НОЧУ ДПО УЦ «Сетевая Академия»

УТВЕРЖДАЮ
Директор НОЧУ ДПО УЦ «Сетевая Академия»
_____/Шикова Ю.В./

Образовательная программа
дополнительного профессионального образования
(повышения квалификации)
«Настройка безопасности в Windows Server 2016
(20744 Securing Windows Server 2016)»

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:

- IT-специалистов, которые администрируют доменную среду на базе Windows Server 2016, управляют доступом к Интернет и облачным службам, поддерживают решения на базе Windows Server;
- подготовки к сертификационному экзамену 70-744 «Securing Windows Server 2016» сертификации MCSE: Cloud Platform and Infrastructure.

Целью обучения является формирование у слушателей знаний сетевой инфраструктуры и навыков, необходимых для необходимым для настройки безопасности ИТ-инфраструктуры на базе Windows Server 2016.

Для изучения данной Программы рекомендуется обладать следующими знаниями и навыками:

- Два или более года опыта развертывания, администрирования и управления службами Windows Server 2012 или Windows Server 2008.
- Знания и навыки, эквивалентные обучению на курсах 20740 «Установка, организация хранилища и работа в Windows Server 2016», 20741 «Настройка сетевой инфраструктуры в Windows Server 2016» и 20742 «Администрирование служб проверки подлинности в Windows Server 2016».
- Практическое понимание сетевых основ, включая стек протоколов TCP/IP, протоколы UDP и DNS.
- Практическое понимание принципов работы доменных служб Active Directory (AD DS).
- Практическое понимание основ виртуализации Microsoft Hyper-V.
- Понимание принципов безопасности Windows Server.

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 обучения слушатель сможет:

- Настраивать безопасность Windows Server.
- Управлять безопасностью при разработке приложений для серверной инфраструктуры.
- Управлять базовыми планами безопасности.
- Настраивать и использовать функционал Just-In-Time (JIT) administration и Just Enough administration (JEA).
- Управлять безопасностью данных.
- Настраивать брандмауэр Windows и распределенный программный брандмауэр.
- Управлять безопасностью сетевого трафика.
- Защищать виртуальную инфраструктуру.
- Управлять обнаружением вредоносных программ и угроз.
- Настраивать расширенный аудит.
- Управлять обновлениями программного обеспечения.
- Управлять обнаружением угроз с помощью средства расширенного анализа угроз (Advanced Threat Analysis) и Microsoft Operations Management Suite (OMS).

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.	Обнаружение нарушений и использование инструментов Sysinternals	3	2	1	Опрос, практические занятия
2.	Защита учетных данных и привилегированный доступ.	2,5	1,5	1	Опрос, практические занятия
3.	Ограничение прав администратора с помощью функции JEA.	2	1	1	Опрос, практические занятия
4.	Управление привилегированным доступом и административные леса.	3,5	1,5	2	Опрос, практические занятия
5.	Противодействие вредоносным программам и угрозам.	3	1,5	1,5	Опрос, практические занятия
6.	Анализ активности с помощью расширенного аудита и журналов аналитики.	3	1,5	1,5	Опрос, практические занятия
7.	Анализ активности с помощью Microsoft Advanced Threat Analytics и Operations Management Suite.	2	1	1	Опрос, практические занятия
8.	Обеспечение безопасности виртуализации инфраструктуры.	3,5	1,5	2	Опрос, практические занятия
9.	Настройка безопасности при разработке приложений и рабочей инфраструктуры сервера.	3,5	1,5	2	Опрос, практические занятия
10.	Защита данных с помощью шифрования.	2	1	1	Опрос, практические занятия
11.	Ограничение доступа к файлам и папкам.	3	2	1	Опрос, практические занятия
12.	Использование брандмауэров для управления трафиком в сети.	3	1,5	1,5	Опрос, практические занятия

13.	Обеспечение сетевого трафика.	2	1	1	Опрос, практические занятия
14.	Обновление Windows Server	2	1	1	Опрос, практические занятия
15.	Итоговая аттестация	2	-	2	Тестирование
	Итого:	**40**	**19,5**	**20,5**	

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: 40 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: 5 дней.

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

Модуль 1: Обнаружение нарушений и использование инструментов Sysinternals.

