ОЦЕНКА ВЛИЯНИЯ ПРОТОКОЛОВ VPN КАНАЛЬНОГО УРОВНЯ НА ПАРАМЕТРЫ ТРАНСПОРТНОЙ СИСТЕМЫ ИНФОКОММУНИКАЦИОННОЙ СЕТИ НА ТЕХНОЛОГИИ IP-QoS

Н.Н. Мошак, OTZI@lou.cbr.ru
СПбГУТ, Санкт-Петербург, Россия

Введение

Известно [1, 2], что помимо технологических и экономических аспектов создания ИКС, другой не менее важной проблемой в глобальном информационном обществе является обеспечение международной информационной безопасности (ИБ), так как только убытки от предпринимаемых вирусных атак на национальные информационные ресурсы в сети Интернет ежегодно составляют миллиарды долларов США. Сегодня годовой ущерб только от несанкционированного доступа (НСД) к информации, составляет сейчас около 0,5 млрд. долларов и ежегодно увеличивается в 1,5 раза. Например, ущерб, нанесенный вирусом «I love you» в 1999 году превысил 10 млрд. долларов [3]. Общий ущерб компаний от НСД к информации в 2002 году оценивается $24 млрд. (Forrest Research, 2002). В информационном обществе обеспечение международной ИБ затрагивает интересы мировой информационной безопасности. Защита национальных информационных ресурсов сегодня является одной из составных задач обеспечения информационной безопасности Российской Федерации. Национальная информационная безопасность основывается на законодательстве Российской Федерации, а также на государственных нормативно-методических документах в области ИБ (в т. ч. руководящих документах Федеральной службы безопасности и Федеральной службы по экспортному и техническому контролю). В Доктрине информационной безопасности Российской Федерации [4], утвержденной Президентом Российской Федерации 09.09.2000 года, понятие «информационная безопасность» рассматривается как одно из составляющих национальной безопасности. Информационная безопасность страны определяется как состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Доктриной так же определено, что национальные интересы России в информационной сфере включают в себя защиту информационных ресурсов от НСД, а так же обеспечение безопасности информационных и телекоммуникационных систем.

Известно, что любая система защиты вносит избыточность в информационное окружение сети и приводит к ухудшению ее вероятносто-временных характеристик (ВВХ). Становится ясным, что разработка моделей и методов расчета ВВХ защищенной транспортной системы (ТС) инфокоммуникационной сети (ИКС), позволяющих оценить влияние механизмов защиты на эффективность использования сетевых ресурсов, несомненно, является актуальной задачей [5, 6].

Данная работа посвящена оценке влияния протоколов VPN канального уровня на параметры ТС ИКС. Сравнительная оценка проводится на модели

однородного транспортного канала в режиме установленного соединения. Методики расчёта базируются на построении и оптимизации общего функционала использования пропускной способности ТС с учетом ее архитектуры [7].

Технология VPN

Использование технологии защищенных виртуальных сетей (Virtual Private Network - VPN) позволяет обеспечить криптозащиту информации в открытой сетевой среде, включая Интернет, при организации доступа пользователей к ресурсам локальной вычислительной сети (ЛВС) удаленных филиалов своих организаций и/или организации защищенных каналов связи или туннелей между защищенными ЛВС корпоративных сетей. Привлекательность технологии VPN для пользователей обусловлена низкой стоимостью услуги и практически неограниченной масштабируемостью. По данным Frost & Sullivan прогноз рынка средств VPN в 2004г. составил 18,77 млрд долларов. Однако, помимо вопросов защиты информационного обмена пользователя интересует также вопрос качества обслуживания и, в частности, вопрос: на сколько медленнее будет работать корпоративная сеть после установки VPN.

Каждый выделенный виртуальный канал VPN формируется с помощью механизмов тунелирования (инкапсуляции) базового примитива протокола логического уровня корпоративной сети в примитив защищенного протокола в компьютере пользователя или в пограничных серверах удаленного доступа (RAS) провайдера входа в открытую сеть общего пользования. VPN-агенты могут осуществлять функции шифрования/расшифрования, аутентификации, а также контроль целостности сообщения посредством электронной цифровой подписи (ЭЦП) или имитовставки (ИВ).

