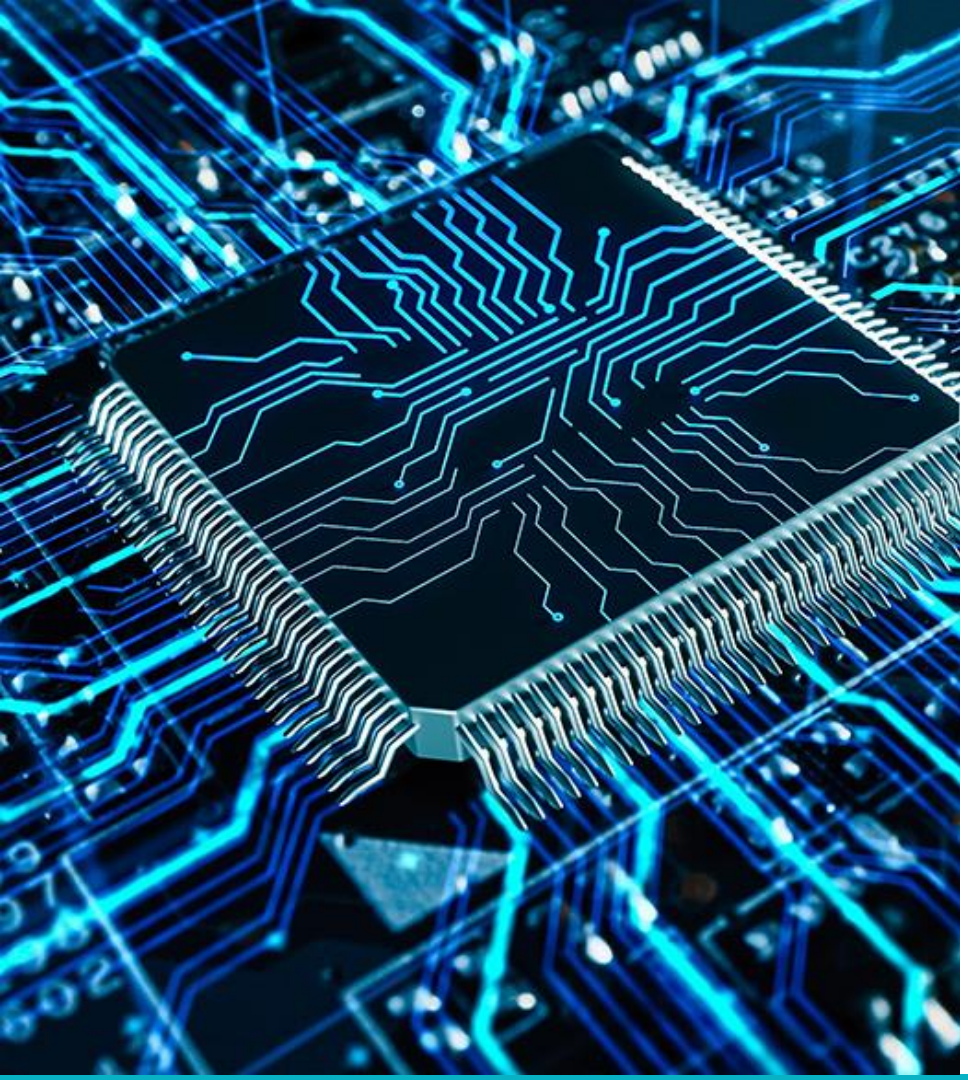
ViPNet QKDSim: симулятор для системы квантового распределения ключей

Иванов Олег
Менеджер

ViPNet QKDSim

ViPNet QKDSim наглядно показывает эмуляцию принципов квантового распределения ключей, основанного на принципах генерации и считывания оптических информационных состояний.

