

УДК 621.383.523

Д.А. Махорин, А.Б. Галиев, А.С. Задорин

Возможность реализации линейного режима счета фотонов на лавинном фотодиоде S8664-05K при комнатной температуре

Дан анализ помехоустойчивости цифрового приемного оптического модуля системы квантового распределения ключей в линейном режиме фоторегистрации при комнатной температуре. Предложен способ ее оптимизации за счет эквалайзирования его АЧХ. Рассмотрена модель управления уровнем ошибок и скоростью генерации ключа. Показана функциональность модели приемного оптического модуля на основе ЛФД S8664-05K при комнатной температуре.

Ключевые слова: лавинный фотодиод, счет фотонов, помехоустойчивость приемного оптического модуля.

Технология квантового распределения ключей (КРК), как известно, основывается на возможности регистрации одиночных фотонов, находящихся в том или ином кодовом состоянии – поляризованном, фазовом или временном [1–4]. Способность приемного оптического модуля (ПрОМ) системы КРК обеспечивать предельную светочувствительность и надежную регистрацию указанных кодовых состояний фотона, таким образом, становится одним из важнейших системных показателей, определяющих среднюю битовую скорость V_k генерации одномерного двоичного массива K секретного ключа на обеих сторонах системы. В качестве количественных показателей помехоустойчивости приемника КРК удобно использовать два показателя – вероятность P_l пропуска сигнальных посылок в моменты опроса пороговой схемы регенератора ПрОМ и вероятность генерации ложных символов P_f в ключе K .

Перспективы повышения помехоустойчивости (снижения P_l и P_f) ПрОМ связаны, в основном, с развитием соответствующей элементной базы – высокочувствительных и быстродействующих фотодиодов, малозумящих широкополосных электронных усилителей и др. Доступная номенклатура и хорошие параметры данных компонент в настоящее время позволяют реализовать режим регистрации одиночных фотонов уже при комнатной температуре.

Целью данного сообщения является анализ помехоустойчивости такого ПрОМ, построенного на основе лавинных фотодиодов (ЛФД) S8664-05K фирмы Hamamatsu [5] в линейном режиме фоторегистрации. Под линейностью здесь понимается режим пропорционального усиления сигнального тока i_s за счет лавинного размножения фотоэлектронов в обедненной области p - n -перехода ЛФД в M раз [6]. Альтернативой линейному режиму, как известно, является ключевой гейгеровский режим, реализуемый в ЛФД специальной конструкции [1].

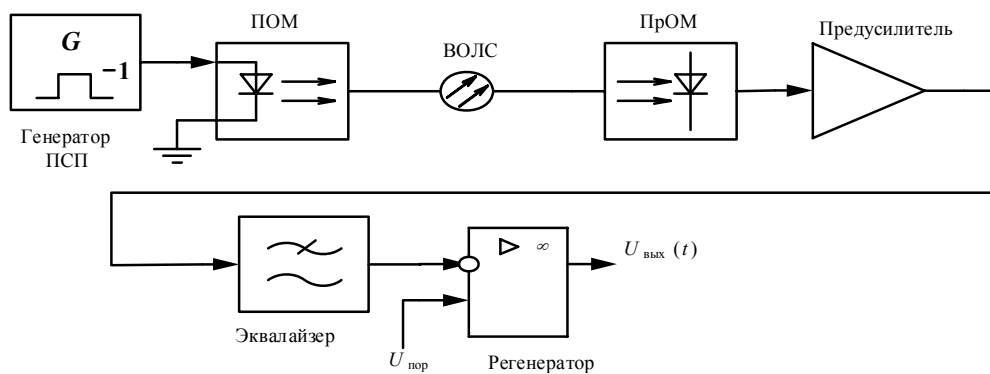


Рис. 1. Структурная схема приемопередающей части системы КРК

Следуя общей схеме построения систем КРК [1–4], будем полагать, что в передающем оптическом модуле (ПОМ) приготавливаются неортогональные кодовые однофотонные состояния (КОФС) в соответствии с возбуждающей их двоичной псевдослучайной последовательностью (ПСП), фор-

мируемой в генераторном блоке G со средней битовой скоростью этого B_0 (рис. 1). Также будем считать, что указанные КОФС предназначены для передачи по волоконно-оптической линии (ВОЛС), связывающей блоки ПОМ и ПрОМ (см. рис. 1). Для исключения разрушений КОФС в ходе транспортировки по оптическому волокну, будем полагать, что их приготовление в блоке ПОМ осуществляется на основе временного кодирования [3, 4].

