

Вопросы к экзамену по курсу  
«Защита информации»

1. Понятие информации. Информационная составляющая программного продукта. Необходимость защиты информации. Способы хищения информации.
2. Вредоносный программный код. Цели написания вредоносного программного кода. Способы распространения и внедрения в программы компьютеры.
3. Современный вирус. Компоненты современного вируса и функциональное назначение.
4. Способы анализа защит программного обеспечения. Аппаратные и программные средства анализа.
5. Системы противодействия отладке на процессоре x86 и специфические для MS Windows, как общей направленности, так и направленные против определенных программ-отладчиков.
6. Packers and unpackers. Создание программ-контейнеров. Методы анализа программ-контейнеров.
7. Типы вызовов подпрограмм, используемые компилятором. Принцип создания obfuscated code при помощи компилятора.
8. Виртуальные машины. Широко распространенные виртуальные машины. Минимально возможная виртуальная машина.
9. Полиморфный и самомодифицирующийся код. Способы разработки и исследования полиморфного и самомодифицирующегося кода.
10. Метаморфный код. Способы разработки и исследования метаморфного кода.
11. Сетевые атаки на HTML и CGI scripts. Их типы, цели и способы защиты от них.
12. Атаки на базы данных. SQL injects. Типы атак на SQL. Blind SQL injection.
13. Правовые основы исследования программ. Ответственность за их нарушение. DMCA. Отличие в законах об авторском праве в России и за рубежом применительно к программным продуктам.