ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «РОСТОВСКИЙ ЦЕНТР ПОВЫШЕНИЯ КВАЛИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ»

«УТВЕРЖДАЮ»
Директор
ЧОУ ДПО «РЦПК ИТС»

_____ Е.И. Самойлова

«30» октября 2024 г.

Программа дополнительного профессионального образования
«Мониторинг и анализ инцидентов информационной безопасности»

Целью обучения по программе является изучение специалистами современных способов обнаружения и расследования инцидентов информационной безопасности, получение первичных навыков работы с источниками событий аудита ИБ, получение первичных навыков работы в SIEM-системе, изучение методологии целевых APT-атак, методологии расследования инцидентов ИБ.
Обучающиеся по программе повышения квалификации готовятся к осуществлению следующих профессиональной видов деятельности: 1-ая и 2-ая линии мониторинга Security Operations Center.
Объектами профессиональной деятельности обучающихся являются корпоративные сети.

Поставленная цель достигается решением следующих задач:

- Изучением базовых ИТ- и ИБ-модулей (основы ИБ, основы ОС, компьютерные сети, сетевые атаки, сетевые СрЗИ, хостовые и комплексные СрЗИ, домены ActiveDirectory, введение во вредоносное ПО);
- Изучением и практической отработкой навыков по работе с типовыми источниками событий аудита (ОС Windows, ОС Linux, приложения);
- Изучением методологии расследования инцидентов ИБ в SIEM-системе и отработкой на стенде MP SIEM практических навыков расследования инцидентов разного уровня сложности, составления отчётов о проведённых расследованиях.

Категория обучающихся:
Уровень образования лица, поступающего на обучение – среднее профессиональное /высшее образование по специальностям в области информационной безопасности или информационных технологий.