ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ИНВЕНТА» (ЧОУ ДПО «ИНВЕНТА»)

УТВЕРЖДАЮ:
Директор ЧОУ ДПО «ИНВЕНТА»
Потехин Е.Г
____
«17» июня 2020 г.
м.п.

Дополнительная профессиональная
образовательная программа повышения квалификации
RH415 « Red Hat Security: Linux in Physical, Virtual, and Cloud»

Москва
2020 год

1. Целевая установка

Цель обучения: Целью реализации программы является обучение слушателей администраторам безопасности, инженерам безопасности и другим специалистам, отвечающим за дизайн, внедрение, поддержку и управление безопасности на серверах под управлением Red Hat Enterprise Linux, а также за соответствие настроек этих серверов политикам безопасности организации

Категория слушателей: Курс предназначен для администраторов безопасности и системных администраторов, управляющих настройками безопасности Red Hat Enterprise Linux в физической, виртуальной или облачной среде.

2. Планируемые результаты обучения

Реализация Программы направлена на повышение профессионального уровня в рамках имеющейся квалификации, определяемой профессиональным стандартом «06.026 Системный администратор информационно-коммуникационных систем», утвержденным Приказом Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем".

Результатами обучения по Программе станут знания и умения, соответствующие следующим обобщенным трудовым функциям указанного профессионального стандарта:

Администрирование системного программного обеспечения инфокоммуникационной системы организации.

Совершенствуемые компетенции в соответствии с трудовыми функциями профессионального стандарта:

Компетенция	**Содержание компетенции** Трудовые функции	**Код**
Администрирование системного программного обеспечения инфокоммуникационной системы организации	Установка системного программного обеспечения	F/01.7
	Оптимизация работы дисковой подсистемы (подсистемы ввода-вывода)	F/02.7
	Администрирование файловых систем	F/03.7
	Оценка критичности возникновения инцидентов для системного программного обеспечения	F/04.7
	Реализация регламентов обеспечения информационной безопасности системного программного обеспечения инфокоммуникационной системы организации	F/05.7

После завершения курса слушатели получат навыки, позволяющие им:

- управление безопасностью и рисками
- автоматизация настроек параметров безопасности при помощи Ansible
- защита данных при помощи LUKS и NBDE
- ограничение доступа к устройствам USB
- контроль аутентификации при помощи PAM
- сохранение системных событий при помощи audit
- отслеживание изменений файловой системы
- уменьшение рисков при помощи SELinux
- обеспечение совместимости с политиками безопасности при помощи OpenSCAP
- автоматизация процесса обеспечения совместимости с политиками безопасности при помощи Red Hat Satellite
- анализ и устранение проблем безопасности при помощи Red Hat Insights

3. Учебный план

№ п/п	Наименование модулей/дисциплин и тем	Трудоемкость, час.	В том числе				Форма аттестации, трудоемкость, ак. час
			лекционного типа	Практические, семинарские занятия, лабораторные работы	Тренинги, деловые и ролевые игры, круглые столы	Выездные занятия, эл.обучение и т.д.	
1	Управление безопасностью и рисками	3	2,5	0,5	-	-	Прак. занятие
2	Автоматизация настроек параметров безопасности при помощи Ansible	2	1	1	-	-	Прак. занятие
3	Защита данных при помощи LUKS и NBDE	3,5	2,5	1	-	-	Прак. занятие
4	Ограничение доступа к устройствам USB	1,5	0,5	1	-	-	Прак. занятие
5	Контроль аутентификации при помощи PAM	3	1,5	1,5	-	-	Прак. занятие
6	Сохранение системных событий при помощи audit	3	1,5	1,5	-	-	Прак. занятие
7	Отслеживание изменений файловой системы	3	1	2	-	-	Прак. занятие
8	Уменьшение рисков при помощи SELinux	2	1	1	-	-	Прак. занятие
9	Обеспечение совместимости с	2	1	1	-	-	Прак. занятие

№ п/п	Наименование модулей/дисциплин и тем	Трудоемкость, час.	В том числе				Форма аттестации, трудоемкость, ак. час
			лекционного типа	Практические, семинарские занятия, лабораторные работы	Тренинги, деловые и ролевые игры, круглые столы	Выездные занятия, эл.обучение и т.д.	
	политиками безопасности при помощи OpenSCAP						
10	Автоматизация процесса обеспечения совместимости с политиками безопасности при помощи Red Hat Satellite	3	2	1	-	-	Прак. занятие
11	Анализ и устранение проблем безопасности при помощи Red Hat Insights	2	1	1	-	-	Прак. занятие
12	**Итоговая аттестация** (лабораторная работа)	**4**	-	**4**	-	-	Прак. занятие
	ИТОГО	**32**	**15,5**	**16,5**	**0**	**0**	

4. Календарный учебный график

Календарный учебный график составляется в форме расписания занятий при наборе группы и прилагается к программе повышения квалификации.

Форма обучения: очная с отрывом от производства
Трудоемкость программы: 32 часа
Сроки освоения программы: 4 дня
Режим занятий: 8 (Восемь) часов в день, перерыв на обед 45 минут.

