УДК 004.75

А.В. НЕЙВАНОВ, А.Н. РОХМАИЛ, С.А. ГОЛОВАШИЧ

ООО «Криптомаш», Украина

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЁННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Статья посвящается рассмотрению подходов к решению вопросов обеспечения информационной безопасности в распределённых вычислительных сетях. Рассмотрены три подхода построения виртуальных частных сетей ориентированные для различных условий применения.

локальные вычислительные сети, техническая защита информации, аппаратные модули, программные модули, аппаратно-программные решения

Введение

На данный момент времени активно развиваются сетевые технологии, на рынке появляется новое коммуникационное оборудование, растут и масштабируются локальные вычислительные сети (ЛВС). Для конечного пользователя персонального компьютера (ПК) не составляет проблемы обзавестись коммуникационным оборудованием и своей собственной локальной сетью. Также мы можем наблюдать активный рост сетей предприятий среднего и крупного бизнеса. Активно развиваются каналы связи компаний предоставляющих услуги Интернет, так называемых Интернет-провайдеров. С ростом сетей и каналов связи как локальных, так и глобальных всё более актуальной становится проблема защиты информации (ЗИ) циркулирующей в ней и подвергающейся обработке. Обостряется необходимость в обеспечении таких базовых услуг защиты информации как конфиденциальность, аутентификация, целостность, контроль доступа, причастность.

На коммерческий рынок стали с большой активностью выходить фирмы предоставляющие услуги по разработке, внедрению и сопровождению как аппаратных и программных, так и аппаратно-программных средств защиты информации.

Что же касается разработки, внедрения и сопровождения комплексных концептуальных решений в области защиты информации [1 - 3], то эта часть рынка, по-прежнему, остаётся пустой и на данный момент всё более востребованной, поэтому целью данной статьи и является рассмотрение подходов к решению данных вопросов.

Спектр решений в области технической и криптографической защиты информации

Прежде чем говорить о решениях в области технической и криптографической защиты информации не будет лишним привести определение данных понятий. Под определением техническая защита информации (ТЗИ) следует понимать комплекс мероприятий, направленных на предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, на предупреждение преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе ее создания, хранения, обработки и передачи.

Что же касается криптографической защиты информации (КЗИ), то сам термин криптография произошёл от двух греческих слов criptos – тайна и graphos – пишу, а под данным определением следует

понимать вид защиты, что реализуется при помощи криптографического преобразования информации.

Для разработки, внедрения и сопровождения комплексных концептуальных решений в области ЗИ необходимым и достаточным есть использование как криптографической, так и технической защиты информации.

Компания ООО «Криптомаш» представляет комплексные решения по построению шифрованных каналов связи для корпоративных сетей, удаленных офисов и филиалов компаний.

Наши решения обеспечивают защиту конфиденциальной информации обрабатываемой, хранящейся и передающейся в электронном виде по различным сетям и каналам связи, использующим протоколы семейства TCP/IP. Выбирая решения для построения защищенных каналов связи, необходимо учитывать множество факторов.

Главными критериями являются: масштабируемость, интероперабельность, модернизация, показатели производительности, ценовая политика и оперативная техническая поддержка.

Наши решения представляют собой новый класс специализированных устройств, обладающих высокой производительностью и широким набором функций сетевой безопасности. К подробному рассмотрению предлагаются три варианта защищённых сетей:

1. Объединение удалённых филиалов. Объединение филиалов (рис. 1) осуществляется с помощью программно-аппаратного комплекса и позволяет создать надежный шифруемый канал связи. Решение включает в себя межсетевые экраны для повышения уровня защиты от вторжений. Является интероперабельным, позволяя взаимодействовать с различными аппаратными, программными и аппаратно-программными решениями различных производителей; масштабируемым – позволяя расширять внутренние сети посредством технологии VLAN; гибким – возможна реализация системы обнаружения атак и вторжений. Комплекс поддерживает статическую маршрутизацию и может организовать работу пользователей локальной сети, как в защищенном, так и в открытом режиме, позволяя производить обмен открытой информацией с внешними ресурсами сети Интернет.

2. Подключение мобильных станций. Подключение мобильных станций (рис. 2) позволяет реализовать взаимодействие по защищённому

3. каналу между сегментами корпоративной сети (центральным офисом или филиалами) и одиночным пользователем. При этом пользователь может использовать для подключения к корпоративным ресурсам, как домашнюю рабочую станцию, так и мобильное устройство: Cell Phone, Pocket PC, Laptop. Данный вариант отличается от первого тем, что удаленный пользователь, зачастую, не имеет статического адреса. Подключение к ресурсу осуществляется с использованием виртуального туннеля VPN. Функции туннеля для удалённого пользователя могут быть реализованы как в программном, так и в аппаратно-программном виде. Немаловажной особенностью является работа клиента из под любых операционных систем (ОС) как семейства Windows так и Unix-подобных.

