ЛИТЕРАТУРА

1. Компьютерная безопасность на ядерных установках справочное руководство международное агентство по атомной энергии. Вена, 2012 год. Серия изданий МАГАТЭ по физической ядерной безопасности, № 17

2. Положения об общих требованиях к системам физической защиты ядерных объектов: ТКП 360-2011 (02300). – Введ. 02.01.2012 – Минск : МЧС РБ, 2012. – 47 с.

В.К.ЖЕЛЕЗНЯК[1], И.Б.БУРАЧЁНОК[1]

НАПРАВЛЕНИЯ РАЗВИТИЯ СОВРЕМЕННЫХ СИСТЕМ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ УТЕЧКИ

[1]Учреждение образования «Полоцкий государственный университет», г. Новополоцк, Республика Беларусь

Объем научных знаний стремительно обогащается, появляются новые научные направления, новые области исследований, многие из которых тесно связаны с практикой. Вникая в новые области, необходимо развивать более общие и гибкие подходы к изменяющимся условиям, снижать области неопределенности в знаниях.

Безопасности и технической защите информации (ТЗИ) сегодня принадлежит важнейшая роль в практической потребности общества. Указом президента Республики Беларусь А.Г. Лукашенко и Постановлением Совета Министров Республики Беларусь, безопасность информации и связи рассматривается как единая важная государственная задача [1-2]. Проблемные задачи по развитию микроэлектроники – микроминиатюризации элементной базы решает НАН Республики Беларусь совместно с промышленностью.

Техническая защита информации является научным направлением информатики. С развитием информатики расширяются и традиционные знания в области ТЗИ. Как наглядный пример, стремительное расширение объема научных знаний обусловили развитие волоконно-оптических линий связи, обеспечивающих высокую скорость передачи данных [3]. Следует отметить и то, что за последнее время резко повысились требования предъявляемые к системам передачи информации: увеличение скорости, расстояния, качества принимаемых сигналов, верности передачи в условиях воздействующих факторов, в первую очередь помех и наводок высокого уровня в заданных диапазонах частот. Переход на цифровую форму передачи информации обусловил потребность в разработке новых методов и способов преобразования аналоговых сигналов, оценке их качества [4]. Таким образом, касаясь передачи речевого сигнала (РС), решение перечисленных проблем с целью повышения защищенности информации по техническим каналам утечки (ТКУ) является актуальной научной задачей.

Перечисленные проблемы необходимо решать объединением усилий коллективов ряда научных организаций, в том числе и вузов, предназначенных вести подготовку новых научных кадров по передовым технологиям и новым научным направлениям, так как их решение влияет в первую очередь на развитие связи и обороноспособности страны. Развитие новых научных направлений оказывает огромное влияние и на повышение уровня защищенности информации по ТКУ, в первую очередь речевой, видео- и передачи данных.

Речевой сигнал и частично видеосигналы являются биологическими. Первый формируется и воспринимается человеком. Прямое и обратное преобразование Фурье такого сигнала позволяет обеспечить согласование с цифровым каналом передачи, решая вопросы повышения качества приема и исключая помехи линий передачи, особенно при передаче на большие расстояния. Верность передачи такого сигнала – безусловное требование, которое оценивается вероятностью ошибочного приема бита. Предложенная математическая модель, устанавливает однозначную зависимость коэффициента разборчивости речи (разборчивости речи) с численным значением величины вероятности ошибочного приема бита.

Видеоинформация воспринимается органами зрения человека из окружающей среды. Аналогично зрительным анализатором воспринимается и информация, сформированная техническими средствами передачи информации. Помехоустойчивость и помехозащищенность первичных преобразователей приемопреобразовательных устройств и помехозащищенность

устройств передачи информации в условиях воздействующих шумов реализуют через схемно-конструктивные решения технических средств передачи данных [5].

