Оценка эффективности мер защиты от атаки лазерного повреждения на компоненты волоконно-оптических систем квантового распределения ключей

Бугай Кирилл
Специалист ООО «СФБ лаборатория»

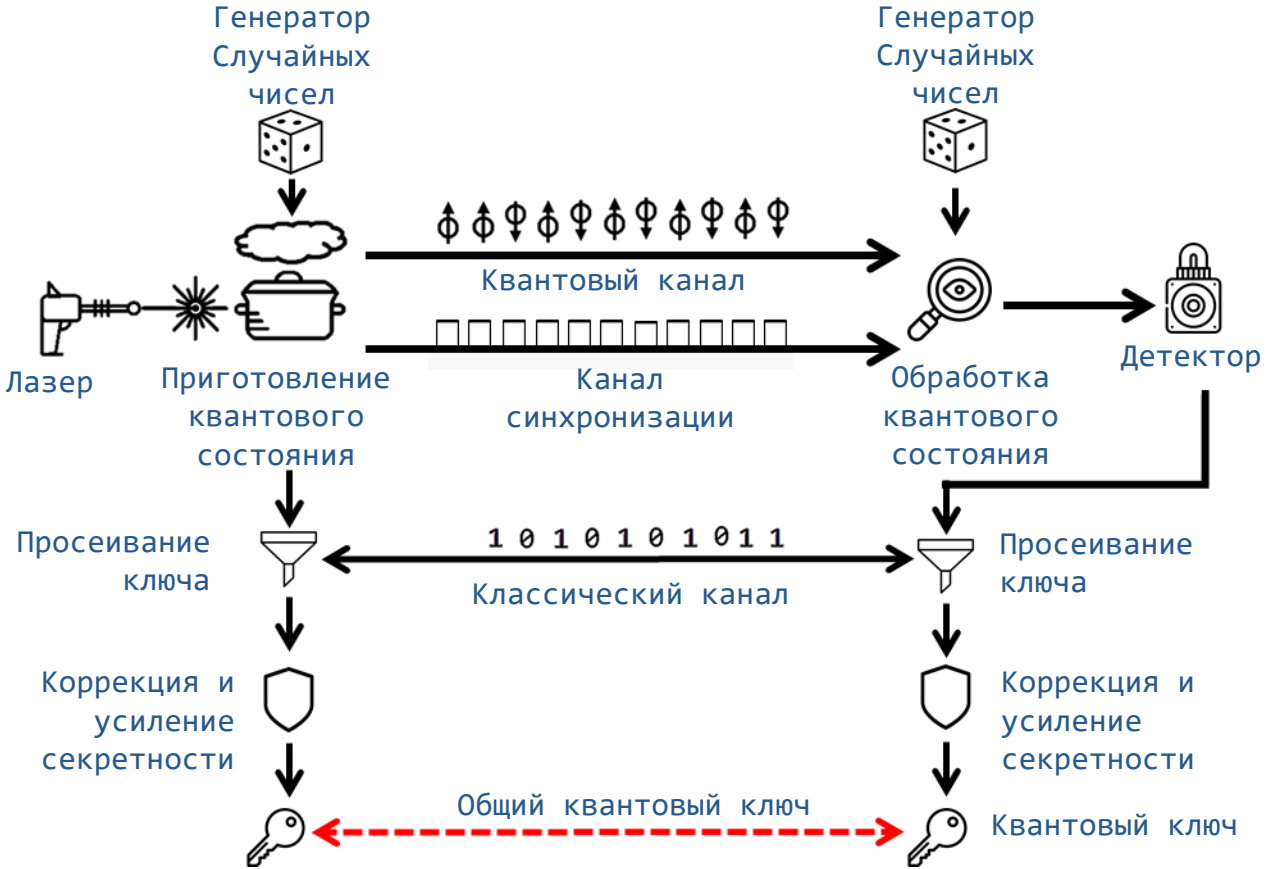
Содержание

Введение

> Криптография – это очень серьезная наука. Не исключаю того, что самая сложная математическая дисциплина.

