Чернова Е.В., Старков А.Н., Доколин А.С.

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ПРИМЕНЕНИЯ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ПОДГОТОВКЕ КОНКУРЕНТОСПОСОБНОГО ИТ-СПЕЦИАЛИСТА

ФГБОУ ВПО «Магнитогорский государственный университет»

Введение

Повсеместное внедрение информационных технологий во все сферы человеческой деятельности приводит к повышению актуальности проблем, связанных с информационной безопасностью и защитой информации. Под информационной безопасностью организации принято понимать целенаправленную систематическую деятельность подразделений и должностных лиц с использованием определенных средств для достижения состояния защищенности информационной среды организации и обеспечение ее нормального функционирования и развития. Для наилучшего обеспечения защиты данных организации необходим комплексный и системный подход к построению реализации политики информационной безопасности с внедрением программно-технических средств, а так же работой с кадрами. Все эти мероприятия должен обеспечивать специальный отдел по обеспечению информационной безопасности, с профессиональными сотрудниками, получившими образование в данной области и обладающими навыками обеспечения защиты безопасности, построения и реализации политики информационной безопасности в организации.

Зачастую выпускникам вузов приходится дополнительно проходить обучение на специализированных курсах от разработчиков узконаправленного программного обеспечения, что требует как временных, так и финансовых затрат. Было бы правильно сразу в вузе готовить ИТ-специалиста в области информационной безопасности с использованием наиболее распространенных программных средств.

1. Особенности подготовки специалиста по информационной безопасности

По прогнозам аналитиков, значимость специалистов по информационной безопасности будет расти. Наша страна постепенно приближается к западной модели управления – где руководители структурных подразделений, отвечающих за информационную безопасность компании, входят в совет директоров и часто становятся вторым-третьим лицом в компании. Заказчиками специалистов по информационной безопасности являются: федеральные органы государственной власти и управления РФ; органы государственной власти субъектов РФ; государственные учреждения, организации и предприятия; оборонная промышленность; органы местного самоуправления; учреждения, организации и предприятия негосударственной формы собственности.

Подготовка специалистов в области информационной безопасности в последнее время жизненно важной для существования предприятия. Риски для компании, связанные с различными воздействиями на ее информационную инфраструктуру, являются неотъемлемой частью процесса управления непрерывностью бизнеса. Однако, как утверждает Игорь Семенихин, «при этом зачастую, особенно в небольших компаниях, в вопросах защиты информации руководители полагаются на рядовых сотрудников, не имеющих соответствующей квалификации. Отдельные менеджеры считают, что справиться с задачей обеспечения информационной безопасности компании может практически любой человек, знакомый с ИТ, способный установить и настроить необходимые программные и аппаратные средства. Однако большая часть проблем в данной области не решается только путем применения программно-аппаратных средств – большое значение имеют организационные меры. Умение взглянуть на проблему защиты информации и обеспечения информационной безопасности в целом требует от сотрудников не только знания технологий, но и менеджерских навыков в данной области». [2]

Вопрос конкурентоспособности выпускника вуза является краеугольным камнем всей системы высшего образования. Не секрет, что на сегодняшний день в системе образования есть ряд проблем, которые нельзя не учитывать при построении образовательной траектории: уменьшение количества абитуриентов, рост и вариативность требований работодателей к содержанию подготовки будущего работника, изменения на рынке труда. На данный момент подготовкой специалистов в области информационной безопасности занимается большое количество высших учебных заведений страны. Каждый ВУЗ разрабатывает свой курс, в соответствии требуемым стандартам. В основном ведется подготовка специалистов в таких областях как:

- теория информации и теория сложности;
- теория моделирования;
- теория искусственного интеллекта;
- теория надежности программного обеспечения;
- теория методов и средств защиты программных комплексов;
- операционных систем, баз данных и знаний, сетей и других видов распределенных систем;
- углубленная подготовка в области систем телекоммуникаций.

