ЗАО «ПРОМИНФОРМ»

СИСТЕМА ДИСТАНЦИОННОГО УЧАСТИЯ

Руководство пользователя

ИЖВН.425790.001-06.И3.38

2021

Инв. №подл.	Подпись и дата	Взам. инв. №	Инв. №дубл.	Подпись и дата

Формат А4

Первое применение

Справ.№

Подпись и дата

Инв. №дубл.

Взам. инв. №

Подпись и дата

Инв. №подл.

СОДЕРЖАНИЕ

1. ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

1. АПК – аппаратно-программный комплекс;
2. ВКС TrueConf – сервер видеоконференцсвязи TrueConf;
3. ВМ – виртуальная машина;
4. ИСЗ – информационная система зала;
5. Клиент – дистанционный участник заседания;
6. ОС – операционная система;
7. ПО – программное обеспечение;
8. СДУ – система дистанционного участия;
9. СУП – служба управления пультами;
10. СУТ – служба управления терминалами;
11. СЭГ – система электронного голосования.

2. НАЗНАЧЕНИЕ СИСТЕМЫ ДИСТАНЦИОННОГО УЧАСТИЯ

Система дистанционного участия предназначена для работы в составе аппаратно-программного комплекса зала заседаний для обслуживания дистанционных участников заседания (клиентов). В задачи системы входит хранение файлов веб-приложения и обеспечение доступа к этим файлам, управление подключениями клиентов, взаимодействие со службой управления пультами (ядро системы электронного голосования) и обеспечение видеоконференцсвязи для клиентов. Система дистанционного участия состоит из компонентов:

1. служба управления терминалов, функционирующая под управлением ОС Linux;
2. сервер видеоконференцсвязи TrueConf, функционирующий под управлением ОС Windows Server;
3. веб-сервер nginx, функционирующий под управлением ОС Linux;
4. кодек ВКС для СДУ, функционирующий под управлением ОС Windows;
5. приложение дистанционного участника заседания, функционирующее под управлением ОС Windows.

Схема работы СДУ показана на рисунке 1.

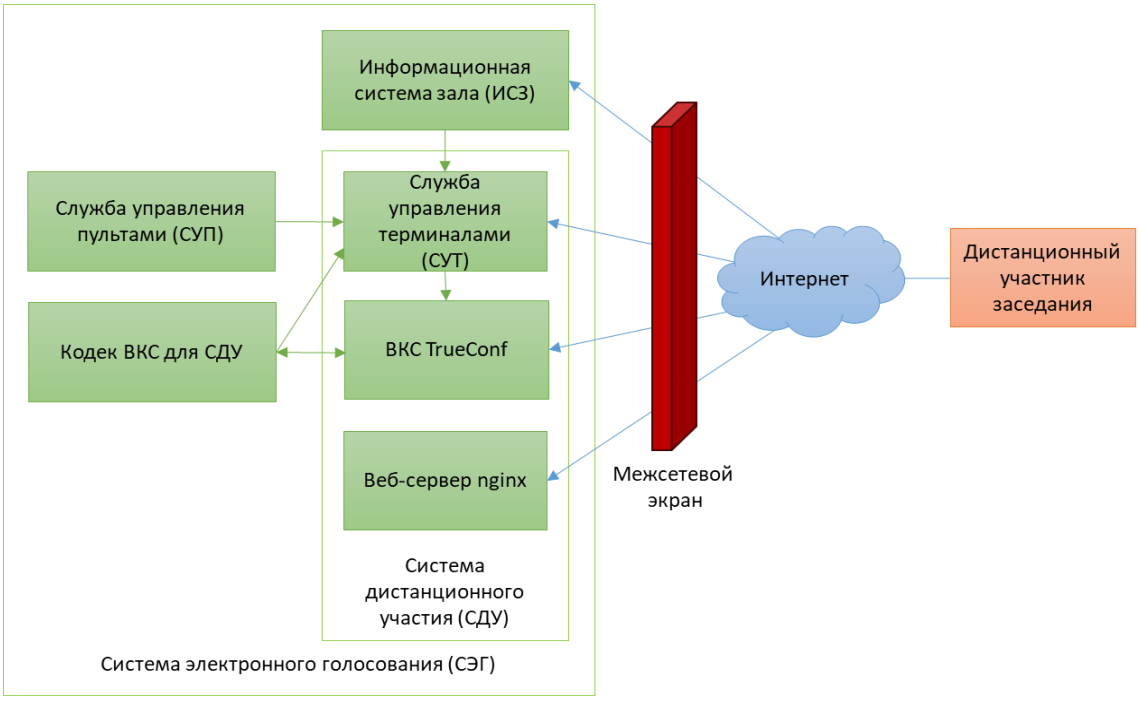


Рисунок 1. Схема взаимодействия основных компонентов системы

3. СОСТАВ СИСТЕМЫ ДИСТАНЦИОННОГО УЧАСТИЯ

В состав ПО входят следующие компоненты:

- служба управления терминалами;
- веб-сервер nginx;
- сервер видеоконференцсвязи TrueConf;
- кодек ВКС для СДУ;
- приложение дистанционного участника заседания.

3.1. Служба управления терминалами

СУТ предназначена для коммуникации с СУП, подключения дистанционных клиентов и приема/передачи информации от них/к ним, управления сервером ВКС TrueConf. СУТ представляет собой исполняемый jar-файл, настраивается СУТ с помощью файлов конфигурации в формате yaml.

Обмен данных между СУТ и СУП происходит с помощью протокола TCP/IP. Инициатор создания подключения – СУП – подключается к порту СУТ 8900. При этом в конкретный момент времени может быть активна только одна сессия СУП-СУТ. Данные, отправляемые между службами, имеют формат JSON. После установления соединения между службами СУП отправляет набор данных: информация о депутатах, текущем режиме, и пр. В дальнейшем происходит обмен данными между СУТ и СУП в рамках текущей работы: изменения режима, подключения пользователей, изменение списков депутатов и пр.

Для поддержания сессии в актуальном состоянии серверы обмениваются служебной информацией – «пинг-понг». В случае разрыва соединения в течение нескольких секунд СУТ будет продолжать работу в штатном режиме, ожидая восстановления соединения со стороны СУП. В случае продолжительного отсутствия нового подключения СУП разорвет все подключения с дистанционными участниками заседания и очистит кэши: справочники депутатов, текущее состояние и пр.

Основная задача СУТ – обеспечение работы дистанционных участников, которые подключаются к СУТ с помощью защищенных веб-сокетов. Аутентификация и авторизация пользователей происходит на основе пары логин/пароль в установленном шифрованном канале связи. Обмен данными между клиентами и СУТ происходит по STOMP-протоколу. Для поддержания сессии в актуальном состоянии так же используется «пинг-понг» между сервером и клиентом. В случае длительного отсутствия связи дистанционный участник заседания будет отключен.

Помимо обмена данными между СУП и клиентами, СУТ управляет сервером TrueConf: при приеме команды включения питания от СУП сервер создает пользователей на сервере ВКС и начинает конференцию. После получения команды выключения питания СУТ удаляет пользователей с сервера TrueConf и завершает конференцию. При получении команд о наличии/отсутствии выступающего СУТ добавляет/удаляет участника конференции на/с трибуны. Для работы с TrueConf серверу необходимо указать учетные данные (секреты): первый секрет необходим для непосредственно управлением сервером (права на все операции), второй – для создания ссылки для автоматического подключения пользователя к ВКС.

Дополнительная возможность СУТ – формирование списка присутствующих на заседании в формате JSON, в котором указаны депутаты и постоянные приглашенные, которые участвуют в заседании как дистанционно, так и непосредственно в зале, а также временные приглашенные, подключенные к конференции TrueConf. На основе результатов данного запроса ИСЗ формирует страницу присутствующих.

3.2. Веб-сервер

Веб-сервер nginx предназначен для хранения файлов веб-приложения дистанционных участников заседания. Веб-приложение состоит из набора файлов (html, js, css и др.) и исполняется на устройстве дистанционного участника заседания.

При запуске приложения дистанционного участника в первую очередь происходит обращение к веб-серверу для получения файлов веб-приложения. После получения статических файлов, приложение запускает полученные скрипты, которые отображают интерфейс пользователя и выполняют подключение к СУТ.

Распространяется nginx свободно в виде дистрибутива.

3.3. Сервер видеоконференцсвязи

Сервер видеоконференцсвязи TrueConf предоставляет возможности видеоконференции дистанционным участникам: передача аудио- и видеоинформации с устройств захвата между клиентами. TrueConf интегрируется в приложение дистанционного участника заседания и управляется с помощью СУТ. Распространяется согласно лицензионному соглашению в виде дистрибутива.

Управление происходит с помощью TrueConf Server API. Реализованы следующие методы по управлению сервером ВКС:

1. получение информации об объектах (конференции, пользователи, группы, выступающие);
2. создание объектов (конференции, пользователи, группы);
3. редактирование объектов (конференции, пользователи, группы);
4. удаление объектов (конференции, пользователи, группы);
5. добавление пользователей на трибуну;
6. удаление пользователей с трибуны;
7. формирование ссылки для автоматического подключения дистанционного участника заседания.

3.4. Кодек ВКС для СДУ

Кодек ВКС для СДУ представляет собой физически выделенную машину с подключенной к ней платой захвата BlackMagic DeckLink MiniRecorder. Предназначен кодек ВКС для СДУ для подключения к конференции ВКС и

передачи полученной информации в систему видеомикширования с помощью вывода сигнала по HDMI/SDI.

Управляется кодек ВКС для СДУ службой управления терминалами: после запуска ОС кодек ВКС для СДУ в автоматическом режиме выполняет попытки подключения к СУТ до тех пор, пока соединение не будет установлено. После установки соединения СУТ отправляет информацию для подключения к конференции: на основании полученных данных кодек ВКС для СДУ запускает клиента TrueConf с опциями командной строки. Запущенный клиент автоматически выполняет подключение к серверу TrueConf и попадает в конференцию. СУТ обеспечивает постоянное нахождение пользователя на трибуне.

В момент запуска кодек ВКС для СДУ считывает по протоколу DHCP-опцию 229, которая имеет формат ip-адреса. Эта опция содержит значение ip-адреса машины, на которой развернута служба управления терминалами.

ОС кодека ВКС для СДУ защищена средствами Windows от записи: все изменения в системе будут удалены после перезагрузки.

3.5. Приложение дистанционного участника заседания

Приложение дистанционного участника заседания предназначено для обеспечения работы депутатов (пользователей) из сети Интернет.

После запуска приложение выполняет подключение к веб-серверу, загружает необходимые файлы веб-приложения и выполняет подключение к серверу управления терминалами.

Работа с ВКС осуществляется с сервером ВКС TrueConf по протоколу WebRTC. Для захвата аудио- и видеоизображения используется камера и микрофон по умолчанию.

Приложение также взаимодействует с ПО LibreOffice для конвертации документов в pdf.

4. ПОДГОТОВКА СДУ К ЗАПУСКУ

Перед запуском компонентов СДУ необходимо выполнить инсталляцию ПО и его конфигурирование. Запуск СДУ выполняется в автоматическом режиме после успешной инсталляции и конфигурирования.

4.1. Подготовка СУТ к запуску

4.1.1. Инсталляция СУТ

Перед инсталляцией сервиса управления терминалами на виртуальной машине с ОС Linux необходимо установить дополнительное ПО: Java 8 (JRE 8u202). Дистрибутив хранится на официальном сайте компании-разработчика Oracle (https://www.oracle.com/java/technologies/javase/javase8-archive-downloads.html) и распространяется свободно.

Установка Java выполняется в командной строке от имени суперпользователя:

```
sudo mkdir -p /usr/java
sudo cp jdk-8u202.tar.gz /usr/java;
cd /usr/java
sudo tar zxvf /usr/java/jdk-8u202.tar.gz;
sudo rm jdk-8u202.tar.gz
sudo update-alternatives –install \
"/usr/bin/java" "java" "/usr/java/jdk1.8.0_202/bin/java" 0;
```

Проверить установку можно с помощью команды:

```
java –version
```

Инсталлируется СУТ копированием файла terminal-manager.jar в каталог /usr/prominform/sut.

```
cp terminal-manager.jar /usr/prominform/sut
```

После копирования исполняемого файла необходимо создать systemd-службу для автоматического запуска ПО, для чего следует создать файл с именем sut.service в каталоге /etc/system/system:

```
sudo touch /etc/system/system/sut.service
```

После чего необходимо создать скрипт в каталоге /usr/prominform/sut с именем run.sh для запуска ПО с содержимым:

```
#!/bin/sh
APP="$(ls | grep .jar)";
java -Dspring.profiles.active=remote -Dfile.encoding=UTF-8 -jar $APP >> /dev/null;
```

Затем следует настроить systemd-службу, заполнив файл /etc/system/system/sut.service:

```
[Unit]
Description=Terminal manager (SUT)
After=syslog.target network.target

[Service]
WorkingDirectory=/usr/prominform/sut
SuccessExitStatus=143
ExecStart=/bin/bash /usr/prominform/sut/run.sh
TimeoutStopSec=10
Restart=on-failure
RestartSec=5

[Install]
WantedBy=multi-user.target
Службу sut.service необходимо включить в автозапуск:
sudo systemctl daemon-reload
sudo systemctl enable sut.service
```

4.1.2. Конфигурирование СУТ

Конфигурация СУТ содержится в файле конфигурации application-remote.yaml, который находится в каталоге /usr/prominform/sut. Параметры конфигурации описаны в приложении А.

После выполненных операций по конфигурированию СУТ необходимо перезапустить службу:

```
sudo systemctl restart sut.service
```

4.2. Подготовка ВКС к запуску

4.2.1. Инсталляция ВКС

На выделенную виртуальную машину с ОС Windows Server необходимо установить дистрибутив TrueConf Server версии 4.7.3, дистрибутив находится на официальном сайте TrueConf (https://trueconf.ru/products/server/server-videokonferenciy.html).

Подробная инструкция по установке содержится в руководстве администратора TrueConf Server'а, которое также находится на официальном сайте TrueConf (https://docs.trueconf.com/manual/server/trueconf-administrator-ru.pdf).

4.2.2. Конфигурирование ВКС

После инсталляции необходимо активировать и зарегистрировать ПО. Инструкции по регистрации и конфигурированию содержится в руководстве администратора TrueConf Server, которое находится на официальном сайте TrueConf (https://docs.trueconf.com/manual/server/trueconf-administrator-ru.pdf).

4.3. Подготовка веб-сервера к запуску

4.3.1. Инсталляция веб-сервера

На ВМ с ОС Linux необходимо установить дистрибутив сервера nginx. Установка осуществляется из официального репозитория linux с помощью терминала командой:

```
sudo apt install nginx
```

Архив с веб-приложением (terminal-frontend.zip) необходимо распаковать и разместить в каталоге /usr/prominform.

Службу nginx необходимо включить в автозапуск:

```
sudo systemctl enable nginx.service
```

4.3.2. Конфигурирование веб-сервера

После инсталляции в файле конфигурации виртуального веб-сервера nginx (/etc/nginx/sites-available/default) необходимо указать порт для работы веб-приложения (секция server):

```
listen 9443 default_server;
listen [::]:9443 default_server;
```

Необходимо активировать ssl-шифрование (процедура установки и обновления ключей описана в приложении Б), секция server:

```
ssl on;
ssl_certificate /usr/prominform/public.crt;
ssl_certificate_key /usr/prominform/private.pkcs8;
ssl_prefer_server_ciphers on;
```

И указать путь к веб-приложению (секция server):

```
root /usr/prominform/terminal-frontend;
```

После выполненных операций необходимо перезапустить службу nginx:

```
sudo systemctl restart nginx.service
```

4.4. Подготовка кодека ВКС для СДУ к запуску

4.4.1. Инсталляция кодека ВКС для СДУ

Перед инсталляцией на машине с ОС Windows необходимо установить дополнительное ПО:

1. Java 8 (JRE 8u202). Дистрибутив хранится на официальном сайте компании-разработчика Oracle (https://www.oracle.com/java/technologies/javase/javase8-archive-downloads.html) и распространяется свободно.
2. TrueConf 7. Дистрибутив хранится на официальном сайте компании-разработчика (https://trueconf.ru/downloads/windows.html) и является свободно распространяемым.

Распространяемый исполняемый файл vcs-grabber.jar необходимо разместить в каталоге C:\grabber, после чего в ветке реестра

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon изменить значение опции Shell на:

```
javaw –jar C:\garbber\vcs-grabber.jar
```

После того, как инсталляция успешно выполнена, необходимо убедиться, что DHCP-опция 229 установлена и имеет формат ip-адреса.

Последним шагом в командной строке от имени администратора необходимо активировать фильтр для защиты от записи:

```
uwfmgr filter enable
```

После чего выполнить перезагрузку системы.

4.4.2. Конфигурирование кодека ВКС для СДУ

Конфигурирование кодека ВКС для СДУ подразумевает под собой настройку TrueConf. Для этого необходимо деактивировать фильтр защиты от записи и выполнить перезагрузку системы:

```
uwfmgr filter disable
```

В настройках клиента TrueConf в графическом интерфейсе необходимо выполнить следующие операции:

1. выключить автоматический запуск приложения;
2. выключить автоматическую авторизацию;
3. убрать режим уведомлений;
4. выключить сворачивание в трей при закрытии;
5. отключить зеркальное изображение;
6. включить повышенную частоту кадров.

После выполненных операций необходимо активировать фильтр и выполнить перезапуск ОС.

4.5. Подготовка приложения дистанционного участия к запуску

4.5.1. Инсталляция приложения

Инсталляция приложения дистанционного участия осуществляется с помощью поставляемого инсталлятора для ОС Windows: файл «АРМ Участник

заседания.exe». Чтобы начать инсталляцию необходимо запустить файл установщика и далее идти по предлагаемому установщиком сценарию.

1. Выбрать язык установки – «Русский». Нажать кнопку «Ок».
2. Ознакомиться с намерением установщика создать ярлык и нажать кнопку «Далее».
3. Нажать кнопку «Установить».
4. Дождаться окончания распаковки файлов установщиком.
5. Далее отобразится начало установки компонента Java 8 (JRE 8u202). Нажать кнопку «Install».
6. Дождаться окончания инсталляции компонента. Нажать «Close».
7. Далее отобразится начало установки компонента LibreOffice 7.0.6.2. Нажать «Далее». Согласиться с установкой в каталог по умолчанию.
8. Дождаться окончания инсталляции компонента. Нажать «Готово».
9. Нажать «Завершить» в основном окне установки приложения «Рабочее место дистанционного участника заседания».

Описанный алгоритм является верным и точным для ситуации, когда не установлен ни один из компонентов, поставляемых совместно с нашим приложением или аналогов этих компонентов. В иных случаях шаги алгоритма могут отличаться в зависимости от данных, поступающих на вход инсталлятору от операционной системы.

4.5.2. Конфигурирование приложения

Конфигурирование приложения не требуется. Пользователь может воспользоваться ярлыком на рабочем столе, запустить приложение и удостовериться в его работоспособности.

5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СДУ

Безопасность коммуникации между компонентами основана на использовании шифрования (протокол HTTPS, TLS-шифрование). Все компоненты СДУ находятся за межсетевым экраном, который обеспечивает необходимый уровень защиты, фильтруя запросы извне.

Дистанционные участники заседания подключаются к серверам-компонентам СДУ также с использованием безопасных протоколов. Все каналы обмена данных являются шифрованными. Дополнительно при этом подключиться к серверу СУТ могут только доверенные клиенты: клиенты, запросы которых поступают с веб-сервера СДУ.

Общая схема защищенного взаимодействия изображена на рис. 2.

