С. В. Запечников (к. т. н., доцент), Н. Г. Милославская (к. т. н., доцент),
А. И. Толстой (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)

СПЕЦИАЛИЗАЦИЯ «БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ» СПЕЦИАЛЬНОСТИ 090105

Введение

В рамках специальности 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем» в 2000 г. в МИФИ на факультете «Информационная безопасность» была разработана, а в 2005 г. уточнена специализация «Безопасность открытых информационных систем».

Для начала осуществления подготовки специалистов по новой специализации в первую очередь были доработаны квалификационные характеристики выпускника, которые нашли отражение в дополнение к паспорту специалиста.

Объектом его профессиональной деятельности являются открытые системы обработки, хранения и передачи информации, методы и средства обеспечения информационной безопасности (ИБ) в открытых информационных системах (ОИС).

1. Квалификационные характеристики выпускников по специализации

После обучения названный специалист владеет основами проектирования, администрирования и обеспечения ИБ в ОИС и дополнительно к указанным в паспорте специалиста обладает следующими профессиональными качествами:

· знает основы организации и функционирования, стандарты и протоколы ОИС;

· способен выявлять возможные способы и пути нарушения ИБ в этих системах и предлагать методы защиты от несанкционированных воздействий и их предотвращения;

· может выбирать политику безопасности для ОИС;

· способен осуществлять мониторинг сетевой безопасности, т. е. администрировать ОИС;

· имеет представление об основных тенденциях и закономерностях развития ОИС, средствах и методах защиты информации в них;

· имеет представление об основных тенденциях и закономерностях развития телекоммуникационных систем, средствах и методах защиты информации в них;

· знает современные криптографические средства защиты для ОИС, умеет осуществлять их обоснованный выбор;

· умеет тестировать программно-аппаратные и технические средства защиты ОИС и определять эффективность их функционирования;

· знает организационно-правовые и нормативные основы защиты информации в ОИС.

2. Учебный план специализации

Перечень учебных дисциплин для специализации был составлен на основе утвержденного ранее Учебного плана подготовки специалистов по специальности 090105. Он был дополнен дисциплинами, относящимися к разделам «Специализация», «Курсы по выбору» и «Региональный компонент».

С шестого по десятый семестр включительно студентам преподаются следующие *дисциплины специализации*:

· «Открытые информационные системы» (68 ч);

· «Криптографические протоколы и стандарты» (144 ч);

· «Информационная безопасность открытых систем» — части 1 и 2 (по 280 ч каждая);

· «Аудит информационных технологий» (96 ч).

Первый три курса уже читаются студентам МИФИ семь лет подряд, а четвертый курс в настоящее время находится в стадии разработки.

Вопросы, непосредственно связанные со специализацией, также рассматриваются каждый семестр, начиная с пятого, при выполнении студентами учебно-исследовательских работ. Приведем некоторые темы этих работ:

· «Изучение сервисов безопасности по защите электронной почты»;

· «Разработка архитектуры защищенной системы обнаружения вторжений»;

· «Исследование протоколов безопасных платежей по банковским картам в Интернете»;

· «Аудит ИБ крупных корпоративных систем на соответствие требованиям международных стандартов по ИБ»;

· «Создание программного комплекса по моделированию атак на веб-сервер»;

· «Разработка архитектуры системы комплексного сетевого сканирования защищенности»;

· «Система сбора данных журналов регистрации событий операционных систем»;

· «Выявление и анализ уязвимостей в корпоративных вычислительныхWi-Fi-сетях»;

· «Анализ и оценка рисков ИБ с помощью специализированных систем»;

· «Исследование способов повышения защищенности корпоративных сетей с помощью программно -аппаратных комплексов обеспечения сетевой безопасности»;

· «Защищенный доступ пользователей к прикладным системам» и т. п.

Общий объем часов для выполнения этих работ составляет 260, включая 130 аудиторных занятий.

К дисциплинам специализации также относится курс «Технология построения защищенных автоматизированных систем», взятый из стандарта специальности. Он читается студентам факультета на девятом семестре.

Общий объем часов преподавания дисциплин специализации составляет 920, включая 460 часов аудиторных занятий.

Для студентов названной специализации также предлагаются четыре учебных *курса по выбору* (из трех возможных на каждом семестре, однозначно соответствующих трем другим специализациям, разработанным на факультете; две другие специализации связаны с криптографией и юриспруденцией) с зачетом в конце обучения:

· «Защита электронного документооборота» (108 ч);

· «Криптография в банковском деле» (136 ч);

· «Защита информации в банковских системах» (108 ч);

· «Катастрофоустойчивость информационных систем» (72 ч).

Общий объем занятий по курсам по выбору составляет 424 ч, включая 212 ч аудиторных занятий.

