https://glab.com.ua

Програма GRAPH для станції моніторингу. Інструкція з інсталяції та експлуатації.

Львів 2022

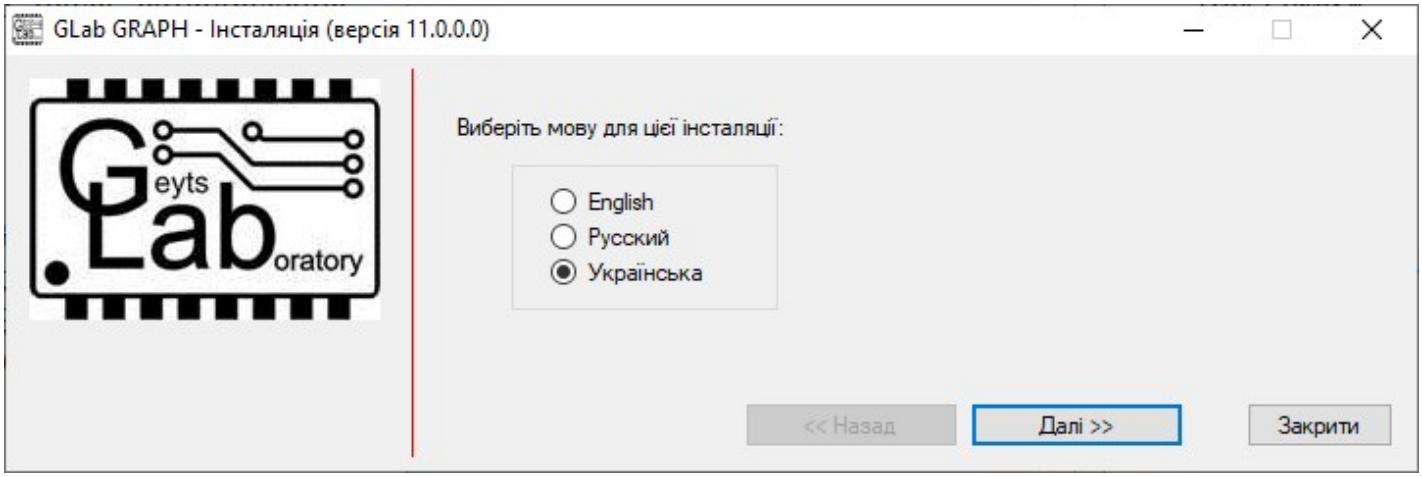
Зміст

Призначення

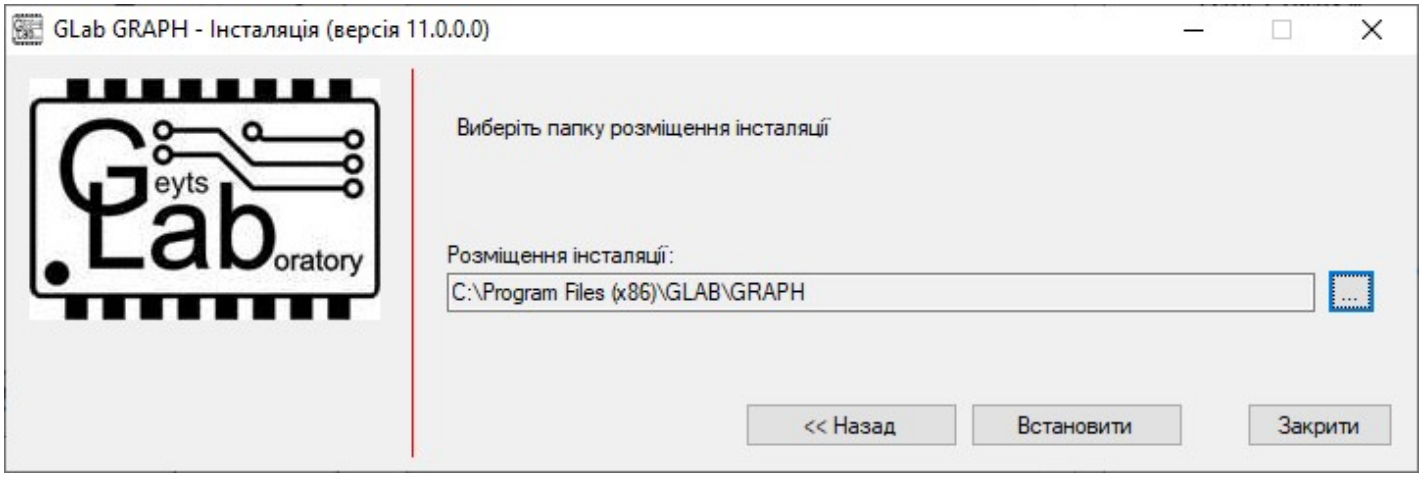
Серверна частина програмного забезпечення призначена для приймання та дешифрування повідомлень у протоколі GLab-crypto, а також для реєстрації нових пристроїв передачі з видачею ключа шифрування (для захисту від підміни пристрою). Дешифровані повідомлення у форматі Shur-GARD ContactID пересилаються у існуючий у системі COM порт або на іншу IP адресу.
Системна служба GRAPH буде запускатись автоматично після встановлення програми.
УВАГА! Для роботи програмі необхідна принаймні одна статична IP адреса (рекомендовано) або підключений сервіс динамічного DNS до динамічної IP адреси перед NAT (“біла” IP адреса з DDNS).