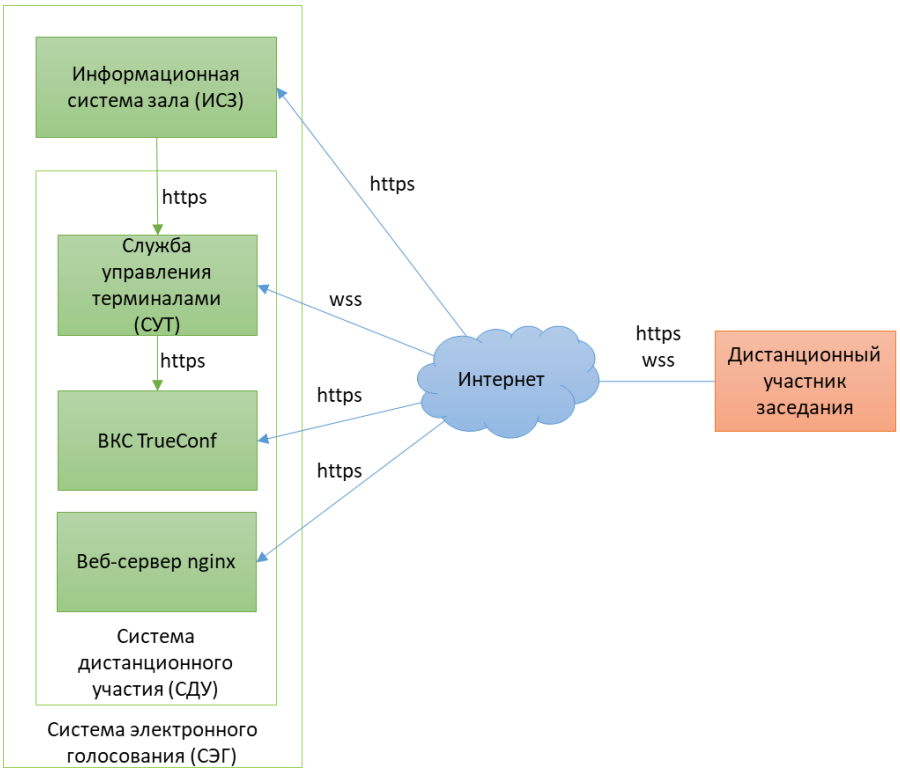


Рисунок 2. Протоколы защищенного взаимодействия СДУ

Запросы, выполняемые к СУТ по http/https требуют аутентификации и авторизации с помощью JWT – json вебтокена, который генерируется на основе закрытого ключа, входящего в конфигурацию СУТ.

Канал связи между дистанционным участником и СУТ является авторизованным после создания подключения в случае успешной аутентификации, иначе канал закрывается со стороны СУТ.

6. СОСТАВ ПО ЭКСПОРТА

В состав ПО входят следующие наборы файлов: terminal-manager.jar, terminal-frontend.zip, vcs-grabber.jar, «АРМ Участник заседания.exe».

6.1. Назначение файлов

1. terminal-manager.jar – исполняемый модуль СУТ;
2. terminal-frontend.zip – архив с файлами веб-приложения;
3. vcs-grabber.jar – исполняемый модуль кодека ВКС;
4. АРМ Участник заседания.exe – инсталлятор приложения дистанционного участника заседания.

ПРИЛОЖЕНИЕ А. ОПИСАНИЕ КОНФИГУРАЦИИ СУТ

Для корректной работы службы управления терминалами до старта службы необходимо корректно заполнить файл конфигурации. Описание параметров конфигурации, которые необходимо настроить, приведено в таблице ниже.

№ п/п	Название опции (полный путь)	Описание
1.	app.jwt-vis.key-store	Путь к ключевому контейнеру, содержащему ключевую пару для проверки валидности токена в запросах к серверу
2.	app.jwt-vis.key-alias	Имя ключевой пары для проверки валидности токена в запросах к серверу в ключевом контейнере
3.	app.jwt-vis.key-store-password	Пароль для ключевой пары для проверки валидности токена в запросах к серверу в ключевом контейнере
4.	server.ssl.key-store	Путь к ключевому контейнеру, содержащему ключевую пару для создания безопасного соединения с клиентом
5.	server.ssl.key-alias	Имя ключевой пары для создания безопасного соединения с клиентом в ключевом контейнере
6.	server.ssl.key-store-password	Пароль для ключевой пары для создания безопасного соединения с клиентом в ключевом контейнере
7.	app.vs-grabber.login	Логин для подключения ПО граббера (кодека ВКС)

8.	app.vs-grabber.password	Пароль для подключения ПО граббера (кодека ВКС)
9.	app.vis.postfix	Порт для подключения к ИСЗ через сеть Интернет для дистанционных участников заседания
10.	app.trueconf.internal-host	Путь к TrueConf для подключения из локальной сети
11.	app.trueconf.external-host	Путь к TrueConf для подключения из сети Интернет
12.	app.trueconf.server-id	Server-id для приложения (в терминах TrueConf) для управления сервером TrueConf
13.	app.trueconf.server-secret	Client-id для приложения (в терминах TrueConf) для управления сервером TrueConf
14.	app.trueconf.client-id	Server-id для приложения (в терминах TrueConf) для создания ссылки для подключения клиента
15.	app.trueconf.client-secret	Client-id для приложения (в терминах TrueConf) для создания ссылки для подключения клиента
16.	app.trueconf.conference-name	Имя конференции TrueConf
17.	app.trueconf.conf-owner.login-name	Логин владельца конференции TrueConf
18.	app.trueconf.conf-owner.visible-name	Отображаемое имя владельца конференции TrueConf
19.	app.trueconf.conf-owner.password	Пароль владельца конференции TrueConf

20.	app.trueconf.conf-hall.login-name	Логин постоянного выступающего (зал заседаний) TrueConf
21.	app.trueconf.conf-hall.visible-name	Отображаемое имя постоянного выступающего (зал заседаний) TrueConf
22.	app.trueconf.conf-hall.password	Пароль постоянного выступающего (зал заседаний) TrueConf
23.	app.trueconf.max-podiums	Максимальное количество выступающих в конференции TrueConf

ПРИЛОЖЕНИЕ Б. ПРОЦЕДУРА ОБНОВЛЕНИЯ SSL-КЛЮЧЕЙ

Для корректной работы всех компонентов системы необходимо установить SSL-ключи в каждый из компонентов системы. SSL-ключи представляют собой ключевой контейнер, который содержит пару закрытый-открытый ключи, а также закрытый ключ в виде отдельного файла и публичный ключ в виде сертификата.

Заранее необходимо получить сертификат в удостоверяющем центре. Рекомендуется получать SSL Сертификат с поддержкой субдоменов (WildCard SSL Certificates).

Один и тот же ключевой контейнер (в формате PKCS12) используется для СУТ (локальный и удаленный) и ИСЗ. Публичный ключ (сертификат) и приватный ключ используются также в nginx (внешний контур).

Для создания ключевого контейнера рекомендуется использовать утилиту KeyStore Explorer 5.4 (консольные альтернативы: keytools — входит в состав java, openssl).

В ключевом контейнере должны находиться две ключевых пары:

- ключевая пара (основная) для СУТов и nginx – сертификат должен быть подписан доверенным УЦ;
- ключевая пара для коммуникации между СУТ и ИСЗ — простая сгенерированная ключевая пара, подтверждать УЦ не требуется.

Описание ключей и пути их размещения

Компонент АПК	Заменяемые файлы

Локальный СУТ
Имя ВМ: nginx
	Ключевой контейнер (p12-файл).
	Внести изменения в файл /usr/prominform/sut/application-local.yaml
	`jwt-vis:`
	`  key-store-type: PKCS12`
	`  key-store: "/usr/prominform/sut/keystore.p12"`
	`  key-alias: jwtkey_wildfly`
	`  key-store-password: pinform`

Внешний СУТ
Имя ВМ: remote
	Ключевой контейнер (p12-файл).
	Внести изменения в файл /usr/prominform/sut/application-remote.yaml
	`jwt-vis:`
	`  key-store-type: PKCS12`
	`  key-store: "/usr/prominform/sut/keystore.p12"`
	`  key-alias: jwtkey_wildfly`
	`  key-store-password: pinform`
	`server:`
	`  port: 8443`
	`  ssl:`
	`  enabled: true`
	`  key-store-type: PKCS12`
	`  key-store: "/usr/prominform/sut/keystore.p12"`
	`  key-alias: '*.gorodperm.ru'`
	`  key-store-password: pinform`

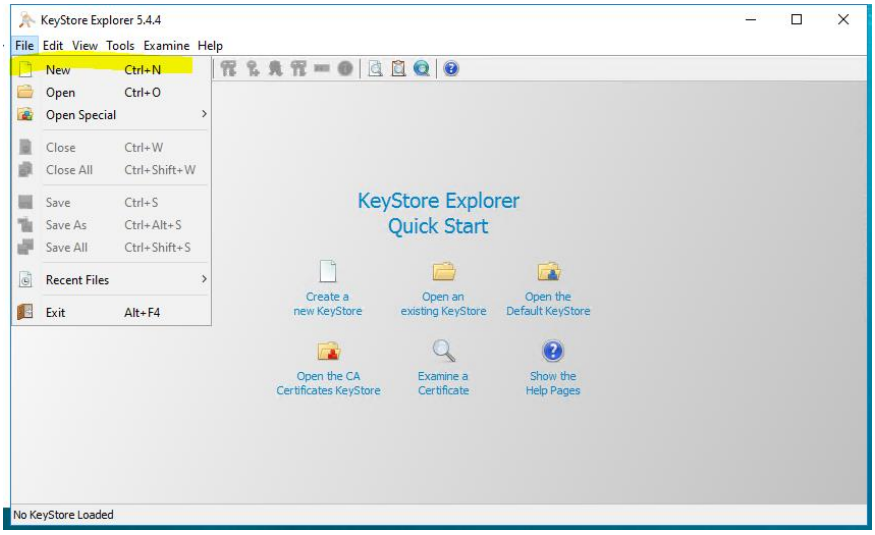
Внешний nginx
Имя ВМ: nginx
	Публичный и приватный ключи.
	Внести изменения в файл /etc/nginx/sites-available/default
	`ssl on;`
	`ssl_certificate /usr/prominform/public.crt;`
	`ssl_certificate_key /usr/prominform/private.pkcs8;`
	`ssl_prefer_server_ciphers on;`

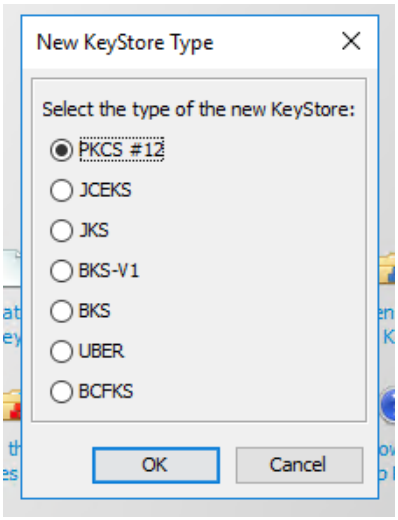
ИСЗ
Имя ВМ: information
	Ключевой контейнер (p12-файл).
	Внести изменения в файл /opt/wildfly/standalone/configuration/nvis-wf10-standalone.xml
	`<system-properties>`
	`  <property name="storage.path" value="/media-server/media/"/>`
	`  <property name="oneAE" value=""/>`
	`  <property name="altVoteResCount" value="3"/>`
	`  <property name="keystore.name" value="perm.p12"/>`
	`  <property name="keystore.password" value="pinform"/>`
	`  <property name="keystore.webserver.alias" value="*.gorodperm.ru"/>`
	`  <property name="keystore.jwt.alias" value="jwtkey_wildfly"/>`

Сервер TrueConf Имя ВМ: trueconf	Публичный и приватный ключи заменяются в веб-интерфейсе администратора, вкладка Веб — HTTPS

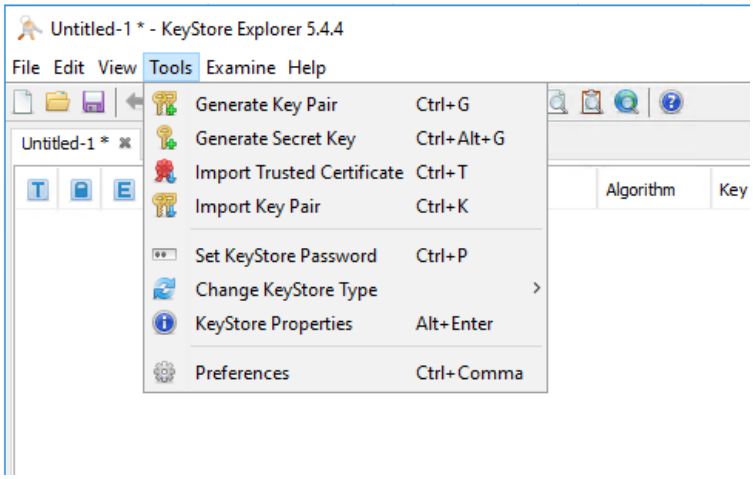
Импорт ключей (приватного и публичного) в ключевой контейнер

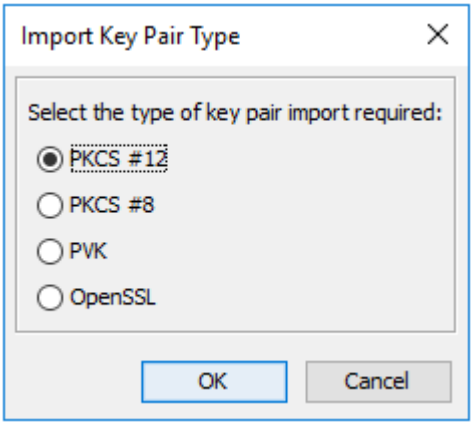
1. Создайте ключевой контейнер (File – New), формат PKCS #12



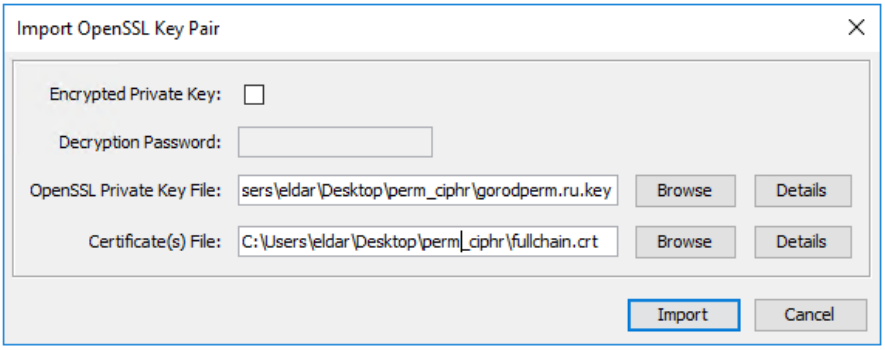


2. Выберите опцию импорта (Tools – Import Key Pair), выберите формат ключевой пары. Как правило, это PKCS #8 или OpenSSL (зависит от поставщика услуг).

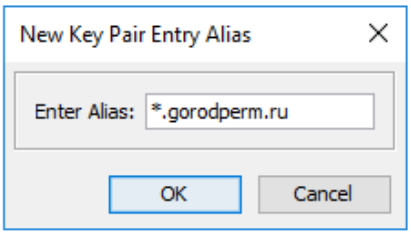




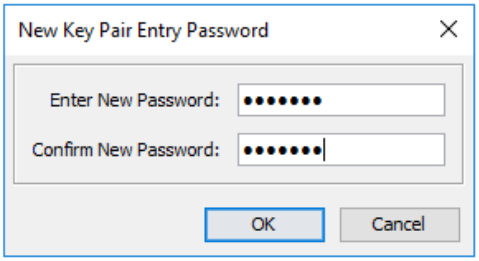
При импорте ключей необходимо выключить опцию дешифрования приватного ключа (Encrypted Private Key), если поставщик услуг не сообщил об обратном. Пример импорта для ключевой пары, сгенерированной с помощью OpenSSL:



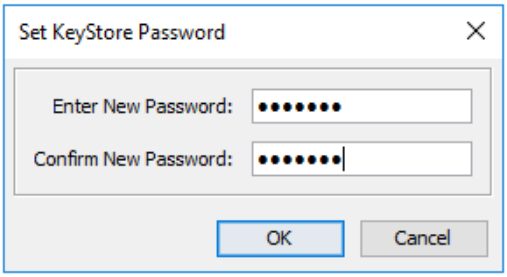
3. Имя алиаса (ключевой пары) не должно содержать пробелов, рекомендуется называть его по wildcard, например:



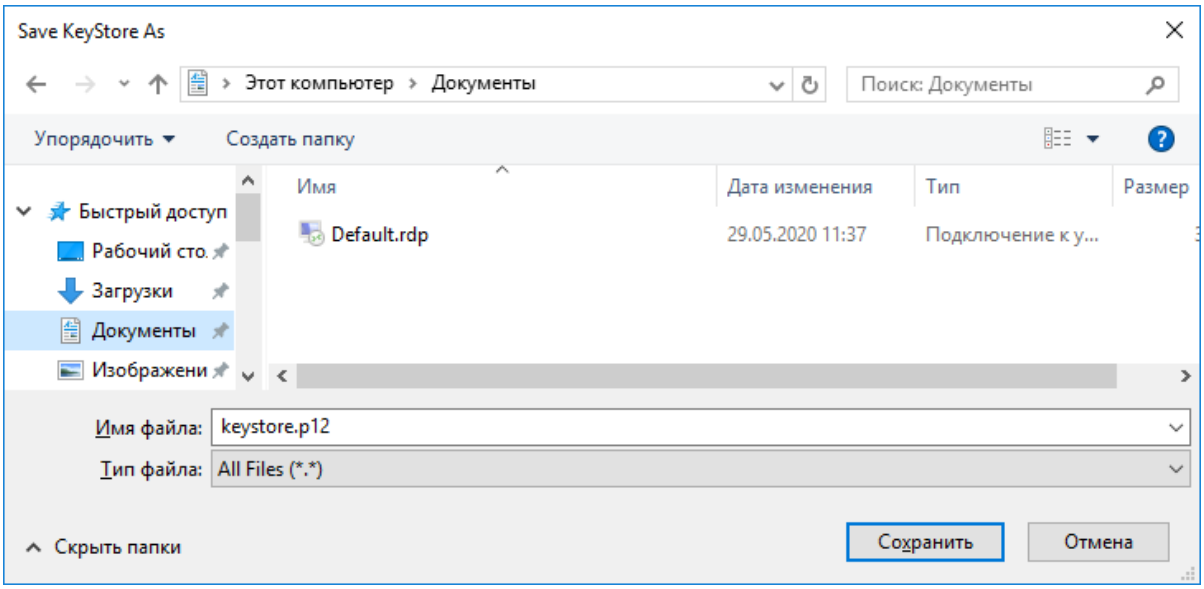
4. После необходимо задать пароль алиаса (как правило, в конфигурации используется pinform)



5. При сохранении ключевого контейнера (File – Save) рекомендуется ввести тот же пароль, что был введен не предыдущем шаге:



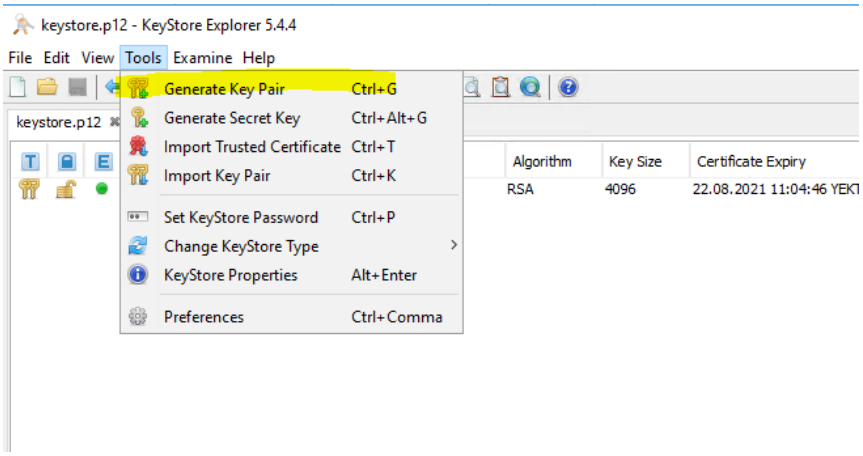
И сохранить контейнер на диск (расширение файла выбрать p12):

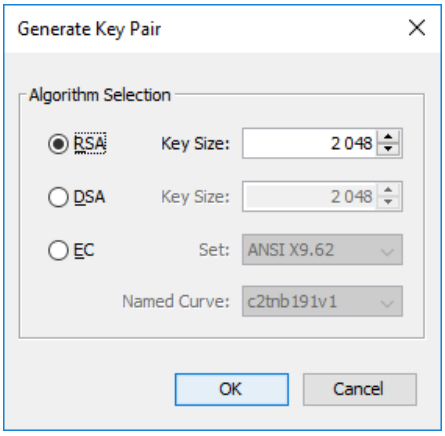


Для обновления ключей в АПК необходимо также создать ключевую пару для ИСЗ (см. ниже).

