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

Бугай К.Е., специалист, СФБ Лаборатория

Зызыкин А.П., ведущий специалист, СФБ Лаборатория

Булавкин Д.С., специалист, СФБ Лаборатория

Богданов С.А., специалист, СФБ Лаборатория

Сущев И.С., специалист, СФБ Лаборатория

Дворецкий Д.А., к.т.н., ведущий специалист, СФБ Лаборатория

конференция РусКрипто

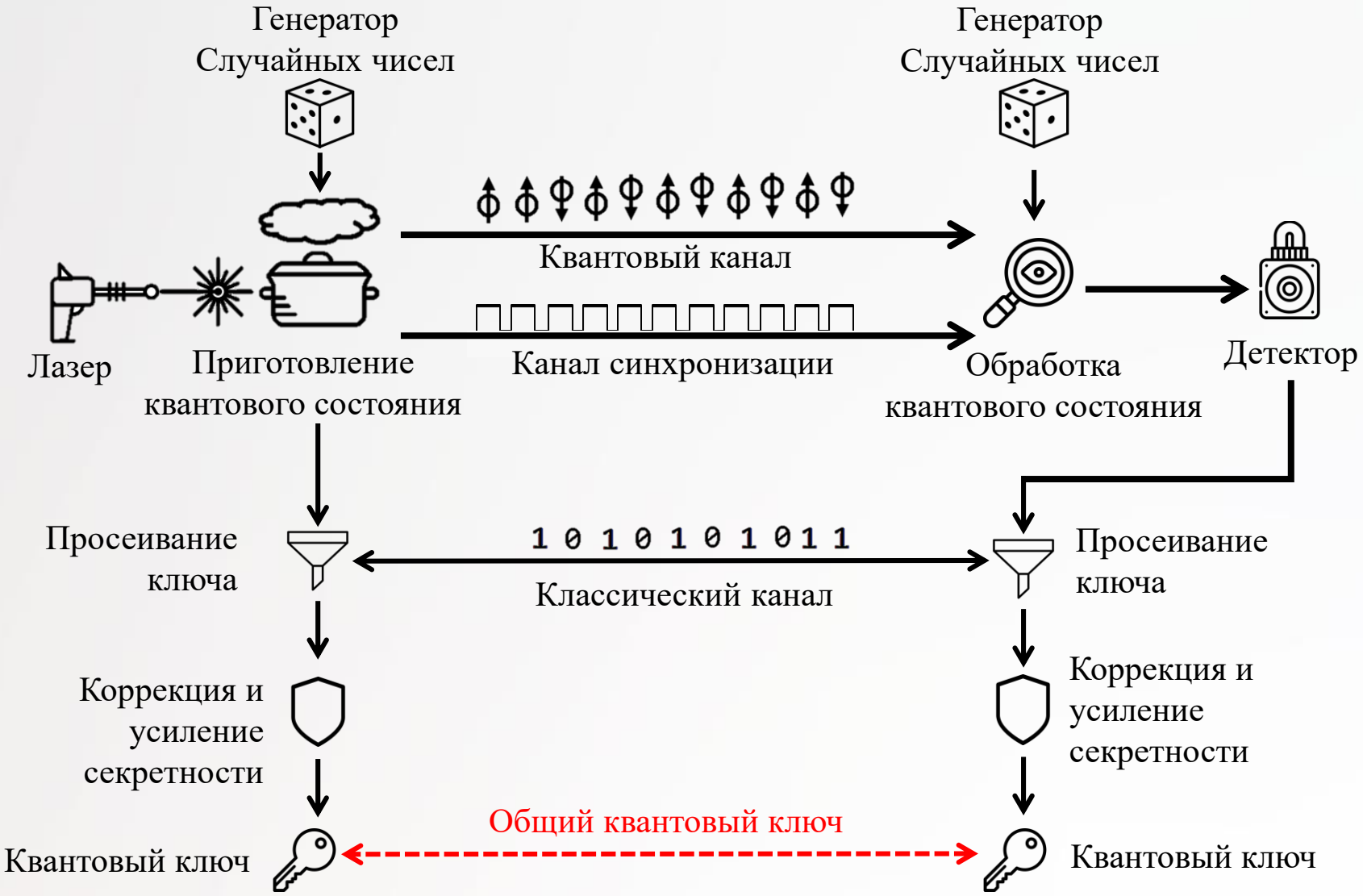
Содержание

1.

Введение

О чем это и почему это важно?

