Оптический журнал

Физическая оптика

УДК 621.383.92

Регистрация оптического излучения переменной интенсивности лавинным фотодиодом в режиме счета фотонов

© 2021 г. И. Р. Гулаков, доктор физ.-мат. наук; А. О. Зеневич, доктор техн. наук; О. В. Кочергина, аспирант; Е. В. Новиков, кандидат техн. наук; С. А. Гоибов, аспирант

Белорусская государственная академия связи, Минск

E-mail: o.kochergina@bsac.by

Поступила в редакцию 29.07.2021

DOI:10.17586/1023-5086-2021-88-11-09-15

Продемонстрирована возможность осуществления атаки «ослеплением» кремниевых лавинных фотодиодов, работающих при комнатных температурах, используемых для регистрации однофотонных импульсов излучения с длиной волны 850 нм в квантовых криптографических системах. Определены характеристики кремниевых лавинных фотодиодов различных марок при их «ослеплении». Установлено, что атаку «ослеплением» на лавинный фотодиод можно обнаружить путем контроля значения электрического тока, протекающего через фотодиод. Получено, что при имитации одноквантовых импульсов разным лавинным фотодиодам требуются различные энергетические экспозиции многофотонных оптических импульсов, при этом длительность оптического импульса должна быть менее 1 мкс. Определено, что для осуществления атаки «ослеплением» при выборе интенсивности оптического излучения и энергетической экспозиции многофотонных оптических импульсов необходимо обладать информацией о характеристиках лавинного фотоприемника, применяемого в квантовой криптографической системе. Приведена структурная схема экспериментальной установки, на которой проводились исследования атаки «ослеплением», и осциллограммы выходных сигналов лавинного фотодиода в этих условиях.

Ключевые слова: *счет фотонов, атака «ослеплением», лавинный фотодиод, квантовая криптография, однофотонный импульс.*

Код OCIS: *270.5568*

ВВЕДЕНИЕ

В настоящее время при передаче данных по оптическому волокну информационная безопасность наиболее эффективно обеспечивается квантовыми криптографическими системами. Это связано с тем, что протоколы квантовой криптографии основаны на таких законах квантовой механики как принцип неопределенности Гейзенберга и теореме о запрете клонирования [1–7]. Однако из-за несовершенства оборудования, применяемого в квантовых криптографических системах, они могут быть не устойчивы к различного рода атакам. Значимой угрозой для квантовых криптографических систем, в том числе выпускаемых промышленностью, является атака, получившая в литературе название «удаленное управление детекторами единичных фотонов с использованием адаптированного яркого освещения», или кратко — «ослепления» [8–19].

Суть атаки состоит в том, что несанкционированный пользователь полностью перехватывает информацию, передаваемую однофотонными импульсами передатчика санкциониро-

ванного пользователя, и транслирует ее дальше по каналу связи, но использует для этого многофотонные импульсы, передаваемые на фоне оптического излучения постоянной интенсивности. Поскольку для регистрации оптического излучения в квантовых криптографических системах используются лавинные фотодиоды (ЛФД), работающие в режиме счета фотонов, то воздействие оптического излучения постоянной интенсивности переводит ЛФД из режима счета фотонов в режим пропорционального умножения. В этом режиме ЛФД не чувствителен к однофотонным импульсам.

Несанкционированный пользователь подбирает такую длительность и интенсивность многофотонного импульса, чтобы у санкционированного пользователя на выходе ЛФД, переведенного в режим пропорционального умножения оптическим излучением постоянной интенсивности, появился импульс тока, имитирующий сигнал от однофотонного импульса, посланного другим санкционированным пользователем [8–12]. Таким образом, несанкционированный пользователь считывает всю информацию, передаваемую по квантовому каналу связи, и при этом остается незамеченным. В связи с этим обнаружение атаки «ослепления» квантовыми криптографическими системами является актуальной задачей.

В выполненных ранее исследованиях атаки «ослепления» использовались ЛФД, регистрирующие в режиме счета отдельных фотонов оптическое излучение с длиной волны 1550 нм [8–10].