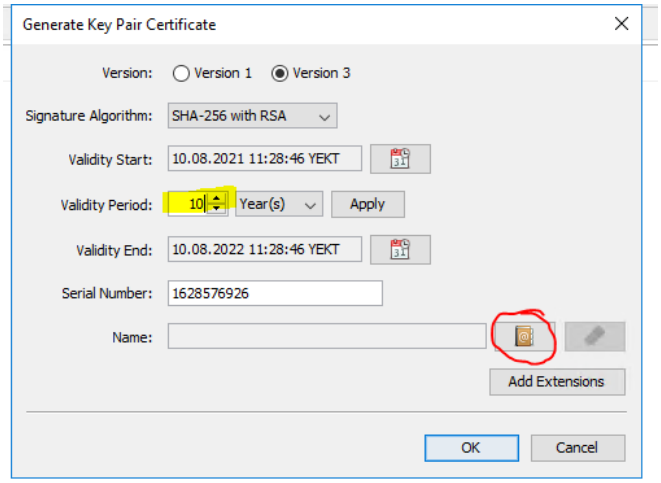
Генерация ключевой пары в ключевом контейнере (ИСЗ)

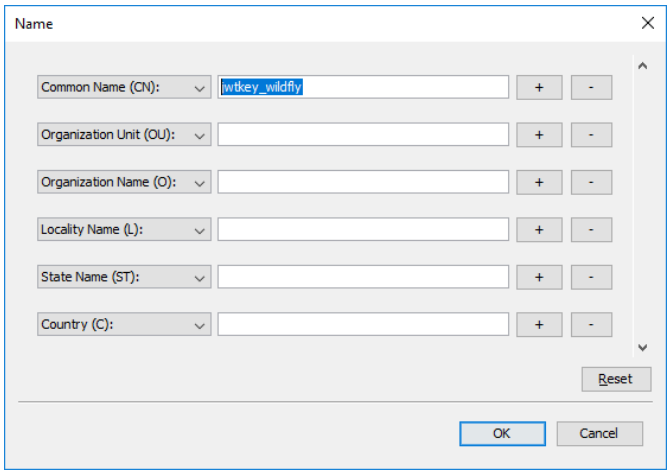
1. В уже созданном контейнере необходимо выбрать функцию создания новой ключевой пары (Tools – Generate Key Pair), алгоритм RSA, длина ключа 2048 бит:



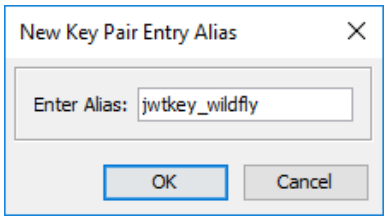


2. Срок действия ключа должен быть установлен с таким же сроком, что и ключ, полученный от поставщика (можно поставить заведомо больший период — 10 лет). В этом же окне необходимо заполнить поле CN со значением jwtkey_wildfly:

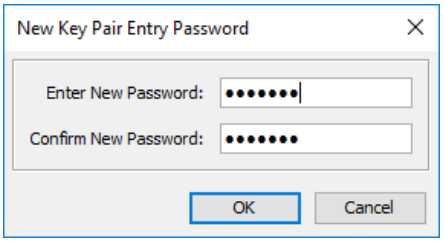




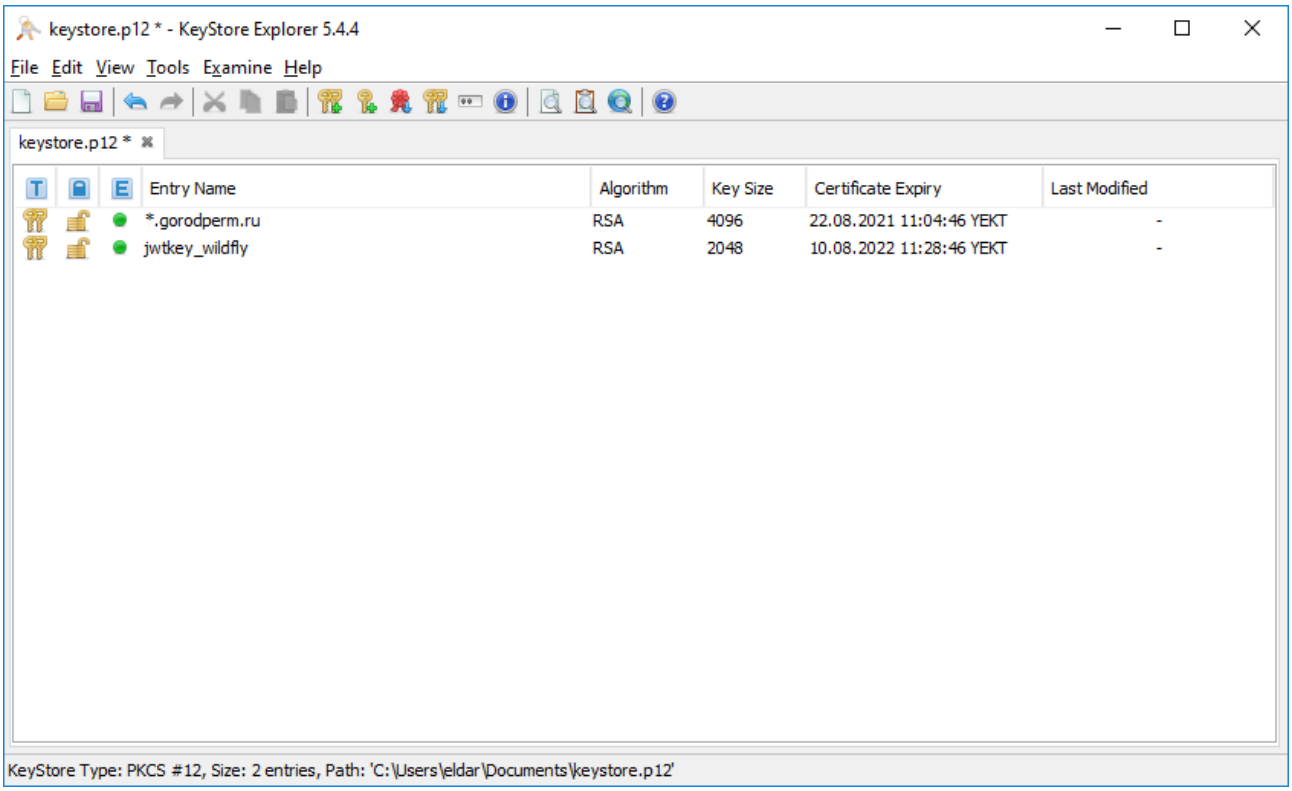
3. Имя алиаса оставить как есть (заполненное автоматически jwtkey_wildfly):



4. Пароль установить такой же, как и для первого ключевого контейнера (pinform):



Результат:



Полученный контейнер необходимо сохранить: он готов для размещения на площадке.

Инструкция

по работе в дистанционном режиме
с использованием устройств дистанционного
участия в заседаниях

После включения ноутбука дождитесь загрузки операционной системы

Для работы в дистанционном режиме необходимо подключиться к сети интернет

ПЕРМСКАЯ
ГОРОДСКАЯ
ДУМА

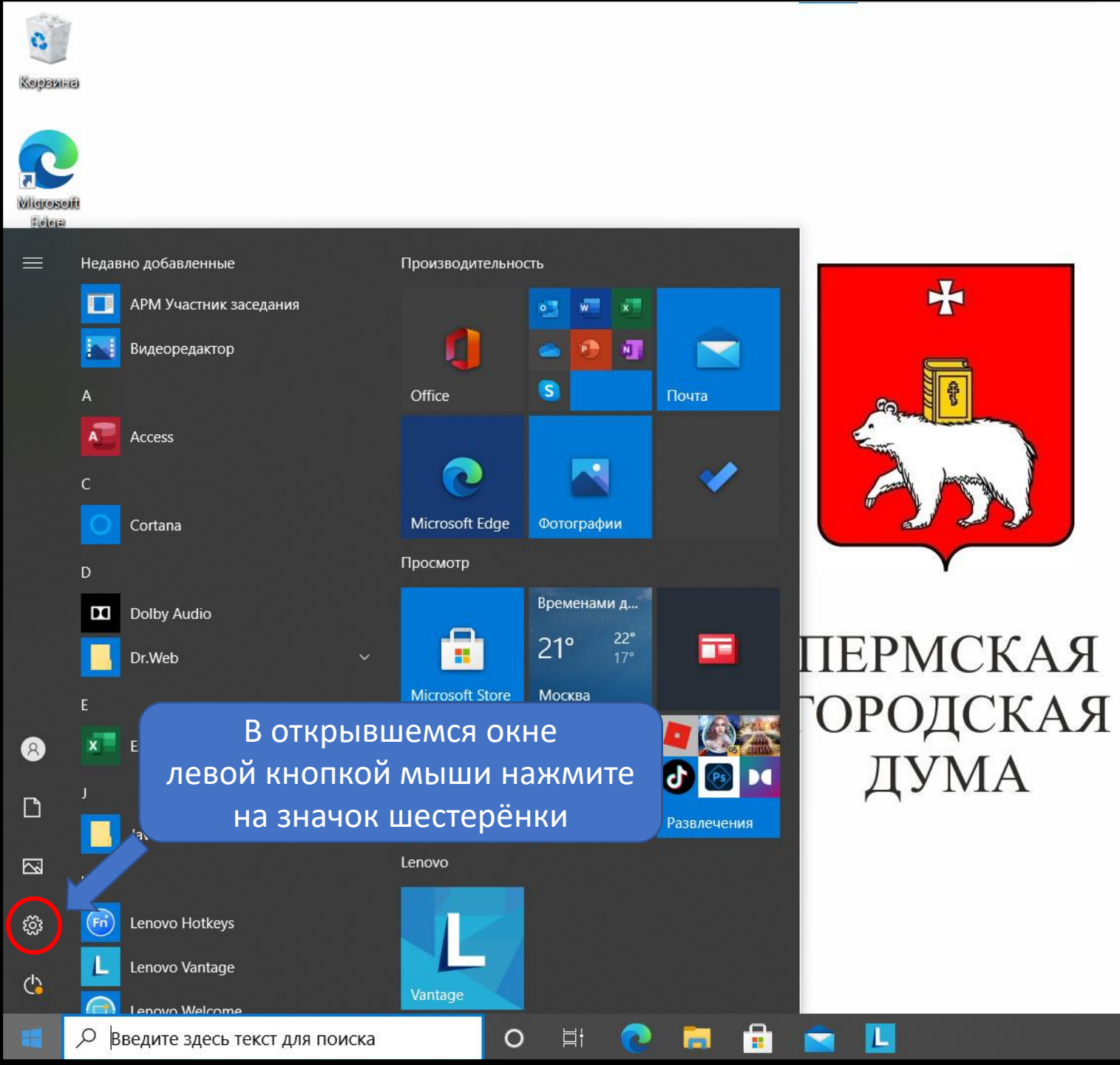
Подключение к сети интернет

Вариант 1.

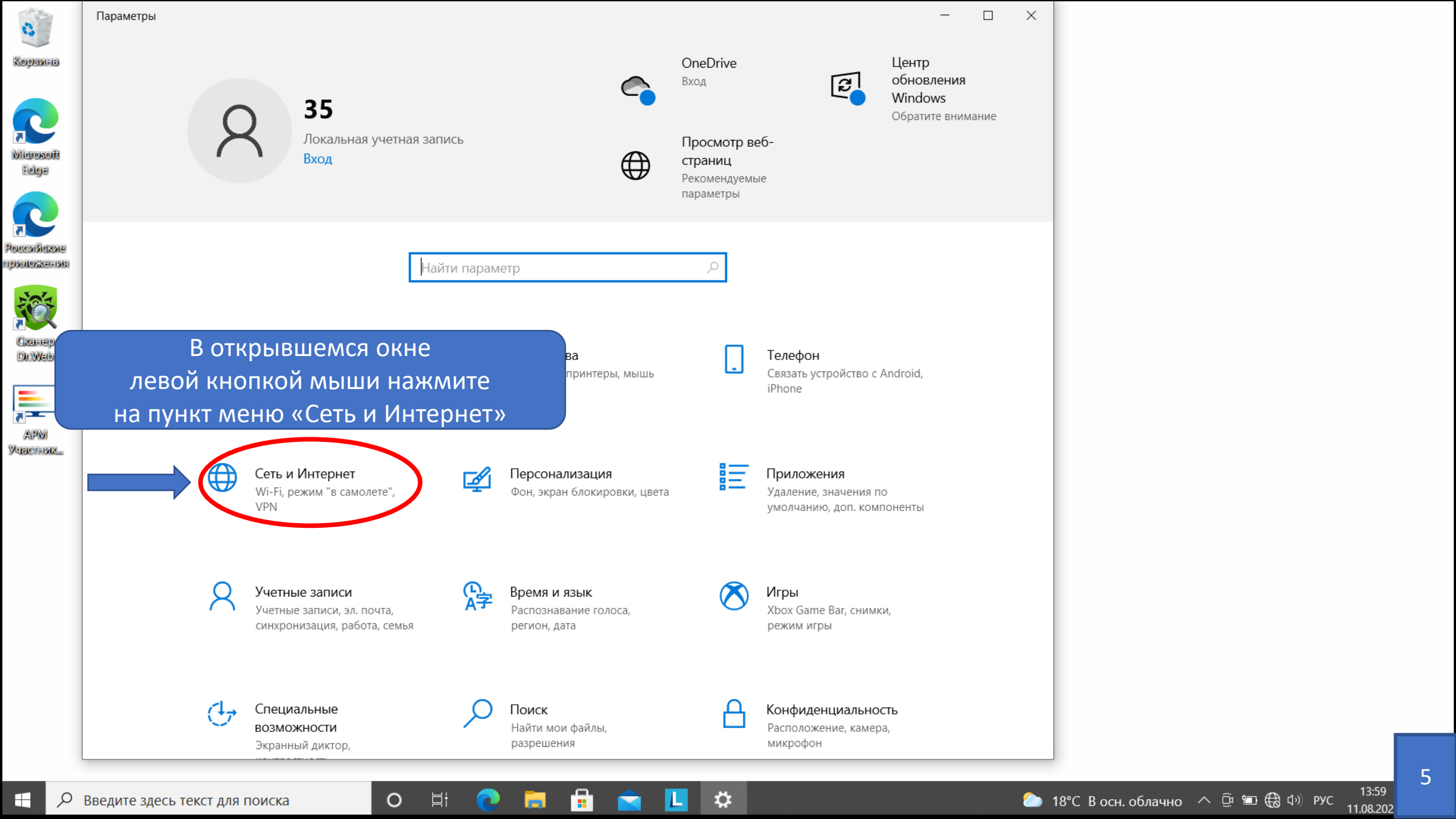
Подключение к сети интернет по проводному каналу

