ЧОУ ДПО “Ростовский центр повышения квалификации в области информационных технологий и связи”

УТВЕРЖДАЮ
Директор ЧОУ ДПО “РЦПК ИТС”

_____ С. Д. Мармоленко

05 мая 2022г.

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

Цели:
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.

Срок обучения:
132 часа

Форма обучения:
смешанная — часть времени отводится аудиторному обучению в очном формате, также занятия проводятся с использованием дистанционных технологий обучения в соответствии с действующей нормативной базой.

Режим занятий:
5 раз в неделю с понедельника по пятницу, от 2 до 6 часов в день.

№ 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.	**Основы информационных технологий и информационной безопасности**	**74,1**	**0**	**0**	**0**	**0**	**7,6**	**15,2**	**51,3**	-
1.1.	**Введение в информационную безопасность**	**4,4**	**0**	**0**	**0**	**0**	**0**	**0,4**	**4**	
1.1.1	Основные понятия ИБ. Триада конфиденциальность-целостность-доступность, политики ИБ.	1	0	0	0	0	0	0	1	
1.1.2	Уровни киберпреступников и их мотивация/возможности. Варианты монетизации кибератак.	1	0	0	0	0	0	0	1	
1.1.3	Детальный разбор наиболее известных кибератак и основных трендов кибербезопасности 2020-2022 гг.	2	0	0	0	0	0	0	2	
1.1.4	Тест по курсу "Введение в информационную безопасность"	0,4	0	0	0	0	0	0,4	0	тест
1.2.	**Введение в операционные системы**	**8,8**	**0**	**0**	**0**	**0**	**1,6**	**1**	**6,2**	
1.2.1	Базовые понятия АРМ и ОС	1,5	0	0	0	0	0	0	1,5	
1.2.2	Эволюция машинного кода ЭВМ	0,5	0	0	0	0	0	0	0,5	
1.2.3	Файлыипроцессы Portable Executable	0,8	0	0	0	0	0	0	0,8	
1.2.4	Wscript и JAR	0,2	0	0	0	0	0	0	0,2	
1.2.5	Разграничение прав доступа в ОС	0,6	0	0	0	0	0	0	0,6	
1.2.6	Способы повышения привилегий в ОС Windows	0,2	0	0	0	0	0	0	0,2	
1.2.7	LSASS, SAM, AAA	0,3	0	0	0	0	0	0	0,3	
1.2.8	Службы и демоны в операционных системах	0,5	0	0	0	0	0	0	0,5	

1.2.9	Планировщики задач	0,3	0	0	0	0	0	0	0,3	
1.2.10	Реестр ОС Windows	0,5	0	0	0	0	0	0	0,5	
1.2.11	Виртуальные машины	0,3	0	0	0	0	0	0	0,3	
1.2.12	ОС Linux	0,5	0	0	0	0	0	0	0,5	
1.2.13	Тест по курсу "Введение в операционные системы"	1	0	0	0	0	0	1	0	тест
1.2.14	Лабораторная работа "Реестр ОС Windows"	0,5	0	0	0	0	0,5	0	0	проверка, выдача обратной связи
1.2.15	Лабораторная работа "Командная строка ОС Windows"	0,5	0	0	0	0	0,5	0	0	проверка, выдача обратной связи
1.2.16	Лабораторная работа "Работа с системными компонентами ОС Windows"	0,6	0	0	0	0	0,6	0	0	проверка, выдача обратной связи
1.3.	**Компьютерные сети. Базовый уровень**	**25,2**	**0**	**0**	**0**	**0**	**3**	**6,5**	**15,7**	
1.3.1	Структура сетевых моделей, различия моделей ISO/OSI и TCP/IP	0,6	0	0	0	0	0	0	0,6	
1.3.2	Физический уровень модели OSI	0,4	0	0	0	0	0	0	0,4	
1.3.3	Тест по курсу "Структура сетевых моделей, различия моделей ISO/OSI и TCP/IP"	0,3	0	0	0	0	0	0,3	0	тест
1.3.4	Канальный уровень модели OSI: адресация, Ethernet, Wi-Fi, сетевое оборудование	0,6	0	0	0	0	0	0	0,6	
1.3.5	Тест по курсу "Канальный уровень модели OSI: адресация, Ethernet, Wi-Fi, сетевое оборудование"	0,1	0	0	0	0	0	0,1	0	тест
1.3.6	Сетевой уровень модели OSI: адресация, маска подсети, NAT, оборудование	2	0	0	0	0	0	0	2	
1.3.7	Тест по курсу "Сетевой уровень модели OSI: адресация, маска подсети, NAT, оборудование"	0,7	0	0	0	0	0	0,7	0	тест
1.3.8	Маршрутизация в сетях	0,6	0	0	0	0	0	0	0,6	
1.3.9	Протоколы IP, ICMP, ARP	1	0	0	0	0	0	0	1	
1.3.10	Технология VLAN, передача трафика внутри и между VLAN	1	0	0	0	0	0	0	1	
1.3.11	Тест по курсу "Технология VLAN"	0,3	0	0	0	0	0	0,3	0	тест