Исследование атаки «ослепления» ЛФД, работающего в режиме счета фотонов, оптическим излучением с длиной волны 1550 нм было выполнено в работе [10].

Однако ЛФД, обеспечивающие реализацию режима счета фотонов на такой длине волны, требуют охлаждения до температуры 240 K и ниже [10, 19–21]. Это усложняет практическое использование квантовых криптографических систем, работающих на данной длине волны. Поэтому для регистрации излучения в таких криптографических системах предлагается использовать кремниевые ЛФД, работающие в режиме счета фотонов при комнатных температурах [10, 19–22]. Максимальная чувствительность этих кремниевых ЛФД к оптическому излучению приходится на длину волны 850 нм.

Поэтому целью работы является определение условий «ослепления» кремниевых лавинных фотодиодов, работающих в режиме счета фотонов при комнатной температуре с использованием излучения с длиной волны 850 нм, установление энергетической экспозиции многофотонных оптических импульсов, имитирующих сигнал от однофотонных импульсов, и обнаружение атаки «ослепления» квантовых криптографических систем.

ЭКСПЕРИМЕНТАЛЬНАЯ УСТАНОВКА И МЕТОДИКА ИССЛЕДОВАНИЙ

Структурная схема экспериментальной установки, на которой проводились исследования, представлена на рис. 1. Установка функционирует следующим образом. Оптическое излучение постоянной интенсивности с длиной волны 850 нм от источника через оптическое волокно ОВ1 и регулируемый оптический аттенюатор А1 поступает на один из входов смесителя оптического излучения. На другой вход оптического смесителя подаются импульсы оптического излучения светодиода через оптическое волокно ОВ2 и регулируемый оптический аттенюатор А2. Аттенюаторы позволяют регулировать коэффициент ослабления интенсивности оптического излучения и энергетической экспозиции оптических импульсов от 0 до 80 дБ. Отметим, что при коэффициенте ослабления 80 дБ можно считать, что оптическое излучение и оптические импульсы на выходах аттенюаторов отсутствуют.

Импульсы оптического излучения светодиода с такой же длиной волны 850 нм инициируются генератором прямоугольных импульсов. Длительность электрических импульсов генератора изменяется от 0,5 до 10,0 мкс, а частота их следования составляет 10^4 Гц.

Смеситель объединяет оптическое излучение источника и светодиода и направляет его в оптическое волокно ОВ5, которое соединено с входом делителя оптического излучения. Делитель разделяет оптическое излучение на две части таким образом, чтобы на его выходах формировалось оптическое излучение равной интенсивности. К выходам делителя с помощью оптического волокна подключены дозиметр лазерного излучения и ЛФД, работающий в режиме счета фотонов.

