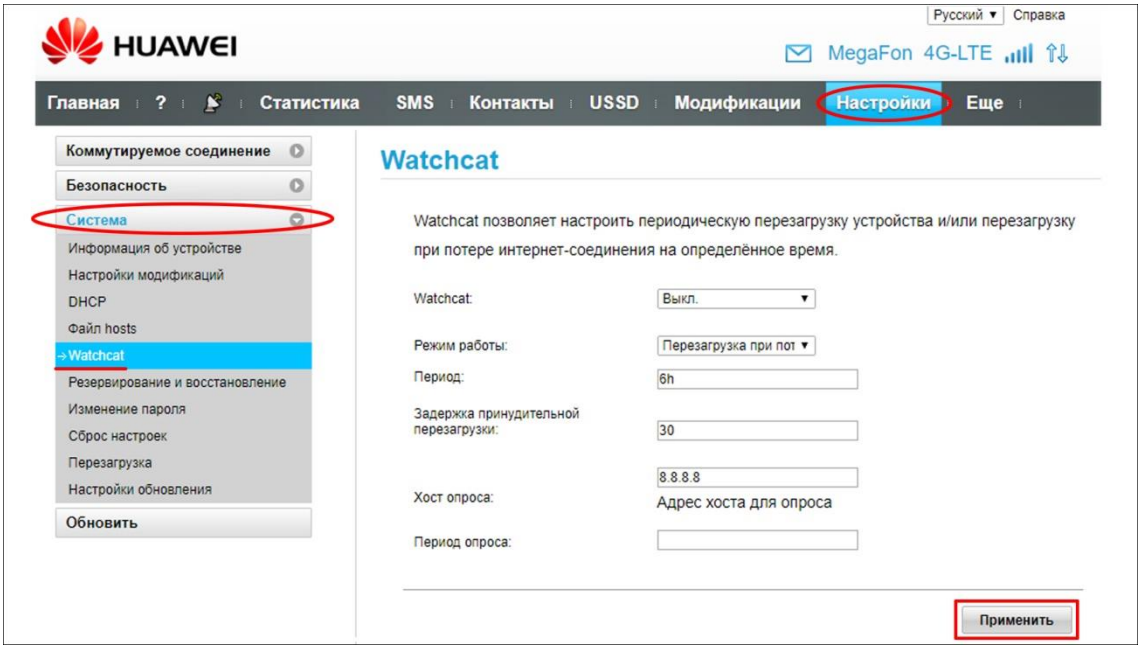


Рисунок А24 – Настройка программной перезагрузки модема

4.5.3. Введите адрес хоста, к которому будет обращаться модем для проверки наличия Интернет-соединения. По умолчанию установлен IP-адрес 8.8.8.8.

4.5.4. Установите периодичность, с которой модем будет проверять наличие Интернет-соединения, обращаясь к хосту для опроса. По умолчанию значения вводятся в секундах. Можно использовать суффиксы «m», «h» и «d» для указания минут, часов и дней.

4.5.5. Завершив настройку программной перезагрузки устройства, нажмите кнопку **Применить**. Настройки будут сохранены и вступят в силу.