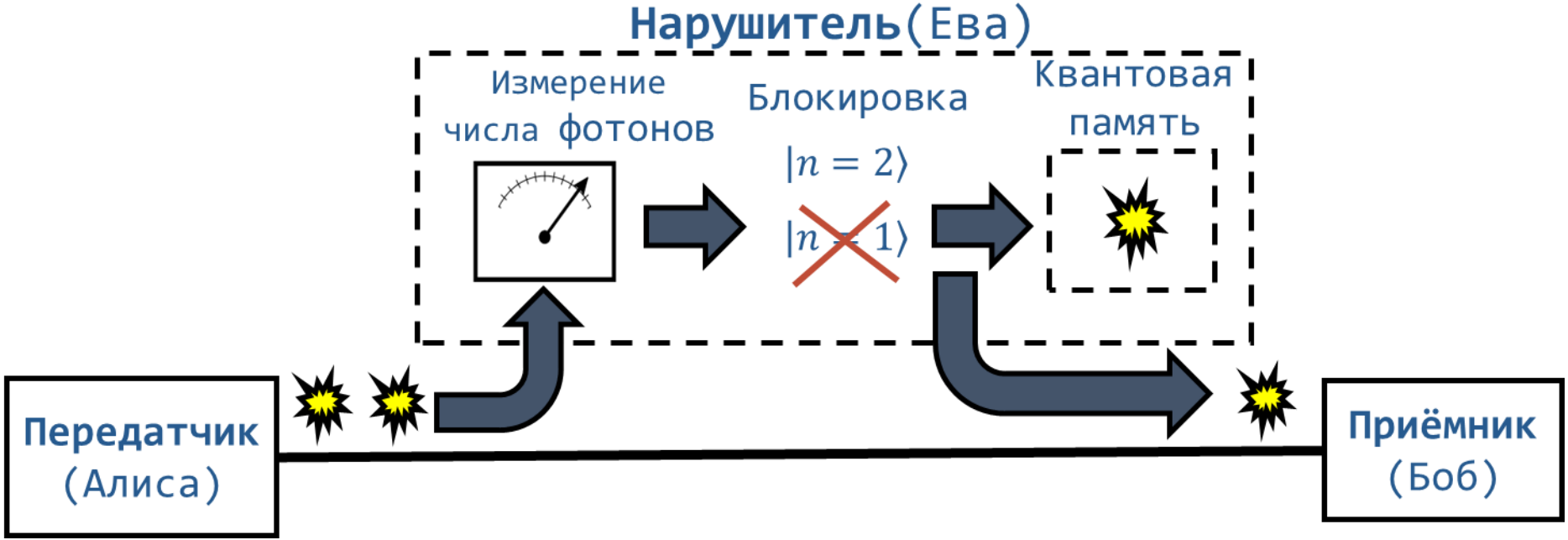
Евгений Касперский

Принцип работы



PNS атака

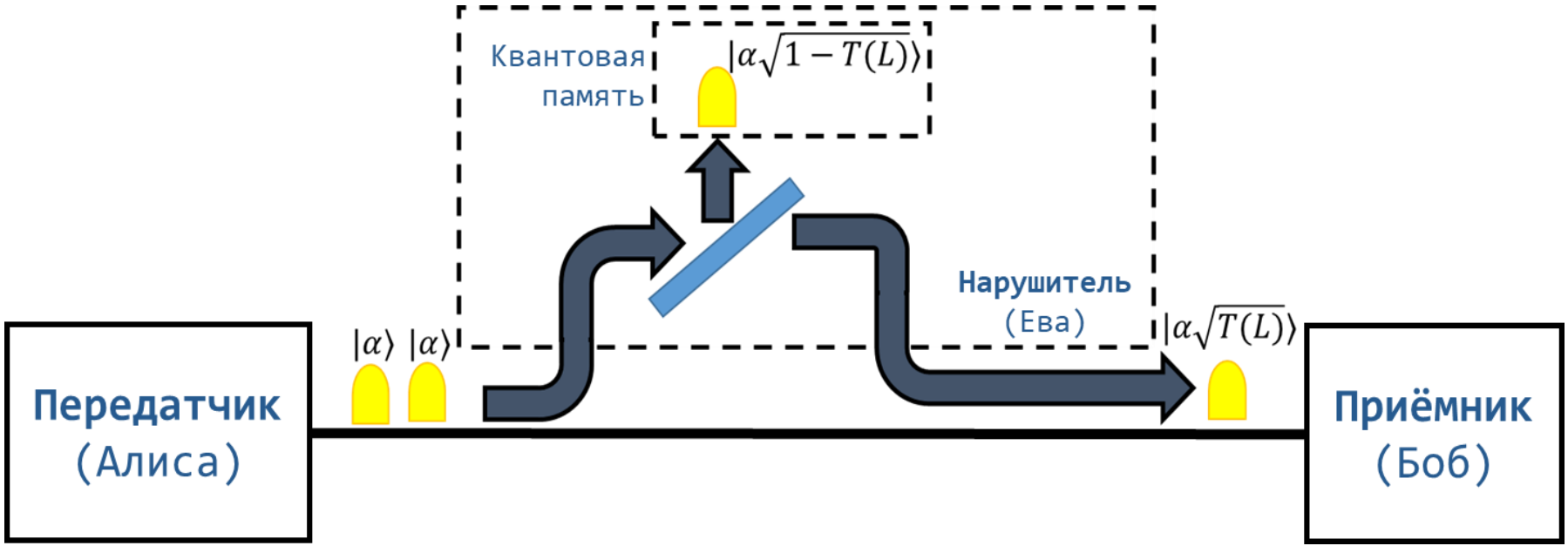
Photon **N**umber **S**plitting – атака с расщеплением по числу фотонов. Применяется к системам КРК, использующих **ослабленные лазерные состояния** вместо **строго однофотонных.**



Lütkenhaus N., Jahma M. //New Journal of Physics.– 2002. – №. 1.