Обозначим длину и погонное затухание ВОЛС через L и α соответственно, а внутренние шумы ПрОМ представим приведенными к его входу шумовыми источниками тока и напряжения S_E, S_I [6].

Сделаем еще одно допущение, касающееся формы импульсной характеристики $\delta_c(t)$ ЛФД, которую определим как его реакцию на одиночный фотон. Эта реакция определяется, с одной стороны, скоростями процесса лавинной ионизации и дрейфа плазменного сгустка в p - n -переходе и разряда емкости C выходной цепи ПрОМ – с другой. Обозначим длительность импульса $\delta_c(t)$ как τ_0 . Экспериментальная осциллограмма отклика $\delta_c(t)$ ЛФД на ряд одиночных фотонов приведена на рис. 2, а [7]. Аппроксимируем указанную импульсную характеристику гауссовой кривой (см. рис. 2, б):

$$\delta_c(t) = \frac{u_0}{\sqrt{2\pi\alpha}} \exp\left(-\frac{t^2}{2\alpha^2 T_0^2}\right), \quad (1)$$

где α – параметр формы импульса, определяющий долю тактового интервала $T_0 = 1/B_0$, занимаемого сигналом $\delta_c(t)$, так что $\tau_0 = \alpha T_0$.

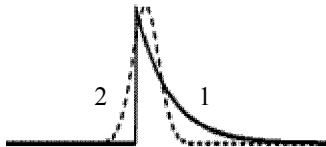


Рис. 2. Форма сигнального тока ЛФД в режиме счета фотонов (1) и гауссова аппроксимация импульсной характеристики ЛФД (2)

Воспользовавшись (1), определим вероятности P_I и P_f , связанные с внутренними источниками шума ПрОМ. Среди этих источников рассмотрим шумы нагрузки ЛФД, а также внутренними шумами источников S_E, S_I . При этом распределение плотностей вероятности $p(n)$ числа n фотоэлектронов в нагрузке ЛФД в отсутствии ($u_c = 0$) и присутствии ($u_c = M$) фотона также будем считать гауссовыми:

$$\begin{cases} p(n/u_c = 0) = \frac{u_0}{\sqrt{2\pi\sigma}} \exp\left(-\frac{n^2}{2\sigma^2}\right), \\ p(n/u_c = M) = \frac{u_0}{\sqrt{2\pi\sigma}} \exp\left(-\frac{(n-M)^2}{2\sigma^2}\right) \end{cases} \quad (2)$$

с безразмерной дисперсией σ [6]:

$$(\sigma(\alpha))^2 = \frac{2i_{tt}}{e} \tau I_2(\alpha) + \frac{\tau I_2(\alpha)}{e^2} \left(S_I + \frac{4kt}{R} \right) + S_E \left[\frac{I_2(\alpha)}{R^2} + (2\pi C)^2 \frac{I_3(\alpha)}{\tau e^2} \right], \quad (3)$$

где t – температура в градусах Кельвина; k – постоянная Больцмана; i_{tt} – темновой ток; R – нагрузочное сопротивление ЛФД; $\tau = 1/B$ – длительность импульсной характеристики ПрОМ, обратная ширине полосы частот приемника B .

Коэффициенты I_2, I_3 в формуле (4) называются интегралами Персона и выражаются через отношение спектров огибающей оптического сигнала на выходе и входе ПрОМ [6]. Аргументом этих зависимостей является безразмерная нормированная частота $\Omega = \omega/T$:

$$I_2 = \int_0^\infty \left| \frac{H'_{\text{ВЫХ}}(\Omega)}{H_{\text{ВХ}}(\Omega)} \right|^2 d\Omega, \quad I_3 = \int_0^\infty \left| \frac{H_{\text{ВЫХ}}(\Omega)}{H_P(\Omega)} \right|^2 \Omega^2 d\Omega. \quad (4)$$

Искомые параметры помехоустойчивости ПрОМ, вероятности P_I и P_f выражаются через формулы (2), (3) как

$$P_I = \int_{-\infty}^{U_{\text{пор}}} p(n/u_c = 0) dn, \quad P_f = \int_{-U_{\text{пор}}}^{\infty} p(n/u_c \neq 0) dn, \quad (5)$$

где $U_{\text{пор}}$ – порог срабатывания приемника, выраженный через число электронов n , проходящих через нагрузку ЛФД за время τ .

