УДК 681.518:378

**Воропаева[1] В.Я. (канд. техн. наук, доц.), Шапо[2] В.Ф. (канд. техн. наук, доц.)**
1) Донецкий национальный технический университет, г. Донецк
кафедра автоматики и телекоммуникаций
2) Одесская национальная морская академия, г. Одесса
кафедра теории автоматического управления и вычислительной техники
E-mail: voropayeva@meta.ua, stani@te.net.ua

# МЕТОД РАСЧЕТА ПРОПУСКНОЙ СПОСОБНОСТИ МЕЖСЕТЕВЫХ ЭКРАНОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПРЕДПРИЯТИЙ

*Предложен метод расчета пропускной способности межсетевых экранов при создании и эксплуатации информационных систем предприятий. Проанализированы различные типы программных приложений, генерирующих и принимающих сетевой трафик через межсетевой экран при обращении к различным сервисам сети Интернет и использовании облачной модели в территориально распределенной информационной системе предприятия.*
***Ключевые слова**: пропускная способность, межсетевой экран, ЛКС, трафик.*

**Общая постановка проблемы**. С бурным развитием сети Интернет появилось множество вредоносных программ разного назначения, активно распространяющихся по ней и заражающих в короткое время сотни, тысячи или даже десятки тысяч компьютеров, что приводит к колоссальным материальным и временным потерям, связанным с простоем оборудования и вынужденным бездействием сотрудников. Велик также и ущерб, связанный с несанкционированным уничтожением данных, промышленным шпионажем и воровством интеллектуальной собственности [1, 2, 3]. В связи с этим чрезвычайно актуальна задача защиты рабочих мест в локальных компьютерных сетях предприятий от вторжений извне. Одним из возможных решений данной проблемы является применение программно-аппаратных межсетевых экранов (англ. термин Firewall, нем. Brandmauer), обладающих широким спектром возможностей и высоким быстродействием [4, 5].

Современные информационные системы (ИС) предприятий и организаций все шире используют подключение к сети Интернет для реализации облачной модели [6] эксплуатации программного обеспечения классов ERP (Enterprise Resource Planning, планирование ресурсов предприятия), MRP (Manufacturing Resources Planning, планирование ресурсов производства), CRM (Customer (Client) Relationships Management, управление взаимоотношениями с клиентами) и т.д. и офисных программных продуктов (например, Microsoft Office 365), что позволяет уменьшить необходимое количество лицензий, их более гибкое использование и экономию материальных ресурсов для их приобретения. Очевидно, что в дальнейшем применение этой модели будет лишь расширяться. Облачная модель также дает возможность использовать морально устаревшие компьютеры с использованием браузеров в качестве основного исполняемого программного приложения. В свою очередь, это позволяет шире использовать бесплатно распространяемые программные продукты с открытым исходным кодом (free and open source software) — например, операционные системы (ОС) семейства Linux вместо ОС семейства Windows, что также весьма актуально для множества предприятий различного размера и разных сфер деятельности.

Поскольку ИС множества предприятий являются территориально распределенными, для связи сотрудников через сеть Интернет между собой и с клиентами в бизнес-целях широко используются функции обмена мгновенными сообщениями, интернет-пейджеры, работа в многочисленных социальных сетях и других Интернет-сервисах, без чего развитие современных бизнес-отношений совершенно невозможно. Поэтому каждая локальная компьютерная сеть (ЛКС) обособленного подразделения предприятия, подключенная к Интернет, должна быть защищена межсете-

вым экраном во избежание заражения вредоносным программным обеспечением, вторжения злоумышленников и связанной с этим потери данных, кражи интеллектуальной собственности и т.д. Ряд проблем, связанных с защитой данных и системами информационной безопасности, рассмотрены в работах [7, 8, 9].

**Решение задач и результаты исследований.** В данной работе предлагается метод расчета пропускной способности аппаратных межсетевых экранов, для достижения необходимого быстродействия построенных на базе отдельных устройств, а не на базе компьютеров. Структурная схема территориально распределенной компьютерной сети предприятия с применением межсетевых экранов для защиты ЛКС подразделений представлена на рис. 1.