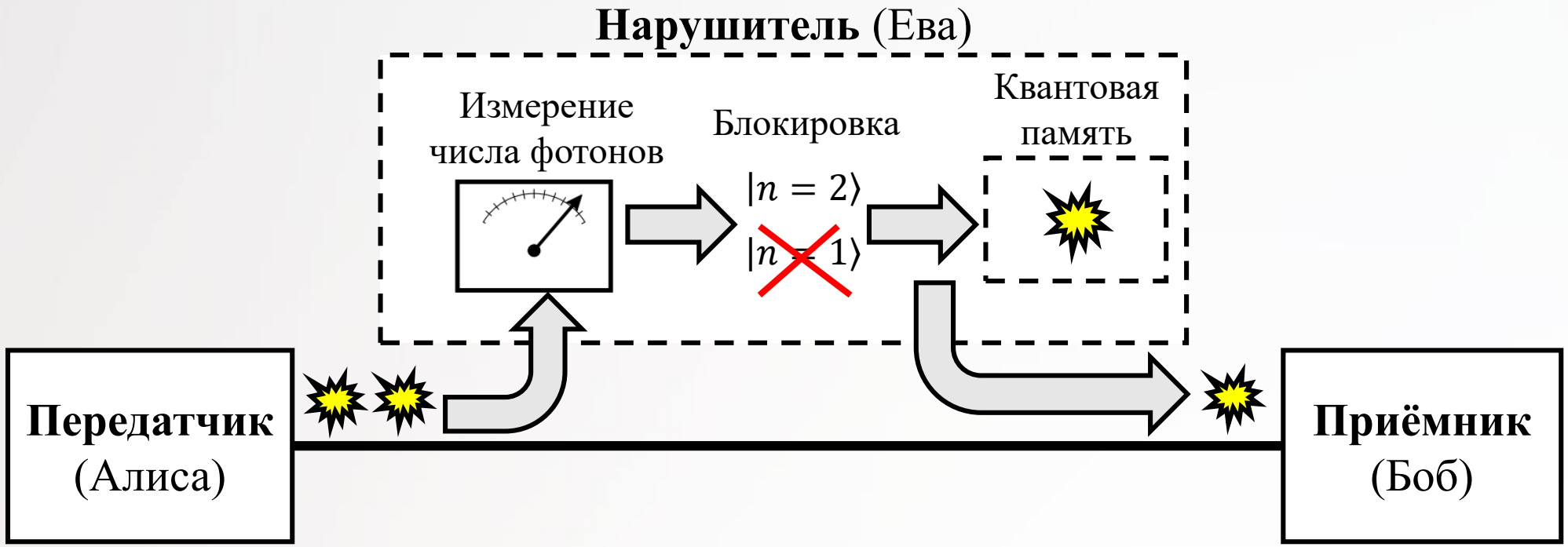
Принцип работы



PNS атака

Photon Number Splitting – атака с расщеплением по числу фотонов. Применяется к системам КРК, использующих **ослабленные лазерные состояния** вместо **строго однофотонных**.

Атака основана на том, что **число фотонов** в импульсах передатчика (Алисы) имеет **пуассоновскую статистику**.

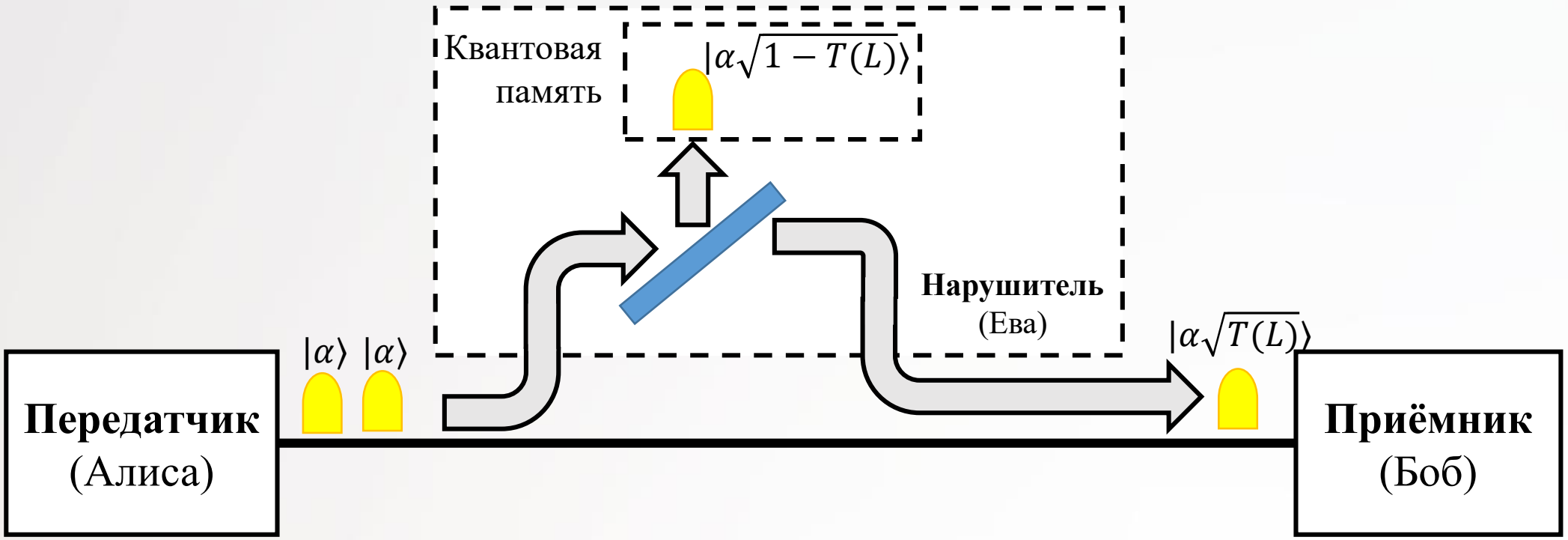


Lütkenhaus N., Jahma M. //New Journal of Physics. – 2002. – Т. 4. – №. 1. – С. 44.

BS атака

Beam **S**plitting – атака светоделителем. **Ева отводит часть** каждого состояния в свою квантовую память, а оставшуюся часть посылает Бобу **по каналу без затухания**. Боб получает состояния в точности той интенсивности, которую он ожидает, поэтому **атака не детектируется** на приемной стороне, но Ева получает лишь частичную информацию, ограниченную **величиной Холево** ее состояний.

Цель Евы в том, чтобы иметь столько же информации о ключе, сколько и Боб.