Все учебные дисциплины специализации и курсы по выбору и лабораторные практикумы к ним разработаны сотрудниками МИФИ.

Региональный компонент представлен для данной специализации более углубленным, чем в стандарте специальности, дополнительным изучением следующих дисциплин:

· «Языки программирования» (170 ч, включая 85 ч аудиторных занятий);

· «Методы программирования» (204 ч);

· «Безопасность систем баз данных» (136 ч);

· «Безопасность операционных систем» (136 ч, включая 68 ч аудиторных занятий);

· «Технические средства и методы защиты информации» (108 ч);

· «Защита информации от вредоносного программного обеспечения» (108 ч) — курс, отсутствующий в стандарте специальности вообще, но очень актуальный на сегодня.

Общий объем занятий по региональному компоненту составляет 862 ч, включая 431 ч аудиторных занятий.

3. Базовая дисциплина специализации

Базовой дисциплиной специализации является курс «Информационная безопасность открытых систем».

Первая часть курса посвящена изучению концепции ОИС, ее модельному представлению и инфраструктуре. Приведем календарный план курса.

1 неделя (3 часа). Концепция открытых информационных систем. Классификация систем ИТ. Основные понятия и определения. Проблемы обеспечения совместимости в гетерогенной среде. Основные положения концепции открытых систем. Среда открытых систем. Роль стандартов в технологии открытых систем. Организационная структура системы стандартизации ИТ. Системообразующие стандарты ISO/IEC.

2 неделя (3 часа). Модельное представление открытых систем. Формы логической организации стандартов. Классификация моделей. Модель ISO OSI. Профили на базе модели ISO OSI. Спецификация POSIX и ее развитие. Модель OSE/RM. Тестирование соответствия профилям. Эволюция моделей открытых систем. Модели распределенных вычислений. Модель TOGAF — современная концепция описания компьютерных систем: метод синтеза архитектуры системы, нормативная техническая модель, описание сложной системы специалистами различных предметных областей, информационная база стандартов.

3 неделя (3 часа). Совместимость открытых систем. Основные аспекты совместимости систем: переносимость и способность к взаимодействию. Базовая модель ОИС, ее основные элементы. Эволюция понятия платформы. Функциональные блоки платформы и способы их взаимодействия: интерфейсы и протоколы. Три аспекта переносимости: переносимость прикладных программ, данных и пользователей. Способы реализации переносимости. Расширение базовой модели ИС для взаимодействующих систем. Взаимодействующие системы и распределенная вычислительная система. Образ единой системы в распределенной вычислительной среде. Способы реализации способности к взаимодействию. Стек протоколов. Коммуникационный интерфейс.

4 неделя (3 часа). Системный подход к описанию функциональности на базе модельного представления открытых систем. Сервисы. Стандартизация сервисов. Классификация сервисов платформы приложений. Внутренние сервисы платформы. Сервисы данных. Сервисы человекомашинного взаимодействия. Сетевые сервисы. Межкатегориальные сервисы. Основные классы прикладных программ.

5 неделя (3 часа). Методологические основы распределенной обработки и хранения данных. Уровни распределения обработки данных в архитектуре открытой системы. Модель RM-ODP. Модели организации распределенных вычислений: клиент-серверная, хостовая, «ведущий-ведомый», иерархическая, одноранговая, объектная. Сильная и слабая связность процессоров: многопроцессорные ВК, кластеры, сетевые вычисления, концепция GRID. Задачи распределения обработки:

диспетчеризация, синхронизация, маршрутизация, балансировка, управление ресурсами, обработка ошибок. Архитектура распределенного хранения данных. Сети хранения данных (SAN — Storage Area Networks). Средства сетевого хранения. Виртуализация хранения. Файловые системы SAN.

6 неделя (3 часа). Коммуникационная инфраструктура открытых систем. Концепция глобальной коммуникационной инфраструктуры. Физические способы реализации инфраструктуры: проводные, оптические, радиоканалы. Транспортные задачи коммуникационной инфраструктуры: эффективное кодирование, помехоустойчивость, управление линией передачи данных, управление каналами, задержки в сетях передачи данных, множественный доступ к несущей, маршрутизация, управление потоками. Примеры архитектур транспортного уровня: локальные сети, FDDI, SLIP, ISDN, SONET/SDH, X.25, ATM, FrameRelay.

7—8 недели (5 часов). Инфраструктура безопасности открытых систем. Управление криптографическими ключами. Жизненный цикл ключей. Стандарт ISO/IEC 11770. Модели управления ключами: централизованная и децентрализованная. Типовая структура ключевой системы. Концепция инфраструктуры открытых ключей (PKI): основные модели, стандарты и рекомендации. Управление ключами в многодоменных информационных системах.