1.3.12	Транспортный уровень модели OSI: NAPT, протоколы TCP, UDP	1	0	0	0	0	0	0	1	
1.3.13	Тест по курсу "Транспортный уровень модели OSI: NAPT, протоколы TCP, UDP"	0,5	0	0	0	0	0	0,5	0	тест
1.3.14	Сеансовый уровень модели OSI, уровень представления	0,5	0	0	0	0	0	0	0,5	
1.3.15	Тест по курсу "Сеансовый уровень модели OSI, уровень представления"	0,1	0	0	0	0	0	0,1	0	тест
1.3.16	Прикладной уровень модели OSI: протоколы DNS, HTTP, SMTP, Whois	3	0	0	0	0	0	0	3	
1.3.17	Лабораторная работа "Nslookup"	1	0	0	0	0	1	0	0	проверка, выдача обратной связи
1.3.18	Лабораторная работа "Установка SSH-сервера, проброс порта"	1	0	0	0	0	1	0	0	проверка, выдача обратной связи
1.3.19	Тест по курсу "Прикладной уровень модели OSI: протоколы DNS, HTTP, Proxy, SMTP, Whois"	2	0	0	0	0	0	2	0	тест
1.3.20	Атаки на сетевой и транспортный уровни модели OSI	1	0	0	0	0	0	0	1	
1.3.21	Тест по курсу "Атаки на сетевой уровень модели OSI"	0,3	0	0	0	0	0	0,3	0	тест
1.3.22	Тест по курсу "Атаки на транспортный уровень модели OSI"	0,5	0	0	0	0	0	0,5	0	тест
1.3.23	Атаки на прикладной уровень модели OSI и способы их обнаружения	2	0	0	0	0	0	0	2	
1.3.24	Тест по курсу "Атаки на прикладной уровень модели OSI и способы их обнаружения"	0,5	0	0	0	0	0	0,5	0	тест
1.3.25	Лабораторная работа "DNS cache poisoning"	0,5	0	0	0	0	0,5	0	0	проверка, выдача обратной связи
1.3.26	DDoS-атаки, классификация и механизмы	1	0	0	0	0	0	0	1	
1.3.27	Тест по курсу "DDoS-атаки, классификация и механизмы"	0,2	0	0	0	0	0	0,2	0	тест
1.3.28	Атаки "человек посередине"	1	0	0	0	0	0	0	1	

