



UA.OBCT.00001-01 34 03-1

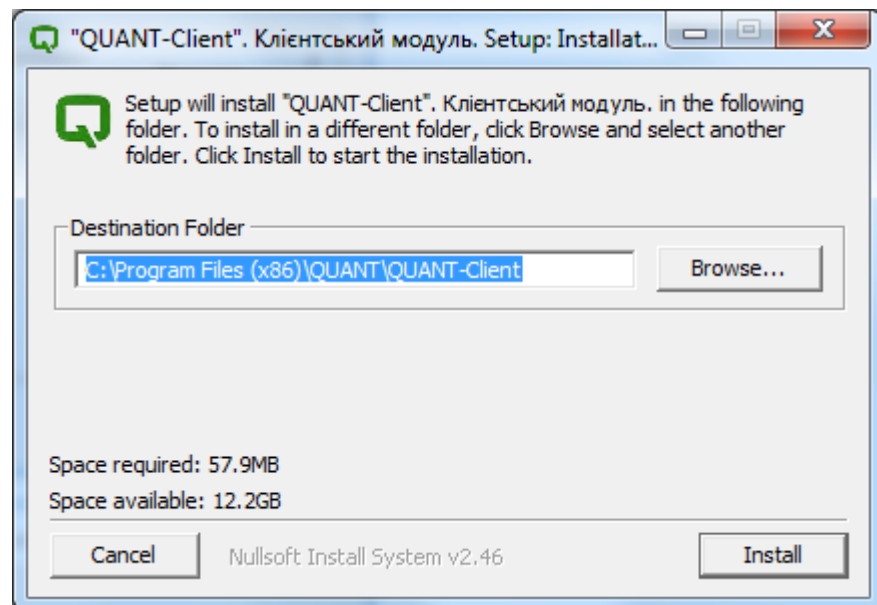
**"КЛІЄНТ" ЗІ СКЛАДУ "КОМПЛЕКСУ
ПРОГРАМНОГО КРИПТОГРАФІЧНОГО
ЗАХИСТУ ІНФОРМАЦІЇ "QUANT"**

Настанова оператора
Версія 1/2018

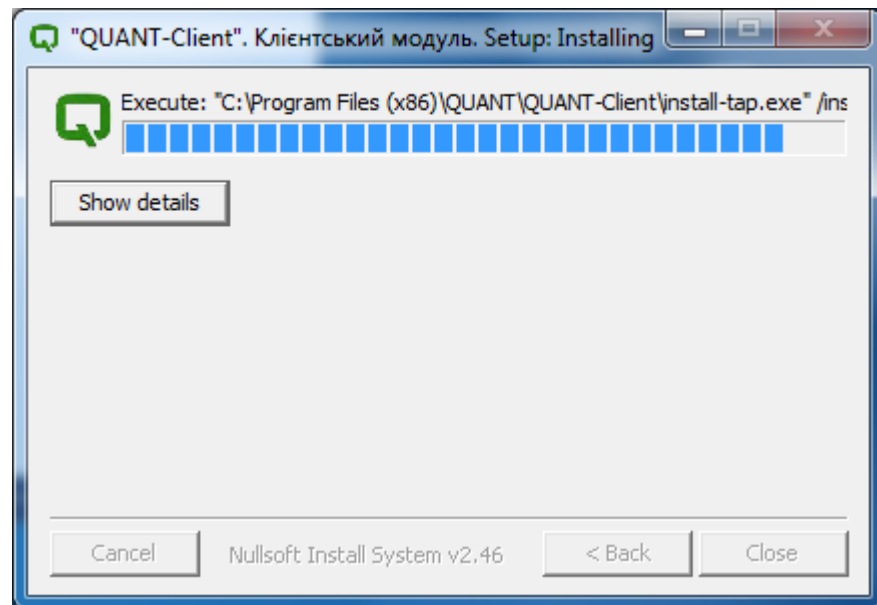
1 ІНСТАЛЯЦІЯ КЛІЄНТУ.

Для встановлення "Клієнта" зі складу "Комплексу програмного криптографічного захисту інформації "QUANT" необхідно запустити виконуючий файл QUANT-Client-1.0.1.exe через файловий менеджер ОС за допомогою виділення його і натиснення клавіші «Enter» або подвійного натискання лівої клавіші миші.

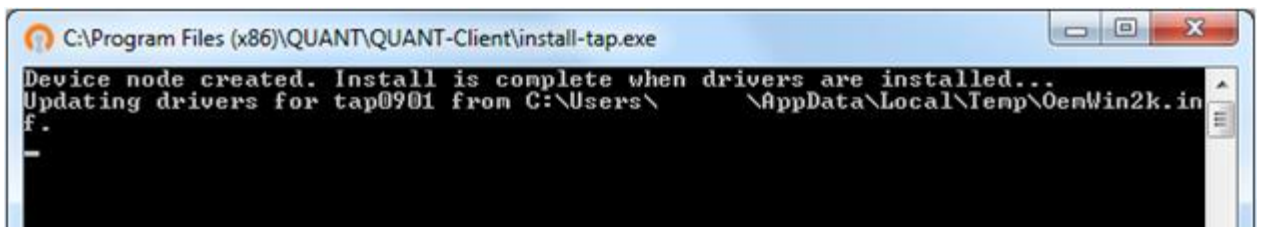
У вікні, що відкриється та зображено нижче, необхідно обрати шлях каталогу для встановлення програмного забезпечення. Рекомендується залишити налаштування за замовчуванням. Для зміни каталогу натисніть «Browse», для завершення і відміни інсталяції натисніть «Cancel», для продовження інсталяції натисніть «Install».



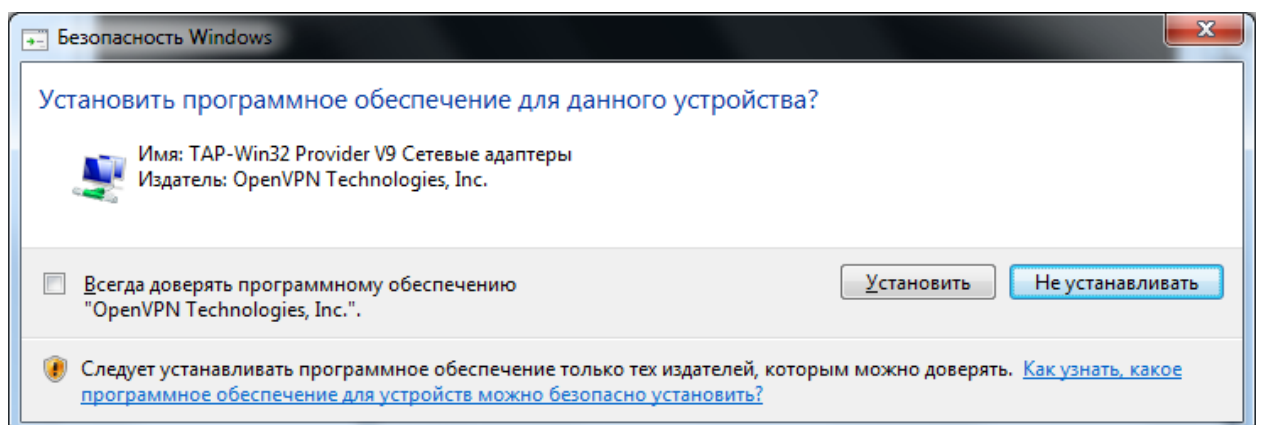
У вікні, що відкриється (зображено нижче), зображено процес інсталяції.



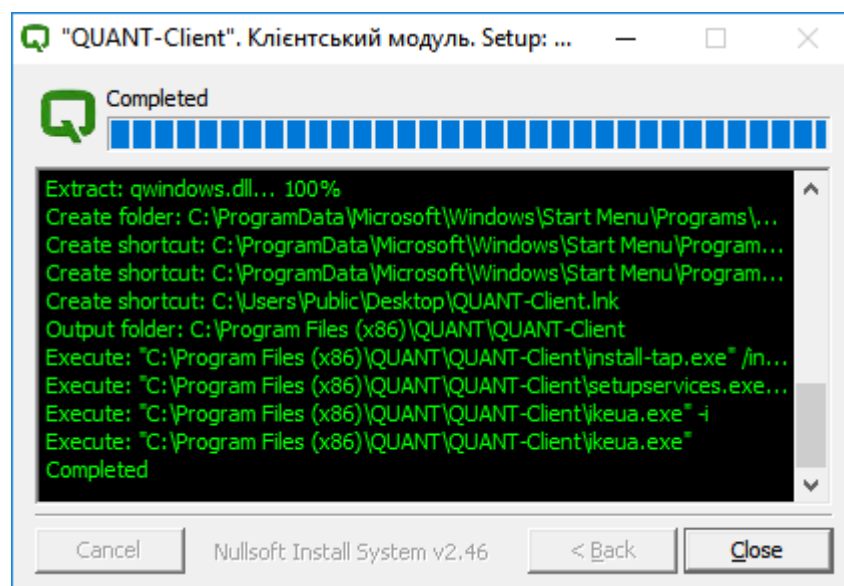
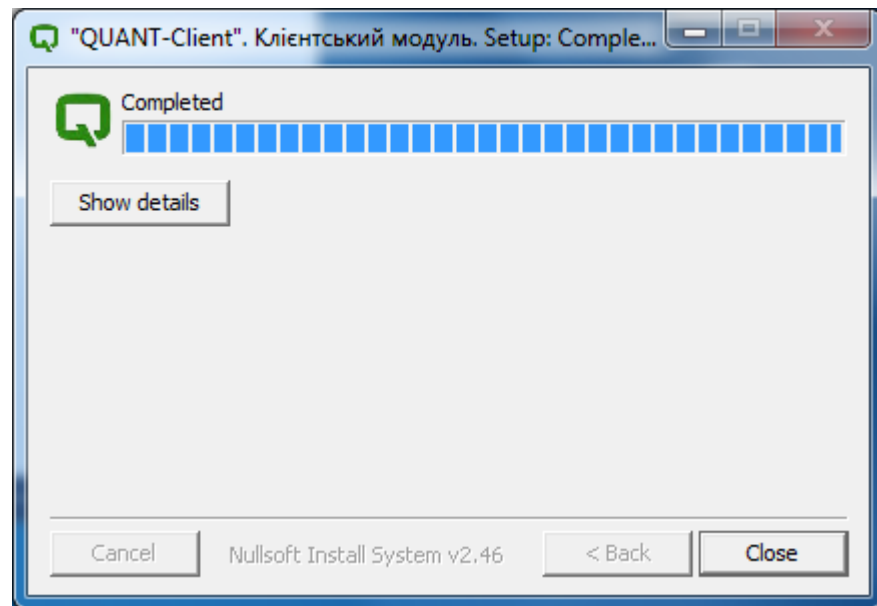
Під час інсталяції відкриється додаткове вікно процесу інсталяції драйвера.



На запит про встановлення драйвера натисніть «Установить».



Нижче зображено вікно, що свідчить про успішне завершення процесу інсталяції. Про це свідчить надпис «Completed». Для завершення натисніть «Close». Для перегляду журналу подій під час інсталяції натисніть «Show details».

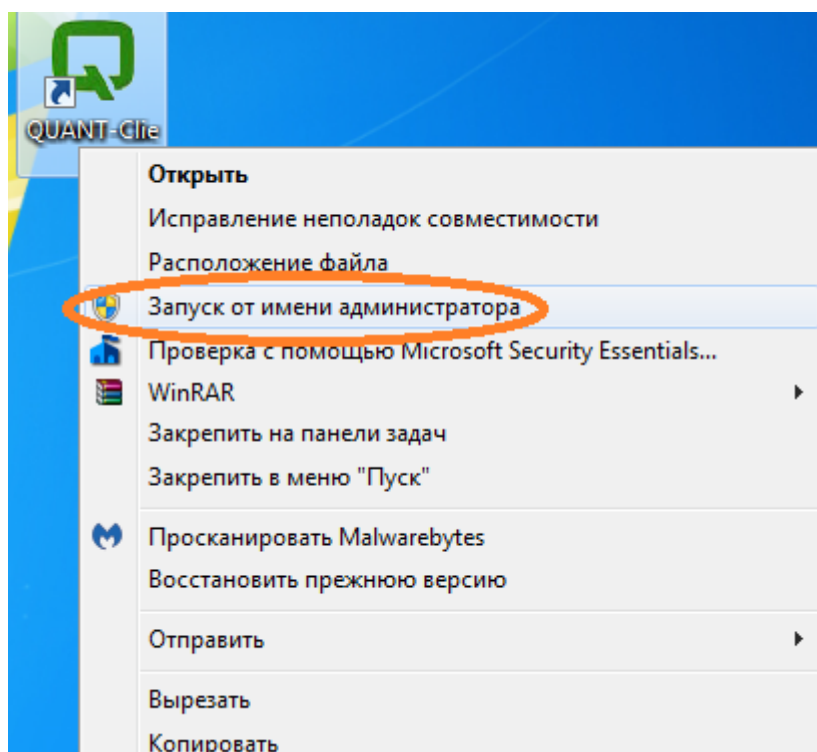


2 ЗАПУСК ПРОГРАМНОГО ПРОДУКТУ.

УВАГА!!! Для внесення змін у конфігурацію запуск програмного продукту необхідно виконати з правами адміністратора, що надасть більш розширені можливості Клієнта.

У інших випадках виконується звичайний запуск програмного продукту.

Для запуску з правами адміністратора натисніть на ярлик програми правою клавішею миші та в контекстному меню оберіть пункт «Запуск от имени администратора».



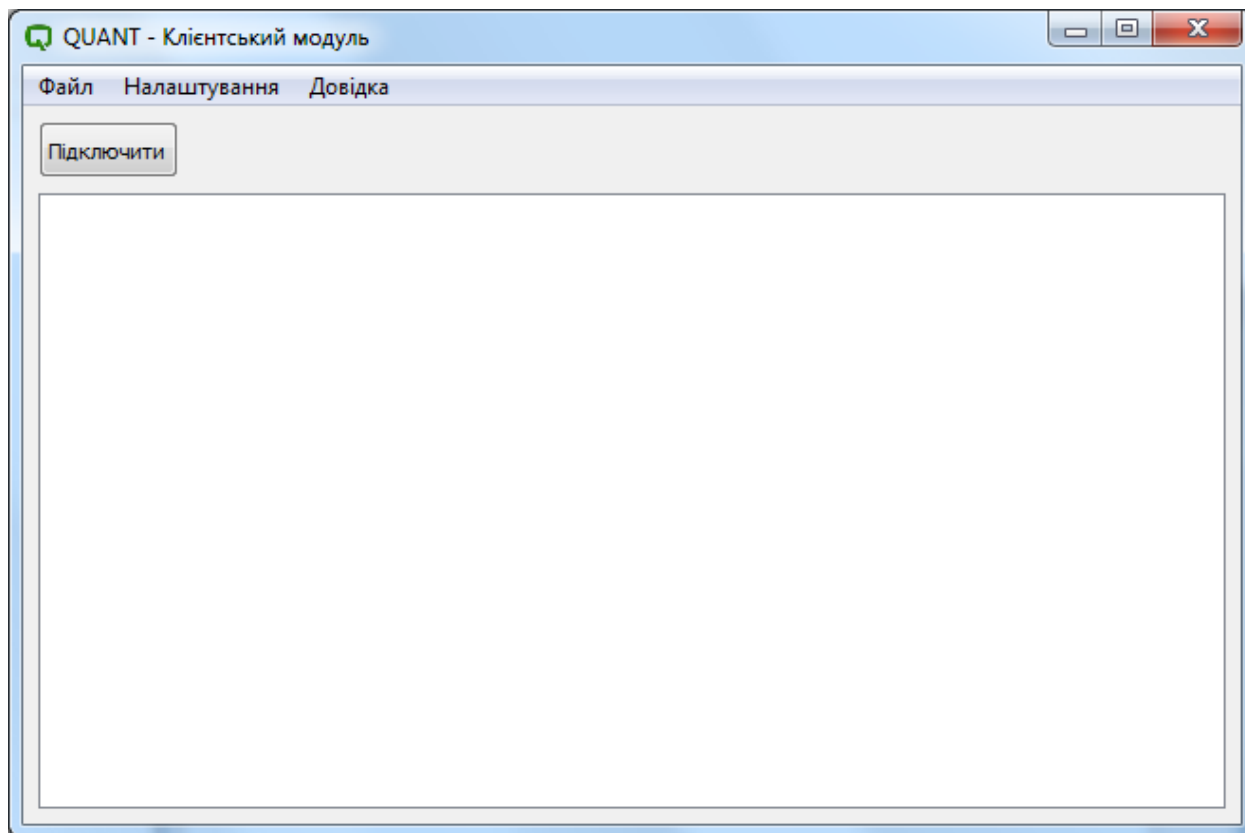
При запуску програмного продукту відкривається вікно головної форми графічного інтерфейсу.

Меню головної форми дає можливість:

- розділ Файл — здійснити підключення до існуючого профілю (Підключити); завантажити профіль у програмний продукт (Імпорт до файлу) або навпаки зберегти поточний профіль на будь-який носій інформації (Експорт до файлу). Дії збереження та завантаження проводяться з файлами формату *.vrp ;

- розділ Налаштування — сформувати новий профіль підключення (Створити), внести зміни до обраного профілю (Редагувати); перейменувати профіль підключення (Змінити назву); видалити будь-який обраний із списку профіль підключення (Видалити).

- розділ Довідка — надає інформацію стосовно версії та ліцензії програмного продукту.



2.1 Створення профіля захищеного підключення.

Для створення нового профіля захищеного підключення необхідно в головному меню натиснути послідовно Налаштування -> Створити.

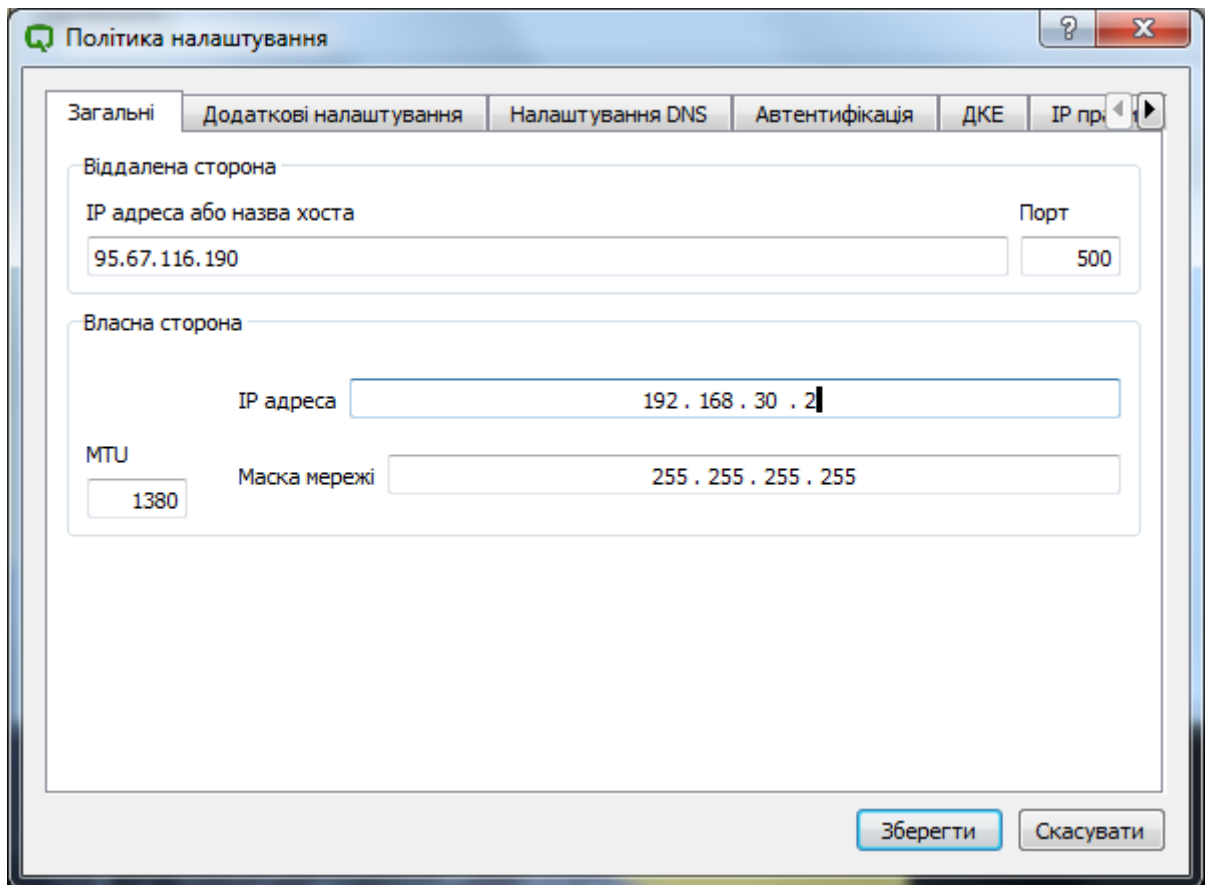
Нове вікно об'єднує декілька вкладок, які необхідно заповнити технічною інформацією.

Далі буде описано тільки ті пункти програмного забезпечення, які потребують внесення або коригування адміністратором.

