7.1. ?????????? ????? ?????????? ?????? ??????

7.1.1. ???????????? ???????????? ????????????? ??????

З метою увімкнення мережевого захисту з використанням вбудованого міжмережевого екрану, необхідно виконати налаштування шлюзу безпечного обміну за допомогою брандмауера IPtables та командної утиліти ufw.

Перед налаштуванням міжмережевого екрану необхідно:

1. Підготувати відомості про адреси наступних локальних компонентів системи «Трембіта»:

- мережеву адресу серверу робочої станції адміністратора (**<IP_PC_адміністратора>**, при виконанні команд необхідно замінити на реальне значення);

- мережеву адресу серверу баз даних та архівування (**<IP_серверу_баз_даних_та_архівування>**, при виконанні команд необхідно замінити на реальне значення);

- мережеву адресу серверу аналізу журналів подій (**<IP_серверу_аналізу_журналів_подій>**, при виконанні команд необхідно замінити на реальне значення);

- мережеву адресу серверів з вебсервісами та вебклієнтами, які реєструється на шлюзі безпечного обміну (**<IP_вебсервіс>** та **<IP_вебклієнт>**, при виконанні команд необхідно замінити на реальне значення. У випадку необхідності можна продублювати команди з цими скороченнями для всіх серверів з вебсервісами та вебклієнтами);

2. Послідовно виконати наступні команди на шлюзі безпечного обміну, відповідно вказуючи адреси з попереднього пункту:

```
sudo ufw allow from <IP_PC_адміністратора> to any port 22 proto tcp
sudo ufw enable
sudo ufw default deny outgoing
sudo ufw default deny incoming
sudo ufw allow in 5500/tcp
sudo ufw allow out 5500/tcp
sudo ufw allow in 5577/tcp
sudo ufw allow out 5577/tcp
```

```
sudo ufw allow in 5599/tcp
sudo ufw allow out 5599/tcp
sudo ufw allow out 4001/tcp
sudo ufw allow from <IP_PC_адміністратора> to any port 4000 proto tcp
sudo ufw allow out 80/tcp
sudo ufw allow out 443/tcp
sudo ufw allow out 8081/tcp
sudo ufw allow from <IP_вебклієнт> to any port 80 proto tcp
sudo ufw allow from <IP_вебклієнт> to any port 443 proto tcp
sudo ufw allow out 53
sudo ufw allow in 53/tcp
sudo ufw allow out 123/udp
sudo ufw allow out 11371/tcp
sudo ufw allow out from any to <IP_серверу_аналізу_журналів_подій> port 1514
sudo ufw allow out from any to <IP_серверу_баз_даних_та_архівування> port 5432 proto tcp
```

7.1.2. ????????? ???????????? ? ???????? ??????? «????????»

Для додавання репозиторію з пакетами системи «Трембіта» необхідно закоментувати всі вже існуючі рядки у файлі /etc/apt/sources.list (вставляючи символ # на початку кожного рядку) та додати наступний новий рядок в кінці файлу:

```
deb https://project-repo.trembita.gov.ua:8081/repository/ss-1.12.6/ bionic main
```

Швидко це можна зробити за допомогою послідовного виконання наступних двох команд, перша з яких додає символ коментування «#» до кожного непустого рядку, а друга – додає новий рядок з посиланням на репозиторій в кінець даного файлу:

```
sudo sed -i 's/^[A-Za-z0-9]/#&/' /etc/apt/sources.list
echo 'deb https://project-repo.trembita.gov.ua:8081/repository/ss-1.12.6/ bionic main' | sudo
tee -a /etc/apt/sources.list
```

Перевірити результат виконання команд можна за допомогою текстового редактора nano, відкривши файл на редагування за допомогою наступної команди:

```
sudo nano /etc/apt/sources.list
```

> **Примітка.** Для виходу з редактору використовується комбінація клавіш «Ctrl + X». Якщо були внесені змін, то потрібно натиснути клавішу «Y» для їх збереження або «N» для відміни.