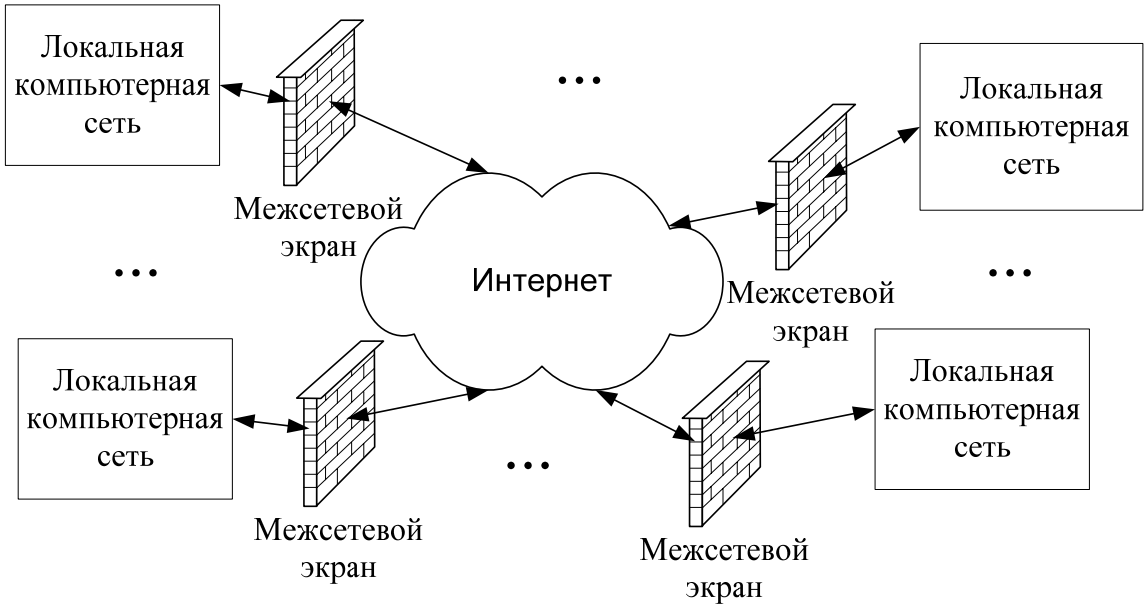


Рисунок 1 — Структура территориально распределенной компьютерной сети предприятия с применением межсетевых экранов

Межсетевые экраны могут быть использованы для ряда нижеследующих целей.

1. Защита и изоляция приложений, служб (сервисов), компьютеров и сетевых устройств внутренней ЛКС от нежелательного трафика, приходящего из внешней сети Интернет, защита от проникновения на компьютер «снаружи» (взлом).

2. Для ограничения или запрещения доступа вычислительных устройств внутренней ЛКС к сервисам внешней сети Интернет, иными словами, защита от несанкционированной передачи данных с компьютера «наружу» (например, предотвращение кражи паролей, номеров кредитных карт и т.д. троянскими программами).

3. Для поддержки преобразования сетевых адресов (network address translation, NAT), что дает возможность задействовать во внутренней сети произвольные (внутренние) IP-адреса и совместно использовать одно общее подключение к сети Интернет либо через единственный реальный (специально выделенный для этой цели) внешний IP-адрес, либо через любой адрес из множества автоматически присваиваемых внешних адресов.

Выделим два основных способа создания наборов правил межсетевого экрана: "включающий" и "исключающий". Исключающий межсетевой экран позволяет прохождение всего трафика, кроме трафика, соответствующего указанному набору правил. Включающий межсетевой экран, наоборот, пропускает только трафик, соответствующий указанным правилам и блокирует все остальное.

Включающий межсетевой экран обеспечивает гораздо больший контроль исходящего трафика и является лучшим выбором для систем, предоставляющих сервисы в Интернет. Он также контролирует тип трафика из Интернет в ЛКС. Трафик, не соответствующий указанным правилам, блокируется, а в log-файл (файл протокола, системный журнал) вносятся со-

ответствующие записи. Включающие межсетевые экраны обычно более безопасны, чем исключающие, поскольку они существенно уменьшают риск пропуска межсетевым экраном нежелательного трафика.