- Обзор обнаружения нарушений.
- Использование инструментов Sysinternals для обнаружения нарушений.
- *Лабораторная работа: Основные обнаружения нарушений и стратегии реагирования на инциденты*.
    - Определение типов атак.
    - Использование стратегии реагирования на инциденты.
    - Изучение инструментов Sysinternals.

Модуль 2: Защита учетных данных и привилегированный доступ.

- Понятие прав пользователя.
- Учетные записи компьютера и служб.
- Защита учетных данных.
- Понятие рабочих станций и серверов привилегированного доступа (Jump servers).
- Развертывание решения для управления паролем локального администратора.
- *Лабораторная работа: Права пользователя, параметры безопасности и учетные записи служб, управляемых группами*.
    - Настройка параметров безопасности.
    - Настройка групп с ограниченным доступом.
    - Делегирование привилегий.
    - Создание и управление учетных записей служб, управляемых группами (group managed service accounts, MSA).
    - Настройка функций Credential Guard.
    - Обнаружение проблемных учетных записей.
- *Лабораторная работа: Настройка и развертывание решений управления паролем локального администратора (local administrator password - LAP).*
    - Установка решений управления паролем локального администратора (LAP).
    - Настройка решений LAP.
    - Развертывание решений LAP.

Модуль 3: Ограничение прав администратора с помощью функции Just Enough Administration (JEA).

- Понятие Just Enough Administration (JEA).
- Настройка и развёртывание JEA.
- *Лабораторная работа: Ограничение прав администратора с помощью функции JEA.*
    - Создание файла ролевых возможностей.
    - Создание файла конфигурации сеанса.
    - Создание точки соединения JEA.
    - Подключение к точке соединения JEA.
    - Развертывание JEA с помощью Desire State Configuration (DSC).

Модуль 4: Управление привилегированным доступом и административные леса.

- Понятие концепции леса с расширенной безопасностью административной среды (Enhanced Security Administrative Environment, ESAE).
- Обзор Microsoft Identity Manager (MIM).

- Реализация Just In Time (JIT) и управление привилегированным доступом с помощью MIM.
- *Лабораторная работа: Ограничение прав администратора с помощью управления привилегированным доступом.*
    - Использование многоуровневого подхода к безопасности.
    - Изучение MIM.
    - Настройка веб-портала MIM.
    - Настройка функции привилегированного доступа.
    - Запрос привилегированного доступа.

Модуль 5: Противодействие вредоносным программам и угрозам.
- Настройка и управление Windows Defender.
- Использование политик ограничения использования программного обеспечения (software restricting policies, SRP) и AppLocker.
- Настройка и использование Device Guard.
- Использование и развертывание Enhanced Mitigation Experience Toolkit (EMET).
- *Лабораторная работа: Защита приложений с помощью AppLocker, Windows Defender, правил Device Guard и EMET.*
    - Настройка Windows Defender.
    - Настройка AppLocker.
    - Настройка и развертывание Device Guard.
    - Развертывание и использование EMET.

Модуль 6: Анализ активности с помощью расширенного аудита и журналов аналитики.
- Обзор технологий аудита.
- Понятие расширенного аудита.
- Настройка аудита в Windows PowerShell и ведение журнала.
- *Лабораторная работа: Настройка шифрования и расширенный аудит.*
    - Настройка аудита доступа к файловой системе.
    - Аудит входа в систему домена.
    - Управление конфигурацией расширенных политик аудита.
    - Ведение журнала и аудит в Windows PowerShell.

Модуль 7: Анализ активности с помощью Microsoft Advanced Threat Analytics и Operations Management Suite.
- Обзор Advanced Threat Analytics.
- Понятие Operations Management Suite (OMS).
- *Лабораторная работа: Использование Advanced Threat Analytics and Operations Management Suite.*
    - Использование Microsoft Advanced Threat Analytics и OMS.
    - Подготовка и развертывание Microsoft Advanced Threat Analytics.
    - Подготовка и развертывание OMS.

Модуль 8: Обеспечение безопасности виртуализации инфраструктуры.
- Обзор защищённой фабрики виртуальных машин (Guarded Fabric virtual machines).
- Понятие экранирования и поддержка шифрования ВМ.

- *Лабораторная работа: Развертывание и использование защищенной фабрики с доверенной проверкой администратора и экранированием ВМ.*
    - Развертывание защищенной фабрики ВМ с доверенной проверкой администратора.
    - Развертывание экранированных ВМ.