Как правило, VPN-агенты поддерживают несколько стандартных протоколов для организации защищенных туннелей, которые могут применяться на различных уровнях логической структуры эталонной модели архитектуры ВОС Международной организации МОС. Хотя указанные протоколы могут размещаться на всех уровнях эталонной модели, к средствам VPN относят только те, которые полностью прозрачны для сетевых служб и приложений пользователя. Это протоколы защищенных туннелей канального, сетевого и транспортного уровней. Указанные три уровня, которые в терминах модели ВОС образуют логическую структуру транспортной системы (ТС) области взаимодействия открытых систем, называют также VPN-уровнями. Логическую структуру ТС IP-сети образуют соответственно уровни TCP/UDP, IP и уровень сетевого интерфейса.

Протоколы создания защищенных виртуальных каналов на канальном уровне лучше всего подходят для защиты информационного взаимодействия при удаленном доступе корпоративной ЛВС. К протоколам формирования защищенного туннеля на канальном уровне относятся протоколы PPTP (Point-to-Point Tunneling Protocol, RFC 2637), L2F (Layer-2 Forwarding, RFC 2341) и L2TP (Layer-2 Tunneling Protocol, RFC 2661). Указанные протоколы инкапсулируют сервисные примитивы протоколов канального уровня, например, PPP (Poit-to-Point Protocol), в сервисные примитивы сетевого уровня: IP, IPX, DECnet и других. При этом, функции защиты обеспечивает только протокол PPTP [8, 9].

Протоколы PPTP и L2F позволяют провайдерам Internet проводить удаленные сеансы по протоколу PPP. Протоколы PPTP и L2F не специфицирует конкретные методы аутентификации и шифрования. Для работы провайдеров Internet с L2F необходимо, чтобы маршрутизаторы и серверы удаленного доступа поддерживали этот протокол, что не обязательно в случае использования протокола туннелирования PPTP. Здесь туннели могут формироваться в конечных точках их создания: ПЭВМ удаленного пользователя и серверах удаленного доступа ЛВС. Однако, L2F по сравнению с PPTP имеет ряд преимуществ. В отличие от протокола PPTP протокол L2F позволяет использовать для удаленного доступа к провайдеру Интернет не только протокол PPP, но и другие протоколы, например, SLIP. Кроме того, L2F не привязан к конкретным протоколам сетевого уровня, используемых для транспортировки PPP-кадров (PPTP ориентирован только на IP).

В гибридном протоколе L2TP объединены лучшие черты вышеуказанных протоколов и добавлены новые функции. Протокол L2TP может поддерживать любые высокоуровневые протоколы и предусматривает управление потоками данных, удаленную аутентификацию пользователей, установку защищенного виртуального соединения. Кроме того, он позволяет открывать между пользователями сразу несколько туннелей, каждый из которых администратор может выделить для того или иного приложения. Спецификация L2TP не описывает методы аутентификации и шифрования, однако если туннель формируется в IP-сетях, то криптозащита должна выполняться в соответствии с протоколом IPSec. По существу протокол L2TP представляет собой расширение PPP - протокола функциями аутентификации удаленных пользователей, установки защищенного виртуального соединения, а также управлением потока данных. Для аутентификации в корпоративной сети перед стартом сессии PPP могут применяться без участия провайдера Internet протоколы CHAP/PAP или другие. Гарантированная доставка информации в сессии обеспечивается за счет нумерации защищенных кадров в соединении, восстановления потерянных и искаженных кадров. Протокол L2TP в качестве сервера RAS использует концентратор доступа AC (Access Concntrator), в котором реализована клиентская часть L2TP и обеспечивает пользователю сетевой доступ к его ЛВС через Internet. Роль сервера удаленного доступа ЛВС выполняет сервер L2TP (L2TP Network Server), функционирующий на любых платформах, совместимых с PPP. Протокол L2TP предусматривает три этапа установления соединения: установление соединения с удаленным сервером ЛВС; аутентификацию пользователя; конфигурацию криптозащитного туннеля [8, 9]. Услуга аутентификации включается здесь в процесс обслуживания протокольного блока уровня для каждого типа информации, а процесс предоставления механизма защиты моделируется как система массового обслуживания (СМО) с протокольной услугой безопасности (СМОПб) [6].