Особенностью оптического приемника системы КРК является малость промежутка времени τ , в котором локализованы сигнальные фотоэлектроны, по сравнению с длительностью тактового интервала $T_0 = 1/B_0$. Как указывалось выше, значение τ определяется уширением импульсной характеристики ЛФД $\delta_c(t)$ τ_0 в тракте ПрОМ в $\zeta = \tau/\tau_0$ раз. Свобода в выборе τ и ζ дает возможность оптимизации помехоустойчивости приемника за счет соответствующей регулировки указанных парамет-

ров. Возможность оптимизации следует из описываемой формулой (3) функции $\sigma(\alpha)$, в которой второй и последний члены показывают противоположные зависимости от τ . В данных условиях для известных параметров $i_{и}$, R , C , S_E и S_I несложно отыскать оптимальное значение τ_{opt} , при котором $\sigma(\zeta)$ достигает минимума. Вывод иллюстрируется графиком $\sigma(\zeta)$ на рис. 3, рассчитанным по формулам (3), (4). График получен для ЛФД S8664-05K с параметрами, взятыми из [5]: $\eta = 0,78$, $C = 1,5$ пФ, $t = 253$ К, $i_{и} = 0,15$ нА, $M = 100$, напряжение смещения диода $U = 380$ В. Номинал нагрузочного сопротивления ЛФД взят равным 5 МОм, а параметры T_0 и τ_0 – 10 мкс и 2 нс соответственно. На практике необходимое значение τ_{opt} достигается за счет соответствующего эквалайзирования АЧХ ПрОМ.

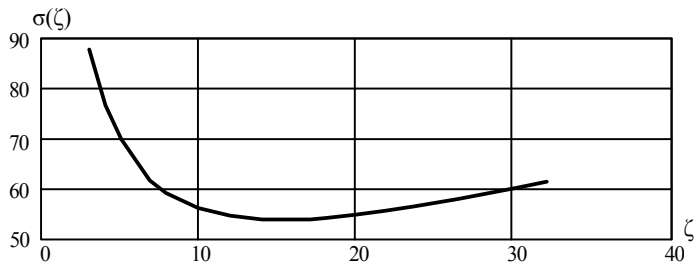


Рис. 3. Зависимость дисперсии шумовых электронов от сжатия $\zeta = \tau/\tau_0$ полосы частот ПрОМ

Подставляя полученные данные в (2), (3) найдем распределения условных плотностей вероятности $p(n/u_c = 0)$ и $p(n/u_c = M)$ числа n фотоэлектронов в нагрузке ЛФД в отсутствие и присутствии фотона. График этих зависимостей приведен на рис. 4.

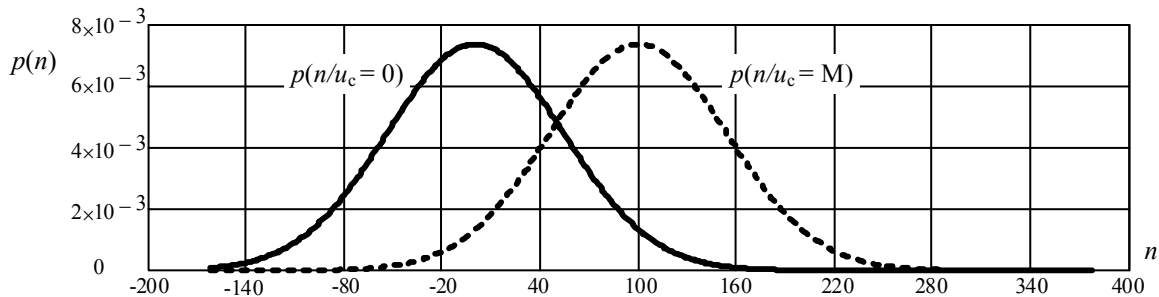


Рис. 4. Зависимость условных плотностей вероятности числа фотоэлектронов в нагрузке ЛФД S8664-05K в отсутствие и присутствии одного фотона

В соответствии с (5) расчет параметров помехоустойчивости P_l и P_f проведем путем интегрирования графиков $p(n/u_c = 0)$ и $p(n/u_c = M)$ в пределах, ограниченных порогом срабатывания $U_{пор}$. Результаты расчета P_l и P_f как функций $U_{пор}$ приведены на рис. 5.