Какие-то высшие учебные заведения полностью охватывают данные области, какие-то частично.

Большинство изучаемых областей основано на усвоении огромного количества теоретического материала, что, несомненно, хорошо влияет на подготовку будущих специалистов. Получив такие глубокие теоретические знания, специалист сможет справиться с поставленной ему задачей. Однако, с другой стороны теоретические знания, не подкрепленные практикой, оставляют брешь в подготовке специалистов данной области. Практическая составляющая курса по информационной безопасности имеет большое значение. Основным направлением при создании практических материалов является программное обеспечение по информационной безопасности. Работа с программными средствами на практических занятиях подготовит специалиста к большинству

возможных угроз информации, а так же, позволит грамотно нейтрализовать их, опираясь на приобретенные практические знания в области специализированного программного обеспечения.

В подобных условиях, особое место в системе подготовки ИТ-специалиста занимает академическое партнерство с ведущими компаниями как российскими, так и международными. Академическое партнерство – это способ сотрудничества на образовательном уровне между разработчиком программного обеспечения и вузом. Компания-партнер предоставляет вузу программные средства и образовательные материалы, для того, чтобы студенты могли освоить тот или иной программный продукт в процессе изучения определенной, взаимосвязанной дисциплины. Выгода от партнерских программ очевидна как для самих компаний, так и для вузов. Вузы получают возможность бесплатно и при техническом сопровождении изучать дорогостоящие программные средства, получать методические материалы для углубленной работы с ними и давать возможность студентам получать дополнительные ИТ-навыки. Как считает Г.Н. Смородин: «Поскольку корпорация является публичной компанией, то можно утверждать, что присутствие академического партнера на рынке образовательных услуг сказывается на курсовой стоимости акций корпорации. Активность академического партнерства непосредственно воздействует на имидж корпорации и на узнаваемость ее бренда. Помимо этого формируется организационная структура Партнерства и накапливается его интеллектуальная собственность» [1]. Таким образом, при минимальных затратах компании получают на местах готовых специалистов, ориентированных на использование именно их программного средства, а не каких-либо еще. Академическое партнерство производителя и вуза осуществляется на безвозмездной основе, что позволяет образовательному учреждению при минимальных затратах получить доступ к максимальному количеству разнообразных программных средств, а так же иметь возможность консультироваться с ведущими

специалистами данных компаний, разрабатывать практические задания с учетом особенностей конкретных программных средств.

Подготовка специалистов в области информационной безопасности предполагает изучение ряда дисциплин, определяющих облик профессионала, готового работать в области информационной безопасности: «Администрирование и безопасность компьютерных систем»; «Администрирование компьютерных сетей (CISCO)»; «Алгоритмы и структуры данных»; «Архитектура компьютера»; «Архитектура корпоративных информационных систем»; «Базы данных»; «Вычислительные системы, сети и телекоммуникации»; «Интеллектуальные информационные системы»; «Информационная безопасность»; «Информационные системы»; «Информационные системы и технологии»; «Информационный менеджмент»; «Компьютерные сети, Интернет и мультимедиа технологии»; «Криптографические методы защиты информации»; «Криптографические методы и средства обеспечения информационной безопасности»; «Мировые информационные ресурсы»; «Операционные системы»; «Организационное обеспечение информационной безопасности»; «Построение компьютерных сетей для малого бизнеса (CISCO)»; «Программирование»; «Программно-аппаратная защита информации»; «Программно-аппаратные средства обеспечения информационной безопасности»; «Программное обеспечение ЭВМ»; «Программно-техническое обеспечение информационной безопасности»; «Проектирование информационных систем»; «Разработка Интернет-ресурсов»; «Разработка приложений»; «Теория информационной безопасности и методологии защиты информации»; «Управление информационной инфраструктурой»; «Управление ИТ-сервисами и контентом»; «Хранилища данных».

В данной работе мы предлагаем вариант разработки практического курса по информационной безопасности с применением различных программных средств, на базе которых студент сможет полностью отладить механизм обеспечения информационной безопасности от построения безопасной сети до

разработки политики информационной безопасности. Следует отметить, что для того, чтобы студенты получили компетенции, позволяющие им обеспечивать защиту информации и информационную безопасность на разных уровнях, а также навыки работы в критических ситуациях – в момент атаки, отказа оборудования или других непредвиденных обстоятельствах, необходимо планировать изучение дисциплины «Информационная безопасность» в тесной интеграции с другими дисциплинами. Особенностью нашей разработки является межпредметная связь данного курса с дисциплинами, посвященными построению и администрированию сетей.

В частности, курс информационной безопасности тесно связан с дисциплинами «Построение компьютерных сетей для малого бизнеса (CISCO)» и «Администрирование компьютерных сетей (CISCO)», читаемыми в рамках Сетевой академии Cisco, открытой на базе университета. В рамках данных курсов подробно рассматриваются вопросы, связанные с информационной безопасностью и защитой информации. Изучаются темы «Основы безопасности», «Обеспечение безопасности проводных и беспроводных сетей». Рассматриваются вопросы сетевых угроз (риски вторжения, источники вторжения, социотехника и фишинг), методы атак, вопросы политики безопасности, использования межсетевых экранов, способы обеспечения безопасности локальных сетей (различные способы ограничения доступа в сеть, шифрования в сети, фильтрации трафика) и др. Параллельно в рамках курса «Информационная безопасность» рассматриваются студентами вопросы идентификации и аутентификации, управления доступом, протоколирования и аудита, шифрования, контроля целостности, экранирования, анализа защищенности, обеспечения отказоустойчивости, обеспечения безопасного восстановления, туннелирования, управления, средств защиты информации от несанкционированного доступа, средств аппаратной поддержки, защиты от вмешательства посторонних лиц, антивирусной защиты и т.д.

2. Анализ специализированного программного обеспечения

Практический курс построен с применением следующих программных средств:

1. «Контур информационной безопасности SearchInform»

Позволяет выявлять утечки конфиденциальной информации и персональных данных через электронную почту; ICQ; голосовые и текстовые сообщения Skype, посты на форумах или комментарии в блогах; внешние устройства (USB/CD); FTP; файл-серверы; ноутбуки, в том числе отключенные от корпоративной сети; документы, отправляемые на печать; а также появление конфиденциальной информации на компьютерах пользователей. Ответственные сотрудники оперативно оповещаются о нарушениях политики безопасности. Расширенные поисковые возможности позволяют эффективно защищать конфиденциальные данные при минимальных трудозатратах на анализ информационных потоков.

При помощи данного программного средства студенты научатся правильно отслеживать информацию внутри организации, выявлять небезопасных сотрудников, противодействовать угрозам извне.

2. «Xspider»

Программное средство для определения уязвимостей сети. После того, как студенты опишут и разработают всю сетевую инфраструктуру, они проведут анализ уязвимостей, построенной ими сети при помощи данного программного средства.

Приведем краткий перечень основных возможностей, являющихся базовыми для обеспечения высокого качества и надежности в поиске уязвимостей программным средством XSpider:

- Полная идентификация сервисов на случайных портах

Дает возможность проверки на уязвимость серверов со сложной нестандартной конфигурацией, когда сервисы имеют произвольно выбранные порты

•Эвристический метод определения типов и имен серверов (HTTP, FTP, SMTP, POP3, DNS, SSH) вне зависимости от их ответа на стандартные запросы

Служит для определения настоящего имени сервера и корректной работы проверок в тех случаях, если конфигурация WWW-сервера скрывает его настоящее имя или заменяет его на другое

•Обработка RPC-сервисов (Windows и *nix) с их полной идентификацией

Обеспечивает возможности определения RPC-сервисов и поиска уязвимостей в них, а также определения детальной конфигурации компьютера в целом

•Проверка слабости парольной защиты

Производится оптимизированный подбор паролей практически во всех сервисах, требующих аутентификации, помогая выявить слабые пароли

• Глубокий анализ контента WEB-сайтов

Анализ всех скриптов HTTP-серверов (в первую очередь, пользовательских) и поиск в них разнообразных уязвимостей: SQL инъекций, инъекций кода, запуска произвольных программ, получения файлов, межсайтовый скриптинг (XSS), HTTP Response Splitting.

• Анализатор структуры HTTP-серверов

Позволяет осуществлять поиск и анализ директорий доступных для просмотра и записи, давая возможность находить слабые места в конфигурации

• Проведение проверок на нестандартные DoS-атаки

Существует возможность включения проверок "на отказ в обслуживании", основанных на опыте предыдущих атак и хакерских методах

• Специальные механизмы, уменьшающие вероятность ложных срабатываний

В различных видах проверок используются специально под них разработанные методы, уменьшающие вероятность ошибочного определения уязвимостей

• Ежедневное добавление новых уязвимостей и проверок

3. «Код безопасности: Инвентаризация 2.2»

Программный комплекс, предназначенный для сбора, обработки и систематизации информации о программном и аппаратном обеспечении, установленном на компьютерах и серверах в локальной вычислительной сети. С его помощью студенты получат практические навыки инвентаризации устройств и программных средств в сети, что поможет им в правильной настройке политики информационной безопасности. Возможности программного средства:

Инвентаризация программного и аппаратного обеспечения:

- В сетях с наличием Active Directory
- В одноранговых сетях (workgroup)
- Компьютеров не входящих в сеть

Сбор информации. Методы:

- Реестр
- WMI
- HDD

4. «Код безопасности: Security Studio Honeypot Manager»

Honeypot Manager – это проактивное средство обнаружения хакерских вторжений и несанкционированного доступа к информации, основанное на имитации данных и анализе обращений пользователей к имитируемым прикладным программам и сетевым сервисам.

Основная задача системы – регистрация действий злоумышленника и сигнализирование о них с целью нейтрализации угрозы получения доступа (чтение, копирование, изменение) к реальным данным на реальных системах хранения данных. Honeypot Manager имитирует систему хранения данных с помощью специальных ловушек (сенсоров), отслеживает активность на ней и уведомляет о фактах НСД к этим данным.

Таким образом, студент при помощи данного программного средства получит информацию о том, кто пытается получить доступ к системе и пытается ли вообще, а также может определить, перепутал ли сотрудник имя реального сервера и случайно попал на ловушку или действовал преднамеренно

и в сети действительно есть нарушители, пытающиеся найти сервера или службы, работающие с данными, представляющими ценность для компании.

5. «Код безопасности: Secret Net»

Secret Net является сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы в соответствие с требованиями политики информационной безопасности

Ключевые возможности СЗИ от НСД Secret Net:

- Аутентификация пользователей.
- Разграничение доступа пользователей к информации и ресурсам автоматизированной системы.
- Доверенная информационная среда.
- Контроль утечек и каналов распространения конфиденциальной информации.
- Контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации.
- Централизованное управление системой защиты, оперативный мониторинг, аудит безопасности.
- Масштабируемая система защиты, возможность применения Secret Net (сетевой вариант) в организации с большим количеством филиалов.

6. «Антивирус Касперского»

Антивирус Касперского – это решение для базовой защиты вашего компьютера от вредоносных программ. Продукт защищает вас от основных видов угроз, не замедляя работу системы.

- Гибридная защита мгновенно реагирует на новые угрозы.
- Защита от эксплойтов не позволяет вредоносным программам
- использовать уязвимости в системе и приложениях.
- Мониторинг активности выявляет подозрительные действия программ и позволяет отменить вредоносные изменения.

- Мгновенная проверка репутации программ и веб-сайтов.
- Веб-фильтр блокирует опасные веб-сайты.
- Анти-Фишинг обеспечивает защиту ваших личных данных.
- Диск аварийного восстановления позволяет восстановить систему в случае заражения.