1.3.29	Тест по курсу "Атаки "человек посередине"	0,2	0	0	0	0	0	0,2	0	тест
1.3.30	Лабораторная работа по курсу "Атаки "человек посередине""	1,3	0	0	0	0	0,5	0,8	0	тест
1.4.	**Сетевые средства защиты. Базовый уровень**	**9,6**	**0**	**0**	**0**	**0**	**1,5**	**3,6**	**4,5**	
1.4.1	Межсетевые экраны	1	0	0	0	0	0	0	**1**	
1.4.2	Тест по курсу "Межсетевые экраны"	0,5	0	0	0	0	0	0,5	0	тест
1.4.3	Технология VPN	1	0	0	0	0	0	0	**1**	
1.4.4	Тест по курсу "Технология VPN"	0,5	0	0	0	0	0	0,5	0	тест
1.4.5	Аудит на прокси-сервере. Зеркалирование трафика.	2	0	0	0	0	**1,5**	0	**0,5**	
1.4.6	Тест по курсу "Аудит на прокси-сервере. Зеркалирование трафика."	0,1	0	0	0	0	0	0,1	0	тест
1.4.7	Сетевые системы обнаружения вторжений (NIDS)	1	0	0	0	0	0	0	**1**	
1.4.8	Тест по курсу "Сетевые системы обнаружения вторжений (NIDS)"	0,2	0	0	0	0	0	0,2	0	тест
1.4.9	Web Application Firewall	1	0	0	0	0	0	0	**1**	
1.4.10	Тестпокурсу "Web Application Firewall"	0,3	0	0	0	0	0	0,3	0	тест
1.4.11	Финальный тест по компьютерным сетям, сетевым атакам и сетевым средствами защиты информации	2	0	0	0	0	0	2	0	тест
1.5.	**Расширенный курс по компьютерным сетям**	**9**	**0**	**0**	**0**	**0**	**0**	**2,1**	**6,9**	
1.5.1	DNS-over-TLS, DNS-over-HTTPS, DNSSEC, Open resolver, IDN домены	1	0	0	0	0	0	0	1	
1.5.2	SMTP open relay	0,3	0	0	0	0	0	0	0,3	
1.5.3	Протокол SMB	0,3	0	0	0	0	0	0	0,3	
1.5.4	Протокол Whois	0,3	0	0	0	0	0	0	0,3	
1.5.5	Промежуточное тестирование	0,5	0	0	0	0	0	0,5	0	тест
1.5.6	Атаки на сетевой и транспортный уровни модели OSI	0,5	0	0	0	0	0	0	0,5	
1.5.7	Тест по курсу "Атаки на сетевой и транспортный уровни модели OSI"	0,5	0	0	0	0	0	0,5	0	тест
1.5.8	Атаки на прикладной уровень модели OSI и способы их обнаружения	1,5	0	0	0	0	0	0	1,5	
1.5.9	Тест по курсу "Атаки на прикладной уровень модели	0,3	0	0	0	0	0	0,3	0	тест

	OSI и способы их обнаружения"									
1.5.10	Атаки "человек посередине"	0,8	0	0	0	0	0	0	0,8	
1.5.11	Тест по курсу "Атаки "человек посередине""	0,2	0	0	0	0	0	0,2	0	тест
1.5.12	Mail Security & Antispam	1	0	0	0	0	0	0,2	0,8	тест
1.5.13	Защита от DDoS-атак	0,6	0	0	0	0	0	0	0,6	
1.5.14	Тест по курсу "Защита от DDoS. Advanced-уровень"	0,2	0	0	0	0	0	0,2	0	тест
1.5.15	Журналирование RA VPN, NIDS, WAF	0,8	0	0	0	0	0	0	0,8	
1.5.16	Тест по курсу "Журналирование RA VPN, NIDS, WAF"	0,2	0	0	0	0	0	0,2	0	тест
1.6.	**Хостовые и комплексные средства защиты информации**	**4,4**	**0**	**0**	**0**	**0**	**0**	**0,4**	**4**	
1.6.1	Антивирусное программное обеспечение (АВПО)	0,5	0	0	0	0	0	0	0,5	
1.6.2	Средства криптографической защиты информации (СКЗИ)	0,5	0	0	0	0	0	0	0,5	
1.6.3	Средства защиты информации от несанкционированного доступа (СЗИ от НСД)	0,5	0	0	0	0	0	0	0,5	
1.6.4	Хостовые IDS (HIDS)	0,5	0	0	0	0	0	0	0,5	
1.6.5	Endpoint Detection & Response (EDR)	0,5	0	0	0	0	0	0	0,5	
1.6.6	Data Leak Prevention (DLP)	0,5	0	0	0	0	0	0	0,5	
1.6.7	Honeypot	0,5	0	0	0	0	0	0	0,5	
1.6.8	Системы контроля и управления доступом (СКУД)	0,5	0	0	0	0	0	0	0,5	
1.6.9	Тест по курсу "Хостовые и комплексные средства защиты информации"	0,4	0	0	0	0	0	0,4	0	тест
1.7.	**Домены Active Directory**	**8,2**	**0**	**0**	**0**	**0**	**1**	**0,7**	**6,5**	
1.7.1	Домены AD, отличие от workgroup	1	0	0	0	0	0	0	1	
1.7.2	Типовые сервисы в корпоративной сети	1	0	0	0	0	0	0	1	
1.7.3	Протоколы аутентификации в доменах AD	2	0	0	0	0	0	0	2	
1.7.4	Типовые атаки на протоколы аутентификации в доменах AD	1	0	0	0	0	0	0	1	
1.7.5	Групповые политики AD	1	0	0	0	0	0	0	1	
1.7.6	Корпоративная информационная система как объект мониторинга	0,5	0	0	0	0	0	0	0,5	
1.7.7	Тест по курсу "Домены Active Directory"	0,7	0	0	0	0	0	0,7	0	тест

