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