Защищенный атмосферный канал оптической связи

Серенков Р. В., Разгуляев С. И.

Научный руководитель: доктор физико-математических наук, профессор заведующий кафедрой РЗИ Задорин А.С.

Аннотация: Предложена симуляционная модель защищённой системы связи на основе квантового распределения ключей по атмосферному каналу оптической связи по протоколу B92.

Ключевые слова: Квантовое распределение ключей, поляризационное кодирование кубитов, протокол B92.

Введение

Одной из главных проблем создания защищенного канала связи с симметричным шифрованием данных является проблема распределения криптографических ключей [1]. Наиболее совершенными и устойчивыми к внешним атакам являются системы квантового распределения ключей (СКРК) [2], структурная схема которой приказана на рис.1.

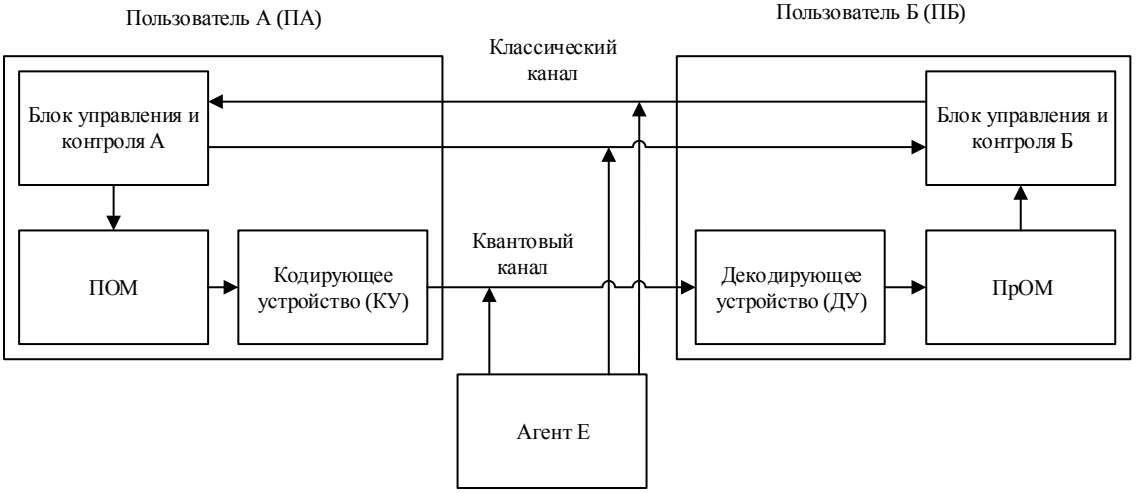

Рис. 1. Структурная схема СКРК

В основе данной системы лежит передача по квантовому каналу двумя легитимными удаленными пользователями Алисой и Бобом набора закодированных двухуровневых однофотонных посылок - кубитов $\{|\psi_j|\}$. Если данное множество представлено двумя состояниями $|\psi_\pm\rangle$ с соответствующей априорными вероятностями $\eta_\pm$, то вероятность минимальной ошибки их измерений стороной Боб, как известно, определяется оценкой Хилстрома (Helstrom):

$$P_e(opt) = \frac{1}{2}(1 - \sqrt{1 - 4\eta_+\eta_-|\langle\psi_+|\psi_-\rangle|^2}) \qquad (1)$$

Из (1) видно, что оценка принимает нулевое значение только в случае ортогональности измерительных базисов кубитов.

Другая стратегия измерений состояний $|\psi_\pm\rangle$ предложена Ивановичем (Ivanovic) [1-3], которая позволяет безошибочное различение неортогональных состояний кубитов, но с

некоторой конечной вероятностью получения третьего, не четкого результата $P_?(opt)$. В работах Дикса (Dieks) и Переса (Peres) установлено, что при одинаковой априорной вероятности $\eta_\pm$ минимальный предел $P_?(opt)$, называемый ограничением Ивановича-Дикса-Переса (Ivanovic-Dieks-Peres/IDP), равен:

$$P_?(opt) = |\langle\psi_+|\psi_-\rangle| \qquad (2)$$

Указанная стратегия измерений положена в основу классического протокола B92 Ч.Беннета 1992 г., на практике реализуемого в поляризационном и фазовом форматах кодирования [3]. Наиболее простым в реализации оказывается вариант поляризационного кодирования $|\psi_i\rangle$.