### 4.6. Резервирование и восстановление конфигурации устройства

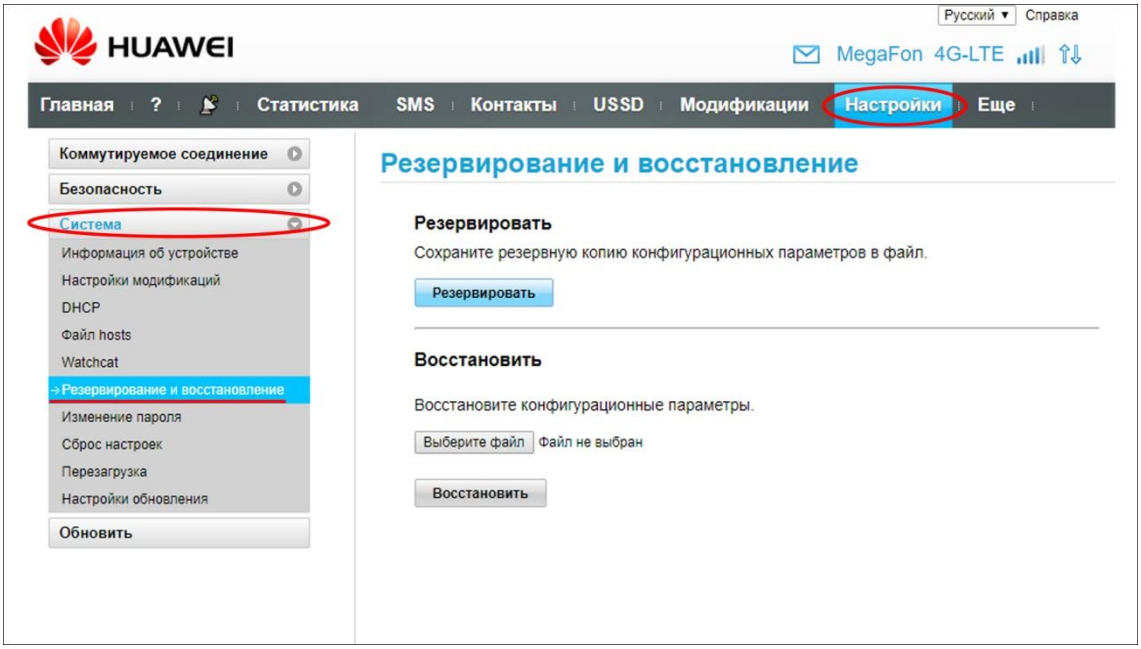


Рисунок А25 – Резервирование и восстановление установок

Резервное копирование предназначено для создания резервных копий, предназначенных для восстановления настроек и данных устройства, возврата (отката) к предыдущим параметрам и настройкам или переносе настроек на другое подобное оборудование.

**Перед обновлением системы или внесением каких-либо изменений, создавайте резервную копию настроек и установок модема!**

4.6.1. Войдите в меню **Настройки** и выберите вкладку **«Резервирование и восстановление»** в разделе **«Система»** (Рисунок А25).

4.6.2. Создайте резервную копию конфигурационных параметров, нажав кнопку **Резервировать**. Укажите директорию, в которой будет сохранен файл с расширением «.bak».

4.6.3. Для восстановления настроек нажмите кнопку **Выберите файл**. Найдите директорию, в которой была сохранена резервная копия и, выделив ее, нажмите кнопку Открыть. Рядом с кнопкой **Выберите файл,** появится имя файла с копией конфигурационных настроек. Нажмите кнопку **Восстановить** и сохраненные в файле резервной копии параметры будут скопированы в модем и применены.

### 4.7. Установка и изменение пароля для входа в web-интерфейс модема

Пароль – условное слово или набор знаков, предназначенный для подтверждения личности пользователя. В вычислительных системах комбинация «имя пользователя – пароль» используется для удостоверения пользователя.

4.7.1. Войдите в меню **Настройки** и выберите вкладку **«Изменение пароля»** в разделе **«Система»** (Рисунок А26).

