ПРЕДЛОЖЕНИЯ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Л.Л. УТИН, В.Н. КОРДЕЛЮК

В настоящее время в Республике Беларусь разрабатывается система межведомственного электронного документооборота государственных органов с использованием средств электронной цифровой подписи. Такая система позволяет в кратчайшие сроки передавать электронные документы (информацию), имеющие равную юридическую силу с документами на бумажных носителях, что сокращает затрачиваемое время на согласование различного уровня документов и количество бумажного документооборота. Однако, данная система предназначена только для обмена открытыми данными.

По аналогии с указанной системой целесообразно создание национальной системы защищенного электронного документооборота. Учитывая, что к такой системе предъявляются повышенные требования к конфиденциальности, целостности, доступности, подлинности и сохранности информации основные ее элементы должны быть сертифицированы установленным порядком. Вместе с тем, на сегодняшний день отсутствуют подходы к синтезу подобных систем.

В докладе предлагается к обсуждению основные подходы к обеспечению информационной безопасности при построении данной системы. В частности, для обеспечения конфиденциальности и сохранности предлагается использовать IP-шифраторы, а для обеспечения целостности и подлинности — средства электронной цифровой подписи.

Применение данных средств позволит снизить нагрузку на фельдъегерско-почтовую связь, ускорить информационный обмен, что в совокупности повысит оперативность принятия решений органами государственного управления. Что особенно актуально в период нарастания военной угрозы.

ПОСТРОЕНИЕ МНОГОУРОВНЕВОЙ СИСТЕМЫ ЗАЩИТЫ БЕСПРОВОДНОЙ МОБИЛЬНОЙ ЯЧЕИСТОЙ СЕТИ С УЧЕТОМ ГИБРИДНОЙ ЭТАЛОННОЙ МОДЕЛИ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ

А.А. ЮРЕВИЧ, А.Г. ШЕРЕМЕТ

Мобильные ячеистые сети строятся на основе беспроводных одноранговых сетей Ad-Hoc, что делает их уязвимыми. Поэтому для построения опорной части беспроводной ячеистой сети (БЯС) необходимо задействовать доступные средства сетевой защиты каждого ее узла. Проведен анализ средств безопасности всех уровней (физического, передачи данных, сетевого, транспортного, прикладного) гибридной модели взаимодействия открытых систем. На физическом уровне для противодействия средствам радиоэлектронной борьбы предлагается использовать смарт-антенны, на уровне передачи данных — протоколы с шифрованием, например WEP в сетях Wi-Fi. На сетевом уровне следует использовать протокол IPv6, содержащий элементы повышения сетевой безопасности. Протоколы маршрутизации для опорной сети, работающие на уровне передачи данных или сетевом должны содержать средства проверки подлинности, целостности обновлений и их шифрование. В случае необходимости для важной части трафика следует задействовать VPN на основе IPSec. Защита на транспортном уровне возможна за счет протоколов TLS/SSL или решений на их основе (OpenVPN, SSH и др.). На уровне приложений безопасность обеспечивается использованием защищенных версий программного обеспечения на маршрутизаторах и/или компьютерах пользователей сети. Некоторые элементы повышения уровня сетевой безопасности, например, VPN с

шифрованием данных, негативно влияют на характеристики сети: время задержки, полезную пропускную способность, время конвергенции и другие. Поэтому важно правильно выбрать необходимые и достаточные средства защиты для конкретной сети.

МОДЕЛЬ НЕРАВНОМЕРНОГО КРИПТОГРАФИЧЕСКОГО КОДИРОВАНИЯ МНОГОРАКУРСНЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ МАТРИЦЫ ПЕРЕКРЫТИЯ

В.Ю. ЦВЕТКОВ, К.С.Ш. АЛЬ-САФФАР, А.Д.К. АЛЬ-ГЕЙЗИ, М.Д.А. АЛЬ-ДЖЕБНАВЕ

Развитие систем передачи многоракурсных изображений, формируемых камерами, установленными на подвижных объектах, требует разработки соответствующих систем защиты. В связи с большим объемом видеоинформации, формируемой и передаваемой в таких системах, актуальной задачей является использование для ее защиты неравномерного криптографического кодирования, выбирающего сложность шифра с учетом важности защищаемой информации. Для решения данной задачи предлагается использовать модель неравномерного криптографического кодирования многоракурсных изображений на основе матрицы перекрытия. Элементами матрицы перекрытия являются фрагменты многоракурсного изображения, относящиеся к определенному ракурсу — оригинальные (главная диагональ), и фрагменты, присутствующие в разных ракурсах — перекрывающиеся (остальные элементы). Элементы главной диагонали сжимаются и передаются независимо друг от друга. Они должны шифроваться наиболее стойким шифром. Остальные элементы являются избыточными. Их сжатие основано на компенсации движения, что предполагает формирование опорных изображений и использование их для предсказания остальных. Из-за перекрытия опорные изображения могут быть равномерно распределены по различным ракурсам и переданы по различным каналам, что усложняет процедуру несанкционированного доступа к ним. В этой связи для шифрования опорных изображений может использоваться менее стойкий шифр по сравнению с оригинальными. Несовершенство методов предсказания приводит к различию прогнозируемых и прогнозных изображений, что требует передачи ошибки предсказания для каждого ракурса. Данная видеоинформация имеет, как правило, малый динамический диапазон и может кодироваться наименее стойким шифром.

СКРЫТНАЯ ПЕРЕДАЧА ДАННЫХ В ИЗОБРАЖЕНИЯХ С ИСПОЛЬЗОВАНИЕМ МАНИПУЛЯЦИИ РАЗМЕРАМИ СЕГМЕНТОВ

В.Ю. ЦВЕТКОВ, О.М. АЛЬМИЯХИ, В.К. КОНОПЕЛЬКО

Предлагается метод скрытной передачи данных в изображениях на основе манипуляции доминирующим размером сегментов. Сущность метода состоит в изменении наиболее часто встречающегося на изображении размера сегментов в соответствии со значениями бит скрываемого сообщения. Алгоритм реализации данного метода состоит из следующих шагов: сегментация изображения; построение гистограммы размеров сегментов; определение локальных экстремумов гистограммы; определение правого доминирующего локального экстремума гистограммы; нормализация гистограммы вблизи локального экстремума (выравнивание размеров сегментов, близких к доминирующему размеру); локализация сегментов доминирующего размера; согласование объема скрываемых данных с числом локализованных сегментов; определение порядка выборки сегментов для манипуляции; манипуляция размеров сегментов в соответствии со значениями бит скрываемого сообщения. Для исключения необходимости последующей обработки границ сегментов, размеры которых в результате манипуляции уменьшаются, предлагается использовать только увеличение размеров сегментов при сокрытии единичных бит данных и сохранение размеров при сокрытии нулевых бит данных.