BS атака

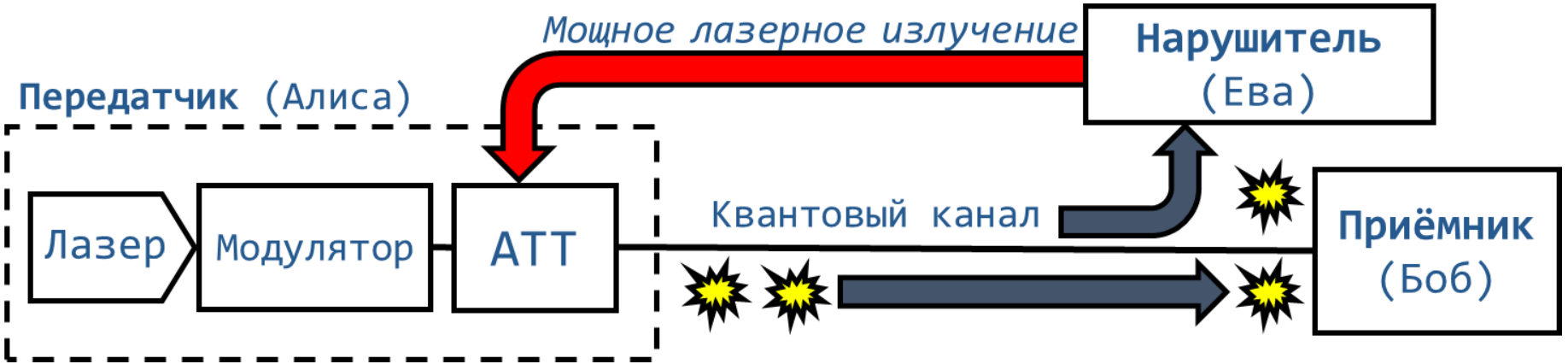
Beam **S**plitting – атака светоделителем. **Ева отводит часть** каждого состояния в квантовую память, а оставшуюся часть посылает Бобу **по каналу без затухания.** Однако Ева получает лишь частичную информацию, ограниченную **величиной Холево.**



Calsamiglia J., Barnett S. M., Lütkenhaus N. //Physical Review A. – 2001.– №. 1.

Атака лазерного повреждения

Воздействие мощным лазерным излучением на волоконно-оптический аттенюатор вызывает изменение его коэффициента поглощения, что приводит к уязвимости систем КРК к атакам на протокол и атакам на техническую реализацию.



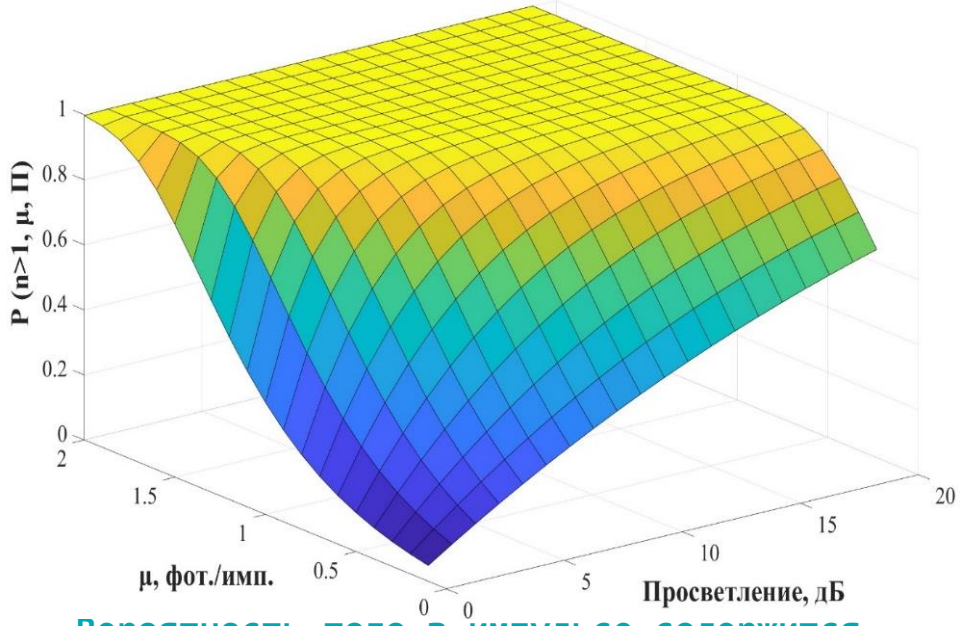
Makarov V. et al. //Physical Review A. – 2016. – №. 3.