8 неделя (1 час). Неделя семестрового контроля (в виде письменного ответа на вопросы из списка изученных тем).

9—10 недели (6 часов). Интранет как ОИС. Понятие интранет как примера ОИС и задачи ее защиты. Структура интранет. Эталонная модель интранет. Экстранет. Порталы: виды порталов, схема, компоненты, базовые сервисы. Корпоративные порталы.

11—12 недели (6 часов). Уязвимость открытых систем на примере интранет. Основные понятия. Угрозы ресурсам интранет. Причины уязвимости. Уязвимость архитектуры клиент-сервер: конфигурация системы, уязвимость операционных систем, уязвимость серверов (уязвимость систем управления базами данных, уязвимость систем электронного документооборота), уязвимость рабочих станций, уязвимость каналов связи (перехват паролей, перехват незащищенного трафика, недостатки протоколов, уязвимости каналообразующего оборудования). Слабости системных утилит, команд и сетевых сервисов на примере стека протоколов TCP/IP (Telnet, FTP, NFS, DNS, NIS, World Wide Web, команды удаленного выполнения, Sendmail и электронная почта, другие утилиты). Средства замены уязвимых сервисов TCP/IP. Слабости современных технологий программирования (Java, ActiveX…) и ошибки в программном обеспечении. Сетевые вирусы.

13—14 недели (6 часов). Информационные и сетевые ресурсы ОИС как объекты атак. Удаленные сетевые атаки. Их классификация. Типовые удаленные атаки: анализ сетевого трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над станцией в сети. Типичные сценарии и уровни атак. Классические методы взлома (взлом парольной защиты). Современные методы взлома: перехват данных при их перемещении по каналам связи и перехват ввода с клавиатуры; мониторинг в графических интерфейсах; подмена системных утилит; нападения с использованием сетевых протоколов.

15 неделя (3 часа). Технологии безопасности в открытых системах. ИБ в ОИС — четырехуровневая модель ОИС. Специфика защиты ресурсов ОИС на примере интранет. Руководящие документы и стандарты по защите открытых сетей. Политика безопасности для интранет: иерархия политик и их разновидности; модели доверия; основные положения политики безопасности; процесс выработки политики безопасности, ее реализация и модификация. Сервисы безопасности. Средства обеспечения ИБ в сетях. Их назначение, особенности применения и примеры.

16 неделя (3 часа). Некоторые средства обеспечения ИБ в ОИС. Топология сети: физическая изоляция; изоляция протокола; выделенные каналы. Аутентификация в сетях: обычные и одноразовые пароли; серверы аутентификации. Адаптивное управление безопасностью. Методы отражения

вторжений. Системные и сетевые системы обнаружения вторжений (СОВ). Интеллектуальные и поведенческие СОВ, обнаружение вторжений/злоупотреблений; обнаружение аномалий/сопоставление с образцом. Применение и примеры систем. Системы предотвращения вторжений. Средства анализа защищенности (сканеры безопасности). Итоговые рекомендации по защите ОИС.

Вторая часть курса посвящена изучению виртуальных сетей и различных технологий, протоколов и средств их построения. Приведем календарный план курса.

1–2 недели (8 часов). Базовые сведения о виртуальных частных сетях. Различные подходы к определению VPN. Цели и задачи применения VPN-технологий. Преимущества VPN по сравнению с защищенными выделенными каналами связи и другими методами организации защищенной связи. Различные подходы к классификации VPN. Специфика построения VPN. Критерии, предъявляемые к VPN. Классификация VPN по решаемым задачам: Intranet VPN, Client\Server VPN, Extranet VPN, Remote Access VPN — определения, характерные черты и особенности использования. VPN в сетях общего пользования. Специфика использования VPN в сетях Frame Relay, ATM, X.25, TCP/IP. Туннелирование; механизм туннелирования как основа построения VPN. Функции протоколов, участвующих в процессе туннелирования. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных. Базовая схема VPN. VPN-агенты, их функции. Обработка входящих и исходящих пакетов. Варианты позиционирования и использования VPN-агентов. Основные виды VPN-каналов: защищенные, частные и промежуточные. Политики безопасности VPN. Интеграция VPN и дополнительных средств защиты: использование PKI, криптографические модули, аудит, антивирусные средства и т. д.

3–4 недели (8 часов). Варианты построения VPN. VPN на базе сетевой ОС, МЭ, маршрутизаторов, специализированного ПО, аппаратных средств — основные характеристики, сравнительный анализ. VPN на основе маршрутизаторов — назначение и основные характеристики, ОС, интерфейсы, команды конфигурирования портов. Межсетевые экраны. Назначение и функции МЭ. Основные компоненты МЭ. Принцип работы МЭ, варианты позиционирования МЭ. Основные типы МЭ: пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, МЭ экспертного уровня. Руководящий документ Гостехкомиссии по МЭ. Профили защиты на МЭ. Профиль защиты на средства построения VPN. Документ консорциума производителей VPN-продуктов VPNC. Классификация VPN согласно консорциуму VPN (VPNC) по степени защищенности: доверенные, защищенные и смешанные VPN.

