ния в Интернет.

1.Меренков А.П., Хасилев В.Я. Теория гидравлических цепей. – М: Наука, 1985. – 278 с.

2.Математическое моделирование и оптимизация систем тепло-, водо-, нефте-, газоснабжения / А.П. Меренков, Е.В. Сеннова, С.В.Сумароков и др. – Новосибирск: ВО «Наука», Сиб. изд. фирма РАН, 1992. – 406 с.

3.Трубопроводные системы энергетики. Развитие теории и методов математического моделирования и оптимизации / Аверьянов В.К., Новицкий Н.Н., Сухарев М.Г. и др. – Новосибирск: ВО «Наука», Сиб. изд. фирма РАН, 2008. – 311 с.

4.Гради Буч. Объектно-ориентированный анализ и проектирование с примерами приложений на C++: Пер. с англ. – 2-е изд. – М.: Бином; СПб: Невский диалект, 1998. – 560 с.

5.Рофейл Э., Шохауд Я. COM и COM+. Полное руководство. – М.: Век, 2000. – 560 с.

6.Байдачный С.С. SilverLight 4: Создание насыщенных Web-приложений – М.: СОЛОН ПРЕСС, 2010. – 288 с. (Серия «Библиотека профессионала»).

7.Описание IIS. http://ru.wikipedia.org/wiki/IIS.

8.Описание Apache. http://apache.org.

9.Описание PHP. http://php.ru

10.Описание ASP. http://ru.wikipedia.org/wiki/Active_Server_Pages.

11.Описание XML. http://ru.wikipedia.org/wiki/Xml.

12.Описание JSON. http://json.org/.

13.Разработка Web-приложений на Microsoft Visual Basic .NET и Microsoft Visual C#.NET. Учебный курс MCAD/MCSD/Пер. с англ. – М.: Изд.-торговый дом «Русская Редакция», 2003. – 704 с.

Получено 17.01.2012

УДК 004.056.5

С.И.БОГУЧАРСКИЙ, Н.И.САМОЙЛЕНКО, д-р техн. наук
Харьковская национальная академия городского хозяйства

МОДЕЛЬ БЕЗОПАСНОГО ДОСТУПА К ГЛОБАЛЬНОЙ СЕТИ INTERNET

Предлагается программно-аппаратная модель безопасного доступа к глобальной сети Internet. Рассматриваются состав и функции основных модулей модели.

Пропонується програмно-апаратна модель безпечного доступу до глобальної мережі Internet. Розглядаються склад і функції основних модулів моделі.

It is proposed hardware and software model of secure access to the Internet. We consider the composition and functions of the basic modules of the model.

Ключевые слова: сетевые угрозы, модель доступа, защита данных.

Современным предприятиям требуется оперативный обмен информацией различного рода. Глобальная сеть Internet решает эту проблему. В рамках этой сети функционируют: электронная почта, социальные сети, специализированные ресурсы электронной отчетности, клиент-банк и многое другое. С одной стороны – всемирная паутина является

положительным изобретением для пользовательской аудитории, с другой – несет различные угрозы тем же пользователям в виде: спамов, «червей», «вирусов», хакерских атак, руткитов, рекламных систем adware, ботнетов (бот-сетей), шпионских вредоносных программ, DoS-(DDoS), атак drive-by при загрузке и других угроз. Нейтрализация вредоносного действия программного обеспечения и хакерских атак является первостепенной задачей в организации и обеспечении безопасной работы любой современной фирмы, пользующейся возможностями Internet. Именно задача защиты корпоративной сети от угроз со стороны Internet рассматривается в настоящей статье.

Существуют два метода предотвращения угроз, поступающих из глобальной сети: аппаратный и программный.

В ходе изучения проблемы рассмотрены различные подходы к защите локальных сетей, предложенные производителями сетевого оборудования и лицензионного программного обеспечения [1, 2]. Анализ рассмотренных подходов послужил основой для принятия решения о целесообразности разработки двухуровневой модели защиты.

В работе предлагается модель с использованием аппаратного и программного модулей, обеспечивающих эффективную защиту от угроз Internet. Модель открыта для реконфигурирования и развития.

Разработка модели включала три проектных этапа:

1. *Выбор технического средства подключения к глобальной сети Internet*. В качестве средства связи была определена фиксированная телефонная линия с предоставлением услуги доступа по технологии ADSL. Принятие такого решения оправдано для предприятий, не имеющих иных проводных средств доступа или беспроводной связи.

2. *Выбор оборудования.* По техническим характеристикам и стоимости оборудования наиболее рациональным решением оказалось использование продукции компании D-LINK [3].

