МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский химико-технологический университет имени Д.И. Менделеева»
(РХТУ им. Д.И. Менделеева)

УТВЕРЖДЕНО
Приказом и.о. ректора
РХТУ им. Д.И. Менделеева
от «15» ноября 2021 № 95 ОД

ПРАВИЛА
пользовании компьютерной сети в РХТУ им. Д.И. Менделеева

Москва
2021 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила использования компьютерной сети (далее – Правила) определяют условия и порядок использования компьютерной сети работниками и обучающимися Федерального государственного бюджетного образовательного учреждения высшего образования «Российский химико-технологический университет имени Д.И. Менделеева» (далее – РХТУ им. Д.И. Менделеева, Университет, ВУЗ).

1.2. Под компьютерной сетью понимается система, обеспечивающая обмен данными между вычислительными устройствами (компьютерами, серверами, маршрутизаторами и другим оборудованием или программным обеспечением).

1.3. Соблюдение настоящих Правил является обязательным для всех работников и обучающихся Университета.

1.4. Использование компьютерной сети, а также проведение работ в области телекоммуникационных технологий и реализация взаимодействия с глобальными информационными ресурсами сети Интернет обеспечивается Центром корпоративной сети передачи данных и телекоммуникаций ДИТ (далее – Центр КСПДиТ).

1.5. Передача обращений в Центр КСПДиТ осуществляется способами, описанными в Приложении 1.

1.6. Руководителям подразделений необходимо согласовывать работы по планированию, разработке и вводу в эксплуатацию телекоммуникаций и локальных компьютерных сетей с руководителем Центра КСПДиТ.

1.7. Центр КСПДиТ обязуется осуществлять заблаговременное уведомление пользователей КС о проводимых технических работах.

2. НОРМАТИВНЫЕ ССЫЛКИ

2.1. Данные Правила основываются на следующих документах:

• Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями);

• Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных";

• Федеральный закон от 29 декабря 2010 г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (с изменениями и дополнениями);

• Федеральный закон от 6 марта 2006 г. № 35-ФЗ "О противодействии терроризму";

• Федеральный закон от 25 июля 2002 г. № 114-ФЗ "О противодействии экстремистской деятельности" (с изменениями и дополнениями);

• Федеральный список экстремистских материалов (http://minjust.ru/extremistmaterials).

3. ТЕРМИНЫ И СОКРАЩЕНИЯ

3.1. В настоящих Правилах используются следующие сокращения, термины и определения:

АРМ	– Автоматизированное рабочее место
ДИТ	– Департамент информационных технологий
КС	– Компьютерная сеть
Сетевая служба	– Программное обеспечение, предоставляющее определенные услуги по обработке информации и/или доступу к ней и взаимодействующее с распределенными клиентскими приложениями через свой внешний интерфейс

Сетевой трафик	– объём информации, передаваемой через компьютерную сеть за определённый период времени
Точка доступа	– Сетевое оборудование, предназначенное для обеспечения беспроводного доступа к компьютерной сети
Файрвол	– программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами
Центр КСПДиТ	– Центр Корпоративных сетей передачи данных и телекоммуникаций

4. ПРАВИЛА РАБОТЫ В КОМПЬЮТЕРНОЙ СЕТИ УНИВЕРСИТЕТА

4.1. Для осуществления подключения АРМ и прочего служебного оборудования к КС пользователю требуется подать заявку в Центр КСПДиТ одним из способов, указанных в Приложении 1.

4.2. Подключение АРМ и прочего служебного оборудования к КС осуществляется сотрудниками ДИТ.

4.3. Подключение личных портативных устройств к КС осуществляется через открытую Wi-Fi сеть “muctr_free”. Процедура подключения описана в Приложении 2 и осуществляется пользователем самостоятельно.

