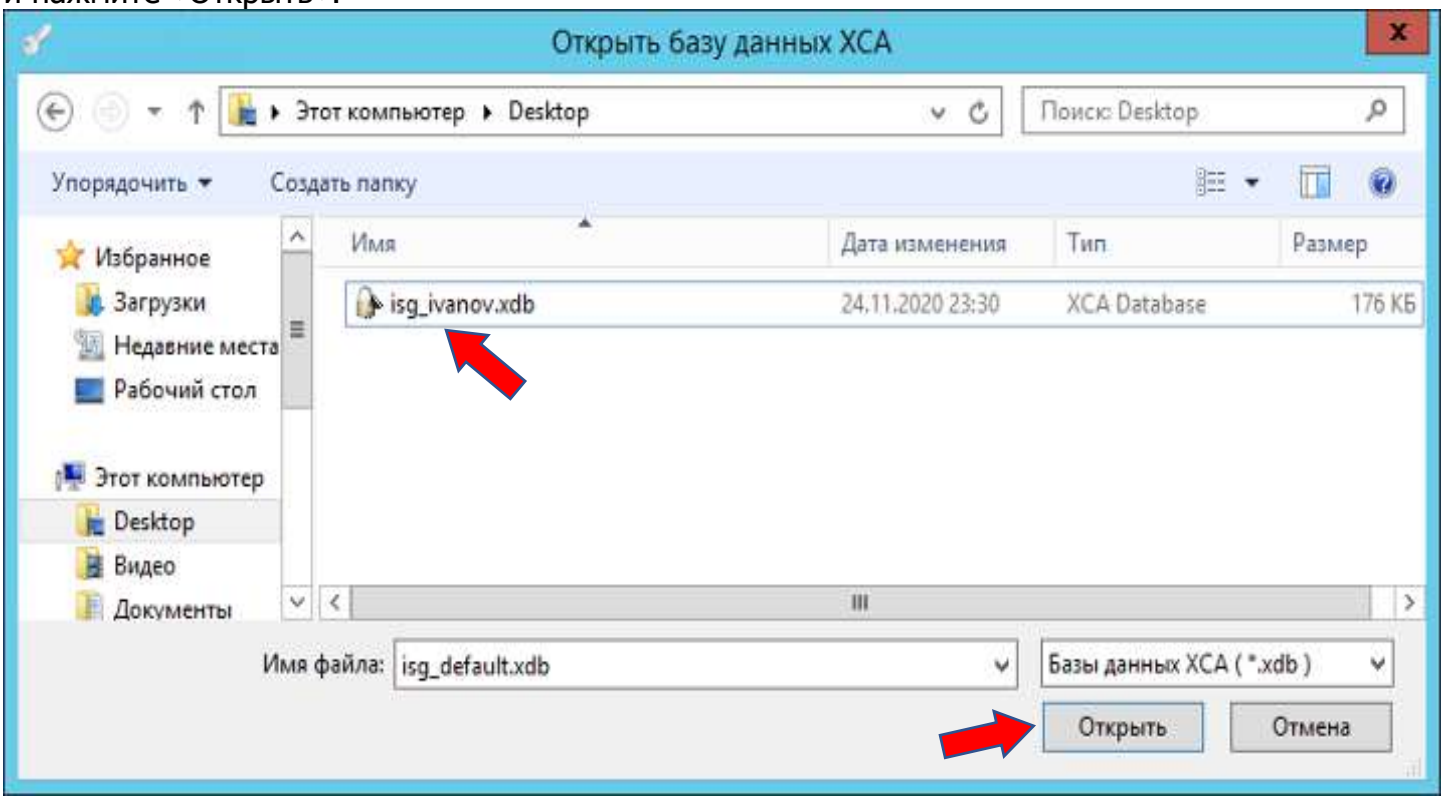
Уважаемый сотрудник/партнер!

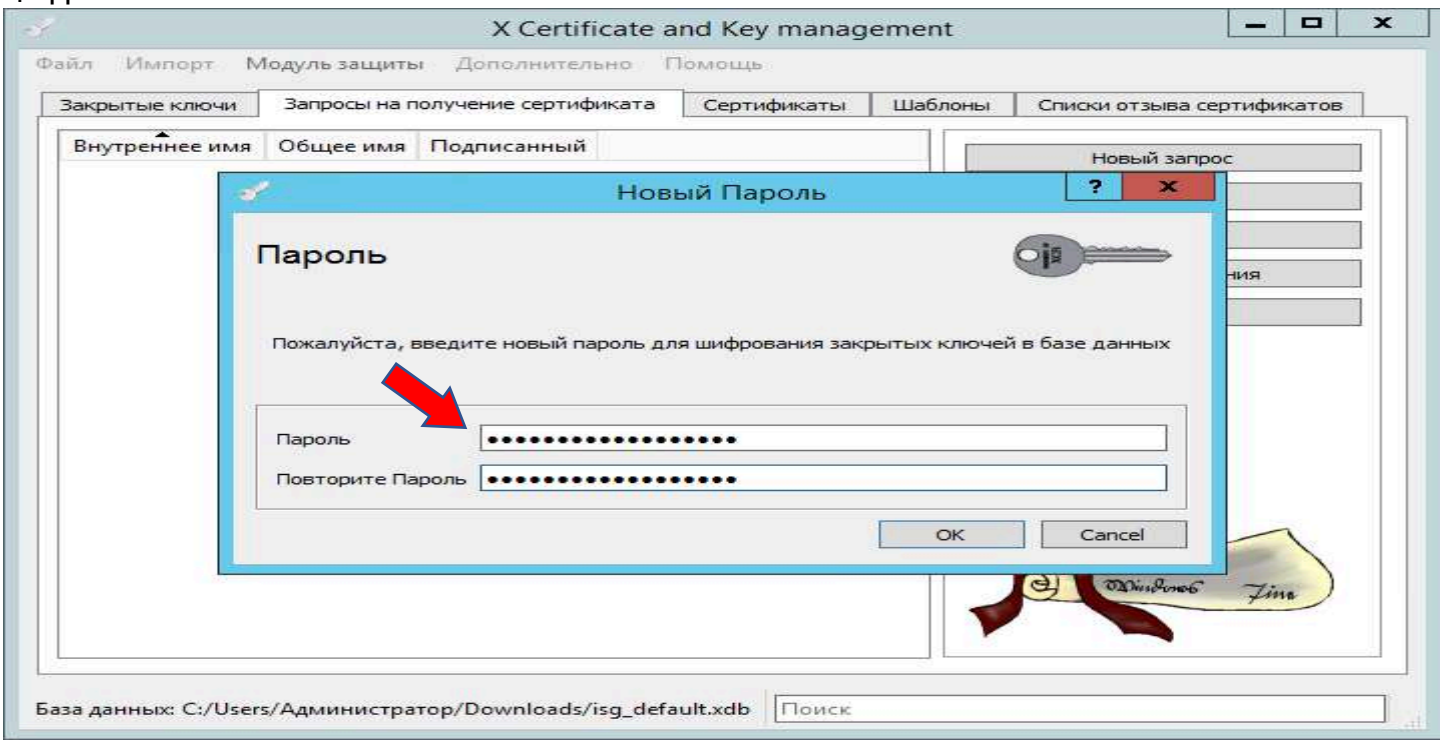
Вы получили инструкцию для получения защищенного доступа в информационную систему Группы компаний «Информ-Системы». Доступ позволит быстро и безопасно использовать сервисы группы (электронную почту, телефонию, видеоконференцсвязь, систему коллективной работы, мессенджеры и т.д.) в любой точке мира, а также подписывать электронной подписью необходимые документы. Каждому сотруднику/партнеру выдается 2 сертификата: для VPN доступа и ЭЦП необходимых документов, в рамках данной инструкции будет создано 2 соответствующих запроса. Просим Вас следовать описанным ниже инструкциям и желаем успехов! Инструкция подходит для операционных систем Windows, Mac OS X, Linux.

1. Создание запроса на получение сертификата

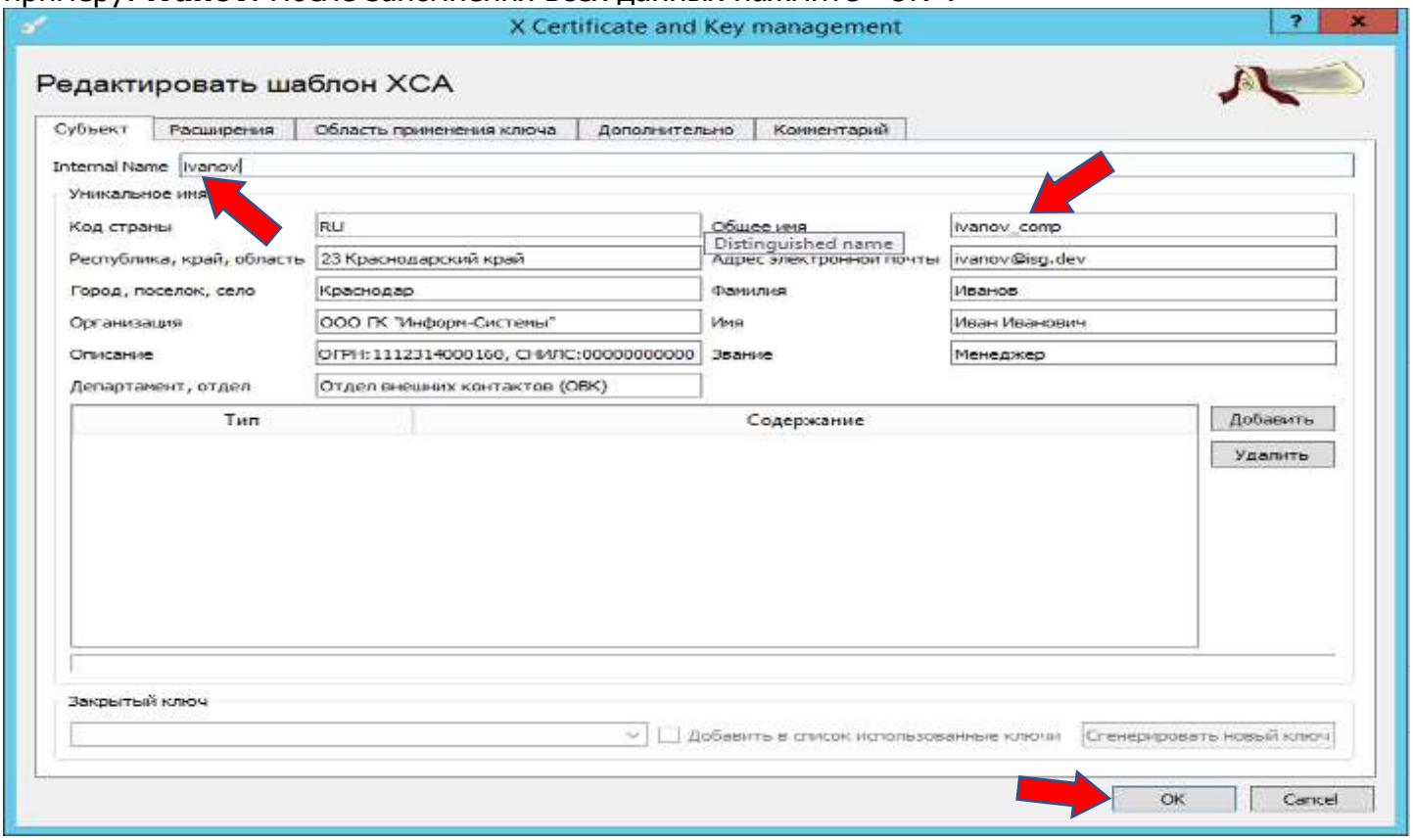
1.1 Для хранения закрытых ключей и генерации запросов сертификатов группа использует open-source приложение XCA. Скачайте шаблон хранилища сертификатов (https://ftp.isg.dev/certs/isg_default.xdb) и приложение «**XCA**» под вашу операционную систему (https://hohnstaedt.de/xca/index.php/download). Переименуйте шаблон базы данных в личный, к примеру: **isg_ivanov.xdb,** переместите в надежную директорию, желательно зашифрованную. Установите приложение «**XCA**» в систему, откройте установленное приложение, далее выберите *«Файл»* -> *«Open DataBase»*, в появившемся окне укажите вашу базу данных (**isg_ivanov.xdb**) и нажмите «Открыть».



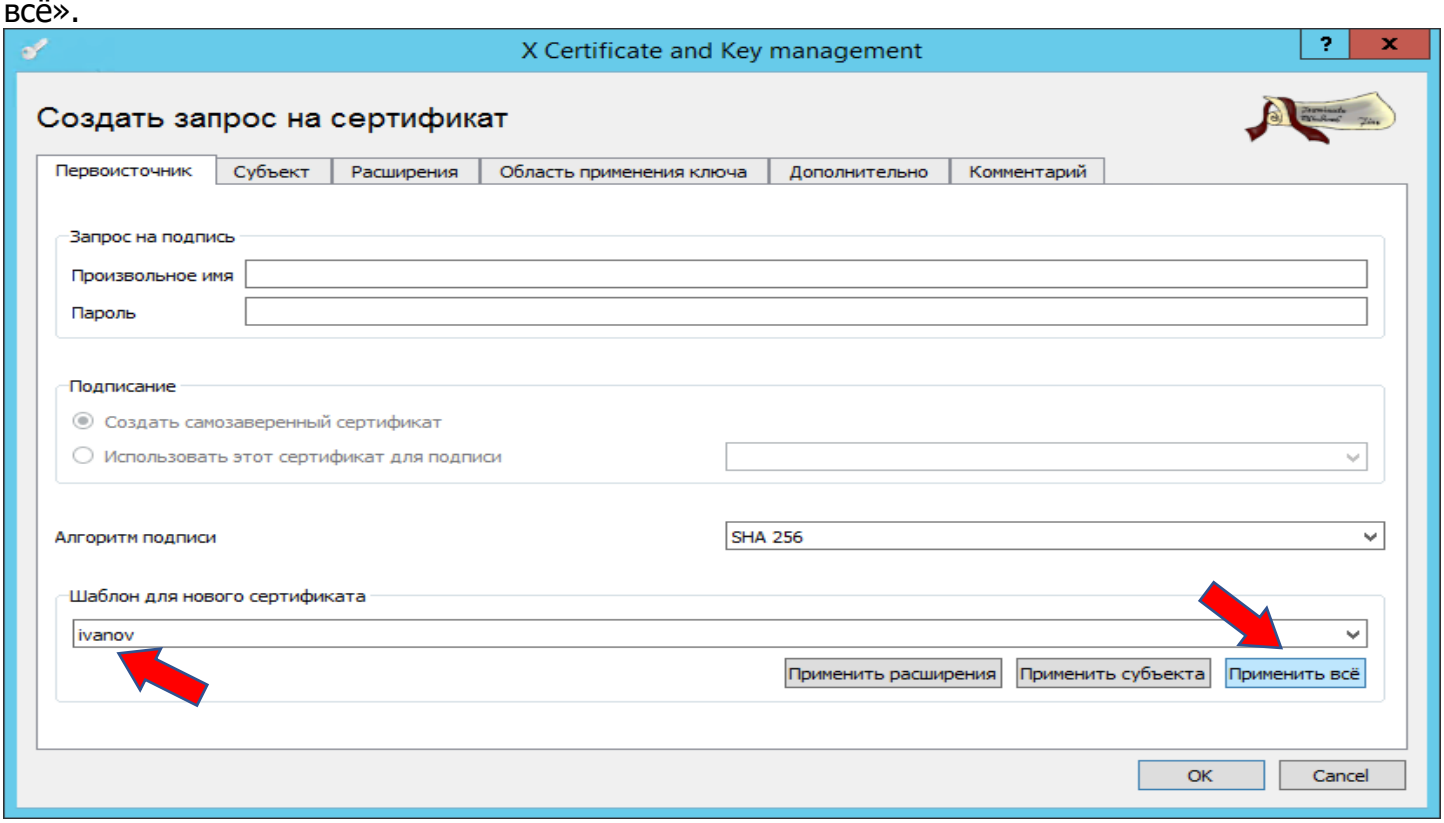
1.2 Выберите *«Дополнительно»* -> *«Изменить пароль базы данных»* и смените пароль на личный, с достаточным уровнем сложности, содержащий не менее 8 символов разного регистра, цифры и символы.



