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.

Учебный план

программы дополнительного профессионального образования
«Развертывание системы мониторинга предприятия»

Целью обучения: является изучение специалистами современных способов управления инцидентами информационной безопасности, получение навыков работы с множеством источников событий аудита ИБ, получение навыков работы в SIEM-системе на продвинутом уровне, получение навыков написания контента для выявления инцидентов ИБ.

Обучающиеся по программе повышения квалификации готовятся к осуществлению следующих профессиональной видов деятельности: аналитик мониторинга Security Operations Center.

Объектами профессиональной деятельности обучающихся являются корпоративные сети.

Поставленная цель достигается решением следующих задач:

Предподготовка по введению в аудит ИБ, категориям и приоритетам событий, архитектурам и механизмам аудита, расширенному аудиту ОС Windows, технологиям Windows Event Forwarding и Windows Event Collector, Sysmon. Также, изучаются типовые корпоративные инфраструктуры в контексте аудита источников в ней.

Изучение и практическая отработка навыков по работе с типовыми источниками событий аудита (ОС Windows, ОС Linux, приложения), практика применения аудита в корпоративных сетях;

Изучение методологии SOC – линии, экспертиза, метрики, процессы.

Изучение последовательности обработки событий в SOC.

Изучение языка написания контента XP в PT MP SIEM. Изучение методологии работы с контентом, структуры контента. Изучение формул нормализации, правил обогащения, правил корреляции.

Навыки контроля за состоянием мониторинга ИБ в корпоративной сети. Ведение статистики срабатываний правил корреляции. Профилирование активности. Работа с исключениями.

Также изучаются другие аспекты работы SOCи аспекты роли аналитика SOC.

ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ ПОСТУПАЮЩЕГО НА ОБУЧЕНИЕ

Уровень образования лица, поступающего на обучение: среднее-профессиональное или высшее образование по специальностям в области информационной безопасностии/или информационных технологий.

Наличие опыта работы по специальности как минимум 2 года.

Желательно наличие первичных навыков работы с SIEM-системами и расследованием инцидентов ИБ.

Форма обучения: очная

Длительность обучения: 116 ак. часов

№ п/п	Наименование учебных модулей, тем	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		

