НОЧУ ДПО УЦ «Сетевая Академия»

УТВЕРЖДАЮ
Директор НОЧУ ДПО УЦ «Сетевая Академия»
_____/М.М. Макарова/

Образовательная программа
дополнительного профессионального образования
(повышения квалификации)
«Средство анализа защищенности RedCheck»
(код курса – RCPC)

Содержание

Описание образовательной программы

Настоящая образовательная программа повышения квалификации (далее – Программа) разработана в соответствии с:

1. Федеральным законом от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации»
2. Приказом Минобрнауки России от 1 июля 2013 г. N 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»
3. Уставом НОЧУ ДПО УЦ «Сетевая Академия»

Структура Программы включает цели, планируемые результаты обучения, учебный план, календарный учебный график, рабочую программу, организационно-педагогические условия, формы аттестации и оценочные материалы.

Цели Программы содержат описание целевой аудитории, целей обучения и необходимых начальных знаний и навыков слушателей.

Планируемые результаты обучения представлены в виде перечня профессиональных компетенций в рамках имеющейся квалификации (с отсылкой к профессиональному стандарту), качественное изменение которых осуществляется в результате обучения.

Учебный план определяет перечень, трудоемкость, последовательность и распределение модулей, иных видов учебной деятельности обучающихся и формы аттестации.

Календарный учебный график определяет основные параметры учебного процесса при организации занятий по освоению настоящей Программы, включая формы обучения, расписание занятий очных групп и т.п.

Рабочая программа раскрывает рекомендуемую последовательность изучения разделов (модулей).

Описание организационно-педагогических условий реализации Программы определяет организационные и методические требования НОЧУ ДПО УЦ «Сетевая Академия» к организации и проведению обучения по Программе.

Формы аттестации и оценочные материалы определяют формы проведения промежуточной и итоговой аттестации по Программе и форму учебно-методических материалов, необходимых для проведения указанных видов аттестации.

Цели программы

Данная программа предназначена для:

- системных администраторов, поддерживающих работоспособность сетевой среды передачи данных и программного обеспечения, установленного на подконтрольных машинах парка вычислительной техники предприятия;
- IT-специалистов, в рамках ответственности которых находится обеспечение безопасности IT-инфраструктуры предприятия;
- администраторов информационной безопасности, отвечающих за выполнение Политик безопасности предприятия.

Целью обучения является формирование у слушателей знаний и навыков, необходимых для администрирования и поддержания в работоспособном состоянии программного комплекса RedCheck, а также эффективной работы с программным комплексом.

Для изучения данной Программы рекомендуется обладать следующими знаниями и навыками:

- Профессиональные навыки в эксплуатации операционных систем семейства Windows.
- Опыт администрирования сетевого программного обеспечения.

Планируемые результаты обучения

Реализация Программы направлена на повышение профессионального уровня в рамках имеющейся квалификации, определяемой профессиональными стандартами «06.026 Системный администратор информационно-коммуникационных систем», утвержденным Приказом Минтруда России от 29.09.2020 №680н «Об утверждении профессионального стандарта «Системный администратор информационно-коммуникационных систем».

Результатами обучения по Программе станут знания и умения, соответствующие следующим обобщенным трудовым функциям указанных профессиональных стандартов:

- Обслуживание информационно-коммуникационной системы.
- Обслуживание серверных операционных систем информационно-коммуникационной системы.