Разработанная первоначально в Советском Союзе система измерительная автоматизированная К6-6 для оценки защищенности речевой информации в речевом диапазоне частот 100 Гц–10 кГц и на ее базе пакет нормативных документов АРР-200 представляла собой высокопроизводительную локальную измерительную систему. Результаты оценки защищенности представлялись в виде энергетического показателя (отношение мощности сигнала к мощности шума $\frac{P_{\text{с}}}{P_{\text{ш}}}$) практически в реальном масштабе времени. Измерительным сигналом (ИС) являлся высокоточный гармонический сигнал, формируемый в полосах равной разборчивости РС [6]. Производительность таких систем в 200 раз выше по сравнению с неавтоматизированными системами, основанными на использовании измерительной аппаратуры широкого применения. В данных системах для измерений использовался информационный показатель – словесная разборчивость речи [6].

Наряду с такими параметрами как: чувствительность, разрешающая способность по частоте и минимизация времени обработки ИС, необходимо максимально исключить искажения передаваемых сигналов, возникающие в результате наводок активных шумовых маскирующих сигналов. В настоящее время широко используется компенсационный метод подавления сигналов в ТКУ речевой информации. Остаточные сигналы подавляются генератором маскирующего шума, пик-фактор которого соответствуют пик-фактору РС. В этой связи важно отметить, что для оценки защищенности РС предложен сложный ИС в полосах равной разборчивости, имеющий преимущество перед гармоническим ИС в полосах равной разборчивости Обобщенная селективность такого сигнала $2\Delta f T_{\text{с}}$, где $2\Delta f$ – ширина полосы частот, а $T_{\text{с}}$ – его длительность [7].

Разнообразная по целевому назначению аппаратура (прием, передача, хранение и обработка речевой информации) имеет в большинстве случаев стандартизированные измерительные параметры. Однако эти параметры не позволяют произвести сравнительную оценку из-за отсутствия единого критерия при пороговых и максимальных предельных значениях. Это обусловливает необходимость проводить оценку параметров защиты информации на многомерных объектах (в двух- и трехмерной системе координат) с введением временной координаты, так как в ряде случаев время является крайне ограниченным по величине параметром.

Преобразование Фурье аналогового РС в цифровую форму и его обратное преобразование обусловливает возникновение дополнительных каналов утечки информации. Для решения данной проблемы важно обосновать модель ИС, преобразованного в цифровую форму и пригодного как для канала передачи информации, так и для каналов утечки информации. Следовательно, ИС должен обладать универсальностью.

Одним из наиболее важных средств современного анализа являются корреляционно-регрессионные исследования тесноты связи и линейности процесса между источниками излучений информационных полей рассеивания методами парной и множественной корреляции. Это позволяет исключить избыточные связи для повышения устойчивости систем и снижение уровня паразитных излучений.

Таким образом, значительные достижения по защите РС в ТКУ ставят новые актуальные задачи, позволяющие обосновать единую теорию оценки защищенности речевых информационных каналов утечки для внедрения в практику.

ЛИТЕРАТУРА

1. Постановление Совета Министров РБ 10 февраля 2000 Г. №186 «О некоторых мерах по защите информации в Республике Беларусь».

2. Указ Президента Республики Беларусь от 09.11.2010 г. №575 «Об утверждении Концепции национальной безопасности Республики Беларусь».

3. Зеневич, А.О. Обнаружители утечки информации из оптического волокна / А.О. Зеневич. – Минск: Белорусская государственная академия связи, 2017. – 144 с.

4. Защищенные радиосистемы цифровой передачи информации / П.Н. Сердюков, А.В. Бельчиков, А.Е. Дронов [и др.] – М.: АСТ, 2006. – 403 с.

5. Харкевич, А.А. Борьба с помехами. / А.А. Харкевич. – М.: Гос. изд-во физ.-мат. лит., 1965, 276 с.

6. Железняк, В. К. Защита информации от утечки по техническим каналам: учеб. пособие / В. К. Железняк. – СПб.: ГУАП, 2006. – 188 с.

7. Железняк, В. К. Оценка нормативного показателя защищённости речевого сигнала сложным сигналом с большой базой / В. К. Железняк, И. Б. Бурачёнок // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. – 2015. – № 12. – С. 10–14.