4. Защищённый доступ к удалённым ресурсам. Защищённый доступ к удалённым ресурсам (рис. 3) представляет усовершенствованное объединение возможностей первого и второго варианта. Доступ осуществляется через централизованный кластер, разработанный компанией ООО «Криптомаш».

Данное решение вносит ряд весомых преимуществ:

– отказоустойчивые каналы связи и собственная оптоволоконная сеть с динамической маршрутизацией трафика;

– реализация гибкой корпоративной политики безопасности с использованием межсетевых экранов;

– мониторинг несанкционированного доступа (НСД); сокрытие внутренней структуры защищаемых сетей;

– внедрение систем обнаружения вторжений на разных уровнях;

– централизованное управление;

– круглосуточная поддержка клиентов 24/7;

– централизованный аудит всей системы в целом.

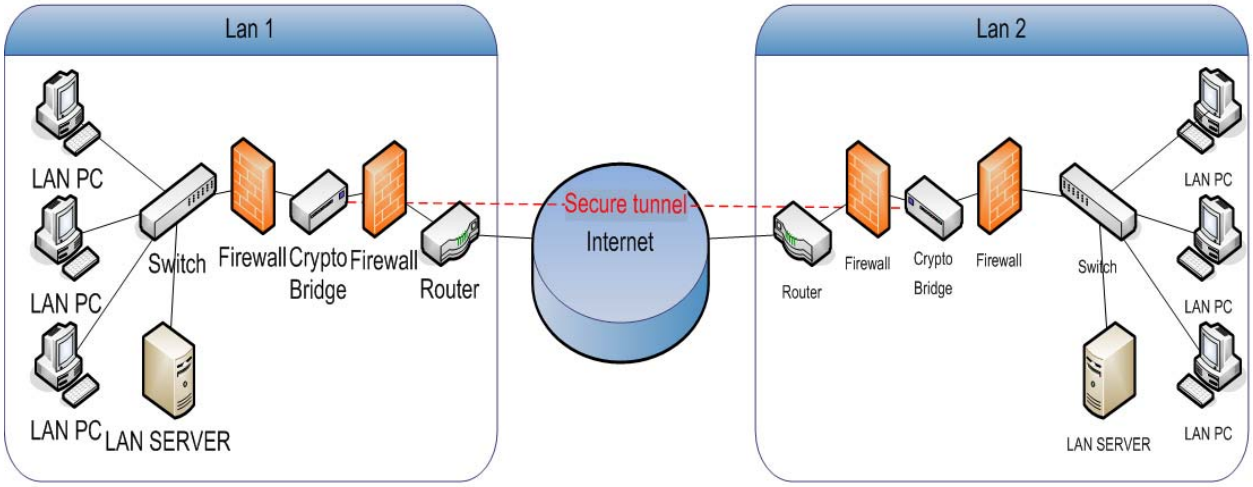

Рис. 1. Схема объединения удалённых филиалов

