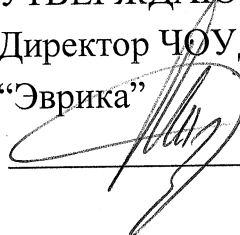


Частное образовательное учреждение дополнительного образования
«Учебный центр «Эврика»
(Наименование образовательного учреждения)

УТВЕРЖДАЮ
Директор ЧОУДО «Учебный центр
«Эврика»

/Мазепин С.А.

Образовательная программа дополнительного профессионального образования
(повышения квалификации)
по направлению

19. Основы управления сетевой безопасностью-Код безопасности
(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».

Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Программа обучения рассчитана на освоение системы базовых знаний по программным и техническим решениям защиты информации на примере продуктов компаний Код Безопасности.

«Континент» – семейство продуктов для обеспечения сетевой безопасности при подключении к сетям общего пользования посредством межсетевое экранирования, построения частных виртуальных сетей (VPN) и системы обнаружения вторжений (СОВ).

АПКШ «Континент» предназначен для решения следующих типовых задач:

Средство защиты информации Secret Net 7 предназначено для защиты информации на рабочих станциях и серверах в соответствии с требованиями регулирующих органов и контроля утечек и каналов распространения защищаемой информации

В результате обучения слушатели получают теоретические знания и практические навыки,

В результате обучения слушатели получают теоретические знания и практические навыки, необходимые для инсталляции и управления компонентами комплекса, настройки защиты данных, передаваемых по сетям общего пользования, межсетевое экранирование и маршрутизации трафика.

Во время прохождения обучения слушатели будут создавать виртуальные частные сети на основе общих сетей передачи данных, правильно настраивать межсетевое экранирование и маршрутизацию трафика, скрывать внутреннюю структуру ЛВС с применением технологии NAT, осуществлять мониторинг и аудит системы.

Во время прохождения обучения слушатели ознакомятся с возможными нештатными ситуациями в системе защиты, научатся диагностировать их средствами АПКШ «Континент» и выполнять необходимые меры по их устранению.

В результате обучения слушатели получают теоретические знания и практические навыки, необходимые для диагностики и предупреждения проблемных ситуаций, навыков «тонкой» настройки механизмов защиты, способов отладки и обеспечения бесперебойной работы системы.

Программа обеспечивает получение теоретических знаний и практических навыков, необходимых для инсталляции компонентов, настройки защитных подсистем, управления политиками безопасности, аудита и мониторинга состояний рабочих станций.

В процессе прохождения обучения слушатели ознакомятся с особенностями развертывания компонентов vGate, конфигурированием и применением механизмов защиты виртуальных машин, возможностями управления доступом к конфиденциальным ресурсам посредством иерархических и неиерархических меток безопасности

Во время прохождения обучения слушатели будут учиться устанавливать и настраивать механизмы защиты системы Secret Net Studio, используя интерфейс администрирования SNS в автономном и сетевом режимах

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-информационным 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

19. Основы управления сетевой безопасностью-Код безопасности

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: 96 академических часов

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

п/п	Наименование разделов и соответствующим модулям (номер или аббревиатура курса)	Всего часов	В том числе:		Формы контроля
			Лекции	Практические занятия	
1	2	3	4	5	6
1	Администрирование АПКШ Континент 3.9.	32	17	15	

	Базовый (Cont39_base)				
1.1	Обзор технологий и развертывание системы защиты				минитест
1.2	Управление компонентами комплекса	4	2	2	минитест
1.3	Правила фильтрации IP-пакетов и правила трансляции	3	2	1	минитест
1.4	Детектор атак	3	2	1	минитест
1.5	Организация и управление VPN-соединениями	3	1	2	минитест
1.6	Обеспечение отказоустойчивости комплекса	4	2	2	минитест
1.7	Мониторинг и диагностика системы защиты	3	1	2	минитест
1.8	Обновление версии ПО	3	1	2	минитест
1.9	Резервирование и отказоустойчивость каналов связи	3	2	1	минитест
1.10	Поиск и устранение неисправностей	3	2	1	минитест
2	Администрирование АПКШ Континент 3.9. Дополнительные настройки (Cont37_ext)	8	4	4	
2.1	Управление QoS	4	2	2	минитест
2.2	Поддержка динамической маршрутизации в "АПКШ Континент"	4	2	2	минитест
3	Применение системы защиты Secret Net Studio (SN8_base)	32	17	15	
3.1	Принципы построения системы Secret Net Studio и способы ее развертывания	6	3	3	минитест
3.2	Настройка и применение компонентов базовой защиты Secret Net Studio	4	2	2	минитест
3.3	Настройка и применение компонентов локальной защиты Secret Net Studio	6	3	3	минитест
3.4	Персональный межсетевой экран	6	3	3	минитест
3.5	Защита от вирусов и вредоносного ПО	4	2	2	минитест
3.6	Организация защиты средствами Secret Net Studio	6	4	2	минитест
4	Отчеты, инциденты, их анализ и порядок реагирования в Secret Net Studio (SN8_report)	8	5	2	
4.1	Основные термины и понятия при рассмотрении инцидентов информационной безопасности	2	1	1	минитест
4.2	Нормативные документы в области обеспечения аудита и анализа инцидентов информационной безопасности в организациях банковской сферы Российской Федерации	2	1	1	минитест
4.3	Особенности организации аудита событий в Secret Net Studio	2	1	1	минитест
4.4	Особенности настройки механизма аудита событий в Secret Net Studio (автономная версия)	1	1	0	минитест
4.5	Лабораторный практикум	1	1	0	минитест
5	Защита виртуальных инфраструктур средствами vGate (vGate)	16	6	10	
5.1	Применение vGate для обеспечения информационной безопасности в виртуальной среде.	4	2	2	минитест
5.2	Настройка и применение компонентов защиты vGate	4	2	2	минитест

5.3	Аудит событий в системе и подготовка отчетов защиты vGate	4	1	3	минитест
5.4	Некоторые вопросы, связанные с использованием системы vGate	4	1	3	минитест
	ИТОГО:	96	49	46	Зачет