ИСПОЛЬЗОВАНИЕ ЭЛЕМЕНТОВ ВЕБ-СЕРВИСОВ AMAZON ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНТЕРНЕТ-ПРИЛОЖЕНИЙ

П.В. ШЕЛЕСТОВИЧ

С ростом количества и популярности публичных интернет сервисов, приложений и социальных сетей все острее встает вопрос обеспечения безопасности данных пользователей и их постоянной доступности. Например, личные данные профиля и важная конфиденциальная информация, хранящаяся посредством облачных сервисов, должна быть доступна из любого места и устройства, поддерживающего соединение с интернетом и, при этом, быть надежно защищенной от злоумышленников.

Обеспечение полноценной инфраструктуры для защиты содержимого своего интернет приложения — это длительный и дорогостоящий процесс, требующий усилий и опыта зачастую гораздо более затратных, чем реализация основного функционала предоставляемого сервиса. Были проведены исследования по обеспечению безопасности с помощью облачных веб-сервисов. Наилучшие результаты по простоте использования, надежности, доступности и стоимости услуг показали элементы веб-сервисов от Amazon. Задача безопасности там целиком ложится на поставщика облачной инфраструктуры. Создание условий для функционирования средств защиты информации в первую очередь подразумевает формирование доверенной среды. Этот процесс происходит автоматически и полностью лишен возможности ошибок человеческого фактора. Внутри доверенной среды такие сервисы защиты информации, как подпись, аутентификация, идентификация и другие, также становятся облачными сервисами, доступными всем доверенным пользователям на общих основаниях. Перенос основных сервисов защиты информации в облачную среду снимает с участника сложную инфраструктурную часть средств защиты информации и передает ее в руки лучшим специалистам по безопасности интернет приложений в мире, которые удаленно следят за их работоспособностью.

Полученные результаты исследований показывают целесообразность и приоритетность использования веб-сервисов Amazon для обеспечения безопасности данных. Такой способ защиты информации идеально подходит для небольших и средних интернет приложений и проектов.

ВАРИАНТЫ ПОСТРОЕНИЯ КОРПОРАТИВНОЙ СИСТЕМЫ РАДИОСВЯЗИ В УСЛОВИЯХ ПОДЗЕМНОЙ ЭКСПЛУАТАЦИИ

Д.В. ШУЛЯК

Корпоративная система радиосвязи предназначена для обеспечения производственной деятельности организаций, управления технологическими процессами в производстве. Корпоративные радиосети обмена данными создаются для решения комплекса функциональных задач, связанных с организацией мониторинга состояния (сбора данных о техническом и/или оперативном состоянии), оперативно-диспетчерского управления и информационного обеспечения в условиях, когда использование других средств связи невозможно или нецелесообразно.

Современные программно-технические средства позволяют создавать относительно недорогие, эффективные и гибкие радиосети обмена данными, способные функционировать на протяжении многих лет с минимальным техническим обслуживанием.

Наиболее высокая надежность работы достигается в системах, в которых обеспечивается прямая радиовидимость между объектами. Однако в условиях подземной эксплуатации обеспечить прямую видимость на расстояниях 100–200 м крайне сложно. Также не следует забывать, что среда распространения в стволе шахты имеет повышенную концентрацию соляной пыли и повышенную влажность, что вызывает сильное поглощение энергии электромагнитного поля.

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