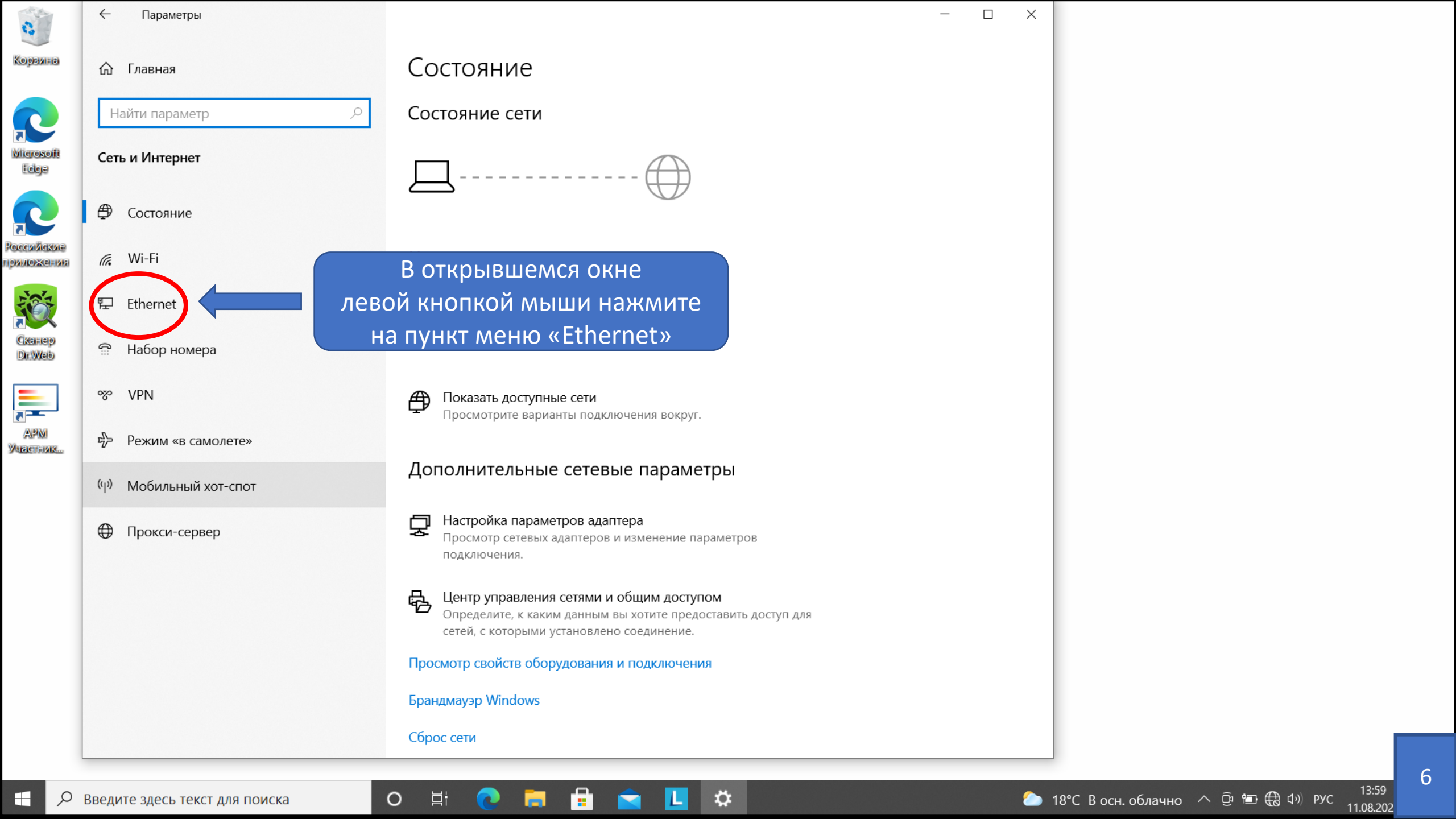
ПЕРМСКАЯ ГОРОДСКАЯ ДУМА

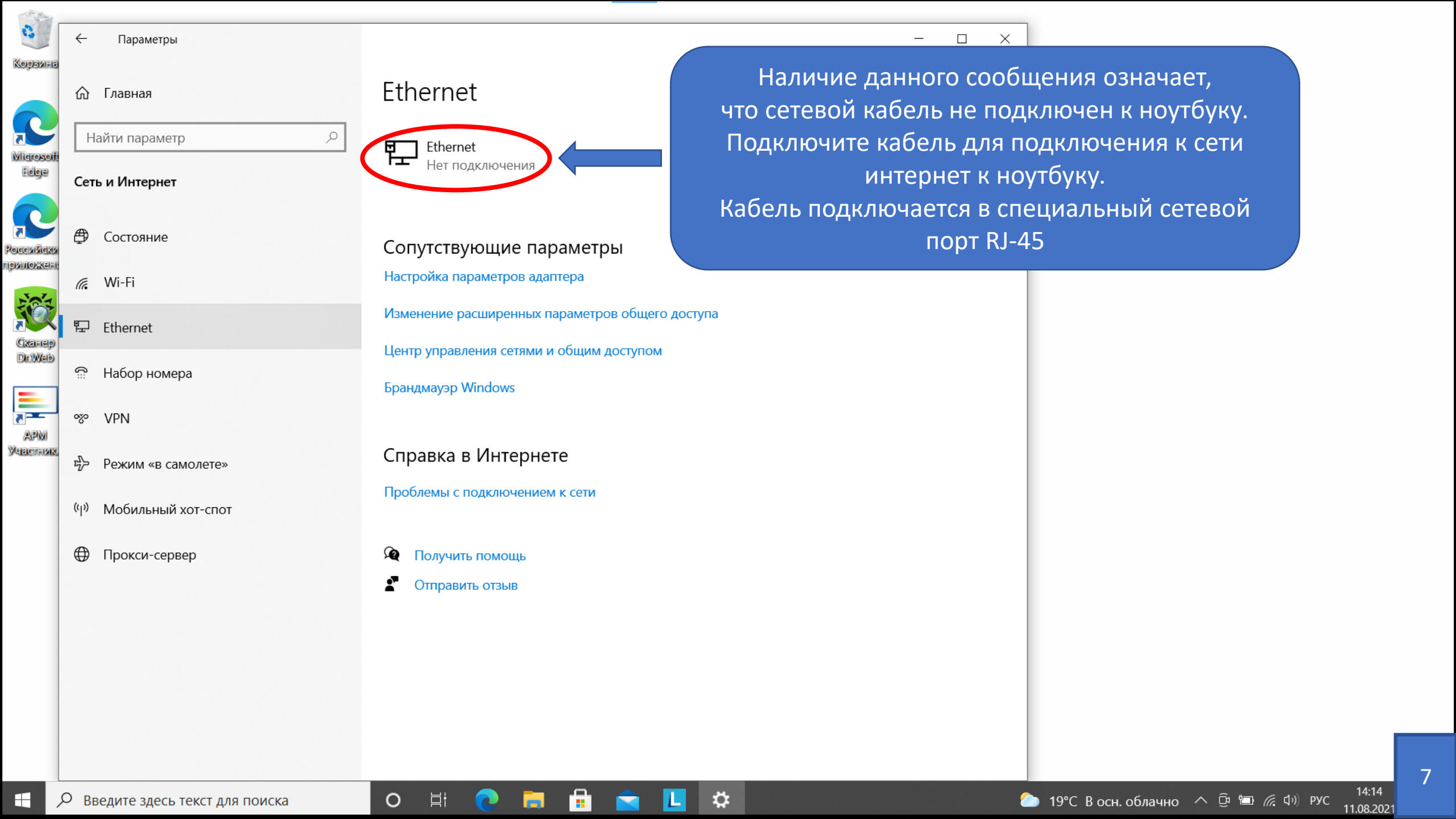
Левой кнопкой мыши нажмите на меню «Пуск»

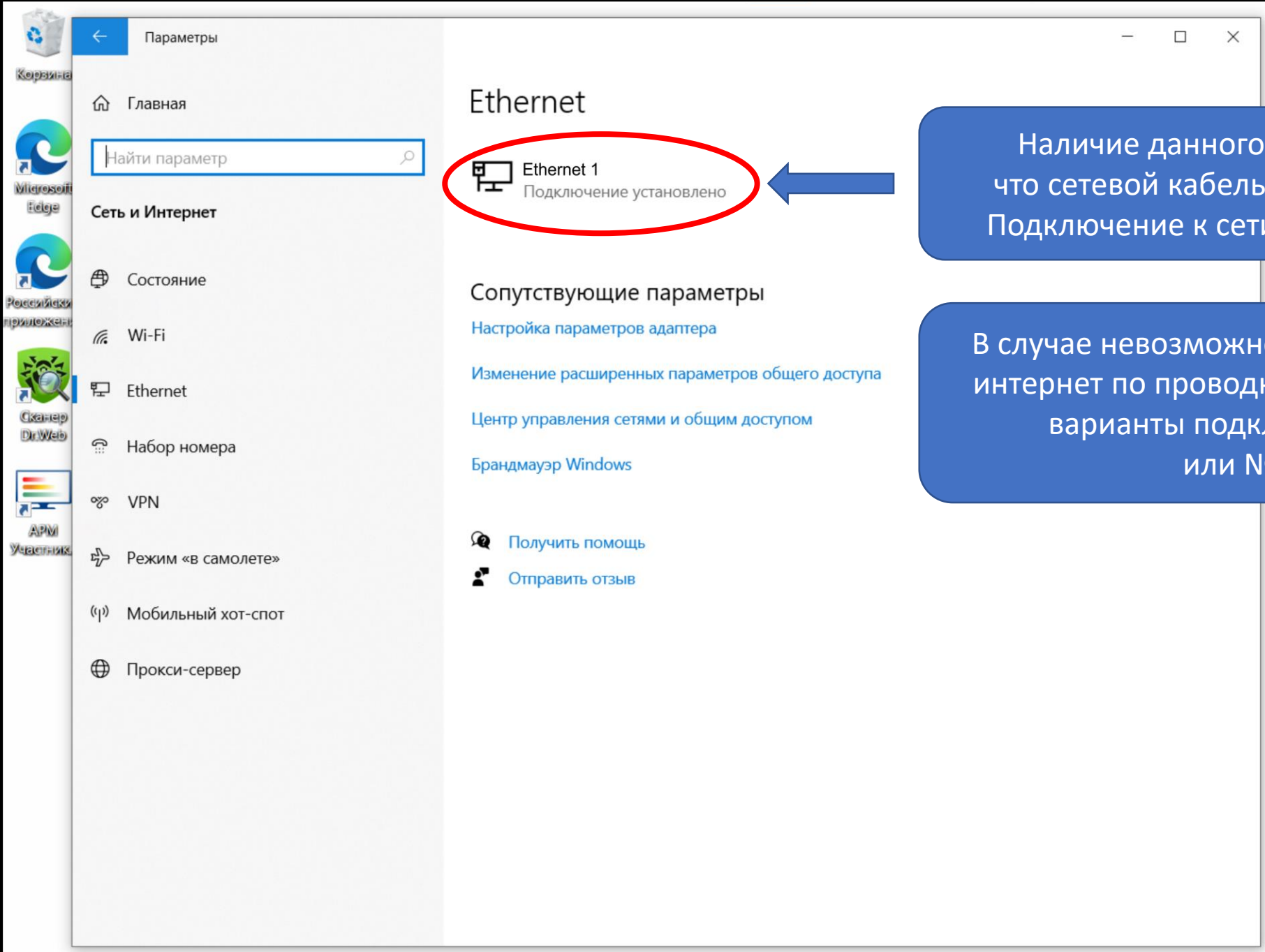


ПЕРМСКАЯ
ГОРОДСКАЯ
ДУМА


Параметры
35
Локальная учетная запись
Вход
OneDrive
Вход
Центр обновления Windows
Обратите внимание
Просмотр веб-страниц
Рекомендуемые параметры
Найти параметр
Телефон
Связать устройство с Android, iPhone
Сеть и Интернет
Wi-Fi, режим "в самолете", VPN
Персонализация
Фон, экран блокировки, цвета
Приложения
Удаление, значения по умолчанию, доп. компоненты
Учетные записи
Учетные записи, эл. почта, синхронизация, работа, семья
Время и язык
Распознавание голоса, регион, дата
Игры
Xbox Game Bar, снимки, режим игры
Специальные возможности
Экранный диктор,
Поиск
Найти мои файлы, разрешения
Конфиденциальность
Расположение, камера, микрофон
Корзина
Microsoft Edge
Российские приложения
Сканер Dr.Web
АРМ Участник...
В открывшемся окне
левой кнопкой мыши нажмите
на пункт меню «Сеть и Интернет»
Введите здесь текст для поиска
18°C В осн. облачно
РУС
13:59
11.08.202


Параметры
Главная
Найти параметр
Сеть и Интернет
Состояние
Wi-Fi
Ethernet
Набор номера
VPN
Режим «в самолете»
Мобильный хот-спот
Прокси-сервер
Состояние
Состояние сети
В открывшемся окне
левой кнопкой мыши нажмите
на пункт меню «Ethernet»
Показать доступные сети
Просмотрите варианты подключения вокруг.
Дополнительные сетевые параметры
Настройка параметров адаптера
Просмотр сетевых адаптеров и изменение параметров подключения.
Центр управления сетями и общим доступом
Определите, к каким данным вы хотите предоставить доступ для сетей, с которыми установлено соединение.
Просмотр свойств оборудования и подключения
Брандмауэр Windows
Сброс сети
Корзина
Microsoft Edge
Российские приложения
Сканер Dr.Web
АРМ Участник...
Введите здесь текст для поиска
18°C В осн. облачно
РУС
13:59
11.08.202


Параметры
Главная
Найти параметр
Сеть и Интернет
Состояние
Wi-Fi
Ethernet
Набор номера
VPN
Режим «в самолете»
Мобильный хот-спот
Прокси-сервер
Ethernet
Ethernet
Нет подключения
Сопутствующие параметры
Настройка параметров адаптера
Изменение расширенных параметров общего доступа
Центр управления сетями и общим доступом
Брандмауэр Windows
Справка в Интернете
Проблемы с подключением к сети
Получить помощь
Отправить отзыв
Наличие данного сообщения означает, что сетевой кабель не подключен к ноутбуку. Подключите кабель для подключения к сети интернет к ноутбуку.
Кабель подключается в специальный сетевой порт RJ-45
Введите здесь текст для поиска
19°C В осн. облачно
РУС
14:14
11.08.2021



Наличие данного сообщения означает, что сетевой кабель подключен к ноутбуку. Подключение к сети Интернет установлено

В случае невозможности подключения к сети интернет по проводному каналу используйте варианты подключения №2 (стр.9) или №3 (стр.14)

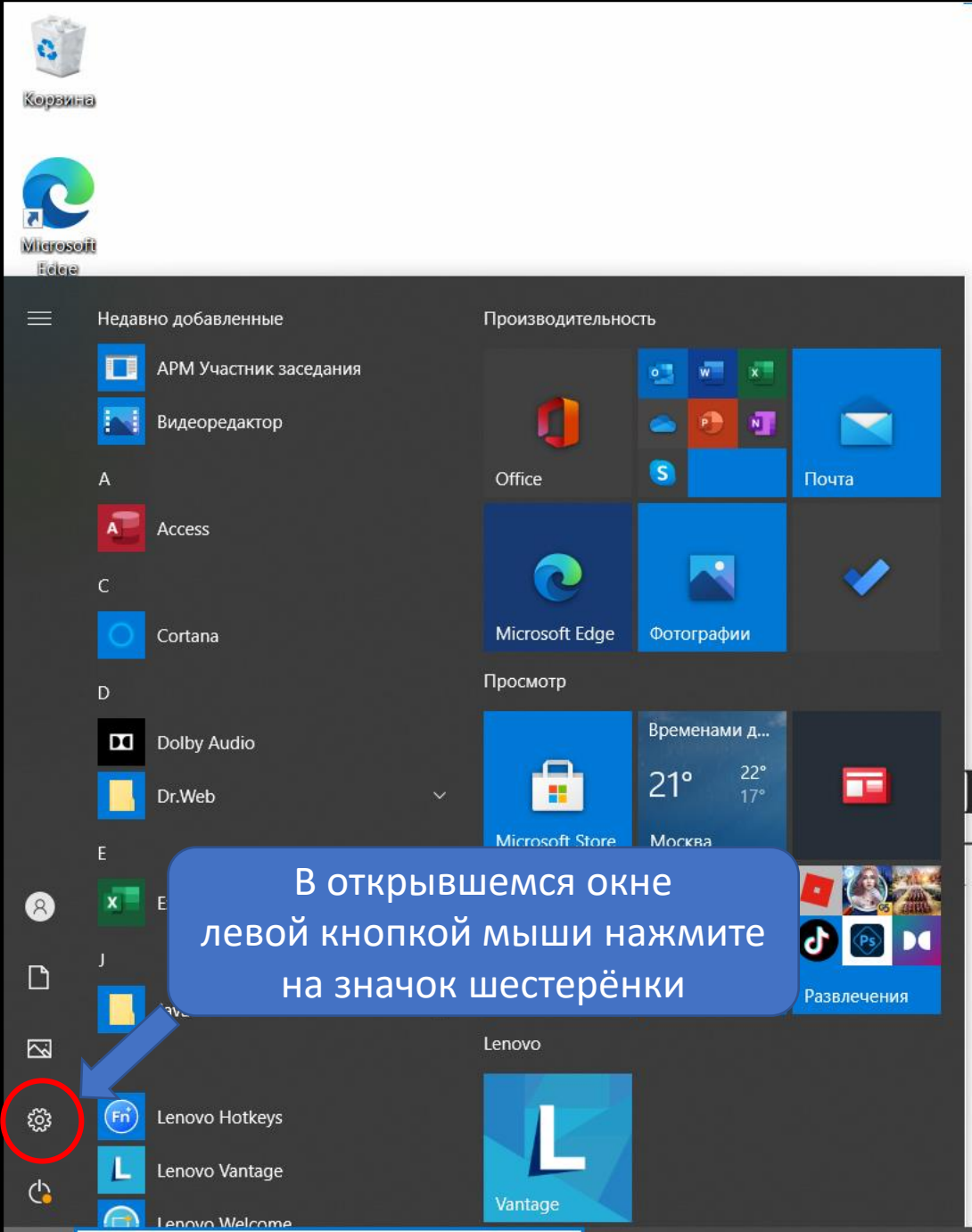
Подключение к сети интернет

Вариант 2

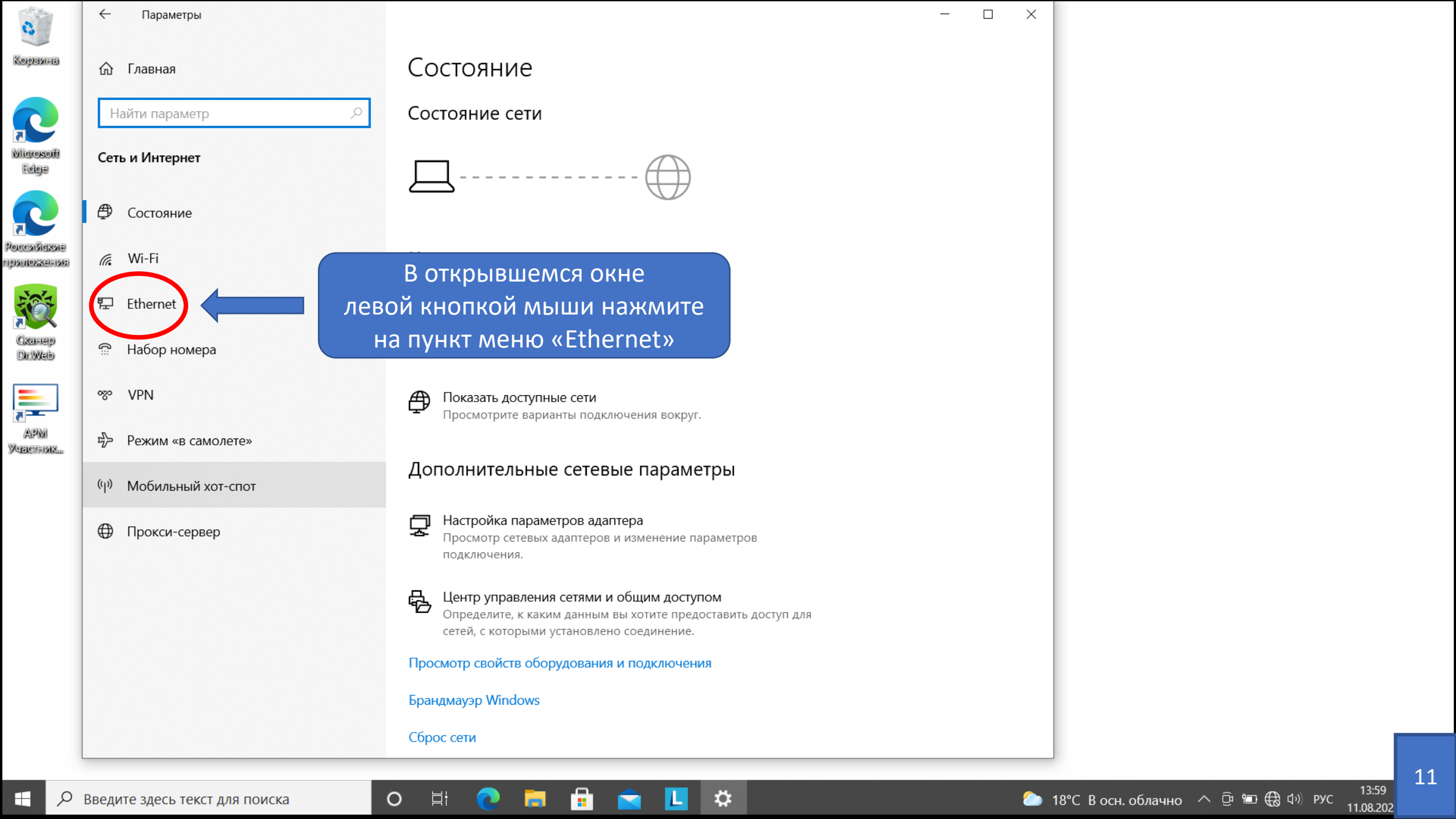
Подключение к сети интернет при помощи 3G/4G USB модема