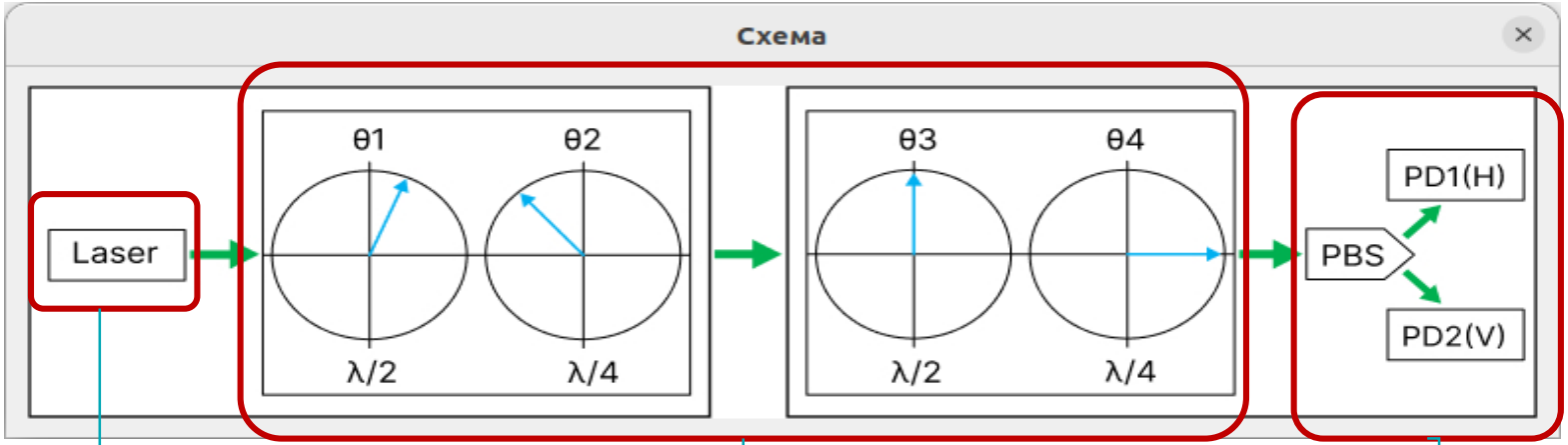
Информация в оптических состояниях кодируется и декодируется путем изменения параметров поляризации генерируемого светового потока, которые интерпретируются как параметры протоколов КРК.



Назначение ViPNet QKDSim

- Подготовка специалистов по информационной безопасности
- Подготовка специалистов по квантовым технологиям
- Обучение в продвинутых школах и колледжах

Оптическая схема



Алиса
Лазер

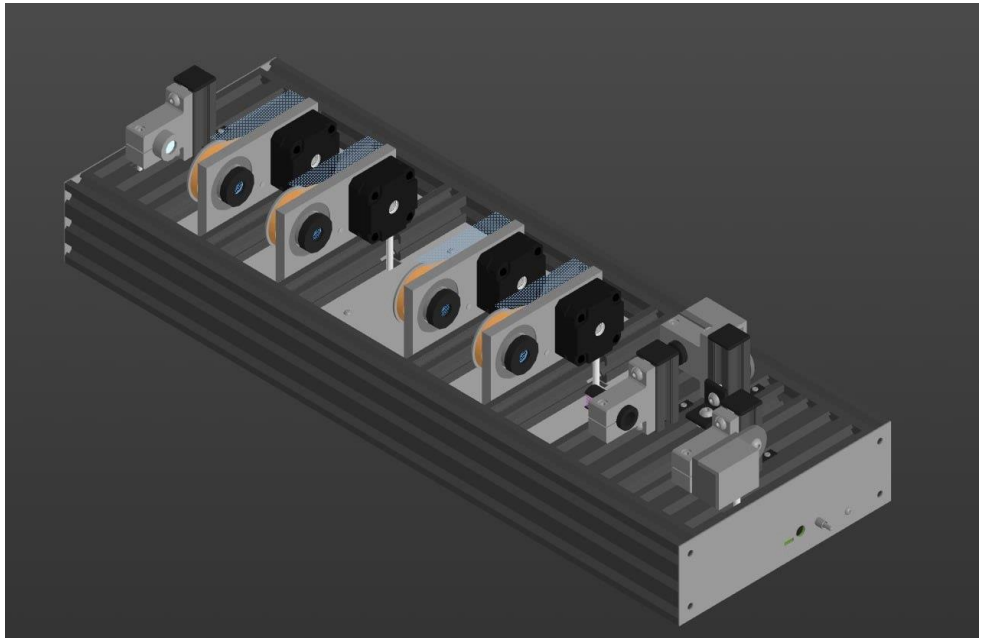
Модулятор
поляризации света

Боб
Поляризационный куб
и 2 фотодетектора

Аппаратная платформа

Особенности:

- Управление с помощью ПК (ноутбука)
- Усиливает восприятие материала
- Возможность установить дополнительные элементы



Применение в образовательной сфере

Физические основы

- Формирование поляризационных состояний
- Регистрация поляризованного света

Классическая передача информационных бит

- Принципы поляризационного кодирования бит
- Принципы детектирования бит
- Шумы в детекторах
- Ошибки передачи