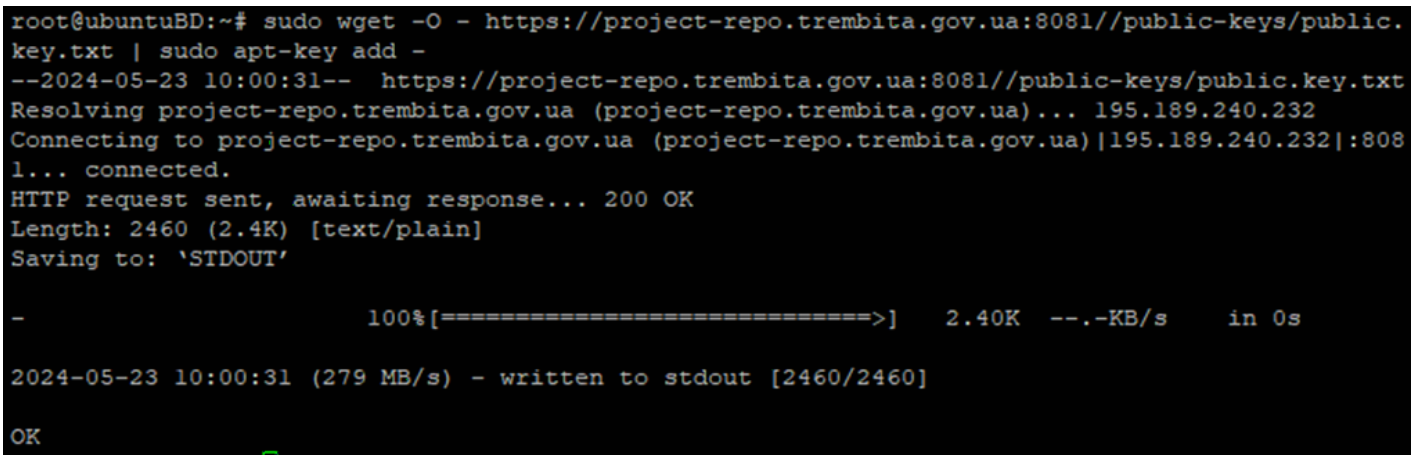
7.1.3. ????????? GPG ????? ??? ???????????

Для встановлення програмного забезпечення з репозиторію системи «Трембіта» потрібно завантажити та додати в систему GPG ключ даного репозиторію.

Для цього Адміністратору локальних компонентів (системному адміністратору) необхідно виконати наступну команду:

```
sudo wget -O - https://project-repo.trembita.gov.ua:8081//public-keys/public.key.txt | sudo apt-key add -
```

Якщо команда виконана успішно, буде виведено повідомлення «OK»