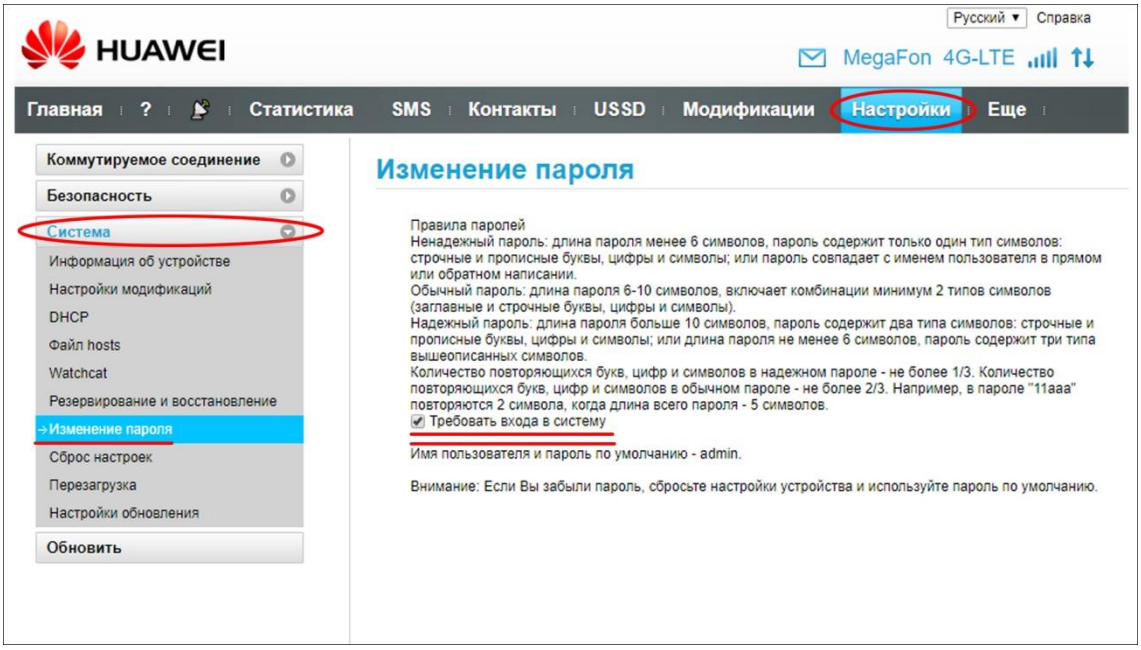


Рисунок А26 – Включение функции авторизации в web-интерфейсе

4.7.2. Для защиты web-интерфейса от несанкционированного входа, установите «галочку» возле опции **Требовать входа в систему**.

4.7.3. Для входа в web-интерфейс модема необходимо будет ввести **имя пользователя** и **пароль.** По умолчанию **имя пользователя** *admin*, **пароль** *admin*. Данный пароль является ненадежным и при первой возможности его нужно изменить на более надежный.

4.7.4. Чтобы изменить пароль, используемый по умолчанию, войдите в меню **Настройки** и выберите вкладку **«Изменение пароля»** в разделе **«Система»** (Рисунок А27)

4.7.5. Введите текущий пароль (по умолчанию пароль *admin*) и новый пароль в соответствующие строки. Web-интерфейс модема проверит уровень надежность нового пароля. Введите новый пароль еще раз в строке подтверждения пароля и нажмите кнопку **Применить**. Дальнейший вход в web-интерфейс будет возможен только по новому паролю.