Совершенствуемые компетенции в соответствии с трудовыми функциями профессионального стандарта:

Компетенция	**Содержание компетенции** Трудовые функции	**Код**
Обслуживание информационно-коммуникационной системы	Выполнение работ по выявлению и устранению инцидентов в информационно-коммуникационных системах	B/01.5
	Обеспечение работы технических и программных средств информационно-коммуникационных систем	B/02.5
	Реализация схемы резервного копирования, архивирования и восстановления конфигураций технических и программных средств информационно-коммуникационных систем по утвержденным планам	B/03.5
	Внесение изменений в технические и программные средства информационно-коммуникационных систем по утвержденному плану работ	B/04.5
	Проведение обновления программного обеспечения технических средств информационно-коммуникационных систем по инструкциям производителей	B/05.5
	Диагностика исчерпания типовых ресурсов информационно-коммуникационных систем с использованием прикладных программных средств и средств контроля	B/06.5
Обслуживание серверных операционных систем информационно-коммуникационной системы	Выполнение работ по выявлению и устранению нетипичных инцидентов, возникающих в серверных операционных системах информационно-коммуникационной системы	D/01.6
	Проведение анализа и определение основных причин сложных проблем, возникающих на серверах и в серверных операционных системах	D/02.6
	Выполнение планирования резервного копирования, архивирования и восстановления конфигурации серверов и серверных операционных систем	D/03.6
	Планирование изменений параметров работы серверов и серверных операционных систем	D/04.6
	Выполнение обновления программного обеспечения серверных операционных систем	D/05.6
	Прогнозирование влияния внешних и внутренних воздействий на поведение серверных операционных систем	D/06.6
	Прогнозирование потребности в изменении объемов необходимых ресурсов для обеспечения бесперебойной работы серверов и серверных операционных систем	D/07.6

	Планирование и проведение работ по распределению нагрузки между имеющимися ресурсами, снятию нагрузки на серверы и серверные операционные системы перед проведением регламентных работ, восстановлению штатной схемы работы в случае сбоев	D/08.6

После обучения слушатель сможет:

- Подготовить инфраструктуру для установки программного комплекса RedCheck.
- Установить сканер RedCheck и агентов RedCheck.
- Подготовить хосты и другие объекты инфраструктуры для сканирования.
- Выполнять сканирование различных типов.
- Обеспечить правильное функционирование программного комплекса RedCheck.
- Настроить программный комплекс RedCheck в соответствии с принятой на предприятии Политикой безопасности.

Учебный план

Учебный план Программы определяет перечень, трудоемкость, последовательность и распределение модулей, иных видов учебной деятельности обучающихся и формы аттестации.

№ п/п	Наименование разделов (модулей)	Всего, час	В том числе		Форма аттестации
			Лекции	Практические занятия	
1.	Средство анализа защищенности RedCheck. Введение.	1,25	1	0,25	Опрос, практические задания
2.	Установка программного комплекса	4,5	2	2,5	Опрос, практические задания
3.	Настройка	4,5	2,25	2,25	Опрос, практические задания
4.	Сканирование	3,5	1,75	1,75	Опрос, практические задания
5.	Детали архитектуры, настройки, сценарии применения	1,25	1	0,25	Опрос, практические задания
6.	Итоговая аттестация	1	-	1	Экзамен-тест
	Итого:	**16**	**8**	**8**	

Допускается формирование индивидуального учебного плана для каждого слушателя в пределах осваиваемой Программы в порядке, установленном Положением об организации образовательного процесса в НОЧУ ДПО УЦ «Сетевая Академия».

Календарный учебный график

Учебный год: круглогодичное обучение.

Продолжительность Программы: 16 академических часов.

Форма организации образовательного процесса: очная, очно-заочная (вечерняя) и заочная формы обучения, в том числе, с применением дистанционных образовательных технологий и электронного обучения.

Сменность занятий (при очной форме обучения): I смена.

Количество учебных дней в неделю при очном обучении: 2 дня.

Начало учебных занятий: 9.30

Окончание учебных занятий: 17.00

Продолжительность урока: 45 минут (1 академический час).

Продолжительность перемен: 15 минут, перерыв на обед – 60 минут.