Постановка задачи анализа ТС ИКС на базе общих функционалов оценки ее эффективности

В работе мы уделим внимание исследованию влияния протокола L2TP на характеристики ТС инфокоммуникационной сети на технологии IP-QoS в ре-

жиме установленного соединения без задействования протокола IPSec. Кадры, циркулирующие в рамках сессии L2TP, имеют следующую структуру: заголовок канального уровня, используемый внутри Интернет, например, заголовок кадра Frame Relay; заголовок IP; заголовок L2TP; исходный пакет PPP, включающий пакет IP, IPX или NetBEUI. В качестве методологической базы для анализа ТС инфокоммуникационной сети на технологии IP-QoS, удовлетворяющих перечисленным выше требованиям, будем использовать концепцию ее архитектуры. В рамках этой концепции, эффективность использования IP-сети с интеграцией служб в режиме установленного соединения по аналогии с [7] предлагается оценивать с помощью набора функционалов использования пропускной способности каждого ЛЦТ $ij \in J$, входящих в состав виртуального пути $\widehat{l}^{k}_{st,m} = \{ si_1, i_1 i_2, ..., i_{p-1} t \}^{k}_{st,m}$, трафиком различных классов и учитывающих особенности реализации протокола каждого логического уровня ТС. Для каждого ЛЦТ этот функционал

$$K^{k}_{ij} = \prod_{h=1}^{4} K^{k}_{h,ij}, \qquad (1)$$

Нижний индекс $h = \overline{1,4}$ - соответствует логическому уровню архитектуры модели IP-сети: соответственно – транспортного, межсетевого взаимодействия, сетевого интерфейса и физического), а верхний k – классу трафика (B, C, D). На транспортном уровне IP-сеть рассматривается как набор транспортных соединений, включающих все образующие их логические каналы, при заданных условиях передачи. По аналогии с [7] $K^{k}_{4,ij} = K^{k}_{TCP} = \dfrac{s^k \beta^k}{N^k (L^k - H_{IP})}$ функционал, использования пропускной способности межузлового линейно-цифрового тракта (ЛЦТ) на транспортном уровне, учитывающий процедуру «нарезки» сообщений и речевых сегментов на блоки данных IP-уровня $\dfrac{s^k}{N^k (L^k - H_{IP})}$, а также механизм организации обратной связи на транспортном уровне (протокол TCP) с целью защиты от ошибок соответствующих сегментов: коэффициенты β^B и β^C (т. к. речевые сегменты не переспрашиваются, то β^B=1). Здесь H_{IP} — длина IP-заголовка, бит; L^B — длина речевого пакета, бит; L^C — длина пакета данных, бит; $s^B = \tau^B \upsilon^B$ - средняя длина речевого фрагмента на транспортном уровне, бит; $\tau^B = \int_0^\infty t dF^B(t)$ - средняя длительность активного речевого фрагмента с учетом служебной информации уровня, с, а υ^B — скорость работы речепреобразующего устройства (РПУ), бит/с; $s^C = \int_0^\infty l dF^C(l)$ — средняя длина сообщения данных на транспортном уровне с учетом служебной информации уровня, бит; N^B — среднее число информационных частей речевого пакета в активном речевом фрагменте; N^C — среднее число информационных частей пакета данных в сегменте данных на транспортном уровне. $K^{k}_{3,ij} = \rho^{k}_{ij} \dfrac{L^k - H_{IP}}{L^k}$, $K^{k}_{2,ij} = \dfrac{L^k}{L^k + H_{NI}}$, $K^{k}_{1,ij} \cong 1$,

где ρ_{ij}^{B} и ρ_{ij}^{C} — коэффициенты загрузки уровня межсетевого взаимодействия соответственно речевыми пакетами и пакетами данных; H_{NI} — длина заголовка протокольного блока уровня сетевого интерфейса, бит.

Обозначим через $K_{st,m}^{k}$ - коэффициент использования m - го виртуального пути из множества M_{st}^{k}. Этот коэффициент также можно трактовать как коэффициент передачи системы, составленной из цепочки каналов заданной пропускной способности $ij \in l_{st,m}^{k}$, и представить в виде среднегеометрического составляющих коэффициентов использования пропускной способности пути m-го выбора для пары $st \in S^{k}$

$$K_{st,m}^{k} = K_{TCP}^{k} \sqrt[r_{st,m}^{k}]{\prod_{ij \in l_{st,m}^{k}} K_{ij}^{k}} . \qquad (2)$$