4.4. При работе в КС запрещается:

- Самовольное подключение к КС путем кабельного соединения;
- Организация точек доступа к КС для третьих лиц, а также организация удаленного доступа к АРМ без согласования с ДИТ;
- Установка точек беспроводного доступа к КС без согласования с Центром КСПДиТ;

- Физическое повреждение компонентов КС;
- Установка на рабочем месте сетевых служб без согласования с Центром КСПДиТ;
- Сканирование сети и подбор паролей других пользователей;
- Изменение сетевых атрибутов (в частности IP-адресов, MAC-адресов) и/или идентификационных данных;
- Подмена адреса отправителя при использовании электронной почты;
- Массовая рассылка электронных сообщений (спам);
- Разработка или распространение вредоносного программного обеспечения;
- Проведение сетевых атак;
- Несанкционированный доступ или попытки несанкционированного доступа к информации;
- Использование КС в личных и коммерческих целях;
- Необоснованная производственной необходимостью загрузка сети;
- Распространение информации, запрещенной законодательством РФ;
- Распространение информации, противоречащей нормам морали и нравственности, порочащей честь и достоинство граждан, рассылка обманных или угрожающих сообщений;
- Нарушение авторских прав, модификация, повреждение, удаление не принадлежащих пользователю данных;
- Использование КС в деятельности, противоречащей законодательству РФ.

4.5. Нарушители частично или полностью отстраняются от пользования КС и несут ответственность в соответствии с законодательством РФ и локальными нормативными актами Университета.

4.6. При обнаружении нарушений, проблем или сбоев в сети, а также больших потоков трафика, производится временное отключение пользователя или компонента КС до выяснения и устранения причин.

4.7. В случае необходимости организации больших потоков трафика, во избежание отключения от КС, необходимо предварительное согласование с Центром КСПДиТ.

5. БЕЗОПАСНОСТЬ В КОМПЬЮТЕРНОЙ СЕТИ УНИВЕРСИТЕТА

5.1. Обеспечение информационной безопасности предусматривает комплекс организационных, технических мероприятий, направленных на исключение или существенное затруднение противоправных деяний, злоупотреблений в отношении компонентов КС.

5.2. Политика обеспечения информационной безопасности в КС строится Центром КСПДиТ в соответствии с законодательством РФ и локальными нормативными актами Университета.

5.3. Сетевой трафик пользователей подлежит фильтрации, с целью блокировки доступа к ресурсам, идущим в разрез с локальными нормативными актами и законодательством РФ.

5.4. Фильтрация трафика осуществляется следующими средствами:

- Системой фильтрации со стороны Интернет-провайдера;
- Системой фильтрации трафика ДИТ;
- Встроенным в АРМ сотрудников фаерволом.

5.5. Система фильтрации трафика блокирует доступ пользователя КС Университета к запрещенным ресурсам.

6. ОТВЕТСТВЕННОСТЬ

Пользователи несут ответственность за:

- Нарушение функционирования КС Университета вследствие нарушения правил работы в КС Университета;
- Нарушение законодательства РФ при использовании КС Университета;

- За генерирование, распространение и прием трафика, запрещенного и/или ограниченного законодательством РФ;
- За коммерческое использование КС Университета.

Приложение №1

Способы подачи обращений в КСПДиТ

Взаимодействие с ДИТ по вопросам использования КС Университета осуществляется путем направления обращения одним из следующих способов:

- Посредством корпоративной электронной почты Заявителя на почтовый адрес **support@muctr.ru** в свободной форме, с указанием необходимой информации (ФИО, подразделение, должность, номер телефона, помещение, краткое описание обращения).
- Телефонным звонком на номер **+74992502765**;
- Посредством заполнения формы «Обращение в ДИТ» на официальном сайте Университета;
- Личным обращением в пом. 182 главного корпуса Миусского комплекса;
- В виде служебной записки от имени руководителя структурного подразделения Университета на имя директора ДИТ.

