УДК 681.3.06

В.В. КАРАСЮК, канд. техн. наук,
В.А. ПАЗЫЧ, НЮАУ (г. Харьков)

АНАЛИЗ ЗАЩИЩЕННОСТИ ЛОКАЛЬНОЙ СЕТИ ВУЗА

У статті розглянута модель системи захисту інформації у локальній мережі. Для опису моделі пропонується використати системний підхід та побудувати матрицю відповідності. Наведені відомості про реальну локальну мережу ВУЗа та загрози інформаційній безпеці, які мали місце впродовж року експлуатації даної мережі. Описані можливості апаратних та програмних засобів захисту, які є вбудованими у комутатори, що встановлені у вузлах локальної мережі. Запропоновані подальші напрямки досліджень і розробок інтелектуальних систем захисту інформації у локальних комп'ютерних мережах.

In article the model of system for protection of the information in a local network is considered. For the description of model it is offered to use the system approach and to construct a matrix of conformity. Data on a real computer network of a higher educational institution and threat of information safety, which took place during a year of operation in the given network are resulted. Opportunities of equipment in network and software of protection, which are built in switches, are described. These switches are used in units of a local network. Directions of the further researches and development of intellectual systems for protection of the information in local computer networks are offered.

Постановка проблемы. Анализ защищенности локальных компьютерных сетей относится к слабо структурированным проблемам системного анализа, потому что ее решение сталкивается с широким набором альтернатив нарушений безопасности, зависит от технологических достижений в аппаратном и программном обеспечении информационных систем, по которым нет полной информации, является внутренне сложной проблемой вследствие комбинирования ресурсов, необходимых для защиты компьютерных сетей, и для нее не определены формальные требования защищенности. Локальная компьютерная сеть представляет собой сложный программно-аппаратный и телекоммуникационный комплекс, распределенный территориально и объединяющий большое количество аппаратных устройств, которые динамично взаимодействуют во времени под управлением программного обеспечения. В настоящее время используется много различных эвристических способов оценки защищенности информационных систем, однако единого математического аппарата для решения данной проблемы не существует, эта проблема не тривиальна, что порождает индивидуальные подходы для разрабатываемых и эксплуатируемых информационных систем [1].

Анализ литературы. В соответствии с моделью сетевых взаимодействий в сети анализ безопасности проводится на уровнях: пользовательских приложений; СУБД; операционной системы; на сетевом (физическом) уровне; интегрированный подход [2]. В силу значимости рассматриваемой проблемы,

она получила широкое обсуждение в литературе. Известные исследователи в этом направлении – А. Лукацкий, Ю. Цаплев, М. Степашкин, Р. Просянников, А. Астахов, А. Шелупанов, Д. Зегжда, П. Джангк, В. Эймс, О. Бойцев, Дж. Говард и другие [2 – 9]. Для рассмотрения предлагаются: технологии обнаружения атак на основе нарушений политики безопасности; исследования уязвимости информационных систем; анализ журналов регистрации транзакций и сетевого трафика; графовые модели атак; сценарные модели; подходы, ориентированные на использовании агентно-ориентированного моделирования компьютерного противоборства злоумышленников и компонентов защиты и другие. Однако совершенные интеллектуальные средства защиты еще не получили должного распространения, требуют настройки на конкретную сеть и затрат на сопровождение (затрат времени, ресурсов компьютерных систем).

Цель статьи. Исходя из позиций системного подхода и существующих реальных угроз для информации в сети, выполнить анализ потенциальной защищенности локальной сети от несанкционированного доступа. Сформулировать условия для оптимального применения средств защиты локальной сети высшего учебного заведения. Провести анализ и выбрать конкретные средства аппаратной и программной защиты.

Информационная инфраструктура локальной сети. Созданная локальная сеть имеет развитую структуру, распределенную территориально. Некоторые узлы вынесены из головного корпуса на расстояние до 3 км. Число рабочих станций в сети ныне составляет более 500 компьютеров, и в процессе развития это количество будет расти. На рис. 1 показана обобщенная инфраструктура сети.