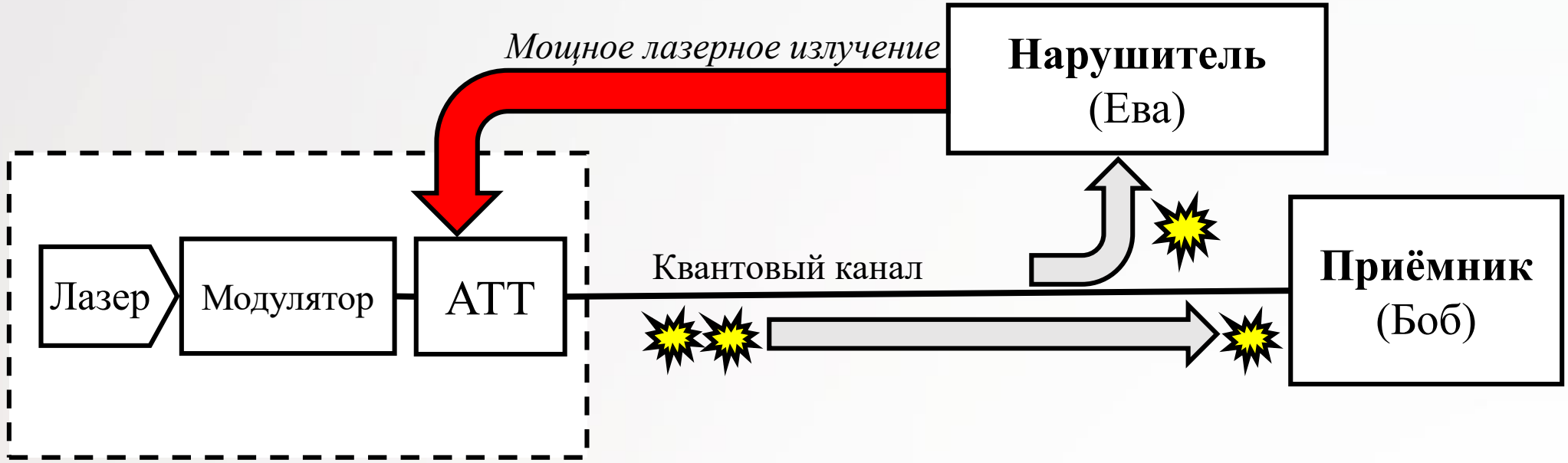


Calsamiglia J., Barnett S. M., Lütkenhaus N. //Physical Review A. – 2001. – Т. 65. – №. 1. – С. 012312.

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.

Просветление – это относительная величина **изменения коэффициента поглощения** аттенюатора при воздействии **мощного лазерного излучения**, выраженная в децибелах (дБ) **относительно** его начального значения.



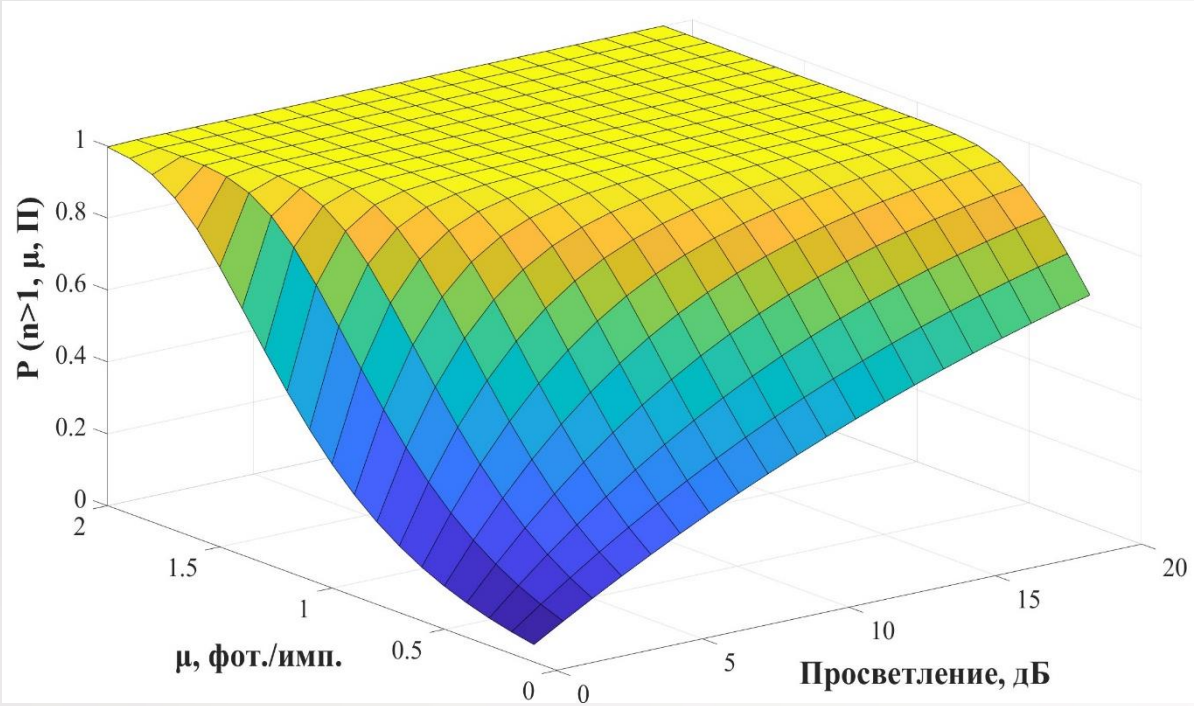
Makarov V. et al. Creation of backdoors in quantum communications via laser damage //Physical Review A. – 2016. – Т. 94. – №. 3. – С. 030302.

12.