Расписание занятий для очных групп:

	№ урока	**Время**
Конкретный день недели согласовывается во время учебного процесса	1, 2	09:30 - 11:00
	3, 4	11:15 - 12:45
	5, 6	13:45 - 15:15
	7, 8	15:30 - 17:00

Рабочая программа

Тема 1: **Средство анализа защищенности RedCheck. Введение**

- О программном комплексе.
- Возможности RedCheck.
- Аудит уязвимостей.
- Объекты для аудита уязвимостей.
- Репозитории OVALdb.
- Аудит защищенности СУБД.
- Контроль конфигураций и оценка соответствия политикам и стандартам безопасности.
- Управление обновлениями.
- Аудит серверов приложений.
- Аудит в режиме Пентест.
- Детальный аудит платформ виртуализации.
- Инвентаризация сети.
- Контроль целостности.
- Контроль состояния.
- Документирование.
- Создание интегральных и дифференциальных отчетов.
- Другие полезные функции.
- Аудит безопасности.
- Аттестация объектов информатизации.
- Реализация мер защиты ГИС и ИСПДн.
- Архитектура сканера.
- *Тестирование: Возможности RedCheck.*

Тема 2: Установка программного комплекса

- Лицензирование.
- Редакции программы RedCheck.
- Требования к аппаратному обеспечению.
- Расчет объема HDD, предназначенного для хранения контента безопасности и результатов сканирования RedCheck.
- *Упражнение: Расчет объема HDD, предназначенного для хранения контента безопасности и результатов сканирования RedCheck.*
- Типы учетных записей для работы с консолью RedCheck.
- Ролевая модель RedCheck.
- Основные задачи ролей в программе RedCheck.
- *Практическая работа 1. Подготовка учетных записей.*
- Общие рекомендации по настройке учетных записей.
- Подготовка СУБД.
- Настройка СУБД в режиме смешанной авторизации.
- Настройка СУБД в режиме Доменной авторизации.
- *Практическая работа 2. Подготовка доменной среды для установки СУБД Microsoft SQL Server.*
- Подключение к внешней СУБД.
- *Практическая работа 3. Установка СУБД Microsoft SQL Server.*
- *Практическая работа 4. Настройка SQL Server.*
- *Практическая работа 5*. Установка SQL Server Management Studio.*
- Требования к программному обеспечению.
- Получение дистрибутива RedCheck.
- Требования к сетевой инфраструктуре.
- Установка сканера RedCheck.

- Выбор типа синхронизируемого контента.
- Продолжение процесса установки.
- *Практическая работа 6. Установка консоли управления и сканера RedCheck.*
- Синхронизация контента безопасности.
- *Практическая работа 7. Обновление контента синхронизации в режиме офлайн.*
- Веб-консоль RedCheck.
- *Практическая работа 8. Установка WEB-консоли управления RedCheck.*
- *Практическая работа 9*. Настройка браузера Internet Explorer для работы в RedCheckWeb.*
- Установка агента RedCheckAgent.
- *Практическая работа 10. Установка агента RedCheckAgent.*
- Развертывание агента для Windows-систем средствами Active Directory.
- *Тестирование: Установка программного комплекса.*

Тема 3: Настройка

- Настройка сетевого взаимодействия для сканирования Windows систем с применением агента.
- *Практическая работа 11. Локальная настройка сетевого взаимодействия для безагентского сканирования с использованием службы WMI.*
- Настройка сетевого взаимодействия для безагентского сканирования с использованием службы WMI.
- *Практическая работа 12. Настройка сетевого взаимодействия для безагентского сканирования с использованием службы WMI.*
- Настройка сетевого доступа.
- Настройка контроля учетных записей пользователей.
- Полное отключение UAC.
- Отключение UAC для всех учетных записей сканируемого узла при удаленных подключениях.
- Использование доменной учётной записи.
- *Практическая работа 13. Создание доменной учетной записи с правами локального администратора на доменных хостах.*
- Настройка сетевого взаимодействия для сканирования с использованием службы Remote Engine (WinRM).
- Настройка сканируемого узла.
- *Практическая работа 14. Настройка сетевого взаимодействия для сканирования Windows систем с использованием WinRM.*
- *Практическая работа 15. Настройка сканируемого узла для использования WinRM.*
- Настройка сервера управления RedCheck.
- *Практическая работа 16. Настройка сервера управления RedCheck.*
- Графический интерфейс.
- Статусная панель.
- Статус проверки обновления контента.
- Вкладка «Главная».
- Вкладка «Хосты».
- Вкладка «Задания».
- Вкладка «История».
- Значения в столбце Риск.
- Действия с заданиями.
- Результаты сканирования для задания «Аудит уязвимостей».
- Фильтр сканирований заданий.
- Вкладка «Контроль».
- Создание контроля.