Інсталяція

Для інсталяції потрібно завантажити останню версію програми GRAPH за посиланням ***https://glab.com.ua/ua/downloads.html***, після чого розархівувати до теки на комп’ютері. Клікнути правою кнопкою миші по розархівованій програмі **GRAPH.exe** та вибрати запуск з правами адміністратора. Погодитись із запитом системи безпеки на виконання програми у режимі “Адміністратор”.
Після цього обрати мову та натиснути кнопку “Далі”:



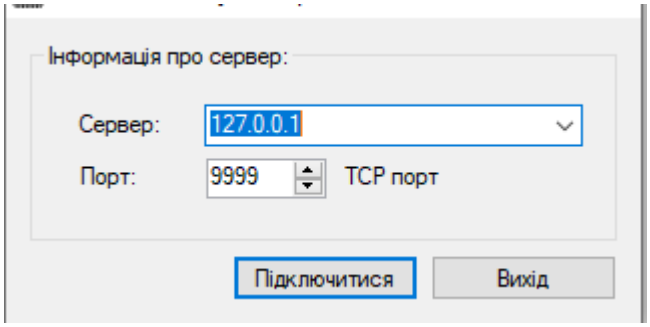
Далі можна обрати теку для інсталяції програми (опціонально) та натиснути кнопку “Встановити”:



Програму буде встановлено на комп'ютер. Системну службу GRAPH буде запущено після інсталяції автоматично.

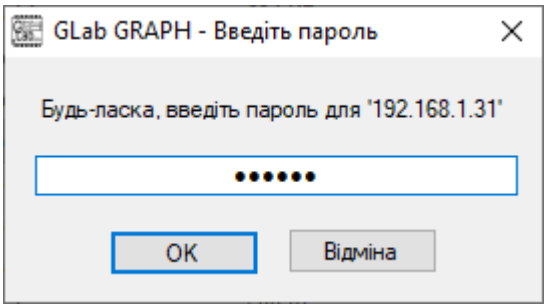
Конфігурація

Запуск клієнтської частини сервера: для цього двічі клікнути по іконці «GRAPH Client». У діалозі вибрати IP адресу комп'ютера, на якому запущений сервер,та номер порту для

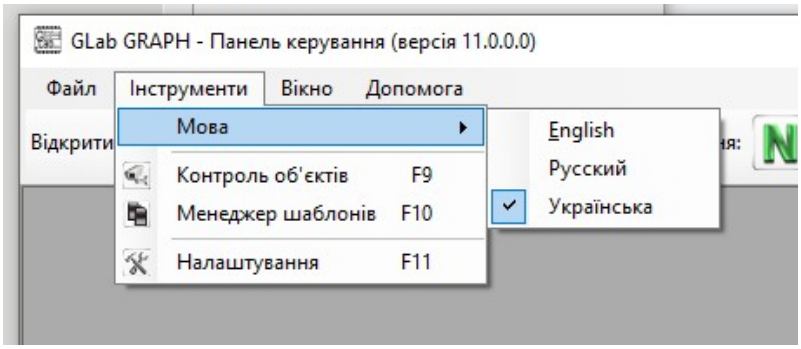


підключення та натиснути «Підключитися». Номер порту за замовчуванням 9999.

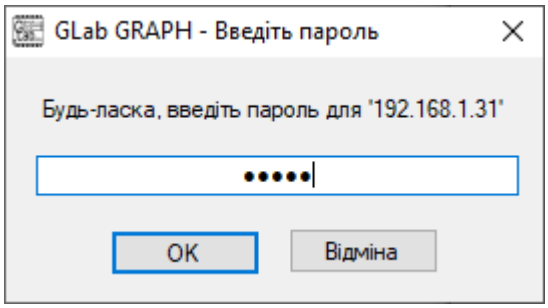
Пароль за замовчуванням програми – **«master»**.