Угрозы для защищенности локальной сети. После создания основной части локальной сети, она была подключена через городскую сеть провайдера к сети Inernet. За время эксплуатации (около 1 года) сеть неоднократно подвергалась воздействию со стороны внешних и внутренних атак, направленных, в первую очередь, на получение информации, находящейся на локальных компьютерах у пользователей. Зафиксированные атаки можно разделить на два вида: попытки получения информации при помощи вирусов, троянских и шпионских программ; атаки на компьютеры, предпринятые через "дыры" в защитных программах (брэндмауэрах) и в программном обеспечении компьютера. За год работы локальной сети наиболее часто встречающимися вирусами на персональных компьютерах были "черви" (Worms), рассмотренные ниже. *Win32.HLLM.Perf* – почтовый червь массовой рассылки. Распространяется по электронной почте в виде вложения. Подделывает адрес отправителя. *Trojan-Dropper.Win32.Delf.sq* – троянский вирус, который устанавливает и запускает на исполнение другие вредоносные программы без

ведома пользователя. *Trojan-PSW.Win32.Ldpinch.air* – троянский вирус, ворующий пароли.

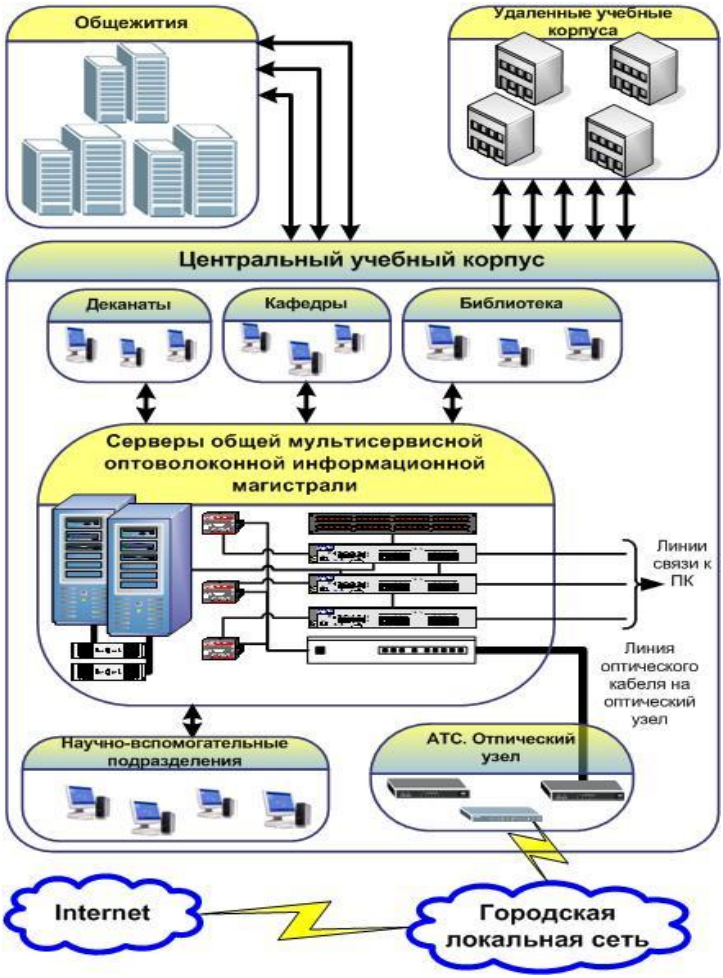

Рис. 1. Обобщенная инфраструктура локальной сети.

Trojan-Proxy.Win32.Horst.aa – довольно сложный многокомпонентный троян, который вначале модифицирует исполняемые файлы, а потом ломает систему безопасности, и использующий различные полиморфные технологии для осложнения обнаружения антивирусными программами. *Virus.Win32.Hidrag.a* – резидентный Win32-вирус. Заражает приложения Win32. При заражении шифрует часть заражаемого файла. *Macro.PPoint.Attach* – был найден на нескольких персональных компьютерах. Является первым

известным вирусом, который заражает файлы-презентации MS PowerPoint. Способен получить управление, активизироваться и размножаться в случае, когда в заражаемом файле-презентации содержится хотя бы одна форма (UserForm) [7,8].

Индивидуальные требования защищенности информационных ресурсов. Учитывая, что локальная сеть состоит из довольно большого числа компьютеров, и они находятся в различных подразделениях, от деканатов, кафедр, учебных классов до бухгалтерии и отдела кадров, возникает необходимость индивидуальной защиты рабочих мест в подразделениях и отделах. Это выполняется несколькими способами: закрытием доступа аппаратными способами – установкой на линии к отделам роутера; закрытием доступа с использованием запрограммированных портов на управляемом коммутаторе.