Степень $1/r_{st,m}^{k}$ вводит эффект «усреднения» функционала использования ЛЦТ составного виртуального пути. При заданных функциях распределения длительностей активного речевого фрагмента и длины сообщений данных $F^{B}(t)$ и $F^{C}(l)$ [7]

$$N^{B} = \sum_{k=1}^{\infty} k \left[F^{B}\left(\frac{L^{B} - H_{IP}}{\upsilon^{B}} k\right) - F^{B}\left(\frac{L^{B} - H_{IP}}{\upsilon^{B}} (k-1)\right) \right],$$

$$N^{C} = \sum_{k=1}^{\infty} k \left[F^{C}((L^{C} - H_{IP})k) - F^{C}((L^{C} - H_{IP})(k-1)) \right].$$

В силу того, что транспортное виртуальное соединение может быть организовано между парой $st \in S^{k}$ по нескольким виртуальным путям с вероятностью $p_{st,m}^{k}$, - выражение для общего функционала использования всех транспортных соединений имеет следующий вид

$$K_{st}^{k} = \sum_{m=1}^{M_{st}^{k}} p_{st,m}^{k} \; K_{TCP}^{k} \sqrt[r_{st,m}^{k}]{\prod_{ij \in l_{st,m}^{k}} K_{ij}^{k}} , \; k = \overline{1,2} . \qquad (3)$$

Выпишем выражения для общих функционалов использования пропускной способности ЛЦТ

$$K_{ij}^{B} = \frac{s^{B} \rho^{B}(L^{B})}{N^{B}(L^{B} + H_{NI})}, \; K_{ij}^{C} = \frac{s^{C} \rho_{ij}^{C}(L^{B}, \rho^{B}, L^{C}) \beta_{ij}^{C}(L^{C})}{N^{C}(L^{C} + H_{NI})} . \qquad (4)$$

Проведя соответствующие подстановки в (3) с учетом (4) получим выражения для K_{st}^{k}:

$$K_{st}^{B} = \frac{s^{B}}{N^{B}(L^{B} + H_{NI})} \sum_{m=1}^{M_{st}^{B}} p_{st,m}^{B} \sqrt[r_{st,m}^{B}]{\prod_{ij \in l_{st,m}^{B}} \rho_{ij}^{B}(L^{B})} ,$$

$$K_{st}^{C} = \frac{s^{C} \beta_{ij}^{C}(L^{C})}{N^{C}(L^{C} + H_{NI})} \sum_{m=1}^{M_{st}^{C}} p_{st,m}^{C} \sqrt[r_{st,m}^{C}]{\prod_{ij \in l_{st,m}^{C}} \rho_{ij}^{C}(L^{B}, \rho_{ij}^{*B}, L^{C})} . \qquad (5)$$

В формулах (5) ρ_{ij}^{k} - максимальная загрузка ЛЦТ трафиком k - класса с учетом потерь b_{ij}^{k} по вызовам.

Оценку эффективности использования ресурсов ТС IP-QoS с учетом механизмов VPN проведем на примере протокола туннелирования L2TP. Для установления соединения с сервером L2PT ЛВС удаленный пользователь связыва-

ется по протоколу PPP с концентратором доступа АС провайдера, который может выполнить его аутентификацию от имени провайдера. После этого АС по имени пользователя определяет IP-адрес сервера L2PT ЛВС. Между концентратором АС и сервером L2PT ЛВС устанавливается сессия по протоколу L2TP и осуществляется аутентификация пользователя на сервере L2PT ЛВС. В случае успешной аутентификации между АС и сервером создается криптозащищенный туннель.

С учетом избыточности, вносимой протоколом L2PT, общие функционалы K_{ij}^C и K_{ij}^B использования пропускной способности ТС даются выражениями

$$K_{ij}^k = \frac{s^k \beta^k \rho^k}{N^k (L^k + H_{NI} + H_{L2TP})}, \quad (6)$$

В силу существенных преимуществ [10], целесообразно предположить, что функция распределения времени обслуживания пакетов в УК имеет экспоненциальный характер.

