Основные аспекты обеспечения безопасности встраиваемых систем Linux

Код: SECR-009

Длительность: 28 ч.

Описание:

Добро пожаловать в эру интернета вещей, где соединенные высокоскоростной сетью устройства вторгаются в каждый аспект нашей жизни – дома, офисы, автомобили и даже человеческие тела!

С возросшей популярность протокола IPv6 и повсеместным распространением Wi-Fi-сетей интернет вещей растет с угрожающей скоростью, по прогнозам исследователей, количество подключенных устройств к 2020 г. достигнет сорока миллиардов.

Интернет вещей предоставляет пользователям новые возможности, которые раньше было трудно даже представить. Но у каждой медали есть обратная сторона – новые технологии открывают новые возможности и вектора атак для киберпреступников.

Большинство устройств в интернете вещей используют различные варианты ОС Linux в качестве платформы для запуска.

Данный курс поможет вам ответить на следующие вопросы:

- что такое безопасность встраиваемых систем;
- как встраиваемые системы подвергаются атакам;
- как я могу обезопасить свою систему;
- какие продукты и технологии я могу использовать для защиты моего кода и системы;
- как работает интернет вещей;
- технологии защиты интернета вещей;
- как я могу интегрировать тестирование безопасности в процесс разработки программных продуктов.

Также тренинг содержит несколько практических работ, направленных на знакомство студентов с процессом защиты программного обеспечения и данных.

Цели:

Целью данного курса является предоставление исчерпывающей информации о существующих проблемах в области встраиваемых систем и методах их решения.

Разбираемые темы:

- Основные понятия информационной безопасности;
- Цикл безопасной разработки ПО;
- Основные атаки и управление рисками;
- Загрузка ОС Linux;
- Информационная безопасность;
- Уровень приложения;
- Модули безопасности Linux;
- Тестирование и выпуск релизов.

Целевая аудитория:

разработчики, тестировщики.

Примечание:

Материалы курса представлены на английском языке.