Принципы построения системы защиты локальной сети. В результате проведенного анализа угроз и с учетом поставленных требований защищенности информационных ресурсов выработан план мероприятий по повышению уровня защиты сети. Использован интегрированный подход, который предполагает применение многоуровневых средств, рассредоточенных по инфраструктуре сети. Для учета соотнесения средств защиты с защищаемыми ресурсами построена матрица соответствия

$$Z = \left\| z_{i,j} \right\|,$$

где столбец матрицы – множество узлов и рабочих станций сети, подлежащих контролю защищенности; строка – множество средств защиты, имеющихся в сети; элементы $z_{i,j}$ – состояние *j* средства защиты на *i* узле. Иерархическая структура сети предполагает наличие иерархической структуры службы защиты информации. Это нашло отражение в структуре матрицы соответствия, которая является инструментом формального анализа состояния средств системы информационной защиты сети.

Возможности аппаратных и программных средств защиты в локальной сети. В рассматриваемой сети применено следующее оборудование, которое выполняет функции защиты. Управляемый коммутатор 2-го уровня D-Link DGS-1216T – поддерживает статическую таблицу MAC-адресов для ограничения доступа к сети. Аутентификация 802.1x на основе портов позволяет использовать внешний RADIUS-сервер для авторизации пользователей. Дополнительные функции, такие как D-Link Safeguard Engine, защищают коммутатор от вредоносного трафика, вызванного активностью вирусов (червей). Управляемый коммутатор D-Link DES-3550 может контролироваться и обслуживаться через уникальный IP-адрес с любой рабочей станции, имеющей Web-браузер. Обеспечивает расширенный набор функций безопасности для управления подключением и доступом пользователей. Это Access Control Lists (ACL) на основе MAC-адресов, портов

коммутатора, IP адресов и (или) номеров портов TCP/UDP, аутентификацию пользователей 802.1x и контроль MAC-адресов. Помимо этого, DES-3500 обеспечивает централизованное управление административным доступом через TACACS+ и RADIUS. Эти функции обеспечивают авторизованный доступ пользователей и предотвращают распространение вредоносного трафика. Управляемый коммутатор DES-3526 имеет функции, практически аналогичные DES-3550 [9]. Перечисленные средства защиты размещены по структуре сети в соответствии с исходной матрицей соответствия. При обнаружении понижения уровня защищенности, последующими действиями пользователя должны стать: устранение обнаруженных уязвимостей и "узких" мест (обновление конфигурации сети и политики защищенности); повторный анализ защищенности сети, заданной обновленными спецификациями.

Выводы. Проблема защиты информации в компьютерных сетях является чрезвычайно важной и болезненной для всех пользователей и администраторов сетей. Состояние защищенности динамически изменяется во времени и необходим ее постоянный контроль. Для этой цели уже существуют интеллектуальные средства анализа защищенности, но они еще не вышли на уровень практической реализованности. Поэтому системные администраторы продолжают изыскивать приемы эффективной защиты своих сетей. В работе на примере конкретной локальной компьютерной сети ВУЗа показан подход, основанный на формальном анализе матрицы соответствия средств защиты предъявляемым требованиям защищенности.

Дальнейшая реализация предлагаемого подхода предполагается в программной реализации сопровождения матрицы соответствия и разработки подхода к формированию численных оценок защищенности узлов сети в рамках своих метрик, основанных на качественных методиках анализа угроз.

Список литературы: 1. Системный анализ в защите информации: Учеб. пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности / *А.А.Шумский, А.А.Шелупанов.* – М.: Гелиос АРВ, 2005. – 224 с. **2.** *Лукацкий А.В.* Обнаружение атак. – СПб.: БХВ-Петербург, 2001. – 624 с. **3.** *Степашкин М.В., Котенко И.В., Богданов В.С.* Интеллектуальная система анализа защищенности компьютерных сетей // http://www.raai.org/library/library.shtml, 2006. – 9 с. **4.** *Столлинг В.* Основы защиты сетей. Приложения и стандарты: Пер. с англ. – М.: Издат. дом "Вильямс", 2002. – 432 с. **5.** *Громико І.А.* Загальна парадигма захисту інформації // http://www.crime-research.ua, 2004. – 13 с. **6.** *Эймс В.* Шпионские программы: риск и ответственность // Открытые системы. – 2005. – № 2. – С. 42 – 47. **7.** *Джангк П., Шим С.* Оперативная безопасность в Internet // Открытые системы. – 2004. – № 7. – С. 53 – 59. **8.** *Бойцев О.М.* Удаленное проникновение, или золотые правила безопасности сети // Компьютерная газета HARD'n'SOFT, 2006. – № 10. – С. 3. **9.** *Черников Ф.* Обзор решений для обеспечения защиты корпоративной информации // CHIP. – 2004. – № 1. – С. 86 – 91.

Поступила в редакцию 03.04.2007