1.7.8	Лабораторная работа "Windows Server"	1	0	0	0	0	1	0	0	проверка, выдача обратной связи
1.8.	**Вредоносное ПО. Введение.**	**4,5**	**0**	**0**	**0**	**0**	**0,5**	**0,5**	**3,5**	
1.8.1	Введение в тему вредоносного ПО	0,5	0	0	0	0	0	0	0,5	
1.8.2	Классификация ВПО	1	0	0	0	0	0	0	1	
1.8.3	Алгоритм работы вируса	0,5	0	0	0	0	0	0	0,5	
1.8.4	Средства удалённого администрирования	1	0	0	0	0	0	0	1	
1.8.5	Анализ срабатываний АВПО	0,5	0	0	0	0	0	0	0,5	
1.8.6	Тест по курсу "Вредоносное ПО. Введение."	0,5	0	0	0	0	0	0,5	0	тест
1.8.7	Лабораторная работа "Подключение по PsExec"	0,5	0	0	0	0	0,5	0	0	проверка, выдача обратной связи
2.	**Мониторинг и анализ инцидентов ИБ**	**57,9**	**30,5**	**14,3**	**10,3**	**6**	**6**	**0,5**	**20,9**	
2.1	**Построение и функционирование Центра мониторинга**	**6**	**6**	**3**	**3**	**0**	**0**	**0**	**0**	
2.1.1	Принципы построения и функционирования Центров мониторинга	1,5	1,5	1,5	0	0	0	0	0	
2.1.2	Распределение обязанностей между сотрудниками	1	1	1	0	0	0	0	0	
2.1.3	Термины и метрики SOC	0,5	0,5	0,5	0	0	0	0	0	
2.1.4	Взаимодействие с НКЦКИ и ГосСОПКА	1	1	0	1	0	0	0	0	
2.1.5	Подготовка плана на реагирования на компьютерные инциденты	2	2	0	2	0	0	0	0	
2.2	**Инструменты Центра мониторинга**	**5,5**	**5,5**	**5,5**	**0**	**0**	**0**	**0**	**0**	
2.2.1	Полезные источники событий в корпоративных сетях	4	4	4	0	0	0	0	0	
2.2.2	Особенности настройки аудита ОС Windows и ОС Linux в корпоративных сетях	1,5	1,5	1,5	0	0	0	0	0	
2.3.	**Аудит и Log Management. Базовый уровень**	**17**	**4**	**0**	**4**	**0**	**6**	**0**	**7**	
2.3.1	Аудит ОС Windows. Политики аудита. Фильтрация событий в журналах.	2	0	0	0	0	0	0	2	
2.3.2	Интерпретация событий аудита ОС Windows	3	0	0	0	0	0	0	3	