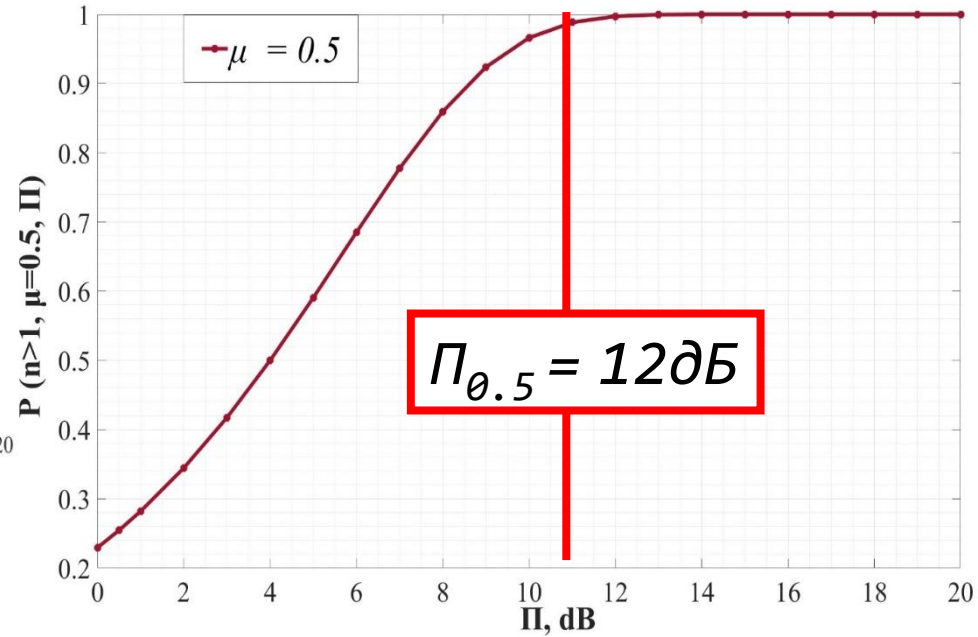
Метод и критерий

> Поощряйте тех кто ищет истину, но опасайтесь тех, кто найдет её.

Вольтер

Критерий оценки



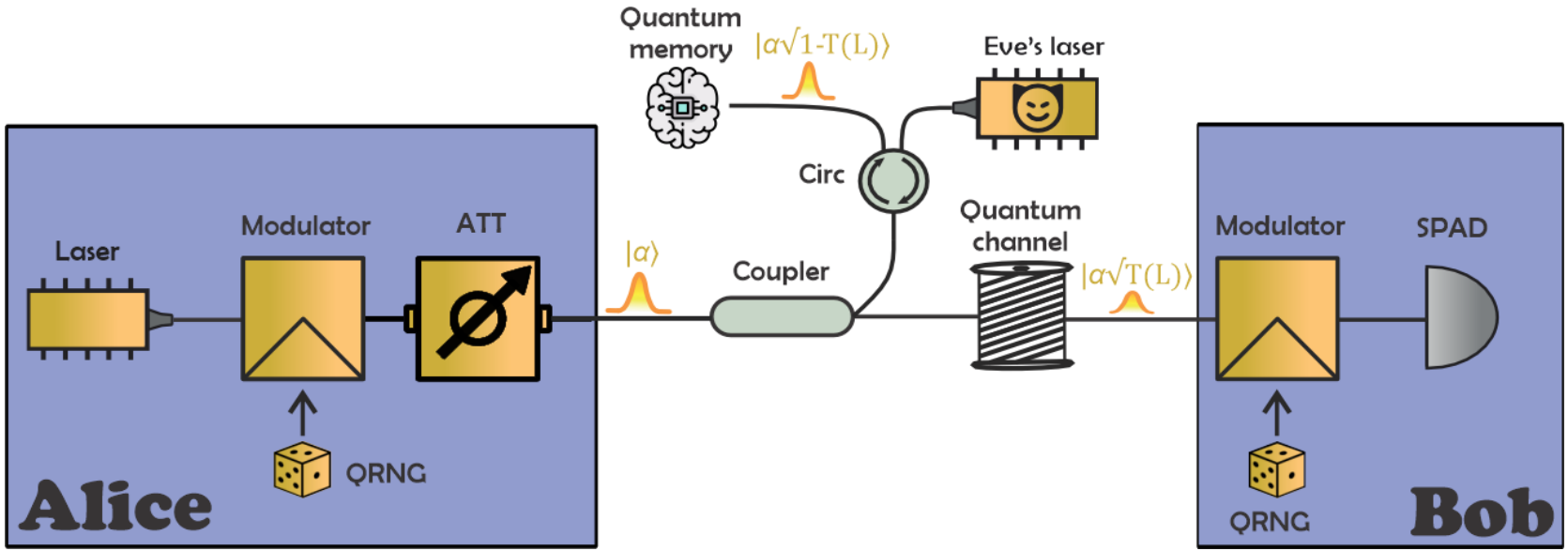


Вероятность того в импульсе содержится более одного фотона:

$$P(n>1|n>0,\Pi,\mu)=\frac{1-e^{-\mu\cdot 10^{\frac{\Pi}{10}}}\left(1+\mu\cdot 10^{\frac{\Pi}{10}}\right)}{1-e^{-\mu\cdot 10^{\frac{\Pi}{10}}}}$$

Критерий оценки

Нарушитель может воспользоваться **атакой светоделителем совместно** с использованием **атаки лазерного повреждения.**



Критерий оценки

В результате такой атаки энтропия Фон Неймана будет равна:

$$H(\rho_{XE}|\rho_{E}) = 1 - \chi(\mu),$$

Величина Холево будет равна:

$$\chi(\mu) = e^{-\mu \cdot 10^{\frac{\Pi}{10}}(1-T(L))} \sum_{k=1}^{\infty} \frac{\left(\mu \cdot 10^{\frac{\Pi}{10}}\right)^{k} \left(1-T(L)\right)^{k}}{k!} = 1 - e^{-\mu \cdot 10^{\frac{\Pi}{10}}(1-T(L))}$$

Рассмотрим случай, когда T(L = 20 км) = 0.398, μ_{max}=0.25.