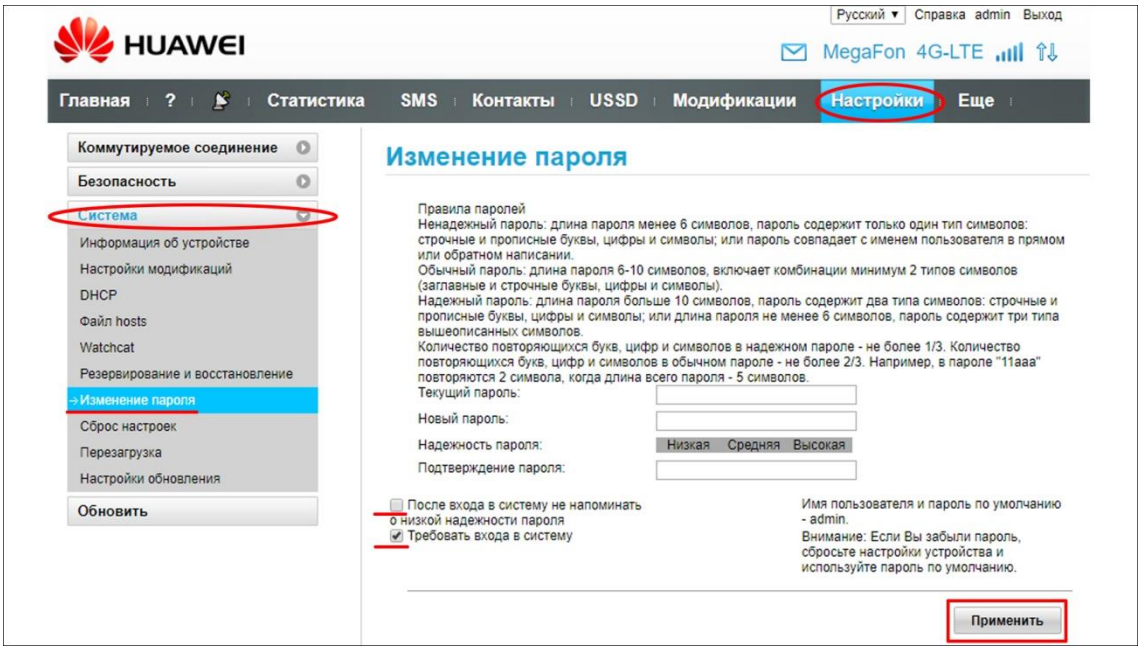


Рисунок А27 – Изменение пароля используемого по умолчанию

4.7.6. Если пользователь использует ненадежный пароль, web-интерфейс устройства будет после каждого входа в систему напоминать ему о низкой надежности пароля. Пользователь может отключить это напоминание, установив «галочку» возле соответствующей опции. Для отключения авторизации при входе в web-интерфейс, снимите «галочку» возле опции **Требовать входа в систему**. Нажмите кнопку **Применить**, чтобы настройки были сохранены и вступили в силу.

### 4.8. Перезагрузка модема

В случаях, когда модем физически недоступен (находится в другом помещении, размещен на роутере в гермобоксе антенны, пользователь заходит в web-интерфейс, используя протоколы удаленного доступа и т.п.) произведите программную перезагрузку устройства.

4.8.1. Войдите в меню **Настройки** и выберите вкладку **«Перезагрузка»** в разделе **«Система»** (Рисунок А28).

4.8.2. Нажмите кнопку Перезагрузка для программной перезагрузки модема.