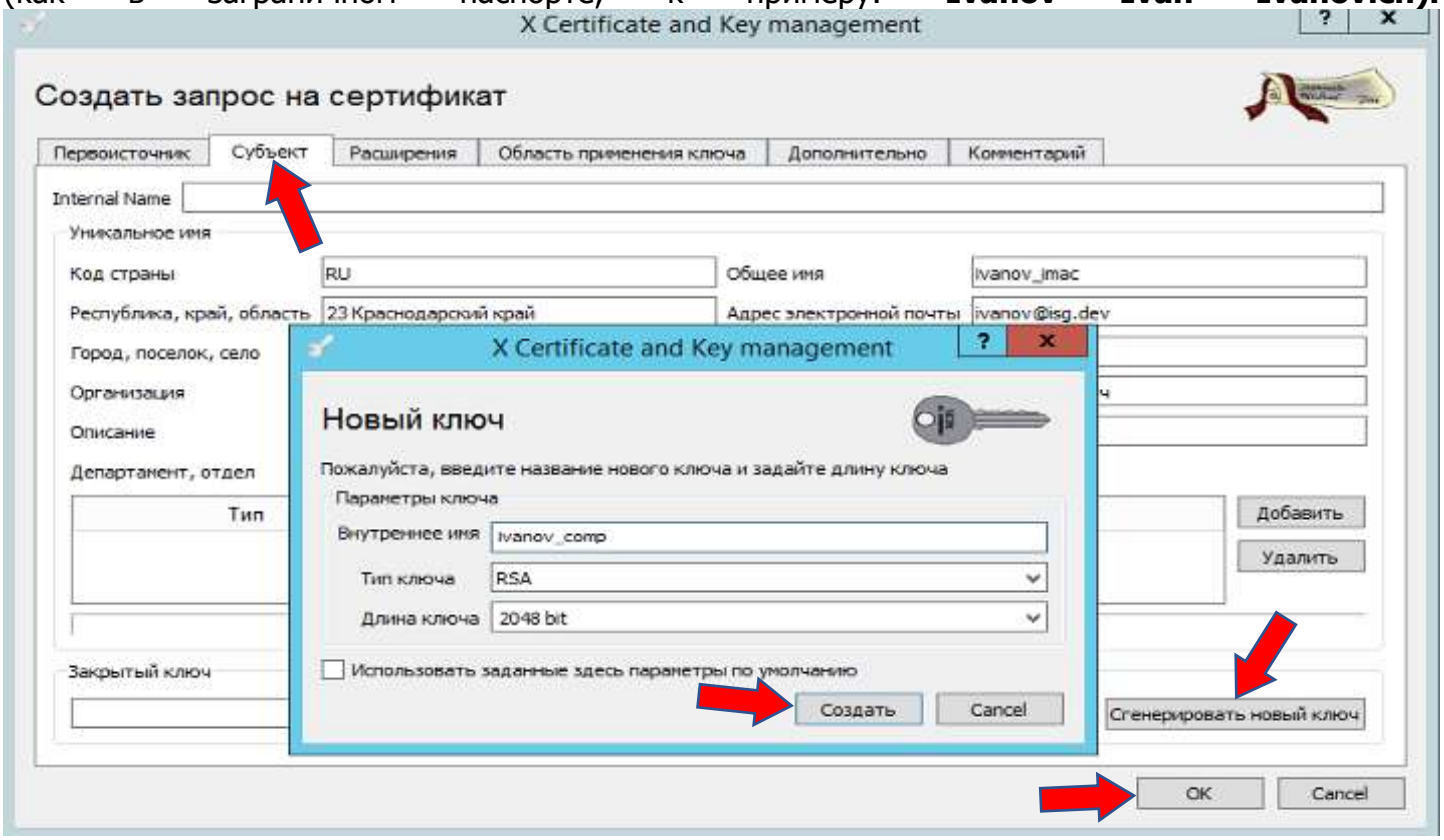
1.3 Перейдите на вкладку «Шаблоны», выберите шаблон ISG, нажмите «Изменить шаблон». Замените все данные на ваши. Для VPN доступа с вашего устройства в поле «Общее имя» указывается фамилия на английском языке, после чего через «нижние подчеркивание» тип вашего устройства, к примеру: **ivanov_comp** – для стационарных компьютеров, **ivanov_book** – для ноутбуков, **ivanov_tablet** – для планшетов, **ivanov_phone** – для мобильных телефонов и смартфонов. В поле «Internal Name» так же укажите свою фамилию латинскими буквами, к примеру: **ivanov**. После заполнения всех данных нажмите «ОК».



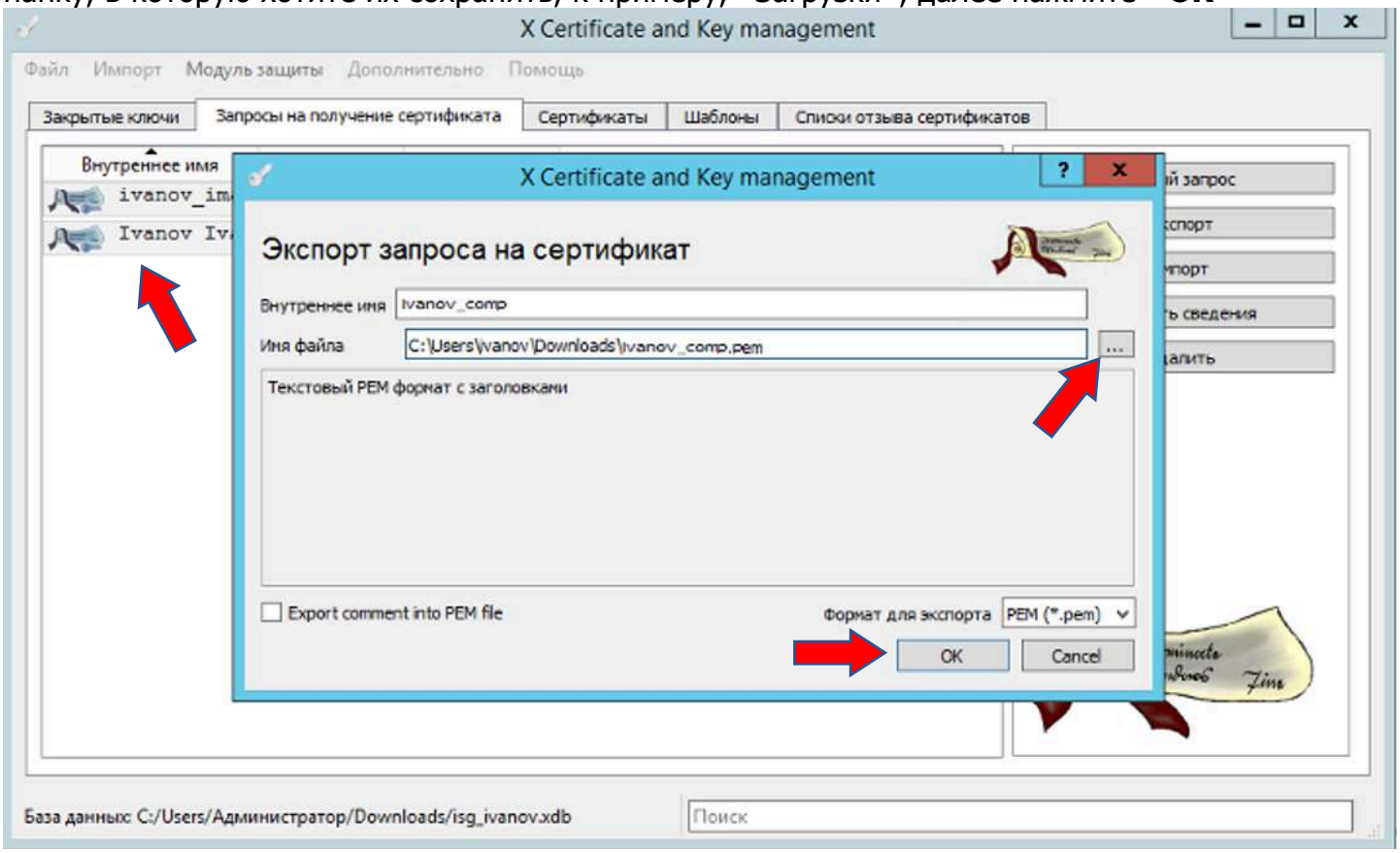
1.4 Перейдите на вкладку **«Запросы на получение сертификата»** и нажмите на кнопку «Новый запрос». В выпадающем меню появившегося окна выберите «Шаблон для нового сертификата» - только что измененный шаблон с Вашей фамилией, нажмите кнопку «Применить всё».



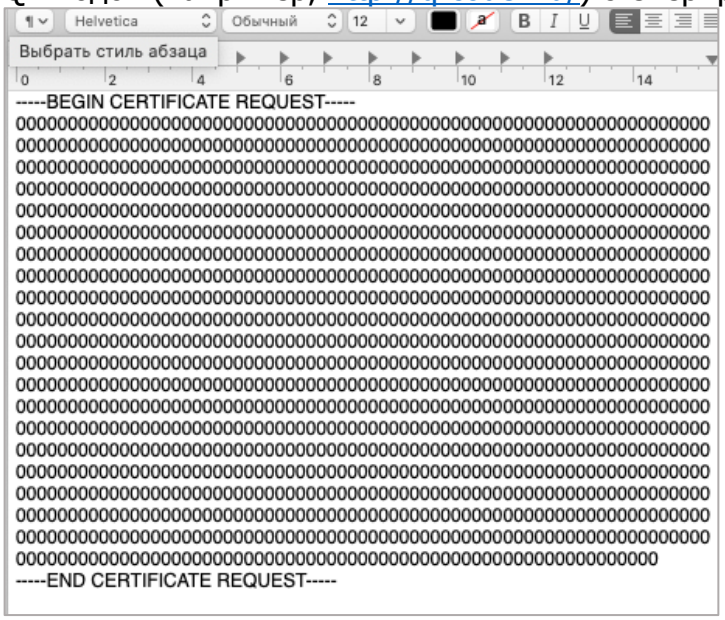
Перейдите на вкладку «Субъект», в нижней части окна нажмите **«Сгенерировать новый ключ» -> «Создать»,** далее **«Ок»**. В списке появится запрос сертификата открытого ключа (для VPN). Для генерации запроса сертификата ЭЦП повторите действия с п.1.4, заменив текст на вкладке «Субъект», в графе **«Общее имя»** на «Фамилию Имя Отчество» латинскими буквами (как в заграничном паспорте, к примеру: **Ivanov Ivan Ivanovich).**



1.5 Выберите Ваши запросы и нажмите кнопку **«Экспорт».** В открывшемся окне выберите папку, в которую хотите их сохранить, к примеру, «Загрузки», далее нажмите **«ОК»**

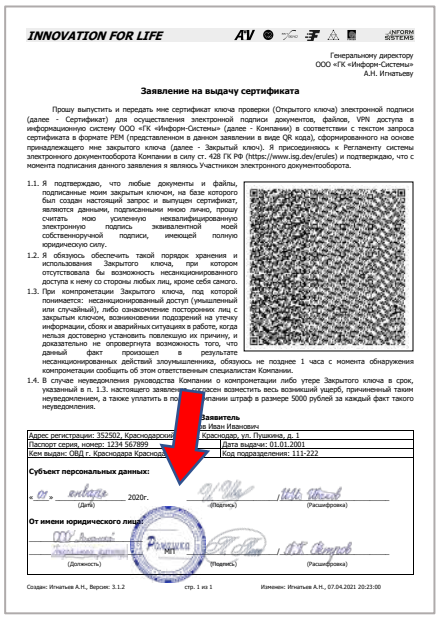


1.6 Откройте сохраненный запрос сертификата в любом текстовом редакторе (например, «WordPad», TextEdit), скопируйте весь содержащийся в нем текст, после в онлайн-генераторе QR-кодов (например, http://qrcoder.ru/) сгенерируйте из него QR код и сохраните изображение.



1.7 Скачайте на ftp сервере группы (https://ftp.isg.dev/request/) заявление на выдачу сертификата для сотрудников (access_request_employee.docx), либо для партнеров (access_request_partner.docx). Ознакомьтесь со всеми пунктами заявления и замените выделенный красным текст на Ваши данные. Для сотрудников группы поля «Организация», «ИНН», «ОГРН» - остаются неизменны, в то время как для партнеров в данных полях указываются данные Вашей организации.

1.8 Удалите выделенный красным «шаблон» QR-кода и вставьте на его место ваш QR-код с запросом VPN (режим обтекания - «Перед текстом», размер 8x8 см). Уберите красное выделение во всем документе, распечатайте, синей ручкой поставьте дату, подпись и расшифровку подписи, для партнеров – дополнительно подпишите у директора и поставьте печать организации. **Повторите пункты 1.6-1.8** для подготовки второго заявления на сертификат ЭЦП. Сохраните 2 заполненных заявления на своем компьютере.



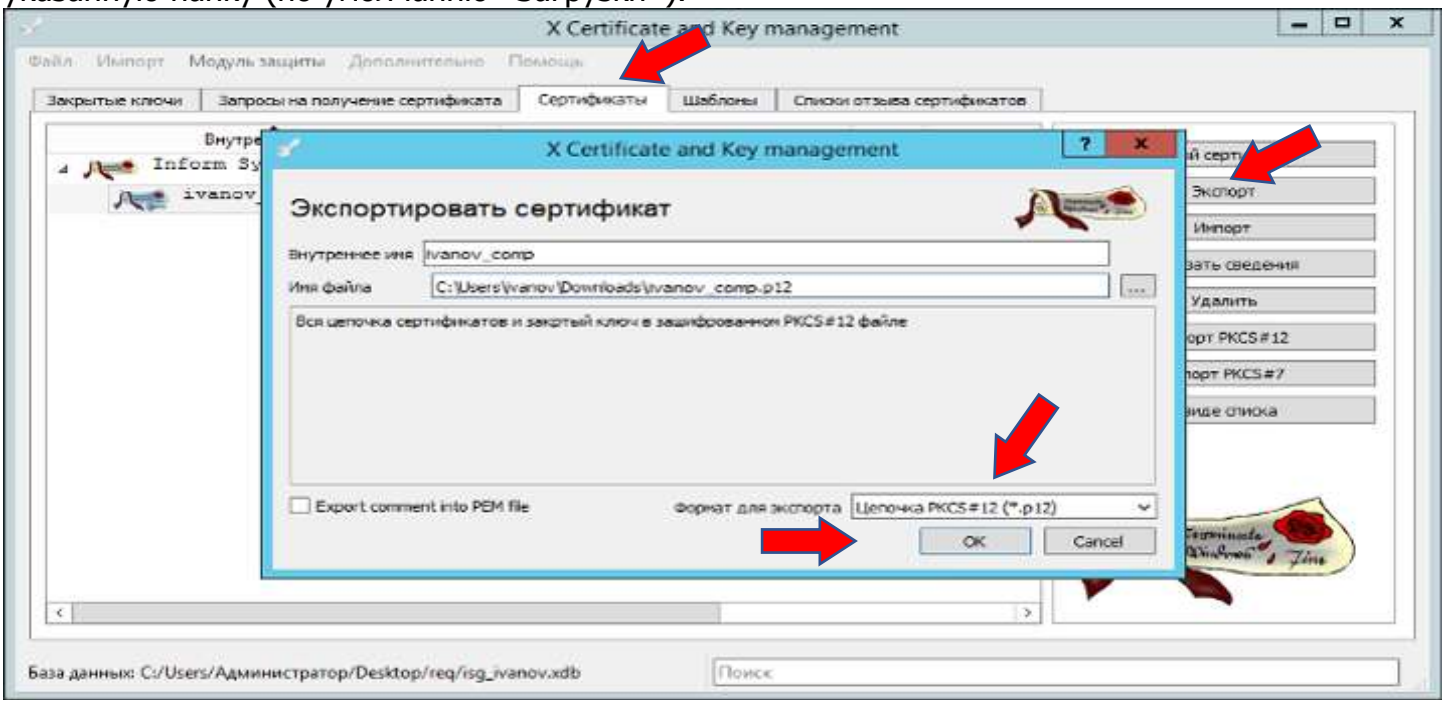
Передайте 2 оригинала заявления (для VPN доступа и ЭЦП) в службу поддержки Группы компаний «Информ-Системы»: +7 (861) 201-12-21.