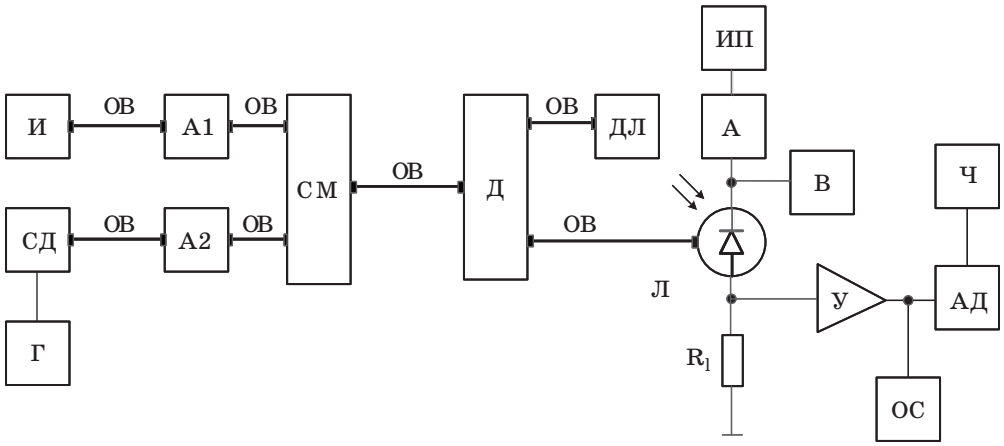

Рис. 1. Блок-схема экспериментальной установки. И — источник постоянного оптического излучения, А1 и А2 — регулируемые оптические аттенюаторы, СД — светодиод, Г — генератор прямоугольных электрических импульсов, ОВ1–ОВ7 — многомодовые оптические волокна, СМ — смеситель оптического излучения, Д — делитель оптического излучения, ДЛ — дозиметр лазерного излучения, У — усилитель, ОС — осциллограф, АД — амплитудный дискриминатор, Ч — частотомер, А — амперметр, В — вольтметр, ИП — источник напряжения, R_l — резистор нагрузки, ЛФД — лавинный фотодиод, работающий в режиме счета фотонов.

Дозиметр используется для измерения интенсивности оптического излучения и энергетической экспозиции оптических импульсов светодиода.

Режим счета фотонов реализован по схеме пассивного гашения лавины [21]. Для этого на ЛФД подается постоянное напряжение питания от источника, равное или близкое к напряжению пробоя ЛФД. Последовательно с ЛФД включен резистор нагрузки $R_l = 1$ кОм. Это наименьшее значение R_l, при котором удается реализовать счет фотонов на исследуемых ЛФД.

При воздействии на ЛФД оптического излучения на его выходе возникают как одноквантовые импульсы электрического тока, инициированные одним фотоном, так и темновые импульсы электрического тока, вызванные термогенерированными носителями заряда, возникающими в ЛФД.

Одноквантовые и темновые импульсы тока с резистора нагрузки R_l ЛФД поступают на вход широкополосного усилителя. После усиления они подаются на вход амплитудного дискриминатора и осциллографа. Дискриминатор осуществляет их амплитудную селекцию. Импульсы, амплитуды которых превышают порог амплитудной селекции дискриминатора, вызывают его срабатывание и на выходе формируются импульсы одинаковой амплитуды и длительности. Порог амплитудной селекции устанавливается над уровнем собственных шумов усилителя.

Осциллограф используется для контроля формы и параметров сигнала на выходе усилителя.

Значение электрического тока, протекающего через ЛФД, измеряется амперметром, а напряжение, приложенное к фотодиоду — вольтметром.

Импульсы с выхода дискриминатора поступают на вход частотомера.

Интенсивность оптического излучения источника измерялась при отсутствии оптических импульсов светодиода. Для этого коэффициент ослабления энергетической экспозиции оптических импульсов аттенюатора А2 устанавливался равным 80 дБ. Энергетическая экспозиция оптических импульсов определялась при отсутствии оптического излучения от источника. В этом случае коэффициент ослабления интенсивности оптического излучения аттенюатора А1 также устанавливался равным 80 дБ.

Исследовались серийно выпускаемые кремниевые лавинные фотодиоды марок ФД-115Л, КОФ 101А и ВРУР 52.

Поскольку исследуемые ЛФД имели различные напряжения пробоя U_{br}, то для сравнения их характеристик между собой использовалась величина перенапряжения $\Delta U = U - U_{br}$,

где U — напряжение питания фотоприемника. Напряжения пробоя лавинных фотодиодов определялись по их вольт-амперной характеристике в соответствии с методикой, предложенной в работе [21].

Исследования проводились при постоянной температуре 297 K. Значения перенапряжений изменялись в диапазоне $\Delta U = -0{,}2–0{,}5$ В. Это связано с тем, что при меньших перенапряжениях не удается реализовать режим счета фотонов, а при более высоких перенапряжениях частота темновых импульсов была не менее 10^6 Гц. Реализация счета фотонов при таком большом числе темновых импульсов нецелесообразна, так как начинает проявляться эффект мертвого времени фотодиода, что ведет к потере большого количества одноквантовых импульсов [21].

РЕЗУЛЬТАТЫ ИЗМЕРЕНИЙ И ИХ ОБСУЖДЕНИЕ.

