

из критериев оценки надежности квантово-криптографических каналов связи является вероятность ошибочной регистрации данных [1, 3]. Поскольку до настоящего времени исследование влияния такого параметра счетчика фотонов, как мертвое время, на вероятность ошибочной регистрации данных применительно к квантово-криптографическому каналу связи не выполнялось, это являлось целью данной работы. Объектом исследования являлся асинхронный двоичный несимметричный однородный волоконно-оптический канал связи без памяти и со стиранием. Предметом исследования являлось установить влияние средней скорости счета импульсов при передаче двоичных символов «0» на выходе счетчика фотонов n_{s0} на вероятность ошибочной регистрации этих символов $P_{ош0}$. Определено, что с увеличением средней скорости счета сигнальных импульсов на выходе счетчика фотонов зависимости $P_{ош0}(n_{s0})$ вначале уменьшаются, достигая наименьшего значения, после чего растут. Это имеет место как при наличии мертвого времени продлевающегося типа, так и при его отсутствии. Установлено, что в диапазонах средних скоростей счета сигнальных импульсов n_{s0} , на которых зависимости $P_{ош0}(n_{s0})$ уменьшаются, увеличение средней длительности мертвого времени продлевающегося типа τ_d при прочих равных параметрах приводит к росту вероятностей ошибочной регистрации символов «0». Однако в диапазонах n_{s0} , на которых зависимости $P_{ош0}(n_{s0})$ растут, увеличение τ_d , напротив, приводит к уменьшению $P_{ош0}$.

Список литературы

1. Щеглов А.Ю. Анализ и проектирование защиты информационных систем. СПб., Профессиональная литература, 2017. 415 с.
2. Румянцев К.Е. Повышение эффективности алгоритма вхождения в синхронизм системы квантового распределения ключей // Известия ЮФУ. 2015. № 8 (169). С. 6–18.
3. Тимофеев А.М. Влияние времени однофотонной передачи информации на вероятность ошибочной регистрации данных асинхронных квантово-криптографических каналов связи // Вестник ТГТУ. 2019. Т. 25, № 1. С. 36–46.

ОЦЕНКА ПОТЕРЬ ИНФОРМАЦИИ ОДНОФОТОННОГО КАНАЛА СВЯЗИ С ПРИЕМНЫМ МОДУЛЕМ НА ОСНОВЕ СЧЕТЧИКА ФОТОНОВ

А.М. Тимофеев, И.Г. Веремейчик, В.А. Касько, И.А. Ковалев

Одной из наиболее важных задач, решаемых при передаче двоичных данных по волоконно-оптическим каналам связи, является обеспечение скрытности и конфиденциальности передаваемой информации [1]. Для решения этой задачи применяют, как правило, комплекс мер, включая организацию квантово-криптографических каналов связи. Такие каналы характеризуются наиболее высоким уровнем информационной безопасности, что достигается за счет применения маломощных оптических сигналов и, соответственно, высокочувствительных приемных модулей – счетчиков фотонов [1, 2]. При этом весьма важно, чтобы приемное оборудование легитимных пользователей обеспечивало наименьшие потери передаваемой информации. Отметим, что потери информации в указанных каналах связи обусловлены наличием мертвого времени счетчиков фотонов – времени, в течение которого счетчик фотонов не чувствителен к падающему на него оптическому излучению. Поскольку до настоящего времени оценка влияния мертвого времени счетчиков фотонов на потери информации, передаваемой по квантово-криптографическим каналам связи, не выполнялась, это являлось целью данной работы. Применительно к квантово-криптографическим каналам связи получены выражения для оценки вероятностей ошибочной регистрации двоичных символов («0» и «1») и условной энтропии, которые учитывают среднюю длительность продлевающегося мертвого времени счетчика фотонов. По результатам выполненных исследований установлено, что с увеличением средней длительности мертвого времени продлевающегося типа наименьшие потери передаваемой информации наблюдаются при более высоких средних скоростях счета сигнальных импульсов на выходе счетчика фотонов как при регистрации символов «0», так и при регистрации символов «1».

Список литературы

1. Квантовая криптография: идеи и практика / С.Я. Килин [и др.]. Минск: Беларус. наука, 2007. 391 с.
2. Тимофеев А.М. Устройство для передачи и приема двоичных данных по волоконно-оптическому каналу связи // Приборы и методы измерений. 2018. Т. 9, № 1. С. 17–27.

МОДЕЛИРОВАНИЕ ВОЗДЕЙСТВИЯ ЭЛЕКТРОМАГНИТНЫХ ПОМЕХ НА ИНТЕГРАЛЬНЫЕ МИКРОСХЕМЫ Н.А. Титович, В.Н. Теслюк, В.А. Тарасенко

При исследовании влияния электромагнитных помех (ЭМП) на интегральные микросхемы (ИМС), блоки и устройства радиоаппаратуры целесообразно проводить испытания с использованием ТЕМ-камеры. При этом перед экспериментом проводится предварительное расчетное моделирование влияния ЭМП на ИМС и устройства. Это позволяет значительно сократить затраты времени и средств. Используя для расчетов библиотеку ранее разработанных простых моделей, можно прибегать к проведению эксперимента только на стадии испытаний законченного изделия.

Анализ известных подходов к моделированию воздействия ЭМП на работоспособность ИМС показывает, что при расчете удобнее разбивать модель на составные части: ядро, корпус, цепи питания и входные/выходные цепи. На основе более простых моделей была создана методика для расчетной оценки восприимчивости ИМС к ЭМП. При расчетах удобно использовать фрагменты моделей электромагнитного излучения (ИСЕМ) той же микросхемы. В основе этого довода лежит принцип взаимности, который применительно к ИМС заключается в том, что наибольшая восприимчивость микросхем к воздействию ЭМП наблюдается на частотах с максимальными уровнями паразитных излучений. Для описания входных/выходных цепей используются IBIS модели. Для контроля сбоя необходима функциональная модель, а также некоторый критерий сбоя, который зависит от конкретного приложения. Таким образом, нет необходимости в подробных данных о внутренней структуре микросхемы, что позволяет рассматривать ее как черный ящик.

По описанной выше методике проведен расчет восприимчивости микросхемы КР1533ЛАЗ к воздействию ЭМП. Выделена модель входных/выходных цепей, построенная на основе IBIS модели, модель цепи питания, построенная по описанным в стандартах методикам, функциональная модель, которая представляет собой таблицу истинности и модель испытательной установки, которая построена согласно условиям эксперимента. При проведении расчетов было замечено, что подтверждаются общие тенденции, выявленные при различных исследованиях: устойчивость к помехам увеличивается с ростом частоты ЭМП. В целом расчетные данные для ИМС КР1533ЛАЗ хорошо согласуются с данными проведенных ранее экспериментов.

GENERAL DATA PROTECTION REGULATION И ПРОЕКТ ЗАКОНА РЕСПУБЛИКИ БЕЛАРУСЬ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

К.И. Тишук, А.М. Прудник

General Data Protection Regulation [1] уже вступил в действие с 25 мая 2018 г., а в нашей стране в настоящее время рассматривается закон Республики Беларусь «О персональных данных» [2]. Согласно GDPR, персональными данными (ПД) является любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. В свою очередь, идентифицируемое физическое лицо определено как лицо, которое может быть идентифицировано прямо или косвенно с использованием идентификатора, например: имени, идентификационного номера, данных о его местоположении, онлайн-идентификатора, или использованием параметров, характеризующих лицо с физиологической, генетической, психологической, экономической, культурной или социальной точек зрения. Под обработкой ПД понимается любая операция или набор операций, выполняемых с ПД или набором ПД