1.9 Получите от службы поддержки сертификаты открытых ключей в формате *.crt и импортируйте их в личную базу сертификатов в приложении **«XCA»** (*«Файл» -> «Open DataBase» «Сертификаты» -> «Импорт»*).

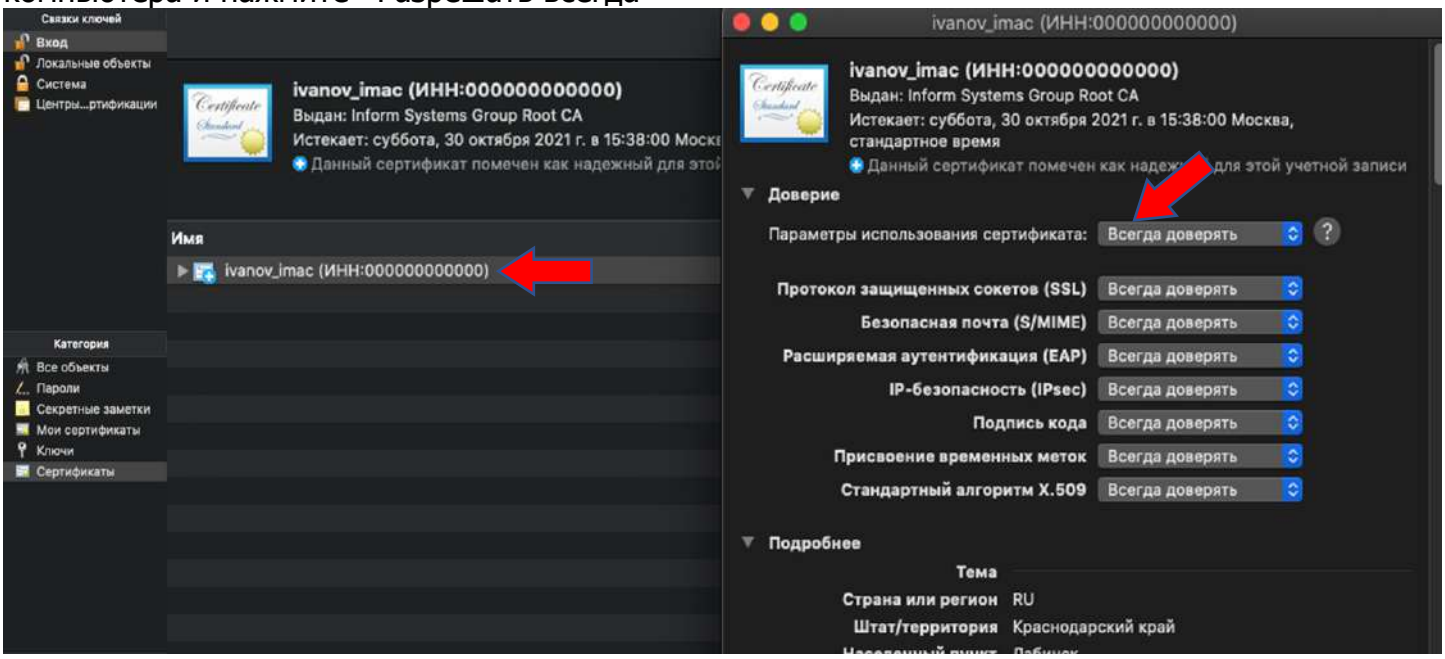
Поздравляем! Вы получили сертификаты открытых ключей для VPN доступа и подписи документов, а также импортировали их в собственное хранилище сертификатов. Для обеспечения сохранности базы данных, созданной в пункте 1.2, к примеру: **isg_ivanov.xdb**, сохраните ее на шифрованном диске и используйте в будущем для создания новых запросов с уже заполненным шаблоном ваших данными.

2. Настройка VPN подключения в MAC OS X:

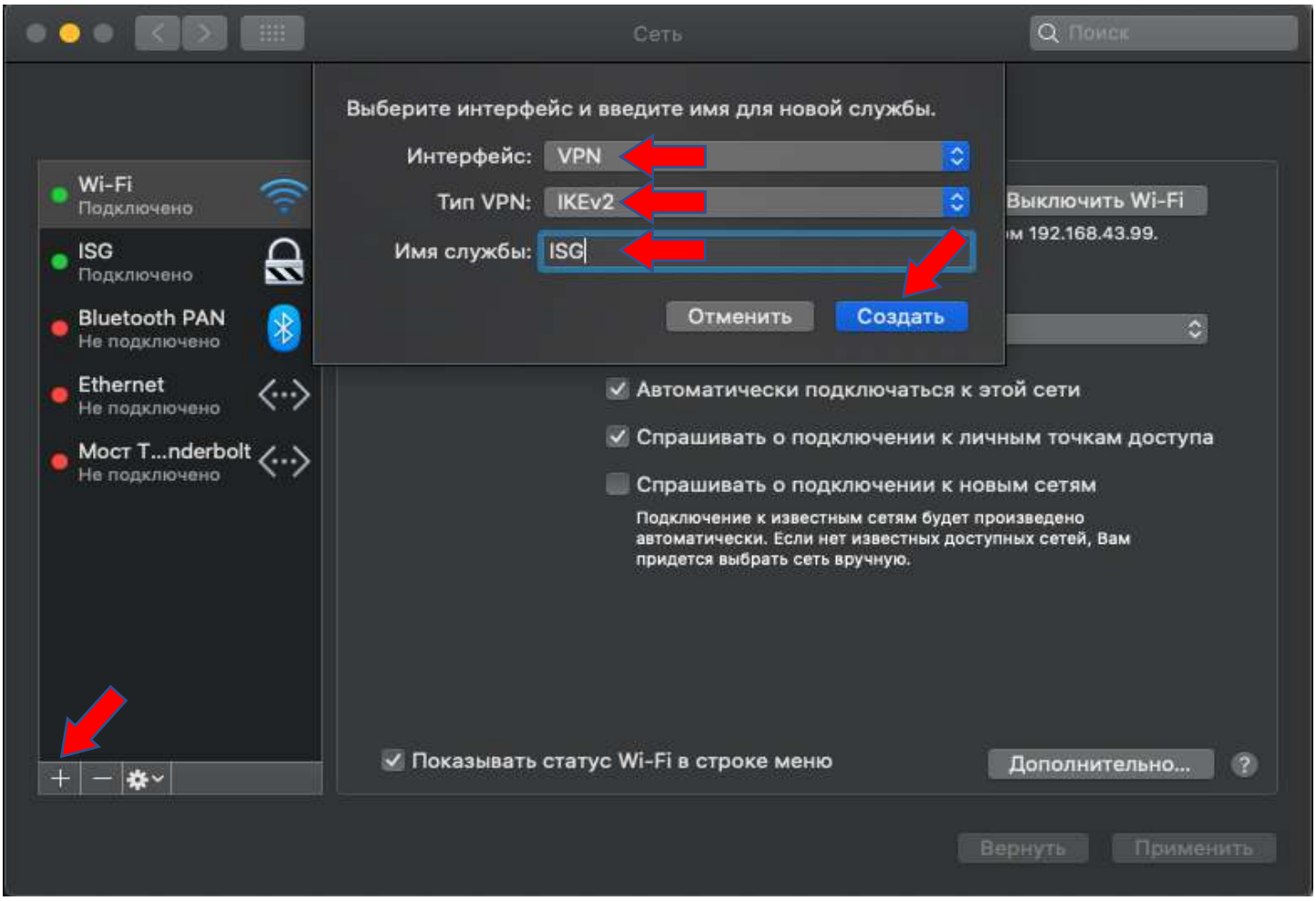
2.1 Войдите в приложение **«XCA»**, откройте вкладку **«Сертификаты»**, нажмите «Экспорт», укажите «Формат для экспорта» - Цепочка PKCS #12 (*.p12) и нажмите «OK», после чего произойдет экспорт полной цепочки сертификатов и закрытого ключа в контейнере PKCS12 в указанную папку (по умолчанию «Загрузки»).



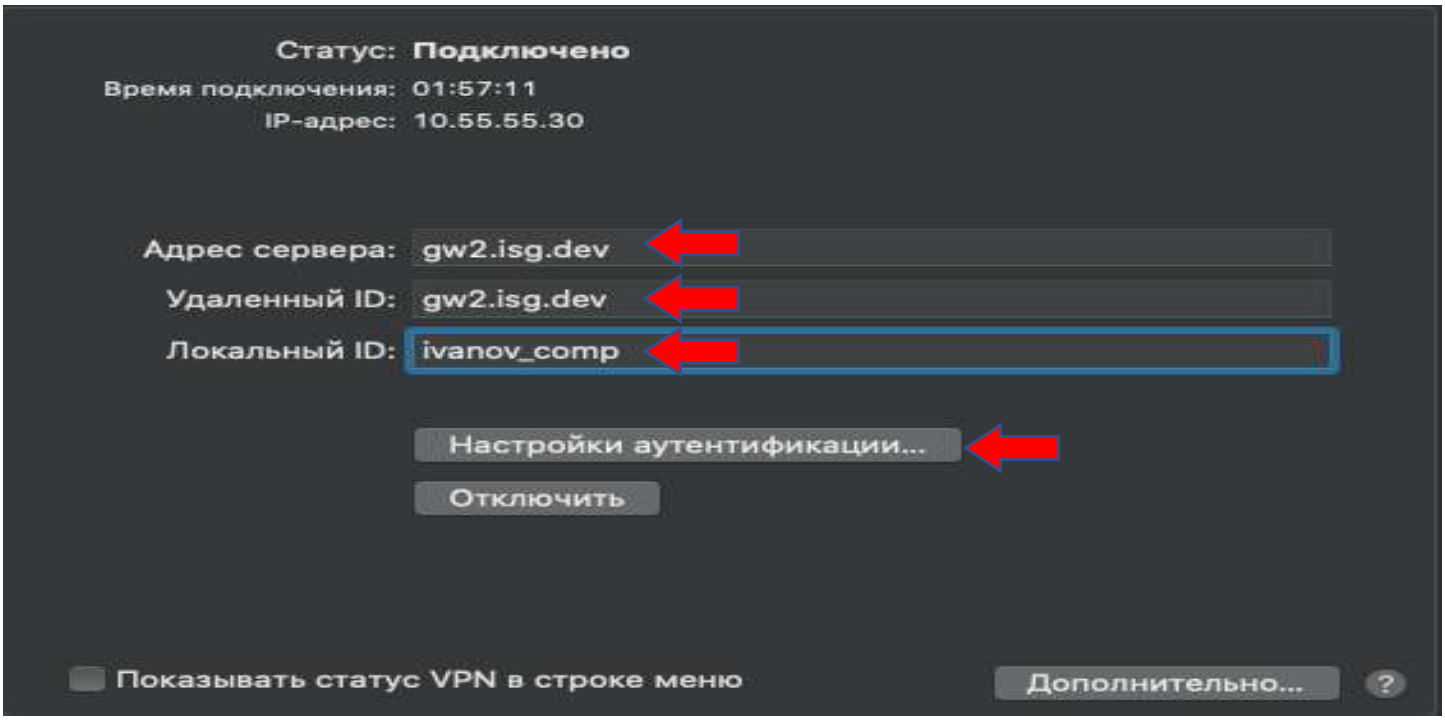
2.2 Откройте в «Связке ключей» экспортированный контейнер PKCS12, к примеру, **«ivanov_comp.p12»**, в блоке «Категория» выберите «Сертификаты», найдите сертификат с именем **«Inform Systems Group Root CA»**, нажмите на него правой кнопкой мыши -> *«Свойства»* -> *«Доверие»* и в строке «Параметры использования сертификата» выберите **«Всегда доверять»**, после чего подтвердите операцию паролем вашей учетной записи компьютера и нажмите «Разрешать всегда»



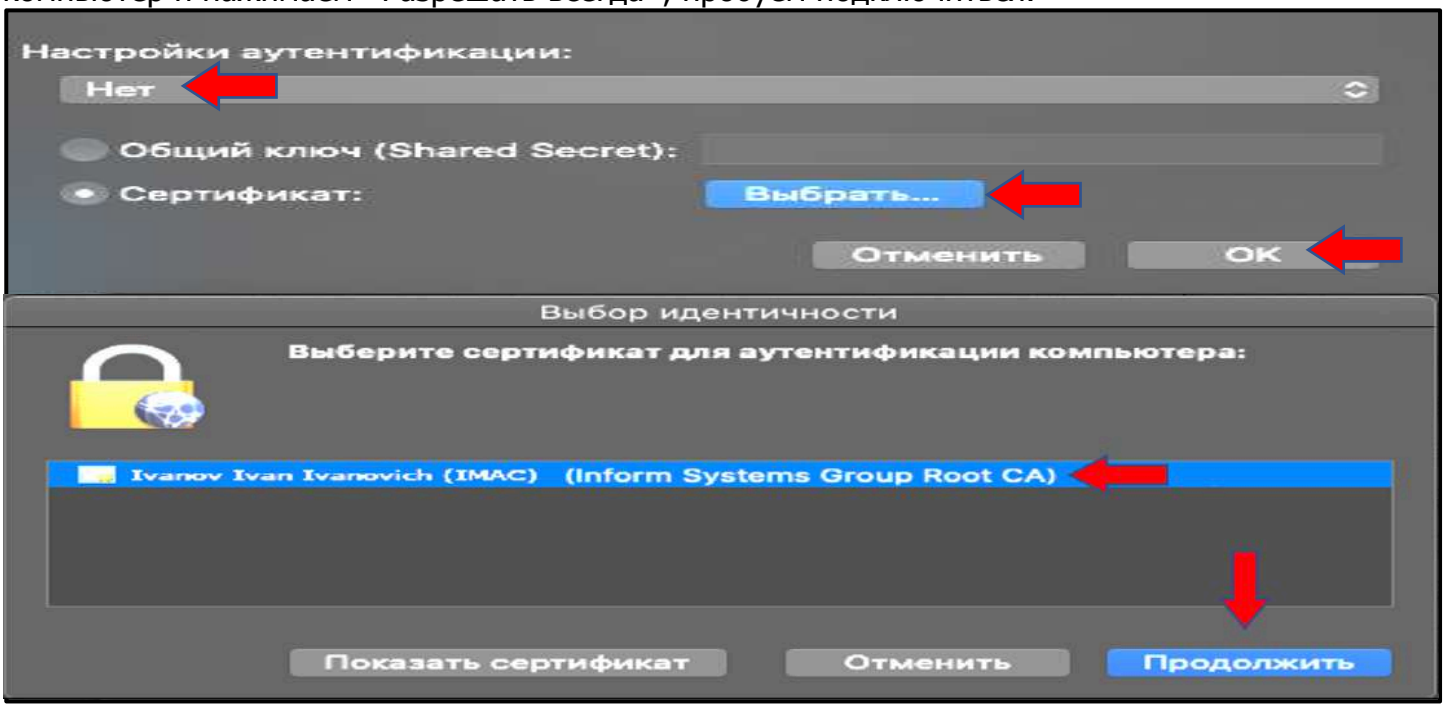
2.3 Откройте «Системные настройки» -> «Сеть» -> нажмите на «+» в нижней части окна, в строке «Интерфейс» выберите **«VPN»**, введите имя службы: ISG, тип: **IKEv2**, нажмите «Создать»:



2.4 Укажите «Адрес сервера» gw2.isg.dev и «Удаленный ID»: gw2.isg.dev, «Локальный ID»: Ваше «Общее имя», указанное при создании запроса на сертификат, к примеру: **ivanov_comp**, нажмите «Настройка аутентификации…»

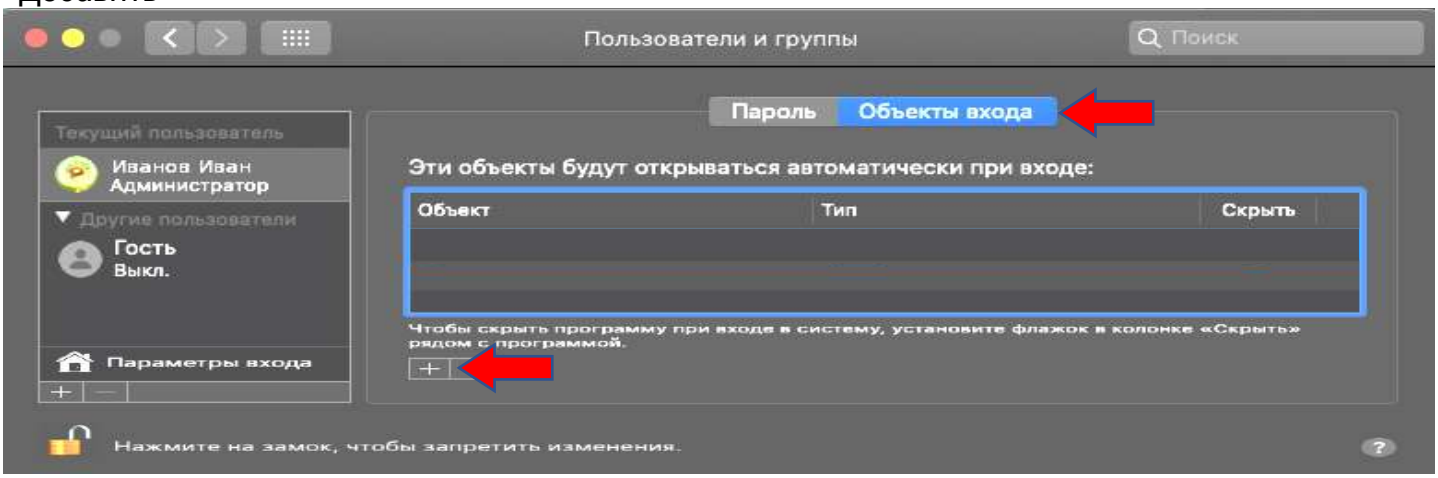


2.5 В настройках аутентификации вместо «Имя пользователя» необходимо выбрать «Нет», после чего напротив надписи «Сертификат» нажимаем «Выбрать», в списке выбираем ваш сертификат, нажимаем «Продолжить», «ОК», после «Применить», вводим пароль от входа в компьютер и нажимаем «Разрешать всегда», пробуем подключиться.



