случайные числа относительной небольшой длины, предназначенные для использования в качестве ключей шифрования. От надежности ключа зависит надежность всей криптографической системы. В связи с этим имеется потребность в оценке статистических свойств каждого ключа. Целью данной работы является разработка методики тестирования последовательностей ключей.

Предлагается методика тестирования ключевых последовательностей, включающая следующие этапы:

1. Проверка статистических свойств совокупности ключей для выявления возможных зависимостей между ключами, которые позволили бы прогнозировать появление одних ключей с большей вероятностью, чем других.

2. Проверка статистических свойств каждого ключа для исключения использования слабых ключей.

Для указанных проверок используется две группы тестов. Первая группа содержит 15 тестов и предназначена для тестирования битовой последовательности, сформированной из всех сгенерированных ключей. Вторая группа содержит 7 тестов для исследования каждого ключа и характеризуется тем, что все тесты группы требуют длины последовательности от 100 бит.

По предложенной методике проведено тестирование последовательности 4492 ключей длиной 256 бит, полученной из ЭПК. Сформированная из ключей последовательность длиной 1149952 бит прошла все тесты первой группы. Все тесты второй группы прошли 4277 ключей, которые могут быть использованы в системах защиты информации.

ИССЛЕДОВАНИЕ ЖИВУЧЕСТИ ПАССИВНЫХ ОПТИЧЕСКИХ СЕТЕЙ ДОСТУПА PON

В.И. КИРИЛЛОВ, Е.А. КОВРИГА

При рассмотрении различных вариантов построения пассивных оптических сетей доступа PON одним из определяющих критериев является живучесть сети, отражающая способность сети продолжать нормально функционировать после попытки злоумышленника вызвать угрозу «отказ сервиса» с помощью разрыва ребер сети PON [1]. В статье [2], где проведен анализ живучести сетей PON по показателю средней относительной длины пути, получены некорректные графики зависимости показателя живучести сети от числа оконечных устройств: для топологии «дерево» живучесть сети возрастает и стремится к 1 с ростом числа узлов. Здесь не учтены особенности сетей PON, связанные с тем, что абонентские оптические сетевые терминалы ONT не могут взаимодействовать между собой напрямую, а связываются только через оптический линейный терминал OLT. Поэтому живучесть сетей PON должна определяться как отношение числа ONT, не потерявших связь с OLT, к общему числу ONT [1].

Очевидно, что меньший урон сети PON будет нанесен при использовании топологии «звезда» или при разрыве ближайшего к ONT ребра в топологии «дерево». Наиболее критичным участком для «дерева» PON является участок от OLT до первого сплиттера. Поэтому помимо так называемых «физических» средств защиты (датчиков вибраций, специальных конструкций волоконно-оптических кабелей, затрудняющих их разделку) целесообразно применять фидерное резервирование данного участка [1].

Литература

1. *Кириллов В.И., Коврига Е.А.* // Веснік сувязі, 2014 (в печати).

2. *Саморуков А.П.* // T-COMM: Телекоммуникации и транспорт, 2013. № 8. С. 107–111.