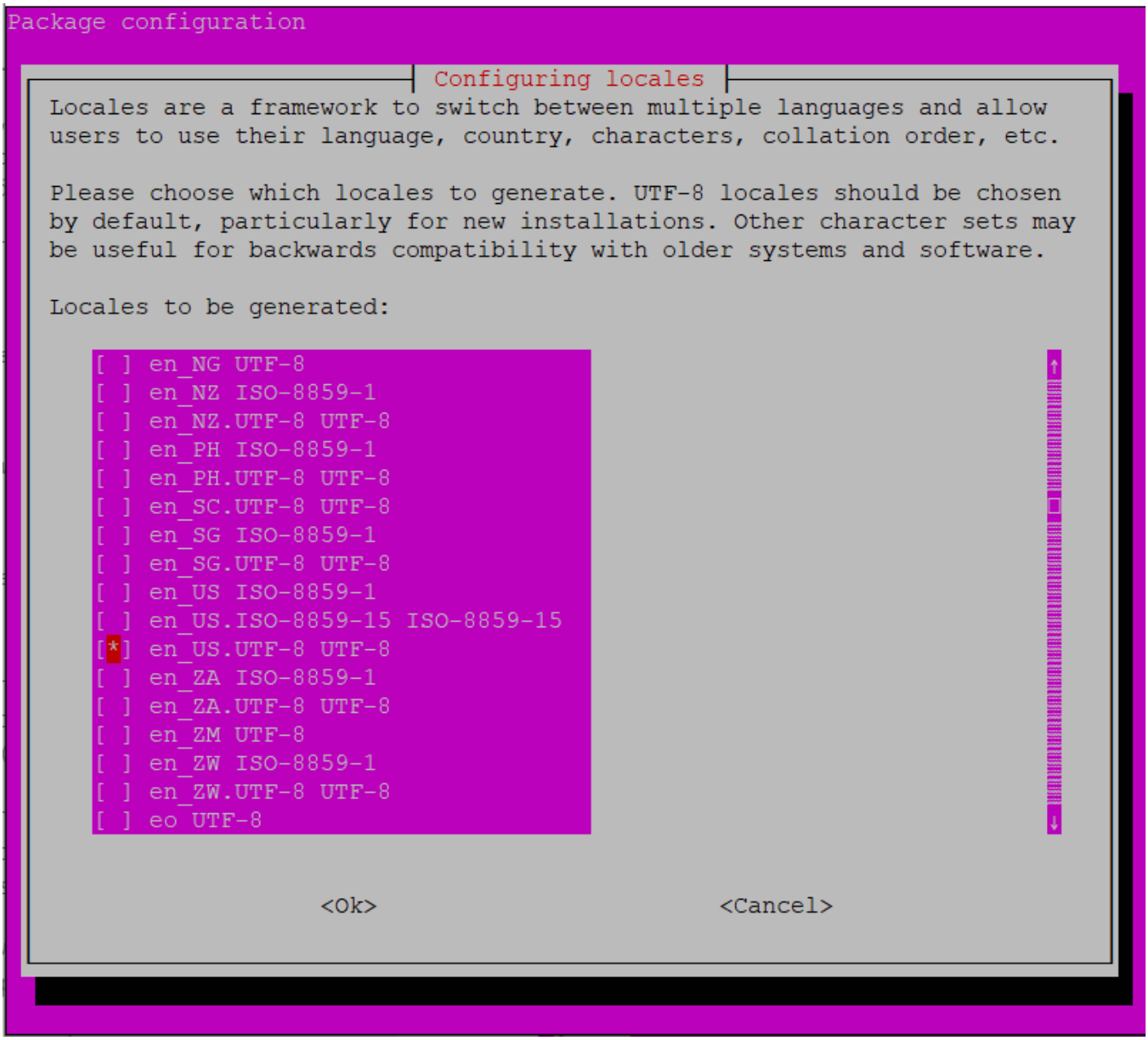


7.1.4. ???????????? ??????

Якщо локалі «en_US.utf8» немає в системі, Адміністратору локальних компонентів (системному адміністратору) необхідно згенерувати її за допомогою послідовного виконання наступних команд:

```
sudo locale-gen en_US.UTF-8
sudo dpkg-reconfigure locales
```

У наступному діалоговому вікні необхідно знайти запис «en_US.UTF-8 UTF-8», встановити відповідну позначку шляхом натискання кнопки [SPACE] та натиснути на кнопку [ENTER]:



У діалоговому вікні «Default locale for a system environment» потрібно обрати «en_US.UTF-8» та перезайти в обліковий запис користувача (наприклад, закривши поточну та ініціювавши нову сесію SSH).

В операційній системі шлюзу безпечного обміну має бути встановлена локаль «en_US.UTF-8». Для встановлення даної локалі необхідно виконати наступну команду:

```
echo 'LC_ALL=en_US.UTF-8' | sudo tee -a /etc/environment
```

Та перезавантажити змінні оточення за допомогою виконання наступної команди:

```
. /etc/environment
```

> **Важливо!** Варто звернути увагу на наявність пробілу після першої крапки у команді вище.

