Частное образовательное учреждение дополнительного образования
«Учебный центр «Эврика»
(Наименование образовательного учреждения)

УТВЕРЖДАЮ
Директор ЧОУДО “Учебный центр “Эврика”
_____/Мазепин С.А.

Образовательная программа дополнительного профессионального образования
(повышения квалификации)

по направлению

21.Обеспечение безопасности сетевой инфраструктуры предприятия.

(наименование программы)

Образовательная программа дополнительного профессионального образования повышения квалификации (далее - Программа) разработана на основании Федерального закона от 29.12.2012 г. №273-ФЗ «Об образовании в Российской Федерации» и в соответствии с приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

Программа предоставляет слушателям знания и навыки для формирования системного подхода к обеспечению безопасности компьютерных сетей, учит планировать и осуществлять организационные мероприятия, а также выбирать и применять основные виды технических средств защиты информации. Программа предоставляет развернутые знания по обеспечению компьютерной безопасности современных систем и будет важен администраторам безопасности в качестве справочника по различным методам и средствам взлома компьютерных сетей и систем. Также курс полезен сотрудникам службы безопасности для повышения эффективности работы с учетом новых уловок злоумышленников, и бесспорно данный курс будет интересен руководителям отделов ИТ для формирования реалистичной оценки современной ситуации в сфере обеспечения компьютерной безопасности. Также в программе широко представлены программные продукты по сбору и восстановлению информации, свидетельствующей о вторжении в систему.

Методика проведения занятий.

Организация учебного процесса регламентируется программой обучения, учебным планом, расписанием и режимом занятий обучающихся. При реализации дополнительных профессиональных программ применяется форма организации образовательной деятельности, основанная на модульном принципе представления содержания образовательной программы и построения учебных планов.

Режим занятий для обучающихся устанавливается в рамках пятидневной недели с понедельника по пятницу с 10:00 до 18:00 с двумя перерывами на кофе-брейки и перерывом на обед с 13:30 до 14:30.

Расписание занятий составляется на весь период обучения и размещается на сайте ЧОУДО «Учебный центр «Эврика».

Для всех видов аудиторных занятий академический час установлен в 45 минут. Длительность учебного дня устанавливается не более 8 академических часов, с перерывами. В течение учебного дня обучающимся предоставляется один длительный перерыв для отдыха и питания продолжительностью не менее 45 минут. Время предоставления перерывов и их продолжительность может корректироваться с учетом расписания учебных занятий.

При проведении обучения осуществляется контроль обучающихся на соответствие их персональных достижений каждому модулю соответствующей программы в режиме минитестов. Освоение полной программы дополнительного профессионального образования завершается итоговой аттестацией обучающихся в форме зачета.

При проведении занятий используются электронные версии учебных пособий и лабораторных работ. Слушателю предоставляется электронный учебник по соответствующему модулю
Для доступа к электронным библиотечно-информационными ресурсам, слушателям выдается аутентификационная информация (логин и пароль).

Каждому слушателю предоставляется рабочее место (компьютер Core i7 (32/64Gb RAM, 2*1Tb HDD, 1Gbit netcard) с двумя TFT мониторами (19+21)). Один монитор используется для работы с электронным учебником, второй монитор для выполнения лабораторных и практических работ. Состояние оборудования, оснащённость кабинетов соответствует современным требованиям. Обеспечен доступ в сеть Интернет для каждого рабочего места слушателя.

Дистанционное обучение проводится в режиме максимально приближенного к очному.
Лекционная часть с демонстрациями и примерами проводится в режиме видеоконференции. через сервис веб-конференций.
Практическая часть выполняется слушателями индивидуально на индивидуальном лабораторном стенде, размещенном на стороне Учебного Центра. Слушатели подключаются к компьютерам в классах ЧОУДО “Учебный центр “Эврика”.

Программа дистанционного обучения, время проведения обучения и количество часов обучения полностью соответствует программе очного обучения.

Учебный план

21.Обеспечение безопасности сетевой инфраструктуры предприятия.

Учебный план Программы представляет собой перечень модулей - учебных курсов (дисциплин), каждый из которых имеет свой учебный план, который определяет перечень, трудоемкость, последовательность и формы контроля

Календарный учебный график определяет основные параметры учебного процесса при организации занятий по каждому образовательному модулю (курсу) при освоении Программы и зависит от трудоёмкости

Категория слушателей: для лиц, имеющих высшее и среднее образование
Срок обучения 120 академических часов

Режим занятий очное с применением дистанционных технологий с отрывом от производства-8 академических часов в день