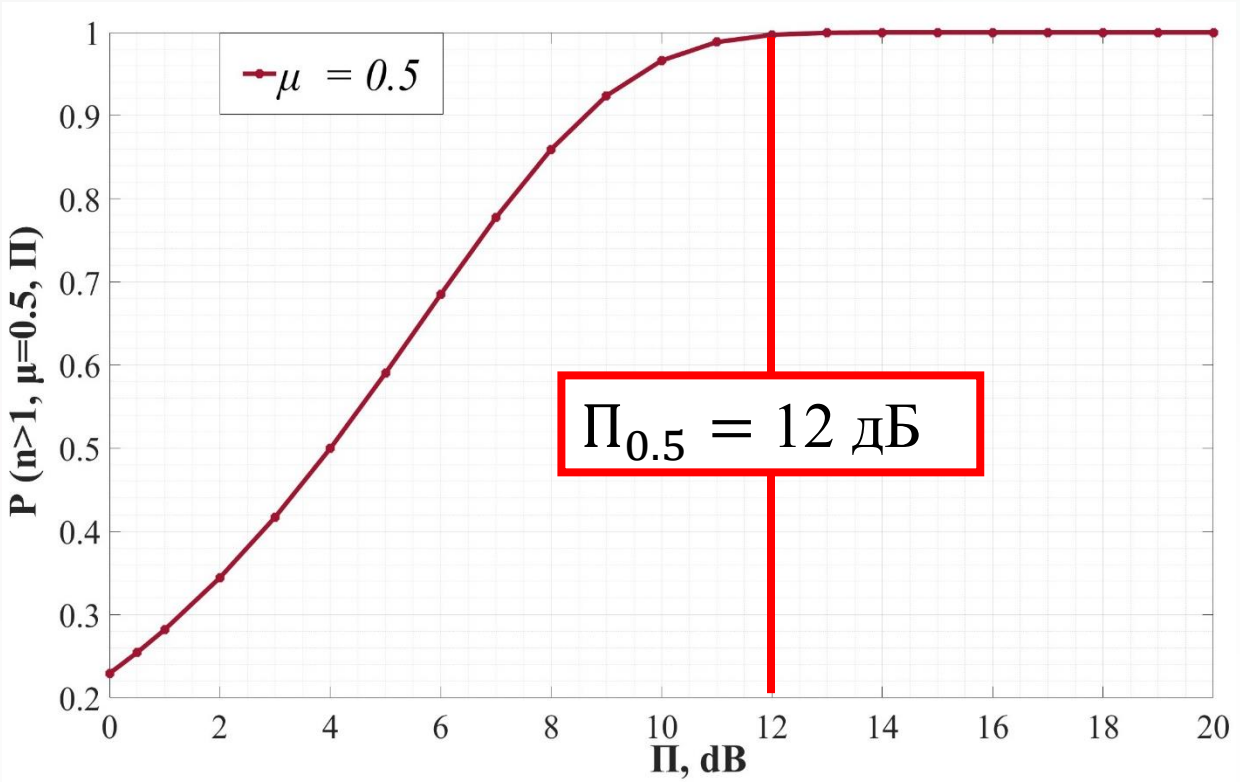
Метод и критерий

Длинная и извилистая дорога.

Критерий оценки



Было выполнено моделирование графика, который иллюстрирует зависимость **вероятности появления двух фотонов в импульсе** от **просветления** (П) и **среднего числа фотонов** (μ).



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

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

Тогда энтропия Фон Неймана будет равна:

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

Величина Холево будет равна:

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

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

Без воздействия атакой лазерного повреждения энтропия Фон Неймана равна:

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

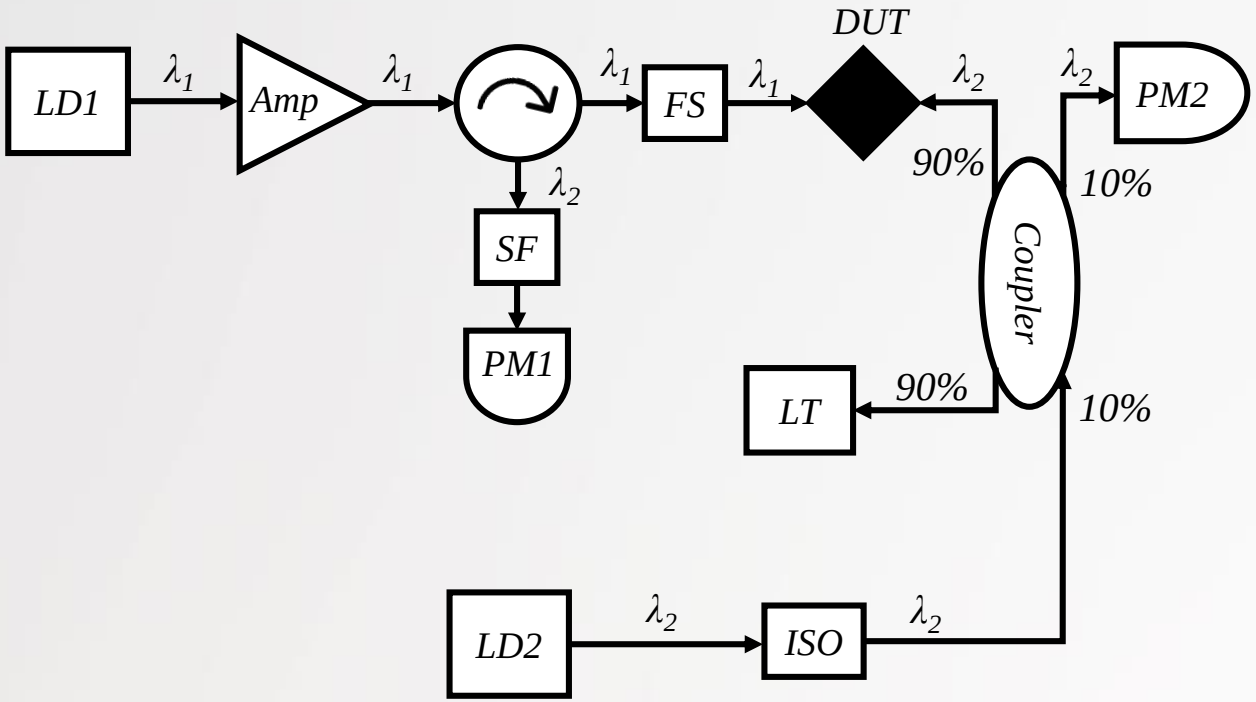
С воздействием атакой лазерного повреждения при П=10 дБ энтропия Фон Неймана равна:

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

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

Молотков С. Н., Кравцов К. С., Рыжкин М. И. //Журнал экспериментальной и теоретической физики. – 2019. – Т. 155. – №. 4. – С. 636-644.

