Анализ вредоносного программного обеспечения

Цель программы — выработать у слушателей практические навыки выявления и тщательного анализа вредоносного ПО, осуществлять расследование киберинцидентов, используя передовые методы компьютерной криминалистики и обратной разработки, а также различных инструментов для реагирования на инциденты.

Выпускники курса получают свидетельство о повышении квалификации государственного образца.

Целевая аудитория:

- руководители структурных подразделений и специалисты центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций;
- специалисты всех наименований и категорий, обеспечивающих кибербезопасность;
- сотрудники правоохранительных органов, занимающихся расследованием киберпреступлений;
- IT-специалисты, заинтересованные в повышении своей квалификации в области кибербезопасности.

Форма обучения – очная (дневная).
Стоимость обучения одного слушателя – 3200 рублей.

Продолжительность программы – 50 академических часов.

Учебный план курса

№ п/п	Название тем курса
	Компьютерная криминалистика операционных систем Windows
1.	Компьютерная криминалистика и продвинутая обработка данных
2.	Анализ реестра, выполнение приложений и криминалистика облачных хранилищ
3.	Элементы оболочки и профилирование съемных устройств
4.	Анализ электронной почты, поиск в Windows, SRUM и журналы событий
5.	Криминалистика веб-браузера
	Обратная разработка вредоносных программ: инструменты и методы анализа вредоносного ПО
6.	Основы анализа вредоносных программ
7.	Обратная разработка вредоносного кода
8.	Анализ вредоносных документов и сценариев
9.	Тщательный анализ вредоносного ПО
10.	Изучение самозащищающегося вредоносного ПО
11.	Основы анализа вредоносных программ
	Продвинутая сетевая криминалистика: поиск угроз, анализ и реагирование на инциденты

12.	Введение
13.	Основные протоколы и агрегация/анализ журналов
14.	NetFlow и протоколы доступа к файлам
15.	Коммерческие инструменты, беспроводные сети и охота за полным пакетом
16.	Шифрование, обратная разработка протоколов, OPSEC и Intel
	Продвинутое реагирование на инциденты, поиск угроз и компьютерная криминалистика
17.	Основы компьютерной криминалистики
18.	Анализ вторжения
19.	Анализ памяти при реагировании на инциденты и поиске угроз
20.	Анализ временной шкалы
21.	Реагирование на инциденты и поиск по всему предприятию. Продвинутое обнаружение противников и анти-криминалистических методов