Поставленную задачу будем решать максимизируя общие функционалы K_{st}^B и K_{st}^C (5), отыскивая при этом оптимальные длины речевых пакетов и пакетов данных. Таким образом, задачу анализа однородной пакетной сети можно записать в виде последовательности двух задач оптимизации:

1. Найти $\arg\max K_{st}^B$, (7)

при условиях $b_{st}^B \le b^B, \Pr_{st}(t \ge \theta^B) \le d^B$, $L^{*B} \lhd \theta^B \upsilon^B - H_{IP}, 0 \lhd \rho_{ij}^B \le 1 \quad \forall st \in S^B : a_{st}^B \ne 0$, (8)

где $\Pr_{st}(t \ge \theta^B)$ - вероятность превышения заданного времени пребывания B-пакета в сети θ^B для пары $st \in S^B$.

2. Найти $\arg\max K_{st}^C$, (9)

при условиях $b_{st}^C \le b^C$, $T_{st}^C \le T^{*C} \ \forall \ st \in S^C : a_{st}^C \ne 0$, (10)

и все параметры задачи (7) найдены и фиксированы.

Здесь $T_{st}^C = \sum_{v=1}^{M_{st}^C} p_{st,m}^C \ T_{st,m}^C + \frac{L^C - H_{IP}}{\omega^C}$ - среднее время передачи пакетов класса C для пары $st \in S^C$ с учетом времени пакетизации на передаче, где $T_{st,m}^C = \sum_{ij \in l_{st,m}^C} T_{ij}^C + \sum_{i:ij \in l_{st,m}^C} T_i^C$. При проведении оптимизации указанных функционалов для упрощения выражений будем считать, что величины θ^B и T_{st}^C включают в себя только три основные временные компоненты: время накопления информационной части пакета в оконечной системе (время ввода пакета в ЛЦТ) соответственно $(L^B - H_{IP})/\upsilon^B$ и $(L^C - H_{IP})/\omega^C$, время обработки на УК $\sum_{i:ij \in l_{st,m}^C} T_i^C$ и собственно время передачи пакетов по тракту $\sum_{ij \in l_{st,m}^C} T_{ij}^C$. ω^C — скорость работы абонентской установки данных, бит/с.

Метод расчета параметров транспортной системы на технологии IP-QoS с учетом протокола туннелирования L2TP канального уровня

Выпишем выражения составляющих общих функционалов использования пропускной способности ТС IP-QoS K_{ij}^{C} и K_{ij}^{B} с учетом избыточности, вносимой в тракт передачи протоколом L2TP.

Выражение для коэффициента β^{C}, который является функцией длины кадра данных класса C и вероятности ошибки в тракте st с учетом сделанных выше предположений имеет вид

$$\beta^{C} = -\frac{p_0}{1-p_0}\ln p_0, \tag{11}$$

где $p_0 = (1-p)^{L^C + H_{NI} + H_{L2TP}}$. Основное условие пропускания нагрузки класса B является

$$\frac{L^B + H_{NI} + H_{L2TP}}{L^B - H_{IP}} \frac{\upsilon^B}{V_{ij}} a_{ij}^{B} \eta \le \rho_{ij}^{*B}. \tag{12}$$

Для однородной пакетной ТС

$$\rho_{st,m}^{*B} = 1 - \frac{z}{b} = 1 - \frac{z\,\upsilon^B (L^B + H_{TCP} + H_{NI} + H_{L2TP})}{\upsilon^B V \theta^B - (L^B - H_{IP}) V}, \tag{13}$$

где, $b = \left(\frac{\theta^B V}{L^B + H_{NI}} - \frac{L^B - H_{IP}}{L^B + H_{TCP} + H_{NI} + H_{L2TP}} \frac{V}{\upsilon^B} \right)$, z - есть решение нелинейного трансцендентного уравнения $\frac{1}{(n-1)!} z^{n-1} + \frac{1}{(n-2)!} z^{n-2} + \cdots + \frac{1}{1!} z + 1 = d^B e^z$.

$$\rho_{st,m}^{*C} = 1 - \rho^B - \frac{\frac{n\rho^B}{1-\rho^B}(L^B + H_{NI} + H_{L2TP}) + n\,(L^C + H_{NI} + H_{L2TP})\frac{1}{\beta^C}}{T_{st,m}^{C} V - (L^C - H_{IP})\frac{V}{\omega^C}} \beta^C, \tag{14}$$