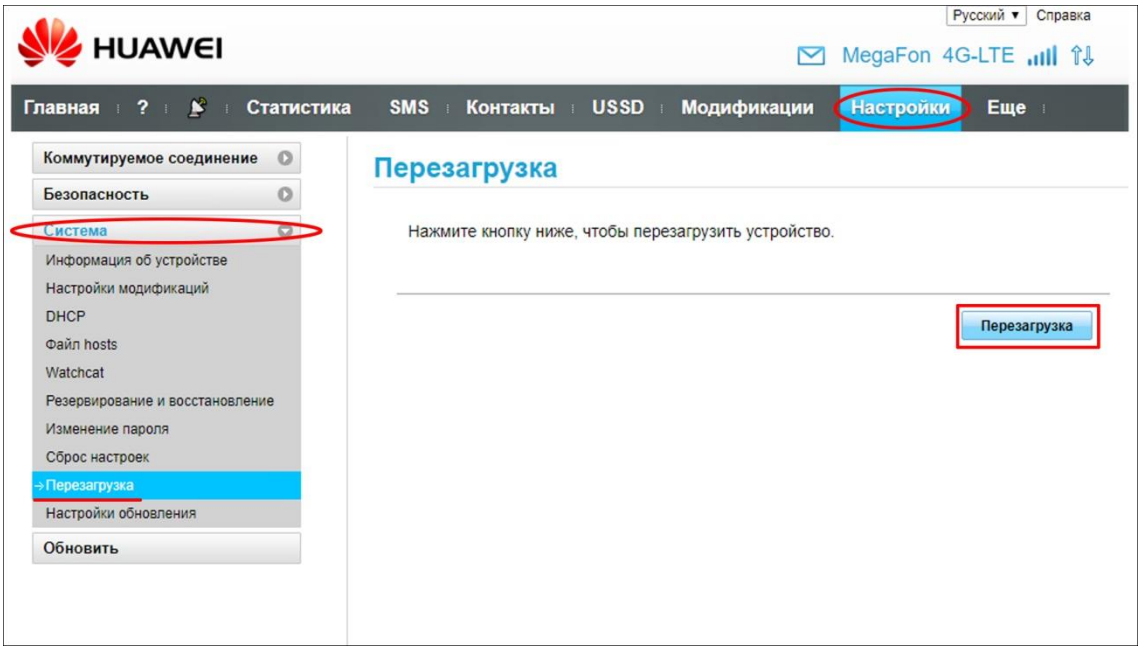


Рисунок А28 – Программная перезагрузка модема

### 4.9. Он-лайн обновление программного обеспечения

Разработчики программного обеспечения постоянно совершенствуют свой продукт, добавляя новые функции, решая проблемы совместимости и исправляя критические уязвимости. Своевременное обновление программного обеспечения модема гарантирует, что вы используете наиболее актуальную версию без ошибок и уязвимостей.

4.9.1. Войдите в меню **Настройки** и выберите вкладку **«Настройки обновления»** в разделе **«Система»** (Рисунок А29).

4.9.2. Произведите настройки обновления. Рекомендуем оставить настройки обновления, установленные по умолчанию. Устройство, выходя в сеть Интернет, отслеживает наличие нового программного обеспечения и, обнаружив новую версию, обновится в автоматическом режиме. Однако рекомендуется отключить автоматическую установку критических обновлений, так как это может повлиять на работу системы модема в целом.

