Казанцев В.В.,
Директор Научно-консультационного центра НТАК, к.ю.н.

Penetration testing: Юридические аспекты

Национальная Телекоммуникационная Ассоциация (НТА) Казахстана

ПЕН-Тест - что это?

Тестирование на проникновение (жарг. *Пентест*) — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. Процесс включает в себя активный анализ системы на наличие потенциальных уязвимостей, которые могут спровоцировать некорректную работу целевой системы, либо полный отказ в обслуживании. Анализ ведется с позиции потенциального атакующего и может включать в себя активное использование уязвимостей системы. *(по материалам Википедии)*

Аудит включает пен-тест?
Пен-тест – это часть аудита?

УК РК: Статья 210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов

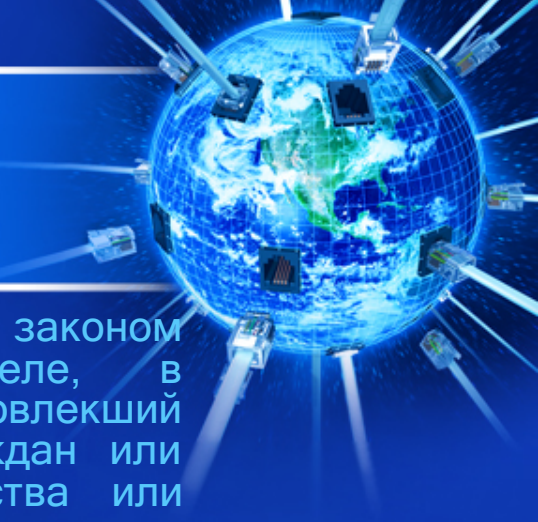
Создание компьютерной программы, программного продукта или внесение изменений в существующую программу или программный продукт с целью неправомерного уничтожения, блокирования, модификации, копирования, использования информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или сетей телекоммуникаций, а равно ***умышленные использование*** и (или) распространение такой программы или программного продукта

Цели/умысел:

- Уничтожение
- Блокирование
- Модификация
- Копирование
- Использование
- А что у вас в договоре на услуги?

Наступление последствий – обязательно?

УК РК: Статья 205. Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций



Умышленный неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций, повлекший существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства.

Отличительные признаки объективной стороны:

- Прямой умысел
- Наличие последствий (Существенность нарушения)
- Причинно-следственная связь

В законодательстве понятие «существенности нарушения прав и законных интересов» не регламентировано и является оценочным понятием.

С учетом судебной практики:

- нарушение конституционных прав и свобод человека и гражданина (права на гражданство, судебную защиту, жизнь, личную свободу, неприкосновенность достоинства человека, жилища, собственности, частной жизни и тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и т.д).
- В отношении юридического лица - связано с незаконным вмешательством в ее деятельность, ограничением свободы предпринимательства, повлекшие крупные убытки.
- Существенное нарушение охраняемых законов интересов общества и государства имеет место при создании серьезных сбоев в работе госорганов, подрыве авторитета органов власти.

Еще ряд статей УК РК:

Статья 206. Неправомерные уничтожение или модификация информации

Умышленные неправомерные уничтожение или модификация охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, а равно ввод в информационную систему заведомо ложной информации, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства.

Статья 207. Нарушение работы информационной системы или сетей телекоммуникаций

Умышленные действия (бездействие), направленные на нарушение работы информационной системы или сетей телекоммуникаций.

Информационная система

Информационная система - организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач (пп.12) ст.1 ЗРК «Об информатизации»)

Характеристики:

- Есть ИКТ
- Есть Персонал
- Есть Техническая документация
- Есть Взаимодействие
- Есть Цель функционирования

Информационно-коммуникационные технологии - совокупность методов работы с электронными информационными ресурсами и методов информационного взаимодействия, осуществляемых с применением аппаратно-программного комплекса и сети телекоммуникаций.

Аппаратно-программный комплекс (АПК) - совокупность программного обеспечения и технических средств, совместно применяемых для решения задач определенного типа.

Информационная система

АПК:

- результат поставки от производителя оборудования/результат оказания услуг, выполнения работ;
- права пользования программным обеспечением;
- что-то еще?

Воздействие при Пентесте на АПК=ИС:

- Гарантийные условия производителя, подрядчика?
- Пользовательские и лицензионные соглашения с правообладателями?
- Иные обременения и инструкции пользования?

А вы учли все ограничения?

Правовое регулирование информационной безопасности

У того, кто решит изучить все законы, не остается времени их нарушать. *(Иоганн Вольфганг Гёте)*

Спасибо за внимание!

www.ntark.kz

www.it-law.kz