Учебный план программы курса повышения квалификации по направлению «Основы компьютерной криминалистики и методики реагирования на инциденты информационной безопасности»

№ п/п	Разделы и темы	Всего часов	Аудиторные занятия, час.		Самост. работа
			Лекции	Практ. занятия	
1.1.	Основы компьютерной криминалистики. Нормативно-правовая база.	6	1	1	4
	Введение в компьютерную криминалистику. Специальность – компьютерный криминалист. Особенности современных подходов: Windows криминалистика, артефакты диспетчера задач. Утилиты Autoruns, cports. Нормативно правовая база преступлений в сфере компьютерной информации.				
1.2.	Расследование инцидентов ИБ. Образ жесткого диска, дамп памяти.	6	1	1	4
	Расследование инцидентов ИБ. Образ жесткого диска, дамп памяти.				
1.3.	Сетевая криминалистика и вспомогательные утилиты	7	1	1	5
	Сетевая криминалистика и вспомогательные утилиты				
1.4.	Исследование дампов оперативной памяти. Востребованные компьютерно-криминалистические утилиты.	8	1	1	6
	Исследование дампов оперативной памяти. Востребованные компьютерно-криминалистические утилиты.				
1.5.	Артефакты ОС Windows и вспомогательные утилиты	7	1	1	5
	Исследование реестра ОС. Системы сбора и анализа журналов ОС. Обращение к системе командная строка(cmd). Утилиты паролей, утилиты,журналов и файлов. Восстановление данных. Исследование истории браузеров. Утилиты артефактов (RS Browser Forensics, USBDeview и др.)				
2.1.	Нормативно-правовое обеспечение определения инцидента ИБ	7	1	1	5
	Понятие события ИБ, понятие инцидента ИБ, возбуждение уголовных дел по преступлениям в сфере высоких технологий, привлечение к расследованию специалистов, осмотр места происшествия, выемка и осмотр средств компьютерной техники и носителей информации, осмотр электронных документов, оперативно-розыскные мероприятия, назначение компьютерной экспертизы.				
2.2.	Основы процесса реагирования на инциденты ИБ	7	1	1	5
	Планирование и подготовка к менеджменту				

№ п/п	Разделы и темы	Всего часов	Аудиторные занятия, час.		Самост. работа
			Лекции	Практ. занятия	
	инцидентов ИБ. Политика обработки сообщений о событиях и инцидентах ИБ. Политика менеджмента инцидентов информационной безопасности. Создание группы реагирования на инциденты информационной безопасности. Обнаружение и оповещение о событиях ИБ. Управление инцидентами ИБ, классификация инцидентов ИБ, этапы реагирования на инциденты.				
2.3.	Техническая и другая поддержка реагирования на инциденты ИБ	8	1	1	6
	Электронные базы данных событий/инцидентов ИБ и технические средства для быстрого пополнения, и обновления базы данных. SIEM-системы: IBM QRadar, MaxPatrol SIEM, ArcSight, Splunk и другие. Технологические тренды развития SIEM-систем. Web application firewall, Sandbox (песочница).				
2.4.	Практическое применение средств реагирования на инциденты ИБ	8	1	1	6
	Работа в Sandbox, работа в SIEM системе, работа в IRP системе.				
2.5.	Восстановление системы после инцидента ИБ	8	1	1	6
	Проверка работоспособности рабочих станций и серверов, мониторинг на предмет повторной компрометации, отчетность и выводы.				
	Всего:	72	10	10	52