Вкладка «Загальні» містить наступну інформацію:

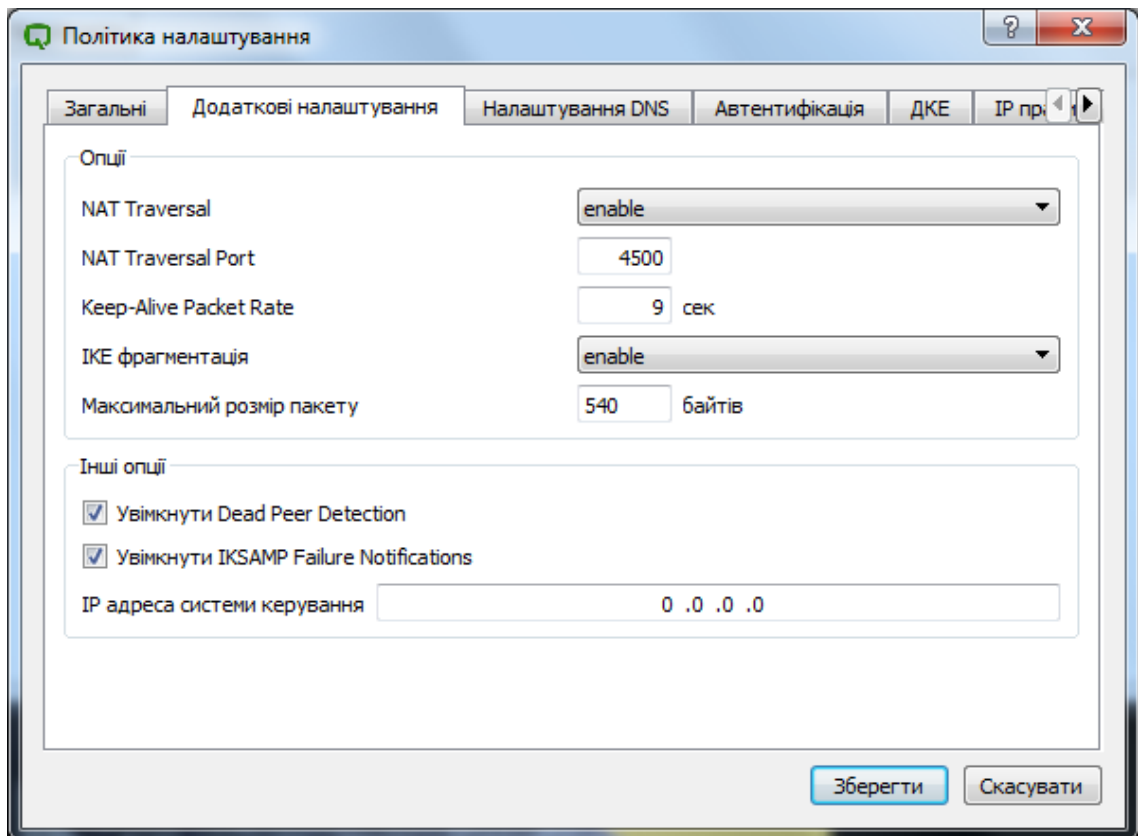
- Віддалена сторона – WAN адреса віддаленої сторони, з якою необхідно встановити захищений канал зв'язку. Як правило, це інший довірений шлюз VPN.

- Власна сторона – локальна IP адреса або мережа (LAN) віртуального адаптеру встановленого Клієнта.

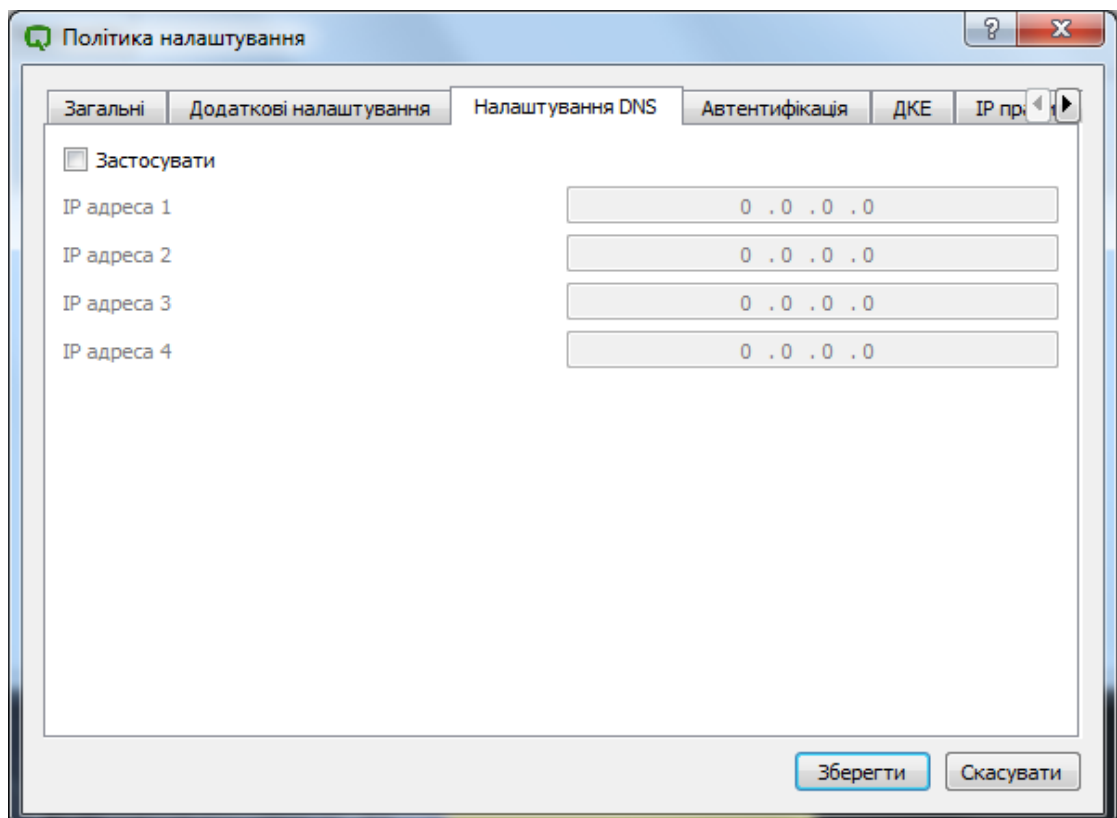


Вкладка «Додаткові налаштування» складається з двох частин - Опції (параметри налаштувань рекомендовано залишити за замовчуванням) та Інші опції:

- NAT Traversal - використання та активування функції NAT.
- NAT Traversal Port – порт для роботи функції NAT.
- Keep-Alive Packet Rate – час життя з'єднання.
- IKE Фрагментація – активування фрагментації пакетів (рекомендовано активувати).
- Максимальний розмір пакету – максимальний розмір пакету, що передається.
- Увімкнути Dead Peer Detection – активується функція перевірки доступності віддаленого серверу.
- Увімкнути ISAMP Failure Notification – активування сповіщення о проблемі підключення.
- IP адреса системи керування – IP-адреса віддаленої системи управління.

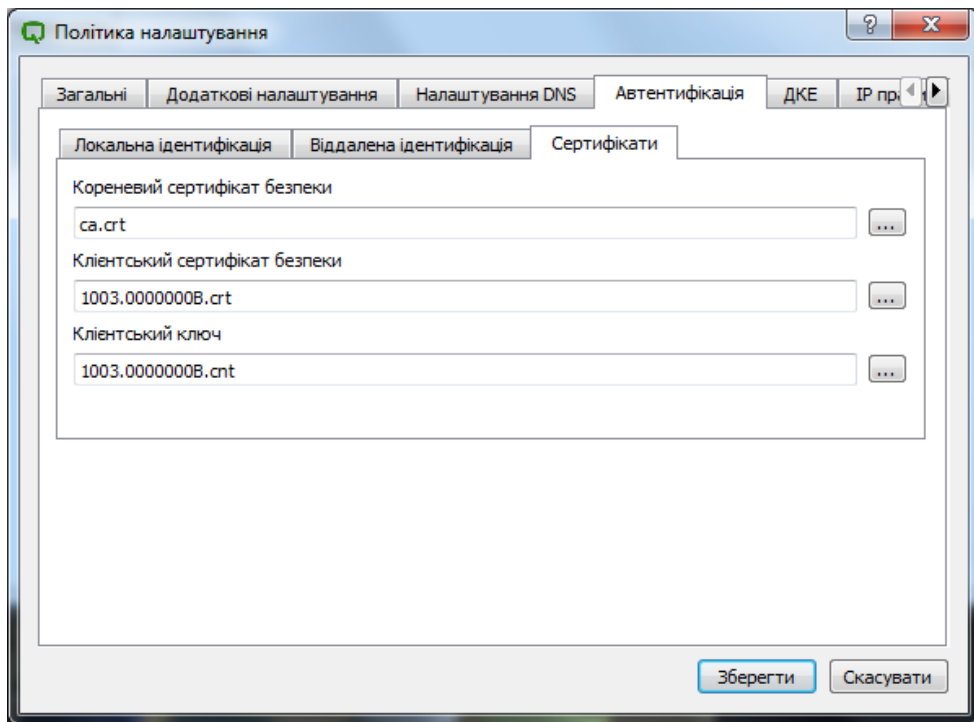


Для налаштування DNS необхідно у вкладці «Налаштування DNS» активувати (поставити відмітку напроти надпису «Застосувати») та вказати внутрішній DNS-сервер, який буде використано при обміні інформації у захищеному середовищі.

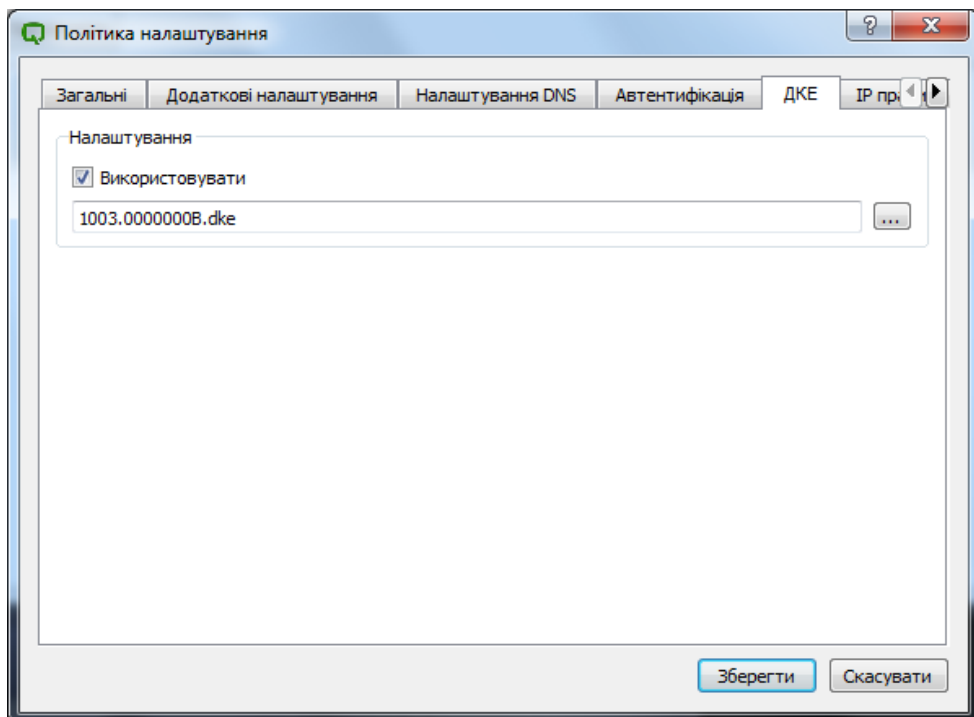


Вкладка «Автентифікація» призначена для введення ідентифікаційних даних користувача. У вкладці «Сертифікати» необхідно вказати шлях на файли-ключі та файли-сертифікати, що надаються адміністратору окремо від програмного продукту:

- Кореневий сертифікат безпеки – тут вказується кореневий сертифікат Засвідчуючого Центру (Trusted CA Certificate). Для цього необхідно у кінці поля натиснути кнопку «...», у вікні, що відкрилося, вибрати файл з СА сертифікатом (...\\ipsec.d\\cacerts\\ca.crt). Обов'язковий параметр для заповнення.
- Клієнтський сертифікат безпеки – тут вказується локальний сертифікат користувача. Для цього необхідно у кінці поля натиснути кнопку «...», у вікні, що відкрилося, оберіть файл з сертифікатом (...\\ipsec.d\\certs\\xxxx.000000xx.crt). Обов'язковий параметр для заповнення.
- Клієнтський контейнер сертифікату безпеки – тут вказується локальний ключ користувача. Для цього необхідно у кінці поля натиснути кнопку «...», у вікні, що відкрилося, оберіть файл з сертифікатом (...\\ipsec.d\\private\\xxxx.000000xx.cnt). Обов'язковий параметр для заповнення.

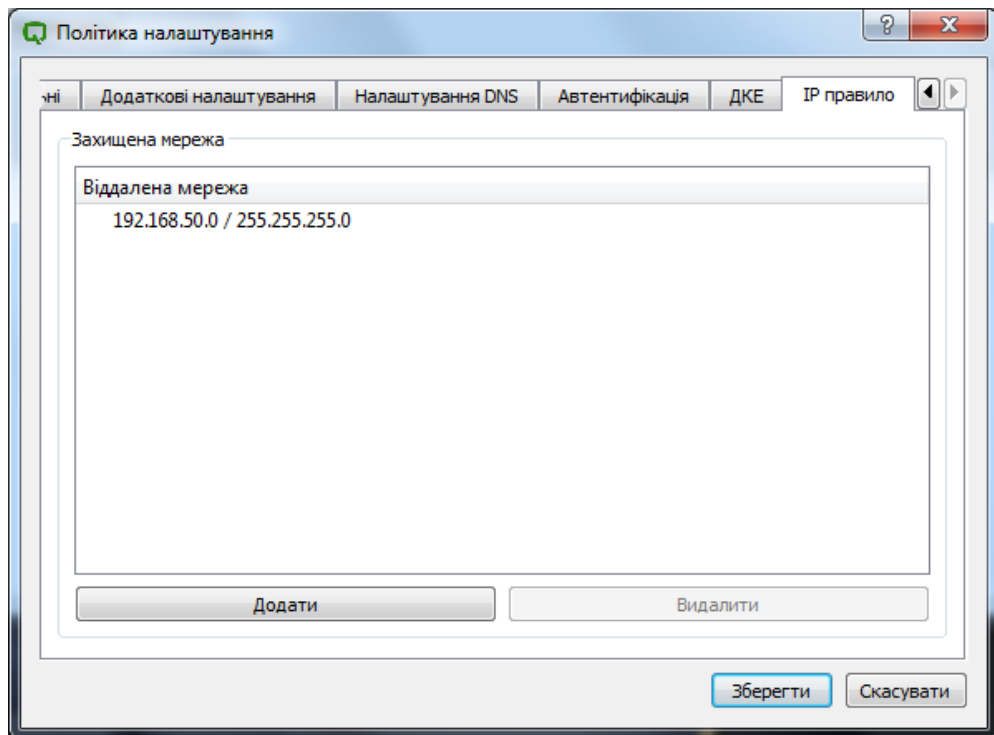


У вкладці «ДКЕ» необхідно активувати використання файлу, що перевіряє сертифікати та вказати на шлях його розміщення. Для цього необхідно у кінці поля натиснути кнопку «...», у вікні, що відкрилося, вибрати необхідний файл (...\\ipsec.d\\dke\\xxxx.000000xx.dke). Обов'язковий параметр.