5 неделя (4 часа). Стандартные протоколы создания VPN (транспортный уровень). Модель OSI и протоколы построения VPN. Стек протоколов TCP/IP и протоколы построения VPN. Транспортный уровень модели OSI — протоколы PPTP, L2F, L2TP. Протокол PPTP: функции, компоненты, сценарии работы, архитектура. Управляющее соединение и управляющие сообщения. Инкапсуляция данных при передаче. Аутентификация, контроль доступа и шифрование. Настройка VPN на базе протокола PPTP в среде Windows 2000. Протокол L2F: основные функции и характеристики протокола. Протокол L2TP: основные функции и характеристики протокола. Управление L2TP-туннелем. Управляющие сообщения L2TP. Обработка входящих и исходящих данных. Настройка VPN на базе протокола L2TP в среде Windows 2000.

6–8 недели (12 часов). Стандартные протоколы создания VPN (сетевой уровень). Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP. Инкапсуляция данных в транспортном и туннельном режимах работы. Форматы заголовков. Защищаемые поля IP-заголовка

при использовании AH в транспортном режиме. Обработка исходящих (поиск SA, генерация порядкового номера, вычисление ICV и шифрование данных, фрагментация) и входящих (сборка, поиск SA, проверка порядкового номера, проверка ICV, расшифрование, проверка на соответствие записи в SPD) пакетов. Использование комбинированных криптографических алгоритмов в ESP. Особенности использования расширенных порядковых номеров. Защита от повторной передачи пакетов. Согласование параметров безопасности с использованием протокола IKE. Порядок обмена сообщениями IKE. Сообщения IKE_SA_INIT для согласования параметров безопасности IKE_SA и обмена по протоколу Диффи-Хеллмана. Сообщения IKE_AUTH для аутентификации и установления CHILD_SA для защиты данных с помощью AH или ESP. Сообщения CREATE_CHILD_SA для согласования дополнительных CHILD_SA в рамках данной IKE_SA. Сообщения INFORMATIONAL для сообщения информации о текущем состоянии или ошибках. Детали работы протокола (согласование версий протокола, использование порядковых номеров, генерирование ключевого материала, обработка ошибок и т. д.). Форматы основного заголовка IKE и заголовков сообщений. Протокол SKIP: основные функции и детали протокола. L2TP/IPSec-инкапсуляция данных. Протокол MPLS.

9–10 недели (8 часов). Стандартные протоколы создания VPN (сеансовый уровень). Протокол SSL: архитектура протокола, обеспечение ИБ, свойства канала, протокол диалога и протокол записей, средства установления туннелей. Протокол TLS: составляющие протоколы, цели протокола, преимущества и недостатки. Протокол SOCKS: особенности, использование, схема установления соединения. Сравнение функциональных возможностей протоколов построения VPN. Уязвимость VPN. Рекомендации специалистов по выбору решений для построения VPN.

11–12 недели (8 часов). Базовые сведения о виртуальных локальных сетях. Виды виртуальных локальных сетей: VLAN с группировкой портов, VLAN с маркированными кадрами, VLAN на основе протоколов высокого уровня. Этапы перехода к VLAN. Протокол VTP. Безопасность в VLAN. Преимущества VLAN.

Семилетний опыт преподавания этого базового для всей специализации учебного курса позволил разработать специальное методическое обеспечение [1] и подготовить в поддержание занятий сначала несколько учебных пособий с грифом Минобразования РФ и УМО [2–4], а в 2006 г. издать первую часть учебника с аналогичным названием с грифом Минобрнауки РФ [5]. Вторая часть учебника выходит весной 2008 г. [6]. Также в МИФИ издан ряд конспектов лекций по отдельным разделам курса (например, удаленным атакам, угрозам и уязвимостям, мониторингу безопасности, технологиям безопасности, сканерам защищенности, межсетевым экранам и т. п.) в виде презентаций из слайдов, используемых преподавателями во время проведения занятий (серия «Учебная книга факультета “Информационная безопасность” МИФИ». Выпуски 1, 6–20).

4. Лабораторный практикум базовой дисциплины

Важно отметить, что подготовка кадров по специализации «Безопасность открытых информационных систем» предполагает большой объем практических лабораторных работ, выполняемых студентами в рамках названных учебных курсов.