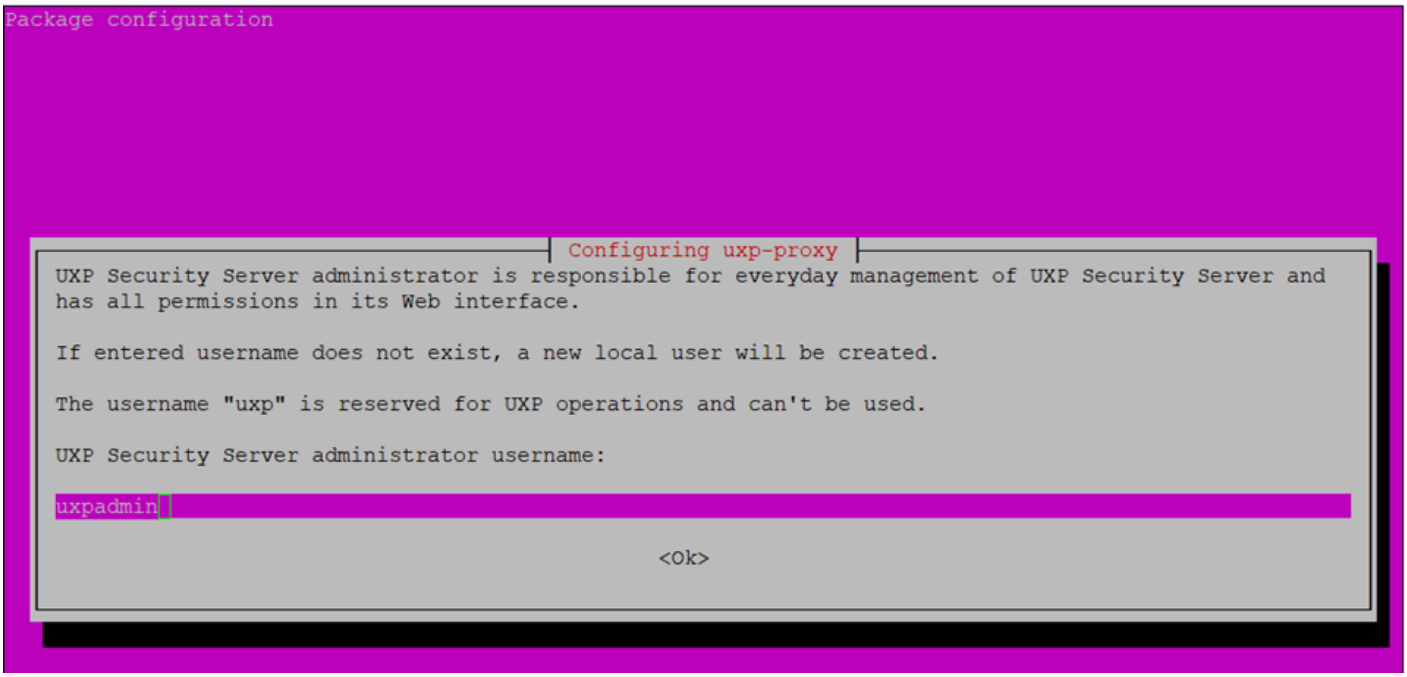
7.1.5. ???????????? ?????? uxp-securityserver-ua

Для встановлення програмного забезпечення UXP Security Server для шлюзу безпечного обміну використовується команда apt. Перед встановленням потрібно оновити список доступних пакетів з репозиторію системи «Трембіта».

Для встановлення зазначеного програмного забезпечення Адміністратору локальних компонентів (системному адміністратору) необхідно послідовно виконати наступні команди:

```
sudo apt update
sudo apt install -y uxp-securityserver-ua libc6=2.27-3ubuntu1.6
```

Під час встановлення необхідно ввести ім’я облікового запису (логін) Адміністратора вебсервісів, що буде адмініструвати функціонал шлюзу безпечного обміну - наприклад, *uxpadmin*:



Цей користувач зможе авторизуватись в вебінтерфейсі адміністрування шлюзу безпечного обміну.

Для перевірки стану виконання встановлених компонентів ПЗ UXP Security Server після інсталяції ШБО необхідно виконати наступну команду:

```
sudo systemctl list-units | grep "uxp"
```

Список сервісів UXP, які мають бути активними (active/running):

```
uxp-confclient.service
uxp-jetty.service
uxp-monitor.service
```

```
uxp-proxy.service
uxp-signer.service
uxp-uaic.service  (якщо встановлений модуль контролю цілісності)
```

7.1.6. ????????? ??????????? ?????????? ?????? ????????????? ???????????

> **Важливо!** В разі, якщо виникає необхідність роботи з вебінтерфейсом ШБО у декількох співробітників Учасника системи "Трембіта", кожен з них обов'язково повинен мати власний обліковий запис!

Шлюз безпечного обміну використовує локальних користувачів і групи операційної системи для контролю доступу до вебінтерфейсу адміністрування шлюзу безпечного обміну.

Обліковий запис, що використовується для входу в вебінтерфейс адміністрування шлюзу безпечного обміну – це обліковий запис Адміністратора вебсервісів (за замовчуванням з логіном uxpadmin).

Для створення додаткового Адміністратора вебсервісів, Адміністратору локальних компонентів (системному адміністраторові) необхідно:

1. Послідовно виконати наступні команди:

```
sudo useradd -M -N <username>
sudo chsh -s /bin/false <username>
sudo passwd <username>
```

де **<username>** - логін створюваного користувача латиницею.

2. Ввести пароль нового користувача двічі.

7.1.7. ????????? ??????????? ?????????? ?????? ????????????? ?? ?????????? ???????