При анализе данных рис. 5 следует учитывать еще одну особенность ПрОМ систем КРК, отличающую их от связанных цифровых приемников. Помехоустойчивость последних, как известно, определяется суммой P_l и P_f [6]. Поэтому наилучшим уровнем порога $U_{пор}$ таких приемников считается точка пересечения кривых $p(n/u_c = 0)$ и $p(n/u_c = M)$ на рис. 4. Для систем КРК связь P_l и P_f с помехоустойчивостью более опосредована. Здесь пропущенные символы удаляются из массива K в ходе протокольных переговоров, поэтому вероятность P_l не вносит никаких ошибок в формирование ключа, а определяет лишь среднюю скорость V_k его генерации [2, 3, 8]:

$$V_k = B_0(1 - P_l)p(1)k_p \exp(\alpha L), \tag{6}$$

где $p(1)$ – вероятность генерации фотона в тактовом интервале B_0 , которая на практике берется равной $\sim 0,1$; k_p – коэффициент снижения скорости, предусмотренный конкретным протоколом КРК.

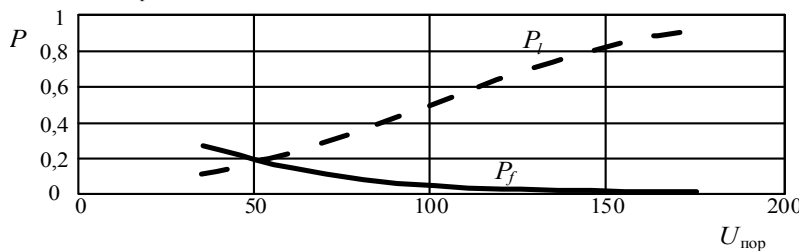


Рис. 5. Зависимости вероятностей P_l и P_f от уровня порога дискриминатора ПрОМ

Уровень ложных сигналов в ключе при этом описывается строго контролируемым параметром P_f . В простейшем случае в качестве инструмента контроля может использоваться пороговый уровень $U_{пор}$. Приведенный на рис. 4 пример зависимостей P_l и P_f от $U_{пор}$ оптического приемника,

строенного на ЛФД S8664-05K, вместе с формулой (6) демонстрирует возможности управления скоростными параметрами системы и уровнем P_f посредством регулировки $U_{пор}$.

Представленные расчеты доказывают функциональность рассматриваемой модели ПрОМ при комнатной температуре. Так, например, при $U_{\text{пор}} = 125$ данный приемник способен обеспечить скорость генерации секретного ключа 7,999 Кб при вероятности ошибок $P_f = 0,01$.

Литература

1. Cova S. Avalanche photodiodes and quenching circuits for single-photon detection / S. Cova, M. Ghioni, A. Lacaita et al. // *Applied Optics*. – 1996. – Vol. 35, № 12. – P. 1956–1976.
2. Килин С. Я. Квантовая информация // *Успехи Физических Наук*. – 1999. – Т. 169. – С. 507–527.
3. Молотков С.Н. Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы // *Письма в ЖЭТФ*. – 2004. – Т. 79, вып. 11. – С. 691–704.
4. Debuisschert T. Time coding protocols for quantum key distribution/ T. Debuisschert, W. Boucher // *Physical Review A*. – 2004. – Vol. 70, Iss. 4. – P. 042306–042321.
5. Si APD S8664 series [Электронный ресурс]. – Режим доступа – http://sales.hamamatsu.com/assets/pdf/parts_S/S8664_series.pdf, свободный (дата обращения 10.11.2013).
6. Keiser G. *Optical Fiber Communications*. – New York: McGraw-Hill Inc., 1991. – 461 p.
7. Скорость генерации кода в системе квантового распределения ключей / А.С. Задорин, А.В. Максимов, Д.А. Махорин и др. // *Доклады ТУСУРа*. – 2011. – № 2 (24), ч. 2. – С. 139–141.

Махорин Дмитрий Алексеевич

Аспирант каф. радиоэлектроники и защиты информации (РЗИ) ТУСУРа
Тел.: 8-913-824-11-11
Эл. почта: mda.tomsk@gmail.com

Галиев Азамат Бахытжанович

Магистрант гр. 142М, каф. РЗИ

Задорин Анатолий Семенович

Зав. каф. РЗИ
Тел.: (382-2) 41-33-65
Эл. почта: Anatoly.Zadorin@rzi.tusur.ru

Makhorin D.A., Galiyev A.B., Zadorin A.S.

The possibility of realization a linear mode of photon counting by avalanche photodiode S8664-05K at room temperature

In the paper we analyze the noise immunity of digital optical receiver module (DORM) of quantum key distribution in the linear mode of photographic at room temperature. We propose a method to optimize at the expense of equalizing the response. We considered a model of the control error rate and the rate of key generation. The functionality of the model is shown in the promo APD S8664-05K at room temperature.

Keywords: avalanche photodiode, photon counting, DORMs noise immunity.