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

32. Основы информационной безопасности с помощью продуктов Лаборатории Касперского

(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».

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности и цифровой приватности с 1997 года. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и рядовых пользователей.

Изучение информационной безопасности с помощью продуктов Лаборатории Касперского направлено на достижение следующих целей:

- **освоение системы базовых знаний**

для внедрения, настройки и обслуживании Kaspersky Security 11 для Windows Server в средних и крупных организациях.

овладение умениями

- Описать возможности Kaspersky Endpoint Security дляWindows и Kaspersky Security Center;
- Спроектировать и внедрить оптимальное решение для защиты сетей Windows, основанное на Kaspersky Endpoint Security и управляемое через Kaspersky Security Center;
- Осуществлять обслуживание внедренной системы на всех стадиях эксплуатации.
- Описать возможности Kaspersky Security для Windows Server;
- Настроить компоненты защиты Kaspersky Security для Windows Server;
- Управлять защитой файловых серверов, сетевых хранилищ, удаленных рабочих столов и киосков.
- Управлять уязвимостями и обновлениями программ на компьютерах сети;
- Захватывать, изменять настройки и устанавливать образы операционных систем;
- Работать с реестрами программного и аппаратного обеспечения, а также управлять лицензиями сторонних приложений и настраивать интеграцию с SIEM-системами
- Описать возможности Kaspersky Security для виртуальных сред | Защита без агента и рассказать о его преимуществах в сравнении с обычной защитой;
- Внедрить защиту в среду виртуализации центра обработки данных;
- Настроить политики защиты и использовать средства мониторинга Kaspersky Security Center и VMware vSphere для обслуживания защиты.
- Развернуть Kaspersky Unified Management & Analysis для демонстрации решения
- Настроить получение событий из разных источников и в разных форматах
- Донастроить нормализацию, агрегацию и обогащение событий согласно требованиям
- Настроить корреляционные правила для обнаружения инцидентов
- Настроить взаимодействие с внешними системами с целью обогащения событий и реагирования на инциденты
- Обработать инциденты и вручную проанализировать события
- Настроить уведомления и создать отчеты о работе решения.
- Спроектировать и реализовать систему управления защитой в большой и/или территориально распределенной сети, в том числе за счет использования иерархии Серверов администрирования;
- Спроектировать и организовать оптимальную архитектуру для распространения обновлений в большой и/или территориально распределенной сети, в том числе с использованием точек распространения;
- Настроить Kaspersky Security Center для управления устройствами за пределами периметра организации, в том числе с использованием шлюзов соединений.

приобретение опыта

- Слушатели получат знания и навыки, на которые будут опираться в своей ежедневной работе системного администратора, специалистов и администраторов безопасности
- смогут выполнять расширенные административные задачи

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

32. Основы информационной безопасности с помощью продуктов Лаборатории Касперского

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

Цель: Подготовка слушателей для обеспечения информационной безопасности с помощью продуктов Лаборатории Касперского.

По окончании обучения слушатели смогут:
Категория слушателей: для лиц, имеющих высшее и среднее профессиональное образование
Срок обучения: 64 академических часа

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	**Курс KL 002.11.6: Kaspersky Endpoint Security and Management**	**24**	**12**	**12**	
1.1	Введение	6	3	3	Минитест
1.2	Управление защитой	6	3	3	Минитест
1.3	Контроль	6	3	3	Минитест
1.4	Сопровождение	6	3	3	Минитест
2.	**Курс KL 005.11 :Защита серверов Windows и встраиваемых систем**	**16**	**12**	**4**	Минитест
2.1	Введение	1	1		Минитест
2.2	Внедрение	2	1	1	Минитест
2.3	Настройка групповых задач	2	1	1	Минитест
2.4	Защита файловой системы	1	1		Минитест
2.5	Защита от сетевых угроз	1	1		Минитест
2.6	Защита служб Удаленного Рабочего Стола	1	1		Минитест
2.7	Компоненты контроля сервера	2	1	1	Минитест
2.8	Контроль устройств	2	1	1	Минитест
2.9	Диагностика системы	2	1		
2.10	Защита систем хранения данных	1	1		Минитест
2.11	Дополнительные настройки	1	1		Минитест

3.	**Курс KL 009.12 Kaspersky Security Center. Systems Management**	**8**	**4**	**4**	Минитест
3.1	Введение	2	1	1	Минитест
3.2	Управление уязвимостями и обновлениями программ	2	1	1	Минитест
3.3	Захват и развертывание образов компьютеров	2	1	1	Минитест
3.4	Интеграция с SIEM и другие возможности Kaspersky Systems Management	2	1	1	Минитест
4.	**КУРС KL 034.2 Платформа унифицированного мониторинга и анализа от Лаборатории Касперского**	**16**	**9**	**7**	Минитест
4.1	Общие сведения	2	1	1	Минитест
4.2	Установка Темы	2	1	1	Минитест
4.3	Сбор и обработка событий	2	1	1	Минитест
4.4	Интеграции	2	1	1	Минитест
4.5	Нормализация	3	2	1	Минитест
4.6	Корреляция и работа с событиями	3	2	1	Минитест
4.7	Реагирование, алерты, отчеты и мониторинг	2	1	1	Минитест
	ИТОГО:	**64**	**37**	**27**	**Зачет**