ВАЖЛИВА ІНФОРМАЦІЯ

Необхідні дії після оновлення ядра операційної системи.

Маємо:

- операційна система:

```
root@QuantUUB:~# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.6 LTS
Release:        16.04
Codename:       xenial
```

- ядро:

```
root@QuantUUB:~# uname -a
Linux QuantUUB 4.4.0-171-generic #200-Ubuntu SMP Tue Dec 3 11:04:55 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
```

В операційній системі Ubuntu 16.04 LTS після чергового оновлення операційної системи активовано механізм автоматичного оновлення ядра у межах версії (по аналогії з Ubuntu 18.04).

Оновлення ядра операційної системи, призведе до непрацездатності модуля шифрування зі складу Комплексу «QUANT» після перезавантаження операційної системи.

Заборонити оновлення операційної системи Ubuntu 16.04 LTS можливо наступним чином:

- заборонити доступ такого хосту до мережі Інтернет, окрім портів udp/500, udp/4500, на мережевому обладнанні.
- відключити механізму автоматичного оновлення операційної системи у файлі /etc/apt/apt.conf.d/50unattended-upgrades закоментуємо символами «//» всі строки блоку «Unattended-Upgrade::Allowed-Origins» і перезавантажимо ОС:

nano /etc/apt/apt.conf.d/50unattended-upgrades

```
 GNU nano 2.9.3              /etc/apt/apt.conf.d/50unattended-upgrades              Modified

// Automatically upgrade packages from these (origin:archive) pairs
//
// Note that in Ubuntu security updates may pull in new dependencies
// from non-security sources (e.g. chromium). By allowing the release
// pocket these get automatically pulled in.
//Unattended-Upgrade::Allowed-Origins {
//        "${distro_id}:${distro_codename}";
//      "${distro_id}:${distro_codename}-security";
        // Extended Security Maintenance; doesn't necessarily exist for
        // every release and this system may not have it installed, but if
        // available, the policy for updates is such that unattended-upgrades
        // should also install from here by default.
//      "${distro_id}ESM:${distro_codename}";
//      "${distro_id}:${distro_codename}-updates";
//      "${distro_id}:${distro_codename}-proposed";
//      "${distro_id}:${distro_codename}-backports";
//};
```

Якщо сервер оновився – необхідно переінсталювати модуль шифрування зі складу Комплексу «QUANT». Для інсталяції необхідно скопіювати архів програмного забезпечення на сервер та виконати наступні команди (шлях та ім'я файлу, наведено як приклад):

```
cd /root/
rm -rf /root/openswan-2.6.39          # видалити каталог
tar -xzf /root/QUANT-UA-VPN.tar.gz    # розпакувати архів
cd /root/openswan-2.6.39
make clean
make programs
make KERNELSRC=/lib/modules/`uname -r`/build module
sudo make KERNELSRC=/lib/modules/`uname -r`/build install minstall
```

Результат інсталяції не повинен мати помилок.

Після інсталяції необхідно перезавантажити сервіс IPSec:

```
/etc/init.d/ipsec restart
```

Наступним кроком необхідно перевірити наявність створеного IPSec-каналу командою:

```
ipsec eroute
```

та доступність серверів захищених периметрів.