ООО «ГАЗИНФОРМСЕРВИС»

Лаборатория развития и продвижения

компетенций кибербезопасности

УТВЕРЖДАЮ

Руководитель Лаборатории
развития и продвижения
компетенций кибербезопасности

К.А. Ахрамеева

«12» ноября 2024

Учебно-тематический план программы повышения квалификации

«Администрирование программного комплекса управления конфигурациями и анализа защищенности Efros Config Inspector»

Цель обучения:	приобретение теоретических знаний в области задач по мониторингу информационной безопасности и реагированию на инциденты информационной безопасности; а также практических навыков: применение средств контроля защищенности с учетом особенностей информационной инфраструктуры; разработка основных организационно-распорядительных документов предприятия и системы мер по обеспечению политики информационной безопасности; организация расследования компьютерных инцидентов.
Категория слушателей:	Специалисты отделов информационной безопасности компаний, осуществляющие функции по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты
Профессиональный стандарт:	06.032 Специалист по безопасности компьютерных систем и сетей 14.09.2022 06.033 Специалист по защите информации в автоматизированных системах 14.09.2022 06.034 Специалист по технической защите информации 09.08.2022
Срок обучения:	40 академических часов, 5 учебных дней
Режим занятий:	8 академических часов в день
Форма обучения:	дистанционная, с отрывом от работы

№№ п.п.	Наименование разделов и тем	Всего часов	В том числе		Форма контроля
			Лекции	Практ. занятия	
1.	**Мониторинг информационной безопасности.**	**4**	**4**	-	**Контр. вопросы**
1.1.	Основные понятия в области инцидентов информационной безопасности. Основные источники угроз безопасности информации на предприятии и предпосылки возникновения инцидентов информационной безопасности. Виды правонарушений в области компьютерной информации. Роль политик информационной безопасности в обеспечении защиты информации на предприятии.	4	4	-	
2.	**Реагирование на инциденты информационной безопасности.**	**8**	**4**	**4**	**Контр. вопросы**
2.1.	Комплекс превентивных и оперативных мероприятий. Сбор и анализ данных с различных объектов инфраструктуры организации на предмет контроля показателей штатной активности. Ведение реестра ресурсов (всех ИТ-систем компании) и их оценка на предмет соответствия нормативным требованиям в области информационной безопасности. Мониторинг подозрительных событий. Анализ выявленной подозрительной активности. Своевременное реагирование на потенциальные угрозы; пресечение распространения угрозы. Восстановление деятельности после реализации угрозы. Разработка и реализация мероприятий по развитию системы информационной безопасности и недопущению повторения инцидентов.	8	4	4	
3.	**Организация проведения контроля информационной безопасности**	**6**	**2**	**4**	**Контр. вопросы**
3.1.	Аудит информационной безопасности и тестирование защищенности сети предприятия. Защита информационных ресурсов компьютерной сети предприятия от несанкционированного доступа. Регистрация и учет событий безопасности. Обеспечение контроля целостности информационных ресурсов и программ.	6	2	4	

4.	**Расследование компьютерных преступлений и инцидентов как функция защиты информации ограниченного доступа**	**8**	**2**	**6**	**Контр. вопросы**
4.1.	Расследование компьютерных преступлений и инцидентов, как функция защиты информации ограниченного доступа. Примеры нарушений политики информационной безопасности. Судебная практика преступлений в области компьютерной информации, основные причины и тенденции. Выявление и фиксация признаков и следов нарушения политики информационной безопасности для расследования инцидентов и судебного преследования виновных.	8	2	6	
5.	**Построение системы контроля защищенности информации с учетом особенностей информационной инфраструктуры. Практический тренинг.**	**12**	**2**	**10**	**Контр. вопросы**
	Всего:	**38**	**14**	**24**	
	Итоговый контроль знаний	**2**		**2**	**Итоговая аттестация: зачет без оценки**
	Итого:	**40**	**14**	**26**	