Для закрепления теоретических знаний в обеих частях базового курса специализации предусмотрены лабораторные работы. Поскольку в 2002 г. на факультете «Информационная безопасность» совместно с ООО НТЦ «Электрон-сервис», при поддержке представительства фирмы Microsoft в Москве и при участии компании «Крок» был создан учебно-научный комплекс «Технологии безопасности» [2] и за 7 лет существования как самого учебного курса, так и этого комплекса накоплен богатый опыт проведения практических работ, был собран целый банк работ, из которого можно выбирать наиболее актуальные на текущий момент задания. В каждой части курса предусмотрено по 4 четырехчасовых лабораторных работы. В банке работ находятся, в частности, следующие варианты практикумов:

· «Эмуляция работы сетевых протоколов»;
· «Эмуляция работы защищенных сетевых протоколов»;
· «Эмуляция конкретных видов атак»;
· «Создание интерфейсов для эмуляции работы средств защиты»;
· «Изучение зависимости между топологией сети и атаками»;
· «Изучение зависимости между используемой средой передачи (Ethernet, FastEthernet, FDDI, ATM…) и атаками»;
· «Изучение особенностей атак для оптоволоконных линий связи»;
· «Изучение особенностей атак при доступе в Internet»;
· «Изучение атак на сетевое аппаратное обеспечение»;
· «Изучение уязвимости и защиты Web-серверов и приложений»;
· «Изучение уязвимостей сетевых сервисов и команд»;
· «Исследование атак на электронный документооборот»;
· «Криптозащита. Электронная цифровая подпись. PKI — инфраструктура открытых ключей»;
· «Изучение атак на межсетевые экраны»;
· «Изучение атак на агентов-«посредников» (proxy) и их обнаружение»;
· «Изучение уязвимостей архитектуры клиент/сервер»;
· «Изучение уязвимостей баз данных и систем управления базами данных»;
· «Изучение основных средств защиты информации в сетях — средства защиты от НСД»;
· «Изучение основных средств защиты информации в сетях — межсетевые экраны»;
· «Изучение основных средств защиты информации в сетях — средства адаптивного управления»;
· «Изучение основных средств защиты информации в сетях — антивирусы»;
· «Изучение основных средств защиты информации в сетях — средства создания виртуальных частных сетей (протоколы, маршрутизаторы, межсетевые экраны, специализированное ПО)»;
· «Изучение основных средств защиты информации в сетях — средства управления политикой безопасности»;
· «Изучение средств шифрования файлов и сеансов связи»;
· «Изучение сетевых систем обнаружения вторжений»;
· «Изучение систем обнаружения вторжений на хостах»;
· «Изучение атак на системы обнаружения вторжений»;
· «Изучение системных сканеров уязвимостей»;
· «Изучение сетевых сканеров уязвимостей»;
· «Исследование защитных сервисов: тесты на возможность проникновения»;
· «Изучение атак на приложения (сетевое прикладное ПО) и защита приложений»;
· «Уязвимость и защита рабочих станций»;
· «Разработка собственных средств и методов защиты».

При этом объектами лабораторных исследований выступают:
· отдельные компьютеры/группа компьютеров во внутренней сети, с конкретной аппаратной платформой и установленным ПО — основным (например, ОС) и прикладным (сетевым);
· отдельные компьютеры/группа компьютеров во внешней среде, связь с которыми осуществляется через Internet, с конкретным аппаратным и программным обеспечением (далее — АО и ПО);
· сетевое АО и ПО;
· сетевые протоколы;
· сетевые службы;
· стандарты, правовые и нормативные документы.

А объектами при изучении методов защиты являются:

· средства обнаружения вторжений;

· средства анализа защищенности программно-аппаратного обеспечения отдельного компьютера/группы компьютеров;

· средства мониторинга сетевой безопасности и анализа трафика;

· средства защиты информации (например, межсетевые экраны, средства шифрования и т. п.);

· средства аудита файловой системы;

· средства разграничения доступа;

· средства защиты прикладных программ;

· политики безопасности;

· новые, разработанные обучающимися технологии и методики защиты информации;

· информационная база документов, регламентирующих действия по обеспечению информационной безопасности.

Это достигается следующими методами лабораторных исследований:

· имитация действий злоумышленника при реализации атак;

· нахождение уязвимостей в системах посредством их сканирования (проверка известных слабых местах и поиск новых «лазеек»);

· эксперименты со средствами защиты и обнаружения НСД для определения их функциональных возможностей и выработки рекомендаций по их установке и усовершенствованию;

· контроль информационных потоков в сети за счет анализа трафика;

· оценка защищенности компьютеров, сетей, сервисов, протоколов, АО и ПО по определенным методикам и в соответствии с российскими стандартами и руководящими документами;

· тестирование политик безопасности и новых методик защиты для определения их полноты и обоснованности;

· анализ документов, регламентирующих информационную безопасность.