Квантовая передача информационных бит

- Детектирование одиночных фотонов
- Шумы в детекторах
- Ошибки передачи

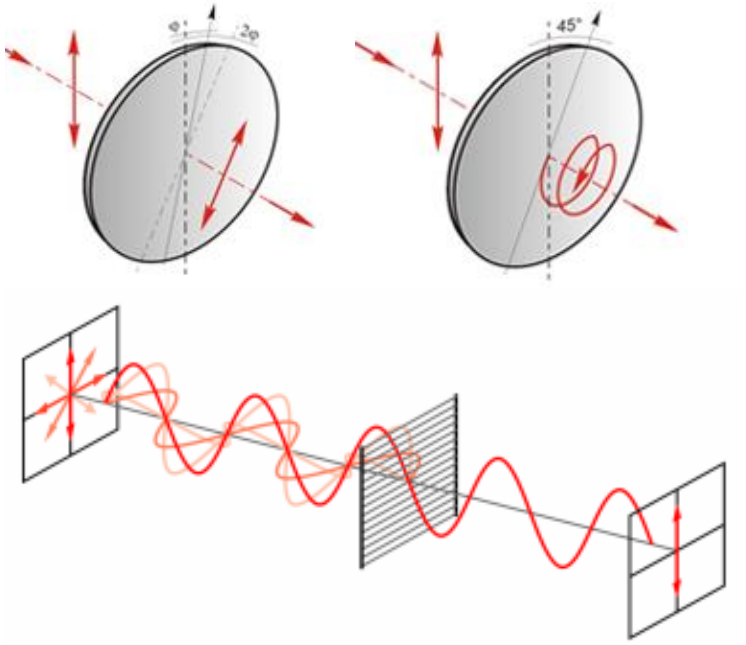
Квантовое распределение ключей

- Понятие о базисах кодирования
- Алгоритмы формирования и детектирования посылок
- Постобработка распределяемой последовательности

Безопасность передачи и распределения ключей

- Проведение атак на протоколы и системы КРК
- Связь ошибки распределения ключей с информацией, доступной нарушителю

Изучение физических основ: темы

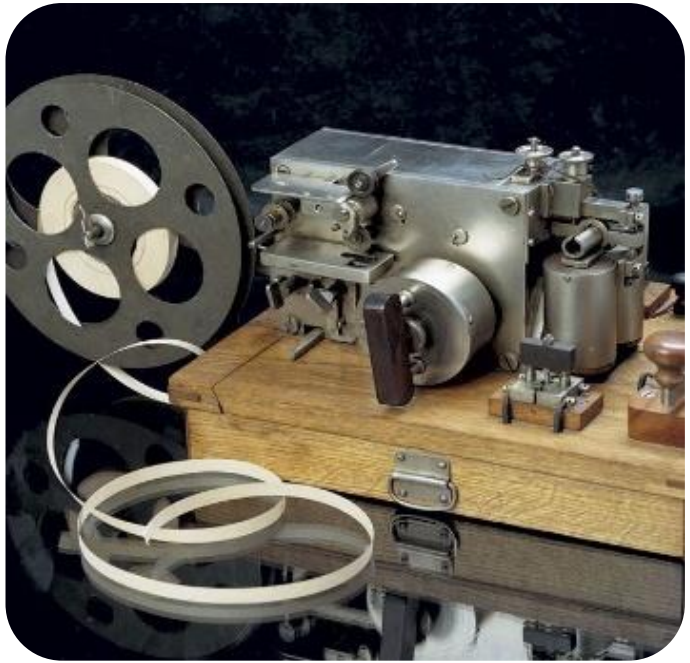


- Поляризация света
- Волновые пластины
- Управление поляризацией света (модуляция/демодуляция)
- Поляризатор-анализатор и регистрация света
- Базисы измерений

Распределение ключей (информационных бит): темы

Классические системы приёма-передачи

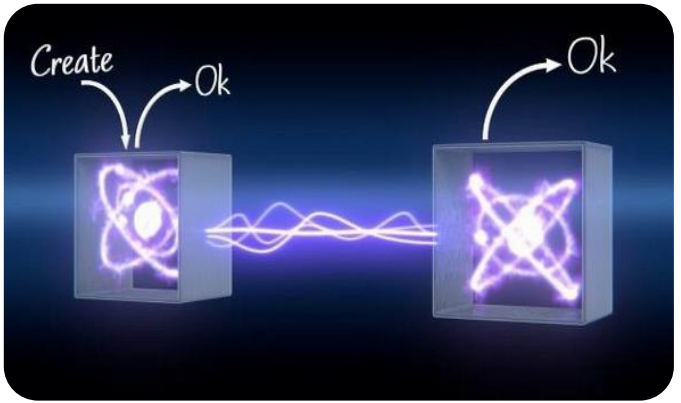
- Классическая передача информации
- Распределение информации с классическим излучателем
- Влияние чувствительности и шумов детекторов на классическую передачу информации (устойчивость системы)
- Влияние нарушителя на классическую передачу информации



Распределение ключей (информационных бит): темы

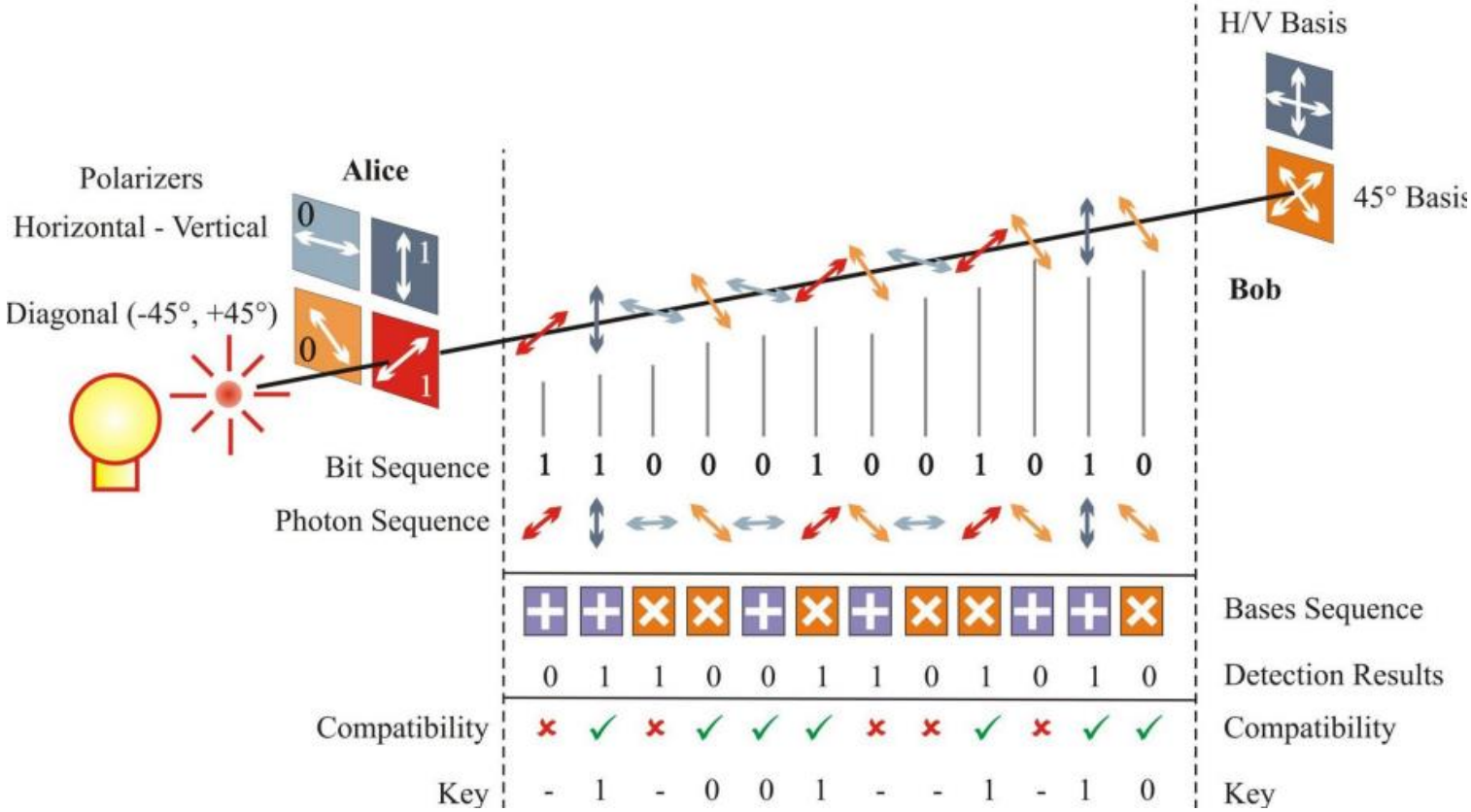
Квантовые системы приёма-передачи

- Однофотонные и квазиоднофотонные излучатели
- Квантовое распределение ключей (информационных бит)
- Влияние чувствительности и шумов детекторов на квантовое распределение ключей (устойчивость системы)
- Влияние нарушителя на квантовое распределение ключей (информационных бит)



Протокол BB84

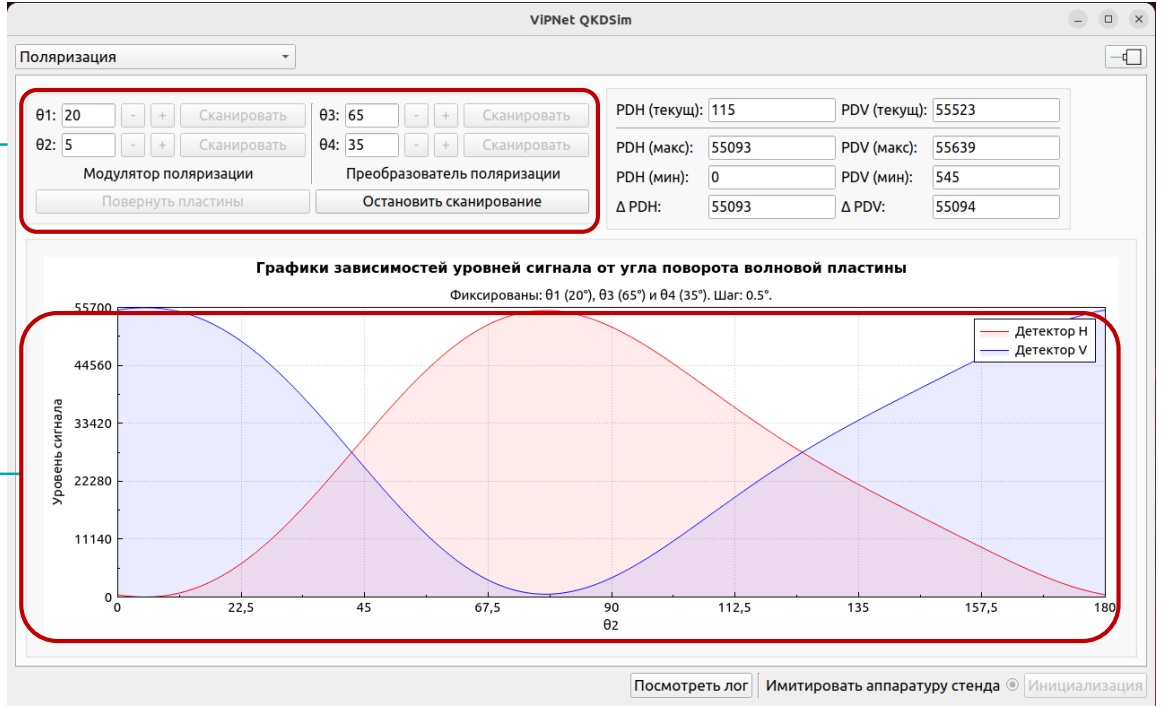
Схема протокола BB84



Определение базиса и сканирование

Задаем значения углов поворота пластин и запускаем сканирование пластины θ2

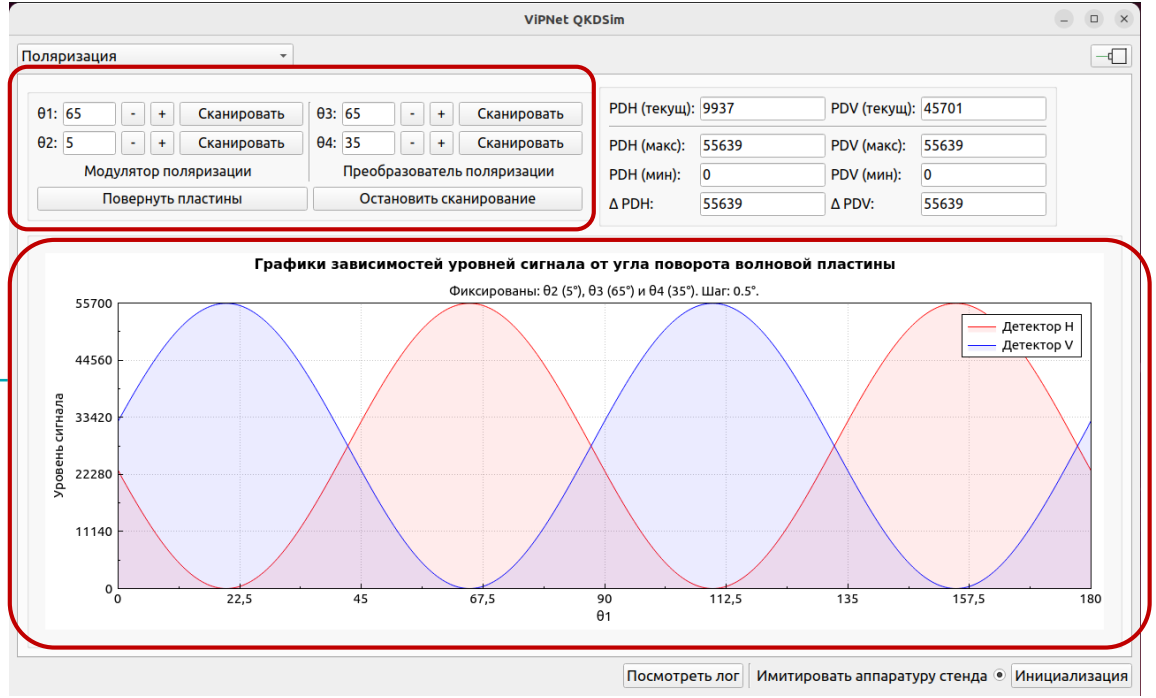
Полученный график



Определение базиса и сканирование

