МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КАНАЛА ЗАЩИЩЕННОЙ СВЯЗИ

Ю.В. Злобина

Частное предприятие «ВитЭлектро», Гродно, Республика Беларусь

На сегодняшний день широкое распространение использования получили волоконно-оптические каналы связи, для описания которых целесообразно использовать математическую модель дискретного канала связи.

Системы связи с возможностью обеспечения конфиденциальности передаваемой информации подразделяются на одноключевые (симметричные), двухключевые (ассиметричные) и системы на основе гибридного метода шифрования данных [1].

Математическая модель защищенной связи позволяет формализовать процессы обмена информацией и определить уязвимости системы, включает в себя описание криптографических протоколов, алгоритмов шифрования и методов аутентификации, позволяет проводить анализ устойчивости системы к различным атакам, включая перехват информации, подделку данных и внедрение вредоносного программного обеспечения. Математическая модель защищенной связи может быть использована для

сравнительного анализа пропускной способности системы передачи конфиденциальных данных между легитимными пользователями без наличия несанкционированного пользователя в системе связи с обеспеченной конфиденциальностью передаваемой информации и при его наличии.

Построение математической модели квантового канала связи строится на том, что передача информации в детекторе осуществляется двоичными символами («0» и «1») [2]. При передаче символа «1» одноквантовый оптический импульс передается в волокно, а при передаче символа «0» – излучение отсутствует. Приемный модуль выполняется в виде счетчика фотонов, который регистрирует фотоны оптического излучения в течение времени передачи синхроимпульса, генерируемого на передающей стороне на время передачи каждого символа. При отсутствии несанкционированного пользователя в системе численные значения вероятностей приема символов «0» и «1», которые определяют вероятность ошибки передачи данных, будут равны.

С помощью построения графов вероятностей получаются выражения, с помощью которых определяется пропускная способность на участке между легитимными пользователями и на участке между легитимной передающей стороной и нелегитимным пользователем.

В присутствии несанкционированного пользователя в системе вероятность ошибки при приеме данных не равна нулю. Это вызвано тем, что вероятность выхода фотона излучения из оптического волокна в результате съема данных при помощи макроизгиба волокна зависит от его диаметра [3]. С уменьшением диаметра макроизгиба волокна увеличивается пропускная способность канала утечки информации. С ростом длины волны оптического излучения увеличивается значение пропускной способности канала утечки информации.

Выражения для оценки пропускной способности на участке между легитимными пользователями учитывают вероятность несанкционированного вывода мощности излучения из оптического волокна, а также параметры счетчика фотонов: вероятность, появления темновых импульсов, квантовую эффективность регистрации

Список литературы

1. Дмитриев С.А. Волоконно-оптическая техника: современное состояние и новые перспективы. М., 2010.

2. Клюев Л.Л. Теория электрической связи. Минск: Техноперспектива, 2008. 423 с.

3. Тимофеев А. М. Оценка влияния интенсивности оптического сигнала на вероятность ошибочной регистрации данных в однофотонном канале связи // Информатика. 2021. Т. 18, № 2. С. 72–82.