Безопасность может быть дополнительно повышена с использованием межсетевого экрана с сохранением состояния. Такой межсетевой экран сохраняет информацию об открытых соединениях и разрешает только трафик через открытые соединения или открытие новых соединений. Недостаток межсетевого экрана с сохранением состояния в том, что он может быть уязвим для атак DoS (Denial of Service, отказ в обслуживании), если множество новых соединений открывается очень быстро. Большинство межсетевых экранов позволяют комбинировать поведение с сохранением состояния и без сохранения состояния, что позволяет создавать оптимальную конфигурацию для конкретной системы.

Выбор межсетевого экрана с учетом производительности и функциональности является нетривиальной задачей, поскольку между моделями различных производителей и различными продуктовыми линейками одного производителя имеется множество отличий, которые можно выделить следующим образом (их можно также использовать в качестве критериев выбора):

область применения;

быстродействие;

максимальное число одновременно открытых сессий (сеансов связи);

характеристики (возможности);

стоимость.

Первым критерием, который должен использоваться при выборе межсетевого экрана, должна являться его производительность (быстродействие), поскольку, если она будет недостаточной и межсетевой экран станет источником «заторов» во время передачи данных, то соответствие остальным вышеперечисленным критериям уже практически не имеет значения. Максимальное число одновременно открытых сессий также является важным критерием, поскольку, если новые сессии не могут быть открыты, запуск новых сетевых или Интернет-приложений становится невозможен.

При работе с сетью Интернет большие объемы передаваемых данных и большое количество одновременно открытых сессий создают следующие основные типы программных приложений.

1. Браузеры сами по себе при Интернет-серфинге (открытие при работе в Интернет множества окон и вкладок при работе с различными ресурсами). Возможно использование сеансов связи в нескольких браузерах одновременно, поскольку браузеры различных разработчиков не совсем одинаково отображают различные Интернет-ресурсы. Наиболее популярны следующие браузеры: Internet Explorer, Mozilla Firefox, Opera, Safari, Google Chrome, Green Browser, TheWorldBrowser, Browse3D, Slim, K-Meleon, Flock, Avant Browser, Netscape Navigator, Maxthon и др.

2. Браузеры при работе в социальных сетях. Наиболее популярны следующие социальные сети: Twitter, LinkedIn, Вконтакте, Одноклассники, LiveJournal, FaceBook, Я.ру, МойМир, FriendFeed, МойКруг и т.д.

3. Браузеры при работе с бизнес-приложениями в соответствии с облачной моделью. Наиболее часто используются системы следующих классов: CRM, ERP, ECM (Enterprise Content Management, управление бизнеса предприятия), DWS (Data Warehouse Systems — системы управления хранилищами данных), WMS (Warehouse Management System, система управления складом), BI (Business Intelligence, бизнес-аналитика), и т.д.

4. Интернет-пейджеры (мессенджеры, средства обмена мгновенными сообщениями). Наиболее популярны QIP, Miranda IM, AOL IM, Yahoo! Messenger, Google Talk, Windows Live Messenger, ICQ, Mail.ru Агент, R&Q**,** Trillian**,** Digsby, MSN, XMPP (Jabber), PSI, Pidgin, Я.Онлайн.

5. Специализированные программные системы организации видеоконференций, из которых самой популярной является Skype.

6. Программные системы Интернет-телефонии (IP-телефонии).

7. Системы дистанционного обучения, используемые для повышения квалификации сотрудников.

8. Вебинары, также используемые для повышения квалификации сотрудников.

9. Чаты и форумы с соответствующими программными клиентами.

10. Электронная почта.

11. Файлообменные сети (BitTorrent, eDonkey, KaZaA и др.)

12. Антивирусное и антиспамерское программное обеспечение, реализованное в нескольких вариантах (домашняя, бизнес- и серверные версии). Наиболее популярны следующие программные продукты: Антивирус Касперского, Доктор Веб, Norton, Eset NOD32, Panda, Avira, BitDefender, Avast!, TrustPort, AdWare, AVG, Simple AntiVirus и некоторые другие.