У випадку, коли локальні компоненти системи «Трембіта» адмініструє Оператор, уповноваженому співробітнику Суб’єкта електронної взаємодії, що відповідає за встановлення інформаційної взаємодії та управління особистими ключами електронної печатки (Відповідальному за управління ключами), потрібно надати доступ до функціоналу ШБО.

Для цього потрібно створити обліковий запис Відповідального за управління ключами, який буде використовуватись для входу в вебінтерфейс адміністрування ШБО, шляхом

послідовного виконання наступних команд:

```
sudo useradd -M -N <security-officer>
sudo adduser <security-officer> uxp-security-officer
sudo chsh -s /bin/false <security-officer>
sudo passwd <security-officer>
```

де **<security-officer>** - логін створюваного користувача латиницею.

Після виконання цих команд необхідно ввести пароль нового користувача двічі.

7.1.8. ???????????? ?????? ???????? ??????????

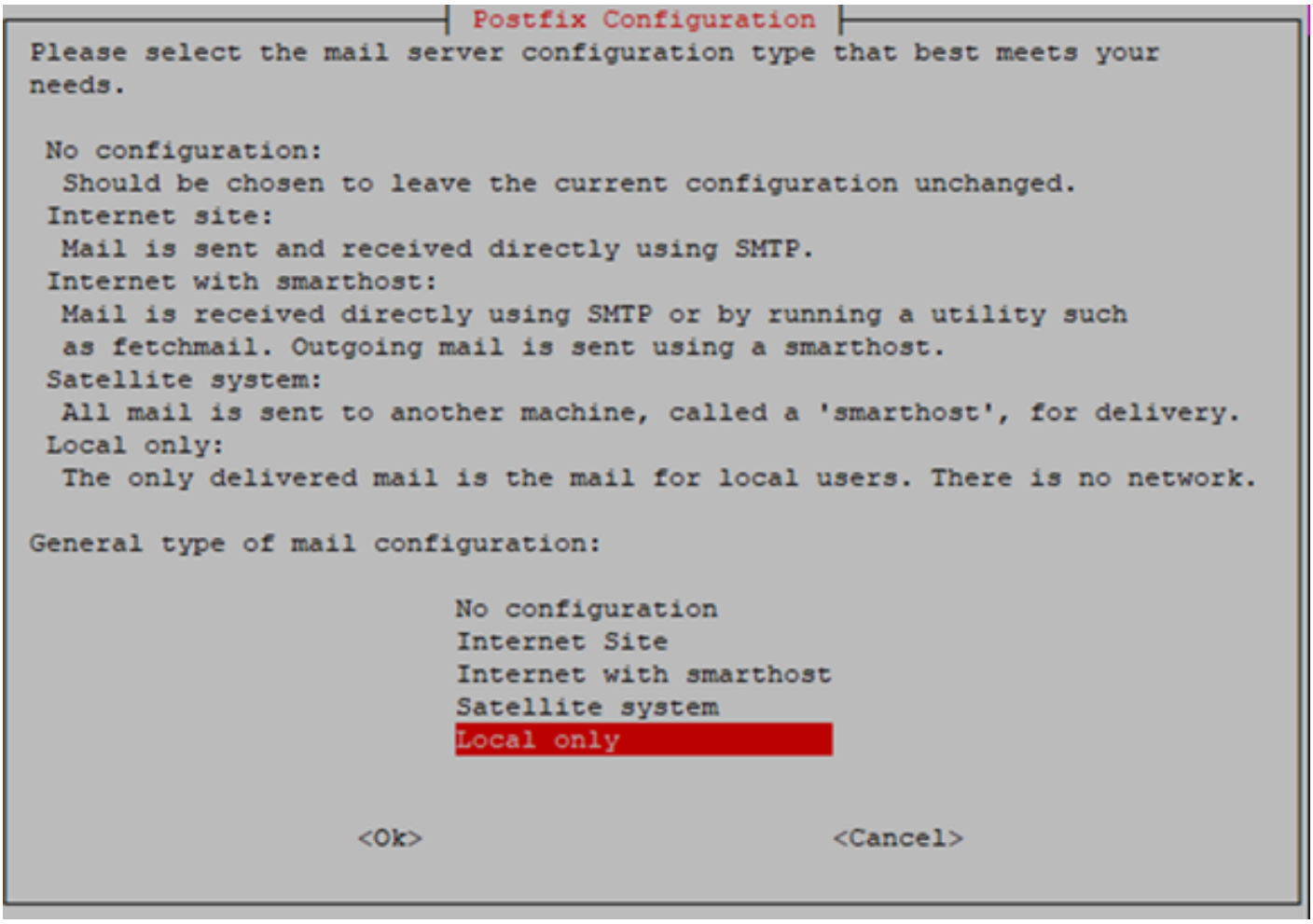
Цілісність програмного забезпечення шлюзу безпечного обміну гарантується модулем контролю цілісності.