Метод измерения



LD1 — лазер с длиной волны λ_1 =1561 нм;
Amp — волоконный усилитель легированный Эрбием;
Circ — волоконно-оптический циркулятор;
FS — катушка с волокном SMF-28 (100±1) м;
Coupler — разветвитель 90/10;
PM1, PM2 — измеритель мощности;
SF — спектральный фильтр;
ISO — мощный волоконно-оптический изолятор;
DUT — исследуемый аттенюатор;
LD2 — лазер с длиной волны λ_2 = 1547.315 нм;
LT — заглушка.

Значение аттенюации формуле:

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

Просветление рассчитывается по формуле:

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

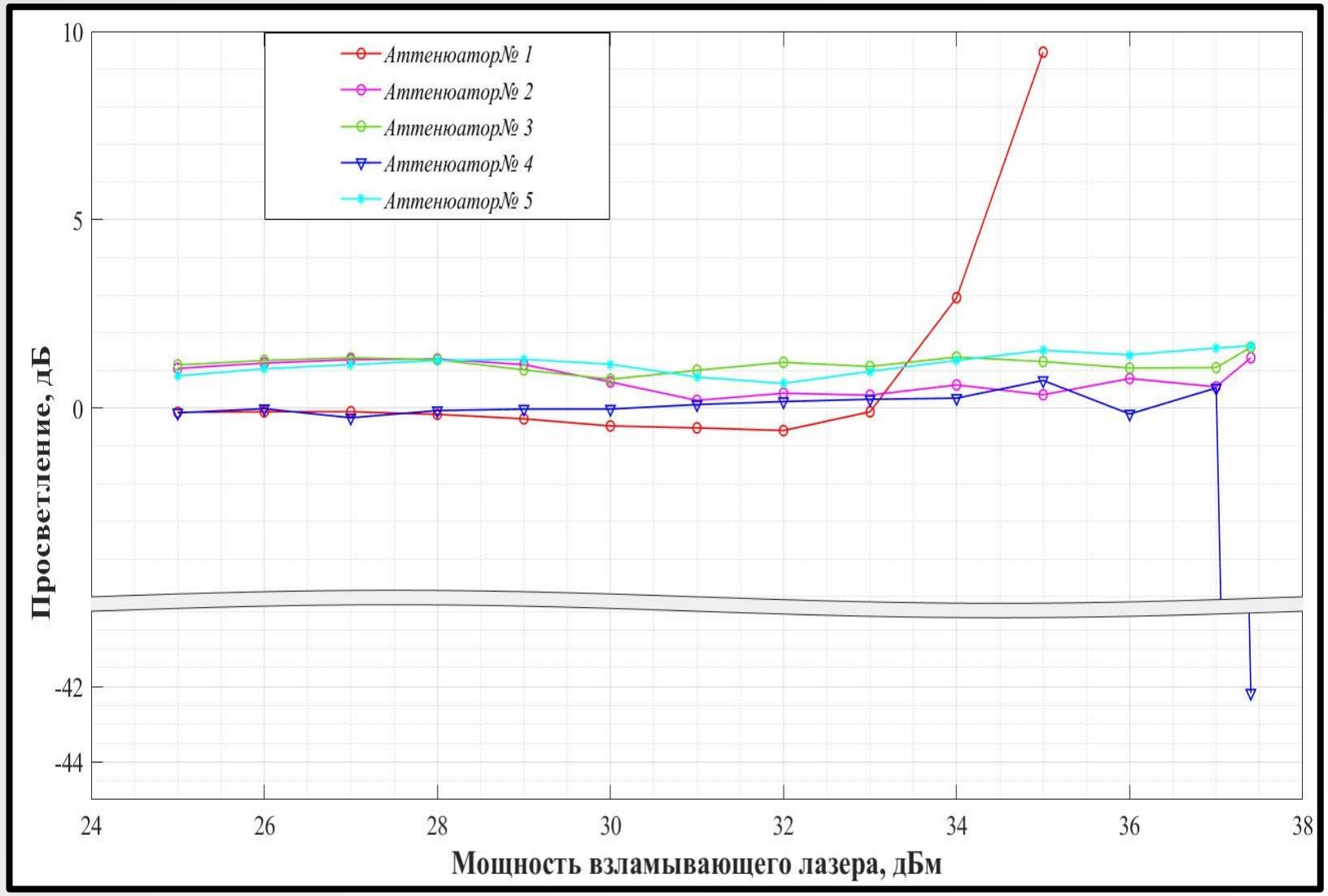
$$П_i = 10 \cdot \log\left(\frac{P_{\text{ср.пи1}} - P_{\text{ср.отр}}}{P_{\text{ср.н.пи1}}}\right), \quad [\text{дБ}]$$

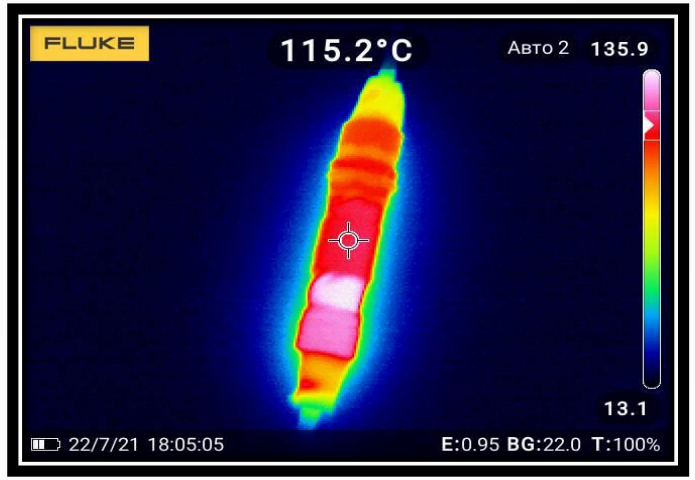
Bugai K. E. et al. //2022 International Conference Laser Optics (ICLO). – IEEE, 2022. – С. 1-1.