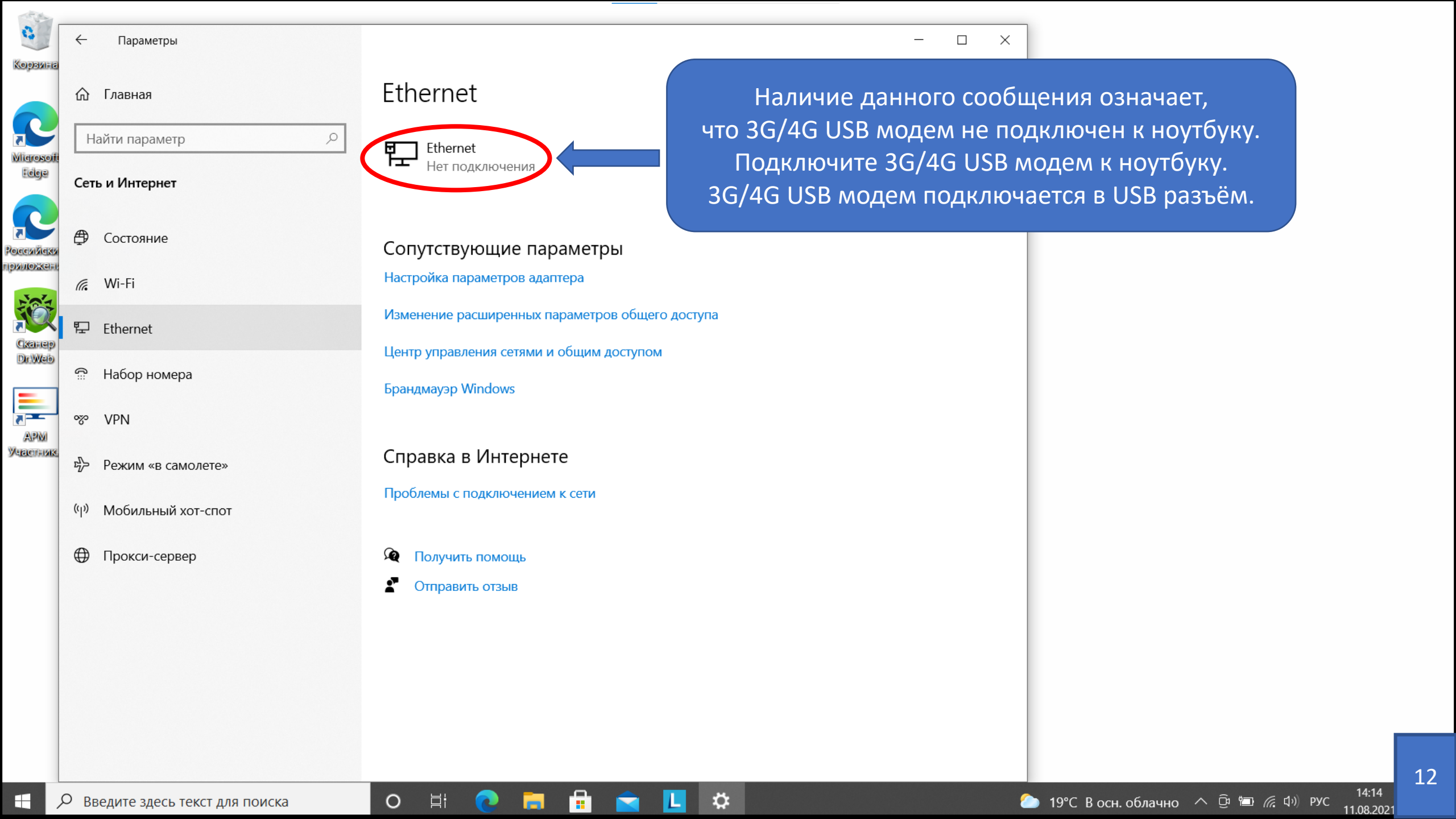
ПЕРМСКАЯ ГОРОДСКАЯ ДУМА

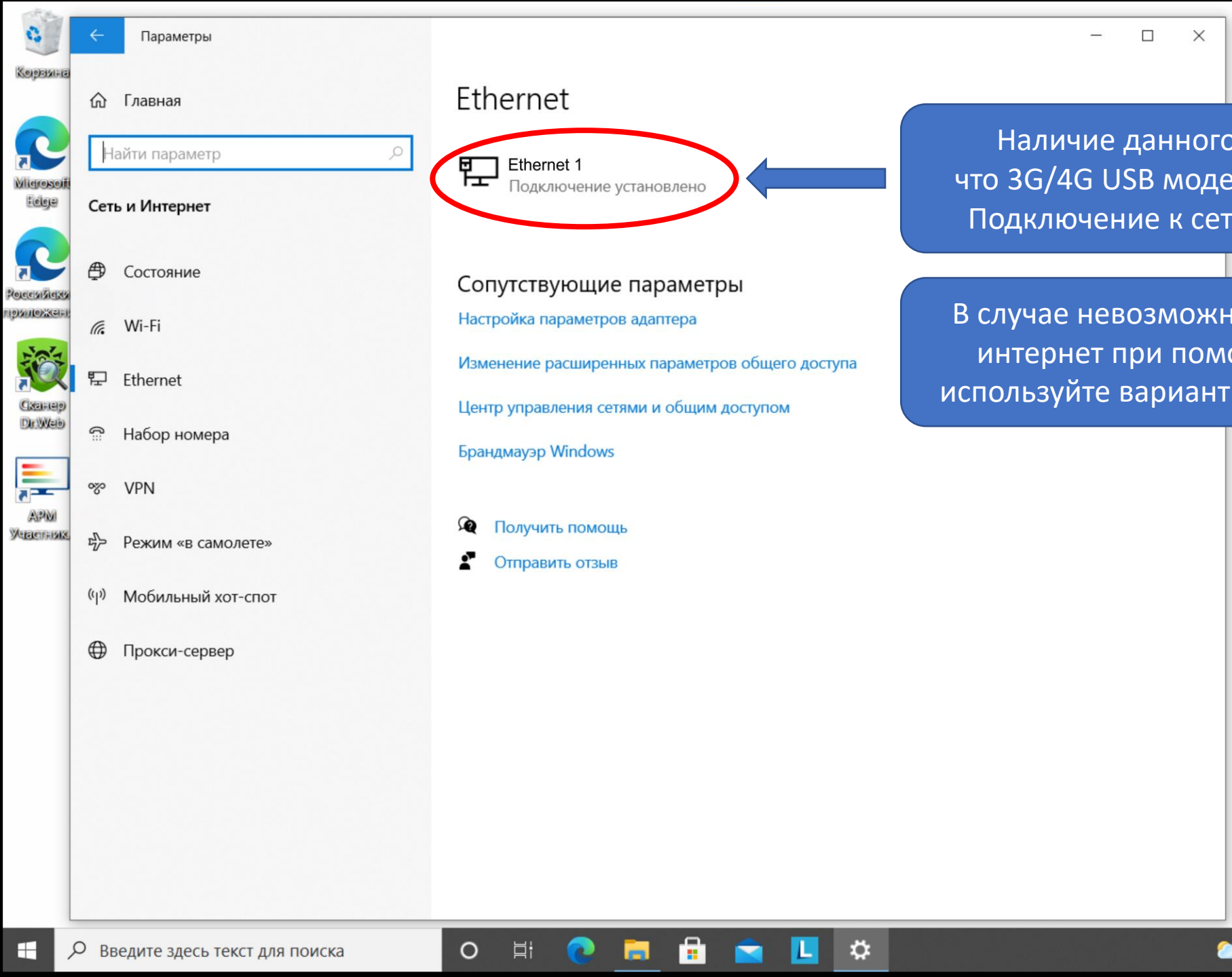
Левой кнопкой мыши нажмите на меню «Пуск»



ПЕРМСКАЯ
ГОРОДСКАЯ
ДУМА


Параметры
Главная
Найти параметр
Сеть и Интернет
Состояние
Wi-Fi
Ethernet
Набор номера
VPN
Режим «в самолете»
Мобильный хот-спот
Прокси-сервер
Состояние
Состояние сети
В открывшемся окне
левой кнопкой мыши нажмите
на пункт меню «Ethernet»
Показать доступные сети
Просмотрите варианты подключения вокруг.
Дополнительные сетевые параметры
Настройка параметров адаптера
Просмотр сетевых адаптеров и изменение параметров подключения.
Центр управления сетями и общим доступом
Определите, к каким данным вы хотите предоставить доступ для сетей, с которыми установлено соединение.
Просмотр свойств оборудования и подключения
Брандмауэр Windows
Сброс сети
Корзина
Microsoft Edge
Российские приложения
Сканер Dr.Web
АРМ Участник...
Введите здесь текст для поиска
18°C В осн. облачно
РУС
13:59
11.08.202


Параметры
Главная
Найти параметр
Сеть и Интернет
Состояние
Wi-Fi
Ethernet
Набор номера
VPN
Режим «в самолете»
Мобильный хот-спот
Прокси-сервер
Ethernet
Ethernet
Нет подключения
Наличие данного сообщения означает,
что 3G/4G USB модем не подключен к ноутбуку.
Подключите 3G/4G USB модем к ноутбуку.
3G/4G USB модем подключается в USB разъём.
Сопутствующие параметры
Настройка параметров адаптера
Изменение расширенных параметров общего доступа
Центр управления сетями и общим доступом
Брандмауэр Windows
Справка в Интернете
Проблемы с подключением к сети
Получить помощь
Отправить отзыв
Введите здесь текст для поиска
19°C В осн. облачно
РУС
14:14
11.08.2021



Наличие данного сообщения означает, что 3G/4G USB модем подключен к ноутбуку. Подключение к сети интернет установлено

В случае невозможности подключения к сети интернет при помощи 3G/4G USB модема используйте вариант подключения №3 (стр.14)

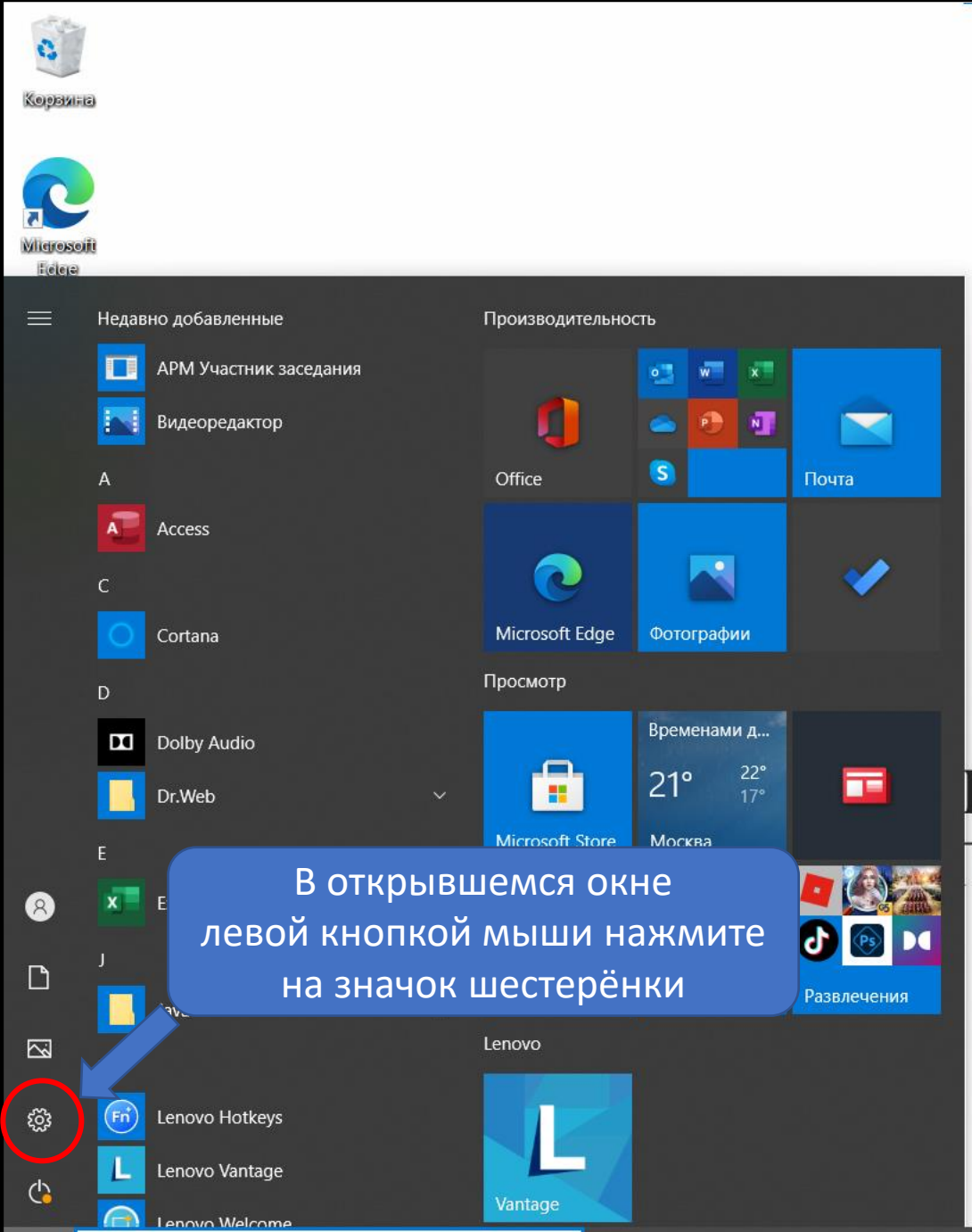
Подключение к сети интернет

Вариант 3

Подключение к сети интернет через сеть Wi-Fi

ПЕРМСКАЯ
ГОРОДСКАЯ
ДУМА

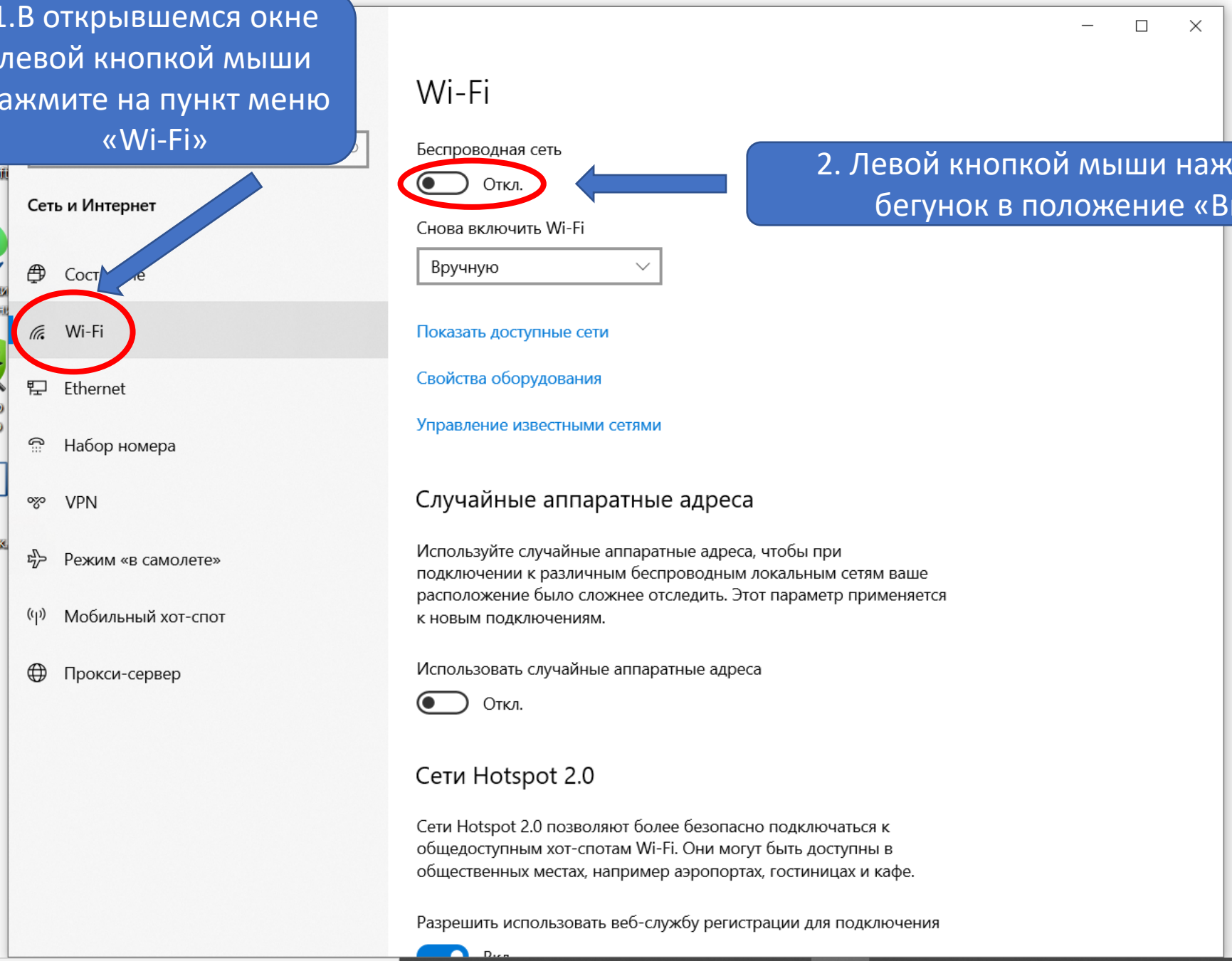
Левой кнопкой мыши нажмите на меню «Пуск»



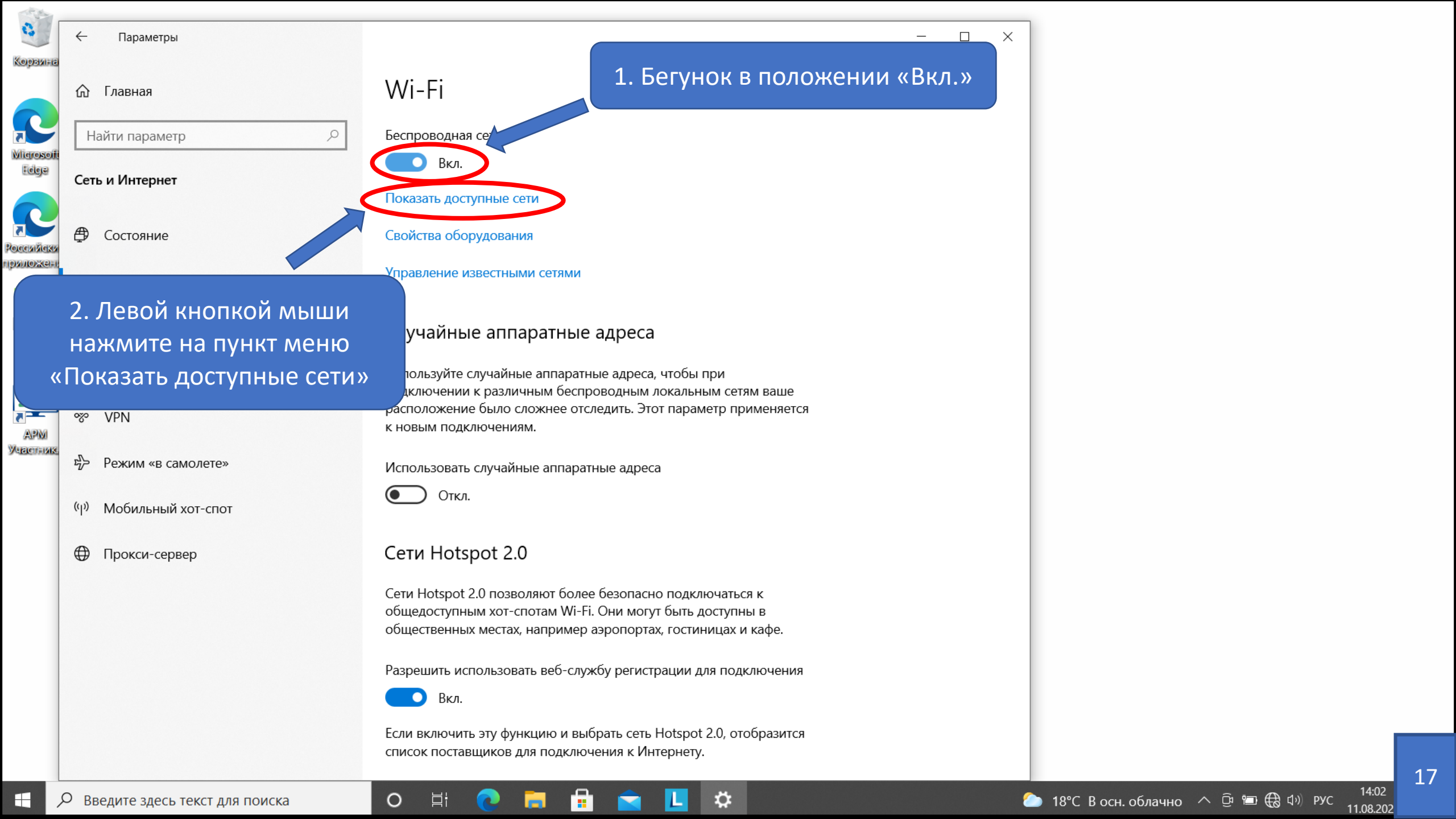
В открывшемся окне
левой кнопкой мыши нажмите
на значок шестерёнки