- Фильтр средств сравнения с эталонными показателями.
- Вкладка «Отчеты».
- Фильтр отчетов.
- Меню «Действия».
- Меню «Инструменты».
- Меню «Инструменты». Пункт «Менеджер аудитов».
- Меню «Инструменты». Пункт «Менеджер конфигураций».
- Меню «Инструменты». Пункт «Консоль WSUS».
- Меню «Инструменты». Пункт «Создать группу».
- Меню «Инструменты». Пункт «Создать хост».
- Меню «Инструменты». Пункт «Импорт хостов».
- Меню «Инструменты». Пункт «Синхронизация».
- Меню «Инструменты». Пункт «Импорт OVAL определений».
- Меню «Инструменты». Раздел «Настройки».
- Меню «Инструменты». Раздел «Настройки». Вкладка «Компонент Nmap».
- Меню «Инструменты». Раздел «Настройки». Вкладка «Доставка».
- Меню «Инструменты». Раздел «Настройки». Вкладка «Дополнительно».
- Меню «Инструменты». Пункт «Журнал событий».
- Меню «Инструменты». Пункт «Подключения».
- Меню «Инструменты». Пункт «Диагностика».
- Меню «Справка».
- Добавление учетных записей.
- Редактирование и удаление учетных записей.
- Принципы работы с учетными записями.
- *Практическая работа 17. Работа с менеджером учетных записей.*
- *Тестирование: Настройка программного комплекса RedCheck.*

Тема 4: **Сканирование**

- Добавление группы хостов.
- *Практическая работа 18. Добавление группы хостов.*
- Добавление хостов.
- *Практическая работа 19. Добавление хостов.*
- Проверка работоспособности туннелей (команда Пинг).
- *Практическая работа 20. Проверка работоспособности туннелей (команда Пинг).*
- Создание профиля сканирования.
- *Практическая работа 21. Создание профиля сканирования.*
- Задания. Параметры заданий.
- Создание заданий.
- Аудит уязвимостей.
- *Практическая работа 22. Создание задания на аудит уязвимостей Windows хоста.*
- *Практическая работа 23. Создание задания на аудит уязвимостей Linux хоста.*
- Аудит обновлений.
- Аудит конфигураций.
- *Практическая работа 24*. Создание задания на аудит конфигураций.*
- Аудит СУБД.
- *Практическая работа 25*. Создание задания на аудит СУБД.*
- Инвентаризация.
- *Практическая работа 26*. Создание задания на инвентаризацию.*
- Фиксация.
- Аудит в режиме «Пентест»
- *Практическая работа 27*. Создание задания на Аудит в режиме «Пентест».*
- История.

- История аудита конфигураций.
- История инвентаризации.
- История аудита обновлений.
- История аудита уязвимостей.
- История фиксации.
- История аудита СУБД.
- История аудита в режиме «Пентест».
- Отчеты.
- Настройки нового отчета.
- Настройка содержимого отчёта.
- *Практическая работа 28. Создание отчета.*
- Настройка доставки отчетов в папку.
- *Практическая работа 29*. Создание задания с использованием профиля сканирования и размещением отчета в сетевой папке.*
- *Тестирование: Выполнение сканирования с помощью RedCheck.*