Выражения для функционалов $K_{st,m}^{B}$ и $K_{st,m}^{C}$ имеют вид

$$K_{st,m}^{B} = \frac{L^B - H_{IP}}{L^B + H_{NI} + H_{L2TP}} \left(1 - \frac{z\,\upsilon^B (L^B + H_{NI} + H_{L2TP})}{\upsilon^B V \theta^B - (L^B - H_{IP}) V}\right).$$

$$K_{st,m}^{C} = \frac{L^C - H_{IP}}{L^C + H_{NI} + H_{L2TP}} \left(1 - \rho^B - \frac{\frac{n\,\rho^B}{1-\rho^B}(L^B + H_{NI} + H_{L2TP}) + n\,(L^C + H_{NI} + H_{L2TP})\frac{1}{\beta^C}}{T_{st,m}^{C} V - (L^C - H_{IP})\frac{V}{\omega^C}} \beta^C\right),$$

$$L^{*B} = \frac{(\theta^B \upsilon^B + H_{IP})\alpha_1 - (H_{NI} + H_{L2TP})\,\upsilon^B}{\alpha_1 + \upsilon^B}, \tag{15}$$

где $\alpha_1 = \sqrt{(H_{IP} + H_{NI} + H_{L2TP}) V / z\theta^B}$.

$$L^{*C} = x + H_{IP}, \tag{16}$$

где $x = \lim\limits_{k\to\infty} x_k$.

$$x_{k+1} = \frac{y-1}{\ln(1-p)} \left\{ 1 + \frac{x_k + \frac{T_{st,m}^{C}\,\omega^C}{\alpha_2\, y} \frac{y-1}{\ln(1-p)}}{(T_{st,m}^{C}\,\omega^C - x_k)\left[\frac{(\rho^B - 1)V}{n\,\omega^C\,\alpha_2}(T_{st,m}^{C}\,\omega^C - x_k) + 1\right]} \right\}, \tag{17}$$

Обращение в нуль знаменателя в выражении (17) происходит при условии, когда $x = T^C_{st,m}\omega^C - \frac{n\,\omega^C}{V}\frac{\rho^B}{(1-\rho^B)^2}(L^B + H_{NI} + H_{L2TP})$. Максимально эффективная скорость передачи трафика класса B, которую может пропустить однородный тракт $st \in S^B$ при заданной величине нагрузки $a^B_{st,m}$, заданном времени θ^B и ограничении d^B, определяется выражением

$$V^B_{st,m} = V\ K^B_{st,m} = V\ \frac{L^B - H_{IP}}{L^B + H_{NI} + H_{L2TP}}\left(1 - \frac{z\,\upsilon^B(L^B + H_{NI} + H_{L2TP})}{\upsilon^B V\,\theta^B - (L^B - H_{IP})V}\right), \quad (18)$$

а максимально эффективная скорость передачи трафика класса C, которую может пропустить тракт $st \in S^C$ при заданной величине нагрузки $a^B_{st,m}$ и заданном среднем времени $T^C_{st,m}$

$$V^C_{st,m} = V\ \frac{L^C - H_{IP}}{L^C + H_{NI} + H_{L2TP}}\left(1 - \rho^B - \frac{\frac{n\,\rho^B}{1-\rho^B}(L^B + H_{NI} + H_{L2TP}) + n\,(L^C + H_{NI} + H_{L2TP})\frac{1}{\beta^C}}{T^C_{st,m}V - (L^C - H_{IP})\frac{V}{\omega^C}}\,\beta^C\right), \quad (19)$$

где L^B и L^C находятся из соотношений (15) и (16).

Показателем качества работы однородной инфокоммуникационной сети на технологии IP может служить коэффициент использования цифрового тракта передачи на транспортном уровне:

$$R = \left[V^B_{st,m}(1-d^B) + V^C_{st,m}\right]/V. \quad (20)$$

Расчет параметров пакетного транспортного канала на технологии IP-QoS в режиме установленного соединения

Ниже приводится описание инженерной методики получения основных числовых характеристик ПТС МСС, позволяющей сравнить различные ТС (защищенных и не защищенных) для конкретных условий проектирования по коэффициентам R и R^S. Методика построена на базе теоретических исследований, проведенных выше. Исходные данные: $V, \nu, \omega, H_{IP}, H_{FR}, H_{L2TP,}\tau_1, T^C_{st,m}, (T^{*C}), \theta^B, B, p, n, d^B, a^B_{st,m}$ (величина речевого трафика в ПТС, эрл.);

1. Положить $H_{L2TP} = 0$. По заданным n, d^B найти z. Перейти к 2.

2. По заданным V, υ^B, θ^B, H_{IP}, H_{FR} и полученным z по формуле (15) найти L^B. Перейти к 3.