Без воздействия атакой лазерного повреждения энтропия Фон Неймана равна:

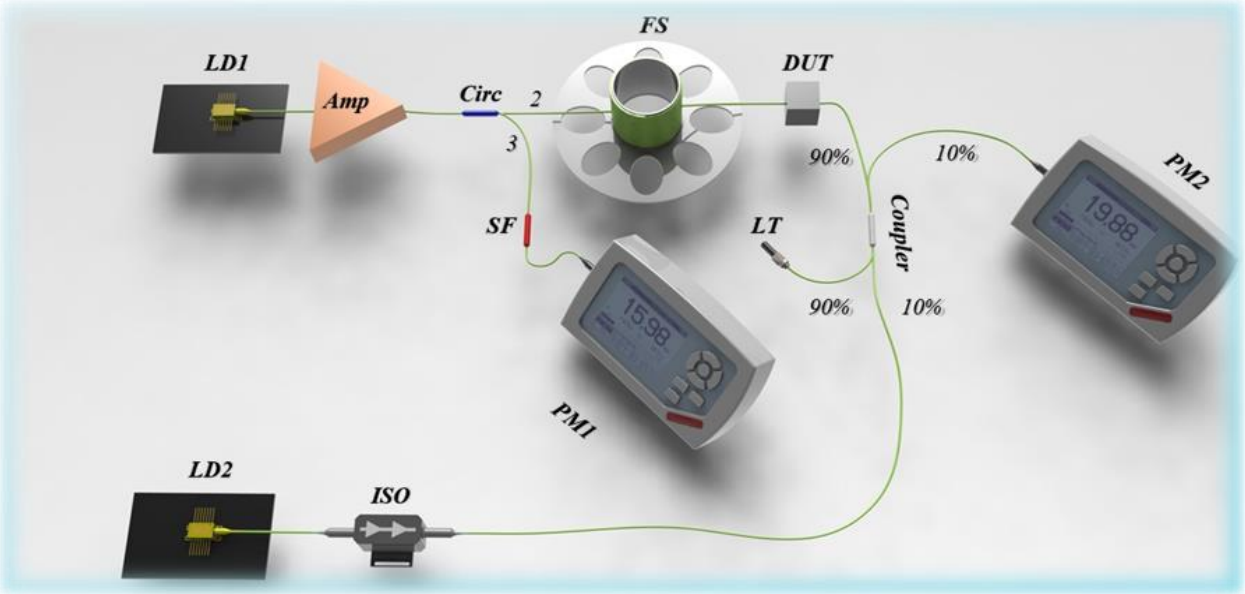
$$H(\rho_{XE}|\rho_{E}) = 0.86$$

С воздействием атакой лазерного повреждения при П=10 дБ энтропия Фон Неймана равна:

$$H(\rho_{XE}|\rho_{E}) = 0.22$$

При **П** > 0 безопасность системы будет нарушена, при достижении μ_{max} заявленного в протоколе

Метод измерения



Просветление рассчитывается по формуле:

$$\Pi_i = P_{\text{ср.пи1}} - \left(P_{\text{ср.отр}} + P_{\text{ср.н.пи1}}\right), \quad [\text{мВт}]$$

$$\Pi_i = 10 \cdot \log\left(\frac{P_{\text{ср.пи1}} - P_{\text{ср.отр}}}{P_{\text{ср.н.пи1}}}\right), \quad [\text{дБ}]$$

Значение аттенюации формуле:

$$\mathrm{A}_i = 10 \cdot \log\left(\frac{P_{\text{ср.пи1}} - P_{\text{ср.отр}}}{P_{\text{ср.пи2}} \cdot 9}\right), [\text{дБ}]$$

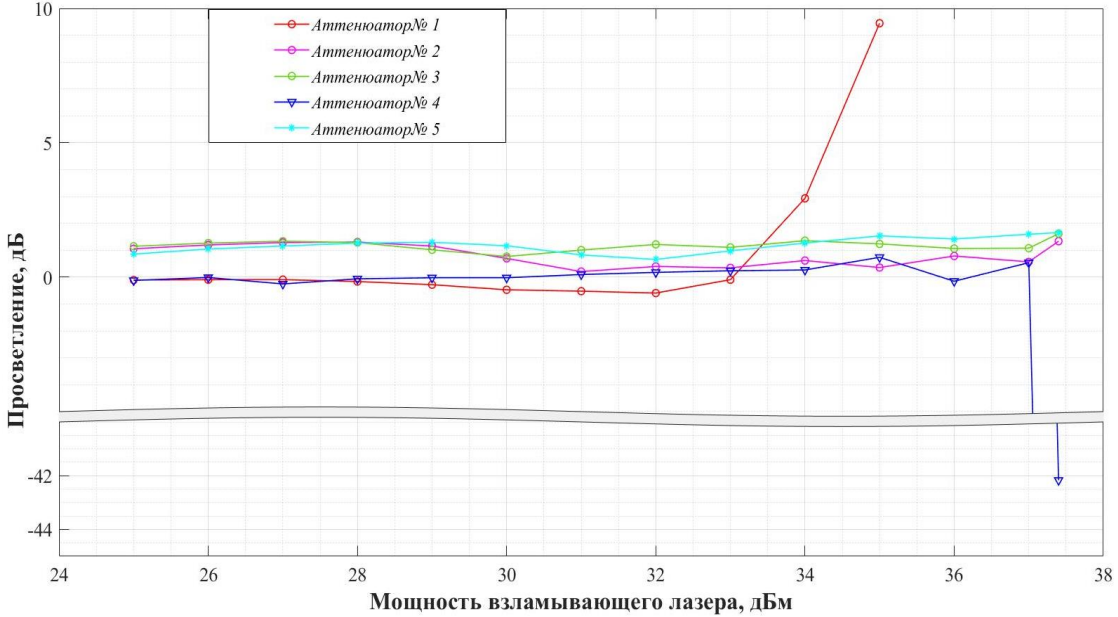
Bugai K. E. et al. //2022 International Conference Laser Optics (ICLO). – IEEE, 2022.