Были выполнены исследования зависимости амплитуды одноквантовых импульсов от интенсивности оптического излучения, регистрируемого ЛФД. На рис. 2 представлены типичные осциллограммы выходного сигнала ЛФД. При таком перенапряжении частота появления темновых импульсов всех ЛФД не превышала 10^3 Гц.

Получено, что существует интервал интенсивностей оптического излучения J, при которых средняя амплитуда темновых и одноквантовых импульсов A_{ave} оставалась постоянной. Так, при $\Delta U = 0{,}1$ В такой интервал составлял для ФД-115Л $J = 0–0{,}1$ мкВт/см^2, для КОФ 101А $J = 0–0{,}5$ мкВт/см^2, для ВРУР 52 $J = 0–0{,}2$ мкВт/см^2. В этих интервалах вид и амплитуды темновых и одноквантовых импульсов совпадали, а частота появления импульсов не превышала 5×10^4 Гц. При данных значениях интенсивности регистрируемого оптического излучения типичный вид выходных импульсов ЛФД представлен на рис. 2а. Фототок при таких интенсивностях засветки не превышал 5 мкА.

С ростом интенсивности оптического излучения и превышением указанных выше ее значений, значение A_{ave} начинает уменьшаться (рис. 2б). Уменьшение амплитуды импульсов обусловлено тем, что после формирования темнового или одноквантового импульсов напряженность электрического поля в области умножения носителей заряда ЛФД понижается. В связи с этим существует промежуток времени, в течение которого напряженности электрического поля в этой области необходимо восстановиться до первоначального значения. В этот промежуток времени ЛФД может зарегистрировать фотон, но сформирует выходной импульс с амплитудой меньшей, чем при полностью восстановленной напряженности [21]. С ростом интенсивности оптического излучения вероятность попадания фотона на ЛФД в такой промежуток времени увеличивается. Амплитуда импульса будет тем меньше, чем ближе этот импульс формируется к началу восстановления напряженности электрического поля. Ток при таких интенсивностях засветки увеличивается до 10 мкА, а наибольшая частота появления смеси темновых и сигнальных импульсов наблюдается у ЛФД ВРУР 52 и составляет 2×10^6 Гц.

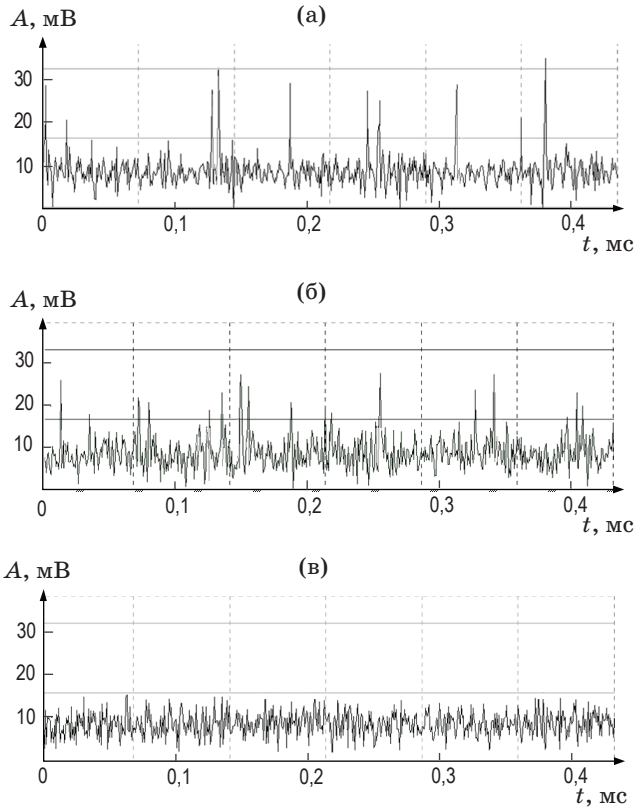

Рис. 2. Осциллограммы выходного сигнала лавинного фотодиода ФД-115Л, полученные при различных интенсивностях оптического излучения ($J = 0{,}1$ мкВт/см^2 — а, $J = 4{,}7$ мкВт/см^2 — б, $J = 41$ мкВт/см^2 — в) и $\Delta U = 0{,}1$ В.

