К.Е. РУМЯНЦЕВ (д.т.н., профессор), **И.Е. ХАЙРОВ** (к.т.н.), **В.В. НОВИКОВ** (магистрант)
(Таганрогский государственный радиотехнический университет)

ДОСТУП К ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО КВАНТОВО-КРИПТОГРАФИЧЕСКОМУ КАНАЛУ

Основным этапом при реализации криптографических протоколов является обмен ключами между абонентами. В обычных системах связи передача этой секретной информации осуществляется по закрытым каналам, в которых ключ представляет собой последовательность нулей и единиц. Идеи создания квантовых компьютеров и бурно развивающаяся в связи с этим области науки квантовой информатики породили новое направление, основной задачей которого является распределение ключа между легальными пользователями, и которое получило название квантовая криптография.

При использовании квантово-криптографических методов генерация ключа может происходить непосредственно в процессе передачи, происходящей по абсолютно открытому каналу. Носителями в данном случае являются элементарные частицы (фотоны), тот или иной физический параметр которых определяет полезную информацию, а надежность самих методов, соответственно, держится на нерушимости базовых законов квантовой механики.

Большинство существующих квантово-криптографических протоколов, таких как BB84, BB92 и ЭПР, используют в качестве параметра тип поляризации фотонов. При экспериментальной реализации протокола, основанного на кодировании по поляризации и осуществляющего обмен данными между пользователями А и Б, исследуется влияние третьего пользователя В. Одним из базовых принципов является принцип неопределенности Гейзенберга, а также теорема о невозможности клонирования неизвестного квантового состояния, представляющего собой суперпозицию базисных состояний, согласно которым взаимодействие макросистемы (измерителя) с микросистемой приведет к разрушению этого состояния. При теоретическом рассмотрении этого процесса, когда передача осуществляется при помощи одиночных фотонов, пользователь В не может отвести часть сигнала, так как нельзя поделить электромагнитный квант на части. В реальных же условиях это вызовет сильное затухание сигнала (либо вообще его отсутствие), что поставит под сомнение корректность приема у пользователя Б. При непосредственном вмешательстве в процесс обмена сильно возрастает уровень ошибок, что делает любой протокол крайне неэффективным. Проанализировать присутствие третьего пользователя В можно, предполагая, что передавался фотон с вертикальным типом поляризации (рис. 1), суперпозиционное состояние которого $|\mathbf{b}\rangle = \langle a_1 | \mathbf{!} \rangle + \langle b_1 | \mathbf{!} \rangle$, где a_1, b_1 - амплитуды вероятностей – коэффициенты, квадрат которых определяет вероятность присутствие того или иного типа поляризации в общем суперпозиционном состоянии.

На рис. 1а пользователи Б и В используют одинаковые измерители, ориентированные так, что их применение позволяет не только извлечь информацию о типе поляризации, но и правильно определить состояние поляризации.

При использовании также одинаково ориентированных анализаторов (рис.1б) видно, что пользователь В определит лишь часть суперпозиционного состояния, причем состояние фотона на выходе его анализатора будет правильно принято пользователем Б и результат их измерений может будет одинаков. Однако он будет неправильным и в том, и в другом случае относительно пользователя А и открытые переговоры между отправителем А и получателем Б, предусмотренные квантово-криптографическими протоколами, позволят обнаружить и скорректировать ошибку.

Применение же различных анализаторов на рис. 1в обусловливает правильность определения поляризационного состояния пользователем В, а при детектировании информации пользователем Б произойдет ошибка. При коррекции неправильной интерпретации бита информации пользователями А и Б результат измерения все равно будет отброшен.