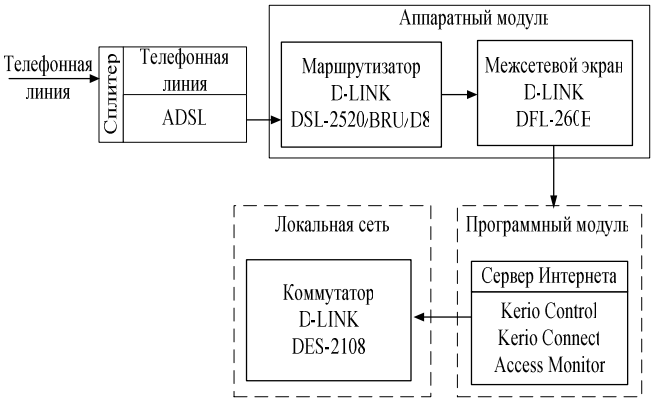
3. *Выбор программного обеспечения*. По критерию функциональной полноты, гибкости и открытости предпочтение было отдано программному обеспечению компании KERIO [4].

Модель безопасного доступа к сети Internet изображена на рисунке.

При разработке данной модели преследовались следующие цели:

- обеспечение безопасности рабочих станций и оборудования локальной сети предприятия;
- организация доступа пользователей предприятия к глобальной сети;
- обеспечение оптимальной пропускной способности (балансировка сетевой нагрузки, уменьшение сетевых коллизий);
- доступ к информационным ресурсам предприятия извне (создание виртуальных сетей);

– мониторинг использования всемирной паутины пользователями локальной сети предприятия;
– централизованная обработка электронной почты (получение, доставка, хранение, проверка на наличие спамов и т д.).



Модель безопасного доступа к глобальной сети Internet

Подключение по технологии ADSL – это предоставление традиционного доступа в Internet по существующим кабельным телефонным сетям. При этом на одном абонентском номере (один кабель телефонной линии) имеется возможность беспрепятственно использовать услугу фиксированной телефонной связи для доступа к глобальной сети Internet. Такой результат достигается установкой специального устройства – сплитера, которое производит частотное разделение на два канала связи: фиксированная телефонная связь и доступ к Internet по технологии ADSL.

Как показано на рисунке, модель имеет три модуля: аппаратный, программный и локальную сеть.

Аппаратный модуль предусматривает установку следующего оборудования: маршрутизатора DLINK DSL-2520/BRU/D8 и межсетевого экрана DLINK DFL-260E [3].

Маршрутизатор – это устройство, подключаемое к телефонной линии, которая предоставляет услугу традиционного доступа к Internet с использование технологии ADSL. Данное устройство имеет высокую производительность. Благодаря применению стандарта ADSL2+ скорость нисходящего потока достигает 24Мбит/с. Маршрутизатор имеет ряд дополнительных функций: поддержку интегрированного межсетевого экрана (проверка состояния пакета SPI); организацию протокола по-

пыток хакерских атак (таких как отказ в обслуживании – DoS и др.); поддержку QoS, обеспечивающей более эффективную передачу данных приложений, чувствительных к задержкам, таких как VoIP, потоковое мультимедиа и др.

Межсетевой экран – это устройство уровня Enterprise NetDefend UTM, представляющее собой законченное решение для управления, мониторинга и безопасного обслуживания сети [3]. Оно подключается к маршрутизатору и обеспечивает всестороннюю защиту от вирусных атак, несанкционированного доступа, нежелательного контента и т.п. Межсетевые экраны уровня NetDefend UTM оснащены профессиональной системой предотвращения вторжений IPS, антивирусной программой AV, аппаратным ускорителем, увеличивающим производительность IPS и AV, системой обнаружения и предотвращения сетевых угроз, а также программным фильтром Web-содержимого на 7 уровне модели ISO. Сервисы обновления IPS, антивируса AV и базы данных URL защищают сеть предприятия от вторжений, «червей», вредоносных кодов. NetDefend UTM имеет встроенный VPN-клиент и сервер, что позволяет работать практически с любой политикой VPN и осуществлять безопасное подключение к сети. UTM-сервис обеспечивает эффективную защиту от угроз из Internet, для чего используются три базы данных, находящиеся в активном состоянии. Данная технология позволяет обходить потенциально опасные объекты, включая Java-апплеты, Java-скрипты/VBS-скрипты, объекты ActiveX и cookies. Она поддерживает автоматическое обновление базы данных сигнатур IPS, защиту сети от атак zero-day и работу антивирусной программы AV в реальном масштабе времени. Межсетевой экран ZoneDefense UTM осуществляет сканирование по наиболее полной и актуальной базе данных антивирусных сигнатур, используя технологию потокового сканирования, что позволяет наиболее эффективно защищать сеть от вирусов. Аппаратный ускоритель для Unified Threat Management – это встроенный аппаратный ускоритель, который позволяет межсетевому экрану осуществлять предотвращение вторжений и антивирусное сканирование одновременно, не ухудшая при этом производительность межсетевого экрана.

