– СТБ ISO/IEC 27000-2012 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь;

– СТБ ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

Законом Республики Беларусь «Об информации, информатизации и защите информации» определено, что защита информации — это комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации. Из приведенных пяти свойств информации в законе дается определение только термину «конфиденциальность» — требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь. Определения остальных указанных свойств информации в законе не приводятся.

В СТБ ISO/IEC 27000-2012 определение термина «защита информации» отсутствует, а используется только понятие информационная безопасность (information security) — сохранение конфиденциальности, целостности и доступности информации. Стандартом допускается возможность включения требования сохранения других свойств информации, таких как подотчетность, неотказуемость, достоверность. В нем приводятся определения всех указанных свойств информации.

В СТБ ГОСТ Р 50922-2006 определено, что безопасность информации (information security) — это состояние защищенности информации при которой обеспечены ее конфиденциальность, доступность и целостность. В стандарте дается определение защиты информации как деятельности, направленной на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Приводятся определения свойств информации.

На основании проведенного анализа можно сделать вывод, что действующие в нашей стране НТПА не дают однозначных определений базовых терминов, используемых в области защиты информации, а в некоторых случаях вступают в противоречия между собой.

Таким образом, с точки зрения законодательства Республики Беларусь корректнее говорить не о системе информационной безопасности (СИБ), а о системе защиты информации (СЗИ) как комплексе правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

АЛГОРИТМЫ БЫСТРОГО ПРЕОБРАЗОВАНИЯ УОЛША

А.А. Будько, Т.Н. Дворникова

Функции Уолша находят применение в различных областях передачи и обработки информации. Преобразование Уолша осуществляется с помощью быстрых алгоритмов.

К настоящему времени имеется определенное количество таких алгоритмов, которые получены в основном используя факторизации матриц Уолша в различных упорядочений. Возможное количество алгоритмов быстрого преобразования Уолша очень велико. Однако они не равноценны. При рассмотрении алгоритмов быстрого преобразования Уолша выделяются так называемые «замечательные» алгоритмы быстрого преобразования Уолша.

В докладе рассматривается метод получения алгоритмов быстрого преобразования Уолша основанный на представлении элементов матриц Уолша в экспоненциальной или показательной форме. Получено два новых алгоритма в системе упорядочения Уолша-Пэлли, которые как и полученные ранее алгоритмы Кули-Туки, Сэнди, Кроузера-Радера-Рошфора, Андрюса-Кейна относятся к «замечательным» алгоритмам. Эти алгоритмы быстрого преобразования Уолша обладают свойствами симметрии, их граф для любой размерности может быть легко получен. Все алгоритмы быстрого преобразования Уолша требуют одинаковое количество арифметических операций, однако решение об использовании для конкретного применения того или иного алгоритма принимается на основе сравнения. Известно, что алгоритмы Кули-Туки и Сэнди не требуют дополнительной памяти, поскольку вычисления осуществляются на местах. В то время алгоритм Кроузера-Радера-Рошфора не позволяет осуществить вычисления на местах и требует дополнительной памяти. Однако граф быстрого преобразования Уолша (алгоритм Гротера-Рейдера) имеет все одинаковые итерации, что дает определенное преимущество при осуществлении вычислений мгновенного спектра по Уолшу.

Полученные два варианта алгоритма быстрого преобразования Уолша в системе упорядочений Уолша-Пэлли являются симметричными и относятся к «замечательным». А рассмотренный метод извлечения алгоритмов быстрого преобразования Уолша может быть использован в различных системах упорядочений.

Литература

1. *Трахтман А.М., Трахтман В.А.* Основы теории дискретных сигналов на конечных интервалах. М., «Сов. Радио», 1975.

2. *C. Yen.* Walsh functions and Gray code. IEEE Transactions, 1971, EMC 13, N 3.

ПРИМЕНЕНИЕ М-ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ СКРЫТНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ. ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ

Д.Н. Буйновский

Проведен обзор М-последовательностей, а также проанализированы перспективы их использования при передаче информации. В наше время, а также в будущем, данные методы кажутся наиболее перспективными при использовании в технологиях беспроводной передачи данных, хотя, безусловно, их можно использовать для любой среды передачи. Применение М-последовательностей позволяет снизить влияние помех в среде передачи, а также скрытно передавать любую информацию.

М-последовательность — бинарная последовательность импульсов определенной длины, характеризуемая рядом свойств, из которых основные, это то что автокорреляционная функция ее, измеренная на конечный интервал времени, представляет собой один узкий треугольник [2].

Одной из интересных возможностей, которой обладают М-последовательности - является скрытная передача информации, путем передачи через общий канал связи шумоподобного сигнала (ШС), на основе М-последовательности.

В системах с ШС обеспечивается скрытность передачи, если код, определяющий форму ШС, известен только своему корреспонденту, а база ШС выбрана такой величины, при которой уровень полезного сигнала меньше уровня флуктуационного шума, возникающего во входных цепях приемника.

М-последовательности, хоть и в разы повышает объем данных, необходимый для передачи сообщения, и снижается скорость передачи сообщения, существенно повышается вероятность успешного его декодирования.

Таким образом, применение М-последовательностей в современных широкополосных системах передачи позволит улучшить качество передачи потоковых данных (голос и видео).

М-последовательности возможно использовать в системах IP телефонии. В первую очередь, как дополнительные меры, для передачи голоса и видео по нестабильным каналам связи.

Литература

1. М-последовательность [Электронный ресурс] — Режим доступа: http://dic.academic.ru/dic.nsf/ruwiki/95625

2. *Клюев Л.Л.* Теория электрической связи. Минск, 2016.

3. М-последовательность [Электронный ресурс] — Режим доступа: https://ru.wikipedia.org/wiki

ШИФРОВАНИЕ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ (NGE)

Д.Н. Буйновский

Проведен обзор нового направления в области криптографии: шифрование следующего поколения. В наше время, а также в будущем, данные методы кажутся наиболее перспективными, так как одиночное использование ни одного из существующих алгоритмов не сможет обеспечить сохранность конфиденциальных данных.

За последние годы, было разработано и использовано множество криптографических алгоритмов во множестве различных протоколов и функций. Однако, криптография не является статической. Устойчивый прогресс в науке и вычислительной технике привели к необходимости использования новых, более безопасных алгоритмов и ключей большего размера. Данная работа посвящена анализу современных методов защиты от угроз информационной безопасности, так называемым методам шифрования нового поколения.

Next generation encryption — новая ветвь развития в области защиты данных. Совершенствование методов анализа данных, прогресс в технике, а также найденные уязвимости