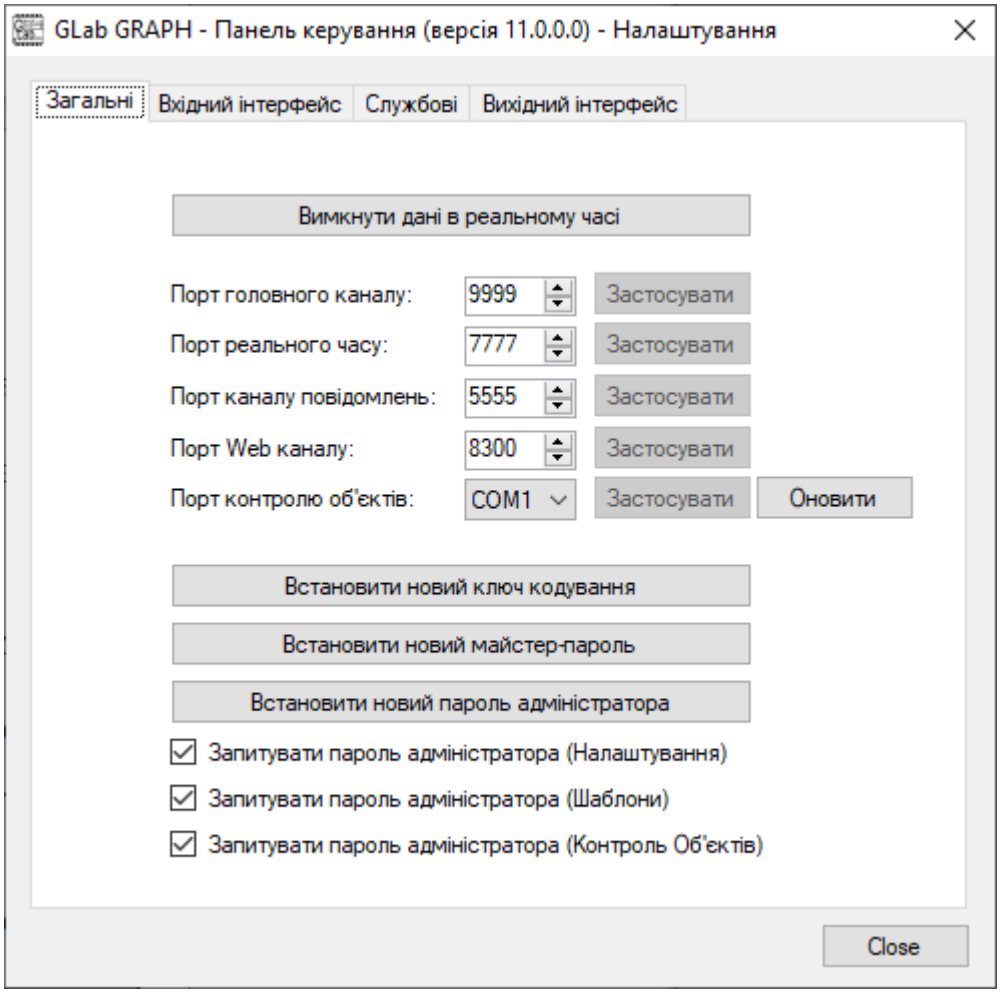
Введіть пароль та натисніть "ОК".
У вікні, що відкрилося, вибрати «Інструменти/Мова» та обрати бажану мову інтерфейсу.



Після цього відкрити «Інструменти/Налаштування»:



Пароль за замовчуванням — **«admin»**. Введіть пароль та натисніть “ОК”. Відкриється наступне вікно:

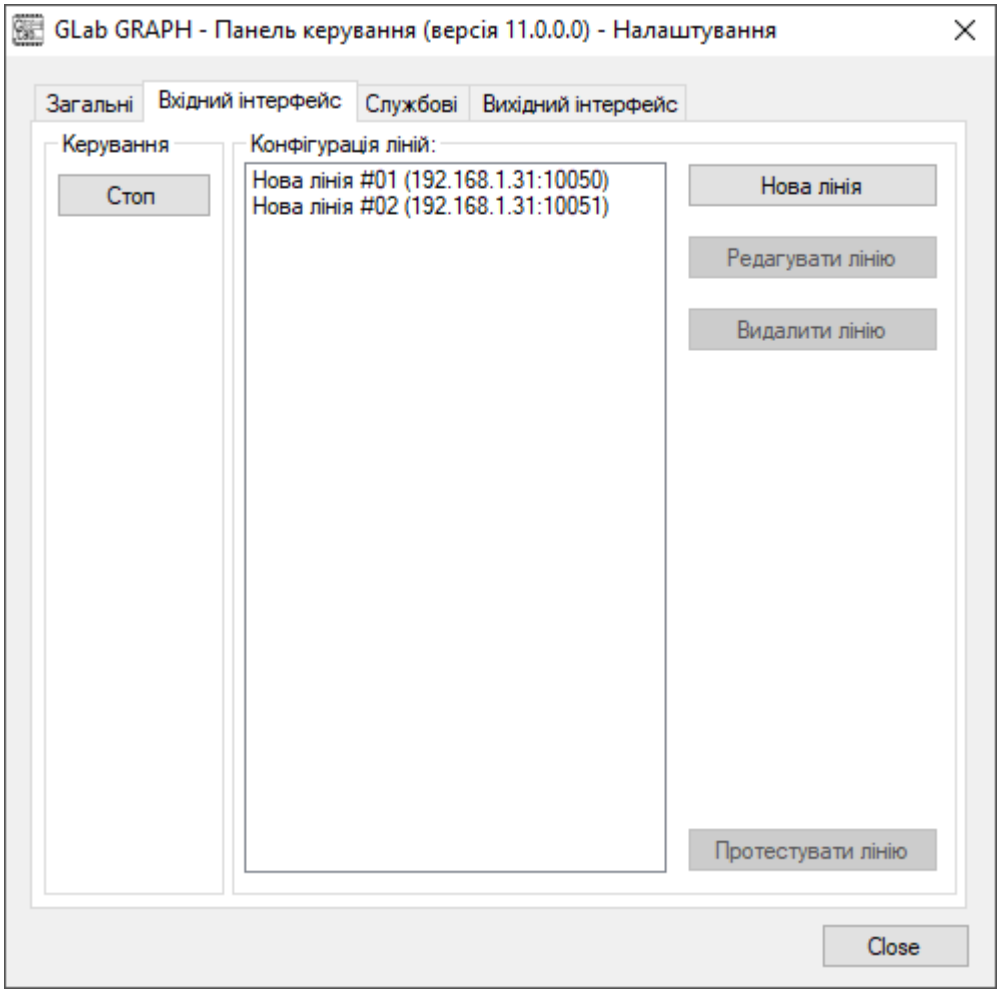


Вкладка «Загальні»:

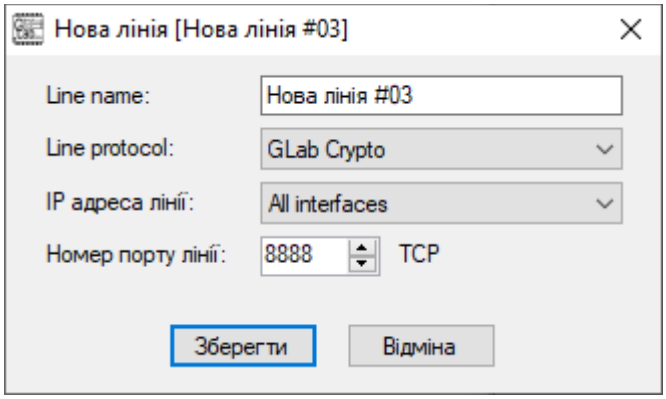
- «Вимкнути/ввімкнути дані в реальному часі» - служить для дозволу або заборони перегляду даних, що надходять для обробки сервером у реальному часі з зовнішніх портів.
- «Порт головного каналу» - порт, через який відбувається підключення клієнтської частини до сервера.
- «Порт реального часу» - порт, через який відбувається передача даних у вікно відображення подій у реальному часі.
- «Порт каналу повідомлень» - порт, через який відбувається відображення повідомлення про запит ключа об'єктовим пристроєм.
- «Порт Web каналу» - зарезервовано для використання в майбутніх версіях. Змінювати не потрібно.
- «Порт контролю об'єктів» - віртуальний COM порт USB GSM модема, якщо він підключений до комп'ютера.
- «Встановити новий ключ кодування» - кодова фраза (мінімум 8 символів), на основі якої програма генерує ключ для шифрування.

> **УВАГА!**
> ***Введену кодову фразу необхідно записати і сховати від сторонніх очей. Якщо Ви не пам'ятаєте кодової фрази, жоден з раніше підключених пристроїв при інсталяції на новий комп'ютер працювати не буде.***

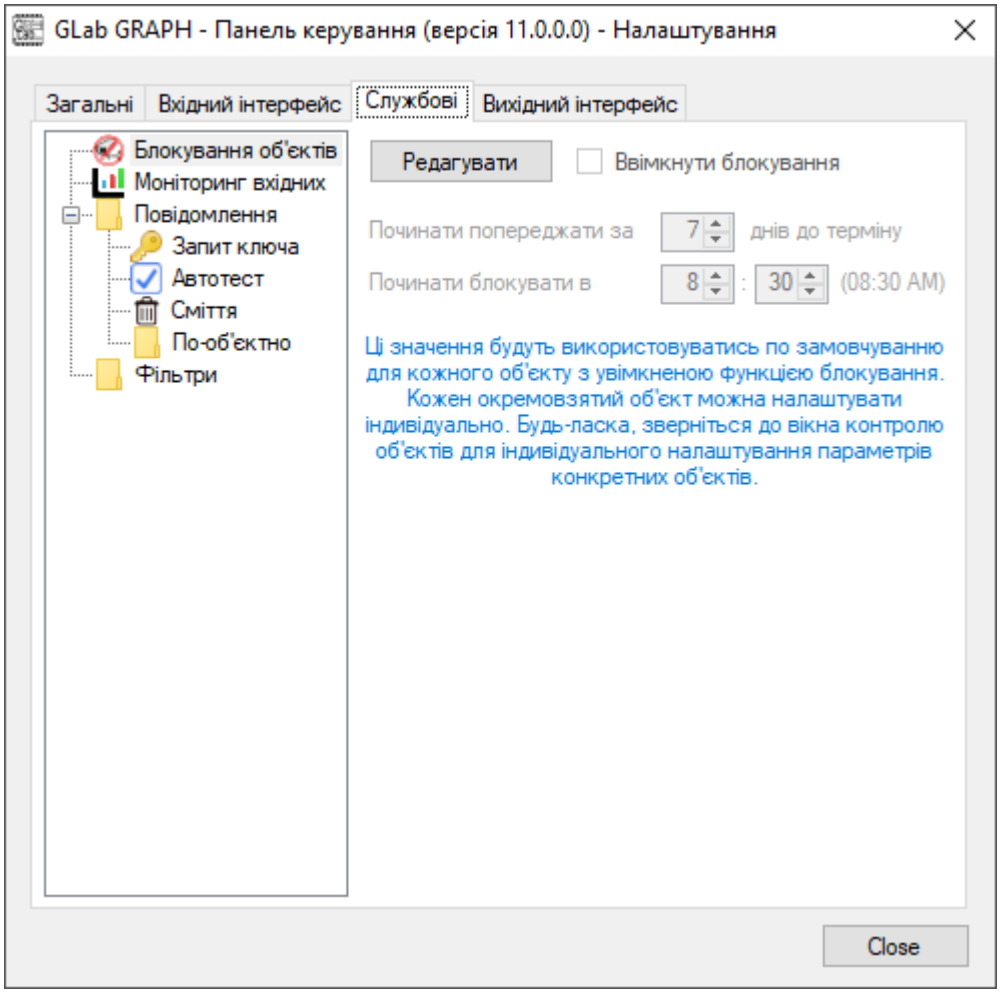
- «Встановити новий майстер пароль» -Зміна паролю для входу до клієнтської частини. Пароль за замовчуванням "**master**". Пароль чутливий до регістру.
- «Встановити новий пароль адміністратора» -Зміна паролю для доступу до налаштувань програми та контролю об'єктів. Пароль за замовчуванням "**admin**". Пароль чутливий до регістру.