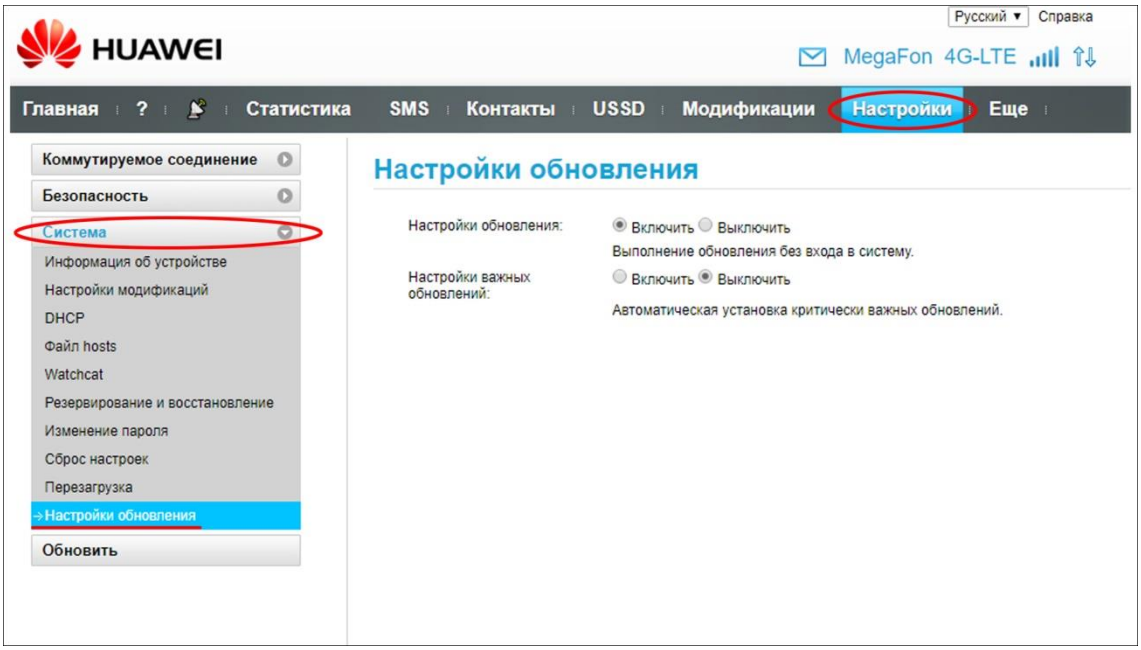


Рисунок А29 – Настройки он-лайн обновления прошивки модема

### 4.10 Локальное обновление модема

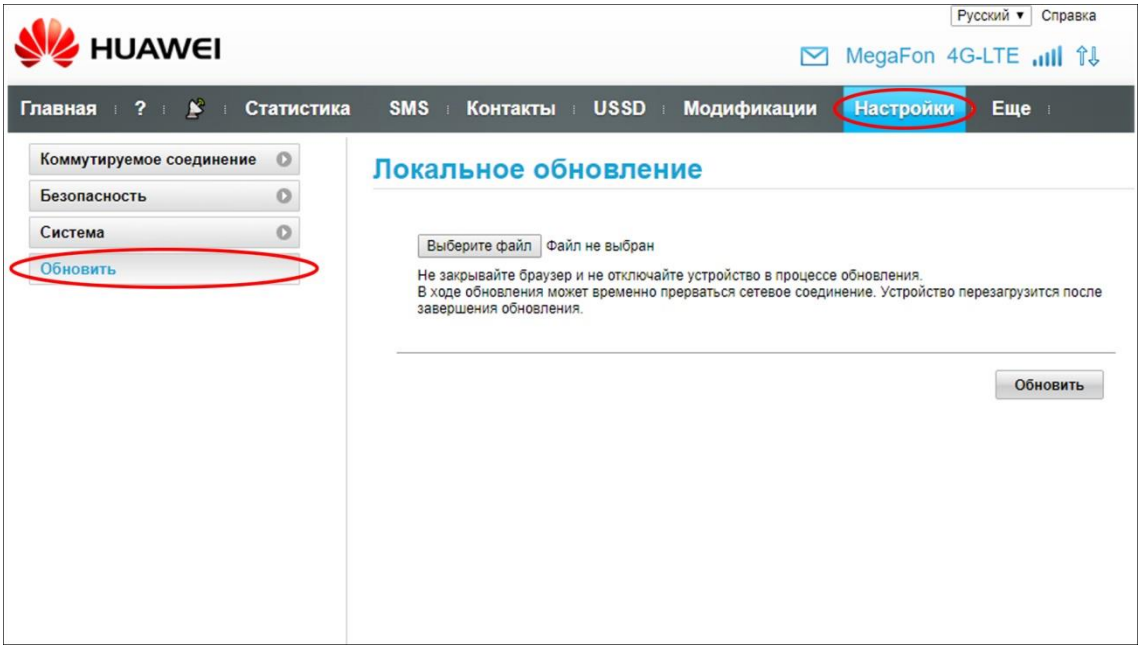


Рисунок А30 – Локальное обновление прошивки модема

Если по каким-то причинам модем не может быть обновлен он-лайн, либо появилось новое обновление, относящееся к критическим, произведите локальное обновление программного обеспечения модема. Настоятельно рекомендуется сохранить резервную копию рабочей версии прошивки согласно п. 4.6. настоящего Приложения.

4.10.1. Выберите раздел **«Обновить»** войдя в меню **Настройки** (Рисунок А30).

4.10.2. Нажмите кнопку **Выберите файл.** Найдите директорию, в которой был сохранен файл обновления и, выделив его, нажмите кнопку Открыть. Рядом с кнопкой **Выберите файл,** появится имя файла с обновлением. Нажмите кнопку **Обновить**, чтобы начался процесс обновления программного обеспечения модема.

**Важно!** Не закрывайте браузер с web-интерфейсом устройства и не отключайте модем в процессе обновления. После завершения обновления модем будет перезагружен.