Система радиосвязи в тоннельных сооружениях реализуется не только посредствам радиомодемов, но и с применением излучающего кабеля, проложенного по всей длине тоннельного сооружения.

Система связи с применением излучающего кабеля позволит обеспечить все потребности в радиосвязи технического персонала и пожарно-спасательных служб, использующих свои стандартные радиосредства, с ближайшей базовой радиостанцией, так как если бы они находились на открытом пространстве.

Излучающий кабель используется в качестве протяженной антенны для обеспечения радиосвязи в тоннельных сооружениях. Кабели такого типа могут крепиться непосредственно на стены при помощи недорогих универсальных аксессуаров.

ШИФРОВАНИЕ ТЕЛЕВИЗИОННОГО СИГНАЛА МЕТОДОМ ПЕРЕСТАНОВКИ

А.И. НЕКОЗЫРЕВ

Цель работы: разработка метода шифрования телевизионного сигнала. В данной работе оценена актуальность темы для нужд народного хозяйства и военно-промышленного комплекса. Проведен обзор наиболее широко применяемых в коммерческих целях систем и рассмотрены их проблемные стороны. В том числе систем Irdeto/Luscrypt, Discret, Videocrypt, Nagravision, Syster, Videocipher II. Рассмотрены возможности шифрования телевизионного сигнала методом гаммирования и методом замены. Обоснован выбор метода перестановки, описан процесс шифрования этим методом. Предложен вариант технической реализации данного метода шифрования телевизионного сигнала.

ПРОСТОЙ АЛГОРИТМ ШИФРОВАНИЯ ЦИФРОВЫХ ПОТОКОВ

В.Н. СЮРИН, П.В. КЛЮЧЕРОВ, В.И. ЦИДИК

При обмене конфиденциальными данными по телекоммуникациям с высокой скоростью возникает необходимость их шифрования в реальном времени. В данной работе разработан и программно реализован алгоритм шифрования различных типов данных с высокой скоростью на основе элементарной перестановки двух битов в каждом байте данных на основе заранее сформированного секретного ключа. В зависимости от требуемого уровня защиты, длина ключа может меняться в широких пределах. Каждый байт данных в блоке при этом шифруется своим субключом.

Для оценки ряда характеристик различных методов шифрования и их сравнения разработана специальная методика и соответствующие программные коды с использованием некоторых стандартных инструментов.

Ряд проведенных машинных экспериментов наглядно показал работоспособность алгоритма и высокие показатели качества.

ШИФРОВАНИЕ АРХИВИРОВАННЫХ ФАЙЛОВ

В.Н. СЮРИН, О.Р. МЫСЛИВЕЦ, Е.А. ДУБАТОВКА

Целью архивирования файлов является сокращение избыточности данных, при этом их энтропия должна стремиться к предельному максимальному значению $\log_2 m$, где m — объём алфавита используемых символов. Практически ту же задачу решают криптографические преобразования (шифрование). В этом случае к энтропии исходного материала добавляется энтропия, внесенная собственно алгоритмом шифрования, при этом конечное её значение также стремится к вышеуказанному значению. В данной работе разработан алгоритм и программные коды шифрования архивированных файлов, заключающихся в модификации (изменении) заголовка архива путём простого преобразования XOR в соответствии с выбранным секретным ключом. Сравнительный анализ криптоустойчивости

разработанного алгоритма и широко известного стандарта AES показал практически одинаковые результаты.

Таким образом, предложенное преобразование при своей чрезвычайной простоте обеспечивает достаточную криптоустойчивость с одновременным уменьшением объёма данных.

ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ X-КОДА: ТЕОРИЯ И ПРАКТИКА

Е.Н. ЛИВАК, О.Р. МЫСЛИВЕЦ

Изучены и систематизированы способы и механизмы внедрения произвольного кода в исполняемые файлы в формате Portable Executable. Целью исследования является определение применимости методов на практике в недеструктивных целях. Одной из основных проблем внедрения X-кода является работа «зараженного» исполняемого файла совместно с антивирусными средствами.

Проектирование X-кода включает решение следующих основных задач: размещение кода внутри файла-контейнера, перехват управления до начала выполнения основных функций, определение адресов API-функций, необходимых для функционирования файла-контейнера.

Проанализированы и практически проверены механизмы, которые не вызывают изменения адресации ни физического, ни виртуального образов; вызывающие изменения адресации только физического образа; вызывающие изменения адресации как физического, так и виртуального образов, а также механизмы внедрения кода в адресное пространство файла-контейнера косвенным путем.

Полученные в результате исследования выводы и практические рекомендации представлены в докладе.

КОРРЕЛЯЦИОННЫЕ СВОЙСТВА КРИПТОАЛГОРИТМА RIJNDAEL

М.В. МУЗЫЧЕНКО, А.В. МАРТИНОВИЧ, Д.М. БИЛЬДЮК

В системах связи, сбора и передачи информации широкое распространение получили методы расширения спектра сигналов. Одним из эффективных методов расширения спектра, при котором сигнал-переносчик информации занимает широкую полосу частот, является метод непосредственной модуляции несущей псевдослучайной последовательностью. При этом методе расширение спектра дополнительная модуляция несущей сигнала никак не связана с передаваемой информацией.

В данной работе были исследованы корреляционные свойства: М-последовательности, ЧКП, коды Касами, криптоалгоритм Rijndael.

Самая лучшая апериодическая АКФ найдена у М-последовательности, а периодическая АКФ — у ЧКП (в районе порога нет шума).

В процессе исследования было выяснено, что криптоалгоритм Rijndael совпадает с корреляционными функциями по боковым лепесткам по случайным последовательностям. Хоть Rijndael и имеет большой недостаток — высокий уровень боковых лепестков, но он имеет большие преимущества, которые не имеют другие последовательности. А именно: за счет криптографических свойств у него произвольная длина, обладает высокой структурной скрытностью.