Постановка задачи

Целью настоящего сообщения является разработка и исследование программной модели СКРК указанного типа.

Основная часть

Программная модель СКРК по рис.1 была реализована с помощью средств ПО Matlab - Simulink. Имеющиеся в нашем распоряжении пакеты расширения Toolbox Matlab-Simulink не содержали оптоэлектронных компонент для контроля поляризации и др. параметров объектов $|\psi_\pm\rangle$, нами была реализована модель СКРК B-92 по схеме фазового кодирования кубитов [3].

Соответствующие алгоритмические схемы S-программ передающий и принимающей сторон представлены на рис.2,3. Здесь показан процесс формирования ключевого кода $\mathbf{k}_i$, создаваемого на основе псевдослучайной последовательности (ПСП) блока “Random Integer”. Биты ПСП в кодирующем устройстве преобразуются в кубиты $|\psi_\pm\rangle$, и в заданной пропорции в квантовом канале смешиваются с тепловыми, гауссовыми шумами. Далее, в соответствии с протокольной процедурой, пользователь Боб по квантовому каналу принимает последовательность $|\psi_\pm\rangle$. При этом, интегратор на рис.4. моделирует функцию призмы-расщепителя стандартной схемы СКРК-B92 [3]. Управляемые данным интегратором базисные сигналы, сдвинуты по фазе относительно тактовой последовательности на $\pi/2$. Таким образом, измеренный принимающей стороной коэффициент корреляции достигает максимума при разности фаз между принятым и сгенерированным битом в 45 градусов, и минимума – когда разность фаз равна 90 градусам. Случайный характер измеряемого состояния поляризации кубитов на приемной стороне симулируется отдельным элементом ПСП.

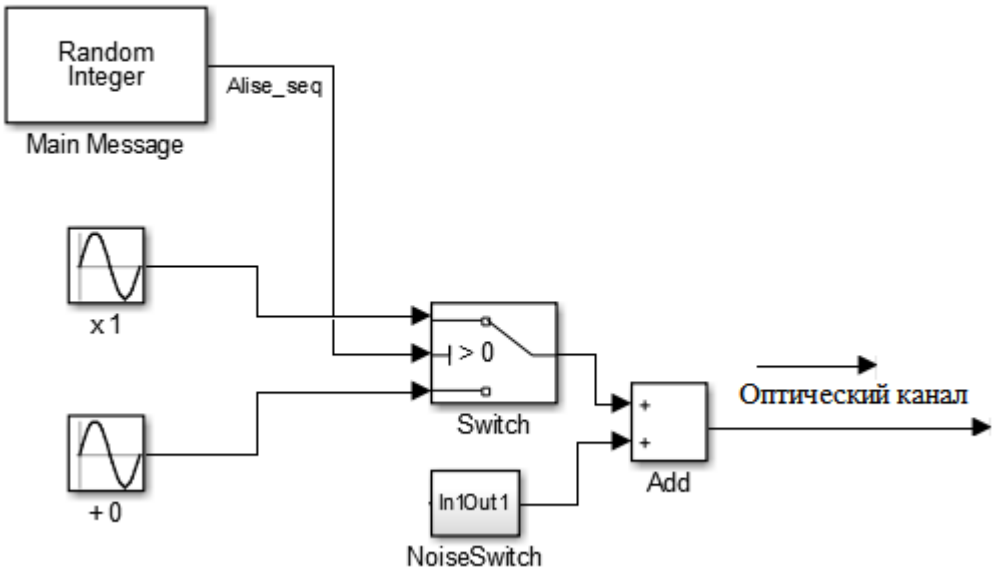

Рис. 2 – Алгоритм работы передающей стороны СКРК

Корреляционные максимумы с выхода интегратора на рис.3. проходят через пороговое устройство (на рис.3 “Combine circuit”), и формируют импульсы, разрешающие запись текущего бита в регистр ключевой последовательности $\mathbf{k}_i$.

