следующему алгоритму: сначала идет изложение необходимого теоретического материала, затем разбирается решение типичных для данной темы задач и, наконец, предлагаются задания по вариантам для выполнения конкретной самостоятельной или лабораторной работы. Приведенные примеры решения типовых задач по изучаемой теме делают материал доступным для понимания, облегчают его усвоение обучаемыми, в том числе и при самостоятельной работе.

Таким образом, внедрение кафедрой высшей математики современных приемов преподавания актуального материала в области информационной безопасности способствует осуществлению качественной подготовки военных инженерных кадров адекватно требованиям времени.

Литература

1. *Липницкий В.А., Михайловская Л.В., Валаханович Е.В.* Защита информации: практикум / Минск: Военная академия РБ, 2012. 86 с.

УЧЕБНАЯ ДИСЦИПЛИНА «ОРГАНИЗАЦИЯ РАБОТЫ В ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ»

М.В. Губич

Опыт защиты различных категорий сведений показывает, что эффективной может быть лишь комплексная система защиты информации, которая сочетает в себе физические, организационные, технические, криптографические, программные и иные специальные меры. Вместе с тем распространение действия такой системы в отношении информации, прямо не охраняемой законодательством Республики Беларусь, является нецелесообразным по ряду причин, в первую очередь, экономическим (стоимость такой информации превышает затраты на ее защиту). Однако, исходя из основного назначения органов внутренних дел (далее – ОВД) – защищать права, свободы и законные интересы участников общественных отношений, – данные органы обязаны осуществлять защиту любой информации, разглашение либо утрата которой могут причинить вред как самим ОВД, их сотрудникам, так и иным участникам общественных отношений.

Изложенное указывает на необходимость обучения персонала ОВД методам защиты информации, в связи с чем в Академии МВД Республики Беларусь организовано обучение курсантов и слушателей по учебной дисциплине «Организация работы в защищенных компьютерных системах», по итогам изучения которой обучающиеся:

– получают знания об аппаратном и программном обеспечении защищенных компьютерных систем (далее – ЗКС), технических требованиях, предъявляемые к ним; каналах утечки информации и методах их обнаружения; методах и средствах защиты информации в компьютерных системах; антивирусном и межсетевом программном обеспечении; основах безопасной работы на персональном компьютере; основных категориях в сфере технической защиты информации, обрабатываемой с использованием средств вычислительной техники; порядке работы с конфиденциальными информационными ресурсами; методах и средствах защиты от противоправных действий обслуживающего персонала и пользователей; требованиях, предъявляемых к сотрудникам ОВД при работе в ЗКС;

– формируют умения и навыки установки и выполнения основных настроек антивирусного и межсетевого программного обеспечения; навигации по файловой системе, операций с каталогами; создания и удаления учетных записей, назначения прав доступа; настройки политики безопасности и аудита системы; работы в ЗКС.

Таким образом, полученные в ходе изучения учебной дисциплины «Организация работы в защищенных компьютерных системах» знания и умения позволят выпускникам Академии МВД Республики Беларусь обеспечить защиту всего объема служебной информации, обрабатываемой посредством средств вычислительной техники, без существенных материальных затрат.

ЗАДАЧИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.М. Кадан, А.К. Доронин

Существенной проблемой процесса обучения практическим мерам защиты компьютерной информации является недостаточная мощность программно-технической базы учебных заведений. Выходом из этой ситуации представляется создание и использование в учебном процессе

современных виртуальных лабораторий, использующих возможности облачных и кластерных архитектур.

Тестирование на проникновение (penetration testing, «пентест») - это поиск уязвимостей с практической проверкой возможностей их реализации. Цель тестирования на проникновение - оценка уровня защищенности, которая заключается в исследовании сети или веб-ресурса для выявление уязвимостей, которые могут быть использованы злоумышленником для реализации угроз информационной безопасности.

В докладе представлен проект и методика использования виртуальной облачной лаборатории, использование которой позволяет существенно повысить качество практической подготовки обучаемых, специализирующихся в обрасти защиты информации.

Целью использования лаборатории является совершенствование навыков тестирования сети на проникновение извне. Работа в лаборатории осуществляется на основе методики «серый ящик»: перед началом исследования предоставляется информация об инфраструктуре в виде схемы и описания деятельности виртуальной компании. Далее обучаемому предлагается выполнить эксплуатацию различных уязвимостей, связанных с работой сетевых и веб-компонентов, криптографических механизмов, ошибками конфигурации и кода, а также с человеческим фактором.

Использование учебных лабораторий данного типа показало их эффективность в условиях необходимости подготовки специалистов, способных решать масштабные задачи анализа и устранения уязвимостей веб-ресурсов.

Лаборатория развернута на платформе облачного кластера Гродненского государственного университета им.Я.Купалы.

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ПРОВЕДЕНИЮ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ

М.А. Кадан, Д.Ю. Сенько

Экспертиза компьютеров, аппаратно-технических средств, программного обеспечения, баз данных вследствие постоянного совершенствования компьютерной техники и программного обеспечения являются одним из самых сложных видов исследований. В то же время, на любом этапе расследования инцидентов информационной безопасности можно встретить противодействие расследованию со стороны злоумышленника.

Основной целью работы является анализ методов и средств противодействия компьютерно-техническим экспертизам и ознакомление с возможностями программного обеспечения для непосредственного установления факта противодействия. Основным методом исследования выбрана систематизация возможных методов сокрытия информации.

В работе дана классификация основных методов противодействия, среди которых выделяются методы общего противодействия (шифрование, анонимность, уничтожение данных) и методы направленного противодействия (обнаружение факта проведения КТЭ для последующего уничтожения, сокрытия или подмены исследуемых данных, поиск ошибок криминалистических программ либо ошибок эксперта-криминалиста для последующей компрометации доказательств).

Рассмотрены популярные в настоящее время методы и программные средства противодействия, основанные на предотвращении создания криминалистически значимых данных: вредоносные программы, работающие только в оперативной памяти; загрузочные диски и виртуальные машины, направленные на отсутствия следов работы при работе с компьютером.

Данные методы и программные средства в большинстве случаев разрабатываются с целью защиты конфиденциальной информации или поддержки свободы слова, но это не исключает их использование злоумышленниками в целях сокрытия или уничтожения доказательств в виде компьютерной информации и противодействия расследованию компьютерных преступлений.

Применение методов противодействия компьютерной экспертизе является серьезным препятствием в раскрытии преступлений, однако на сегодняшний день возможности программного обеспечения позволяют успешно справляться с попытками препятствования расследованию инцидентов информационной безопасности.