Применительно конкретно к изучению безопасности открытых систем это означает:

· проверка описанных в литературе атак;

· обнаружение вторжений и ликвидация их последствий;

· обнаружение уязвимостей установленного на отдельном компьютере или в сети ПО и АО;

· управление системами разграничения доступа к информационным и сетевым ресурсам систем;

· разработка политики безопасности системы и определение мер ее реализации;

· оценка защищенности функционирующих систем и выработка рекомендаций по ее усилению;

· построение, установка, настройка и администрирование средств защиты и «заплат» (patches) для уже работающего в системе ПО и АО.

В 2007/08 уч. г. реализовывались работы, представленные в табл. 1 и табл. 2 по первой и второй частям курса соответственно.

В настоящее время накопленный во время проведения лабораторных работ опыт находится в стадии оформления в виде подробных лабораторных практикумов.

Таблица 1. Лабораторные работы первой части курса «Информационная безопасность открытых систем»

Наименование лабораторного практикума	**Состав используемого оборудования и ПО (учебно-лабораторного стенда)**	**Наименование лабораторных работ, входящих в состав практикума**
1.«Информационная безопасность технологии Internet». Назначение: изучение технологий, протоколов, сервисов и их типичных	АО, объединенных в локальную сеть и имеющих подключение к Internet:	1.1. Знакомство с организацией и работой открытых сетей (на примере глобальной

уязвимостей для открытых информационных систем на примере сети Internet, а также знакомство с основными информационными ресурсами по информационной безопасности, представленными в сети Internet. Цель применения: получение практических навыков работы в сети Internet и ее основными сетевыми сервисами (типа ftp, telnet и другими), а также навыков осуществления поиска информации по уязвимостям в информационных ресурсах сети Internet.	компьютерный класс в составе: 12 компьютеров IBM/PC с процессором AMD Athlon 300 и выше; ПО: виртуальные машины VMWare с ОС Microsoft Windows и Linux.	сети Internet), их протоколами и сервисами (ftp, telnet и другими). 1.2.Изучение уязвимостей некоторых сервисов. 1.3.Поиск информации по уязвимостям.
2. *«Современные методы взлома сетей и их характерные признаки».* Назначение: ознакомление с современными методами взлома сетей и их характерными признаками, позволяющими своевременно обнаруживать и прерывать несанкционированную деятельность злоумышленников. Цель применения: получение практических компетенций по выявлению характерных признаков современных методов взлома сетей на примере таких атак, как прослушивание сетевого трафика, сканирования, «отказ в обслуживании», подмена сетевых объектов, получение удаленного контроля над объектом в сети и т. п.	АО, объединенных в локальную сеть и имеющих подключение к Internet: компьютерный класс в составе: 12 компьютеров IBM/PC с процессором AMD Athlon 300 и выше; ПО: виртуальные машины VMWare с ОС Microsoft Windows и Linux.	2.1.Предварительный сбор информации о системе-жертве. 2.2.Поиск конфиденциальной информации на узлах. «Охота за сокровищами». 2.3.Прослушивание сетевого трафика. 2.4.Знакомство со средствами идентификации сервисов и сетевых устройств. 2.5.Определение топологии сети. 2.6.Взлом паролей в ОС UNIX. Программы подбора паролей. 2.7.Определение операционной системы удаленного хоста 2.8.Реализация атаки SYN-flooding. 2.9.Изучение атак «отказ в обслуживании» 2.10.Удаленное администрирование. Троянский конь
3. *«Продукты «Гриф» и «Кондор» компании Digital Security».* Назначение: приобретение знаний в области анализа рисков информационной безопасности и разработки и управления политикой информационной безопасности для информационных систем. Цель применения: получение практических навыков работы с программным комплексом Digital Security Office 2006 компании Digital Security, включающим два программных продукта – «Гриф», осуществляющий анализ и управление рисками информационной безопасности с помощью модели угроз и уязвимостей и модели информационных потоков, и «Кондор», осуществляющий разработку и управление политикой	АО, объединенное в локальную сеть и имеющее подключение к Internet: компьютерный класс в составе: 12 компьютеров IBM/PC с процессором AMD Athlon 300 и выше; ПО: ОС Microsoft Windows; ПО «Гриф»; ПО «Кондор».	3.1.Анализ модели угроз и уязвимостей. 3.2.Анализ модели информационных потоков. 3.3.Разработка и управление политикой безопасности ИС.