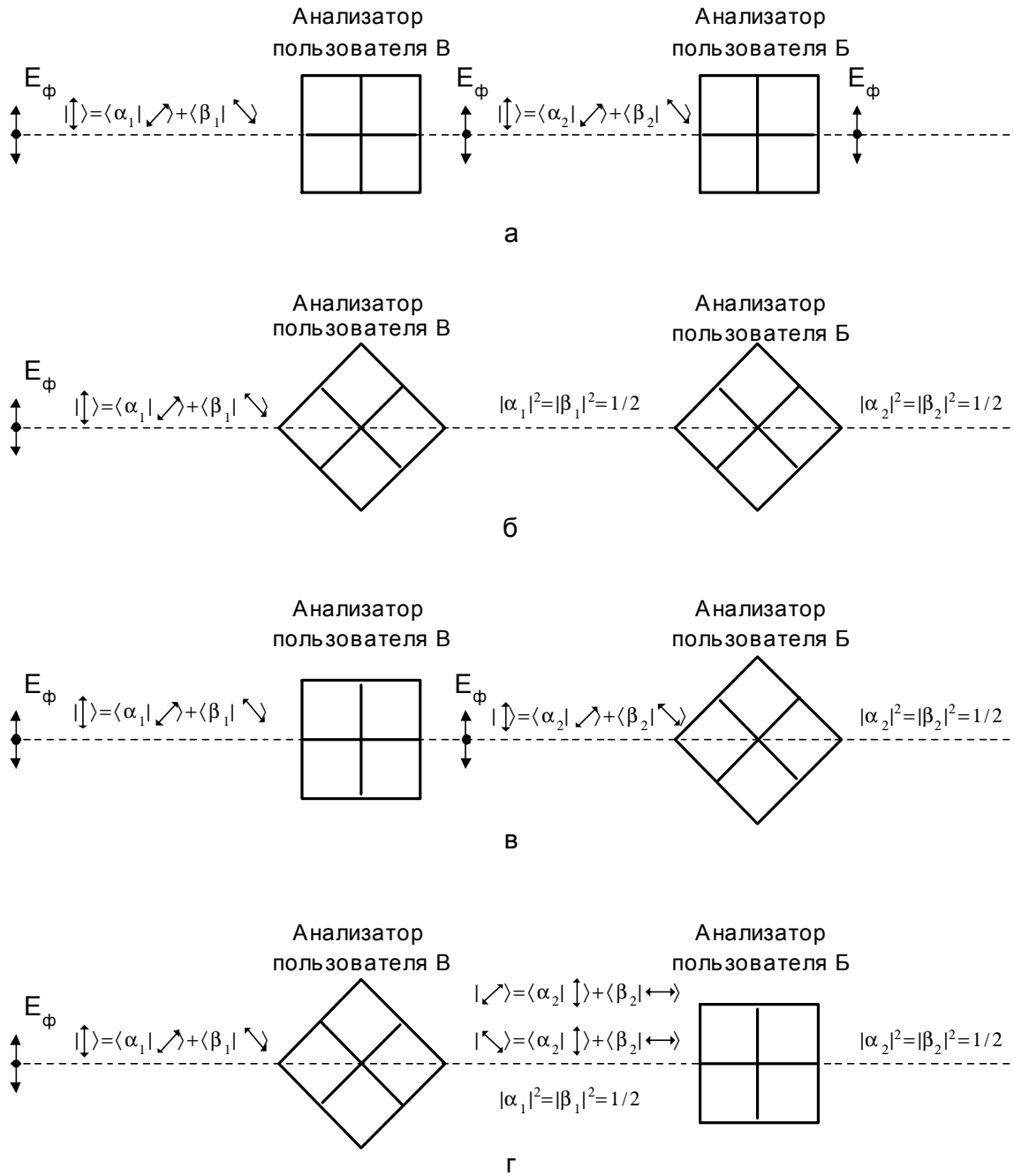

Рис. 1. Непосредственное вмешательство пользователя В в сеанс связи

Интерес представляет последний случай, изображенный на рис. 1г. Неправильная ориентация измерителя пользователя В вносит ошибку в процесс передачи, хотя при отсутствии пользователя В результат измерения пользователя Б был бы правильным.

В работе обосновывается возможность измерения неизвестного поляризационного состояния путем измерения его известного типа поляризации. Данный метод основан на эффекте вынужденного испускания активного вещества, при котором на выходе будет несколько фотонов с одинаковой поляризацией, а вернее с одинаковым типом поляризации. Эффект вынужденного испускания позволяет получить “копии” фотона, проходящего через активную среду, а измерения, производимые над полученной группой фотонов пользователем В, не повлияют на сеанс связи пользователей А и Б.

Применение данного метода не противоречит теореме о невозможности клонирования неизвестного квантового состояния, каким является суперпозиционное состояние поляризации фотона. Метод предполагает копирование только типа поляризации, а измерение суперпозиционного состояния, в конечном итоге, однозначно определяется используемым измерителем. Следует также отметить, что при определенных условиях пользователи А, Б, В будут обладать одной и той же конфиденциальной информацией.