Вкладка «Вхідний інтерфейс»: на цій вкладці необхідно додати «Нову лінію», вибрати IP адресу та номер порту, з яких сервер буде приймати дані від об’єктових приладів та натиснути кнопку «Старт». Створіть правило в брандмауері Windows, що дозволяє усі TCP пакети на цей порт. Після можна протестувати лінію.
Зверніть увагу — необхідно обрати для лінії протокол GLab Crypto.



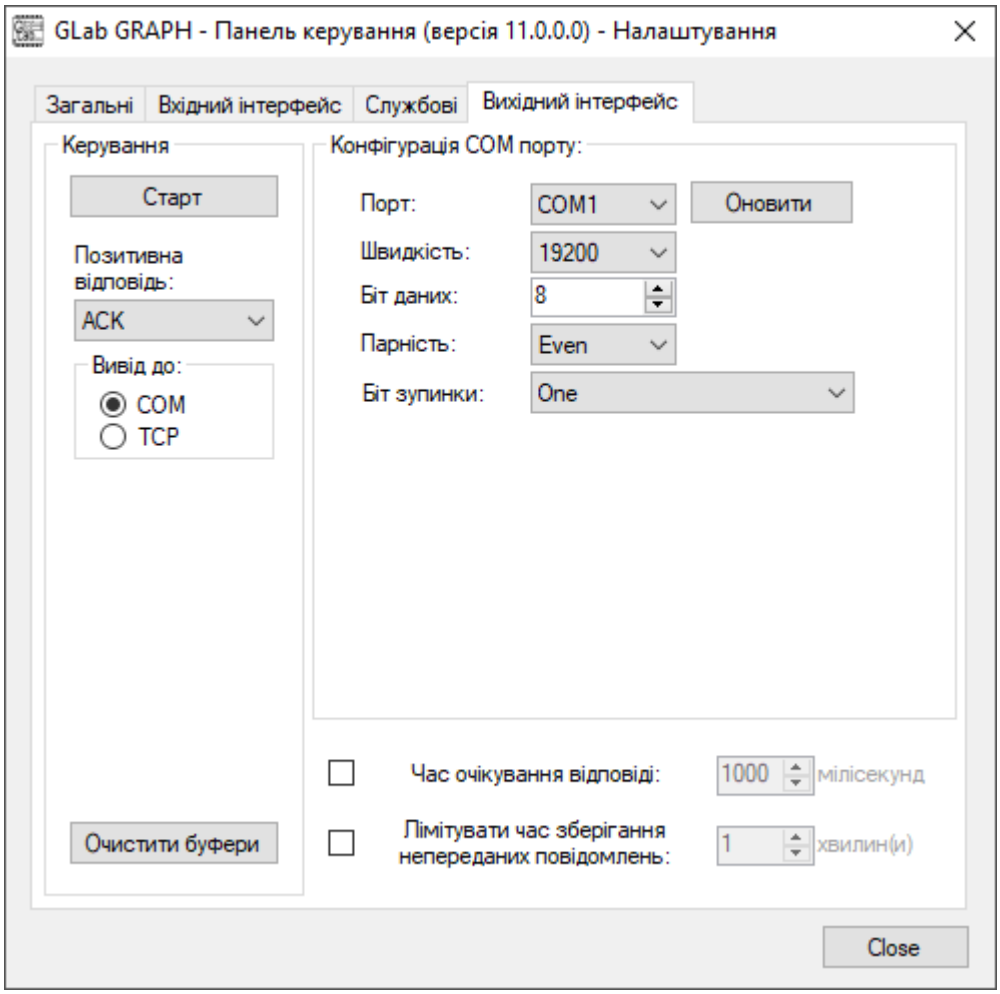
Якщо потрібно створити лінію для резервного каналу, повторіть усе вищезазначене.



Вкладка «Службові»:

- «Блокування об’єктів». Використовується для попередження та блокування постановки під охорону об’єктів, власники яких не оплачують послуги охорони. Для блокування та попередження використовуються виходи ОК1 та ОК2 пристрою easyDTMF.
- «Моніторинг вхідних». Моніторинг вхідних повідомлень призначений для збору інформації про час останнього надісланого повідомлення від об'єктів. У разі, якщо конкретний об'єкт не виходить на зв'язок довше ніж період тесту, повідомлення "Втрата Зв'язку" буде відіслано на вихідний інтерфейс (із зазначеною періодичністю). Повідомлення "Відновлення Зв'язку" буде відіслано на вихідний інтерфейс коли буде прийнято повідомлення від об'єкта (зв'язок відновлено).
- «Повідомлення/Запит ключа». Повідомлення в стандартному форматі Shur-GARD ContactID, яке пересилається у вихідний інтерфейс при отриманні від об’єкта запиту на отримання ключа шифрування.
- «Повідомлення/Автотест». Контроль зв’язку програми GRAPH з системою моніторингу. Повідомлення вигляду «5000 18УУУУЕХХХ00000[0x14]» (замість УУУУ буде підставлятись обраний номер об’єкту, а замість ХХХ — код події) буде надсилатися через обраний час (у секундах) при умові проставленої пташки у чек-боксі.