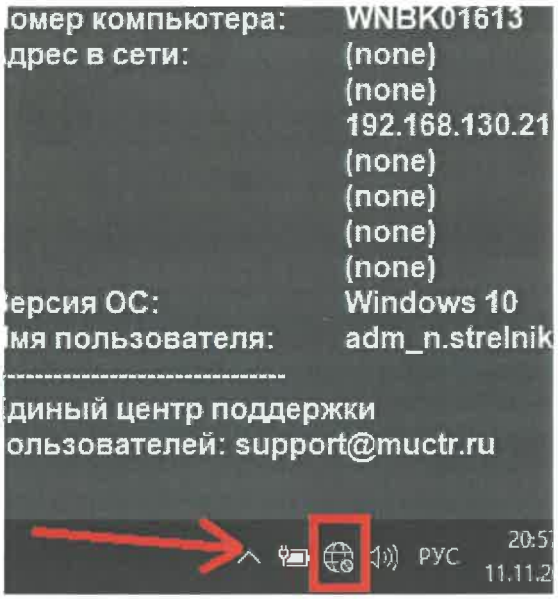
Приложение №2

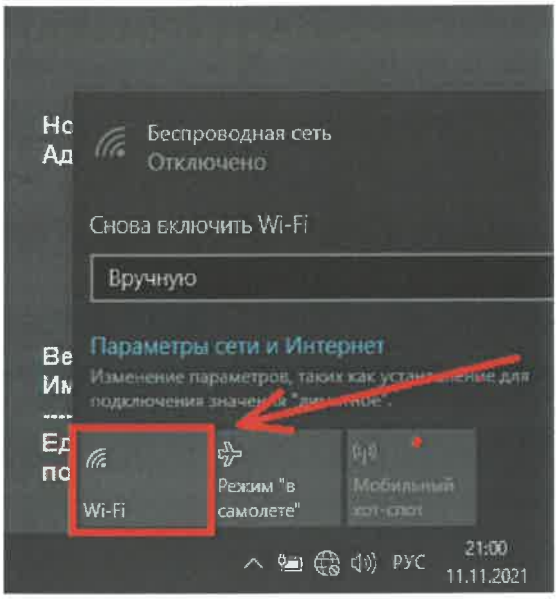
Инструкция подключения личных портативных устройств к компьютерной сети

Подключение личных портативных устройств осуществляется через открытую Wi-Fi сеть “muctr_free”. В ходе подключения требуется пройти процедуру аутентификации через номер мобильного телефона.

Процедура подключения персональных компьютеров:

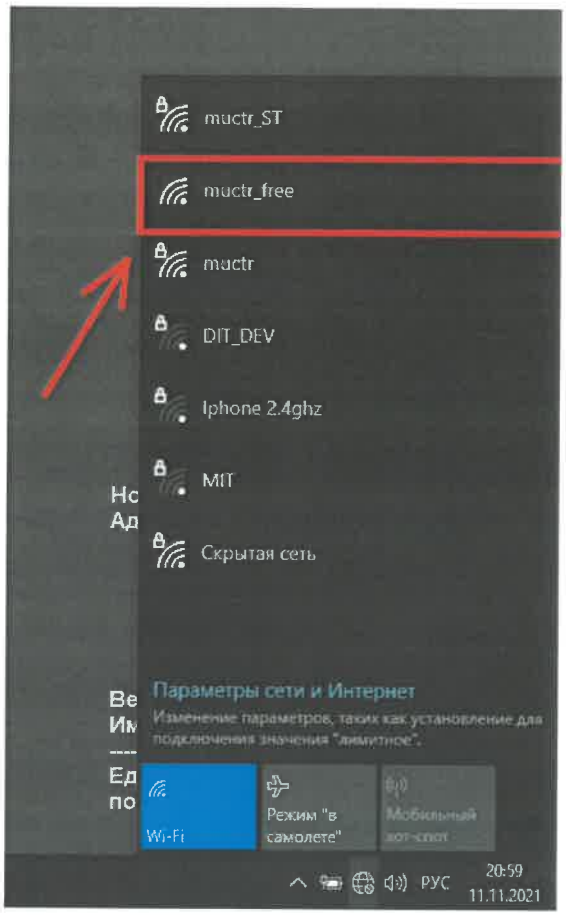
Необходимо открыть меню сетевых подключений и включить Wi-Fi адаптер:

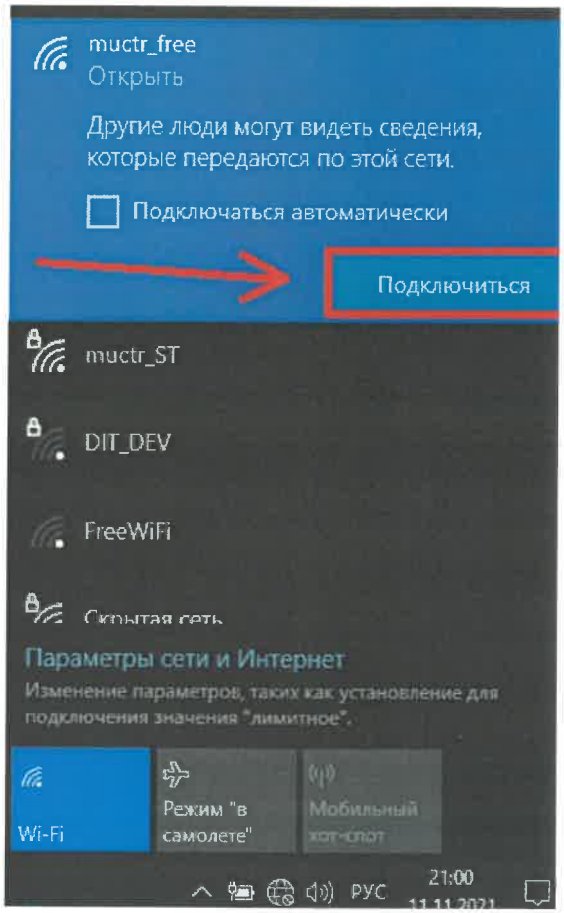




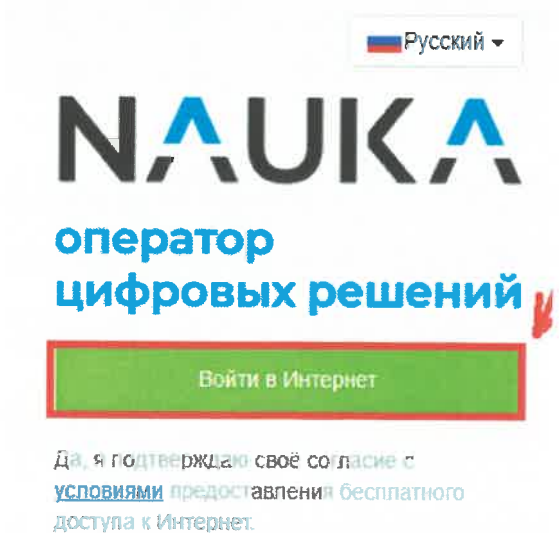
Примечание. В случае, если данный пункт меню отсутствует и/или не является активным, необходимо удостовериться в работе сетевого адаптера устройства или обратиться в службу технической поддержки ДИТ с описанием возникшей проблемы.

Далее необходимо выбрать сеть “muctr_free” из списка доступных и нажать «Подключиться»:



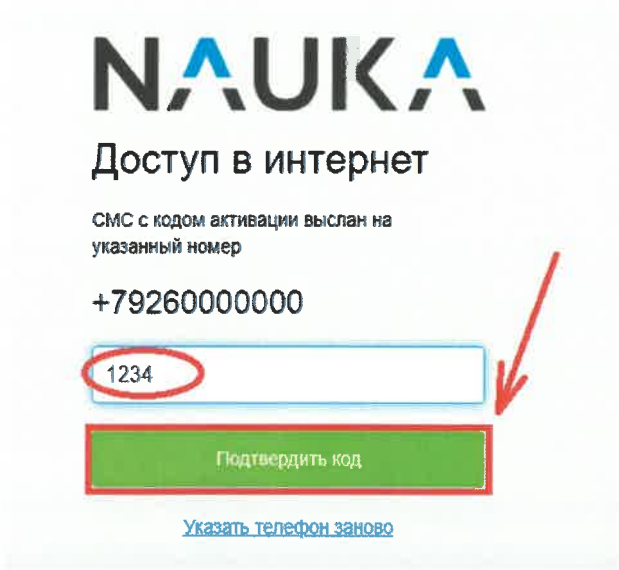


После подключения автоматически откроется странице браузера, на которой необходимо нажать кнопку «Войти В Интернет» и ввести личный номер мобильного телефона и нажать на кнопку «Получить код»:



Примечание: В случае, если номер был введен неверно, необходимо нажать на кнопку «Указать телефон заново»;