информационной безопасности для информационной системы на основе ISO 17799.		
4. *«Знакомство с продуктами обеспечения сетевой безопасности фирмы Computer Associates».* Назначение: ознакомление с современными средствами обеспечения безопасности корпоративной вычислительной сети, реализующими централизованный и комплексный подход к решению задач ее защиты. Цель применения: получение практических навыков работы со средствами сетевой защиты eTrust Computer Associates в составе: 1) eTrust Access Control для управления доступом; 2) eTrust Single-Sign-on для управления аутентификацией пользователей; 3) eTrust Policy Compliance CA для поиска уязвимостей, анализа и мониторинга безопасности в ОС Windows; 4) eTrust Audit для осуществления сетевого аудита; 5) eTrust Security Command Center для управления сетевой безопасностью на уровне корпорации и 6) eTrust Network Forensics CA для анализа сетевой активности, сбора сведений о сетевых атаках и непрерывного контроля сетевых процессов.	АО, объединенное в локальную сеть и имеющее подключение к Internet: компьютерный класс в составе: 12 компьютеров IBM/PC с процессором AMD Athlon 300 и выше; ПО: ОС Microsoft Windows; ПО eTrust Access Control; ПО eTrust Single-Sign-on; ПО eTrust Policy Compliance CA; ПО eTrust Audit; ПО eTrust Security Command Center; ПО eTrust Network Forensics CA.	4.1.Управление доступом при помощи eTrust Access Control. 4.2.Использование eTrust Single-Sign-on для управления аутентификацией пользователей. 4.3.Поиск уязвимостей, анализа и мониторинга безопасности в ОС Windows с помощью eTrust Policy Compliance CA. 4.4.Изучение технологии сетевого аудита на примере е Trust Audit. 4.5.Технология управления сетевой безопасностью на примере eTrust Security Command Center. 4.6. Анализ сетевой активности, сбор сведений о сетевых атаках и непрерывный контроль сетевых процессов с помощью eTrust Network Forensics CA.

Таблица 2. Лабораторные работы второй части курса «Информационная безопасность открытых систем»

Наименование лабораторного практикума	**Состав используемого оборудования и ПО (учебно-лабораторного стенда)**	**Наименование лабораторных работ, входящих в состав практикума**
1. *«Межсетевые экраны ФПСУ-IP».* Назначение: ознакомление с программно-аппаратным комплексом межсетевым экраном ФПСУ-IP компании «АМИКОН», предназначенным для обеспечения защиты от несанкционированного доступа методом реализации межсетевого экранирования и создания VPN-туннелей с целью создания в открытой сети защищенных областей с ограниченным доступом и обеспечением защищенной передачи данных между защищенными областями. Цель применения: получить практические компетенции применения МЭ	АО, представляющее собой фрагмент глобальной вычислительной сети и пяти локальных сетей: компьютерный класс в составе: 9 компьютеров IBM/PC с процессором Intel Celeron 533 и выше; 6 аппаратных комплексов ФПСУ-IP; 3 комплексов ФПСУ-IP/Клиент; 1 плата «Аккорд 5MX» фирмы ОКБ САПР; 4 маршрутизатора Cisco; 5 концентраторов; ПО: ОС Windows 2000; ОС MS-DOS6 и выше; ПО	1.1. Установка программного обеспечения комплекса ФПСУ-IP. 1.2. Установка и настройка удаленного администратора ФПСУ-IP. 1.3. Типовые схемы включения ФПСУ-IP. 1.4. Использование ФПСУ-IP для создания VPN-туннелей. 1.5.Настройка работы ФПСУ при

ФПСУ-IP с целью фильтрации трафика и организации VPN-туннелей в локальных и глобальных сетях.	комплекса ФПСУ-IP; ПО комплекса ФПСУ-IP/Клиент.	использовании нескольких ключевых групп. 1.6. Настройка работы ФПСУ-IP/Клиента.
2. *«Сетевые продукты VipNet (Инфотекс)».* Назначение: ознакомление с технологией и сетевыми программными продуктами ViPNet компании «Инфотекс», предназначенными для создания целостной системы доверительных отношений и безопасного функционирования технических средств и информационных ресурсов корпоративной сети организации, взаимодействующей также и с внешними техническими средствами и информационными ресурсами. Цель применения: получение практических компетенций в применении системы защиты информации ViPNet для защиты конфиденциальности, подлинности и целостности любого вида трафика, передаваемого между любыми компонентами сети, а также защиты управляющего трафика для систем и средств удаленного управления объектами сети от возможных атак из глобальной или корпоративной сети.	АО, объединенное в локальную сеть: компьютерный класс в составе: 13 компьютеров IBM/PC с процессором AMD Athlon 300 и выше; ПО: ОС Windows 2000; ViPNet [Администратор]; ViPNet [Координатор]; ViPNet [Клиент].	2.1.Изучение программного обеспечения. 2.2.ViPNet Администратор. 2.3.Первоначальное развертывание защищенной сети. 2.4.Модификация защищенной сети. 2.5.Организация межсетевого взаимодействия.
3. *«Способы создания виртуальных частных сетей и знакомство с работой защищенных сетевых протоколов в ОС Windows 2000».* Назначение: Исследование одного из способов создания виртуальных частных сетей средствами ОС Microsoft Windows 2000 на примере различных защищенных сетевых протоколов, поддерживаемых названной ОС. Цель применения: Получение практических навыков настройки параметров защищенных сетевых протоколов построения виртуальных частных сетей – PPTP, L2TP, IPSec и SSL/TLS – для клиента и сервера, работающих под управлением ОС Microsoft Windows 2000/XP.	АО, объединенное в локальную сеть и имеющее подключение к Internet: компьютерный класс в составе: 12 компьютеров IBM/PC с процессором AMD Athlon 300 и выше; ПО: ОС Microsoft Windows; пакет прикладных программ и электронный учебник ZSPS (разработка МИФИ), эмулирующий настройку защищенных сетевых протоколов в среде Windows 2000.	3.1.Протокол PPTP в ОС Windows. 3.2.Протокол L2TP в ОС Windows. 3.3.Протокол IP SECURITY (IPSec) в ОС Windows. 3.4.Протокол SSL/TLS в ОС Windows.

