



# Надеждност на QKD мрежите – понятия

- **Надеждност** - вероятност, че дадена система ще изпълнява определени функции при зададени условия в зададен интервал от време;
- **Сигурност** - способността на системата да противодейства на дестабилизиращи фактори и въздействия с цел достъп до ресурси или информация;
- **Изправност** – Всички свойства на системата са налични;
- **Работоспособност** – Съществените свойства на системата са налични;
- **Fail-safe** системи – Системата продължава да изпълнява функциите си по пренос на информация дори да бъде нарушена сигурността ѝ;
- **Fail-secure** системи – Системата прекратява функциите си по пренос на информация, ако сигурността ѝ бъде нарушена.



# Надеждност на QKD мрежите

- Генерирането и предаването на ключове в мрежите за квантово разпространение на ключове (QKD) се считат за много надеждни поради принципите на квантовата механика, на които се основават - принципите на неопределеност и факта, че квантовите състояния не могат да бъдат копирани.
- QKD мрежите гарантират, че всеки опит за прихващане на ключовете ще бъде открит - опитът за прихващане на квантовите състояния, използвани за предаване на ключовете, би нарушил състоянията, от което участващите биха разбрали за присъствието на нарушител. Това гарантира, че ключовете, обменяни в QKD мрежи, остават сигурни и некомпрометирани.



# Надеждност на QKD мрежите

- Надеждността на QKD мрежите може да бъде повлияна от различни фактори:
  - Внедряването на технологията;
  - Качеството на използваните квантови канали;
  - Потенциални уязвимости в системата;
  - Уязвимости в самите устройства съставляващи QKD системата;
  - Несъвършенство на използваните протоколи;
  - Правилен подбор на комуникационната инфраструктура
  - Човешки фактор.



# Надеждност на QKD мрежите

- Надеждността се определя и от правилния избор на „доверени възли“ (Trusted Nodes), в които се извършва т.нар. препредаване на ключовете.
- В тези възли се намесва и сигурността, определена най-вече от човешкия фактор, като продължава развитието на изискванията за „доверен възел“ и дефиниране на границите на сигурността му.
- От съществено значение е да продължи напредъкът в технологията и преодоляването на потенциални предизвикателства, за гарантиране на тяхната ефективност в реални приложения и повишаване на надеждността им във времето.



# Надеждност на QKD мрежите

- QKD мрежите предлагат високо ниво на устойчивост срещу традиционните криптографски атаки, като например атаки човек по средата (Man In The Middle) или опити за силова намеса (brute force).
- Най-важната предпоставка за интегриране на QKD в телекомуникационните мрежи е надеждността ѝ, тъй като мрежите работят 24/7/365.
- Новите устройства в мрежите - QKD, например - не трябва да влошават качеството на услугата - техният параметър MTBF (Mean Time Between Failures) трябва да е поне толкова добър колкото и на комуникационните устройства, чиито трафик следва да бъде криптиран.



# Надеждност на QKD мрежите

- В комерсиалните телекомуникации, в които се предава явна/нечувствителна информация, се предпочита ненадеждна комуникация пред липсата на комуникация. При мрежи с високо ниво на сигурност се предпочита да бъде прекъснатата комуникацията пред това да бъде предадена в явен вид.
- Имплементираните QKD мрежи показват, че е възможна непрекъснатата работа на QKD оборудването и QKD технологията има необходимият потенциал, за да бъде интегрирана в доста сложни мрежови телекомуникационни инфраструктури. Доказала е своята надеждност и устойчивост в реална среда извън лабораторията.

# Заплахи за надеждността и сигурността на QKD

- **Заплахи от естествен произход (касят предимно free space QKD):**
  - ✓ **Атмосферни условия и намеса в околната среда:** атмосферната турбуленция, поглъщане и разсейването влошават качеството на квантовия сигнал по време на предаване – използват се адаптивни системи и се избира подходящо място за разполагане на системите и контрол на околната среда;
  - ✓ **Космическо лъчение:** високоенергийните космически лъчи могат да причинят грешки в квантовите детектори и да въведат шум в квантовите комуникационни системи – техники за екраниране и коригиране на грешки за намаляване на въздействието на космическото лъчение върху квантовите системи;

# Заплахи за надеждността и сигурността на QKD

- **Заплахи, дължащи се на преднамерени действия:**
  - ✓ Подслушване, кибератаки, заглушаване, смущения от изкуствени източници на светлина, саботаж или физически атаки, технологични уязвимости, прекъсвания на захранването и повреда на инфраструктурата;
- **Заплахи от терористичен и военен характер:**
  - ✓ Прекъсване на критична инфраструктура, злоупотреба с квантова технология, враждебна окупация, използване на уязвимости в квантовите комуникационни протоколи или хардуера, подслушване и прихващане на сигнали, кибератаки към класическите комуникационни канали, заглушаване и смущения, физически атаки, заплахи от вътрешен саботаж;

[www.euroqci.bg](http://www.euroqci.bg)

*Проект 101091399 “Национален план за изграждане на QCI за България” е съфинансиран от Европейския съюз.*

*Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.*

*Нито Европейският съюз, нито съфинансиращият орган не носят отговорност за тях.*