Если соединение было установлено и светится **«зеленым»**, значить все прошло успешно, иначе необходимо обратиться к операторам для оказания технической поддержки.

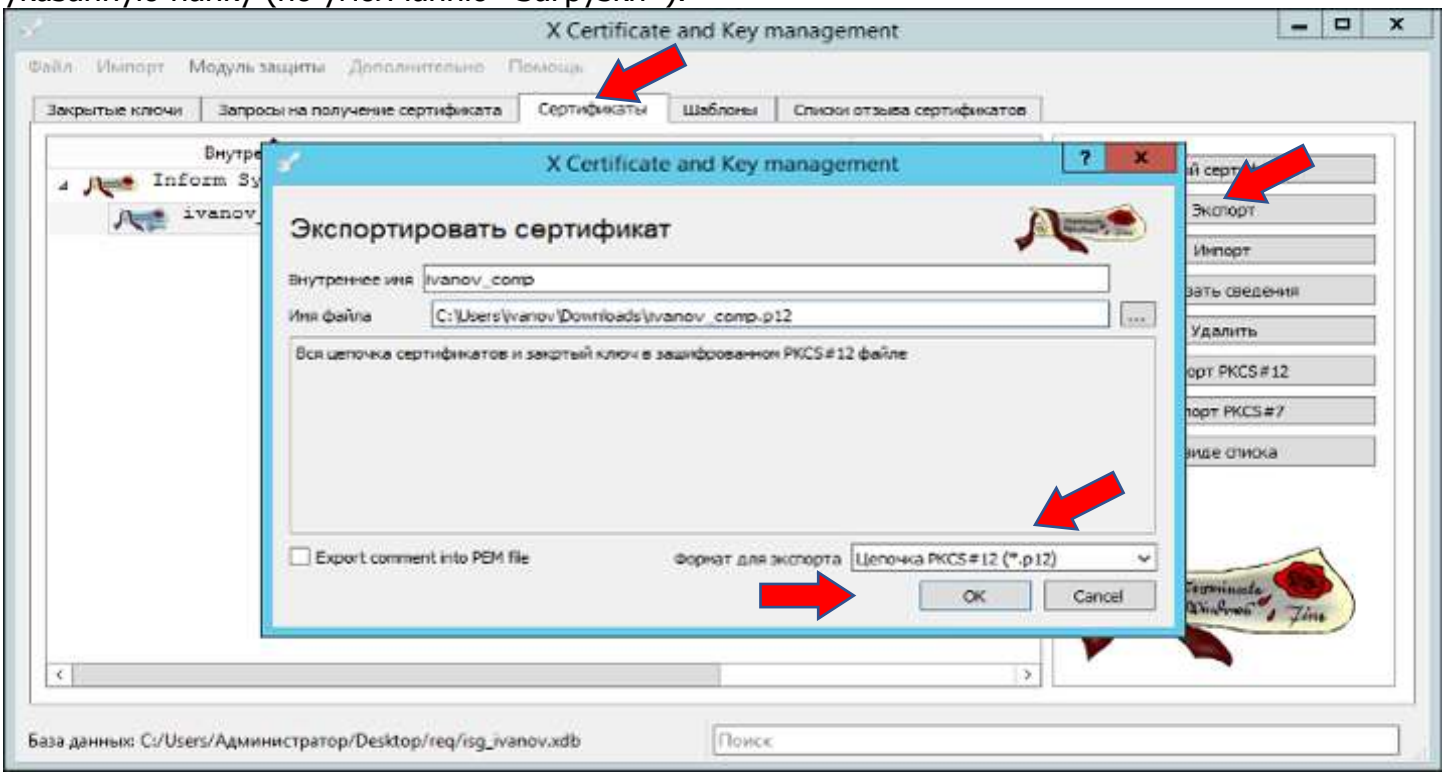
2.6 **Установка программы VPNStatus.** Данное приложение восстанавливает VPN соединение при его обрывах и позволяет всегда находится на связи. Скачайте приложение: https://ftp.isg.dev/soft/utils/vpnstatus.zip, распакуйте и перенесите в «Программы», после запустите его, попутно разрешая открывать приложения, скачанные из сети Интернет: в папке «Программы» удерживая на клавиатуре клавишу «Command» нажмите на иконку приложения VPNStatus правой кнопкой мыши, выберите «Открыть», в появившемся окне вновь выберите «Открыть». В правом верхнем углу появится иконка приложения с буквами VPN, нажмите на нее и установите галку **«Always auto connect»** — это поможет автоматически восстанавливать VPN соединение в случае его обрыва. Для автоматического запуска приложения при входе в систему зайдите в «Настройки» -> «Пользователи и группы» -> «Объекты входа» -> и в низу данной вкладки нажмите «+», далее из папки «Программы» выбрать «VPNStatus», и нажмите «Добавить»



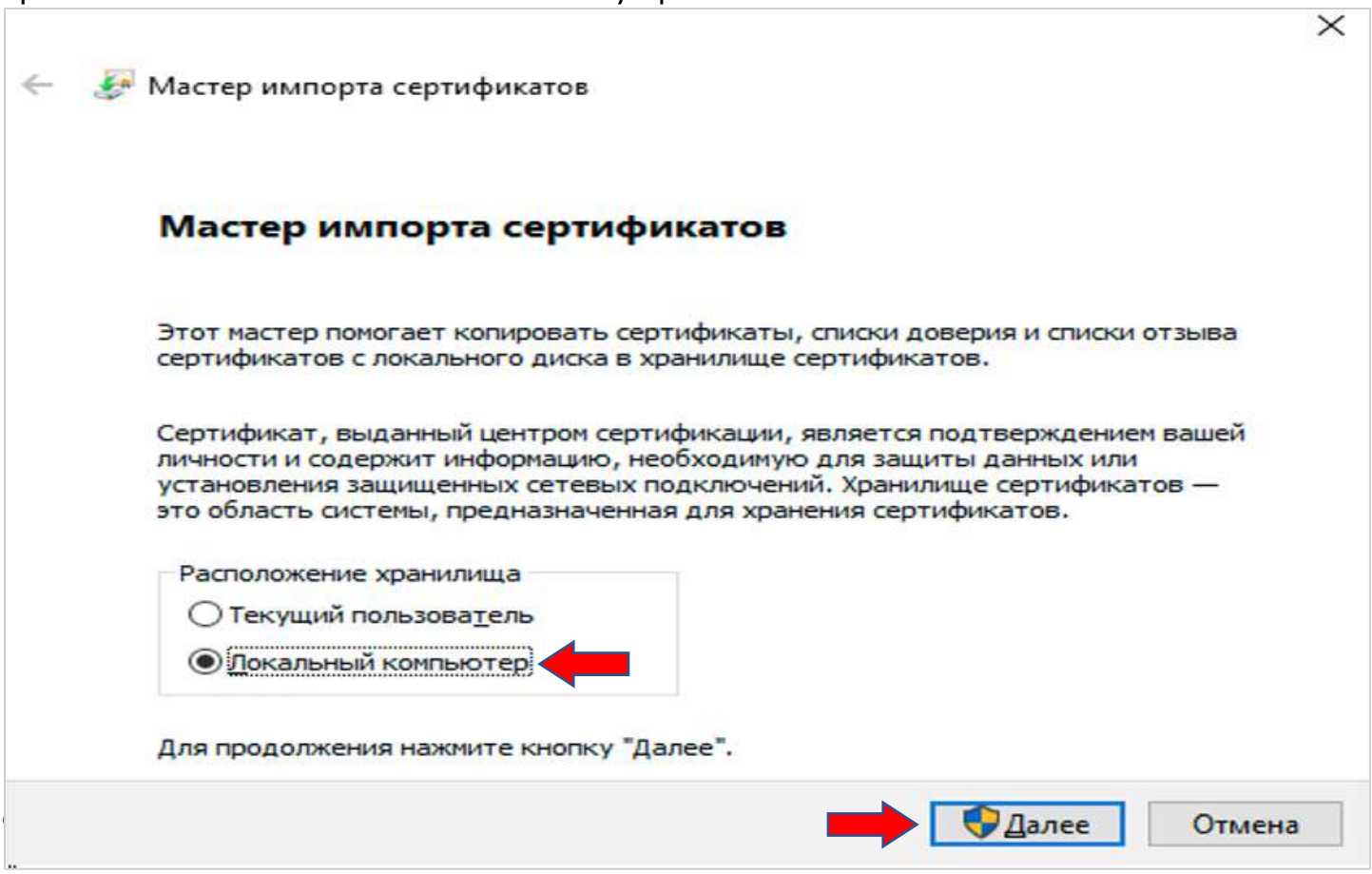
Поздравляем! Вы завершили настройку VPN-соединения. Для получения необходимых учетных записей и доступов к ресурсам группы заполните заявление, следуя инструкции на получение учетных записей: https://ftp.isg.dev/docs/instruction_account_request.pdf

3. Настройка VPN подключения в OS Windows:

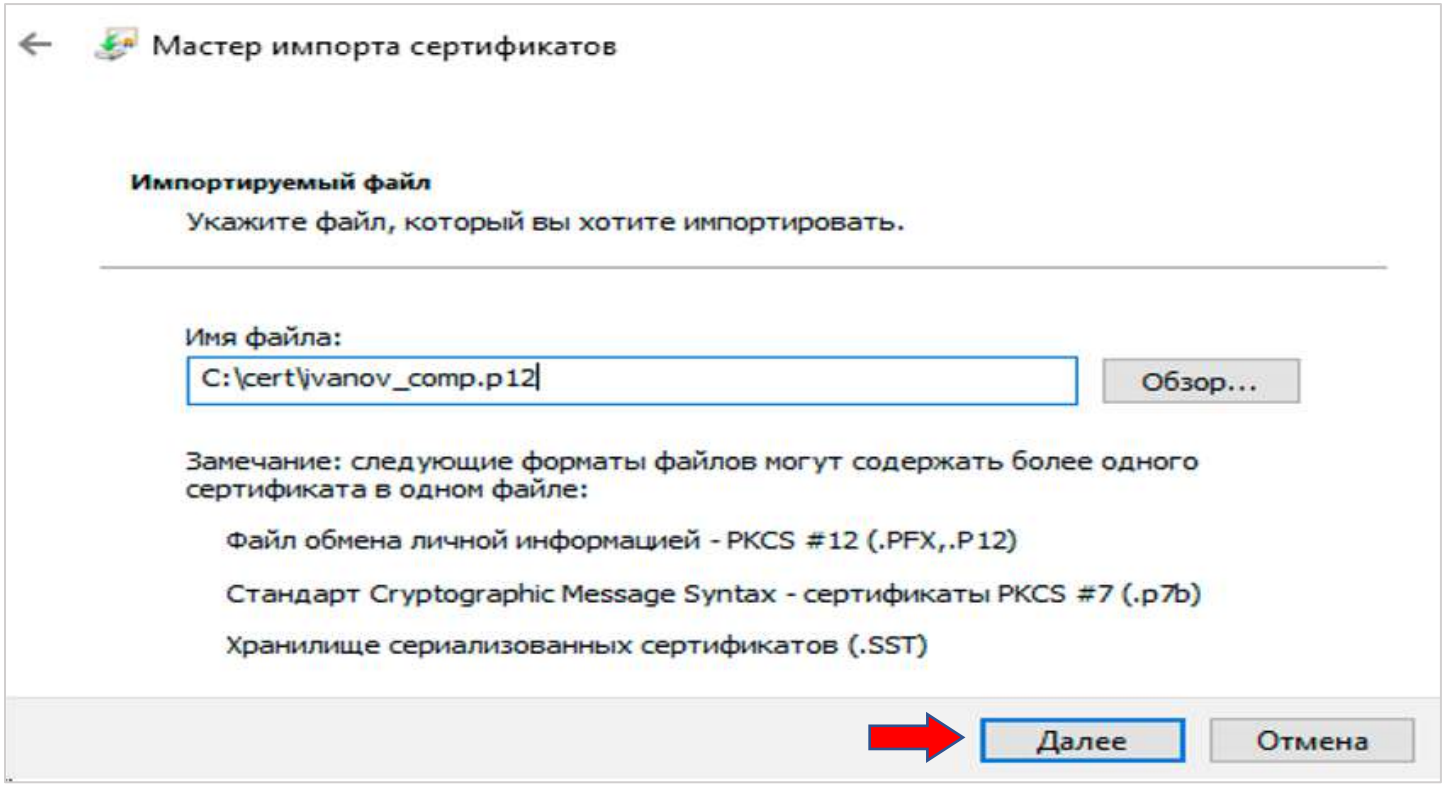
3.1 Войдите в приложение **«XCA»**, откройте вкладку **«Сертификаты»**, нажмите «Экспорт», укажите «Формат для экспорта» - Цепочка PKCS #12 (*.p12) и нажмите «OK», после чего произойдет экспорт полной цепочки сертификатов и закрытого ключа в контейнере PKCS12 в указанную папку (по умолчанию «Загрузки»).