3. По заданным V, υ^B, θ^B, H_{IP}, H_{FR} и полученным z и L^B по формуле (13) найти $\rho^{*B}_{st,m}$ (β^B=1). Если $0 < \rho^{*B}_{st,m} \le 1$, то перейти к 4, иначе положить $a^B_{st,m\max} = 0$, где $a^B_{st,m\max}$ - величина максимально возможного речевого трафика, который может пропустить тракт ПТС, $L^B = H_{IP}$ и перейти к 5.

4. По заданным V, υ^B, H_{IP}, H_{FR} и вычисленным L^B и $\rho^{*B}_{st,m}$ найти $a^B_{st,m\max} = \frac{(L^B - H_{IP})V}{\eta\,(L^B + H_{L2TP} + H_{FR})\upsilon^B}\rho^{*B}_{st,m}$ (обращение формулы 12) Перейти к 5.

5. По заданным $0 \le a^B_{st,m} \le a^B_{st,m\max}, V, \upsilon^B, H_{IP}, H_{FR}, n, T^C_{st,m}, p, \omega^C$ и вычисленном L^B по формуле (16) найти L^C (при $a^B_{st,m} = 0$ положить ρ^B=0). Если $L^C = H_{IP}$, то поло-

жить $V^C_{st,m}$=0, где $V^C_{st,m}$ - максимально возможная эффективная скорость передачи трафика данных при заданных V и $T^C_{st,m}$, иначе перейти к 6.

6. По заданным $0 \le a^B_{st,m} \le a^B_{st,m\max}, V, \upsilon^B, H_{IP}, H_{FR}, n, T^C_{st,m}, p, \omega^C, \eta$ вычисленном L^B и L^C по формулам(11) и (14) найти соответственно β^C и $\rho^{*C}_{st,m}$. Рассчитать $K^C_{st,m}$ и $V^C_{st,m}$. Перейти к 7.

7. По заданным $0 \le a^B_{st,m} \le a^B_{st,m\max}, V, \upsilon^B, \eta,\ d^B$ найти $V^B_{st,m} = \eta\ \upsilon^B\ a^B_{st,m}$. Перейти к 8

8. По формуле (20) найти R.

Провести аналогичные расчеты с учетом протокола VPN канального уровня (Положить $H_{L2TP} = 160$ бит в формулах (13) – (19)) и вычислить R^S.

Величина $\Delta = (\frac{R}{R^{S_\Gamma}} - 1) \times 100\,\%$ характеризует проигрыигрыш в % защищенной системы относительно другой при заданных условиях проектирования.

В качестве примера рассмотрим параметры тракта передачи, характерные для протоколов Frame Relay, TCP/IP v.6. Основные числовые характеристики транспортных каналов на технологии IP, рассчитанные по приведенной выше методике, сгруппированы в таблице, которая описывает зависимость V, ρ^B, $V^C_{st,m}$, R от величины $a^B_{st,m}$ речевого трафика класса B для конкретных значений V, υ^B, ρ^B при $d = 0{,}01$, $T^C_{st,m} = 2c$, $\theta^B = 0{,}3c$, $n = 10$, $\omega^C = 64000$ бит/с, $\tau^B = 0{,}93c$, $H_{L2TP} = 160$ бит, $H_{FR} = 48$ бит, $H_{IP} = 320$ бит, $p = 10^{-6}$, $\eta^B = 0{,}497$. Значения $a^B_{st,m}$ в последних строках табл. для каждого V являются предельными ($a^B_{st,m\max}$) и лимитируются величиной ρ^{*B}. При уплотнении пауз в речевом трафике ($\eta^B = 0{,}497$) значения $a^B_{st,m}$ в табл. следует увеличить примерно в 2 раза.

Сравнительная оценка влияния протоколов VPN на параметры транспортной системы на технологии IP-QoS

Естественно считать ту систему лучшей, у которой при заданной величине речевой нагрузки $a^B_{st,m}$ значение $V^C_{st,m}$ больше при фиксированной величине скорости V в цифровом тракте. Та система лучше, у которой коэффициент R больше. Параметры расчета сравнительного анализа защищенной и незащищенной ПТС МСС приведены в таблице.