Программный модуль предусматривает установку сервера – это отдельно выделенный персональный компьютер, на котором установлено два сетевых интерфейса и специальное программное обеспечение (KERIO CONTROL, KERIO CONNECT, INTERNET ACCESS MONITOR) на базе операционной системы WINDOWS XP.

KERIO CONTROL является программным брандмауэром, предназначенным для комплексной защиты локальных сетей предприятий от полного спектра сетевых угроз и обладающим такими функциональны-

ми возможностями, как [4]:

- защита от несанкционированного доступа (сигнатурный анализ, база данных правил безопасности, список заблокированных IP адресов, журнал безопасности и т.д.);
- поддержка интегрированного прокси-сервера;
- балансировка сетевой нагрузки канала доступа в Інтернет;
- кэширование пакетов;
- тунелирование по TCP-портам;
- поддержка интегрированного антивирусного сканера SOPHOS;
- предотвращение посещения нежелательных сайтов;
- организация VPN туннелей;
- мониторинг и статистика RX- и TX-потоков.

KERIO CONNECT является программным почтовым сервером, который обеспечивает доступ к электронной почте пользователей локальной сети и имеет следующие функциональные возможности [4]:

- доступ пользователей локальной сети предприятия к ресурсам электронной почты;
- выделение отдельных ресурсов для электронных почтовых ящиков каждому пользователю и всего предприятия;
- встроенная модель антивирусной защиты компании SOPHOS;
- защита от спамов: DHA-защита от атак типа Directory Harvest, SpamAssassin (Bayes, эвристика и SURBL), Anti-phishing/anti-spoofing; RBL (обновляющиеся в режиме реального времени, черные списки серверов);
- автоматическое копирование и архивирование данных;
- статистический учет и мониторинг использования информационных ресурсов.

INTERNET ACCESS MONITOR – является программным продуктом, одной из задач которого является мониторинг и сбор статистической информации об использовании канала доступа к глобальной сети Internet пользователями предприятия. Такого рода информация необходима для проведения анализа использования традиционного доступа в Internet. Данные для сбора статистической информации извлекаются из модулей программного продукта KERIO CONTROL.

Локальная сеть – это модуль, который обеспечивает связь локальной сети предприятия с программно-аппаратным комплексом для доступа к Internet [3]. Связь обеспечивается с помощью управляемого коммутатора DLINK DES-2108, позволяющего осуществлять координирование рабочих станций и оборудования при доступе локальной сети к Internet. Кроме того, данное устройство является связующим с иным коммутационным оборудованием локальной сети предприятия и обес-

печивает технологические услуги такие, как Storm Control (внутреннее сглаживание внешних помех), Bandwith Control (ограничение пропускной способности по RX-потоку) и др.

Одной из особенностей данного оборудования является аппаратное разделение доступа к портам коммутатора интегрированными средствами VLAN.

В разработанной модели используется двухуровневая защита от угроз глобальной сети. Блокирование угроз на первом уровне обеспечивается аппаратным брандмауэром, а на втором – программным брандмауэром.

Программное обеспечение, установленное на выделенном компьютере-сервере, обеспечивает совместный доступ к электронной почте, статистике и мониторингу посещения пользователями локальной сети Internet, а также к установленному программному брандмауэру с широким функционалом, предотвращающим различного рода угрозы. Подключение рабочих станций и иного коммутационного оборудования локальной сети к Internet обеспечивает управляемый коммутатор DES-2108.

Работа локальной сети с предлагаемой моделью доступа к глобальной сети не требует постоянного мониторинга со стороны администратора локальной сети. Модель открыта для реконфигурирования и развития, что, в свою очередь, обеспечивает её легкую адаптацию к условиям реально существующих предприятий и корпоративных сетей.

Основной научный результат работы (модель защиты от угроз глобальной сети) внедрен в корпоративную сеть ООО «Архитектурная Строительная Фирма «СОЮЗ». Данная модель успешно эксплуатируется и надежно защищает информационные ресурсы фирмы от сетевых угроз.

1.Леонтьев В.П. Безопасность в сети Интернет. – М.: ОЛМА Медиа Групп, 2008. – 256 с.

2.Ватаманюк А.И. Создание, обслуживание и администрирование сетей на 100%. – СПб.: Питер, 2010. – 232 с.

3.Оборудование D-Link. – http://dlink.ru/.

4.Кроссплатформенный почтовый сервер. – http://www.kerio.ru/.

Получено 17.01.2012