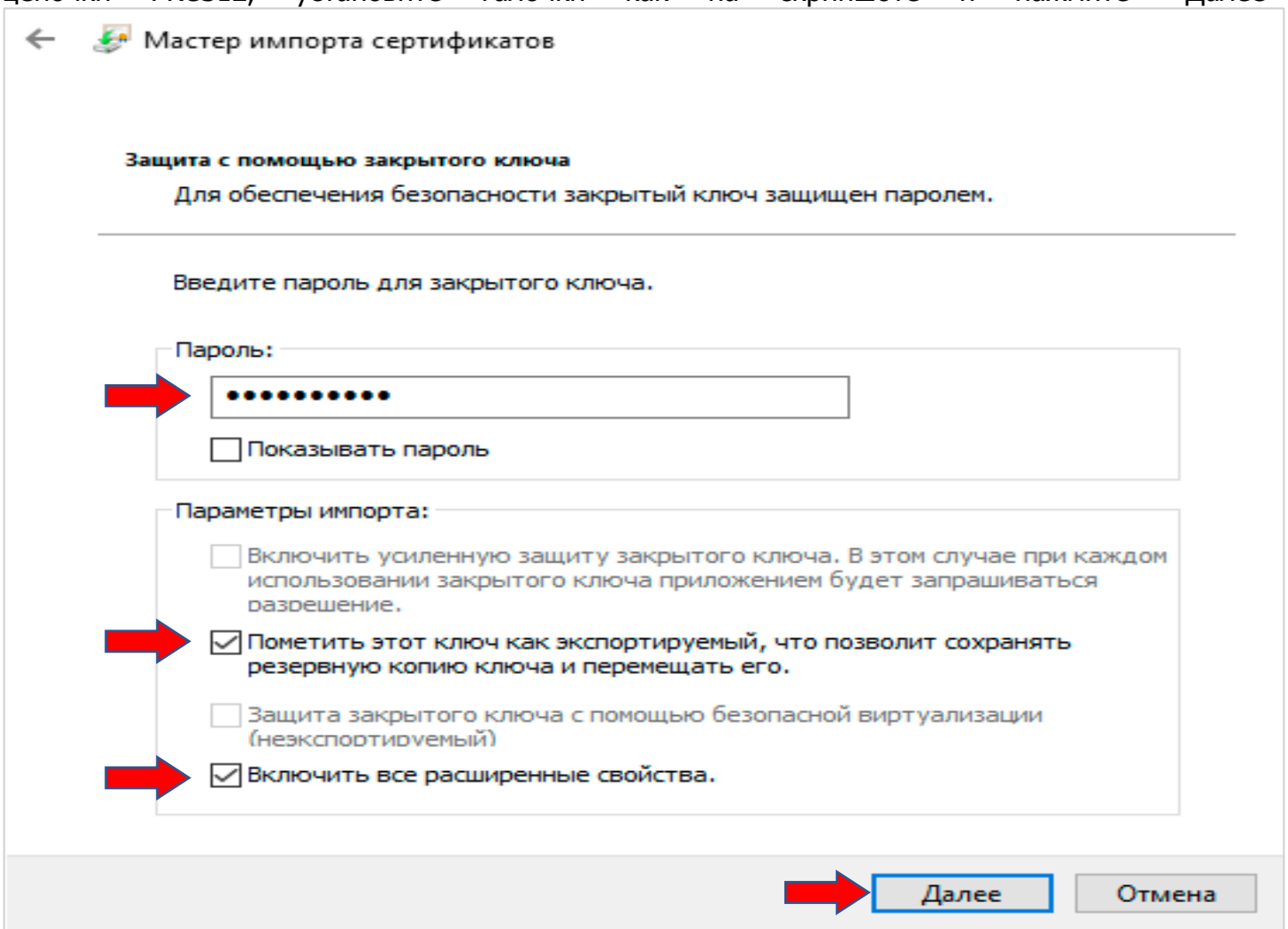
3.2 Откройте экспортированный контейнер PKCS12, к примеру, **«ivanov_comp.p12»**, в расположении хранилища выберите «Локальный компьютер», нажмите «Далее» и разрешите приложению вносить изменения на вашем устройстве.



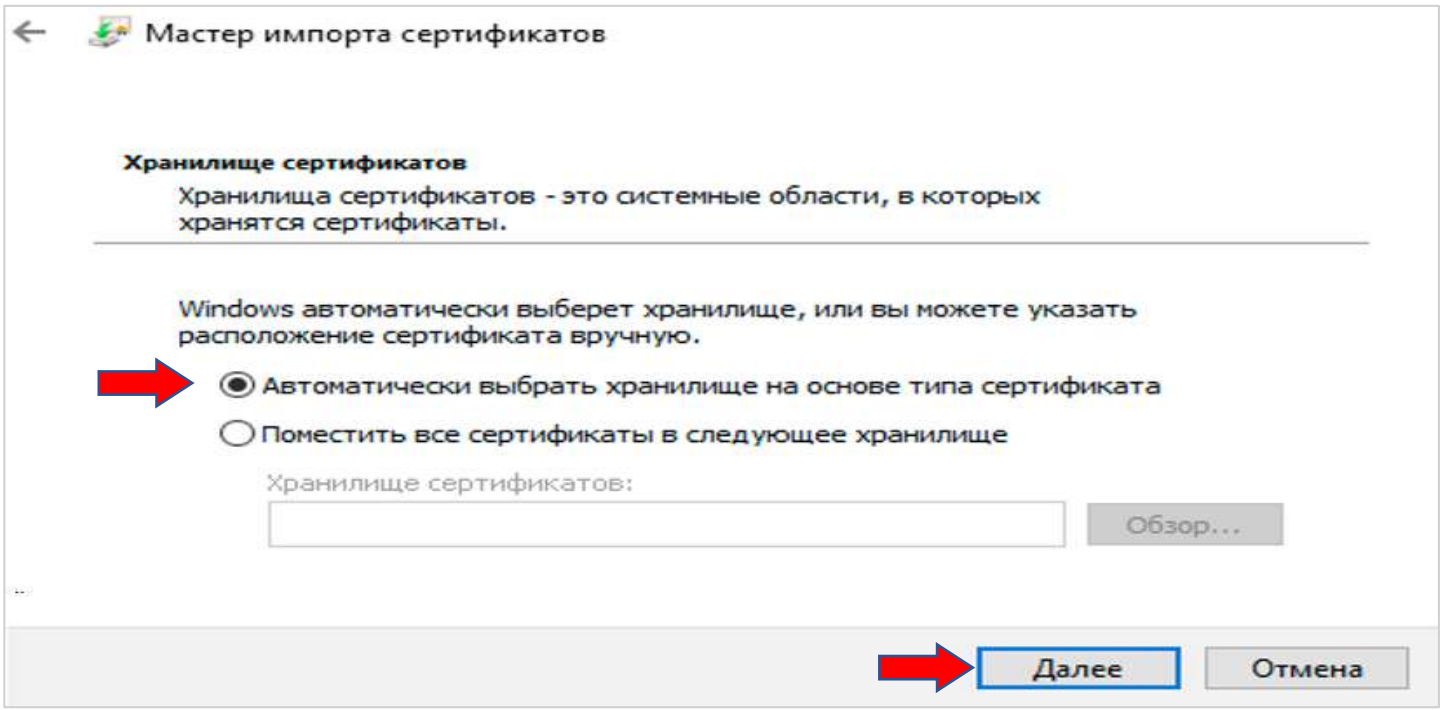
3.3 В следующем окне нажмите «Далее»



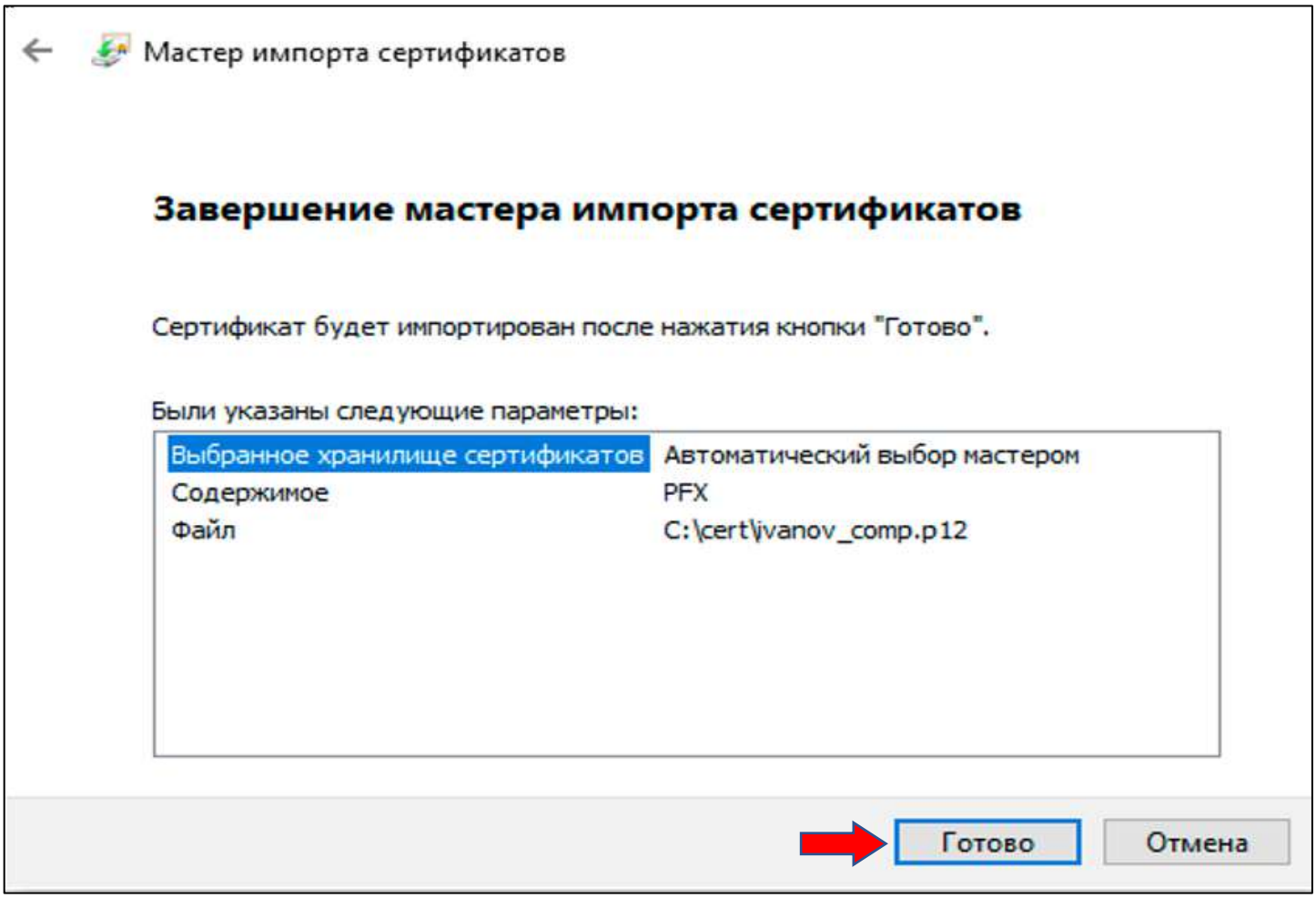
3.4 В следующем окне введите пароль от закрытого ключа, который указывали при выгрузке цепочки PKCS12, установите галочки как на скриншоте и нажмите «Далее»



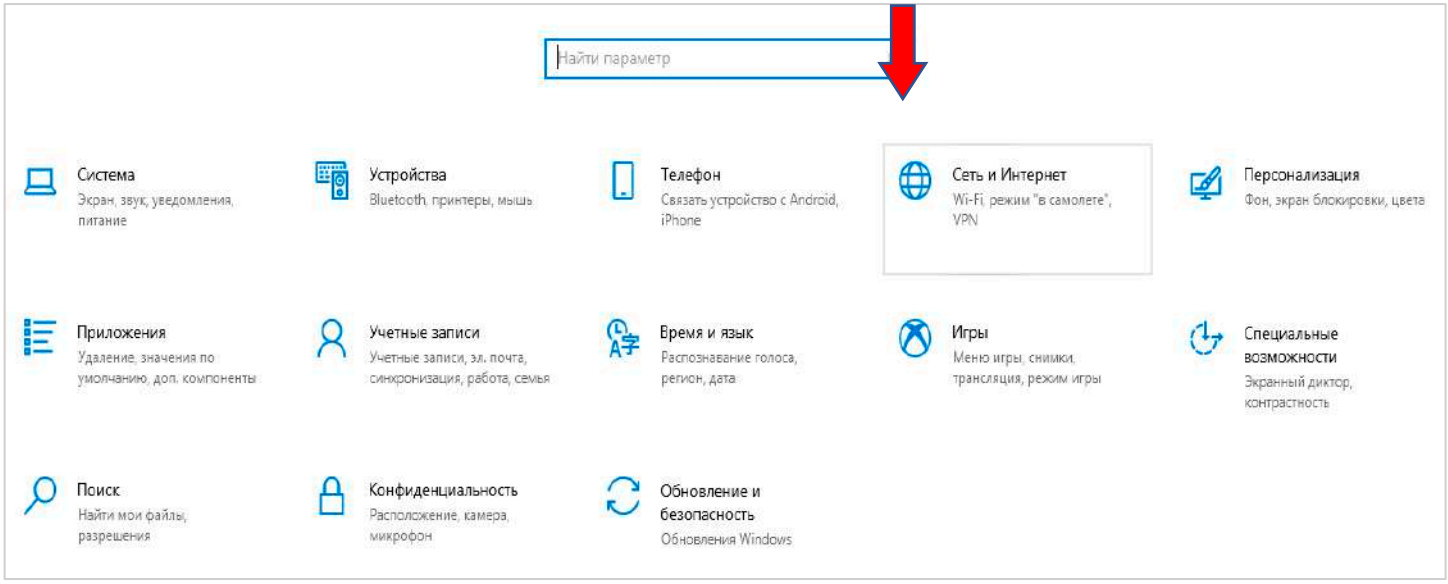
3.5 В следующем окне выберите пункт «Автоматически выбирать хранилище на основе типа сертификата» и нажмите «Далее»



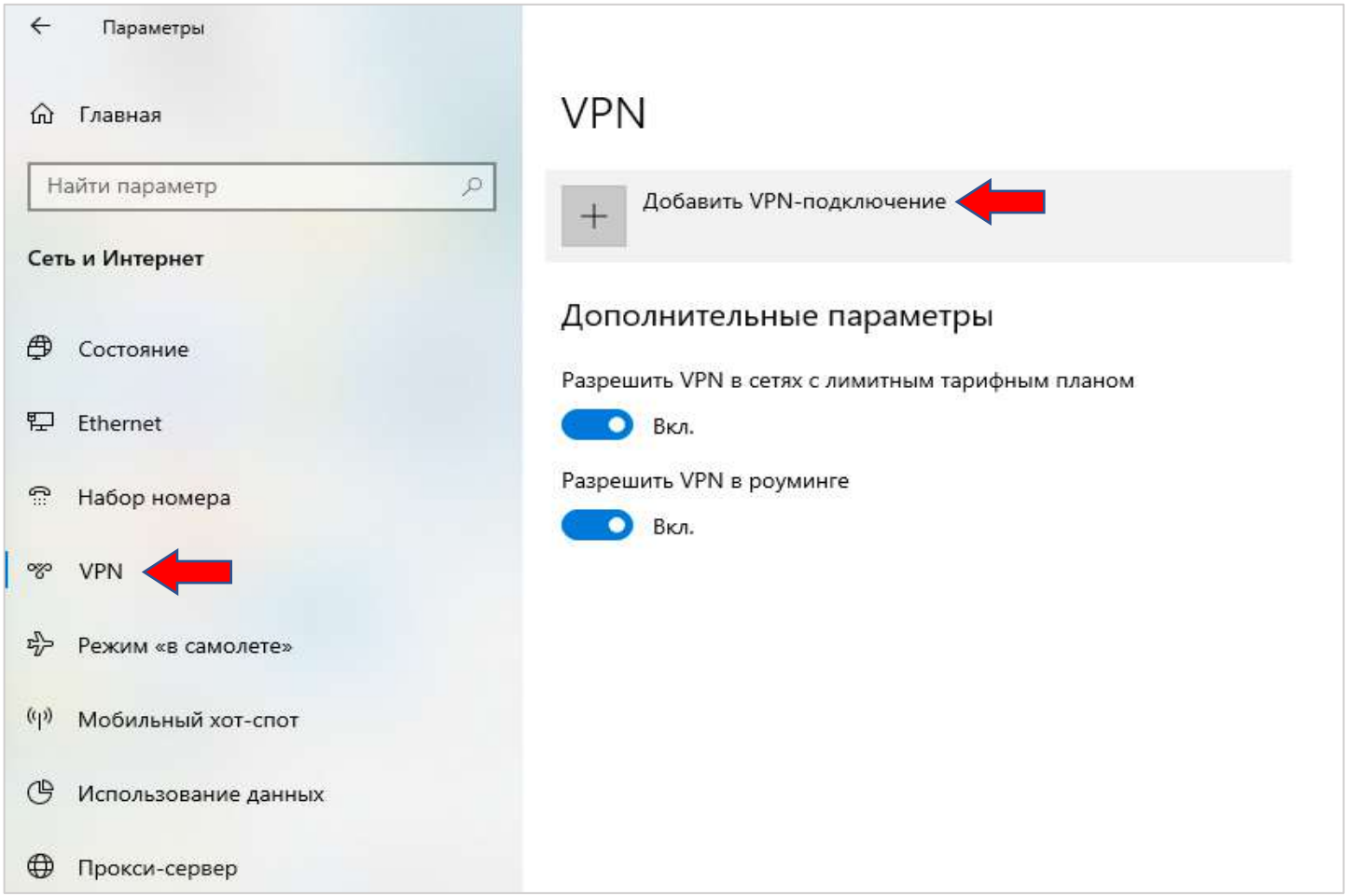
3.6 В следующем окне нажмите «Готово» и дождитесь всплывающего сообщения «Импорт успешно выполнен»



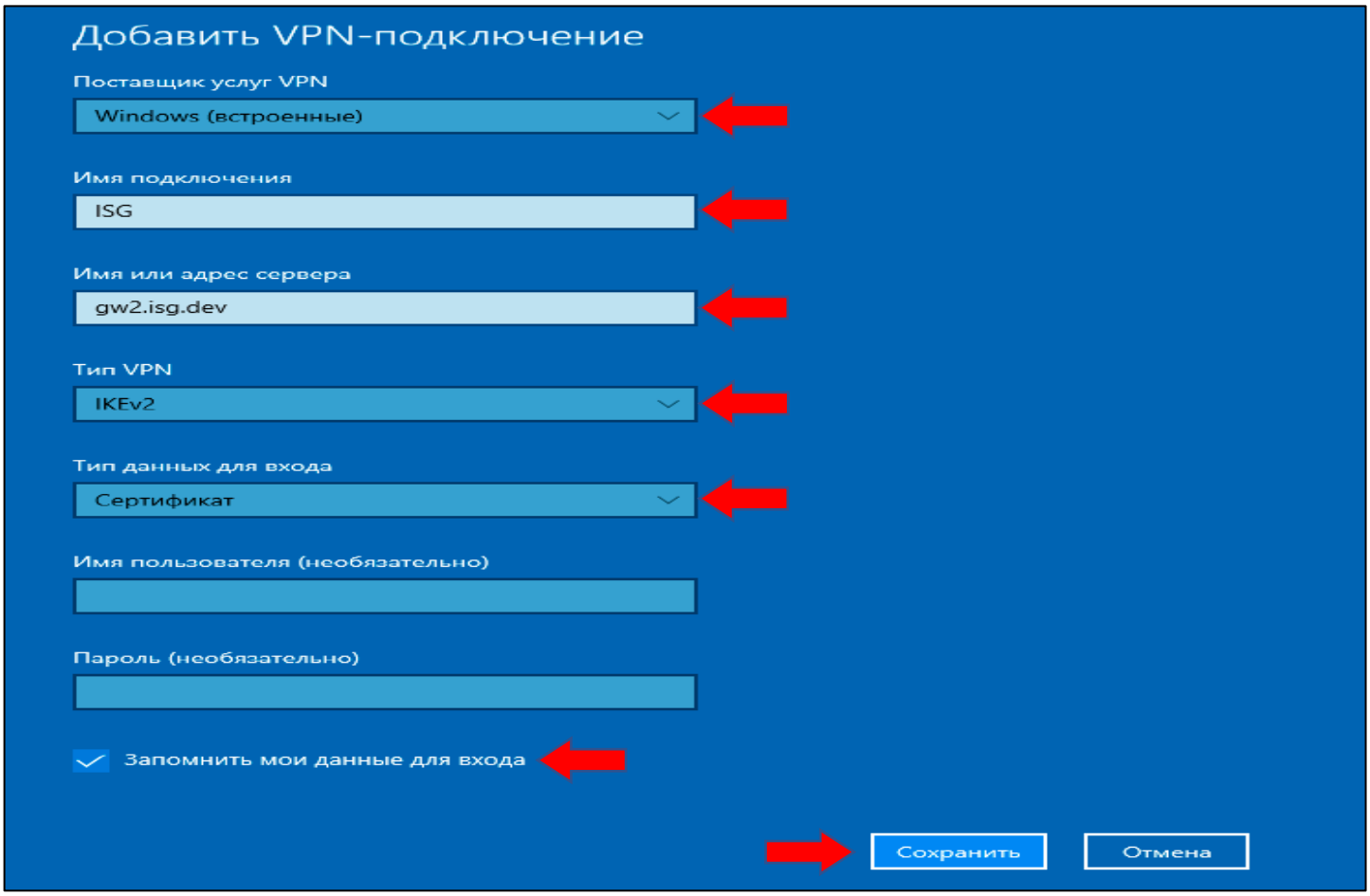
3.7 Для настройки VPN соединения выбирайте «Пуск» -> «Параметры» -> «Сеть и интернет»



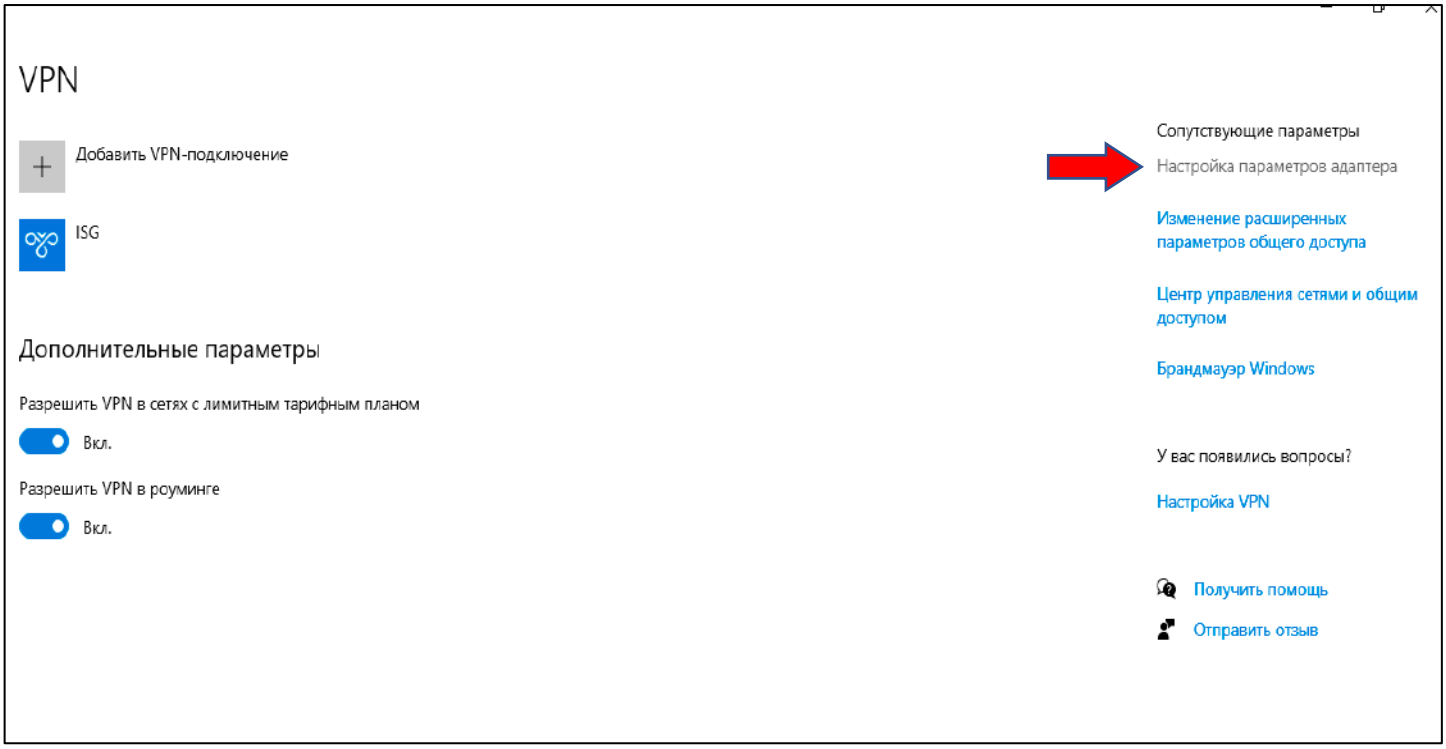
3.8 Далее выбираете «VPN» -> «Добавить VPN соединение»



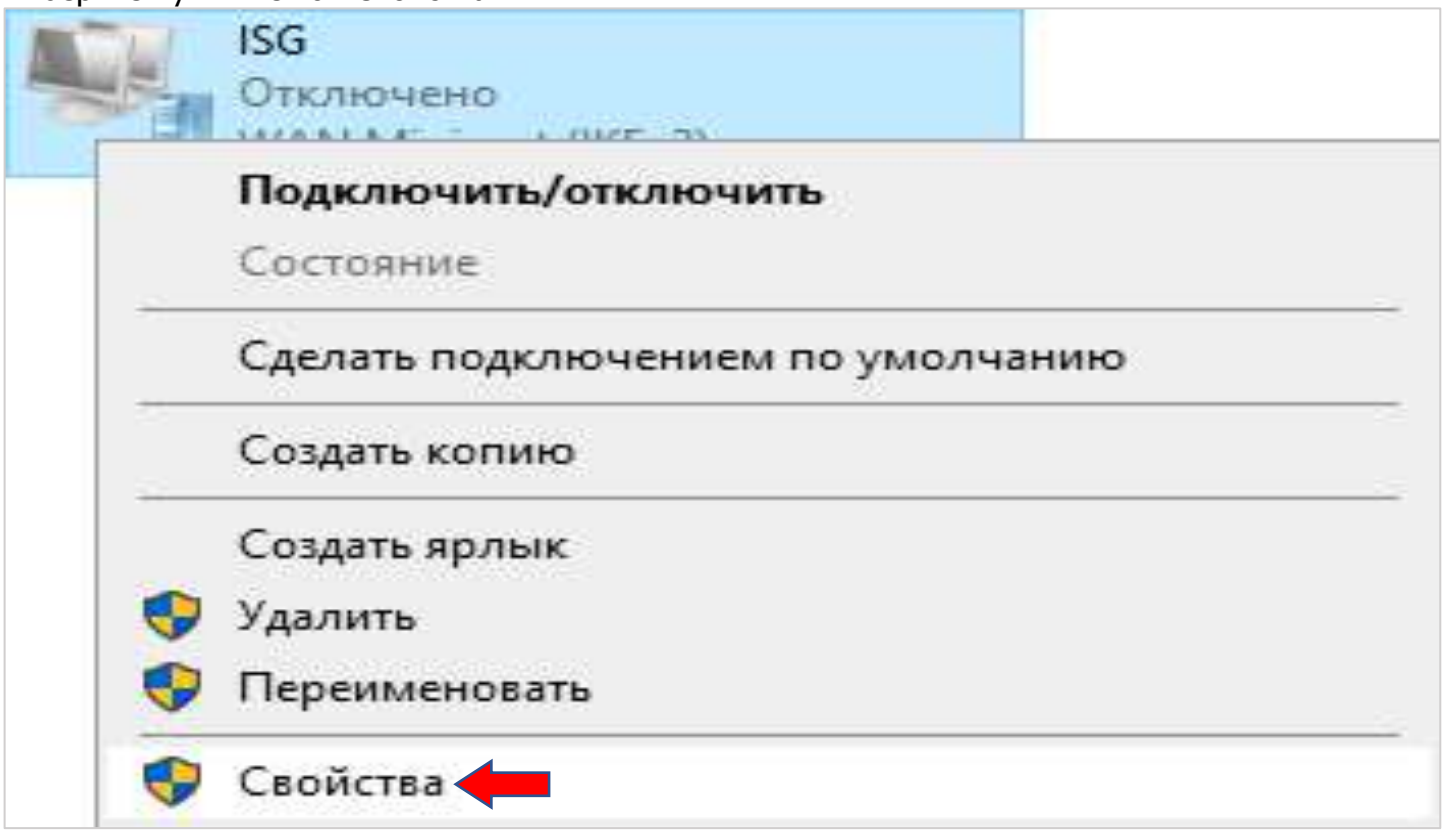
3.9 Заполните все поля как на скриншоте и нажмите «Сохранить»



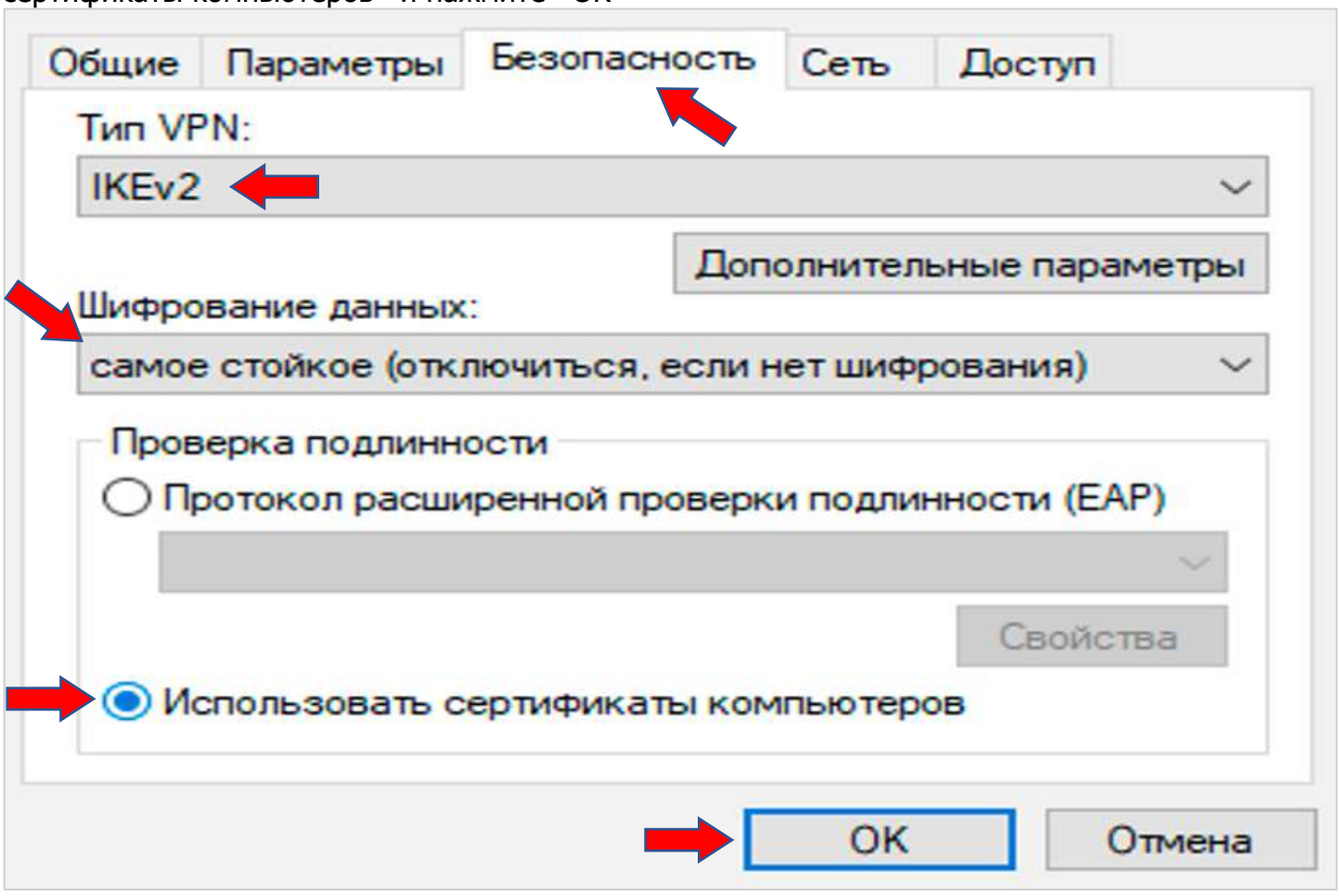
3.10 В блоке «Сопутствующие параметры» откройте «Настройки параметров адаптера»