Таблица. Сравнительный анализ коэффициентов использования пропускной способности защищенной и незащищенной пакетной мульисервисной транспортной системы

d	V	υ^B	$R_{\max}$	$R^S{}_{\max}$	Δ %
0.01	128000	16000	0.5089659	0.4947332	2.88
	1024000	16000	0.6985772	0.6734883	3.73
	204800	16000	0.7441465	0.7201119	3.34
	204800	32000	0.7708604	0.7524964	2.44
0.01	128000	16000	0.5089659	0.4947332	2.88
	1024000	16000	0.6985772	0.6734883	3.73
	204800	16000	0.7441465	0.7201119	3.34

	204800	32000	0.7708604	0.7524964	2.44
0.005	128000	16000	0.5113161	0.4984059	2.59
	1024000	16000	0.7003534	0.6749003	3.77
	204800	16000	0.746691	0.7222697	3.38
	204800	32000	0.7738601	0.7550339	2.49

Выводы

1. Применение протокола VPN канального уровня L2TP (даже без процедуры шифрования) ухудшает эффективность использования пропускной способности пакетной транспортной системы более чем на 3%, при этом при увеличении скорости в тракте передачи это ухудшение увеличивается.

2. При увеличении скорости работы речепреобразующего устройства эффективность использования пропускной способности ТС увеличивается.

3. Уменьшение уровня изохронности речевого трафика улучшает эффективность использования пропускной способности ТС.

4. Можно наметить несколько дальнейших путей исследований данной проблематики. Во-первых, углубляясь в математические модели построения транспортных систем инфокоммуникационной сети можно рассмотреть применение механизмов безопасности с учетом требований различных типов трафика к своей передаче. Это позволит более качественно рассчитывать пропускную способность каналов и вычислительную мощность узлов ТС и нфокоммуникационной сети. Во-вторых, в рамках исследования протоколов защиты, например, IPSec можно сравнить различные алгоритмы шифрования (Triple DES, CAST-128, RC5, IDEA, Blowfish и ARCFour) и аутентификации (SHA-1, CHAP и др.). Кроме того, в данной работе не затронута оценка многоуровневой вложенности туннелей на характеристики ТС, а также объем дополнительного трафика аутентификации, что может в значительной степени увеличить нагрузку на транспортную систему.

ЛИТЕРАТУРА

1. *Н.Н. Мошак, Е.А. Тимофеев.* Особенности построения политики информационной безопасности в инфокоммуникационной сети // Электросвязь. – 2005.–№9.- с. 23-28
2. *ГОСТ Р ИСО 7498-2-99.* Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть.2. Архитектура защиты. – М., ИПК Издательство стандартов, 1999
3. *Бойдо В.Л.* Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. – СПб.: Питер, 2005. – 703 с.: ил.
4. Доктрина информационной безопасности Российской Федерации // Новая газета. – 15 сентября 2000.
5. *Н.Н.Мошак*, Модели оценки влияния механизмов шифрования на параметры пакетной транспортной системы инфокоммуникационной сети. X СПб международная конференция «Региональная информатика-2006 (РИ-2006)», Санкт-Петербург, 24-26 октября 2006 г.: Материалы конференции. – Спбю:СПОИСУ, 2006. 318 с.
6. *Н.Н.Мошак,* Модели оценки влияния механизмов аутентификации на параметры пакетной транспортной системы инфокоммуникационной сети. X СПб международная

конференция «Региональная информатика-2006 (РИ-2006)», Санкт-Петербург, 24-26 октября 2006 г.: Материалы конференции. – Спбю:СПОИСУ, 2006. 318 с.
7. *Н.Н.Мошак,* Теоретические основы проектирования транспортной системы инфокоммуникационной сети: учеб. пособие для вузов (специальность 230201 «Информационнные сети и технологии»)/ИА «Энергомашиностроение». СПб, 2006.159 с.
8. *В.Зима, А.Молдовян, Н.Молдовян.* Безопасность глобальных сетевых технологий.. – СПб.: БХВ-Петербург, 2000. – 320 с.: ил.
9. *Запечников С.В., Милославская Н.Г., Толстой А.И.* Основы построения виртуальных частных сетей: 9. Учебное пособие для вузов М.: Горячая линия-Телеком, 2003. – 249 с..
10. *Клейнрок Л.* Теория массового обслуживания. - М.: Машиностроение, 1979, 432 с

Статья поступила в редакцию в ноябре 2006 года,
после доработки – в декабре 2006 года