может не иметь никаких прав доступа к таблицам БД, с которыми работает первый пользователь.

Оба приведенных примера объединяет то, что информационные потоки по времени, возникающие в результате осуществления описанных действий, реализуются за счет отображения ядром системы информации о ее функционировании в сущностях, к которым субъекты системы непосредственно не получали доступ. Ядро системы само заносит данные о действиях субъектов в доступные на чтение другим субъектам сущности, причем первые могут и не иметь никаких прав доступа к данным сущностям.

В связи с обнаружением информационных потоков по времени нового типа возникает необходимость учета данных потоков при анализе защищенности КС. В рамках семейства ДП-моделей возможно введение нового вида ассоциированных сущностей, указывающих на возможность реализации к ним информационных потоков по времени в зависимости от выполняемых субъектом действий. Кроме того, возможно введение новых правил преобразований, а также формулировка и обоснование необходимых и достаточных условий возможности реализации информационных потоков по времени между сущностями КС.

ЛИТЕРАТУРА

1. *Девянин П. Н.* Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006.

УДК 681.322

ОБУЧЕНИЕ НА ПЛАТФОРМЕ CISCO ОСНОВАМ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ[1]

Д. Н. Колегов

Основным известным подходом к созданию многоуровневой защиты сетевых компьютерных систем является архитектура Cisco SAFE [1]. В ней рассматриваются принципы и механизмы повышения безопасности сетевой инфраструктуры, предлагаются типовые схемы сетей, маршрутизации и коммутации в них, а также приводятся рекомендации по проектированию и настройке сетевых технологий защиты информации. Методы и подходы, изложенные в руководстве Cisco SAFE, в принципе, не зависят от производителя конкретных средств защиты и могут быть применены в сетях, построенных на основе технологий различных производителей, таких, как Cisco Systems, Check Point, Juniper, IBM ISS, Microsoft, H3C, HP, D-Link и др.

Одним из требований ФГОС ВПО третьего поколения в области информационной безопасности является наличие дисциплины «Основы построения защищенных вычислительных сетей». На кафедре защиты информации и криптографии Томского государственного университета данный курс читается автором на протяжении двух семестров и состоит из двух частей — теоретической (лекционной) и практической (лабораторной). В теоретической части, излагаемой на основе [1, 2], рассматриваются основные принципы и методы проектирования защищенных сетей, а в практической — изученные принципы и методы применяются студентами в лабораторных работах, проводимых в среде эмуляции Cisco Packet Tracer [3].

В теоретической части курса рассматриваются следующие основные вопросы:

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).

1) Основные механизмы обеспечения безопасности вычислительных сетей.
2) Общие меры повышения защищенности сетевых устройств.
3) Технологии межсетевого экранирования.
4) Технологии систем обнаружения и предотвращения вторжений.
5) Технологии анализа защищенности сетей.
6) Выбор платформы сетевых средств защиты информации.
7) Принципы разработки и оптимизации современных локальных вычислительных сетей (ЛВС).
8) Принципы построения виртуальных частных сетей.
9) Принципы проектирования защищенных приложений.
10) Анализ рекомендуемых типовых схем защиты сетей.

После изучения вопросов теоретической части студенты выполняют персональное задание по проектированию схемы защиты конкретной вычислительной сети. Приведем пример такого задания.

Предложить техническое решение системы обнаружения и предотвращения вторжений на базе сигнатурного метода и метода обнаружения аномалий. Решение должно обеспечивать контроль информационных потоков на уровне сети предприятия, серверов и рабочих станций пользователей. За основу решения должны быть взяты технологии компании IBM ISS. Техническое решение должно обеспечивать централизованный мониторинг возможных вторжений и два метода управления системой: локальное и централизованное. Необходимой базой для интеграции решения служит сетевая и системная инфраструктура среднего предприятия. Данное предприятие имеет три территориально разнесенных филиала и центральный офис. В центральном офисе предусмотрен корпоративный доступ по беспроводной сети и доступ по VPN. Основной технический персонал отделов ИТ и информационной безопасности находится в центральном офисе. В филиалах работает по одному сотруднику из отдела. Для выполнения данного задания необходимо описать: инфраструктуру предприятия, техническое решение, порядок интеграции технического решения в инфраструктуру, а также порядок управления и мониторинга техническим решением.