Задаем значения углов поворота пластин и запускаем сканирование пластины θ1

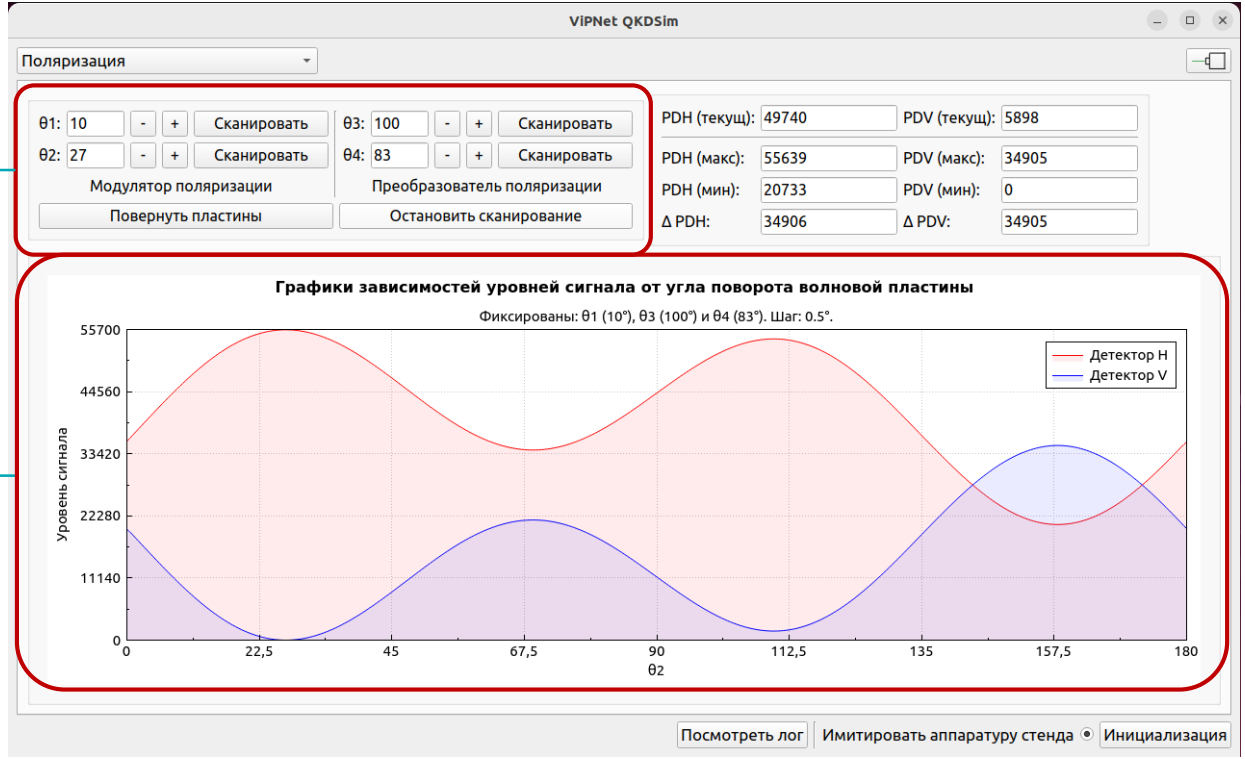
Полученный график



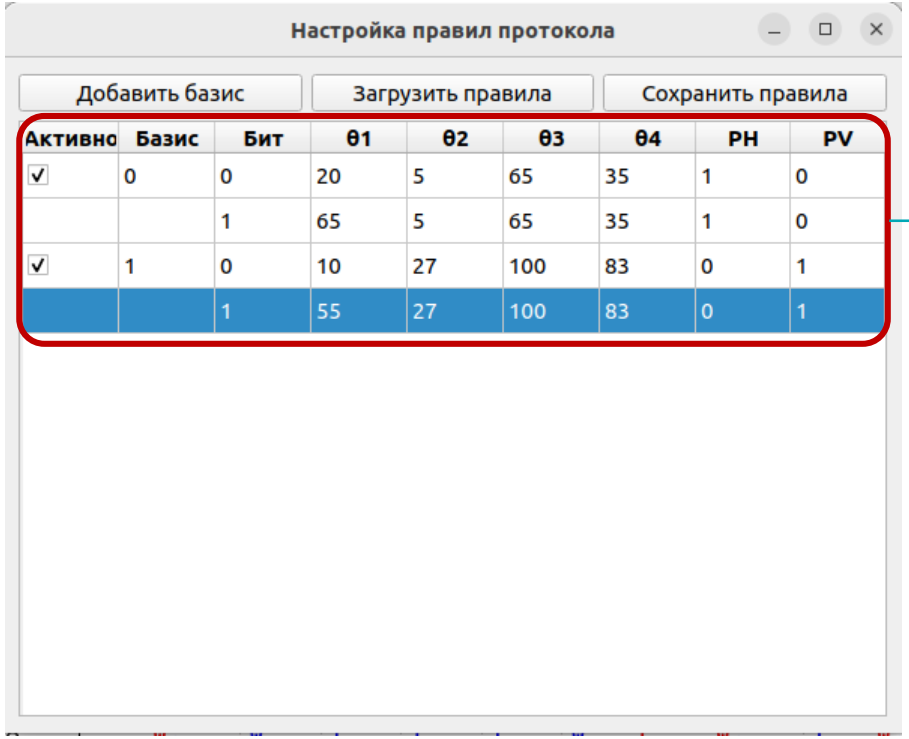
Подбор конфигурации углов

Задаем значения углов поворота пластин и запускаем сканирование пластины θ2

Полученный график