1	2	3	4	5	6	7	8	9	10	11
1.	**Сбор событий ИБ**	**6**	**0**	**0**	**0**	**0**	**0**	**0**	**6**	**-**
1.1	Цели аудита.	1,5	0	0	0	0	0	0	1,5	
1.2	Категории и приоритеты событий	1,5	0	0	0	0	0	0	1,5	
1.3	События кибербезопасности	2	0	0	0	0	0	0	2	
1.4	Архитектура и механизмы аудита	1	0	0	0	0	0	0	1	
2	**Расширенный аудит в ОС Microsoft Windows**	**13,5**	**6**	**5,5**	**0,5**	**0**	**4,5**	**0**	**3**	
2.1	Лабораторнаяработа "Advanced OS Windows audit"	2	0	0	0	0	2	0	0	
2.2	Подсистема аудита Sysmon	4,5	2	2	0	0	0	0	2,5	
2.3	Сравнение стандартного аудита ОС Windows и Sysmon	1,5	1,5	1,5	0	0	0	0	0	
2.4	Дополнительные журналы аудита ОС Windows	2	2	2	0	0	0	0	0	
2.5	Windows Event Collector	3,5	0,5	0	0,5	0	2,5	0	0,5	
3	**Расширенный аудит в Linux ОС**	**3**	**3**	**1,5**	**1,5**	**0**	**0**	**0**	**0**	
3.1	Аудит Syslog	0,5	0,5	0,5	0	0	0	0	0	
3.2	Подсистема аудита Auditd	2	2	0,5	1,5	0	0	0	0	
3.3	Примеры применения аудита ОС Linux в корпоративных сетях	0,5	0,5	0,5	0	0	0	0	0	
4	**Сбор событий с типовых ИТ систем и средств защиты информации**	**17**	**10**	**0**	**1**	**9**	**0**	**0**	**7**	
4.1	Аудит типовой корпоративной ИТ-инфраструктуры	5	0	0	0	0	0	0	5	
4.2	Аудит типовой ИБ-инфраструктуры	2	0	0	0	0	0	0	2	
4.3	Настройка аудита источников	4,5	4,5	0	0,5	4	0	0	0	
4.4	Механизмы и транспорты передачи/получения событий	1,5	1,5	0	0,5	1	0	0	0	
4.5	Подключение источников к SIEM	3	3	0	0	3	0	0	0	
4.6	Диагностика и решение проблем при подключении источников к SIEM	1	1	0	0	1	0	0	0	
5	**Базовые подходы к разработке контента SIEM**	**31,5**	**31,5**	**15,5**	**5**	**11**	**0**	**0**	**0**	
5.1	Задачи L3 и L4 в Security Operations Center, компетенции	0,5	0,5	0,5	0	0	0	0	0	
5.2	Реестр сценариев	1	1	1	0	0	0	0	0	
5.3	Статистика, Customer KB	1,5	1,5	1,5	0	0	0	0	0	
5.4	Последовательность обработки событий	1,5	1,5	1,5	0	0	0	0	0	
5.5	Иерархия правил корреляции	5	5	5	0	0	0	0	0	
5.6	Инцидентные правила корреляции	3	3	3	0	0	0	0	0	
5.7	Правило типа Workflow	1,5	1,5	1,5	0	0	0	0	0	
5.8	Синтаксис языка XP	3	3	0	3	0	0	0	0	
5.9	Нормализация событий	1	1	0	1	0	0	0	0	
5.10	Практическое задание по нормализации событий	7	7	0	1	6	0	0	0	
5.11	Влияние контента на производительность SIEM	1	1	1	0	0	0	0	0	
5.12	Перенос контента между инсталляциями	0,5	0,5	0,5	0	0	0	0	0	
5.13	Генерация отчетов средствами MP SIEM	2,5	2,5	0	0	2,5	0	0	0	
5.14	Визуализация в MP SIEM	2,5	2,5	0	0	2,5	0	0	0	
6	**Практика обнаружения кибератак**	**37**	**37**	**4**	**9**	**24**	**0**	**0**	**0**	

6.1	Рабочий процесс обработки инцидента ИБ	1	1	1	0	0	0	0	0	
6.2	Мониторинг обработки событий и EPS, фильтры событий	0,5	0,5	0,5	0	0	0	0	0	
6.3	Практическое задание по написанию базовых и профилирующих правил	12	12	1	1	10	0	0	0	
6.4	Практическое задание по написанию инцидентных правил	9	9	0	1	8	0	0	0	
6.5	Добавление исключений	2	2	0	2	0	0	0	0	
6.6	Практика по внесению исключений в правила	6	6	0	1	5	0	0	0	
6.7	System Health	0,5	0,5	0,5	0	0	0	0	0	
6.8	Методология расследования инцидентов	4	4	0	4	0	0	0	0	
6.9	Анализ уведомлений об инцидентах	2	2	1	0	1	0	0	0	
7	**Решение класса XDR: защита от кибератак**	**8**	**10**	**0**	**5**	**3**	**0**	**0**	**0**	
7.1	Администрирование KATA	2	3	0	1	1	0	0	0	
7.2	Анализ событий KATA	3	3	0	2	1	0	0	0	
7.3	Реагирование на инциденты ИБ с использованием данных инструментов	3	4	0	2	1	0	0	0	
8	**Итоговая аттестация**	**4**	**-**	**-**	**-**	**4**	**-**	**-**	**-**	**Финальное практическое задание; Тест**
	Итого:	**116**	**97,5**	**26,5**	**22**	**47**	**4,5**	**0**	**16**	