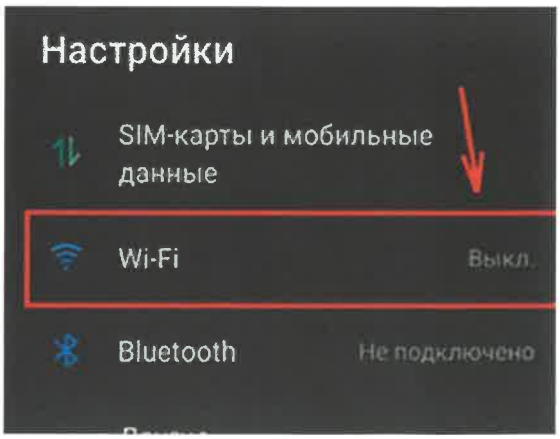
После нажатия на кнопку на указанный телефонный номер придет СМС сообщение с кодом доступа. Необходимо вести код из СМС в соответствующее поле и нажать на кнопку «Подтвердить код», после чего доступ в Интернет будет открыт:

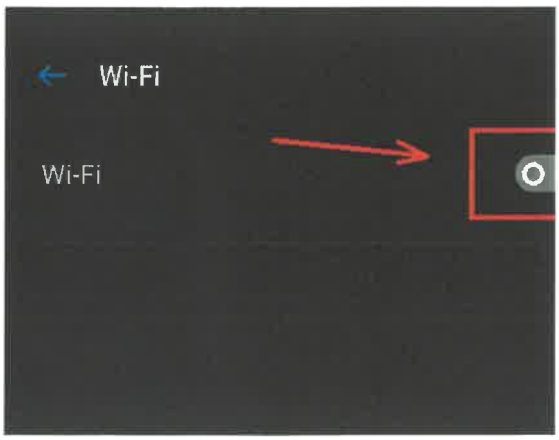


Примечание: В случае возникновения ошибки необходимо нажать на кнопку «Указать телефон заново» и повторить процедуру.

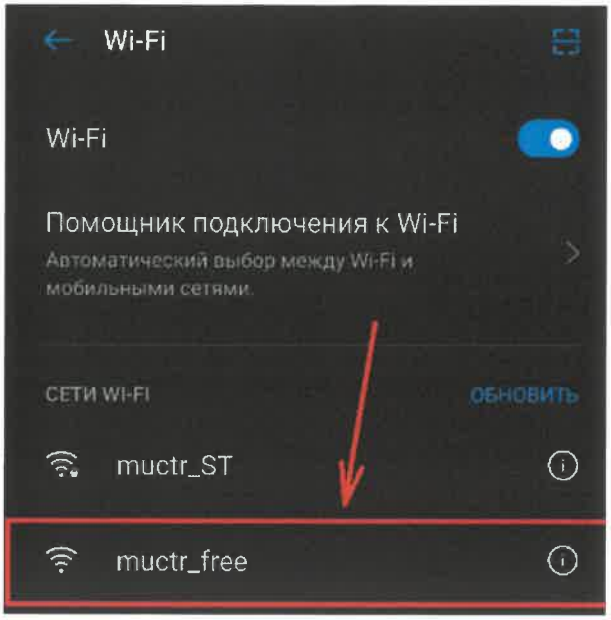
Подключение мобильных устройств к КС:

Необходимо открыть настройки и перейти в меню сетевых подключений, после чего включить Wi-Fi адаптер;