5. Опыт реализации специализации

Специализация реализуется в МИФИ на факультете «Информационная безопасность» с момента утверждения, т. е. с 2002 г. За истекшее время по данной специализации выпущено 240 специалистов по защите информации (начиная с 2005 г.).

Специфика полученных во время обучения знаний и навыков отражается не только в учебном плане специализации, но и в темах дипломных проектов. Приведем некоторые из них:

· «Система аудита ИБ на основе специальных продуктов»;

· «Средства и методы противодействия DoS-атакам»;

· «Разработка документального обеспечения для системы менеджмента ИБ коммерческого банка»;

· «Внутренний аудит СМИБ по стандарту ISO 27001:2005»;
· «Создание системы управления ИБ на основе оценки рисков ИБ банка»;
· «Автоматизированное рабочее место администратора ИБ компьютерной сети федерального органа власти»;
· «Разработка процесса управления инцидентами ИБ в соответствии с требованиями стандарта ISO 27001:2005»;
· «Разработка и исследование виртуальных частных сетей на основе сертифицированных средств криптографической защиты информации»;
· «Защита распределенной корпоративной сети с использованием технологии VPN»;
· «Разработка архитектуры и алгоритмов системы обнаружения вторжений на основе иммунологического подхода»;
· «Сопряжение системы управления средствами антивирусной защиты с системой централизованного мониторинга средств защиты информации»;
· «Проектирование экспертных систем анализа защищенности локальных вычислительных сетей»;
· «Разработка подсистемы межсетевого экранирования корпоративной информационной системы организации»;
· «Разработка и реализация интерактивного загрузочного диска для тестирования настроек и функционирования межсетевого экрана»;
· «Обеспечение ИБ электронных транзакций в системе Интернет-платеж»;
· «Разработка защищенного портала электронной библиотеки кафедры»;
· «Разработка системы защиты веб-приложений»;
· «Разработка статистического анализатора активности пользователей веб-ресурса»;
· «Модель и алгоритмическое обеспечение системы защищенной электронной почты на базе идентификационных криптосистем»;
· «Разработка системы криптографической защиты сетевого трафика для ОС Windows».

Как видно из приведенных названий, подготовка работ была бы невозможна без базовых знаний, полученных в рамках специализации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Милославская Н. Г., Тимофеев Ю. А., Толстой А. И.* Уязвимость и методы защиты в глобальной сети Internet. М., 1997. – 236 с.
2. *Милославская Н. Г., Толстой А. И.* Интрасети: доступ в Internet, защита. Учебное пособие для вузов. М., 2000. — 527 с.
3. *Милославская Н. Г., Толстой А. И.* Интрасети: обнаружение вторжений. Учебное пособие для вузов. М., 2001. — 587 с.
4. *Запечников С. В., Милославская Н. Г., Толстой А. И.* Основы построения виртуальных частных сетей. М., 2003. – 249 с.
5. *Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В.* Информационная безопасность открытых систем. Учебник для вузов. В 2-х томах. М., 2006. Т. I: Угрозы, уязвимости, атаки и подходы к защите. — 536 с.
6. *Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В.* Информационная безопасность открытых систем. Учебник для вузов. В 2-х томах. М., 2008. Т. II: Средства защиты в сетях. — 558 с.
7. *Борискин Д. А., Милославская Н. Г., Толстой А. И., Ушаков Д. В.* Концепция создания учебно-исследовательской лаборатории «Безопасность вычислительных сетей» // Сборник трудов научно-практической конференции «Информационная безопасность». Таганрог, 28–31 мая 2002.