Тема 5: **Детали архитектуры, настройки, сценарии применения**

- Контроль защищенности малых и средних сетей.
- Контроль защищенности территориально удаленной сети.
- Контроль (анализ) защищенности крупных сетей и сетей с филиальной структурой.
- Интеграция с SIEM и СУИБ.
- Лицензирование.
- REDCHECK ENTERPRISE.
- Максимальный состав системы RedCheck Enterprise.
- Установка и настройка дополнительной службы сканирования RedCheck.
- Установка и настройка дополнительной службы синхронизации RedCheck.
- Дискуссия: Лицензирование и размещение компонентов.
- Работа с WEB-сервисом OVALdb. Получение расширенной информации.
- Работа с WEB-сервисом OVALdb. Поиск по OVALdb.
- Другие возможности OVALdb.
- Проверка целостности контента.
- Обслуживание СУБД.
- *Тестирование: Применение RedCheck в различных средах, работа с WEB-сервисом OVALdb.*

Организационно-педагогические условия реализации Программы

При реализации Программы применяется форма организации образовательной деятельности, основанная на модульном принципе представления содержания образовательной программы и построения учебных планов, использовании различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения.

Организационные условия реализации программы в разных формах обучения регулируются следующими локальными нормативными актами:

- Положение об организации образовательного процесса в НОЧУ ДПО УЦ «Сетевая Академия».
- Положение о порядке применения электронного обучения, дистанционных образовательных технологий в НОЧУ ДПО УЦ «Сетевая Академия».

Учебные материалы по Программе включают: рабочую программу, раздаточные материалы по курсу, методические материалы по курсу, данные примеров по курсу. Учебное пособие по Программе выдается слушателям в бумажном или электронном виде в зависимости от формы обучения в порядке, установленном Положением о библиотеке в НОЧУ ДПО УЦ «Сетевая Академия».

Занятия по Программе проводятся преподавателями, предварительно подтвердившими свою квалификацию. В числе базовых требований ко всем преподавателям – требование обязательного прохождения программы «Андрагогика. Эффективное обучение взрослых» в форме учебного курса и/или пробной лекции, а также сдачи технических сертификационных тестов по продукту или технологии, рассматриваемым в курсе.

Формы аттестации и оценочные материалы

Освоение Программы сопровождается промежуточной аттестацией обучающихся в формах, определенных учебным планом, и в порядке, установленном Положением об организации образовательного процесса в НОЧУ ДПО УЦ «Сетевая Академия».

Освоение Программы завершается итоговой аттестацией обучающихся в форме, определенной учебным планом, и в порядке, установленном Положением об организации образовательного процесса в НОЧУ ДПО УЦ «Сетевая Академия».

Слушателям, успешно освоившим соответствующую Программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации на бланке, образец которого самостоятельно устанавливается организацией.

Слушателям, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть Программы и (или) отчисленным из организации, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому организацией.

Оценочные материалы для промежуточной аттестации по Программе разрабатываются в форме лабораторных работ и/или контрольных вопросов после изучения каждого модуля.

Оценочные материалы для итоговой аттестации по Программе разрабатываются в форме теста.

Пример материалов для итоговой аттестации

1. **Вопрос:** Серверные операционные системы Microsoft могут быть объектами аудита RedCheck, начиная с
   Варианты ответов:
   A. Windows Server 2003
   B. Windows Server 2008
   C. Windows Server 2008 R2
   D. Windows Server 2012
   E. Windows Server 2016
   Правильные ответы: A

2. **Вопрос:** Обнаруживать несанкционированные изменения в конфигурационных файлах, папках, ветках реестра или важных файлах данных и оповещать о них позволяет функция RedCheck:
   Варианты ответов:
   A. Аудит уязвимостей
   B. Управление обновлениями
   C. Контроль целостности
   D. Аудит в режиме «Пентест»
   E. Инвентаризация сети
   Правильные ответы: C