При достаточно больших интенсивностях оптического излучения напряженность электрического поля после формирования темнового или одноквантового импульсов не успевает восстановиться к тому моменту времени, когда начинает формироваться следующий импульс. В результате чего амплитуда этих импульсов уменьшается на столько, что эти импульсы не удается выделить на фоне шумов усилителя (рис. 2в). Так, при $\Delta U = 0{,}1$ В наименьшие значения интенсивностей оптического излучения J_{min}, при которых не удавалось выделить темновые и одноквантовые импульсы на фоне шумов усилителя, составляли для ФД-115Л $J_{min} = 41$ мкВт/см^2, для КОФ 101А $J_{min} = 32$ мкВт/см^2, для ВРУР 52 $J_{min} = 35$ мкВт/см^2. Значение фототока при таких интенсивностях засветки было не более 35 мкА.

Зависимости средней амплитуды одноквантовых и темновых импульсов от регистрируемой интенсивности оптического излучения при перенапряжении $\Delta U = 0{,}1$ В представлены на рис. 3. При других значениях перенапряжений зависимости имели аналогичный вид. Наибольшую амплитуду одноквантовых и темновых импульсов в интервале интенсивностей, при которых A_{ave} остается постоянной, имели фотодиоды ФД-115Л, а наименьшую — КОФ 101А во всем диапазоне исследуемых перенапряжений. Так, при $\Delta U = -0{,}2$ В средняя амплитуда импульсов на сопротивлении нагрузки в этом интервале интенсивностей принимала следующие значения: для ФД-115Л — 8 мВ, для КОФ 101А — 3 мВ, для ВРУР 52 — 6 мВ. Увеличение перенапряжения приводит к росту A_{ave} в данном интервале интенсивностей. При максимальном в исследуемом диапазоне значении перенапряжения $\Delta U = 0{,}5$ В средняя амплитуда импульсов имела следующие значения: для ФД-115Л – 33 мВ, для КОФ 101А — 8 мВ, для ВРУР 52 — 18 мВ.

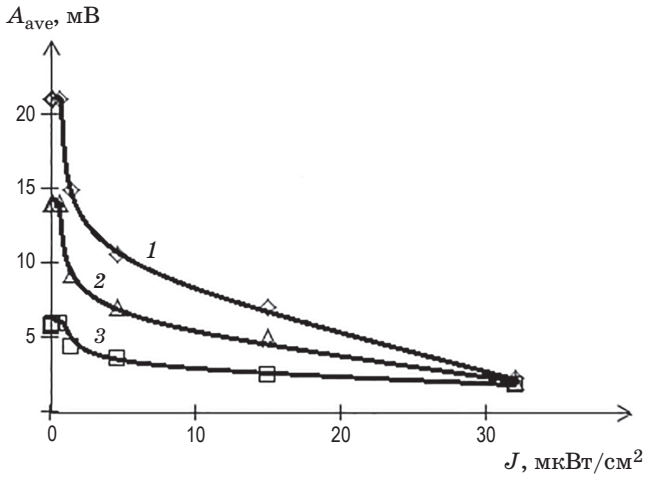

Рис. 3. Зависимости средней амплитуды одноквантовых и темновых импульсов от интенсивности оптического излучения лавинных фотодиодов ФД-115Л (*1*), ВРУР 52 (*2*), КОФ 101А (*3*).

С ростом перенапряжения происходило увеличение значения J_{min}. Это связано с тем, что с увеличением ΔU расширяется динамический диапазон регистрации ЛФД, как это показано в публикации [21].

В исследуемом диапазоне перенапряжений зависимость J_{min} от ΔU была линейной для всех марок ЛФД. Отношение изменения наименьшей интенсивности оптического излучения ΔJ_{min}, при которой не удавалось выделить темновые и одноквантовые импульсы на фоне шумов усилителя, к изменению перенапряжения ΔU_{min} ($\Delta J_{min}/\Delta U_{min}$) имела следующие значения: 40,0 мкВт/(см^2 В) для ФД-115Л, 7,1 мкВт/(см^2 В) для ВРУР 52, 0,5 мкВт/(см^2 В) для КОФ 101А. Таким образом, наиболее сильная зависимость J_{min} от ΔU наблюдается у ФД-115Л, а наименьшая — у КОФ 101А.