При помощи этого программного средства студент изучит теорию о работе вирусов, методов борьбы с ними.

7. Cisco

Компания разработала новаторские образовательные программы в области информационно-коммуникационных технологий (ИКТ), которые соответствуют требованиями Федерального государственного образовательного стандарта (ФГОС) и поэтому могут быть без особых проблем включены в учебные программы по подготовке бакалавров и магистров в области информационных технологий и телекоммуникаций. Видения Cisco по модернизации учебных программ отразилось в фундаментальных курсах CCNA Discovery и CCNA Exploration, учащих планированию, проектированию, монтажу и настройке современных компьютерных сетей. Эти курсы включают теоретические и практические занятия, в ходе которых студенты учатся устанавливать и конфигурировать коммутаторы и маршрутизаторы, осваивают базовые методы поиска и устранения неполадок, узнают о способах повышения производительности и защищенности сети, и т.п.

8. Cisco Packet Tracer

Данный программный продукт разработан компанией Cisco и рекомендован использоваться при изучении телекоммуникационных сетей и сетевого оборудования.

Packet Tracer включает следующие особенности:

- моделирование логической топологии: рабочее пространство для того, чтобы создать сети любого размера на CCNA-уровне сложности;
- моделирование в режиме реального времени;
- режим симуляции;

•моделирование физической топологии: более понятное взаимодействие с физическими устройствами, используя такие понятия как город, здание, стойка и т.д.;

•улучшенный GUI, необходимый для более качественного понимания организации сети, принципов работы устройства;

•многоязыковая поддержка: возможность перевода данного программного продукта практически на любой язык, необходимый пользователю;

•усовершенствованное изображение сетевого оборудования со способностью добавлять / удалять различные компоненты;

•наличие Activity Wizard позволяет студентам и преподавателям создавать шаблоны сетей и использовать их в дальнейшем.

С помощью данного программного продукта преподаватели и студенты могут придумывать, строить, конфигурировать сети и производить в них поиск неисправностей. Packet Tracer дает возможность более подробно представлять новейшие технологии, тем самым делая учебный процесс чрезвычайно полезным с точки зрения усвоения полученного материала.

9. Boson NetSim

Boson NetSim – программное обеспечение, которое моделирует работу сетевого оборудования Cisco, и разработано, чтобы помочь пользователю в изучении операционной системы Cisco IOS.

Большинство других программных продуктов, «моделируя» поведение системы в заранее подготовленных лабораторных работах, фактически не могут отображать ситуаций, которые действительно могут случиться в сети. В отличие от них, NetSim использует технологии, специально разработанные компанией Boson, которые позволяют обойти этот недостаток и моделировать истинное поведение сети. Эти технологии позволят многим пользователям Boson NetSim выйти далеко за рамки выдуманных лабораторных работ, и лучше понять принципы функционирования Cisco IOS.

NetSim имеет очень развитую поддержку, обеспечивающую компанией Boson. Boson выпускает различные версии NetSim, каждая из которых

ориентирована на определенный экзамен Cicso и, соответственно, уровень знания пользователя. Существует три версии NetSim'a для следующих экзаменов: NetSim для CCENT, NetSim для CCNA и NetSim для CCNP.

10. Network Emulator

Разработка программы Network Emulator стартовала в начале 1997 года. Проект превратился, по сути, в программу, обучающую ее пользователя всем тонкостям технологии на разных уровнях: от базовых понятий до особенностей обработки отдельных полей сетевых пакетов. Программа прошла путь от простейшего «роутера пакетов» до интеллектуального организатора виртуальных машин: на любом из компьютеров можно запустить несколько программ-аналогов настоящих приложений. Все они будут исполняться одновременно. В дальнейшем появилось новое назначение программы: обучение студентов принципу администрирования IP-сетей.