3. Экспериментальная часть

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

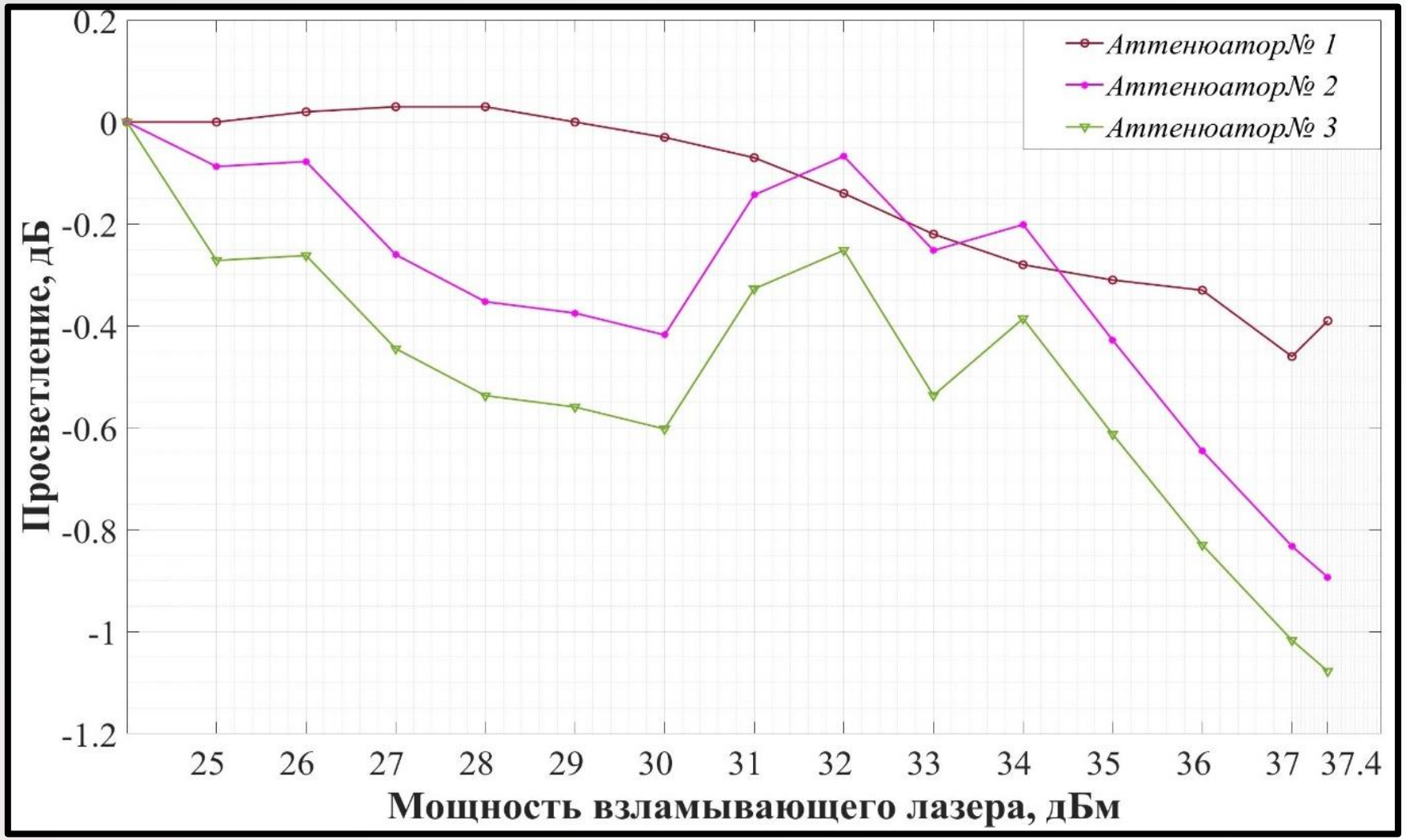
Аттенюатор бочкообразный

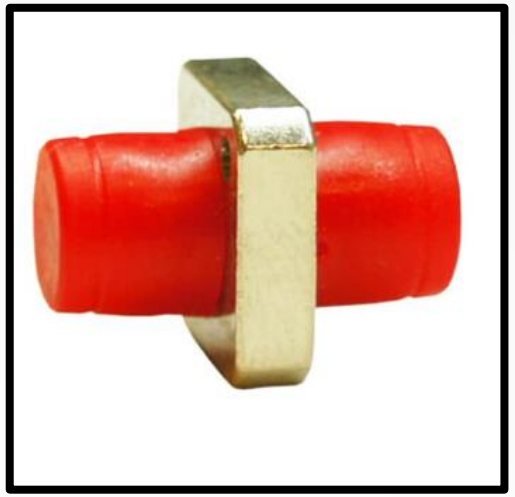




Изменение аттенюации происходит в результате термооптического эффекта

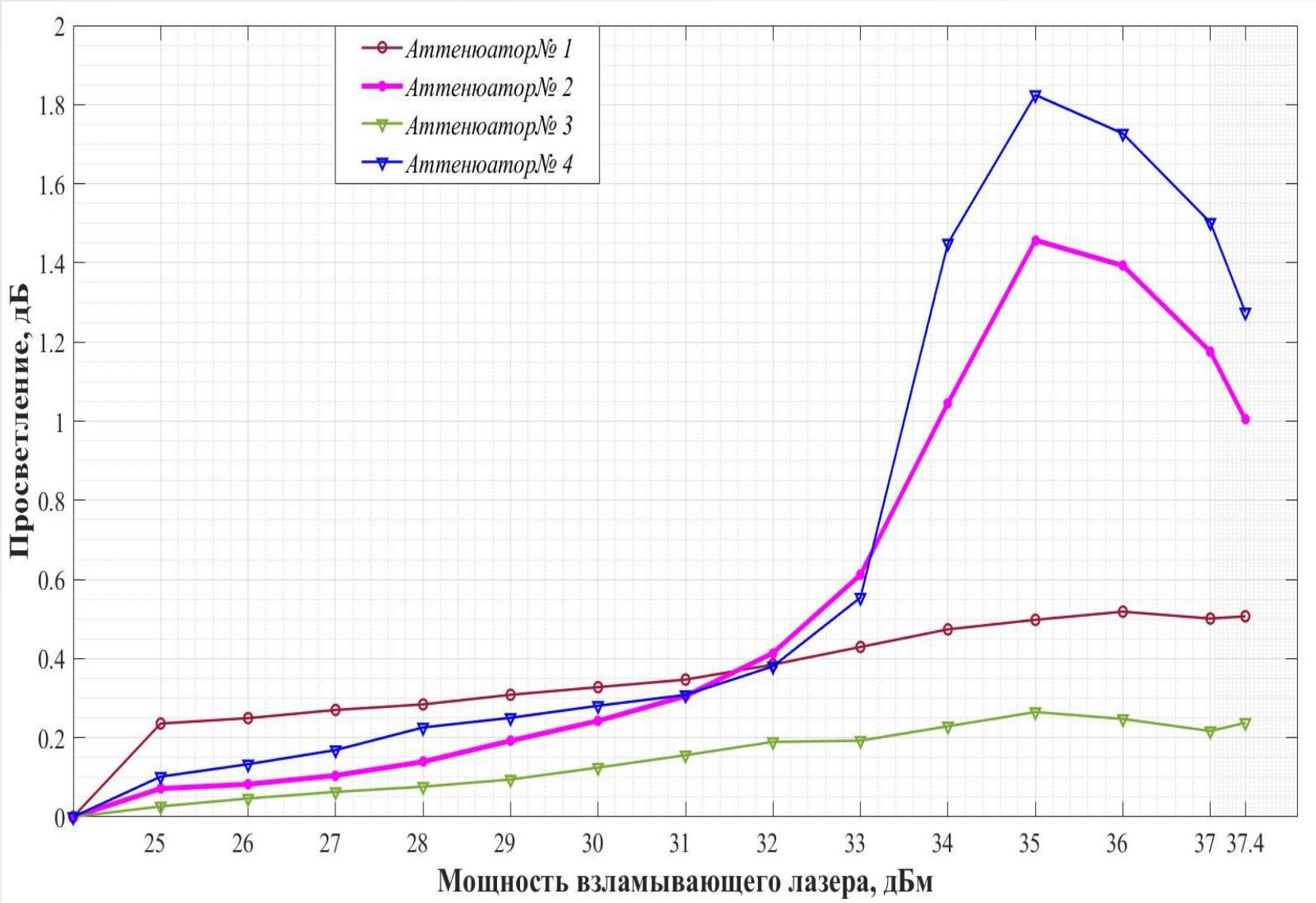
Аттенюатор розеткообразный

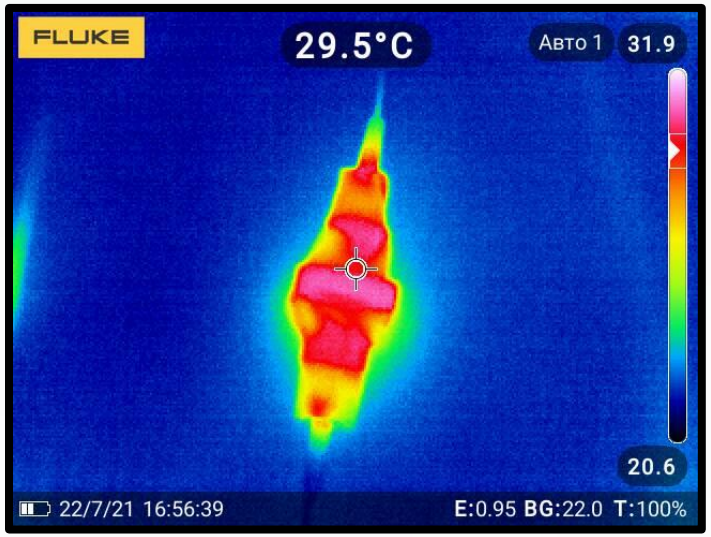




При неравномерном нагреве оптический контакт легко разрушается

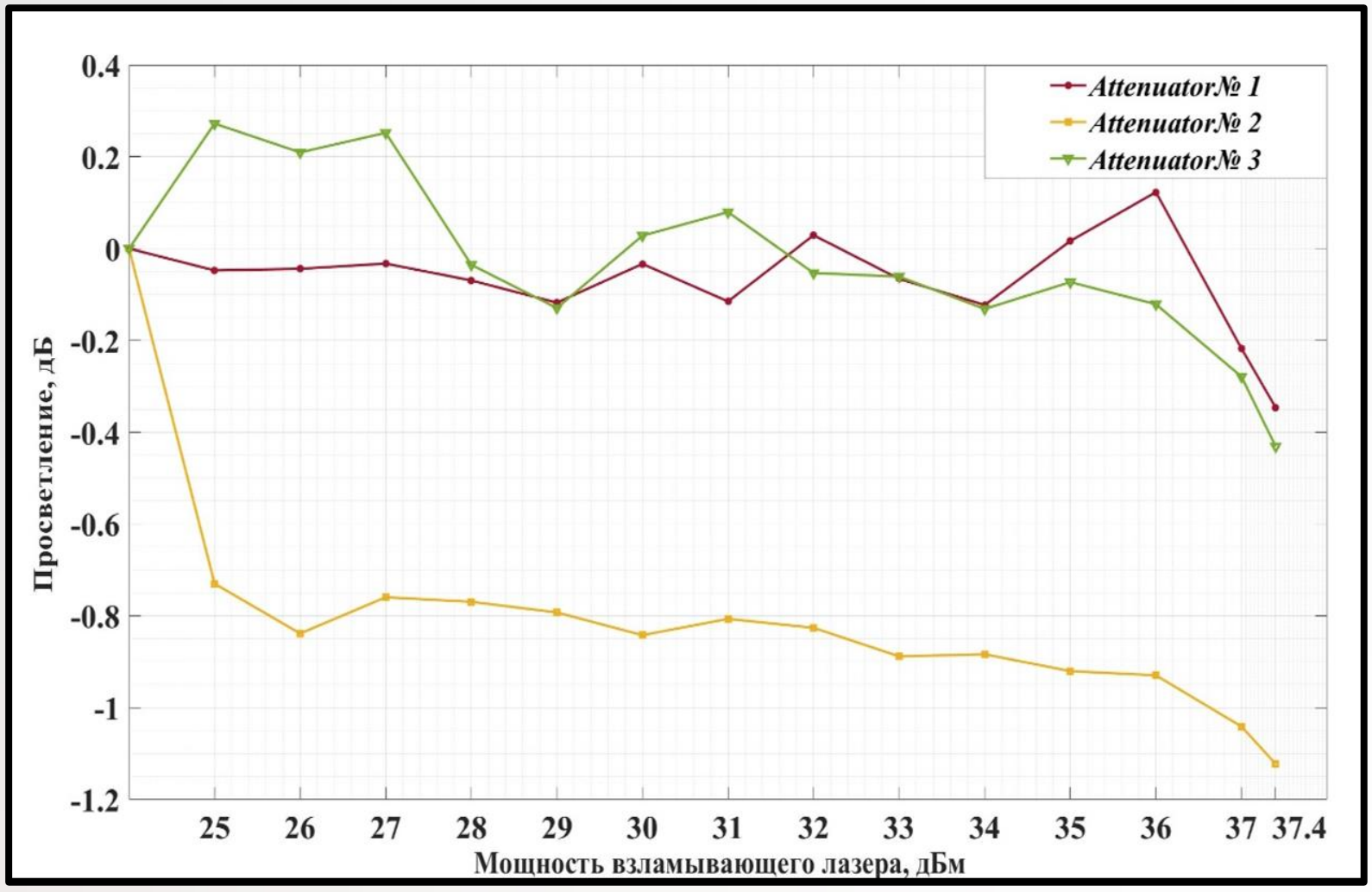
Аттенюатор розеткообразный

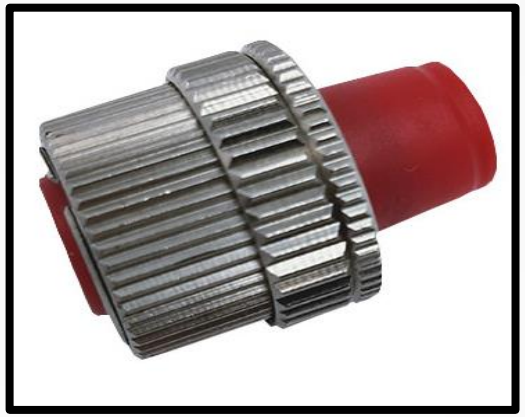




Изменение аттенюации происходит из-за того, что при нагреве металлическое кольцо может расширяться, благодаря чему, происходит увеличения внутреннего диаметра кольца.

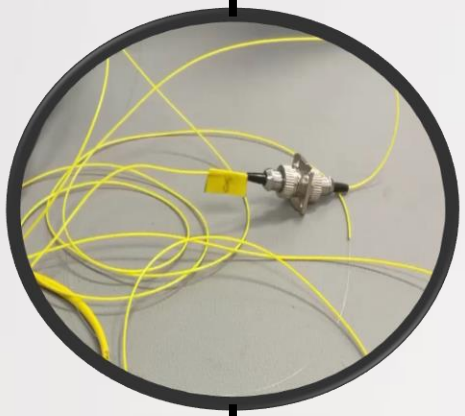
