УДК 004.77

СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

А. Д. Кощей, В. О. Шапорин, Е. Л. Шапорина

Одесский национальный политехнический университет
Украина, г. Одесса
Arturian42@gmail.com

Рассматриваются вопросы обеспечения информационной безопасности локальной вычислительной среды при помощи современных технологий в области сетевых аппаратных и программных средств.

Ключевые слова: компьютерные сети, сетевая безопасность, списки доступа.

Информационная безопасность локальной вычислительной сети любого объекта подразумевает наличие целой системы элементов защиты, которая включает в себя правовой, организационный, инженерно-технический, программно-аппаратный и криптографический методы защиты [1].

В настоящее время ущерб, связанный с реализацией угроз сетевой безопасности, растет стремительно, что и приводит к повышенному вниманию к вопросам сетевой безопасности.

Цели сетевой безопасности могут меняться в зависимости от конкретной ситуации, но основных целей обычно три: обеспечение целостности, конфиденциальности и доступности данных.

Для обеспечения сетевой безопасности определяются следующие организационные и технические меры:

— идентификация пользователей;
— распределение прав групп пользователей;
— разработка списков доступа;
— шифрование трафика;
— создание межсетевых экранов.

Организация защиты средствами межсетевого экрана является отдельной задачей настройки аппаратного и программного обеспечения, при которой необходимо учитывать следующие функциональные возможности:

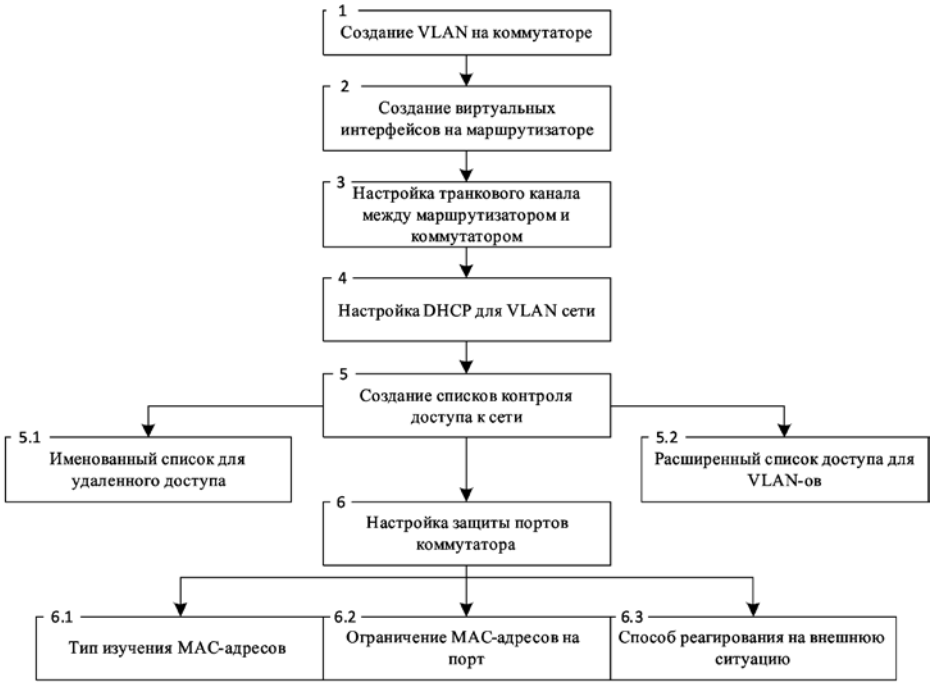
— блокирование нежелательного трафика;
— перенаправление входного трафика только к надежным внутренним системам;
— сокрытие уязвимых систем, которые нельзя обезопасить от атак;
— протоколирование трафика внутренней сети;
— сокрытие информации (имен систем, топологии сети, типов сетевых устройств и внутренних идентификаторов пользователей) от внешней сети;
— обеспечение более надежной аутентификации, чем та, которую представляют стандартные приложения.

Остальные перечисленные меры безопасности можно реализовать на имеющемся активном сетевом оборудовании, исходя из требований к уровню безопасности, реакции на внештатные ситуации и возможностей оборудования.

Как пример, на рисунке представлен процесс обеспечения безопасности сети кафедры университета, включающий в себя этапы реализации функций оборудования. Блоки 1—3 реализуют разбиение начальной сети на виртуальные подсети (VLAN). Данные этапы соответствуют мерам по распределению прав пользователей. Каждая из VLAN соответствует одной из трех групп пользователей: VLAN 10 (Stuff) — подсеть для сотрудников кафедры; VLAN 11 (Student) — подсеть для студентов кафедры; VLAN 12 (Guest) — гостевая подсеть. Такой подход обеспечивает ролевой метод разграничения доступа, где пользователь, входящий в одну из подсетей, принимает права доступа для этой подсети.

Блок 4 реализует динамическую раздачу адресов для каждой из подсетей. Помимо стандартной функции адресации в сети, IP-адрес, полученный из пула одной из подсетей, будет одним из идентифика-

торов принадлежности к определенной группе доступа. Таким образом, функционирование DHCP сервера, в рамках данной работы, становится одним из способов идентификации и авторизации в сети.



Процесс организации безопасности сети

Пятый блок реализует определение прав доступа в сети путем определения списков контроля доступа (ACL). Для осуществления такой меры безопасности целесообразно разбить данный этап на два этапа – создание ACL для подсетей и ACL для удаленного доступа к узловому оборудованию системы. Для подсетей удобно создать расширенный ACL, который позволит ограничить доступ к ресурсам сети на основе протоколов для каждого из VLAN. Именованный ACL позволяет определить устройства, имеющие удаленный доступ к активному оборудованию. Для этого предварительно необходимо зарезервировать соответствующий диапазон адресов в пуле DHCP.

Последним из необходимых шагов является организация защиты портов коммутаторов. Данный этап целесообразно разбить на три этапа: динамическое или статическое задание MAC-адресов устройств, ограничение MAC-адресов, которые могут подключаться к портам, и реагирование на нарушения установленных правил для портов различными способами (отчет об ошибке, выключение порта, игнорирование) [2].

Применение предложенного процесса обеспечения безопасности позволит сохранять целостность документов, снизит вероятность несанкционированного проникновения в локальную сеть и увеличит возможность отражения угроз, как внутренних, так и внешних.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. В. Г. Олифер, Н. А. Олифер. Компьютерные сети. Принципы, технологии, протоколы.— СПб.: Питер, 2010.— 944 с.: ил.

2. В. О. Шапорин, П. М. Тишин, Н. Б. Копытчук, Р. О. Шапорин. Нечеткие лингвистические модели обеспечения безопасности компьютерных сетей // Тр. 14-й МНПК «Современные информационные и электронные технологии». Т. I.— Украина, г. Одесса.— 2013.— С. 155 —156.

A. D. Koshey, V. O. Shaporin, E. L. Shaporina

Process of ensuring the security of computer networks.

This paper discusses the security issues of the local computing environment using modern technology in the field of network hardware and software.

Keywords: *computer networks, network security, access control lists.*