13. Системы наблюдения, основанные на цифровых видеокамерах, передающих видеоданные по компьютерным сетям с использованием протокола TCP/IP, в т.ч. и через сеть Интернет.

Выполненный анализ программных приложений, использующих для работы сеть Интернет, не является окончательным, поскольку их перечень и возможности постоянно расширяются. Кроме того, постоянно появляются новые приложения, решающие известные задачи новым путем, но отличающиеся принципами функционирования и выдвигающие различные требования к межсетевым экранам.

Формализуем проведенный выше анализ.

Будем считать, что к корпоративной ЛКС могут быть подключены не только стационарные компьютеры, но и различные мобильные устройства, принадлежащие сотрудникам: мобильные компьютеры (ноутбуки, нетбуки, ультрабуки и проч.), планшетные компьютеры, смартфоны и т.д., использующие проводные и беспроводные сетевые соединения, количество которых может существенно варьироваться.

Пусть каждое сетевое устройство, работающее в ЛКС, использует несколько различных программных приложений для решения некоторого (определённого) количества задач. Данные, генерируемые этими приложениями, передаются через межсетевой экран во внешнюю сеть. Тогда трафик $V_c$ через межсетевой экран, генерируемый этими приложениями с одного сетевого устройства, можно описать формулой

$$V_c = \sum_{i=1}^{n_v} V_i \ , \tag{1}$$

где $n_v$ — число типов решаемых задач.

Каждая задача может быть решена с помощью запуска нескольких типов программных приложений. Тогда общий трафик $V_{cf}$, генерируемый всеми возможными программными приложениями одного сетевого устройства для решения всего спектра задач, можно описать формулой

$$V_{cf} = \sum_{k=1}^{t} \sum_{i=1}^{n_v} V_{ik} \ . \tag{2}$$

Тогда общий трафик через межсетевой экран, генерируемый всеми сетевыми устройствами ЛКС, можно описать формулой

$$V_{acf} = \sum_{k=1}^{l} \sum_{j=1}^{t} \sum_{i=1}^{n_v} V_{ijk} \ . \tag{3}$$

Определив, в какой период времени $t$ необходимо передать рассчитанный по формуле (3) трафик, можно рассчитать требуемую пропускную способность межсетевого экрана для описанных выше задач и программных приложений для всех сетевых устройств, входящих в корпоративную ЛКС по формуле

$$B_d = \frac{V_{acf}}{t} \ . \tag{4}$$

Формулы (1)–(4) в формализованном виде позволяют описать трафик через межсетевой экран, создаваемый программными приложениями, для которых не требуется обеспечение определенной пропускной способности сети.

Ряд сетевых приложений требует обязательного выделения некоторой пропускной способности сети, обеспечивающей их минимальные потребности. Тогда пропускная способность $B_c$ через межсетевой экран, генерируемый этими приложениями с одного сетевого устройства, можно описать формулой

$$B_c = \sum_{i=1}^{n_b} B_i \ , \tag{5}$$

где $n_b$ — число типов решаемых задач.

Каждая задача может быть решена с помощью запуска нескольких типов программных приложений, требующих для работы определенную пропускную способность сети. Тогда общая пропускная способность $B_{cf}$, требующаяся для всех возможных программных приложений одного сетевого устройства для решения всего спектра задач, можно описать формулой

$$B_{cf} = \sum_{k=1}^{t_b} \sum_{i=1}^{n_b} B_{ik} \ . \tag{6}$$

Тогда пропускная способность межсетевого экрана для приложений, требующих определенный ее минимум для работы, требуемая всеми сетевыми устройствами ЛКС, может быть описана формулой

$$B_{acf} = \sum_{k=1}^{l} \sum_{j=1}^{t} \sum_{i=1}^{n_b} V_{ijk} \ . \tag{7}$$

Полная пропускная способность $B$ межсетевого экрана для обработки всех типов данных всех приложений всех сетевых устройств ЛКС может быть определена по формуле

$$B = B_d + B_{acf} = \frac{V_{acf}}{t} + \sum_{k=1}^{l} \sum_{j=1}^{t} \sum_{i=1}^{n_b} V_{ijk} \ . \tag{8}$$