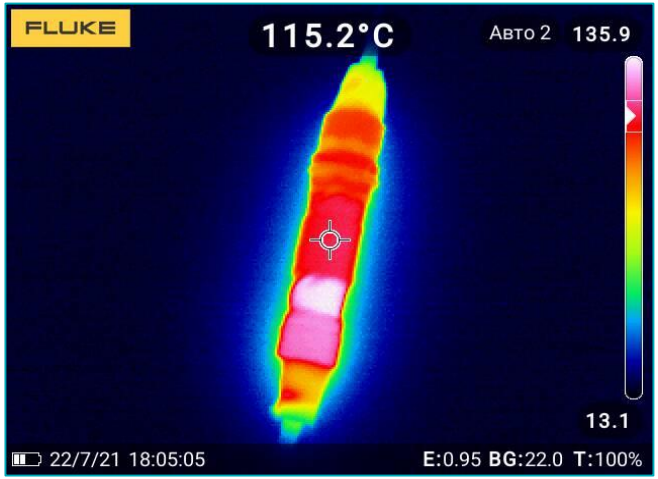
Экспериментальная часть

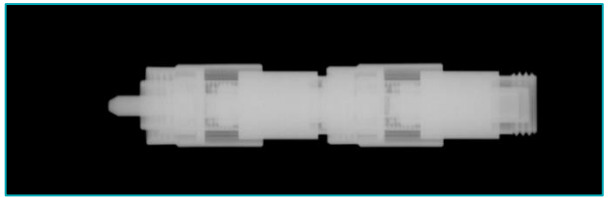
> Опыт – единственное средство познания, которым мы располагаем. Все остальное – поэзия, воображение.