С.А.ГНАТЮК[1], Т.А.ЖМУРКО[1], В.Н.КИНЗЕРЯВЫЙ[1], Х.И.ЮБУЗОВА[2]

СТАТИСТИЧЕСКОЕ ТЕСТИРОВАНИЕ ТРОИЧНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ПРИМЕНЕНИЯ В ТРИТОВЫХ ПРОТОКОЛАХ КВАНТОВОЙ КРИПТОГРАФИИ

[1]*Национальный авиационный университет, г. Киев, Украина*
[2]*Satbayev University, г. Алматы, Казахстан*

Как и все направления науки, заставляющие ученых спорить об их целесообразности, преимуществах и недостатках, квантовая криптография (КК) исследуется многими научными центрами и университетами, в результате чего появляются новые и усовершенствованные протоколы, обеспечиваются сохранение информации, основываясь на незыблемых постулатах квантовой физики, и в своем большинстве достигают теоретико-информационной стойкости. Тем не менее, остается нерешенным ряд задач. Одной из важных задач является повышение информационной емкости протоколов КК, что в некоторых случаях происходит за счет использования многоуровневых квантовых систем (кудитов). Учитывая удельную натуральнологарифмическую плотность записи информации, которая описывается функцией $Y(\mathrm{a}) = \frac{\ln y(\mathrm{a})}{a} = \frac{\ln a}{a}$, где a – основание системы исчисления, следует, что наибольшую плотность записи информации имеет система исчисления с основой равной основе натуральных логарифмов (e=2,718), а среди целочисленных – это троичная система, в случае квантовых систем – это трехуровневая квантовая система (кутрит). Авторами ранее предложено метод повышение эффективности квантовых протоколов [1], который использует именно троичные псевдослучайные последовательности (ПСП).

Как известно, для криптографических приложений статистические свойства сгенерированных ПСП не должны отличаться от случайных последовательностей. Для определения этих свойств используют ряд методик статистического тестирования, в частности методики NIST STS, FIPS 140-2, Д. Кнута, Горбенко-Потия, системы DIEHARD Дж. Марсалья, CRYPT-S X. Густавсона и др. Однако все они ориентированы на оценку бинарных ПСП. В связи с этим, *целью работы* является обоснование метода оценивания качества троичных ПСП.

В [2] авторами предложен метод оценивания, что дает возможность определять статистические параметры и закономерности тритовых ПСП, представленный на рис. 1.

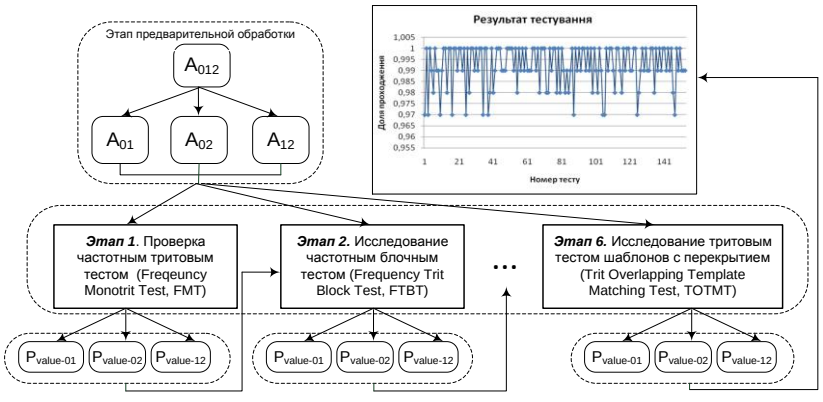

Рисунок 1 – Схематическое представление метода оценивания качества ПСП

Рассмотрим один из этапов, а именно ***тест на совпадение с шаблоном без перекрытия***. Внимание теста сосредоточено на том, какое количество раз встречается заранее заданная строка во входящей последовательности. *Цель теста* – выявить генератор, который формирует последовательность, содержащую очень большое количество заданного апериодического шаблона. В этом тесте для поиска заданного m-тритного шаблона используется m-тритное окно. Окно сдвигается вправо на один трит,