5. Рабочие программы дисциплин

Модуль 1. Управление безопасностью и рисками

- Управление безопасностью и рисками
- Обзор рекомендуемых практик безопасности

Модуль 2. Автоматизация настроек параметров безопасности при помощи Ansible

- Настройка Ansible для автоматизации безопасности
- Исправление проблем с Ansible Playbooks
- Управление Playbook с помощью Red Hat Ansible Tower

Модуль 3. Защита данных при помощи LUKS и NBDE

- Шифрование управляющей файловой системы с помощью LUKS
- Дешифровка контролирующей файловой системы с помощью NBDE

Модуль 4. Ограничение доступа к устройствам USB

- Управление доступа к устройствам USB
- Ограничение доступа к USB-устройствам

Модуль 5. Контроль аутентификации при помощи PAM

- Аудит конфигурации PAM
- Изменение конфигурации PAM
- Настройка требований к качеству пароля
- Ограничение доступа после неудачных входов

Модуль 6. Сохранение системных событий при помощи audit

- Настройка audit для записи системных событий
- Проверка журналов audit
- Написание пользовательских правил audit
- Включение готовых наборов правил audit

Модуль 7. Отслеживание изменений файловой системы

- Обнаружение изменений файловой системы с помощью AIDE
- Изучение изменений файловой системы с помощью AIDE

Модуль 8. Уменьшение рисков при помощи SELinux

- Включение SELinux из отключенного состояния
- Управление доступом с ограниченными пользователями
- Аудит политики SELinux

Модуль 9. Обеспечение совместимости с политиками безопасности при помощи OpenSCAP

- Установка OpenSCAP
- Сканирование и анализ соответствия требованиям
- Настройка политики OpenSCAP
- Устранение проблем OpenSCAP с помощью Ansible

Модуль 10. Автоматизация процесса обеспечения совместимости с политиками безопасности при помощи Red Hat Satellite

- Настройка Red Hat Satellite для OpenSCAP

- Сканирование на соответствие OpenSCAP с Red Hat Satellite
- Настройка политики OpenSCAP в Red Hat Satellite

Модуль 11. Анализ и устранение проблем безопасности при помощи Red Hat Insights

- Регистрация систем с Red Hat Insights
- Просмотр отчетов Red Hat Insights
- Автоматизация устранения проблем

6. Организационно-педагогические условия реализации программы

6.1. Материально-технические условия реализации программы

ЧОУ ДПО «ИНВЕНТА» обеспечивает для проведения обучения следующие средства вычислительной техники:

- персональный компьютер для преподавателя – 1 шт.
- персональный компьютер для каждого Слушателя
- проектор и экран – 1 комплект
- доска – 1 шт.

Персональные компьютеры объединены в локальную вычислительную сеть.

Технические характеристики персональных компьютеров:

- процессор 4 ядра 2,7 ГГц
- оперативная память - 8 Гб
- жесткий диск - 1 Тб
- монитор 21,5 ", разрешение 1920x1080

6.2. Учебно-методическое обеспечение программы

Каждый Слушатель обеспечивается авторизованным учебным пособием на английском языке в электронном или бумажном виде

7. Требования к профессорско-преподавательскому составу

Высшее профессиональное образование и стаж работы в образовательном учреждение не менее 1 года. Статус Red Hat Certified Instructor.

8. Формы аттестации

Текущий контроль успеваемости и качества подготовки, промежуточная и итоговая аттестации слушателей осуществляются в процессе изучения, освоения данной профессиональной образовательной программы повышения квалификации.

Текущий контроль успеваемости и качества подготовки осуществляется в пределах времени, отведенного на учебные занятия, и выполняет одновременно обучающую функцию. Текущий контроль успеваемости проводится в процессе изучения каждого раздела (темы, подтемы) внутри модуля данной дополнительной профессиональной программы и проводится в форме устного опроса преподавателя.

Промежуточная и итоговая аттестации проводятся в форме лабораторных работ на персональном компьютере слушателя, который использовался во время обучения, в классе под наблюдением преподавателя.

По окончании каждого модуля рабочей программы проводится промежуточная аттестация в виде промежуточной лабораторной работы по теме каждого модуля данной профессиональной образовательной программы.

Итоговая аттестация проводится в форме итоговой лабораторной работы. В итоговой лабораторной работе задействуются материалы из всех модулей пройденной программы, а именно:

1. управление безопасностью и рисками
2. автоматизация настроек параметров безопасности при помощи Ansible
3. защита данных при помощи LUKS и NBDE
4. ограничение доступа к устройствам USB
5. контроль аутентификации при помощи PAM
6. сохранение системных событий при помощи audit
7. отслеживание изменений файловой системы
8. уменьшение рисков при помощи SELinux
9. обеспечение совместимости с политиками безопасности при помощи OpenSCAP
10. автоматизация процесса обеспечения совместимости с политиками безопасности при помощи Red Hat Satellite
11. анализ и устранение проблем безопасности при помощи Red Hat Insights

Аттестация считается пройденной в случае успешного завершения итоговой лабораторной работы, а именно: выполнения поставленной задачи: «Настройка системы Red Hat Linux. Создание текстового файла с помощью командной строки. Организация доступа к файловой системе» на персональном компьютере.

Время выполнения итоговой аттестации – 4 часа.