Макс Планк

Аттенюатор бочкообразный

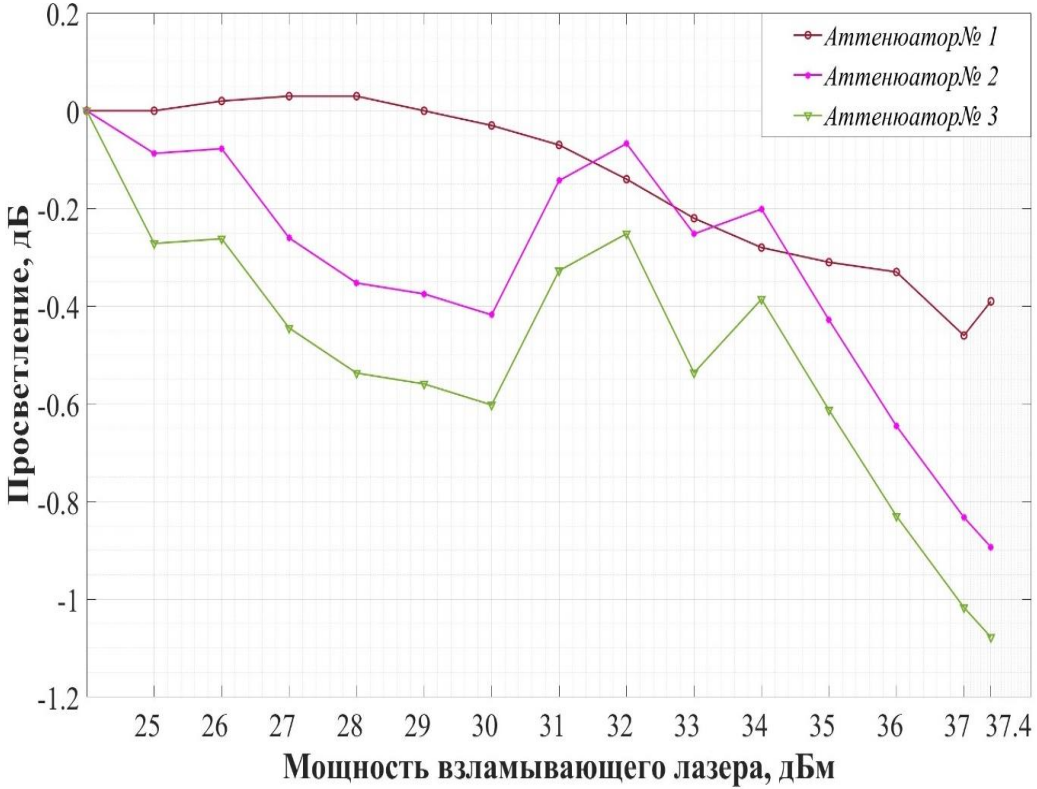


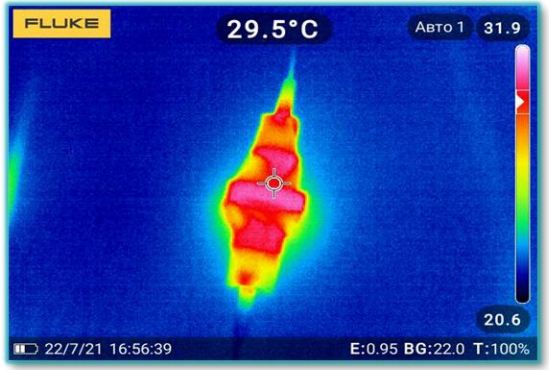


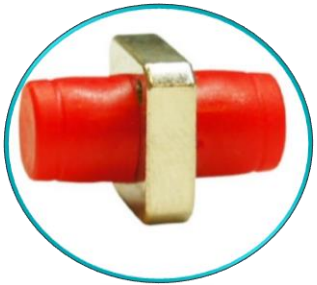


Изменение аттенюации происходит в результате термооптического эффекта

Аттенюатор розеткообразный

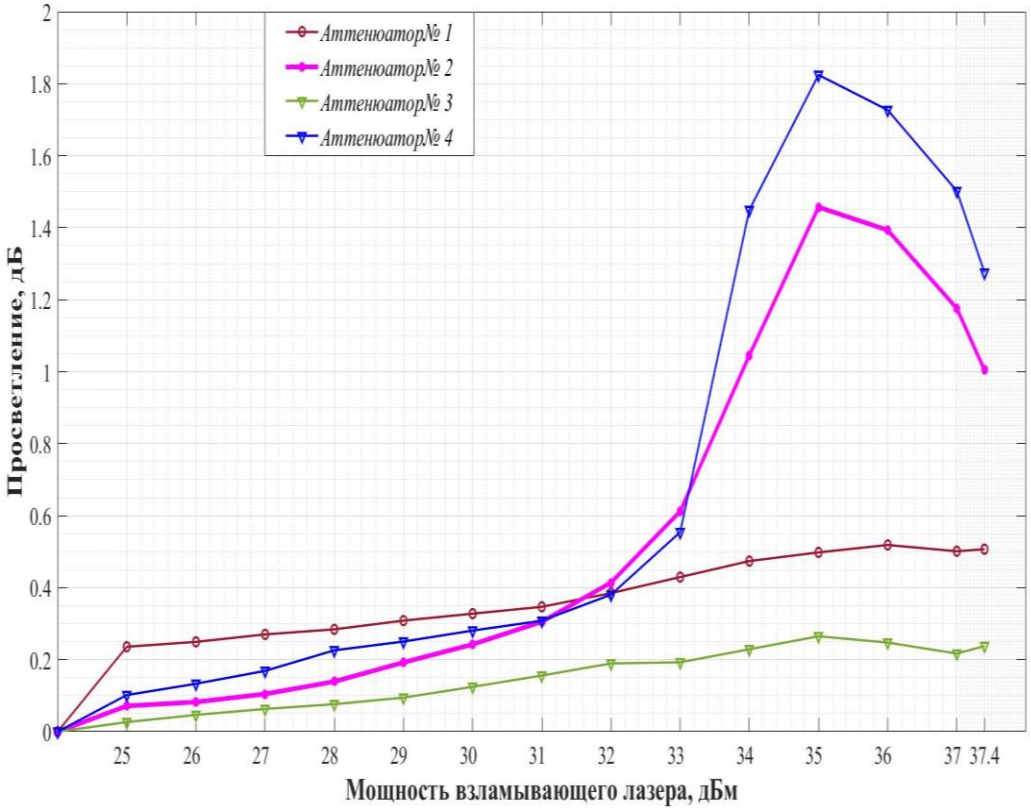


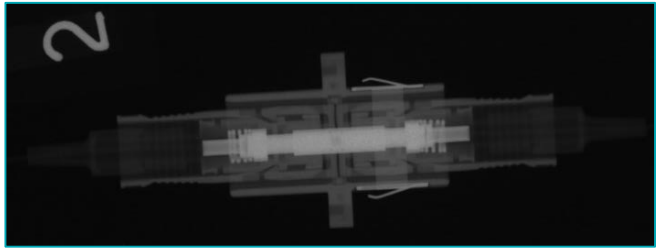


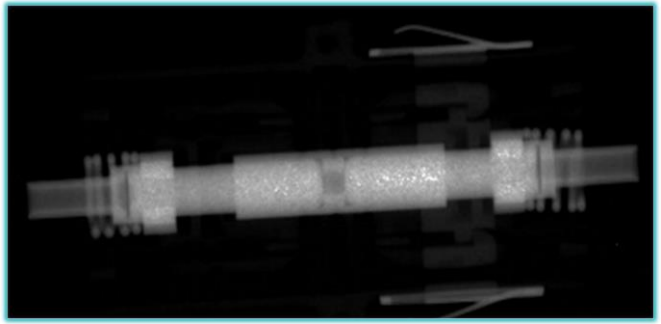


При неравномерном нагреве оптический контакт легко разрушается

Аттенюатор розеткообразный

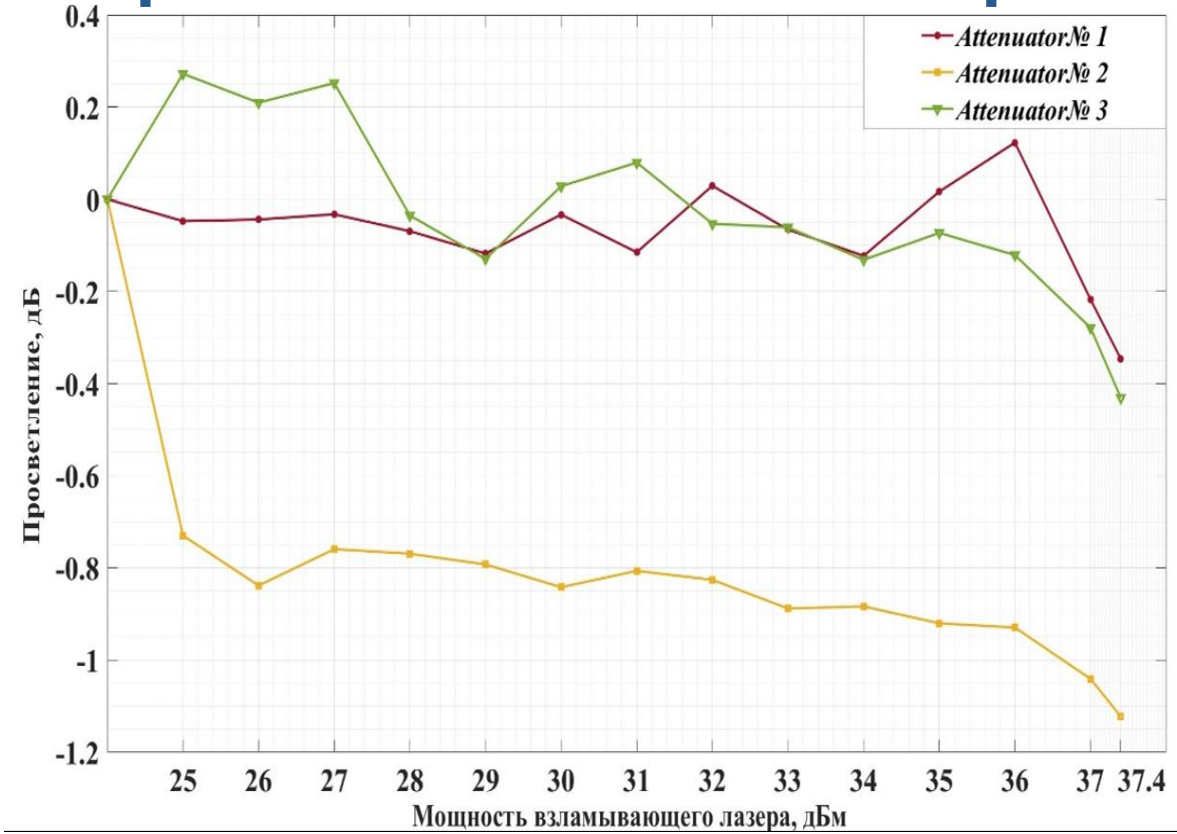






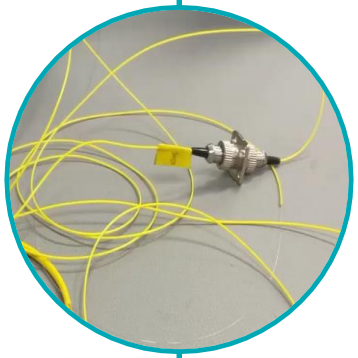
Изменение аттенюации происходит в результате изменения диаметра металлического кольца.

Переменный аттенюатор



Изменение аттенюации может происходить в случае децентрировки из-за диафрагмирования

Контрмеры



Заявка на патент
№ 2022129430

Патент
№ 215524

V. G. Krishtop, K. E. Bugai, et al. // 4th Smart Nanomaterials. – France, 2021.

A. Ponosova, V. Makarov, et al. // PRX Quantum 3,2022.

Заключение

> Успешность любой технологии зависит не только от ее производительности, но и от того, насколько хорошо она защищена от потенциальных угроз.

Чарльз Беннет

Разработана **схема** для исследования устойчивости аттенюаторов систем КРК.

Предложен **метод и критерий оценки** эффективности мер защиты от атаки лазерного повреждения.

Экспериментально поисследованы **аттенюаторы** широко используемые в системах КРК.

В качестве **контрмеры** предлагается применение **оптических предохранителей.**

Спасибо за внимание!

Бугай Кирилл Евгеньевич

Специалист

Email: Kirill.Bugay@sfblaboratory.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363