> **Важливо!** Цей модуль є обов’язковим для встановлення на шлюзі безпечного обміну промислового середовища!

Встановлення модуля контролю цілісності необхідно виконати наступну команду:

```
sudo apt install uxp-addon-securityserver-uaic nginx-light=1.14.0-0ubuntu1.7 libpam0g=1.1.8-3.6ubuntu2.18.04.2 libnginx-mod-http-echo=1.14.0-0ubuntu1.7 nginx-common=1.14.0-0ubuntu1.7 bash=4.4.18-2ubuntu1.2 passwd=1:4.5-1ubuntu2
```

Під час встановлення необхідно налаштувати параметри надсилання повідомлень електронною поштою (за допомогою утиліти Postfix). Якщо даної потреби немає, необхідно обрати варіант «Local only» та підтвердити запропоновані варіанти за замовченням щодо імені хоста та електронної пошти:



Примітка. Після встановлення модуля контролю цілісності, програма встановлення початково призупиняє перевірку цілісності на 30 хвилин, щоб запобігти запуску перевірки цілісності та призупиненню сервісів під час процесу конфігурації шлюзу безпечного обміну. Якщо конфігурування триває довше, необхідно додатково призупинити перевірку цілісності у вебінтерфейсі шлюзу безпечного обміну, натиснувши на кнопку «Перевірка цілісності призупинена на ## хв», щоб отримати більше часу.

7.1.9. ??????? ??????? ?? ????????????? ????? ?????????? ?????? ? ??????? ??????? ?????????????

> **Важливо!** В промисловому середовищі користувачі з ролями «Адміністратор вебсервісів» та «Відповідальний за управління ключами» повинні підключатися до вебінтерфейсу ШБО виключно з робочих станцій адміністратора!

> **Примітка.** Якщо Суб'єкт електронної взаємодії та Учасник є різними юридичними особами, то Суб'єкт електронної взаємодії аналогічно повинен мати власну робочу станцію адміністратора.

Керування доступом до вебінтерфейсу ШБО здійснюється за допомогою налаштувань NGINX.

Перелік IP-адрес, з яких можна підключитись до ШБО знаходиться у файлі дозволених хостів.

> **Важливо!** Даний файл повинен містити виключно адреси довірених робочих станцій адміністратора. Адміністратор локальних компонентів (системний адміністратор) повинен завжди тримати перелік дозволених адрес у актуальному стані.

Для того, щоб додати IP-адресу робочої станції адміністратора до файлу дозволених хостів необхідно:

1. Відкрити на редагування файл /etc/uxp/uaic/allowed_hosts.conf у текстовому редакторі nano за допомогою виконання наступної команди:

```
sudo nano /etc/uxp/uaic/allowed_hosts.conf
```

2. Додати до файлу наступний рядок:

```
allow <workstation-IP>;
```

де **<workstation-IP>** – IP-адреса робочої станції адміністратора, що буде використовуватися для доступу до вебінтерфейсу ШБО.

3. Зберегти зміни і закрити редактор. Для цього необхідно натиснути комбінацію клавіш «Ctrl+X», ввести «Y» для підтвердження збереження внесених змін та натиснути на клавішу

«Enter».

4. Перевірити конфігурацію за допомогою виконання наступної команди:

```
sudo nginx -t
```

Якщо перевірку конфігурації пройдено успішно, буде виведено повідомлення «test is successful»:

5. Перезавантажити сервіс NGINX, щоб застосувати зміни на ШБО, за допомогою виконання наступної команди:

```
sudo service nginx reload
```

Перед виконанням подальших налаштувань ШБО, необхідно обчислити нові значення геш-функцій програмних компонентів ШБО за допомогою виконання наступної команди:

```
sudo uxp-ua-integritychecker.sh recalc_all
```

Версія #16
Admin створив 2024-05-28 09:37:35 UTC
Admin оновив 2024-09-25 11:57:00 UTC