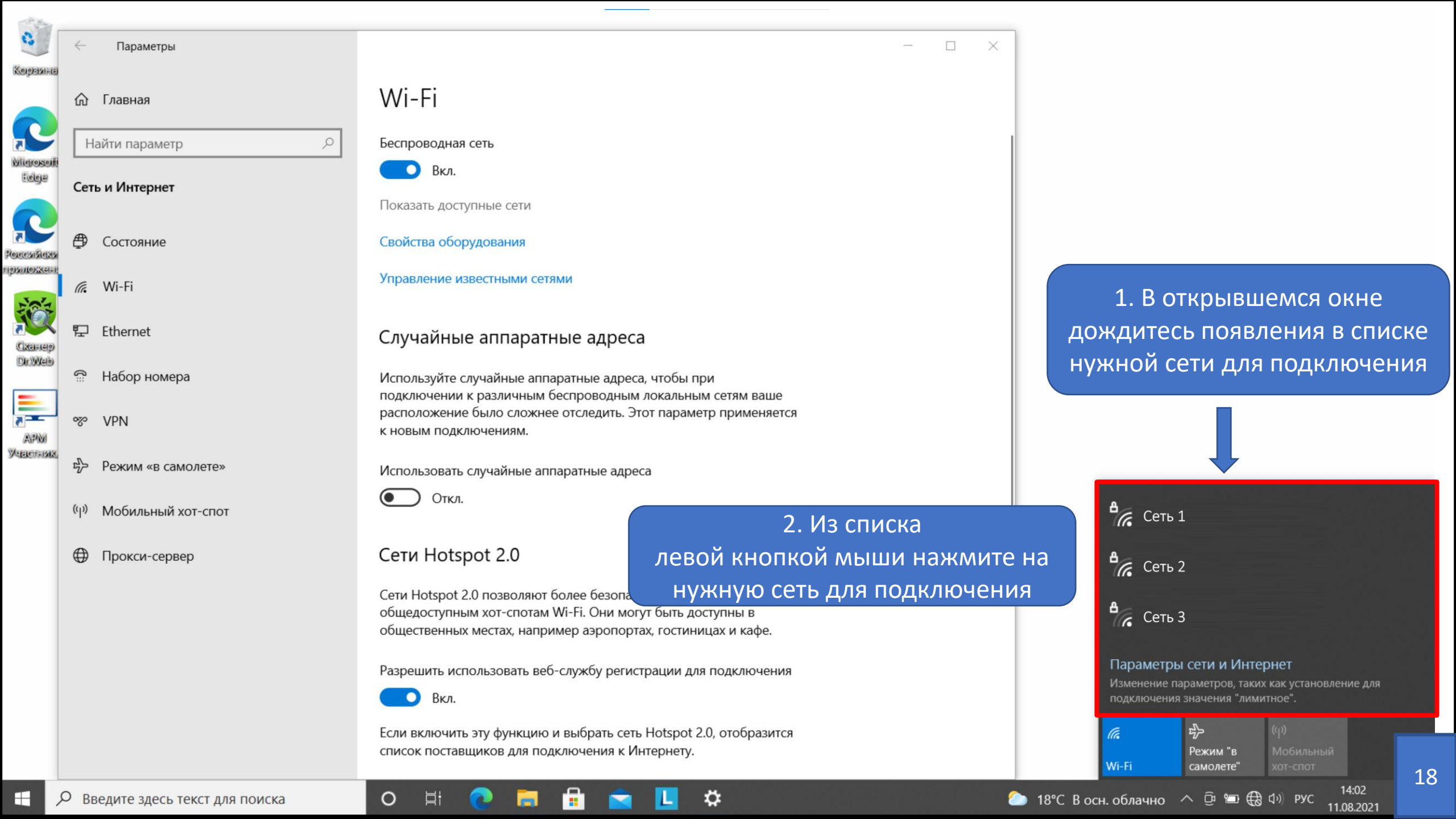
ПЕРМСКАЯ
ГОРОДСКАЯ
ДУМА

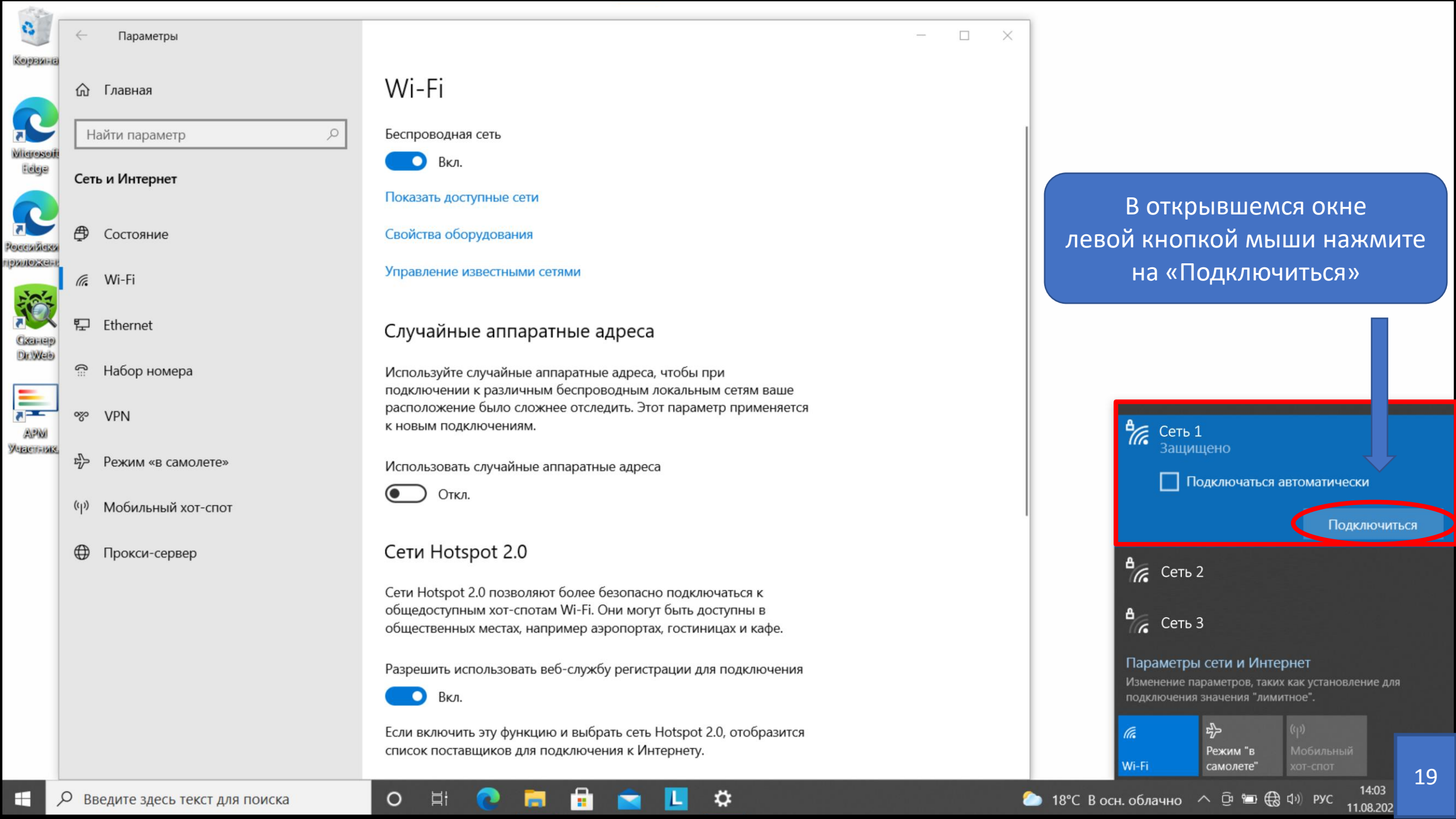
1.В открывшемся окне левой кнопкой мыши нажмите на пункт меню «Wi-Fi»

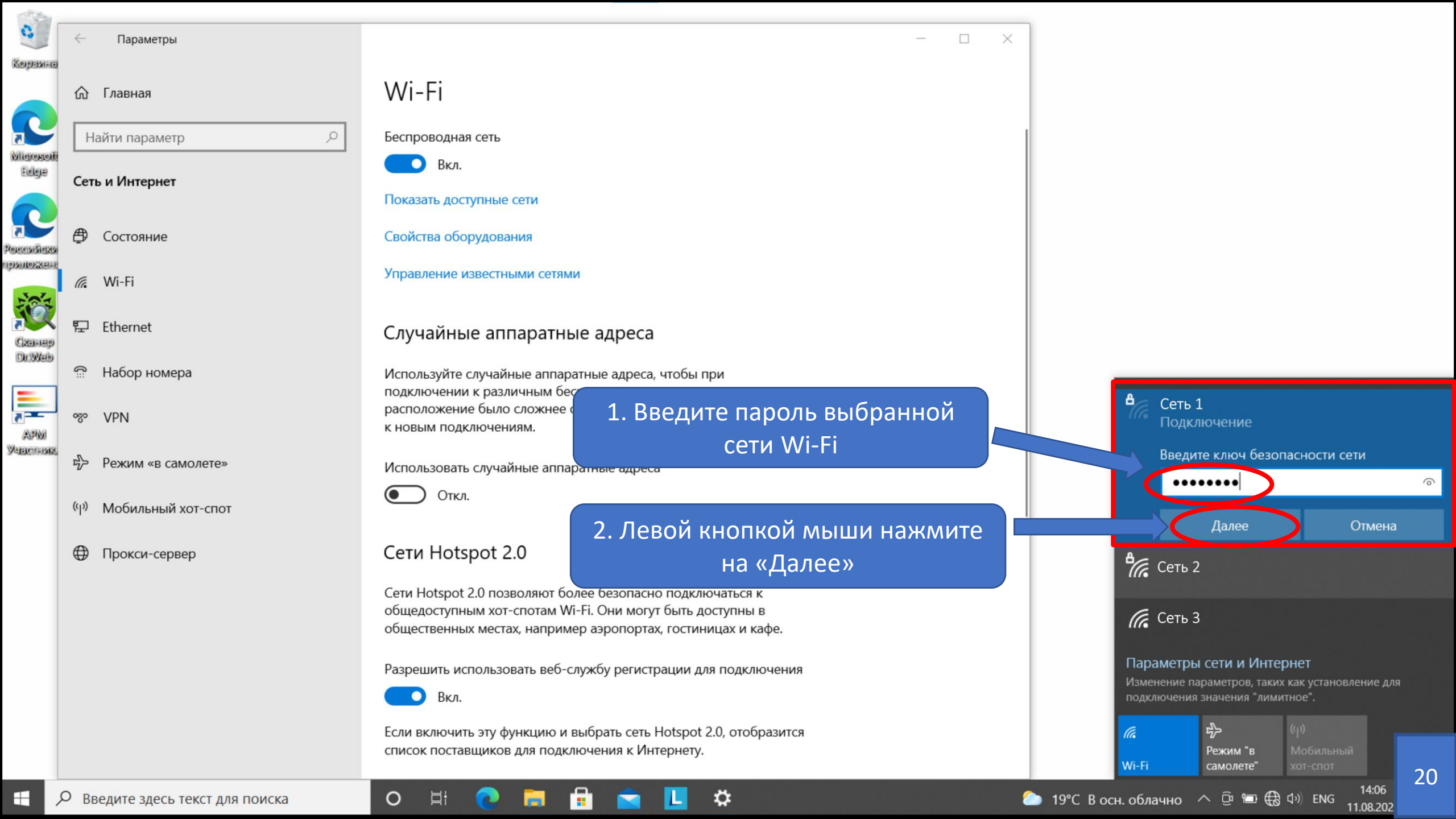


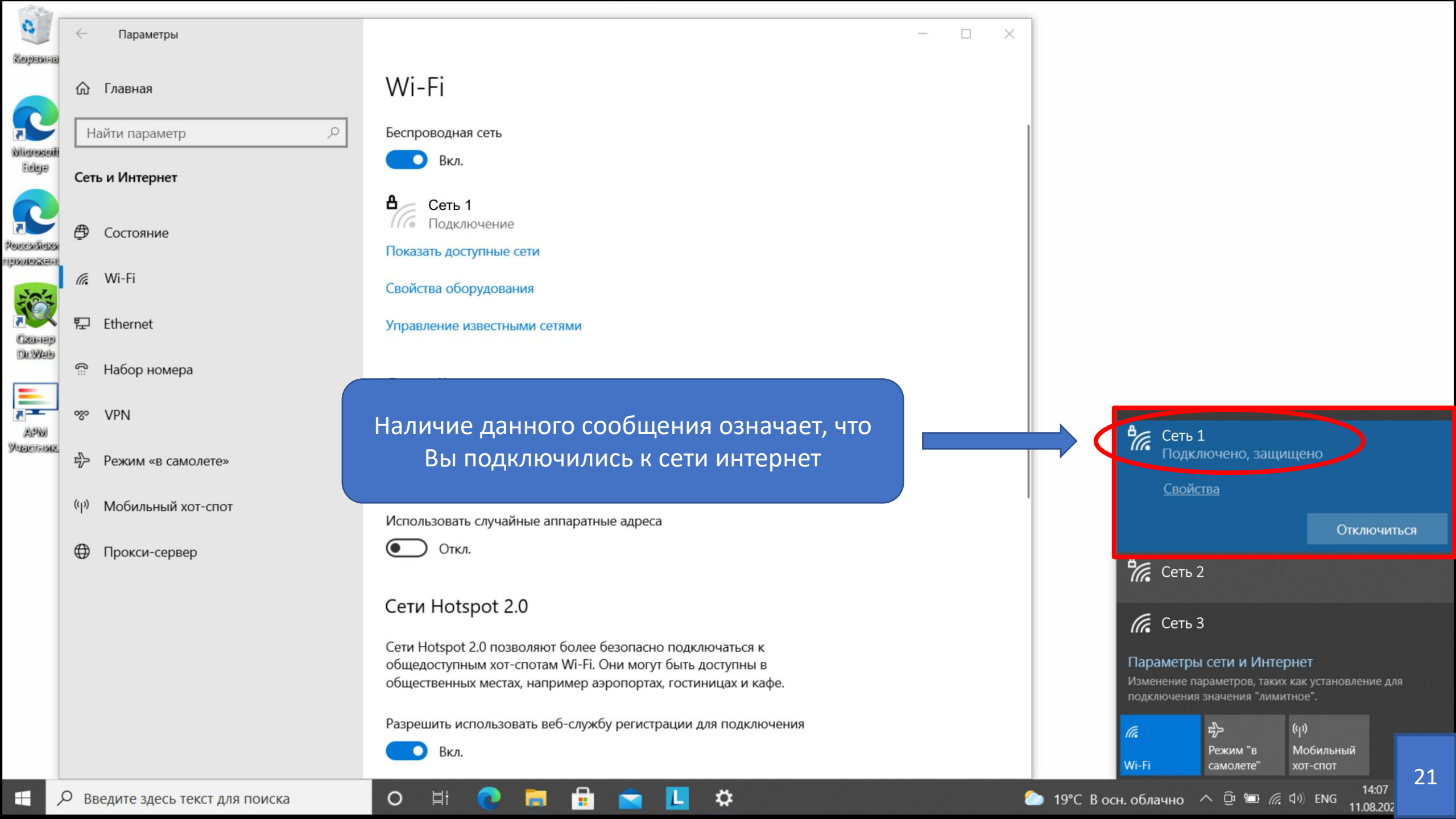
2. Левой кнопкой мыши нажмите на бегунок в положение «Вкл.»


Параметры
Главная
Найти параметр
Сеть и Интернет
Состояние
VPN
Режим «в самолете»
Мобильный хот-спот
Прокси-сервер
Wi-Fi
Беспроводная се
Вкл.
Показать доступные сети
Свойства оборудования
Управление известными сетями
учайные аппаратные адреса
пользуйте случайные аппаратные адреса, чтобы при
дключении к различным беспроводным локальным сетям ваше
асположение было сложнее отследить. Этот параметр применяется
к новым подключениям.
Использовать случайные аппаратные адреса
Откл.
Сети Hotspot 2.0
Сети Hotspot 2.0 позволяют более безопасно подключаться к общедоступным хот-спотам Wi-Fi. Они могут быть доступны в общественных местах, например аэропортах, гостиницах и кафе.
Разрешить использовать веб-службу регистрации для подключения
Вкл.
Если включить эту функцию и выбрать сеть Hotspot 2.0, отобразится список поставщиков для подключения к Интернету.
1. Бегунок в положении «Вкл.»
2. Левой кнопкой мыши нажмите на пункт меню «Показать доступные сети»
Введите здесь текст для поиска
18°C В осн. облачно
РУС
14:02
11.08.202
17

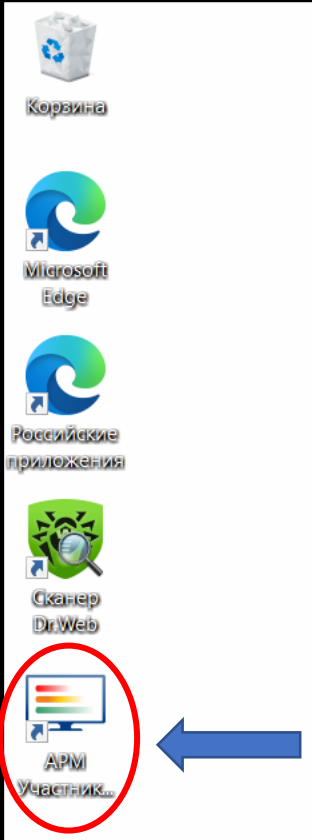

Параметры
Главная
Найти параметр
Сеть и Интернет
Состояние
Wi-Fi
Ethernet
Набор номера
VPN
Режим «в самолете»
Мобильный хот-спот
Прокси-сервер
Wi-Fi
Беспроводная сеть
Вкл.
Показать доступные сети
Свойства оборудования
Управление известными сетями
Случайные аппаратные адреса
Используйте случайные аппаратные адреса, чтобы при подключении к различным беспроводным локальным сетям ваше расположение было сложнее отследить. Этот параметр применяется к новым подключениям.
Использовать случайные аппаратные адреса
Откл.
Сети Hotspot 2.0
Сети Hotspot 2.0 позволяют более безопа
общедоступным хот-спотам Wi-Fi. Они могут быть доступны в общественных местах, например аэропортах, гостиницах и кафе.
Разрешить использовать веб-службу регистрации для подключения
Вкл.
Если включить эту функцию и выбрать сеть Hotspot 2.0, отобразится список поставщиков для подключения к Интернету.
1. В открывшемся окне дождитесь появления в списке нужной сети для подключения
2. Из списка левой кнопкой мыши нажмите на нужную сеть для подключения
Сеть 1
Сеть 2
Сеть 3
Параметры сети и Интернет
Изменение параметров, таких как установление для подключения значения "лимитное".
Wi-Fi
Режим "в самолете"
Мобильный хот-спот
Введите здесь текст для поиска
18°C В осн. облачно
РУС
14:02
11.08.2021
18