2.3.3	Аудит ОС Linux. Параметры аудита. Фильтрация событий в журналах.	2	0	0	0	0	0	0	2	
2.3.4	Занятие "Введение в аудит ОС Windows. Sysmon."	1	1	0	1	0	0	0	0	
2.3.5	Занятие "Интерпретация событий ОС Windows."	1	1	0	1	0	0	0	0	
2.3.6	Занятие "Журналы аудита ОС Linux. Подсистемы аудита Linux."	0,5	0,5	0	0,5	0	0	0	0	
2.3.7	Занятие "Базовая настройка аудита ОС Linux. Auditd. Rsyslog."	0,5	0,5	0	0,5	0	0	0	0	
2.3.8	Занятие "Просмотр событий аудита в ОС Linux. Журналы событий приложений."	1	1	0	1	0	0	0	0	
2.3.9	Лабораторная работа "Настройка политик аудита ОС Windows"	1	0	0	0	0	1	0	0	проверка, выдача обратной связи
2.3.10	Лабораторная работа "Настройка политик аудита ОС Windows через SACL"	0,5	0	0	0	0	0,5	0	0	проверка, выдача обратной связи
2.3.11	Лабораторная работа "Установка подсистемы аудита Sysmon"	1	0	0	0	0	1	0	0	проверка, выдача обратной связи
2.3.12	Лабораторная работа "Расследование инцидента по жураналам событий ОС Windows"	1	0	0	0	0	1	0	0	проверка, выдача обратной связи
2.3.13	Лабораторная работа "Установка подсистемы аудита auditd в ОС Linux". Часть 1.	1	0	0	0	0	1	0	0	проверка, выдача обратной связи
2.3.14	Лабораторная работа "Настройка правил аудита auditd в ОС Linux". Часть 2.	0,5	0	0	0	0	0,5	0	0	проверка, выдача обратной связи
2.3.15	Лабораторная работа "Настройка перенаправления событий в подсистеме Rsyslog".	1	0	0	0	0	1	0	0	проверка, выдача обратной связи
2.4.	**Введение в MaxPatrol SIEM**	**11,4**	**5**	**3**	**0,5**	**1,5**	**0**	**0,5**	**5,9**	
2.4.1	Архитектура и компоненты MaxPatrol SIEM	2	0	0	0	0	0	0	2	

2.4.2	Интерфейс консоли MaxPatrol SIEM	0,4	0	0	0	0	0	0	0,4	
2.4.3	Работа с событиями в MaxPatrol SIEM	1,5	0	0	0	0	0	0	1,5	
2.4.4	Работа с отчётами в MaxPatrol SIEM	1	0	0	0	0	0	0	1	
2.4.5	Работа с табличными списками в MaxPatrol SIEM	0,5	0	0	0	0	0	0	0,5	
2.4.6	Просмотр инцидентов в MaxPatrol SIEM	0,5	0	0	0	0	0	0	0,5	
2.4.7	Тест по курсу "Введение в MaxPatrol SIEM"	0,5	0	0	0	0	0	0,5	0	
2.4.8	Занятие "Введение в MaxPatrol SIEM. Работа в консоли"	2	2	2	0	0	0	0	0	
2.4.9	Занятие "Жизненный цикл инцидента ИБ в Security Operations Center"	0,5	0,5	0,5	0	0	0	0	0	
2.4.10	Занятие "Интерпретация событий в MaxPatrol SIEM"	2	2	0	0,5	1,5	0	0	0	
2.4.14	Занятие "Мониторинг доступности источников событий и работоспособности SIEM. Типовые Use Cases."	0,5	0,5	0,5	0	0	0	0	0	
2.5.	**Методологии, описывающие проведение кибератак**	**4**	**4**	**2,75**	**1,25**	**0**	**0**	**0**	**0**	
2.5.1	APT-атаки. Матрица MITRE ATT&CK, модель Cyber Kill Chain. Индикаторы компрометации.	2	2	2	0	0	0	0	0	
2.5.2	Связывание активности в нескольких инцидентах в один вектор.	0,25	0,25	0,25	0	0	0	0	0	
2.5.3	Обзор отчётов отраслевых CERT	0,5	0,5	0,5	0	0	0	0	0	
2.5.4	Расследование инцидентов Threat Intelligence	1,25	1,25	0	1,25	0	0	0	0	
2.6	**Методология расследования инцидентов**	14	6	0	1,5	4,5	0	0	8	
2.6.1	Занятие "Типовые Use Cases, методология расследования инцидентов ИБ в SIEM"	6	2	0	0,5	1,5	0	0	4	проверка домашнего задания
2.6.2	Занятие "Расследование в консоли MaxPatrol SIEM типовой активности в корпоративной сети"	2	2	0	0,5	1,5	0	0	0	
2.6.3	Занятие "Расследование типовых инцидентов в консоли MaxPatrol SIEM"	6	2	0	0,5	1,5	0	0	4	проверка домашнего задания

3.	**Итоговая аттестация**	**-**	**-**	**-**	**-**	**4**	**-**	**-**	**-**	**Финальное практическое задание**
	Итого:	**132**	**30,5**	**14,3**	**10,3**	**6**	**13,6**	**15,7**	**72,2**	