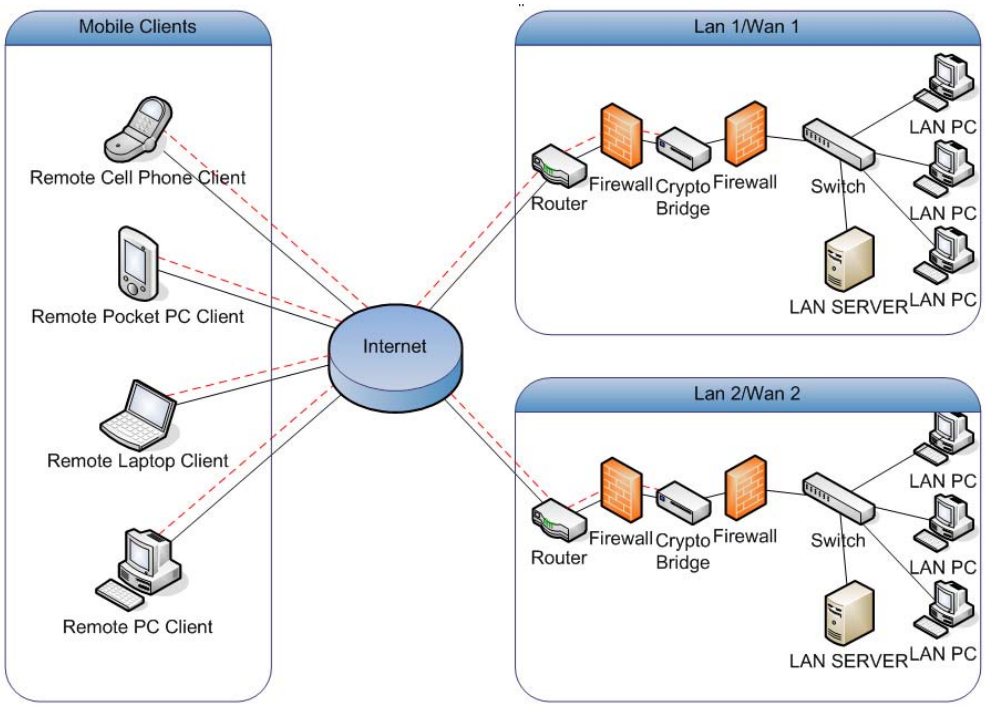

Рис. 2. Схема подключения мобильных станций

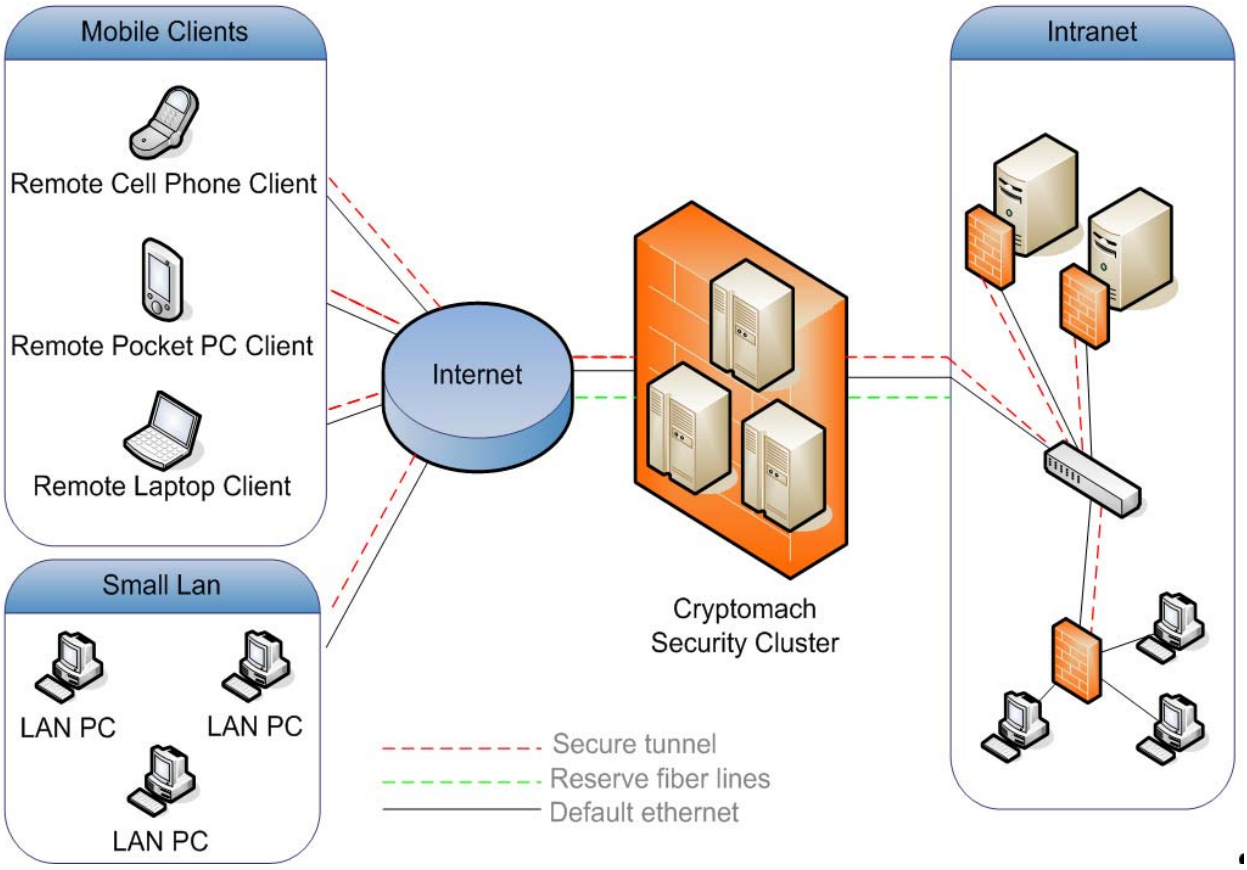

Рис. 3. Схема защищенного доступа к удалённым ресурсам

Заключение

Спектр решений, предоставленных к рассмотрению фирмой ООО «Криптомаш», представляет собой концептуальные подходы в защите криптографической и технической информации, выработанные с годами практики в данной сфере. Наша фирма с каждым днём разрабатывает и внедряет новые аппаратные и программные модули КЗИ. На их основе наши сотрудники разрабатывают и внедряют в жизнь комплексные решения по защите объектов ТЗИ.

Литература

1. ДСТУ Проект Інформаційні технології. криптографічний захист інформації. терміни та визначення.
2. НД СТЗІ ТПКО. – 1995.
3. НД СТЗІ ТР ЕОТ. – 1995.

Поступила в редакцию 16.01.2008

Рецензент: д-р техн. наук, проф. И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков.