

ИНФОРМАЦИОННОЕ ПИСЬМО
УПРАВЛЕНИЯ НАЛОГОВОГО МОНИТОРИНГА ФНС РОССИИ

Уважаемые налогоплательщики!

Управление налогового мониторинга ФНС России в соответствии с приказом ФНС России от 13.03.2023 № ЕД-7-23/163@ «Об утверждении Порядка получения доступа налоговых органов к информационным системам организации» (далее – Порядок получения доступа НО к ИСО) направляет краткую инструкцию, включающую в себя основные шаги для подключения АИС «Налог-3» к информационной системе организации – участника налогового мониторинга (далее – ИС НП), в том числе получение криптографических ключей к аппаратным средствам криптографической защиты информации налогоплательщиком в соответствующем Управлении ФНС России по субъекту Российской Федерации.

ВАЖНО! На момент представления в налоговый орган заявки для настройки защищенной криптографическими средствами сети связи передачи данных (далее – Заявка №1) у организации **строго обязательно:**

1. Должно быть в наличии оборудование СКЗИ, готовое к эксплуатации;
2. Должны быть реализованы сценарии информационного обмена № 1, № 2, № 3, № 4, № 5, № 6, №7, № 9, № 10 в версии, размещенной 02.06.2023 на сайте ФНС России www.nalog.gov.ru в разделе [«Расширенное информационное взаимодействие»](#).

Шаг 1:

Организация – участник налогового мониторинга или организация, планирующая перейти на налоговый мониторинг с 01.01.2024, представляют Заявку №1 в налоговый орган в соответствии с Порядком получения доступа НО к ИСО.

Заявка № 1 содержит информацию об используемых средствах криптографической защиты информации, назначенном администраторе информационной безопасности, адресе для получения криптографических ключей.

При приобретении ПАК VIPNet Coordinator HW необходимо учитывать номер сети 16824 для подключения к контуру промышленной эксплуатации АИС «Налог-3».

При направлении Заявки № 1 необходимо приложить лицензию на подключение ПАК VIPNet Coordinator HW к сети VIPNet (файл лицензии с расширением *.itcslic или *.reg).

Администратором информационной безопасности может быть назначен и утвержден локальным нормативным актом организации **только сотрудник организации**, представившей Заявку № 1. Обязательно приложение скан-образа локального нормативного акта.

Требования к должности «администратор по обеспечению безопасности информации» описаны в Едином квалификационном справочнике должностей руководителей, специалистов и служащих, утвержденном приказом Минздравсоцразвития России от 22.04.2009 № 205.

Шаг 2:

В Уведомлении о результатах рассмотрения заявки для настройки защищенной криптографическими средствами сети связи передачи данных налогоплательщику будет направлено:

- IP-адрес для подключения к сети передачи данных налогового органа;
- адрес местонахождения Управления ФНС России по субъекту Российской Федерации (далее - УФНС) для получения криптоконтейнера;
- пароль от рабочего места участника налогового мониторинга (далее – рабочее место НМ).

Пароль от рабочего места НМ действует 30 дней и после сгорает. Пароль является временной мерой – после первого входа в рабочее место НМ по паролю, пользователь добавляет роли и других пользователей, кто будет пользоваться рабочим местом НМ. Дальнейшие входы этих пользователей осуществляются с использованием усиленной квалифицированной электронной подписи, без использования паролей.

Шаг 3:

Представитель налогоплательщика, ответственный за получение ключей СКЗИ (далее – представитель налогоплательщика), должен явиться по адресу местонахождения УФНС из Уведомления о результатах рассмотрения заявки для настройки защищенной криптографическими средствами сети связи передачи данных со следующими документами:

- документ, удостоверяющий личность (паспорт гражданина РФ);
- **доверенность** на получение ключей СКЗИ, подписанная руководителем организации, в соответствии с пунктом 4 статьи 185.1 Гражданского кодекса Российской Федерации;
- **ИНН** представителя налогоплательщика.

При обращении представителя налогоплательщика в течение срока хранения ключей СКЗИ в соответствующий УФНС, сотрудник УФНС:

- проверяет документы представителя налогоплательщика;
- записывает на USB-накопитель налогоплательщика расшифрованный контейнер с ключевой информацией соответствующего СКЗИ.

При получении ключей СКЗИ представитель налогоплательщика должен иметь при себе USB-накопитель.

Срок хранения ключей от СКЗИ – 30 дней.

Одновременно с этим в рабочее место НМ размещается пароль от криптоконтейнера.

Шаг 4:

В соответствии с Порядком получения доступа НО к ИСО в течение десяти рабочих дней со дня получения криптографических ключей к аппаратным средствам криптографической защиты и IP-адреса для подключения к сети передачи данных организация направляет в налоговый орган заявку для подключения к информационной системе организации (далее – Заявка №2).

В Заявке №2 содержится следующая информация:

- используемые средства криптографической защиты информации, в том числе модель СКЗИ, серийный номер, размещенный на корпусе СКЗИ, указанные в Заявке №1;
- IP-адрес, выданный владельцу криптошлюза при положительном рассмотрении Заявки №1;
- DNS имя, указывающее на IP-адрес, выданный владельцу криптошлюза.

Далее сотрудник налогового органа совместно с администратором информационной безопасности налогоплательщика производят проверку подключения по инструкции, предоставленной по результатам исполнения Заявки №1.

По факту успешной проверки подключения процесс подключения АИС «Налог-3» к ИС НП считается завершенным.

Дополнительно сообщаем о создании единого электронного адреса: integrationprom@gnivc.ru для приема и обработки обращений налогоплательщиков технического и методологического характера, связанных с Порядком получения доступа НО к ИСО.