Параметры
Главная
Найти параметр
Сеть и Интернет
Состояние
Wi-Fi
Ethernet
Набор номера
VPN
Режим «в самолете»
Мобильный хот-спот
Прокси-сервер
Wi-Fi
Беспроводная сеть
Вкл.
Показать доступные сети
Свойства оборудования
Управление известными сетями
Случайные аппаратные адреса
Используйте случайные аппаратные адреса, чтобы при подключении к различным беспроводным локальным сетям ваше расположение было сложнее отследить. Этот параметр применяется к новым подключениям.
Использовать случайные аппаратные адреса
Откл.
Сети Hotspot 2.0
Сети Hotspot 2.0 позволяют более безопасно подключаться к общедоступным хот-спотам Wi-Fi. Они могут быть доступны в общественных местах, например аэропортах, гостиницах и кафе.
Разрешить использовать веб-службу регистрации для подключения
Вкл.
Если включить эту функцию и выбрать сеть Hotspot 2.0, отобразится список поставщиков для подключения к Интернету.
В открывшемся окне левой кнопкой мыши нажмите на «Подключиться»
Сеть 1
Защищено
Подключаться автоматически
Подключиться
Сеть 2
Сеть 3
Параметры сети и Интернет
Изменение параметров, таких как установление для подключения значения "лимитное".
Wi-Fi
Режим "в самолете"
Мобильный хот-спот
Введите здесь текст для поиска
18°C В осн. облачно
РУС
14:03
11.08.202
19

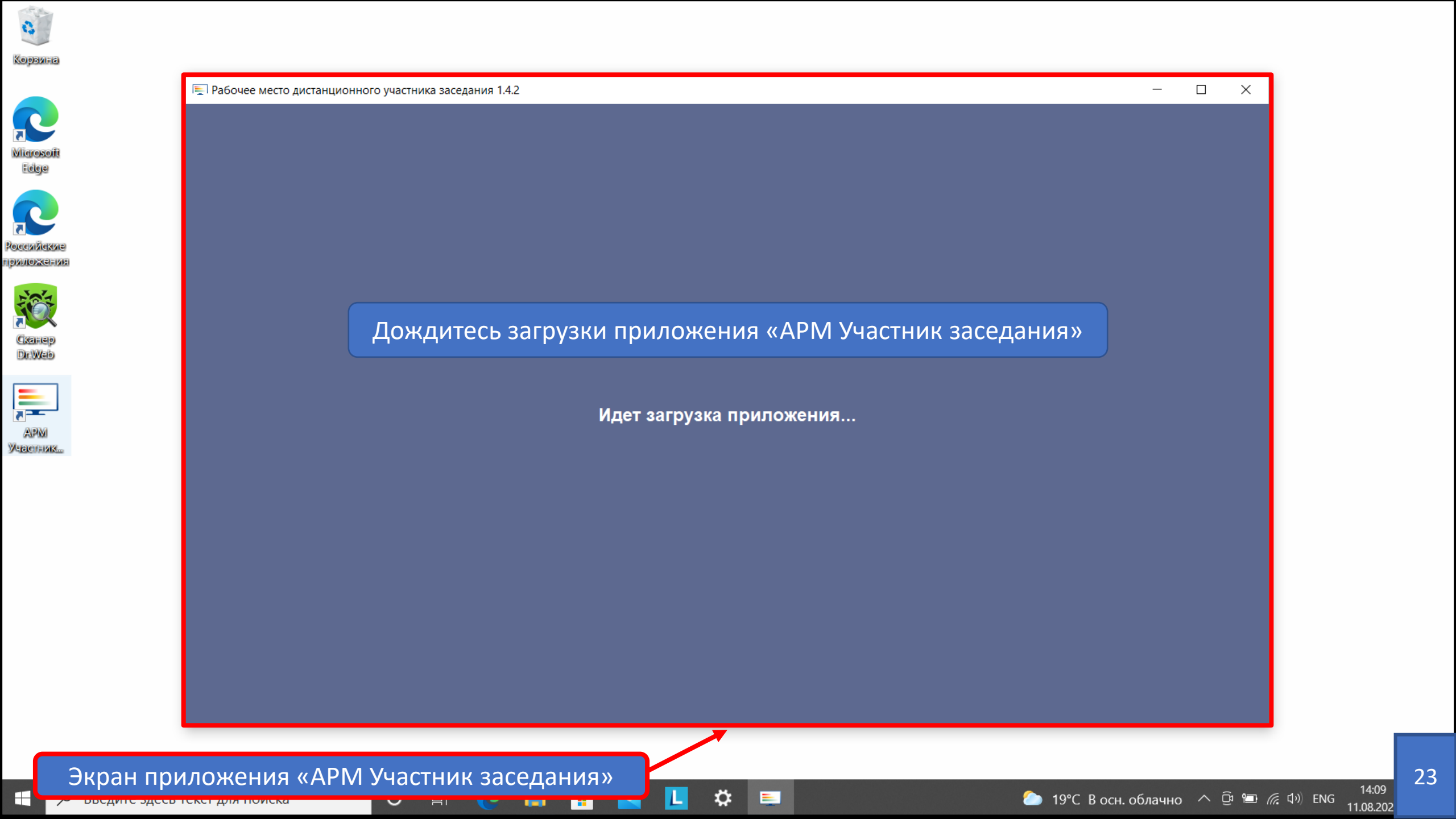

Параметры
Главная
Найти параметр
Сеть и Интернет
Состояние
Wi-Fi
Ethernet
Набор номера
VPN
Режим «в самолете»
Мобильный хот-спот
Прокси-сервер
Wi-Fi
Беспроводная сеть
Вкл.
Показать доступные сети
Свойства оборудования
Управление известными сетями
Случайные аппаратные адреса
Используйте случайные аппаратные адреса, чтобы при
подключении к различным бес
расположение было сложнее
к новым подключениям.
Использовать случайные аппаратные адреса
Откл.
Сети Hotspot 2.0
Сети Hotspot 2.0 позволяют более безопасно подключаться к
общедоступным хот-спотам Wi-Fi. Они могут быть доступны в
общественных местах, например аэропортах, гостиницах и кафе.
Разрешить использовать веб-службу регистрации для подключения
Вкл.
Если включить эту функцию и выбрать сеть Hotspot 2.0, отобразится
список поставщиков для подключения к Интернету.
1. Введите пароль выбранной сети Wi-Fi
2. Левой кнопкой мыши нажмите на «Далее»
Сеть 1
Подключение
Введите ключ безопасности сети
Далее
Отмена
Сеть 2
Сеть 3
Параметры сети и Интернет
Изменение параметров, таких как установление для подключения значения "лимитное".
Wi-Fi
Режим "в самолете"
Мобильный хот-спот
Введите здесь текст для поиска
19°C В осн. облачно
ENG
14:06
11.08.202


Параметры
Главная
Найти параметр
Сеть и Интернет
Состояние
Wi-Fi
Ethernet
Набор номера
VPN
Режим «в самолете»
Мобильный хот-спот
Прокси-сервер
Wi-Fi
Беспроводная сеть
Вкл.
Сеть 1
Подключение
Показать доступные сети
Свойства оборудования
Управление известными сетями
Использовать случайные аппаратные адреса
Откл.
Сети Hotspot 2.0
Сети Hotspot 2.0 позволяют более безопасно подключаться к общедоступным хот-спотам Wi-Fi. Они могут быть доступны в общественных местах, например аэропортах, гостиницах и кафе.
Разрешить использовать веб-службу регистрации для подключения
Вкл.
Наличие данного сообщения означает, что Вы подключились к сети интернет
Сеть 1
Подключено, защищено
Свойства
Отключиться
Сеть 2
Сеть 3
Параметры сети и Интернет
Изменение параметров, таких как установление для подключения значения "лимитное".
Wi-Fi
Режим "в самолете"
Мобильный хот-спот
Введите здесь текст для поиска
19°C В осн. облачно
ENG
14:07
11.08.202

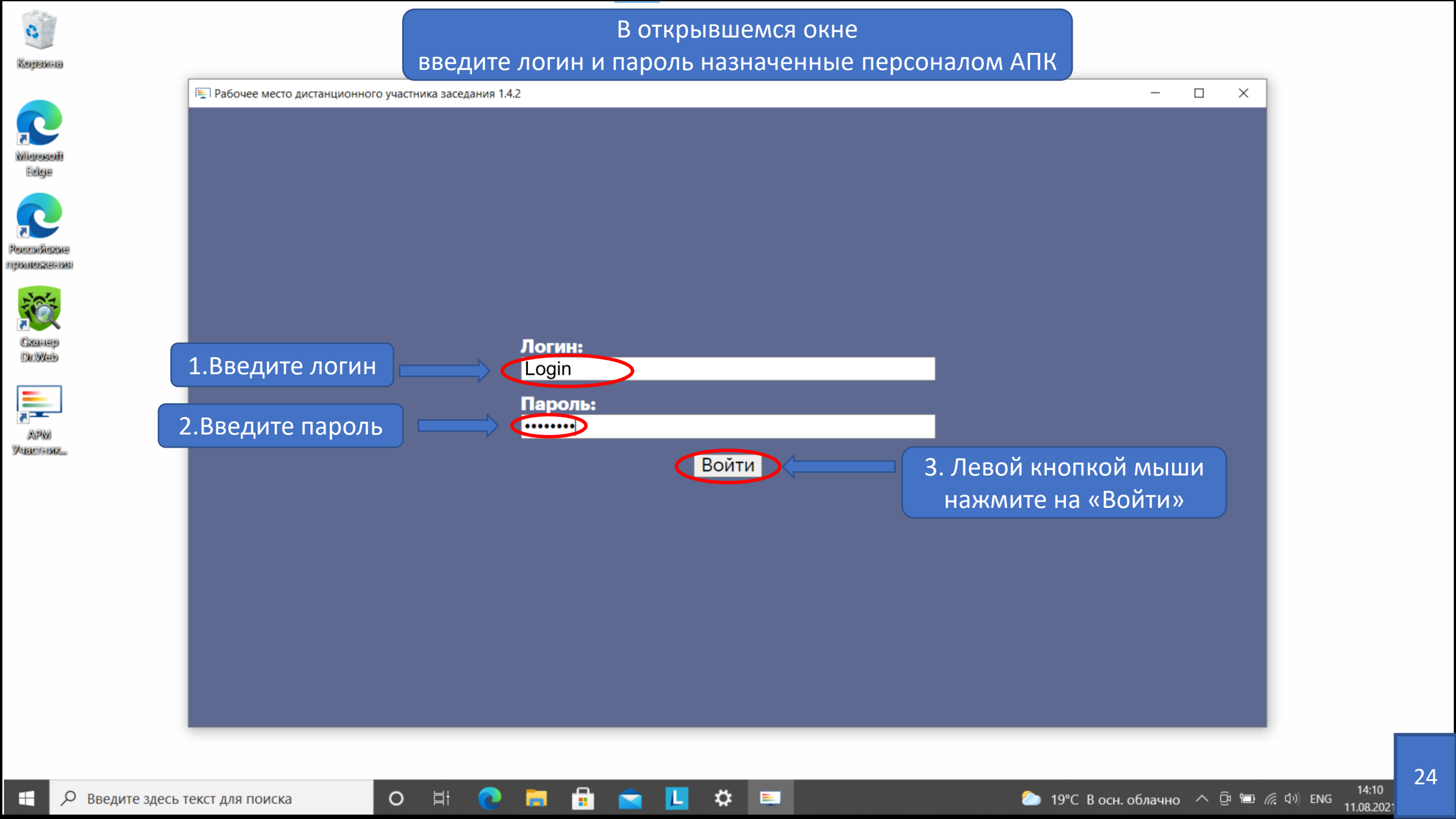
Для подключения к системе АПК зала
нажмите 2 раза левой кнопкой мыши на приложение
«АРМ Участник заседания»

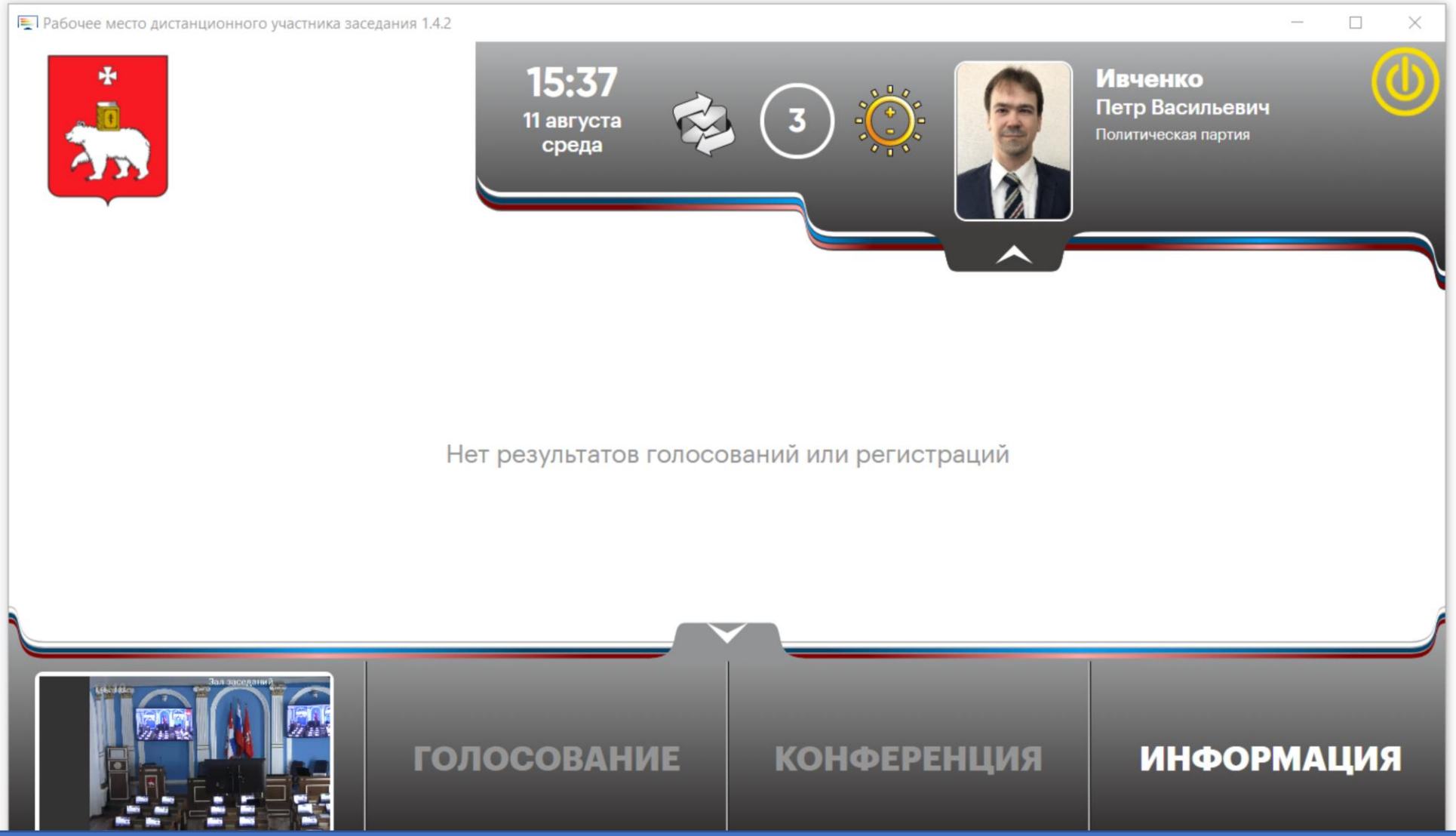


ПЕРМСКАЯ
ГОРОДСКАЯ
ДУМА

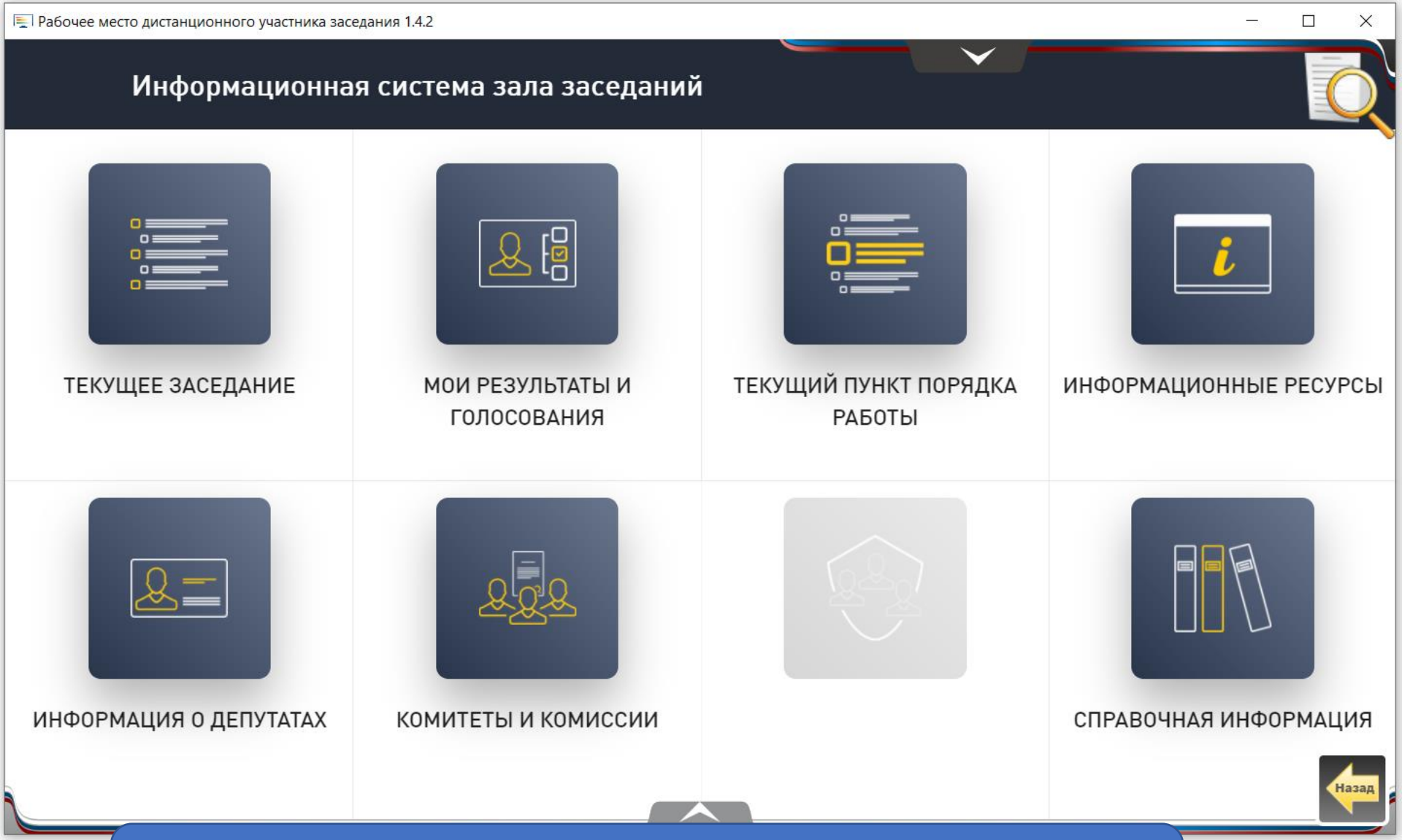

Корзина
Microsoft Edge
Российские приложения
Сканер Dr.Web
АРМ Участник...
Рабочее место дистанционного участника заседания 1.4.2
Дождитесь загрузки приложения «АРМ Участник заседания»
Идет загрузка приложения...
Экран приложения «АРМ Участник заседания»
19°C В осн. облачно
ENG
14:09
11.08.202