Network Emulator включает в себя следующие возможности и технологии:

- маршрутизация, система моделирования каналов, IP-фильтрация;
- типы пакетов: ICMP, UDP, TCP, а так же низкоуровневые ARP-запросы;
- концепция интерфейсов и сокетов (простой, дейтаграммный и потоковый);
- эмуляция хостов, коммутаторов второго уровня и концентраторов;
- установка уровня помех на канале;
- связывание нескольких Network Emulator через реальную сеть TCP/IP.

3. Описание практикума

В процессе обучения студенты приобретут навыки использования специализированных программных продуктов, как в штатном режиме работы, так и в имитации рабочей обстановки, включающей в себя различного рода атаки и нарушение политики безопасности, утечку конфиденциальной информации и многое другое. Такой подход к обучению специалиста по информационной безопасности, подготовит его как теоретически, так и практически. Во время критических инцидентов специалист будет действовать

с пониманием обстановки и принимать соответствующие меры, чтобы свести ущерб к минимуму.

Прежде всего, студент должен освоить теоретический материал, который ему предоставляется в виде лекций: знание базового понятийного аппарата в области информационной безопасности и защиты информации; видов и состава угроз информационной безопасности; принципов и общих методов обеспечения информационной безопасности; основных положений государственной политики обеспечения информационной безопасности; критериев, условий и принципов отнесения информации к защищаемой; видов носителей защищаемой информации; видов и подвидов тайн конфиденциальной информации; видов уязвимости защищаемой информации и форм ее проявления; источников, видов и способы дестабилизирующего воздействия на защищаемую информацию; каналов и методов несанкционированного доступа к конфиденциальной информации; состава объектов защиты информации; классификации видов, методов и средств защиты информации. Основные вопросы, которые затем будут отражены в практикуме:

- принципы отнесения информации к конфиденциальной;
- виды угроз информационной безопасности;
- политика информационной безопасности;
- носители защищаемой информации;
- несанкционированный доступ к информации;
- вредоносное программное обеспечение;
- модель нарушителя;
- регламентация процессов и действий персонала;
- сетевая топология;
- уязвимости в сетях и др.

Структуру курса можно описать следующим образом. Студенты на протяжении всего обучения работают с «виртуальной компанией» «ПромАвтоматика» и по окончании курса они должны иметь представление о построении политики информационной безопасности предприятия с

использованием предлагаемых программных средств. Вначале студенты разбивают по степеням конфиденциальности весь массив информации, состоящий из следующих данных:

- структура виртуальной организации;
- документы всех отделов организации;
- данные по сотрудникам организации;
- данные по уровню допуска каждого сотрудника организации.

Затем определяют группы пользователей, имеющих доступ к каждой степени конфиденциальности. Преподаватель дисциплины «Построение компьютерных сетей для малого бизнеса (CISCO)» дает студентам задание по построению архитектуры компьютерной сети для виртуальной компании. Студенты прорабатывают направления деятельности компании, ее структуру, собирают информацию о том, как будет использоваться новая сеть (количество и тип подключаемых узлов; используемые приложения; требования к общему доступу и подключению к Интернету; безопасность и охрана личной информации; ожидаемая степень надежности и время бесперебойной работы; требования к подключению, в частности, выбор проводной или беспроводной связи). Затем определяют физическую конфигурацию сети (физическое расположение устройств, например, маршрутизаторов, коммутаторов и узлов; соединение устройств; расположение и длина всех кабелей; аппаратная конфигурация оконечных устройств, например узлов и серверов) и логическую конфигурацию сети (местоположение и размер доменов широковещательных рассылок и коллизий; схема IP-адресации; схема именования; конфигурация общего доступа; разрешения). Далее студенты разбивают весь массив информации, циркулирующий в системе, по степеням конфиденциальности, затем определяют группы пользователей, имеющих доступ к каждой степени конфиденциальности. После этого составляется схема физических и логических взаимосвязей ресурсов и доступа к ним пользователей, определяются программные средства и доступ в Интернет. После того, как требования к сети будут задокументированы, а схемы физической и логической топологии

построены, нужно будет протестировать конструкцию сети. Один из способов проверки конструкции сети – создание рабочей модели, или прототипа.