Модуль 9: Настройка безопасности при разработке приложений и рабочей инфраструктуры сервера.
- Использование Security Compliance Manager.
- Знакомство с Nano Server.
- Понятие контейнеров.
- *Лабораторная работа: Использование Security Compliance Manager.*
    - Настройка базового уровня безопасности для Windows Server 2016.
    - Развертывание базовой уровня безопасности для Windows Server 2016.
- *Лабораторная работа: Развертывание и настройка Nano Server и контейнеров.*
    - Развертывание, управление и обеспечение безопасности Nano Server.
    - Развертывание, управление и обеспечение безопасности контейнеров Windows Server.
    - Развертывание, управление и обеспечение безопасности контейнеров Hyper-V.

Модуль 10: Защита данных с помощью шифрования.
- Планирование и реализация шифрования.
- Планирование и реализация BitLocker.
- *Лабораторная работа: Настройка Encrypting File System (EFS) и BitLocker.*
    - Шифрование и восстановление доступа к зашифрованным файлам.
    - Использование BitLocker для защиты данных.

Модуль 11: Ограничение доступа к файлам и папкам.
- Знакомство с Диспетчером ресурсов файлового сервера
- Реализация управления классификацией и задачи управления файлами.
- Понятие динамического контроля доступа (DAC).
- *Лабораторная работа: Настройка квот и блокировки файлов.*
    - Настройка квот FSRM.
    - Настройка блокировки файлов.
- *Лабораторная работа: Внедрение DAC.*
    - Подготовка DAC.
    - Реализация DAC.

Модуль 12: Использование брандмауэров для управления трафиком в сети.
- Обзор брандмауэра Windows.
- Распределенные программные брандмауэры.
- *Лабораторная работа: Брандмауэр Windows в режиме повышенной безопасности.*
    - Создание и тестирование правил входящих подключений.
    - Создание и тестирование правил исходящих подключений.

Модуль 13: Обеспечение сетевого трафика.
- Угрозы безопасности сети и правила безопасного подключения.
- Настройка дополнительных параметров DNS.

- Анализ сетевого трафика с помощью Microsoft Message Analyzer.
- Обеспечение безопасности трафика SMB и анализ трафика SMB
- *Лабораторная работа: Правила безопасного подключения и обеспечение безопасности DNS.*
    - Создание и тестирование правила безопасного подключения.
    - Настройка и тестирование DNSSEC.
- *Лабораторная работа: Шифрование SMB и использование Microsoft Message Analyzer.*
    - Использование Microsoft Message Analyzer.
    - Настройка и проверка шифрования SMB на общих папках.

Модуль 14: Обновление Windows Server.

- Обзор Windows Server Update Services (WSUS).
- Развертывание обновлений с помощью WSUS.
- *Лабораторная работа: Осуществление управления обновлениями.*
    - Установка роли сервера WSUS.
    - Настройка параметров обновления.
    - Одобрение и развертывание обновления с помощью WSUS.

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 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:** Какие из типов вредоносных программ имеют возможность самовоспроизведения?
   Варианты ответов:
   A. Вирус
   B. Троян
   C. Червь
   D. Фишинг
   E. Псевдо-обновления
   Правильные ответы: A, C

2. **Вопрос:** Администратор ввел команду «Enter-PSSession -ComputerName LON-DC1 -ConfigurationName DNSOps». Выберите истинное высказывание о ситуации:
   Варианты ответов:
   A. Будет сформировано соединение с JEA endpoint DNSOps на сервере LON-DC1 от имени текущего пользователя
   B. Попытка установить соединение с JEA endpoint не удастся из-за неуказанного имени пользователя
   C. Будет сформировано соединение с JEA endpoint DNSOps с сервера LON-DC1 от имени пользователя, имя которого будет указано на следующем шаге
   Правильные ответы: A

3. **Вопрос:** Выберите инструменты, с помощью которых можно управлять Bitlocker:
Варианты ответов:
   A. Group Policy
   B. Windows PowerShell
   C. Bitlocker Drive Encryption (Control Panel)
   D. Active Direcoty Administration Tools
   E. Bitlocker Managing and Administration
Правильные ответы: A, B, C