На лабораторных работах решаются типовые задачи по обеспечению безопасности и настройке механизмов защиты сетевой инфраструктуры, основными из которых являются:

1) Создание и настройка защищенных виртуальных локальных сетей.
2) Настройка механизмов защиты сетевой инфраструктуры от несанкционированного доступа.
3) Настройка инфраструктуры защищенной коммутации.
4) Настройка средств управления безопасностью информационных потоков.
5) Настройка защищенной передачи данных через сеть Интернет.
6) Настройка инфраструктуры защищенной маршрутизации ЛВС.
7) Проектирование системы обнаружения и предотвращения вторжений.
8) Проектирование системы межсетевого экранирования и виртуальных частных сетей.
9) Проектирование полностью маршрутизируемой ЛВС с повышенной доступностью.

Описание каждой лабораторной работы данного перечня состоит из следующих частей:

— цель — содержит краткое описание цели, на достижение которой направлена лабораторная работа;
— постановка задачи — содержит описание условий лабораторной работы и используемых элементов сети;
— схема сети — графическое изображение схемы сети, ее адресации, структуры и других необходимых для решения задачи элементов;
— краткие теоретические сведения — содержит минимально-необходимый теоретический материал, которым должен владеть обучаемый для успешного выполнения лабораторной работы;
— последовательность действий обучаемого — содержит описание основных действий (шагов) обучаемого, а также команды, которые необходимо выполнить для корректной настройки сетевого оборудования;
— дополнительное задание — содержит перечень необязательных задач, которые обучаемому предлагается решить самостоятельно.

Использование среды эмуляции Cisco Packet Tracer позволяет каждому студенту создавать, настраивать и исследовать собственную виртуальную вычислительную сеть, наблюдать основные процессы ее функционирования, а также наглядно изучать базовые сетевые протоколы.

ЛИТЕРАТУРА

1. *Cisco Systems, Inc.* Cisco SAFE reference guide [Электронный ресурс]. — `http://cisco.com/go/safe`.
2. *Convery S.* Network security architectures. Cisco Press, 2008. 792 p.
3. *Cisco Systems, Inc.* Cisco Packet Tracer [Электронный ресурс]. — `http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html`.

УДК 519.248

АДАПТИВНЫЙ АЛГОРИТМ ОТСЛЕЖИВАНИЯ АНОМАЛЬНОЙ АКТИВНОСТИ В КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВАНИИ ХАРАКТЕРНЫХ ИЗМЕНЕНИЙ ОЦЕНОК АЛЬТЕРНИРУЮЩЕГО ПОТОКА

О. В. Ниссенбаум, А. С. Присяжнюк

Современные сети связи, в том числе и компьютерные сети, представляют собой чрезвычайно сложные системы массового обслуживания, в которых функционируют различные потоки — заявок, пакетов данных, отказов и т. п. Как правило, такие потоки имеют переменную, случайно изменяемую интенсивность, поэтому могут быть моделированы простейшим потоком лишь на сравнительно небольших отрезках времени. В работе [1] показано, что трафик компьютерной сети с той или иной степенью достоверности может быть представлен дважды стохастическим потоком событий с кусочно-постоянной интенсивностью. В ряде случаев, например в распределенных информационных системах (ИС), где пользователи в основном работают с удаленными базами данных, трафик достаточно хорошо описывается моделью альтернирующего потока [2]. Такой поток имеет два состояния, в первом из которых наблюдается пуассоновский поток с параметром λ, а во втором события потока отсутствуют. Интервалы, на которых поток находится в первом или втором состоянии, распределены по экспоненциальному закону с параметром α_1 и α_2 соответственно.