На сегодняшний день на рынке IT существует несколько программных средств, которые позволяют смоделировать и симулировать работу компьютерной сети. Наиболее распространенными в плане использования для обучения являются Boson NetSim, Cisco Packet Tracer и Network Emulator.

По своему функционалу программа Cisco Packet Tracer наиболее подходящее средство для создания модели сети, более того, она используется при изучении материалов курса CCNA Discovery, изучаемого в рамках дисциплин «Построение компьютерных сетей для малого бизнеса (CISCO)» и «Администрирование компьютерных сетей (CISCO)». Поэтому данная программа используется для обучения студентов в рамках дисциплин «Построение компьютерных сетей для малого бизнеса», «Администрирование компьютерных сетей», «Вычислительные системы, сети и телекоммуникации» и др.

Средство позволяет имитировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров, IP-телефонов и т.д. Работа с интерактивным симулятором дает весьма правдоподобное ощущение настройки реальной сети, состоящей из десятков или даже сотен устройств. Настройки, в свою очередь, зависят от характера устройств: одни можно настроить с помощью команд операционной системы Cisco IOS, другие – за счет графического веб-интерфейса, третьи – через командную строку операционной системы или графические меню. Усовершенствованное изображение сетевого оборудования обладает способностью добавлять / удалять различные компоненты (модули). Модуль Activity Wizard позволяет студентам и преподавателям создавать шаблоны сетей и использовать их в дальнейшем.

Благодаря такому свойству Cisco Packet Tracer, как режим визуализации, студенты могут отследить перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые

устройства, скорость и пути перемещения IP-пакетов. Анализ событий, происходящих в сети, позволяет понять механизм ее работы и обнаружить неисправности. Помимо этого, с помощью Cisco Packet Tracer студент может симулировать построение не только логической, но и физической модели сети и, следовательно, получать навыки проектирования. Схему сети можно наложить на чертеж реально существующего здания или даже города и спроектировать всё кабельное хозяйство, разместить устройства в тех или иных зданиях и помещениях с учетом физических ограничений, таких как длина и тип прокладываемого кабеля или радиус зоны покрытия беспроводной сети.

После построения модели и проведения необходимых экспериментов с сетью в Cisco Packet Tracer, студенты переходят к построению сети с использованием лабораторных стендов с реальным сетевым оборудованием компании Cisco Systems в классе сетевой академии Cisco в университете.

Далее в рамках курса «Информационная безопасность» студенты проводят анализ уязвимостей построенной сети, при помощи программного продукта «XSpider», если сеть удовлетворяет всем критериям безопасности, то производится настройка антивирусного и антишпионского программного обеспечения по учебным материалам, предоставленным «Академией Касперского». Параллельно с этим студенты изучают основы компьютерной вирусологии, действий вредоносного программного обеспечения, последствий и принципов работы антивирусных программ. После этого студенты приступают к работе с программными продуктами «Код безопасности: Инвентаризация 2.2» и «Код безопасности: Security Studio Honeypot Manager». В программе «Код безопасности: Инвентаризация 2.2» студент проводит анализ угроз и уязвимостей системы, получает инвентаризацию ресурсов и видов информации компании, значения рисков для каждого ресурса, перечень уязвимостей, влияющих на значение рисков, слабые стороны построенной системы. И в соответствии с полученными результатами проводит работу с данными в системе, используя «Код безопасности: Security Studio Honeypot

Manager». Затем, по специальным шаблонам, студент разрабатывает политику информационной безопасности:

- классификации информации;
- инвентаризации информационных ресурсов;
- управления рисками ИБ;
- управления ролями ИБ;
- управления доступом к информационным ресурсам;
- управления данными;
- организации рабочего места;
- организации дистанционной работы;
- и др.

