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.