В процессе исследования была определена энергетическая экспозиция многофотонных оптических импульсов H_e, наложенных на оптическое излучение с постоянной интенсивностью J_{min}, амплитуда фотоотклика которых совпадала с A_{ave}. При этом длительность оптических импульсов выбиралась равной длительности одноквантовых импульсов и составляла 1 мкс. В случае уменьшения длительности оптических импульсов длительность импульсов фотоотклика оставалась равной 1 мкс.

В таблице представлены значения энергетической экспозиции многофотонных оптических импульсов H_e для случая, когда ампли-

Характеристики лавинных фотодиодов

Название фотоприемника	ΔU, В	J_{min}, мкВт/см^2	H_e, нДж/см^2
ФД-115Л	0,1	0,7	1,4
ВРУР 52	0,2	0,7	5,0
КОФ 101А	0,2	3,1	1,0

туда фотоотклика была равной A_{ave}. Данные значения получены при ΔU, соответствующих максимальной чувствительности исследуемых ЛФД к оптическому излучению.

Как следует из данных, представленных в таблице, наименьшее значение H_e, необходимое для имитации одноквантовых импульсов, имеют фотодиоды КОФ 101А, а наибольшее — BPYP 52. Таким образом, при имитации одноквантовых импульсов разным ЛФД требуются различные энергетические экспозиции многофотонных оптических импульсов. Это связано с тем, что исследуемые ЛФД имеют свои конструктивные особенности и отличаются по чувствительности к оптическому излучению и коэффициентам усиления фототока.

В частности, для лавинного фотодиода КОФ 101А характерно меньшее значение чувствительности к оптическому излучению. Поэтому в условиях постоянной засветки для него требуется большее значение интенсивности J_{min}.

Лавинным фотодиодам КОФ 101А присуща меньшая амплитуда формируемых одноквантовых и темновых импульсов, в связи с этим для их имитации необходима меньшая энергетическая экспозиция.

ЗАКЛЮЧЕНИЕ

Показана возможность осуществления атаки «ослеплением» кремниевых лавинных фотодиодов, работающих при комнатной температуре, используемых для регистрации однофотонных импульсов излучения с длиной волны 850 нм в квантовых криптографических системах.

Исследованы характеристики различных марок кремниевых лавинных фотодиодов, работающих в режиме счета фотонов, в условиях воздействия на них атаки «ослеплением». Среди исследуемых лавинных фотодиодов наименее устойчивыми к атаке «ослеплением» оказались фотодиоды ФД-115Л и BPYP 52, так как для них требуется наименьшая интенсивность «ослепляющего» освещения оптическим излучением с длиной волны 850 нм.

Установлено, что атаку «ослеплением» лавинного фотодиода несанкционированным пользователем можно обнаружить путем контроля значения электрического тока, протекающего через фотодиод.

Получено, что при имитации однофотонных импульсов разных лавинных фотодиодов требуются различные энергетические экспозиции многофотонных оптических импульсов. При этом длительность оптического импульса должна быть менее 1 мкс.

Определено, что при выборе интенсивности «ослепляющего» оптического излучения и энергетической экспозиции многофотонных оптических импульсов необходимо обладать информацией о характеристиках лавинного фотоприемника, применяемого в квантовой криптографической системе.

Определены условия атаки «ослеплением» серийно выпускаемых кремниевых лавинных фотодиоды марок ФД-115Л, КОФ 101А и BPYP 52, работающих в режиме счета фотонов, оптическим излучением с длиной волны 850 нм. Для этих фотодиодов установлены значения энергетической экспозиции многофотонных оптических импульсов, позволяющих имитировать сигнал от однофотонных импульсов.

Полученные результаты могут быть использованы при проектировании квантовых криптографических систем и разработке устройств их защиты от атаки «ослеплением».

ЛИТЕРАТУРА

1. *Sergienko A.V.* Quantum communications and cryptography. CRC press, 2019. 248 p.
2. *Feihu Xu, Xiongfeng Ma, Qiang Zhang, et al.* Secure quantum key distribution with realistic devices // Rev. Mod. Phys. 2020. V. 92. P. 025002.
3. *Wootters W.K. and Zurek W.H.* A single quantum cannot be cloned // Nature. 1982. V. 299. P. 802.
4. *Dieks D.* Communication by EPR devices // Phys. Lett. A. 1982. V. 92 № 6. P. 271–272.
5. *Баумейстер Д., Экерт А., Цайлингер А.* Физика квантовой информации. М.: Постмаркет, 2002. 376 с.
6. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. М.: Мир, 2006. 824 с.
7. *Прескилл Дж.* Квантовая информация и квантовые вычисления М.: РХД, 2008. Т. 1. 464 с.
8. *Makarov V., Hjelme D.R.* Faked states attack on quantum cryptosystems // J. Modern Optics. 2005. V. 52. № 5. P. 691–705.

9. *Makarov V.* Controlling passively quenched single photon detectors by bright light // New J. Phis. 2009. V. 11. P. 065003.
10. *Yan Z., Hamel D.R., Heinrichs A.K., et al.* Anultra low noise telecom wavelength free running single photon detector using negative feedback avalanche diode // Rev. Scientific Instruments. 2012. V. 83. № 7. P. 073105.
11. *Карамаев М.М.* Уязвимости реализаций систем квантовой криптографии // Научное обозрение. Технические науки. 2020. № 3. С. 30–35.
12. *Молотков С.Н.* Об уязвимости базовых протоколов квантового распределения ключей и о трех протоколах, устойчивых к атаке с «ослеплением» лавинных фотодетекторов // ЖЭТФ. 2012. Т. 141. № 5. С. 812–831.
13. *Василиу Е.В., Лимарь И.В.* Атаки на квантовые системы распределения ключей, эксплуатирующие уязвимость оборудования // Тез. докл. Перспективні напрями захисту інформації. Матеріали третьої Всеукраінськоі наук.практ. конф. 2–6 верасня 2017 р., м. Одеса. Одеса: ОНАЗ ім. О.С. Попова. 2017. С. 9–13.
14. *Килин С.Я., Хорошко Д.Б., Низовцев А.П.* Квантовая криптография: идеи и практика. Минск: Белорус. наука, 2007. 391 с.
15. *Feihu Xu, Xiongfeng Ma, Qiang Zhang, et al.* Secure quantum key distribution with realistic devices // Rev. Mod. Phys. 2020. V. 92. P. 025002.
16. *Gras G., Sultana N., Huang A., et al.* Optical control of single-photon negative-feedback avalanche diode detector // J. Appl. Phys. 2020. V. 127. № 9. P. 094502.
17. *Lydersen L., Wiechers C., Elser C., et al.* Hacking commercial quantum cryptography systems by tailored bright illumination // Nature Photonics. 2010. V. 4. № 10. P. 686–689.
18. *Sauge S., Lydersen L., Anisimov A., et al.* Controlling an actively-quenched single photon detector with bright light // Opt. Exp. 2011. V. 19. № 23. P. 23590–23600.
19. *Василиу Е.В., Гулаков И.Р., Зеневич А.О.* Квантовые системы обеспечения информационной безопасности. Минск: Белорусская государственная академия связи, 2019. 216 с.
20. Техника оптической связи: фотоприемники. Пер. с англ. / Под ред. Тсанга У. М.: Мир, 1988. 526 с.
21. *Гулаков И.Р., Зеневич А.О.* Фотоприемники квантовых систем. Минск: УО ВГКС, 2012. 276 с.
22. *Манова Н.Н. и др.* Система регистрации одиночных фотонов видимого и ближнего инфракрасного диапазона волн // Тез. докл. XXI Междунар. научно-техн. конф. по фотоэлектронике и приборам ночного видения. ФГПУ «НПО «Орион». М., 2010. С. 135–136.