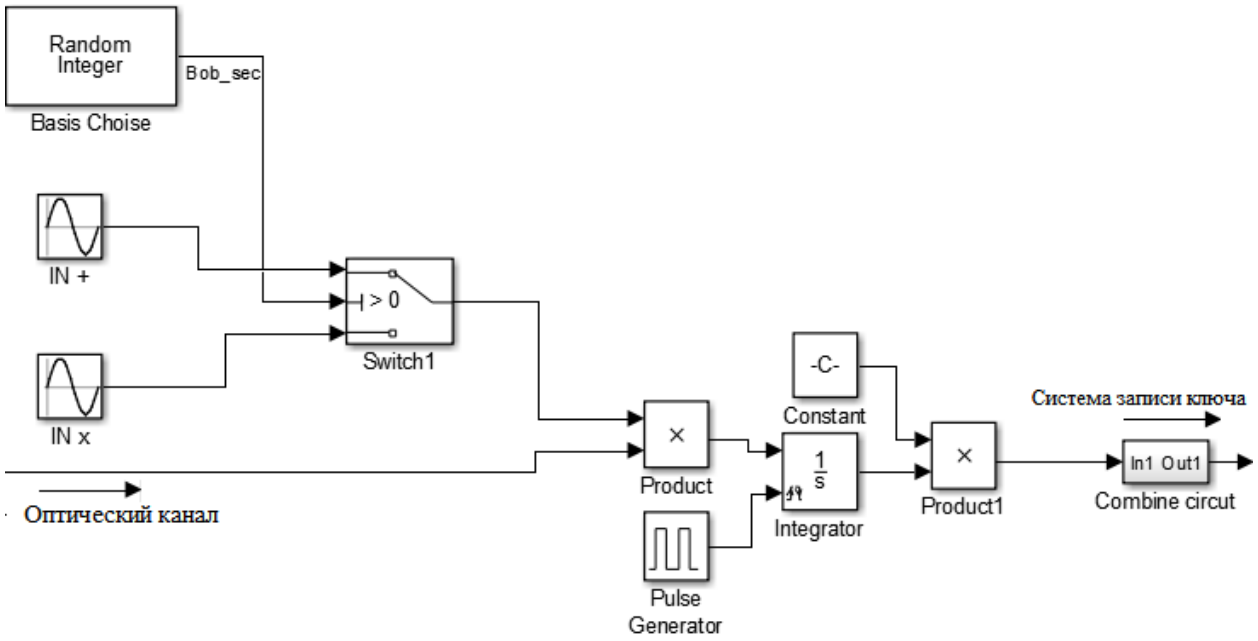

Рис. 3 – Алгоритм работы приемной стороны СКРК

Система записи ключа (рисунок ПА1) моделирует «общение» Боба и Алисы по открытому каналу связи. Боб открыто сообщает Алисе о зафиксированном превышении порогового уровня порогового устройства, указывающего на идентичность значений текущего бита $\mathbf{k}_i$ на обеих сторонах СКРК.

Наличие системных шумов СКРК не только вызывает избыточные ошибки в $\mathbf{k}_i$, но и позволяет злоумышленнику скрывать свое присутствие.

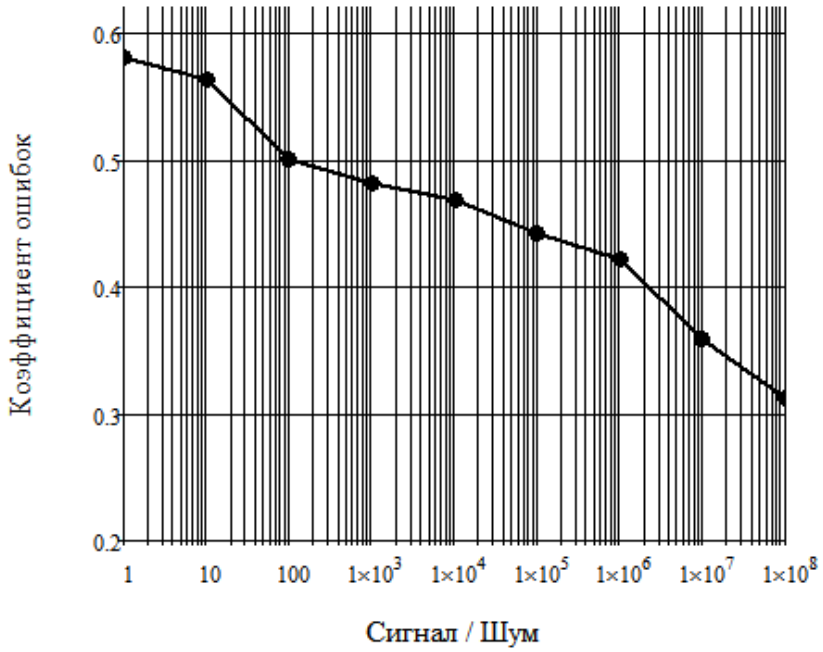

Рис. 4 – Зависимость коэффициента ошибок СКРК от отношения сигнал/шум

На рис.4 представлен полученный с помощью описанной выше модели график зависимости коэффициента ошибок последовательности $\mathbf{k}_i$, от отношения сигнал-шум. Результаты моделирования показывают. что «врезка» злоумышленника АЕ в квантовый канал СКРК приводит к скачку коэффициента ошибок примерно до уровня 0,4 и резкому снижению системного битрейта. Таким образом, контроль за указанными параметрами позволяет надежно детектировать присутствие АЕ.