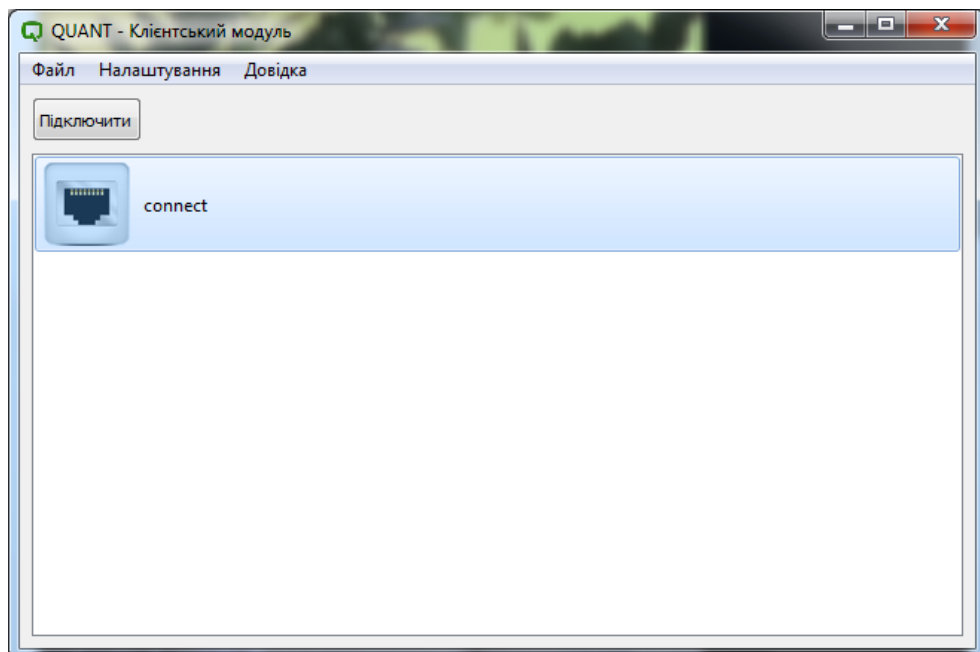


УВАГА!!! Шлях розміщення файлів-сертифікатів та файлу-ключа повинен містити тільки символи латинської розкладки на клавіатурі.

У вкладці «IP правило» необхідно внести інформацію про віддалену мережу партнера, тобто іншого довіреного шлюзу VPN. Для цього натисніть кнопку «Додати» та введіть інформацію.



Кінцевим результатом інсталяції програмного продукту є збереження введених даних кнопкою «Зберегти» та вибору назви поточного профілю.

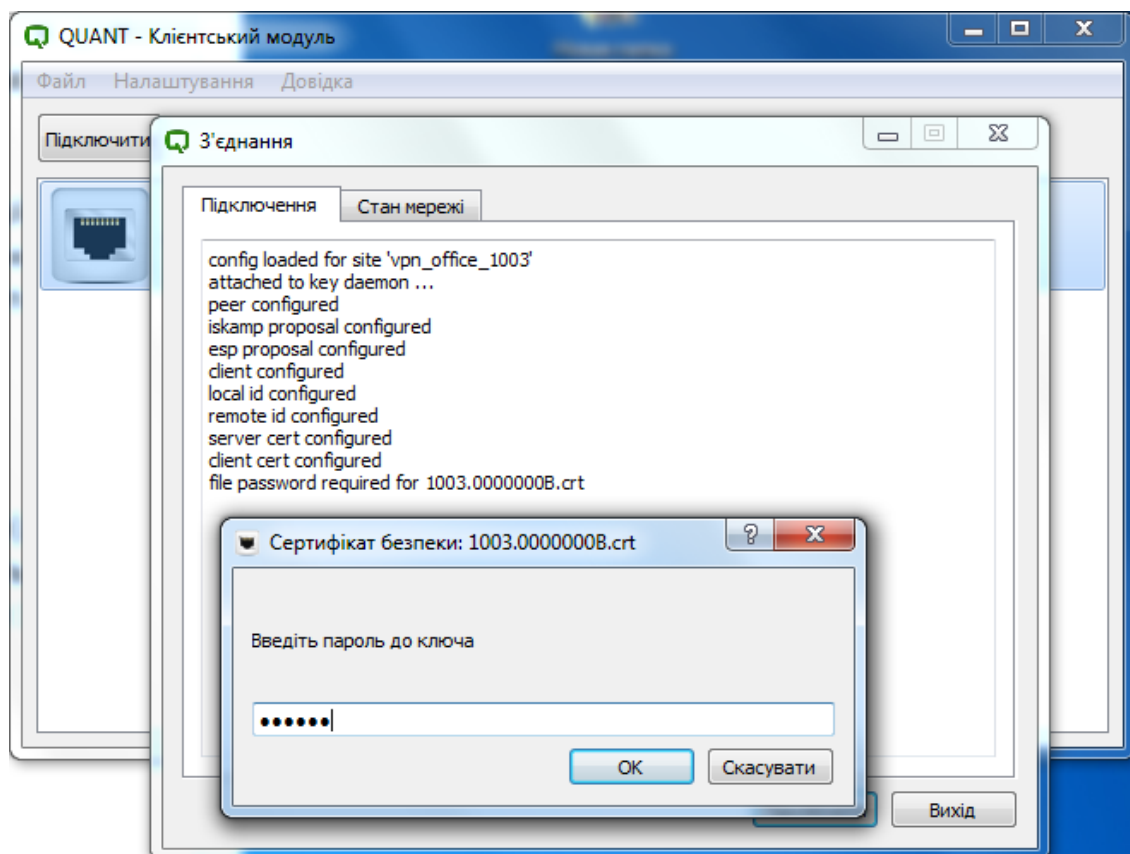


УВАГА!!! Якщо здійснено будь-які зміни у профілі, або додано/видалено профіль, необхідно вийти з програмного продукту та перезавантажити відповідну службу операційної системи.

Для цього необхідно перейти у вікно з переліком всіх служб операційної системи (Панель управління\ Всі елементи панелі управління\ Адміністрування \ Служби), натиснути правою клавішею миші на службу «QUANT IKE Daemon», у контекстному меню вибрати «Перезавантажити».

2.2 Початок роботи з програмним продуктом.

Оберіть лівою клавішею миші необхідний профіль (якщо їх декілька), та натисніть кнопку «Підключити». У новому вікні «З'єднання» натисніть «Підключити», введіть пароль до контейнеру локального сертифікату та підтвердіть кнопкою «ОК».



При вдалому підключенні з'явиться інформаційне вікно з написом «З'єднання встановлено» (tunnel enabled), програмне забезпечення згорнеться до трею. А також, доступ до локальної мережі довіреного шлюзу VPN.