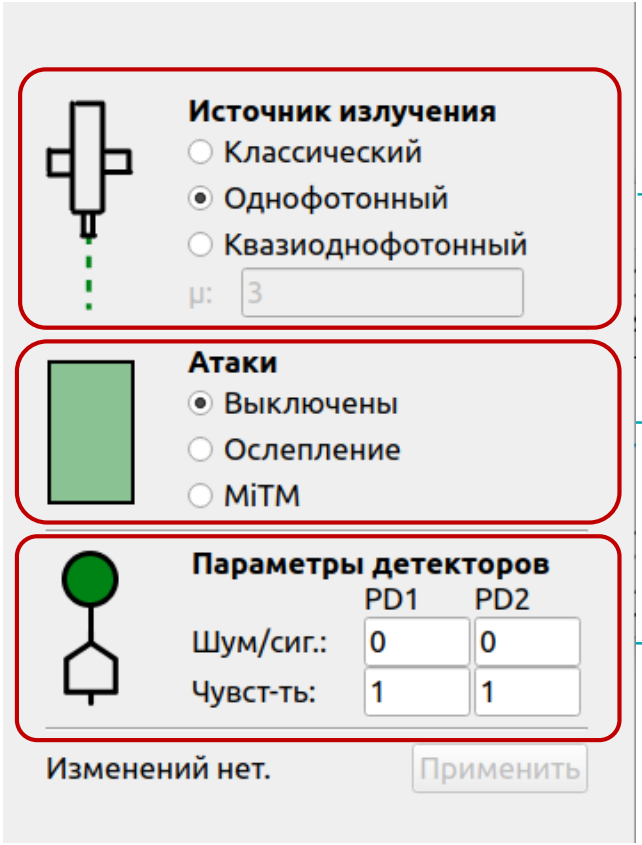


Настройка правил протокола



Результаты сканирования углов добавляем в настройки правил протокола

Имитируемые параметры

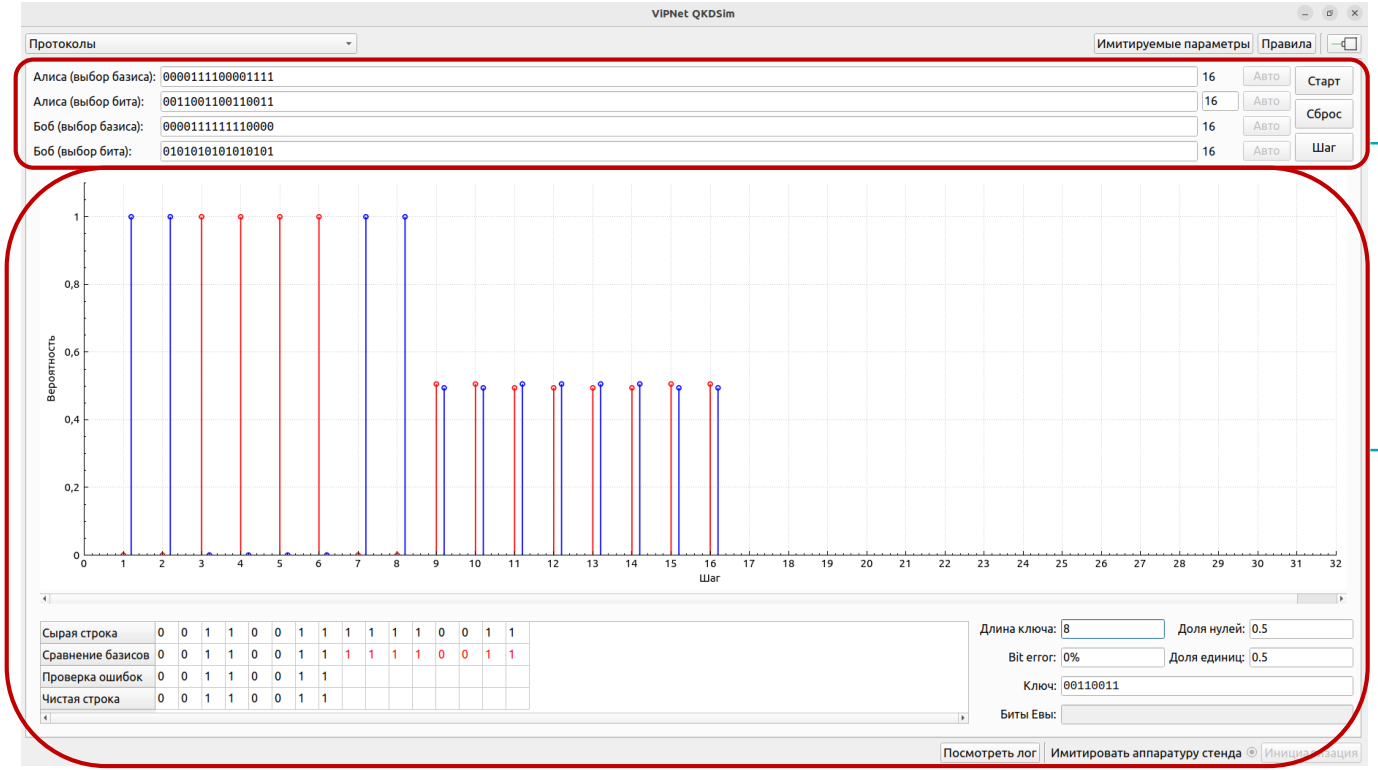


Имитация источника излучения

Имитация нарушителя

Имитация параметров детекторов

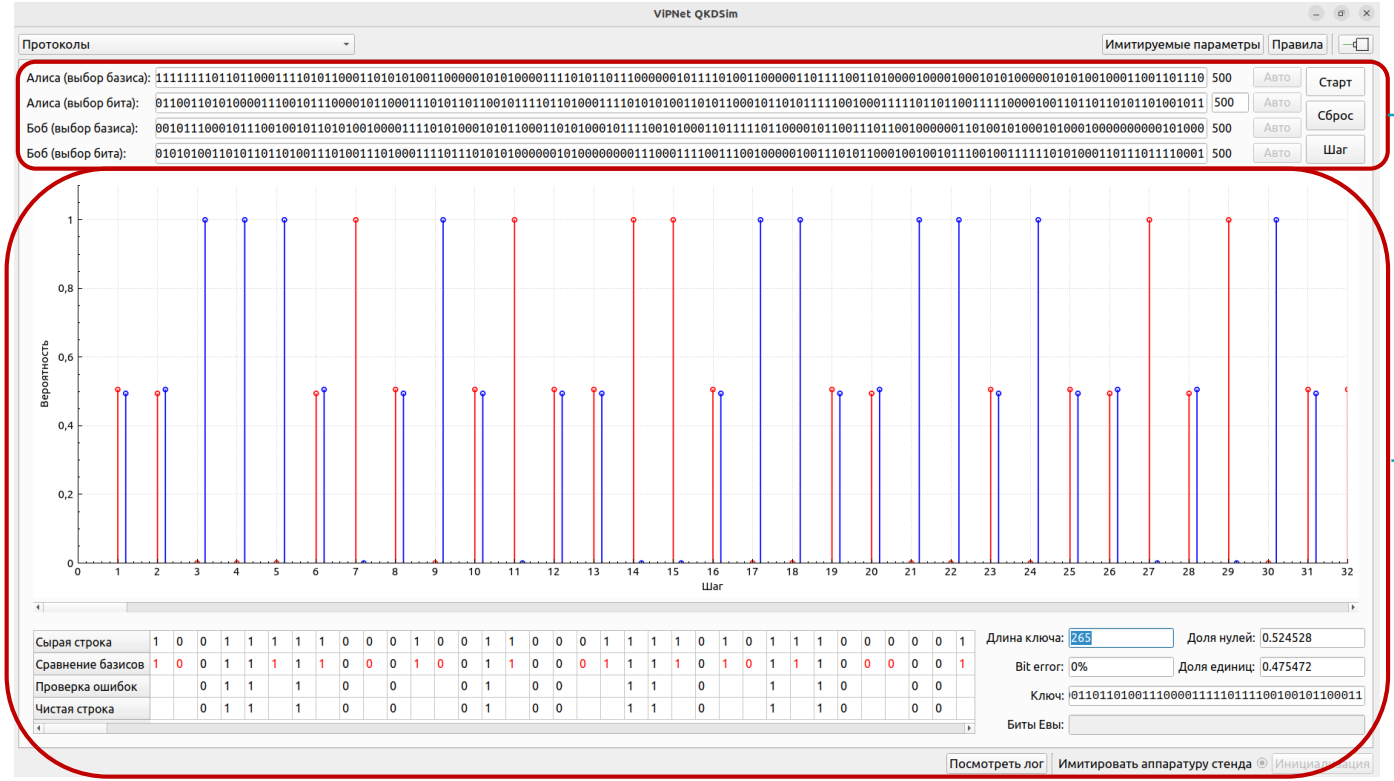
Тестовая комбинация



Тестовая комбинация кодируемых базисов и бит

Результаты выполнения протокола

Тестовая комбинация



Увеличим количество бит до 500

Результаты выполнения протокола

Спасибо за внимание!

Иванов Олег
Oleg.Ivanov@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363