В открывшемся окне
введите логин и пароль назначенные персоналом АПК

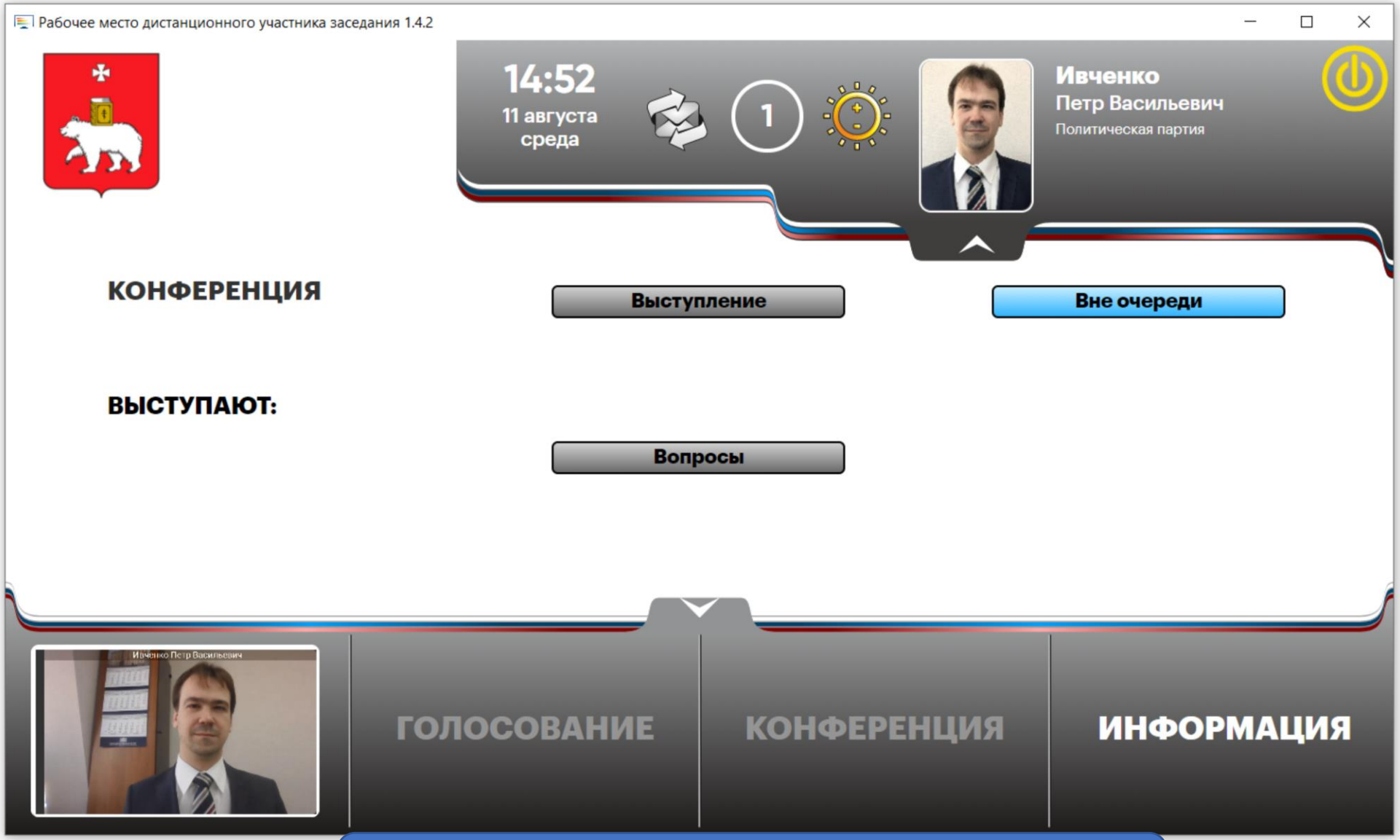




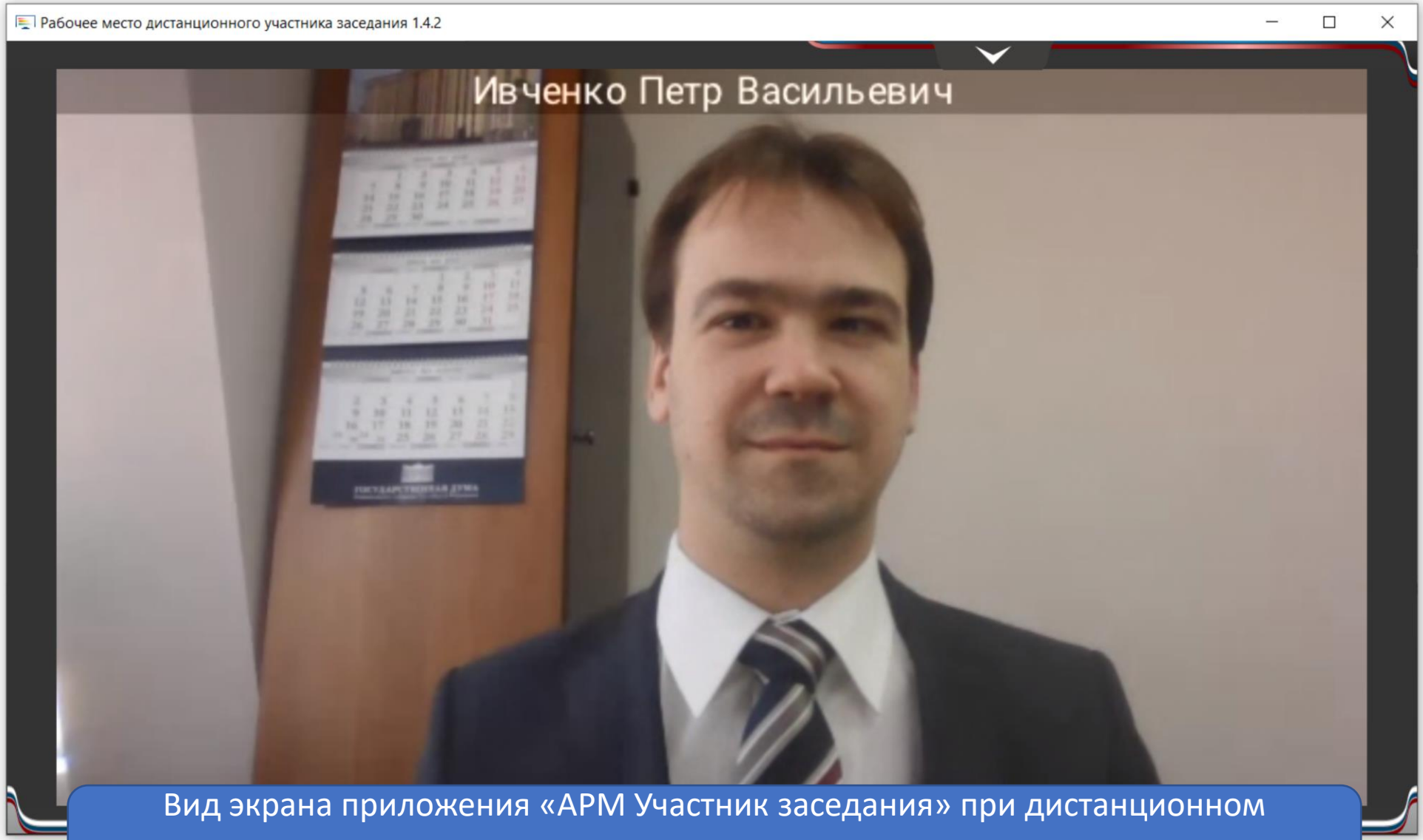
Появление на экране приложения «АРМ Участник заседания» интерфейса аналогичного интерфейсу информационного терминала, установленного в зале заседаний,
означает, что Вы успешно дистанционно подключились к системе АПК зала заседаний



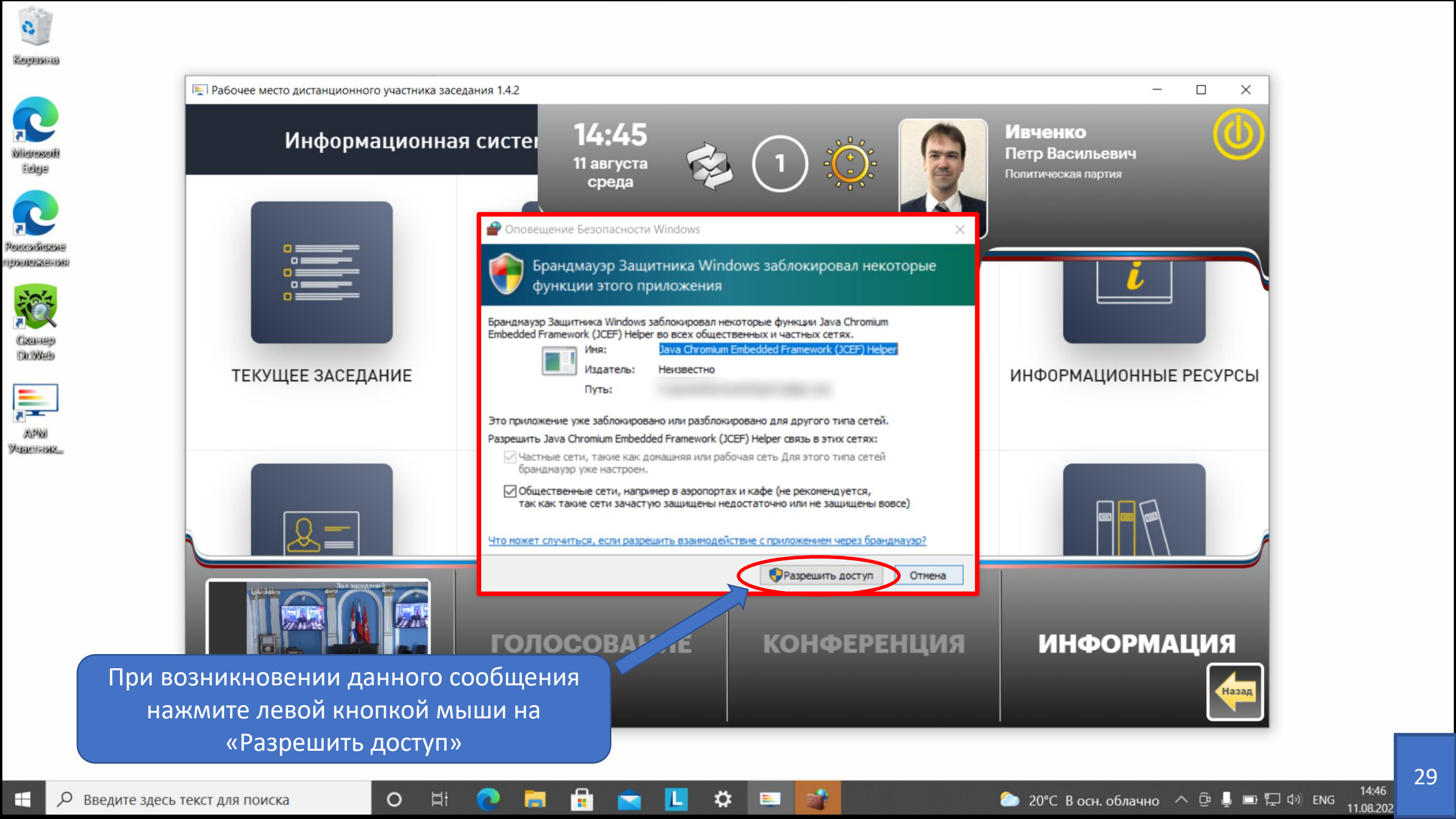
Вид экрана приложения «АРМ Участник заседания» при входе в раздел «Информационная система зала заседаний»



Вид экрана приложения «АРМ Участник заседания» в режиме «Конференция»

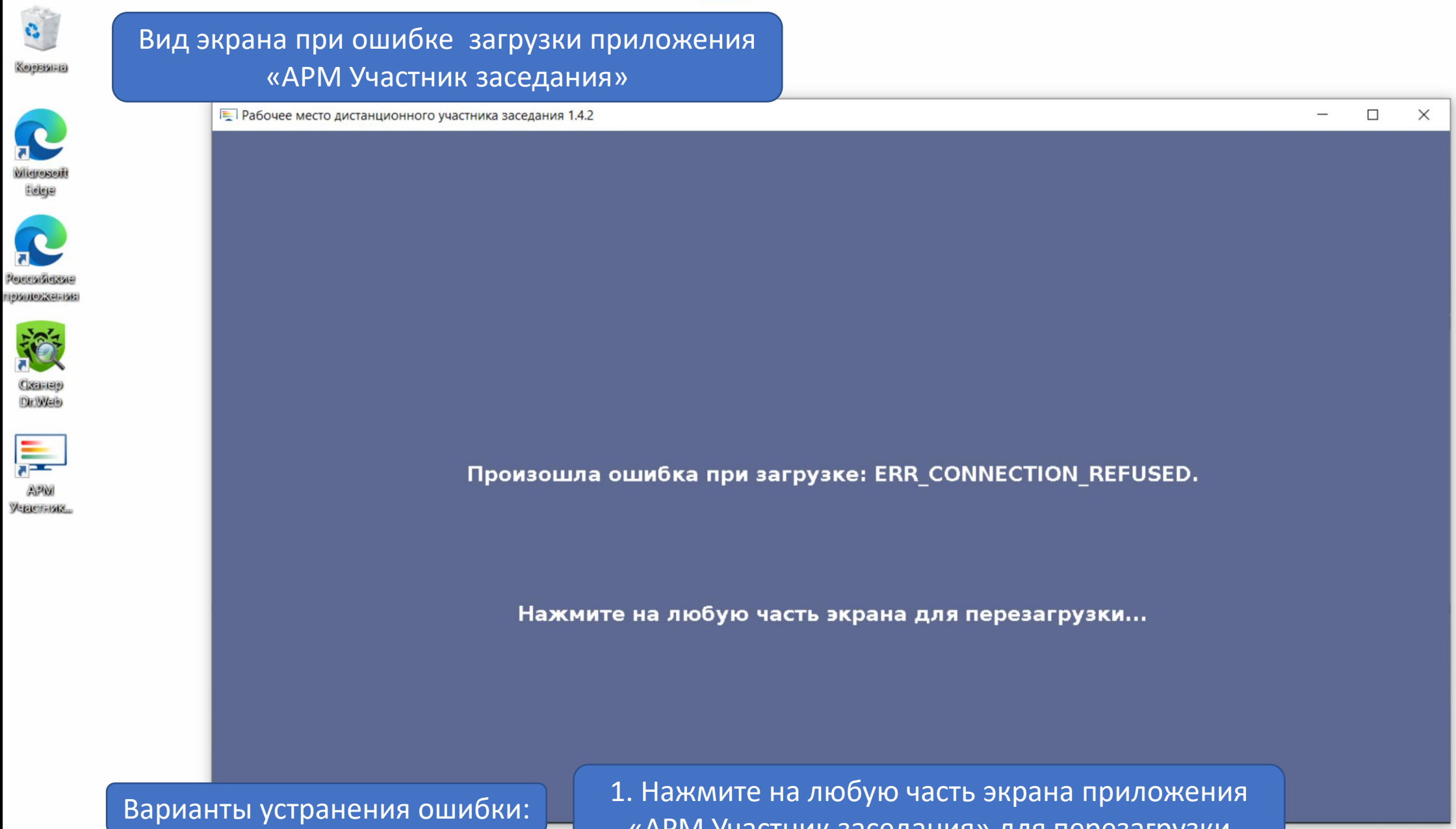


Вид экрана приложения «АРМ Участник заседания» при дистанционном выступлении участника заседания через встроенную систему видеоконференцсвязи



При возникновении данного сообщения нажмите левой кнопкой мыши на «Разрешить доступ»

Вид экрана при ошибке загрузки приложения «АРМ Участник заседания»

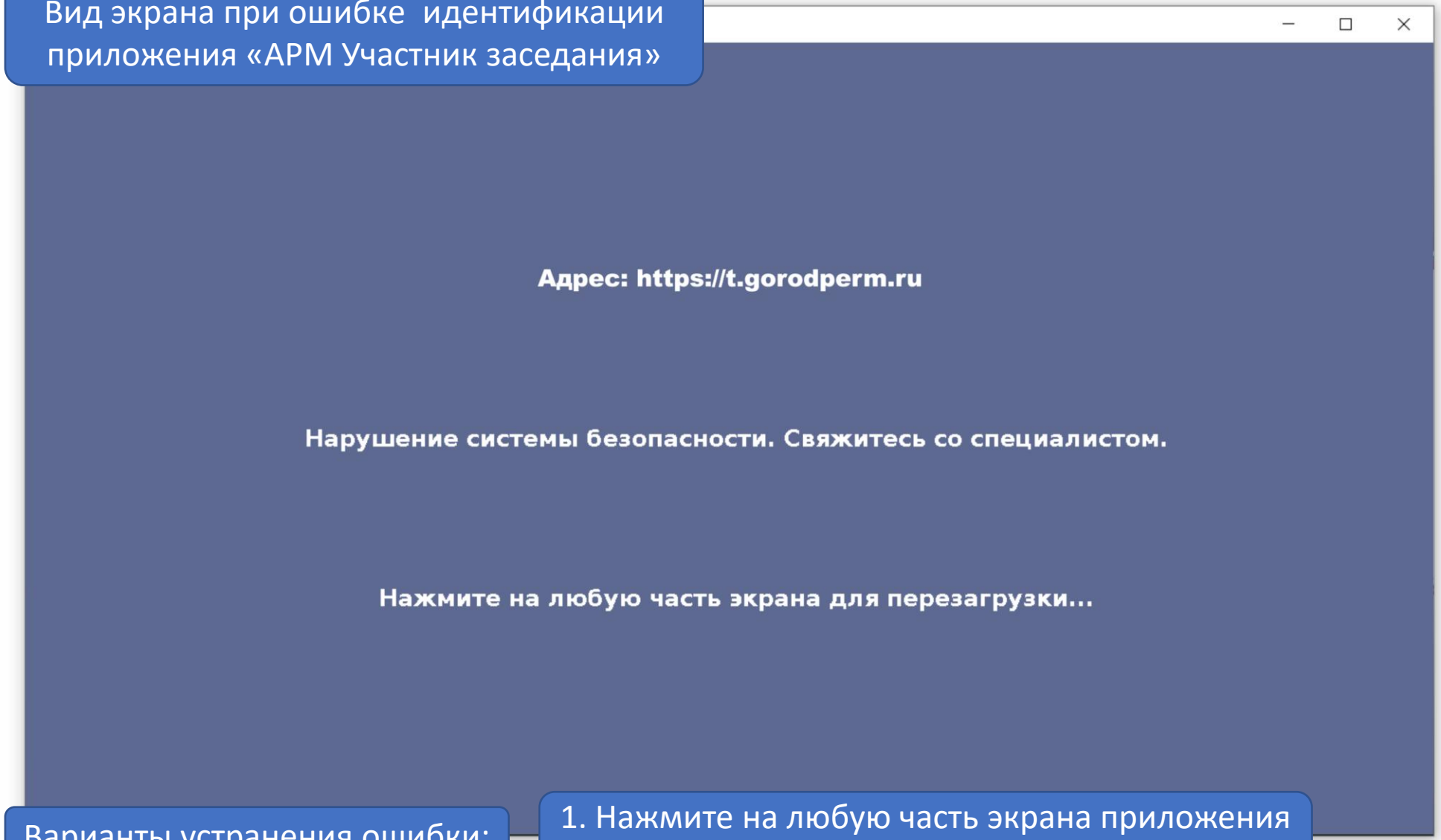


Варианты устранения ошибки:

1. Нажмите на любую часть экрана приложения «АРМ Участник заседания» для перезагрузки

2. Свяжитесь с техническим персоналом АПК

Вид экрана при ошибке идентификации приложения «АРМ Участник заседания»



Варианты устранения ошибки:

1. Нажмите на любую часть экрана приложения «АРМ Участник заседания» для перезагрузки
2. Свяжитесь с техническим персоналом АПК