Переменный аттенюатор





Изменение аттенюации может происходить из-за того, что в результате нагрева данного аттенюатора в случае децентрировки будет происходить диафрагмирование за счет изменения оптической апертуры оптических волокон.

Контрмеры



Заявка на патент № 2022129430

Патент № 215524

V. G. Krishtop, K. E. Bugai, et al. // 4th Smart Nanomaterials: Advances, Innovations and Applications/ Paris. — France, 2021. — С.146-147

Ponosova, V. Makarov, et al. // PRX Quantum 3, 040307 (2022).

14.

СФБ ЛАБ

Заключение

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

Заключение

Вывод 1

Разработана схема для исследования устойчивости аттенюаторов систем КРК к атаке лазерного повреждения. Предложен метод и критерий оценки эффективности мер защиты от атаки лазерного повреждения на компоненты волоконно-оптических систем квантового распределения ключей.

Вывод 2

Экспериментальная часть:

- Аттенюатор бочкообразного типа уязвим для атаки лазерным повреждением;
- Аттенюатор розеткообразного типа с поглощением 20дБ устойчив к атаке лазерного повреждения;
- Переменный аттенюатор с поглощением 27 дБ устойчив к атаке лазерного повреждения;

Вывод 3

В качестве контрмеры к атаке, основанной на лазерном повреждении, предлагается применение оптических предохранителей, которые обеспечивают защиту от угроз безопасности путем ограничения мощности входного сигнала. Такие предохранители позволяют предотвратить нарушение квантового ключа и обеспечить целостность системы.

СПАСИБО ЗА ВНИМАНИЕ!

Бугай Кирилл Евгеньевич

¿Вопросы?