- «Повідомлення/Сміття». Повідомлення, яке буде надсилатися якщо вхідне повідомлення містить сміття (нерозпізнане). Використовується для контролю несанкціонованого доступу.
- «Повідомлення/По-об'єктно». Повідомлення від обраних об'єктів (клік правою кнопкою миші на "По-об'єктно" та вибрати "Додати нове повідомлення по об'єкту") можна дублювати іншими повідомленнями.
- «Фільтри». Для кожного об'єкту можуть бути створені індивідуальні фільтри, які не пропускають певний тип подій, групи зон, зони та коди подій.



Вкладка «Вихідний інтерфейс» - на цій вкладці можна задати вивід прийнятих і дешифрованих повідомлень у COM порт комп'ютера або на IP адресу.
Якщо пультове програмне забезпечення розуміє приймач Sur-GARD на COM порті можна скористатись безкоштовною програмою com0com (https://sourceforge.net/projects/com0com/) для створення пари віртуальних послідовних портів. Встановити у пультовому програмному забезпеченні один з портів com0com як порт Sur-GARD. Після цього обрати другий порт з пари у вкладці «Вихідний», встановити швидкість, кількість біт, контроль парності, кількість стоп бітів, наявність позитивної відповіді від пультового ПО, та натиснути кнопку «Старт». При правильній інсталяції програма готова до роботи.
Пташка "Час очікування відповіді" — час в мілісекундах, який GRAPH буде очікувати відповідь ACK або NACK.

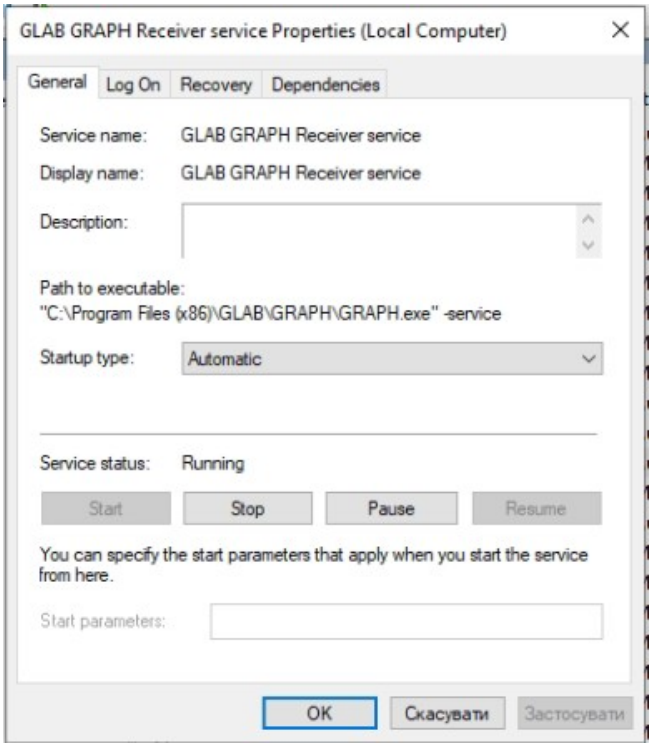
Пташка “Лімітувати час зберігання непереданих повідомлень” — час в хвилинах, після якого не передане повідомлення буде видалено з вихідного буфера.
Кнопка “Очистити буфери” видаляє усі повідомлення з вихідних буферів.
Для зручності адміністрування у програмі передбачена можливість переглядати файли історії по вхідному та вихідному інтерфейсах, а також дані в реальному часі.(закладка «Файл/Відкрити»).
У випадку TCP з’єднання необхідно вибрати IP адресу та порт приймача станції моніторингу. Після цього можна протестувати з’єднання.

Контроль з’єднання

Перед тим, як розпочати контроль з’єднання, необхідно прописати маршрутизацію вхідних (зовнішніх) портів Вашого роутера до вхідних портів програми GRAPH. Для цього необхідно звернутися до інструкції від маршрутизатора.
Для контролю з’єднання можна використати програму “TCPClient” для Android (https://play.google.com/store/apps/details?id=com.sollae.eztcpclient) або “TCP Console” для Apple. Перед застосуванням програми для контролю необхідно вимкнути WiFi в смартфоні, залишивши лише мобільні дані. Це необхідно для підключення до маршрутизатора “ззовні”. Якщо клієнт, встановлений на смартфоні, сповістив “Connected”, маршрут на роутері описаний правильно, програма встановлена і сконфігурована коректно.
У разі сповіщення від клієнта “Failed to connect” необхідно ретельно перевірити налаштування брандмауера Windows та маршрутизатора.

Робота з програмою

Для автоматичного старту сервісу GRAPH зазвичай ніяких дій виконувати не потрібно. Проте якщо сервіс все ж не стартував, переконайтеся, що режим запуску служби вибраний “Автоматично” (“Automatic”). Якщо і після цього служба не стартує автоматично, потрібно проаналізувати діагностичний log файл операційної системи Windows.