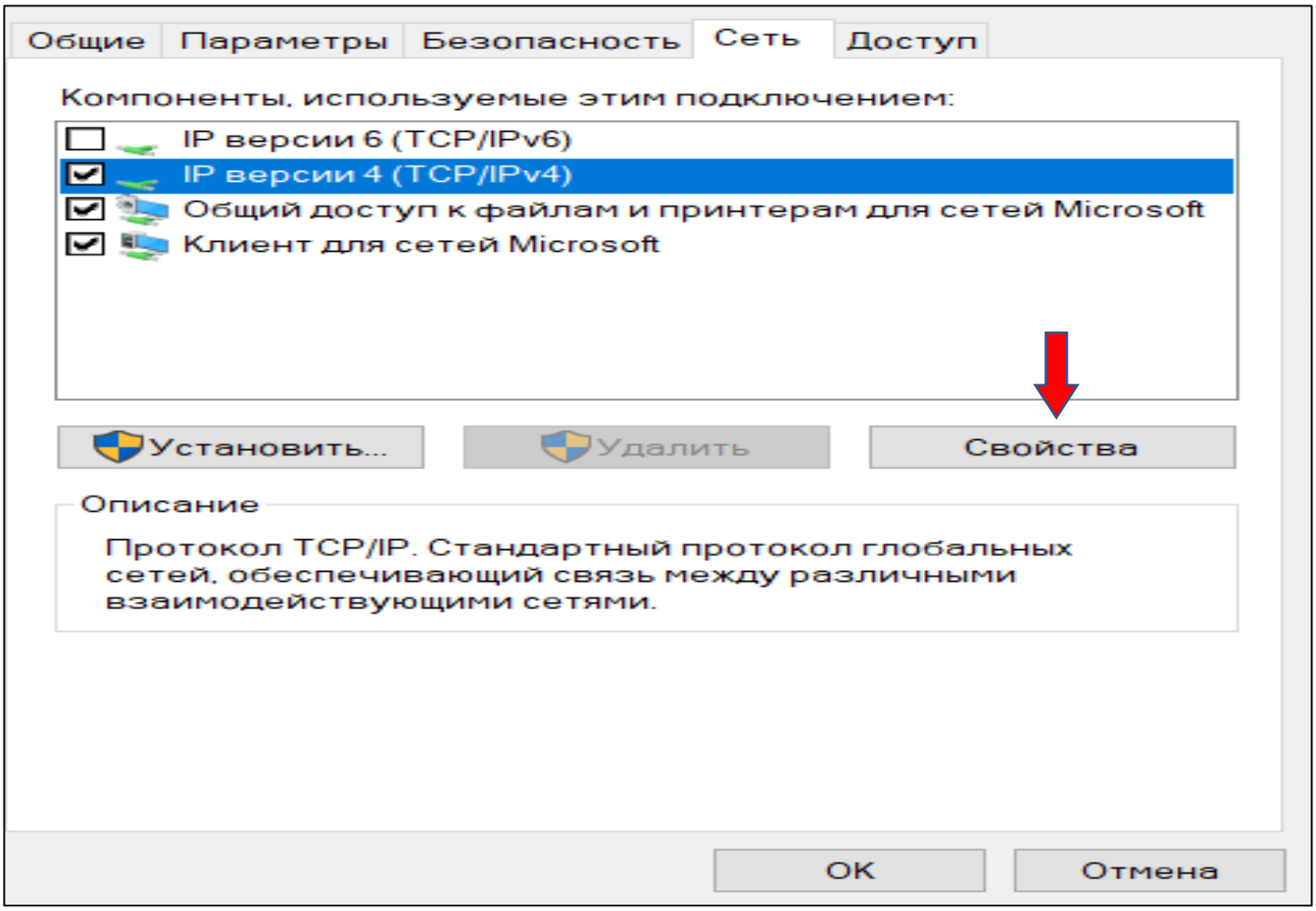
3.11 В открывшемся окне нажмите правой кнопкой мыши на созданное VPN подключение и выберите пункт меню «Свойства»



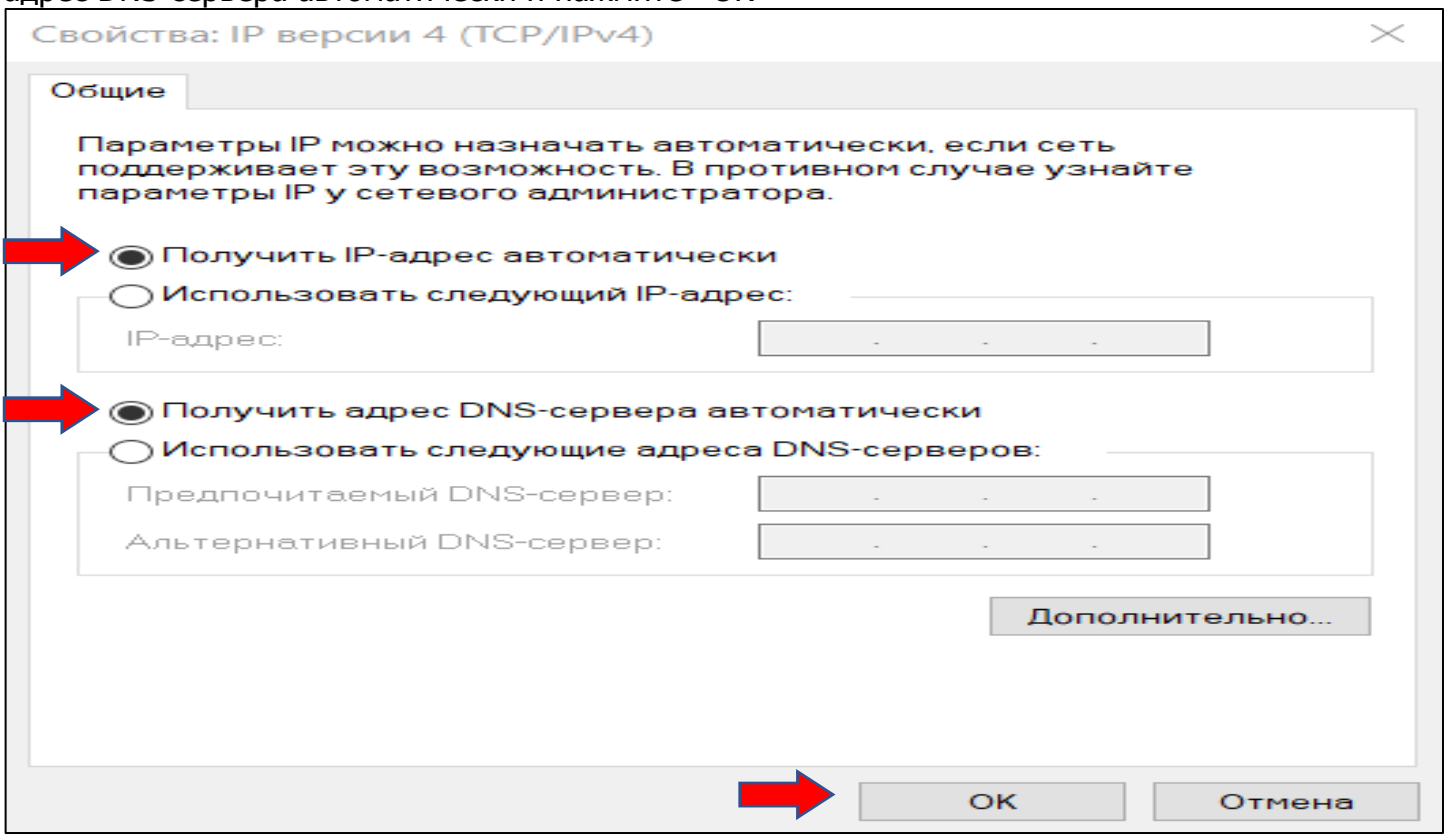
3.12 Перейдите на вкладку «Безопасность» выберите тип VPN «IKEv2», Шифрование данных «самое стойкое (отключиться, если нет шифрования)», выберите пункт «Использовать сертификаты компьютеров» и нажмите «ОК»



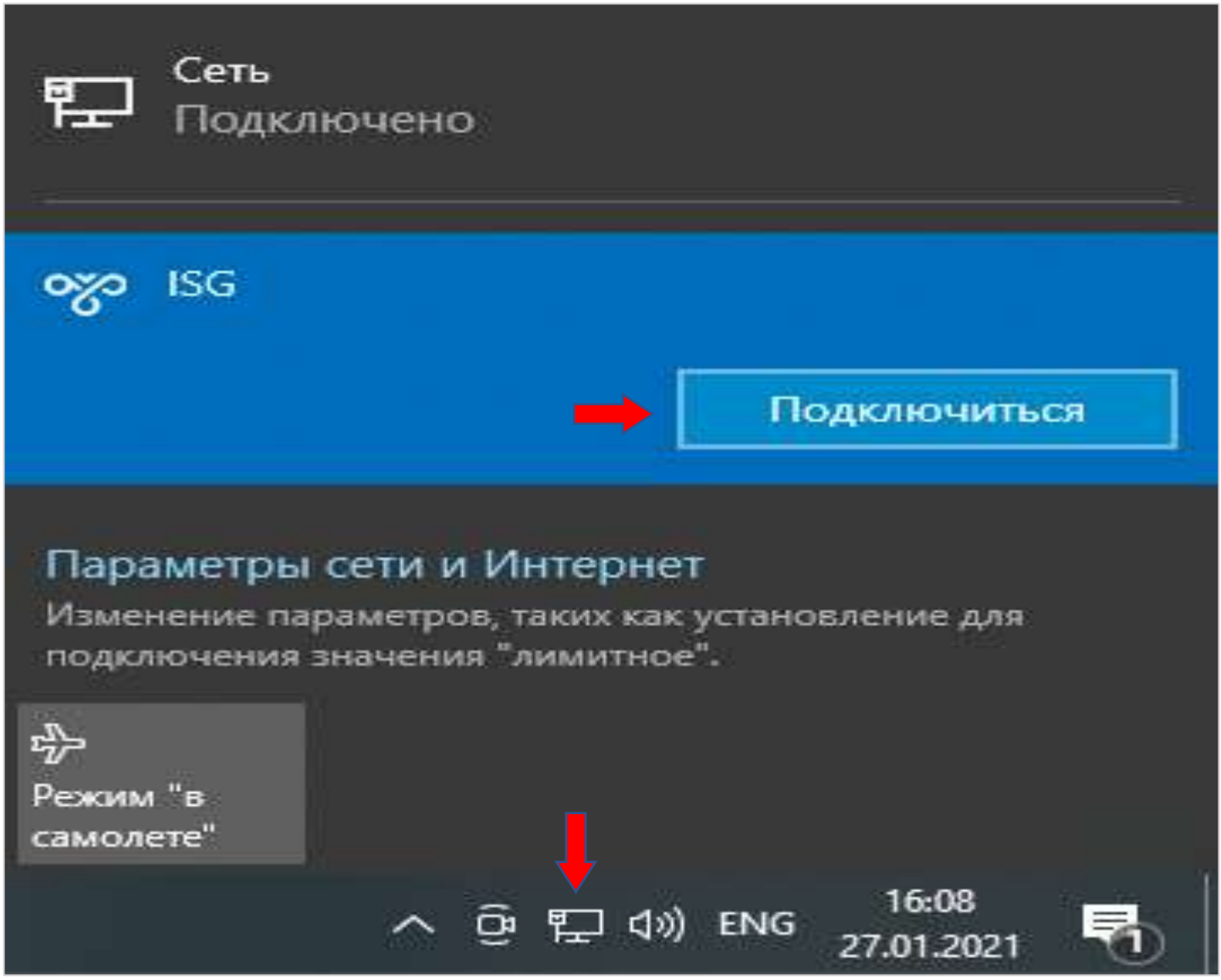
3.13 Перейдите на вкладку «Сеть» выберите пункт «IP версии 4 (TCP/IPv4)» и нажмите «Свойства»



3.14 В открывшемся окне отметьте пункты «Получить IP-адрес автоматически» , «Получить адрес DNS-сервера автоматически и нажмите «ОК»



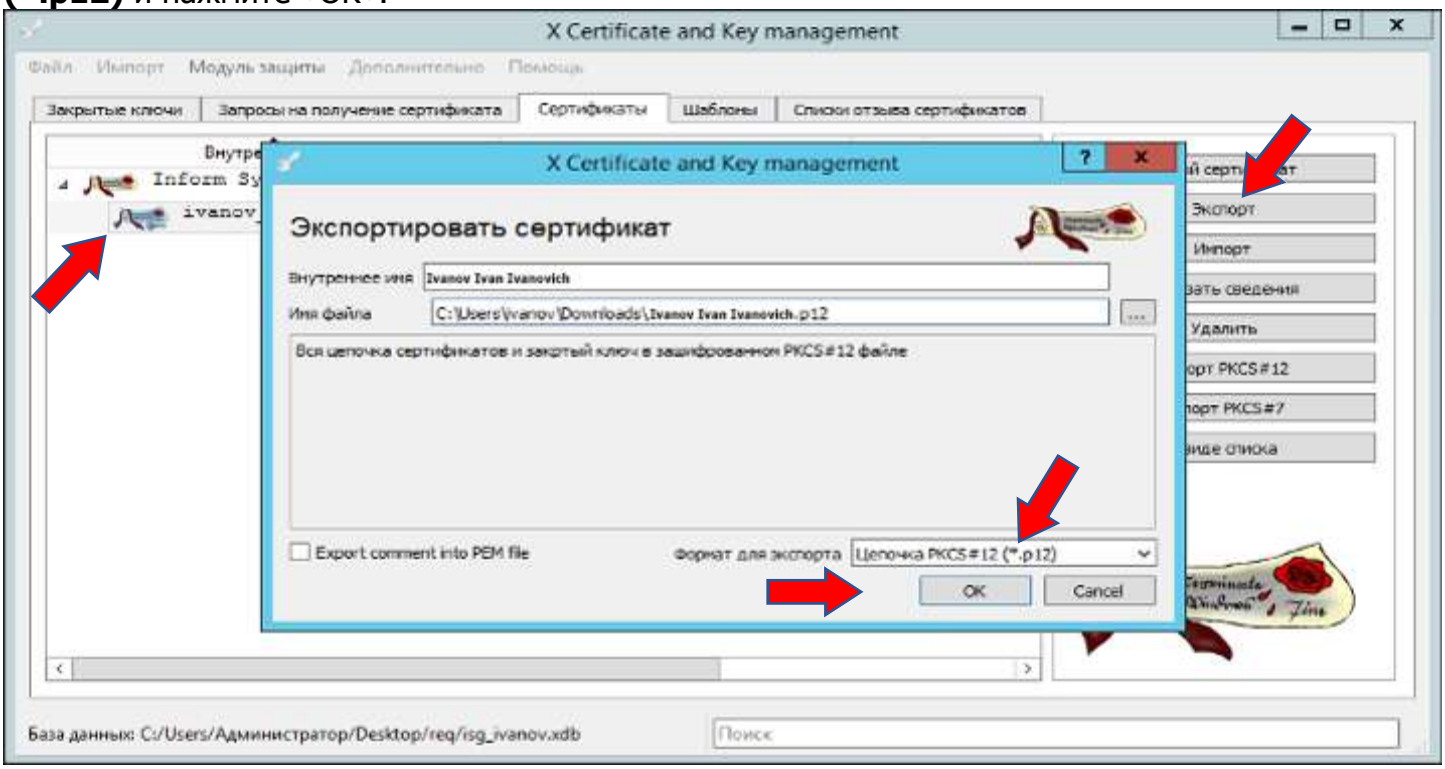
3.15 В нижнем меню рабочего стола выберите иконку «Сеть» и нажмите «Подключиться» на созданном VPN подключении



