# Реверс-инжиниринг

Курс рассчитан на разработчиков программного обеспечения, системных программистов, системных аналитиков, вирусных аналитиков, специалистов по информационной безопасности, devops-специалистов

Длительность курса: 102 академических часа

## 1 Низкоуровневое программирование на ассемблер под x8086/x64

1 **Регистры процессора, работа с памятью**

Домашние задания

1 Установка софта

Необходимо установить следующий софт:
Emu 8086
FASM
x64Dbg
Ida Pro 7
Hiew
Far Manager
ConEmu

2 **Представление данных, кода, опкоды команд.**

Домашние задания

1 Одинаковые команды - разные опкоды

1. Неодходимо составить список как можно больших команд, которые будут иметь один и тот же смысл, но разные опкоды. Пример:
xor ax, ax | 33 c0
xor ax, ax | 31 c0
2. Модифицировать файл в HEX редакторе ex.exe так, чтобы MessageBox показывался два раза.

---

3 **Арифметические, логические команды. Команды условного/безусловного перехода**

Домашние задания

1 Написать keygen к программам CRACKME.EXE (66f573036f8b99863d75743eff84f15d) и Otus_Crackme_01.exe (fb42bfad815a9563b9f6fdd362b47f70)

Необходимо дизассемблировать программу и написать генератор валидных пар login:password.

---

4 **Прерывания BIOS**

Домашние задания

1 Калькулятор суммы

Написать программу, принимающую на вход два слагаемых в виде hex цифр, считает сумму и выводит её не экран тоже, в hex виде.

# 2 Низкоуровневое программирование на ассемблер под MIPS

1 **Регистры процессора. Работа с памятью**

2 **Арифметические, логические команды. Команды условного/безусловного перехода**

Домашние задания

1 Crc32

Переписать программу с MIPS ассемблера на 8086.

3 **Опкоды команд**

# 3 Защищённый режим процессора

## 1 Сегментная организация памяти

## 2 Страничная организация памяти

Домашние задания

1 Стек в PM

1. Написать программку (лучше на python, но можно и на других ЯП), которая на вход будет принимать: адрес сегмента, лимит сегмента, права (чтение/запись/исполнение) и будет возвращать сформированный дескриптор сегмента
2. Добавить дескриптор сегмента, для стека в segmodel.asm

# 4 Внутреннее устройство Windows

1 **Объекты ядра**

2 **Менеджер памяти**

3 **Диспетчер ввода-вывода**

# 5 Системное программирование

1 **PE формат**

2 **WinApi функции. Перехваты WinApi функций**

Домашние задания

1 Pe Loader

Реализовать простейший Pe Loader, который будет считывать с диска Pe (exe) из памяти и запускать его.
Pe файл брать тот, который выдаёт MessageBox и скомпилирован на FASME.

3 **Программирование Native приложений**

4 **Способы добавления в автозагрузку**

5 **Программирование служб**

6 **Настройка рабочей среды для отладки драйверов режима ядра**

# 6 Написание простейших драйверов

## 1 Написание кастомного MBR

# 7 Обратная разработка программ

| | | |
|---|---|---|
| 1 | **Динамический анализ кода** | WinDbg, Sysinternels Tools, WireShark |
| 2 | **Статический анализ кода** | Ida Pro |
| 3 | **Разработка shell кодов** | |
| 4 | **Metasploit** | |
| 5 | **Внедрение реверс шела в некоторые прошивки роутеров** | |
| 6 | **Поиск и эксплуатация уязвимостей Buffer Overflow/UAF** | |

# 8 Проектная работа

| | | |
|---|---|---|
| 1 | **Вводное занятие по проектной работе** | Домашние задания<br><br>1 Проектная работа |
| 2 | **Консультации и обсуждения проектной работы** | |
| 3 | **Консультации и обсуждения проектной работы** | |
| 4 | **Итоговое занятие. Обсуждение проектной работы** | |