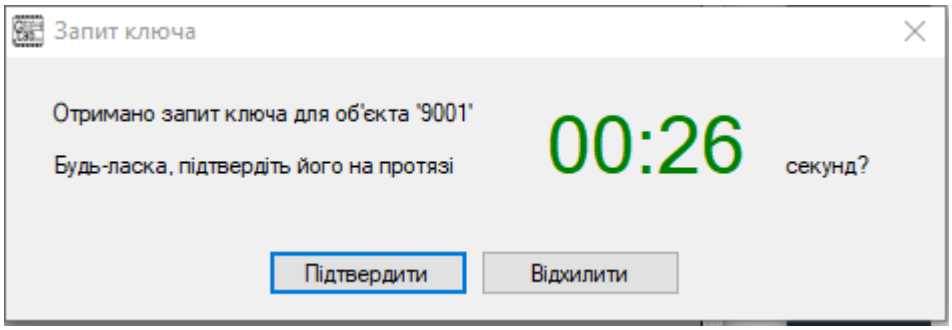


При підключенні кожного нового пристрою до станції моніторингу необхідно, щоб сервіс GRAPH надіслав унікальний згенерований ключ шифрування.

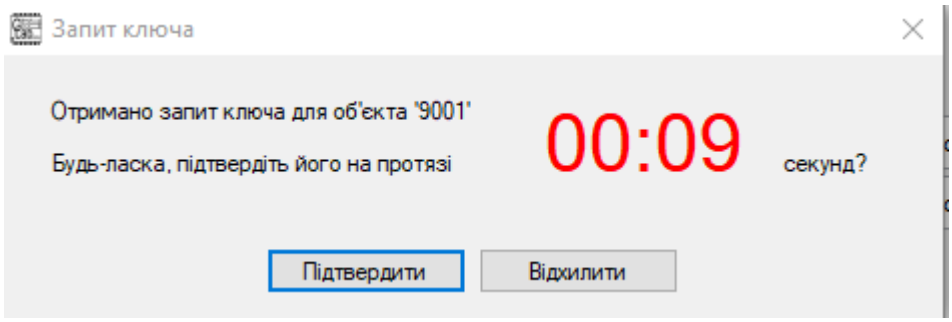
Для того, щоб оператор міг отримувати від сервісу повідомлення про надходження запиту ключа шифрування, на робочому місці слід

запустити програму “GRAPH Agent”. Вона буде показуватись у вигляді іконки на панелі завдань. Тримати активним GRAPH Client при цьому не потрібно — він використовується тільки для конфігурації та тестування каналів зв’язку.

При надходженні запиту ключа для оператора станції моніторингу буде згенеровано вікно з зазначеним номером об’єкту, що запитує ключ та зворотнім відліком від 30 секунд до 0. При цьому буде чутно стандартний сигнал сповіщення Windows.



За 10 секунд до закінчення відліку колір зміниться на червоний.



Оператор повинен або підтвердити надання ключа шифрування для пристрою, або відхилити. При відхиленні або ігноруванні оператором цього повідомлення до станції моніторингу надходить повідомлення “саботаж” (підміна пристрою). Це те повідомлення, яке було вказано при конфігуруванні у пункті «Повідомлення/Запит ключа».

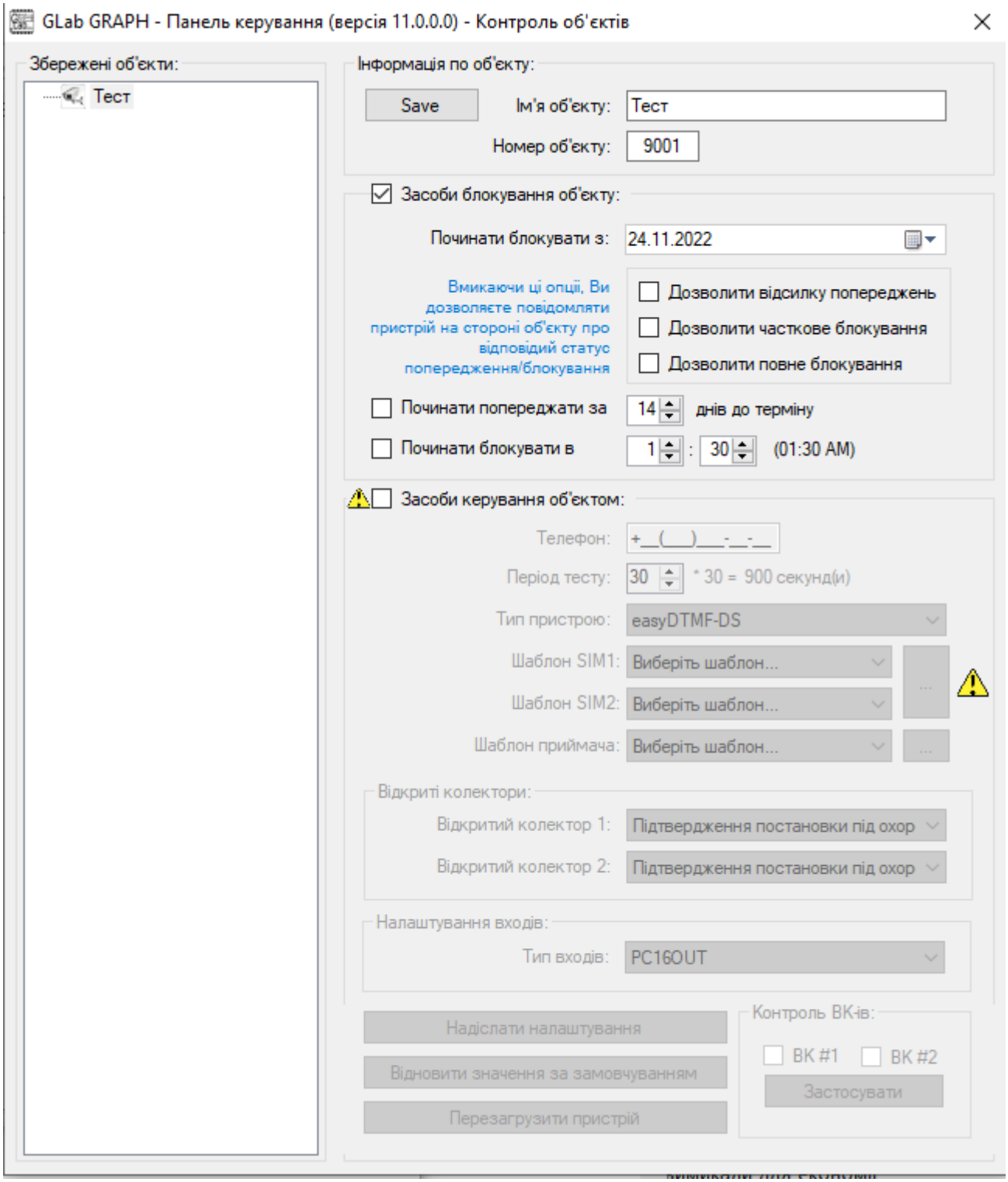
Призначення кнопок у вікні програми GRAPH Client:

 - (або F8) кнопка для перегляду подій у режимі реального часу . Зверніть увагу — для відображення подій необхідно ввімкнути передачу даних у каналі реального часу.

 - (або F5) кнопка для перегляду журналу подій вхідних повідомлень. Вхідні повідомлення згруповані по роках, місяцях та числах місяця. Час від часу журнал вхідних повідомлень слід архівувати, бо файли можуть займати багато місця на диску комп’ютера.

 - (або F6) кнопка для перегляду журналу подій вихідних повідомлень. Вихідні повідомлення згруповані по роках, місяцях та числах місяця. Час від часу журнал вихідних повідомлень слід архівувати, бо файли можуть займати багато місця на диску комп’ютера.

 - (або F9) кнопка для контролю, адміністрування та редагування об’єктів що передають інформацію до станції моніторингу через сервіс GRAPH. При натисненні програма запитає пароль (опціонально — налаштовується в конфігурації),

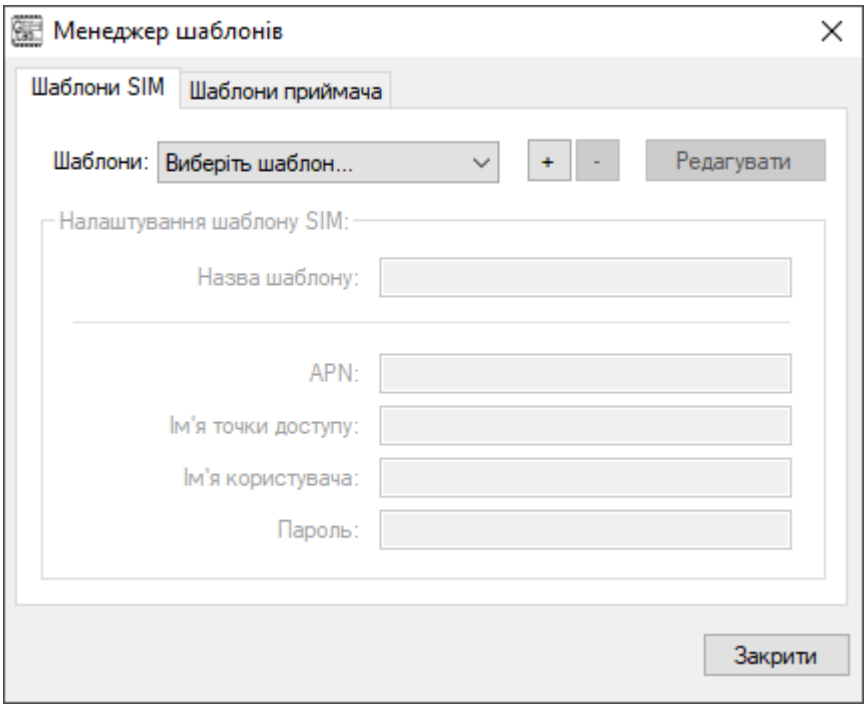


після чого виведе вікно контролю об’єктів. Тут можна створити новий або відредагувати існуючий об’єкт. Якщо до комп’ютера з сервісом GRAPH під’єднано GSM модем, а також створені шаблони для SIM карток в пристроях та вхідних ліній маршрутизатора, можна надсилати SMS з налаштуваннями до пристрою.

Крім того для надсилання SMS з налаштуваннями можна використовувати програму для Android смартфона GRAPH, яку можна завантажити за посиланням: https://glab.com.ua/ua/downloads/APKs/graph.apk

У вікні “Контроль об’єктів” також можливо сконфігурувати алгоритм попередження про блокування, або блокування постановки на охорону об’єктів, власники яких не оплачують послуги охорони.

 - (або F10) кнопка для керування шаблонами. При натисненні програма запитає пароль (опціонально — налаштовується в конфігурації), після чого виведе вікно керування шаблонами.



Шаблони SIM та шаблони приймача можуть бути створені один раз, що дасть змогу економити час при конфігуруванні об’єктів.

 - (або F11) кнопка “Налаштування” призначена для конфігурації програми (дивитись розділ “Конфігурація”).

 - стан каналу отримання повідомлень для GRAPH Client. Якщо колір міняється на червоний -слід перевірити налаштування мережі.