Пропускная способность межсетевого экрана $B_r$ выбирается на базе рассчитанной $B$ следующим образом: имеется $q$ стандартных пропускных способностей межсетевых экранов одной компании-производителя, отсортированных по возрастанию:

$$B = \{B_1, B_2, \ldots, B_m, \ldots, B_q\}.$$

Тогда

$$\forall i, \exists B_m, B_{m\text{-}1} < B_{ij} \ \& \ B_m > B_{ij}.$$

В связи с быстрым увеличением объемов передаваемой информации необходимо выполнить прогнозирование развития ИС и ЛКС предприятия и ввести коэффициенты запаса для расчета пропускной способности межсетевого экрана $\widetilde{B}_r$. Полный трафик через межсетевой экран с учетом прогнозирования

$$\widetilde{B}_r(y+1) = kB_r(y) \ , \tag{9}$$

где $y$ — календарный год, в который выполняется прогноз; $y + 1$ — следующий год; $k$ — коэффициент запаса.

Учитывая рост Интернет-трафика, расширение спектра решаемых задач и реализующих их программных продуктов, целесообразно выбирать коэффициент запаса в диапазоне 1,2 – 1,4.

**Выводы**

1. Выполнен анализ типов и областей применения аппаратных межсетевых экранов. Предложены критерии их выбора для решения конкретных задач при построении информационных систем предприятий.

2. Выполнен анализ спектра решаемых задач и соответствующих программных приложений, используемых при работе непосредственно с сетью Интернет или для связи удаленных подразделений организации между собой с использованием Интернет и создающих нагрузку на межсетевой экран.

3. Предложен метод расчета пропускной способности аппаратных межсетевых экранов, формализующий процедуру их выбора с учетом количества и типа решаемых с использованием межсетевых соединений задач, позволяющий также учесть динамику развития информационной системы предприятия.

**Список использованной литературы**


1. PC WEEK [Электронный ресурс]. — Режим доступа: http://pcweek.ua/themes/detail.php?ID=135897
2. PC WEEK [Электронный ресурс]. — Режим доступа: http://pcweek.ua/themes/detail.php?ID=135891
3. PC WEEK [Электронный ресурс]. — Режим доступа: http://pcweek.ua/themes/detail.php?ID=135928
4. Компания Dlink [Электронный ресурс]. — Режим доступа: http://dlink.ua
5. Компания Cisco [Электронный ресурс]. — Режим доступа: http://cisco.ua
6. PC WEEK [Электронный ресурс]. — Режим доступа: http://pcweek.ua/themes/detail.php?ID=135845
7. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / П.Н. Девянин. — М.: Горячая Линия–Телеком, 2011. — 320 с.
8. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / Шаньгин В. Ф. — М.: Инфра-М, 2008. — 416 с.
9. Воропаева В.Я. Анализ требований к серверной подсистеме при построении информационных систем предприятия / В.Я. Воропаева, В.Ф. Шапо // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. — 2009. — Вип. 17 (148). — С. 14–21.


Надійшла до редакції
15.02.2012 р.

Рецензент:
д-р техн. наук, проф. Скобцов Ю.О.

***V.Y. Voropaeva, V.F. Shapo. Method of firewalls bandwith calculating in enterprises information systems****. Method of firewalls bandwith calculating for creating and exploitation of enterprises information systems is proposed. Different application types which generate and receive network traffic through firewall during appealing to a lot of Internet services and using of cloud model in enterprise territorial distributed information system are analyzed.*
***Keywords****: bandwidth, firewall, LAN, traffic.*

***В.Я. Воропаєва, В.Ф. Шапо. Метод розрахунку пропускної здатності міжмережевих екранів в інформаційних системах підприємств****. Запропоновано метод розрахунку пропускної здатності міжмережевих екранів при побудові та експлуатації інформаційних систем підприємств. Проаналізовано різні типи програмних додатків, які генерують та приймають мережевий трафік крізь міжмережевий екран під час звертання до різноманітних сервісів мережі Інтернет та використання хмарної моделі в територіально розосередженій інформаційній системі підприємства.*
***Ключові слова****: пропускна здатність, міжмережевий екран, ЛОМ, трафік.*