УДК 621.391.63

РАЗРАБОТКА СТАНДАРТНОЙ МОДЕЛИ СЦЕНАРИЯ АТАКИ НА ИНФОРМАЦИЮ, ПЕРЕДАВАЕМУЮ В СЕТЯХ PON

В.И. КИРИЛЛОВ[1], Е.А. КОВРИГА[2]

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
[1]kirillov@bsuir.by; [2]cool_kit@mail.by

На основе предыдущих авторских публикаций дополнена стандартная модель сценария атаки на информацию, передаваемую в пассивных волоконно-оптических сетях PON; выделены преимущества и особенности применения квантовой криптографии в сетях PON.

Ключевые слова: пассивные волоконно-оптические сети PON, защита информации, симметричные/асимметричные криптосистемы, квантовая криптография.

В статье [1] показано, что криптографические средства защиты информации являются единственными эффективными мерами при борьбе с нарушением достоверности передаваемой информации и нарушением конфиденциальности в тех случаях, когда измерительные методы не позволяют выявить злоумышленника.

В современной литературе выделяют два типа криптосистем: симметричные и асимметричные [2]. У обеих этих систем есть существенные недостатки: при симметричном шифровании взаимодействующим сторонам необходим защищенный канал, по которому они могли бы обмениваться секретными ключами, а асимметричные системы основываются только на относительно медленном развитии технического прогресса [2]. Поэтому возникла потребность в криптографических системах, основанных на принципах, отличных от математических. В качестве примера такой системы можно привести квантовую криптографию. Прежде всего, системы квантовой криптографии ориентированы на создание абсолютно защищенного канала для распределения ключа и разделяются на два направления: кодирование квантового состояния одиночной частицы и квантовое перепутывание фотонов [3].

В настоящее время ученые-исследователи стремятся увеличить т.н. «физические» параметры систем квантовой криптографии (а именно протяженность волоконно-оптической линии связи); разрабатывают модифицированные протоколы кодирования, направленные на уменьшение количества полезной информации, которую теоретически может получить злоумышленник, но в то же время на увеличение значения ошибки на приемной стороне, вызванной действиями нарушителя; переходят от систем «точка-точка» к древовидной топологии «точка-многоточка», что становится особенно актуальным в связи с повсеместным развертыванием пассивных волоконно-оптических сетей доступа PON в качестве абонентской «последней мили» (переданный отправителем единичный фотон не может быть разделен или скопирован, но может появиться с некоторой вероятностью на одном из выходов сплиттера) [3].

Приведем несколько примеров актуальных разработок: в статье [4] показано, что скорость распределения квантового ключа можно повысить, установив сплиттер, в отличие от традиционных древовидных схем сетей PON, в т.н. «центральном офисе» у отправителя; в работе [5] вместо обычных пассивных сплиттеров применялись активные оптические переключатели, способные подключать отправителя к любому из получателей, создавая тем самым временные каналы «точка-точка»; в статье [6] смодели-

рована возможность построения звездообразной сети с распределением квантовых ключей без участия «центрального узла».

Таким образом, с учетом всего вышеизложенного полученную в [1] обобщенную модель сценария атаки на информацию, передаваемую по сетям PON, можно дополнить, как показано на рис. 1.

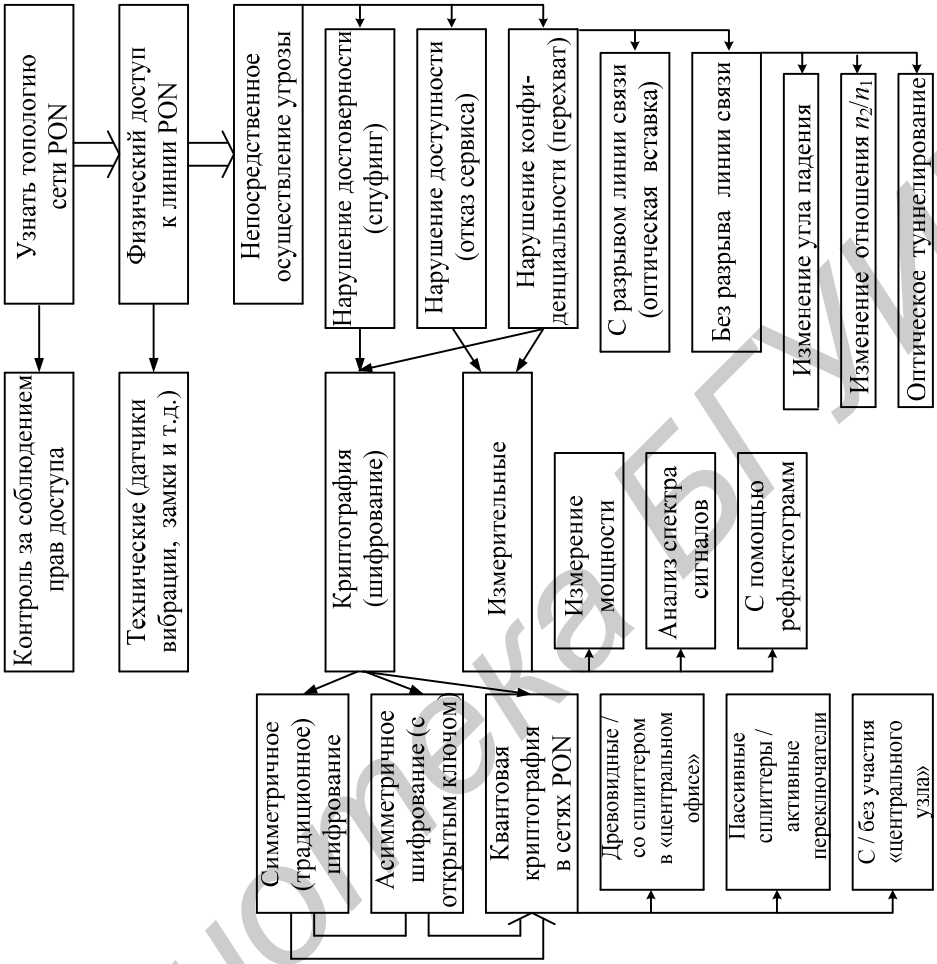

Рис. 1. Стандартная модель сценария атаки на информацию, передаваемую в сетях PON

Список литературы

1. *Кириллов В.И., Коврига Е.А.* Исследование обобщенной модели сценария атаки на информацию, передаваемую по пассивным волоконно-оптическим сетям PON // Веснік сувязі, 2014 *(В печати)*.

2. *Чмора А.Л.* Современная прикладная криптография. 2-е изд., стер. М.: Гелиос АРВ, 2002. 256 с.

3. *Бирин Д.А.* // T-Comm, 2012. №7. С. 27–29.

4. *Fernandez V., Collins R.J., Gordon K.J. etc.* // Optics Express, 2005. V. 13 (8). P. 3015–3020.

5.] *Tang X., Ma L., Mink A. etc.* Demonstration of an active quantum key distribution network [Электронный ресурс]. – Режим доступа: www. proceedings.spiedigitallibrary.org/proceeding. aspx?articleid=1290518. – Дата доступа: 29.11.2013.

6. *Mo X.-F., Zhang T., Xu F.-X. etc.* Quantum key distribution network with wavelength addressing [Электронный ресурс]. – Режим доступа: www.arxiv.org/abs/quant-ph/0610096v2. – Дата доступа: 29.11.2013.