п/п	Наименование разделов и дисциплин	Всего часов	В том числе:		Формы контроля
			Лекции	Практические занятия	
1	**2**	**3**	**4**	**5**	**6**
1	**Обеспечение безопасности компьютерных сетей (CND)**	**40**	**25**	**15**	
1.1	Основы сетевых технологий и обеспечения безопасности сети	2	1,5	0,5	Минитест
1.2	Возможные уязвимости, угрозы и атаки на сеть	2,5	2	0,5	Минитест
1.3	Средства обеспечения безопасности сети	2,5	2	0,5	Минитест
1.4	Разработка и реализация политик безопасности сети	3	2	1	Минитест
1.5	Обеспечение физической безопасности	2	2	0	Минитест
1.6	Защита узлов сети	3,5	1,5	2	Минитест
1.7	Межсетевые экраны	2,5	1,5	1	Минитест
1.8	Системы обнаружения и предупреждения вторжений (IDS/IPS)	3,5	2,5	1	Минитест
1.9	Виртуальные частные сети (VPN)	3,5	2	1,5	Минитест
1.10	Обеспечение безопасности беспроводных сетей	3	2	1	Минитест
1.11	Мониторинг и анализ трафика в сети	3	1	2	Минитест
1.12	Управление рисками и анализ уязвимостей сети	3,5	1,5	2	Минитест
1.13	Резервное копирование и восстановление данных	2,5	1,5	1	Минитест
1.14	Управление инцидентами информационной безопасности	3	2	1	Минитест
2	**Этичный хакинг: тестирование на проникновение (CEH)**	**40**	**20,5**	**19,5**	
2.01	Введение в этичный хакинг	1	0,5	0,5	Минитест

2.02	Предварительный сбор информации о цели	2,5	1,5	1	Минитест
2.03	Сканирование сети	2	1	1	Минитест
2.04	Инвентаризация ресурсов	2,5	1,5	1	Минитест
2.05	Хакинг системы	2	1	1	Минитест
2.06	Трояны и бэкдоры	2	1	1	Минитест
2.07	Вирусы и черви	2	1	1	Минитест
2.08	Снифферы	2	1	1	Минитест
2.09	Социальная инженерия	2	1	1	Минитест
2.10	Отказ в обслуживании	2	1	1	Минитест
2.11	Перехват сеанса	2	1	1	Минитест
2.12	Хакинг веб-серверов	2	1	1	Минитест
2.13	Хакинг веб-приложений	2	1	1	Минитест
2.14	SQL инъекции	2	1	1	Минитест
2.15	Хакинг беспроводных сетей	2	1	1	Минитест
2.16	Хакинг мобильных платформ	2	1	1	Минитест
2.17	Обход систем обнаружения вторжений, брандмауэры и Honey Pot	2	1	1	Минитест
2.18	Переполнение буфера	2	1	1	Минитест
2.19	Криптография	2	1	1	Минитест
2.20	Тестирование на проникновение	2	1	1	Минитест
3.	**Расследование инцидентов компьютерной безопасности v9 (CHFI)**	**40**	**25**	**15**	**40**
3.1	Расследование инцидентов ИБ в современном мире	2	1,5	0,5	Минитест
3.2	Процесс расследования инцидента ИБ	2,5	2	0,5	Минитест
3.3	Сбор доказательств с дисков и файловых систем	2,5	2	0,5	Минитест
3.4	Расследование инцидентов, связанных с операционной системой	3	2	1	Минитест
3.5	Противодействие методам сокрытия доказательств	2	2	0	Минитест
3.6	Методы сбора и копирования данных	3,5	1,5	2	Минитест
3.7	Расследование инцидентов, связанных с сетевыми технологиями	2,5	1,5	1	Минитест
3.8	Расследование атак на веб-приложения	3,5	2,5	1	Минитест
3.9	Расследование инцидентов, связанных с СУБД	3,5	2	1,5	Минитест
3.10	Расследование инцидентов, связанных с облачными приложениями	3	2	1	Минитест
3.11	Расследование инцидентов, связанных с вредоносным кодом	3	1	2	Минитест
3.12	Расследование инцидентов, связанных с электронной почтой	3,5	1,5	2	Минитест
3.13	Расследование инцидентов, связанных с мобильными устройствами	2,5	1,5	1	Минитест
3.14	Подготовка отчетов о расследовании инцидента	3	2	1	Минитест
4	**Обеспечение безопасности компьютерных сетей v10(ECSA v10)**	**40**	**21**	**19**	
4.1	Основы тестирования на проникновение и методология	4	2	2	Минитест

4.2	Область тестирования на проникновение и методология взаимодействия	3	2	1	Минитест
4.3	Методология разведки на основе открытых источников (OSINT)	4	2	2	Минитест
4.4	Социальная инженерия и тестирование на проникновение	2	1	1	Минитест
4.5	Внешнее тестирование на проникновение в сеть	3	2	1	Минитест
4.6	Внутреннее тестирование на проникновение в сеть	4	2	2	Минитест
4.7	Тестирование на проникновение в сеть через пограничные устройства	3	2	1	Минитест
4.8	Методология тестирования на проникновение в веб-приложения	3	1	2	Минитест
4.9	Методология тестирования на проникновение в базы данных	4	2	2	Минитест
4.10	Методология тестирования на проникновение в беспроводные сети	3	2	1	Минитест
4.11	Методология тестирования на проникновение в облачные сервисы	3	2	1	Минитес
4.12	Отчеты и действия после тестирования на проникновение	4	1	3	Минитес
	ИТОГО:	**160**	**91,5**	**68,5**	