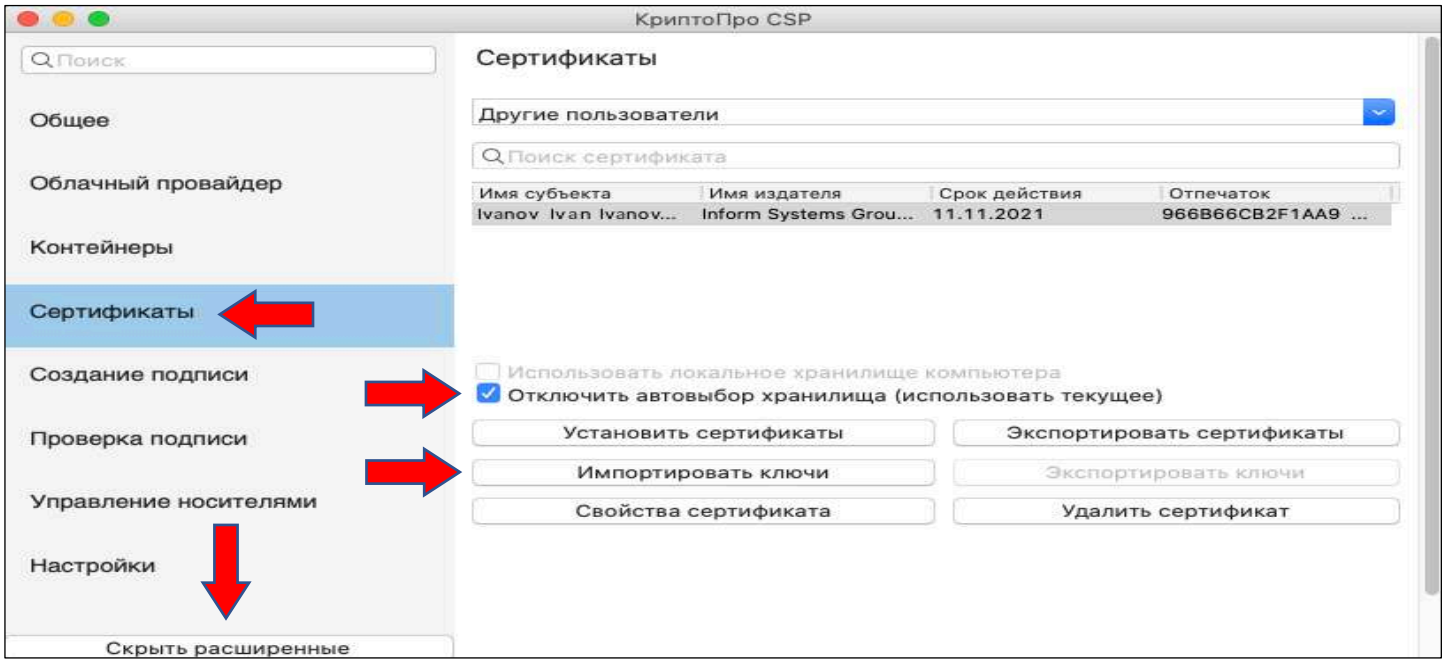
Поздравляем! Вы завершили настройку VPN-соединения. Для получения необходимых учетных записей и доступов к ресурсам группы заполните заявление, следуя инструкции на получение учетных записей: https://ftp.isg.dev/docs/instruction_account_request.pdf

4. Установка сертификата ЭЦП и подпись документов

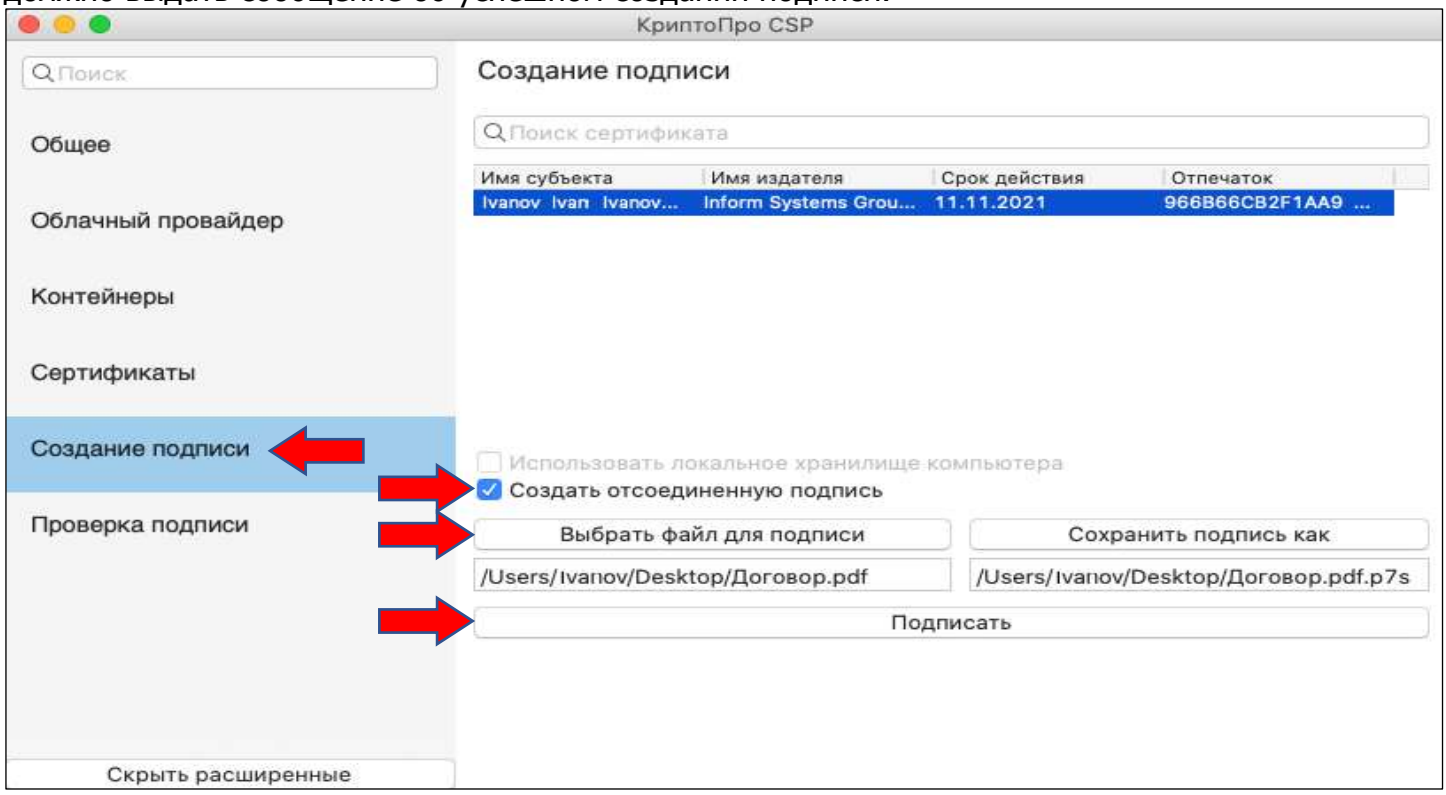
4.1 Откройте приложение **«ХСА»** выберите необходимый файл, к примеру: Ivanov Ivan Ivanovich нажмите кнопку **«Экспорт»**, укажите формат для экспорта - **Цепочка PKCS #12 (*.p12)** и нажмите «OK».



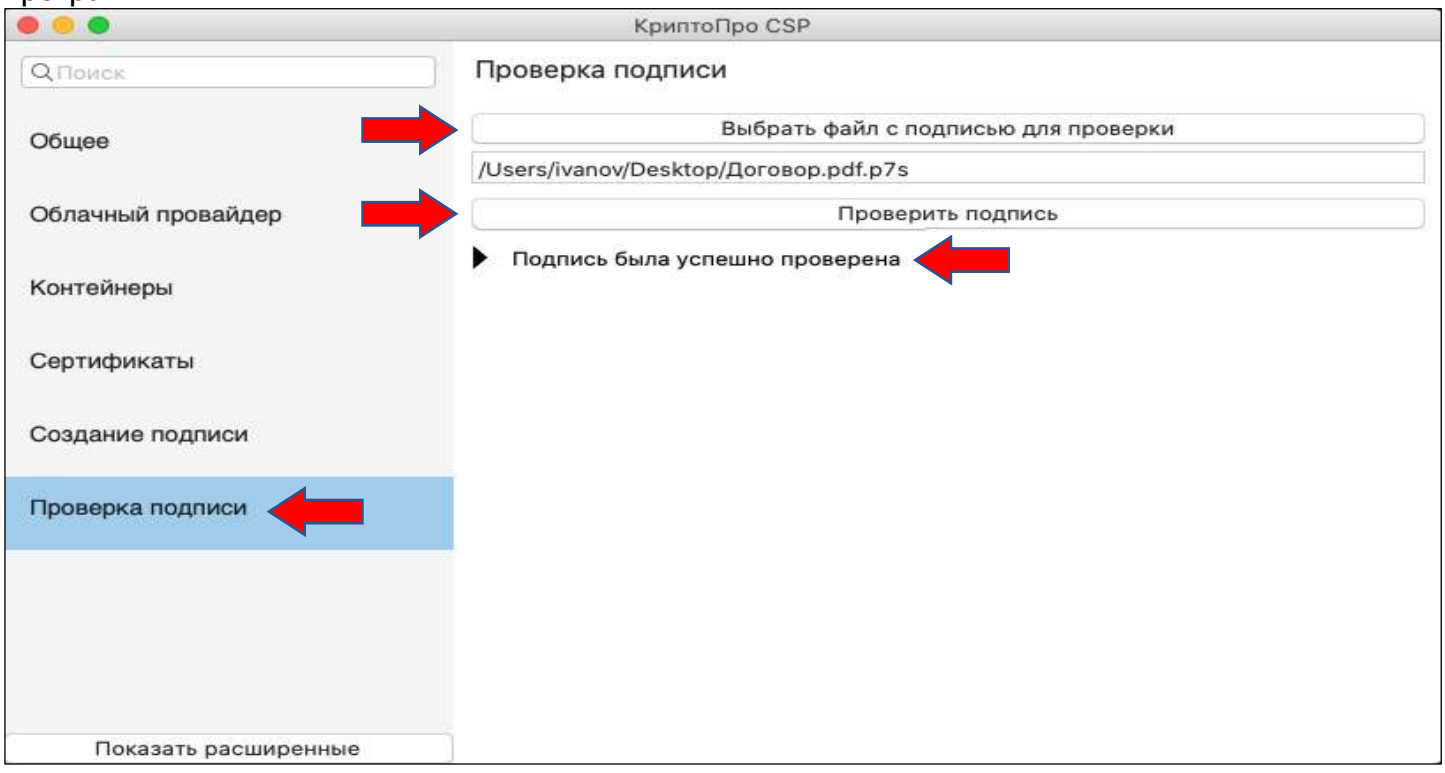
4.2 Для подписи документов используйте любое удобное для Вас приложение, к примеру: КриптоПро, КриптоАРМ и т.д. В инструкции мы приведем пример использования программы **«КриптоПро CSP»**. Скачайте **КриптоПро CSP** с официального сайта (https://www.cryptopro.ru/downloads), установите и запустите «Инструменты КриптоПро». Перейдите на вкладку «Сертификаты» в левом нижнем углу окна программы нажмите **«Показать расширенные»** в меню расширений нажмите на галочку **«Отключить автовыбор хранилища (использовать текущее)»**, нажмите на кнопку «Импортировать ключи» и выберите ваш контейнер PKCS12, к примеру: **«Ivanov Ivan Ivanovich.p12»**



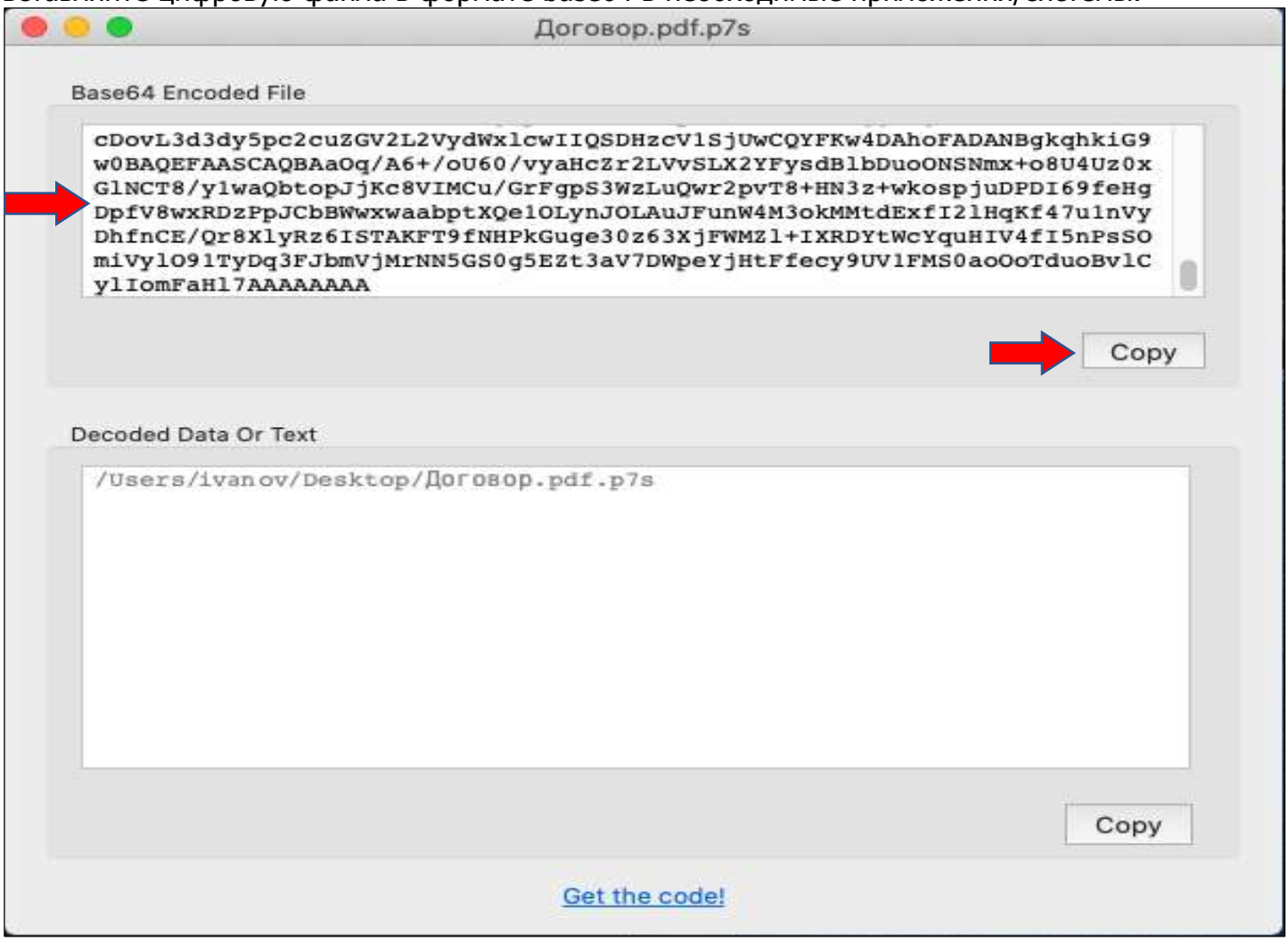
4.3 Для подписи файла перейдите на вкладку **«Создание подписи»**, нажмите на кнопку **«Выбрать файл для подписи»**, в меню создания подписи нажмите галочку **«Создать отсоединенную подпись»**, после чего нажмите на кнопку **«Подписать»**. Приложение должно выдать сообщение об успешном создании подписи.



4.4 Для проверки подписи перейдите на вкладку **«Проверка подписей»**, выберите файл *.p7s и нажмите на кнопку **«Проверить подпись»**, выберите подписанный файл/документ, если его подпись корректная, то на экране появится надпись **«Подпись была успешно проверена»**, в противном случае вы увидите ошибку проверки подписи, что говорит об неверной подписи, измененном файле после его подписания, либо ошибке в настройке программы.



4.5 Для конвертации подписи в формат **base64** воспользуйтесь любым удобным приложением, реализующим данную функцию, к примеру приложение **«Base64Anywhere»**. Перенесите файл формата *.p7s в верхнее окно приложения, после чего нажмите **«Copy»** и вставляйте цифровую файла в формате base64 в необходимые приложения/системы.



Сформированную цифровую подпись файла/документа можно пересылать по электронной почте, либо хранить в централизованном хранилище файлов группы компаний «Информ-Системы» **(WEBDAV)**, где она автоматически верифицируется.