Заключение

Разработанная нами расчетная модель СКРК-B92 с поляризационным кодированием для атмосферного канала оптической связи, позволяет исследовать характеристики разрабатываемого нами прототипа СКРК.

Список использованных источников

1. Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю. Квантовая криптография, (Учебно-методическое пособие) Макс Пресс Москва 2011, 112 с.
2. Имре Ш., Балаж Ф. Квантовые вычисления и связь. Инженерный подход. – М., Физматлит: 2008. – 320 с.
3. Bennett, C.H. Quantum cryptography using any two nonorthogonal states / C.H. Bennett // Phys. Rev. Lett. —1992. —Vol. 68. —P. 3121.

Приложение А

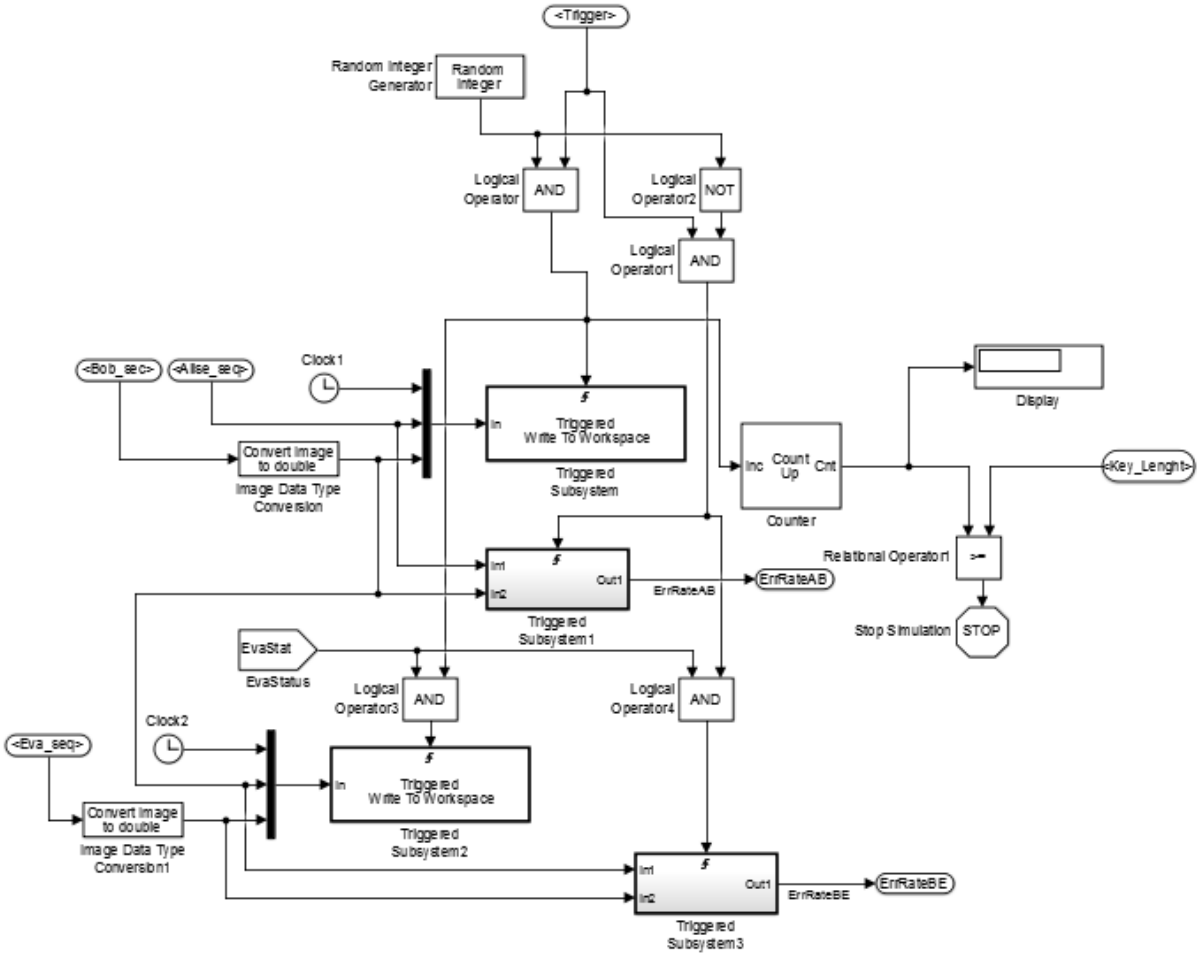

Рисунок ПА1 – Структурная схема открытого канала связи и системы записи ключа.

Приложение Б

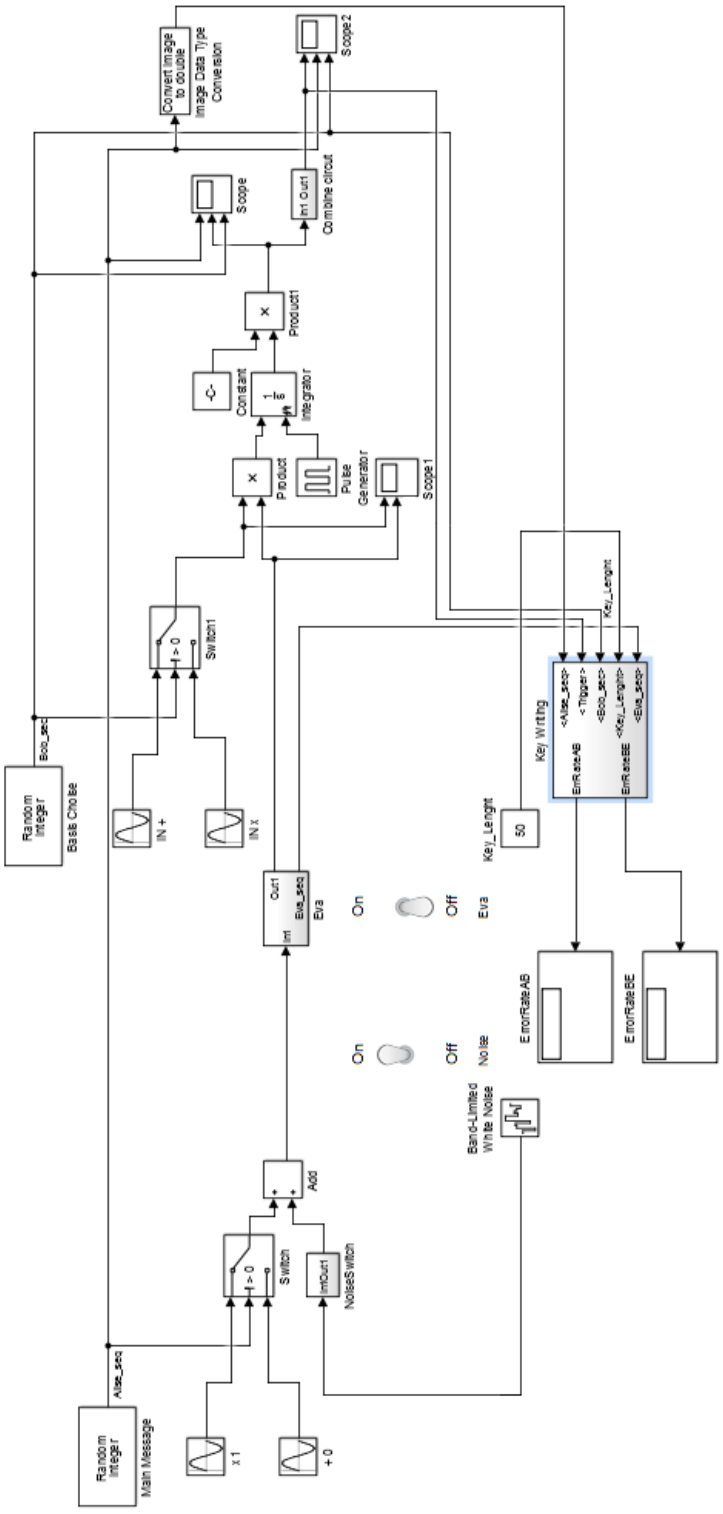

Рисунок ПБ1 – Модель СКРК В-92 по схеме фазового кодирования кубитов.