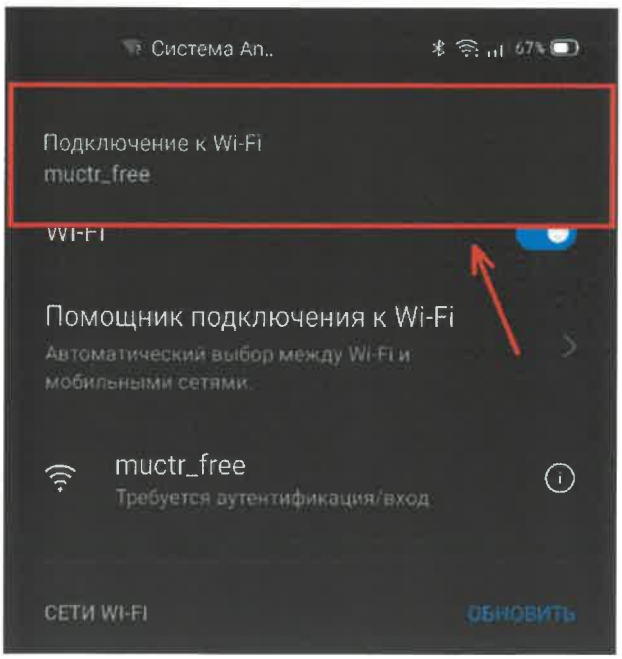




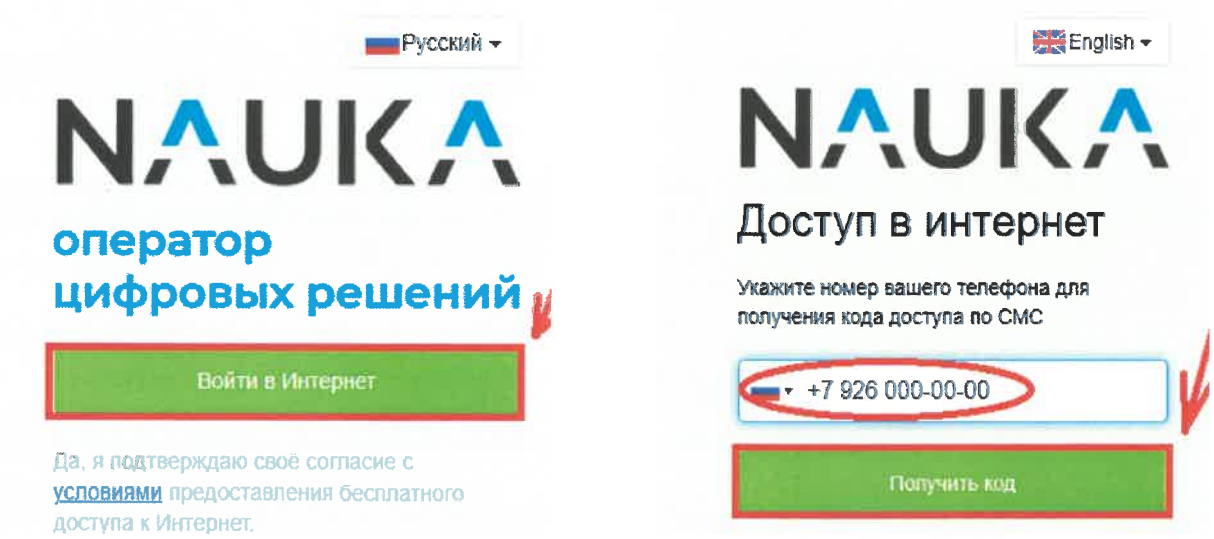
Далее необходимо выбрать сеть “muctr_free” из списка доступных;



После подключения к сети необходимо воспользоваться всплывающим уведомлением или открыть любую страницу в браузере, после чего произойдет перенаправление на страницу аутентификации в сети;

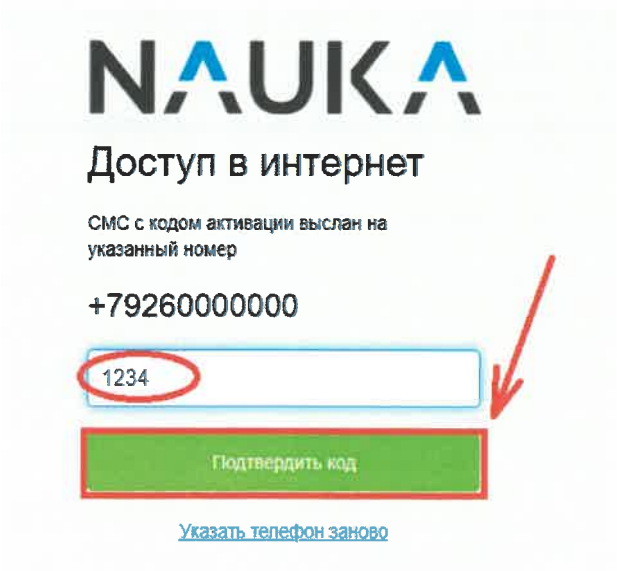


На странице аутентификации необходимо нажать кнопку «Войти В Интернет», ввести личный номер мобильного телефона и нажать на кнопку «Получить код»:



Примечание: В случае, если номер был введен неверно, необходимо нажать на кнопку «Указать телефон заново»;

На указанный телефонный номер придет СМС сообщение с кодом доступа, который необходимо ввести в соответствующее поле и нажать на кнопку «Подтвердить код», после чего доступ в Интернет будет открыт:



Примечание: В случае возникновения ошибки необходимо нажать на кнопку «Указать телефон заново» и повторить процедуру