В программе «Код безопасности: Security Studio Honeypot Manager» студент проверяет разработанную им политику информационной безопасности на соответствие требований международных стандартов по информационной безопасности, затем модифицирует разработанную политику согласно полученным результатам.

Программный продукт «Контур информационной безопасности» ориентирован на выявление внутренних утечек компании, на инсайдеров. Студенты изучают основы работы с персоналом, принципы распределения ролей в системе. Далее они изучают организацию доступа к информации, отслеживание возможных утечек с помощью специального инструментария, входящего в состав программ «Контур информационной безопасности» и «XSpider». Далее, в курсе Cisco, на основе полученных результатов, студенты вносят изменения в физическую и логическую организацию сети виртуальной компании, в целях обеспечения безопасности сети.

В качестве другого задания преподаватель курса Cisco выдает студентам модель компьютерной сети, которая заведомо не удовлетворяет некоторым критериям безопасности. Студенты должны обнаружить все уязвимости и провести работы по их устранению.

В результате работы со специализированными программами студент получает компетенции, позволяющие ему обеспечивать защиту информации и информационную безопасность на разных уровнях – на прикладном (программы), на уровне персонала (распределение степени допуска, работа с утечками, изучение «человеческого фактора»), на уровне предприятия (политика информационной безопасности организации в целом). Кроме того, студент получит навыки работы в критических ситуациях – в момент атаки, отказе оборудования или других непредвиденных обстоятельствах.

При выполнении практических заданий студент в полной мере сможет оценить масштаб утечки конфиденциальной информации на предприятии и все последующие последствия. После прохождения такой практической подготовки, работодателю больше не потребуется самостоятельно обучать сотрудника тем техническим средствам информационной безопасности, с которыми они работают.

Выводы

Повсеместное внедрение информационных технологий во все сферы человеческой деятельности приводит повышению актуальности проблем, связанных с информационной безопасностью и защитой информации. Для наилучшего обеспечения защиты данных организации необходим комплексный и системный подход к построению реализации политики информационной безопасности с внедрением программно-технических средств, а так же работой с кадрами. Все эти мероприятия должен обеспечивать специальный отдел по обеспечению информационной безопасности, с профессиональными сотрудниками, получившими образование в данной области и обладающими навыками обеспечения защиты безопасности, построения и реализации политики информационной безопасности в организации.

В данный момент в учреждениях как высшего, так и среднеспециального образования ведется подготовка специалистов по информационной безопасности, но по большей части только в области теоретических аспектов. На практике выпускники и работодатели сталкиваются с проблемой

неподготовленности ИТ-специалиста перевести свои теоретические знания в прикладную область.

Частично проблему конкурентоспособности и дальнейшего трудоустройства выпускника можно решить, удовлетворив требования работодателей к содержанию подготовки будущего работника. Если обучать студента с применением как практических, так и теоретических материалов в равной степени, как в разработанном курсе, то студент будет готов в полной мере проявить себя на будущем рабочем месте.

В нашей работе описан авторский курс по информационной безопасности с применением различных программных средств, на базе которых студент сможет полностью отладить механизм обеспечения информационной безопасности от анализа информации, циркулирующей в организации и построении безопасной сети, до разработки политики информационной безопасности и реализации ее аспектов на практике с помощью специализированных средств.

Особенностью нашей разработки является межпредметная связь курса по информационной безопасности с дисциплинами, посвященными построению и администрированию сетей, что повышает конкурентоспособность ИТ-специалиста на рынке труда.

Литература:

1. Смородин Г.Н. Академическое партнерство как инвестиционный проект корпорации. [Электронный ресурс]. URL: http://2011.ит-образование.рф/section/77/3897/ (дата обращения: 18.10.2012)
2. Семенихин И. Подготовка специалистов в области информационной безопасности. – «Открытые системы», - № 1, - 2011.