ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ "ЦЕНТР ОБУЧЕНИЯ "СПЕЦИАЛИСТ" УНЦ ПРИ МГТУ ИМ. Н.Э. БАУМАНА
(ОЧУ ДПО «СПЕЦИАЛИСТ»)
123242, город Москва, улица Зоологическая, дом 11, строение 2, этаж 2, помещение №I, комната №12,
ИНН 7701168244, ОГРН 1127799002990

Утверждаю:
Директор ОЧУ ДПО «Специалист»

_____/Е.В.Добрыднева/
«01» июня 2018 года

Дополнительная профессиональная программа повышения квалификации «50255E: Использование групповых политик для управления окружением Windows»

город Москва

Программа разработана в соответствии с приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. N 499 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам".

Повышение квалификации слушателей, осуществляемое в соответствии с программой, проводится с использованием модульного принципа построения учебного плана с применением различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения в соответствии с законодательством об образовании.

Дополнительная профессиональная программа повышения квалификации, разработана образовательной организацией в соответствии с законодательством Российской Федерации, включает все модули, указанные в учебном плане.

Содержание оценочных и методических материалов определяется образовательной организацией самостоятельно с учетом положений законодательства об образовании Российской Федерации.

Структура дополнительной профессиональной программы соответствует требованиям Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 1 июля 2013 г. N 499.

Объем дополнительной профессиональной программы вне зависимости от применяемых образовательных технологий, должен быть не менее 16 академических часов. Сроки ее освоения определяются образовательной организацией самостоятельно.

Формы обучения слушателей (очная, очно-заочная, заочная) определяются образовательной организацией самостоятельно.

К освоению дополнительных профессиональных программ допускаются:

- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

Для определения структуры дополнительной профессиональной программы и трудоемкости ее освоения может применяться система зачетных единиц. Количество зачетных единиц по дополнительной профессиональной программе устанавливается организацией.

Образовательная деятельность слушателей предусматривает следующие виды учебных занятий и учебных работ: лекции, практические и семинарские занятия, лабораторные работы, круглые столы, мастер-классы, мастерские, деловые игры, ролевые игры, тренинги, семинары по обмену опытом, выездные занятия, консультации, выполнение аттестационной, дипломной, проектной работы и другие виды учебных занятий и учебных работ, определенные учебным планом.

Аннотация.

Групповые политики – самый мощный и универсальный инструмент администратора Windows-сетей. Системный администратор, в совершенстве владеющий групповыми политиками, многократно повышает эффективность своей работы и снижает временные и ресурсные затраты на решение типовых административных задач. Окончив курс, слушатель научится использовать групповые политики для управления компьютерами, учетными записями и настройками Windows, а также проектировать инфраструктуру для применения групповых политик. Курс предназначен для ИТ-специалистов, имеющих опыт администрирование и поддержки клиентов и серверов Microsoft и желающих приобрести знания и навыки в вопросах управления OS Windows при помощи групповых политик.

1. Цель программы:

Цель курса – научить слушателей использовать групповые политики для управления компьютерами, учетными записями и настройками Windows, а также проектировать инфраструктуру для применения групповых политик.

1.1. Планируемый результат обучения:

Лица, успешно освоившие программу, должны овладеть следующими компетенциями:

1.2. Совершенствуемые компетенции

№	Компетенция	Направление подготовки ФГОС ВО ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 09.03.02 «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» (УРОВЕНЬ БАКАЛАВРИАТА)
		Код компетенции
1	способностью участвовать в работах по доводке и освоению информационных технологий в ходе внедрения и эксплуатации информационных систем	ПК-15
2	способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию	ПК-28
3	способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества	ПК-30
4	способностью обеспечивать безопасность и целостность данных информационных систем и технологий	ПК-31
5	способностью адаптировать приложения к изменяющимся условиям функционирования	ПК-32
6	способностью выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно-) для решения поставленной задачи	ПК-37

1.3. Совершенствуемые компетенции в соответствии с трудовыми фикциями профессионального стандарта «СИСТЕМНЫЙ АДМИНИСТРАТОР ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ», Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 5 октября 2015 г. N 684н

№	Компетенция Наименование вида ПД - Администрирование информационно-коммуникационных (инфокоммуникационных) систем B5 ОТФ:	Направление подготовки
		ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ «СИСТЕМНЫЙ АДМИНИСТРАТОР ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ»
		Трудовые функции (код)
1	Администрирование прикладного программного	B/01.5 Установка прикладного программного обеспечения

	обеспечения инфокоммуникацио нной системы организации	B/02.5 Оценка критичности возникновения инцидентов при работе прикладного программного обеспечения
		B/03.5 Оптимизация функционирования прикладного программного обеспечения
		B/04.5 Интеграция прикладного программного обеспечения в единую структуру инфокоммуникационной системы
		B/05.5 Реализация регламентов обеспечения информационной

1.4. Планируемые результаты обучения

После окончания обучения слушатель будет знать:

- групповые политики для управления компьютерами, учетными записями и настройками Windows;
- Как проектировать инфраструктуру для применения групповых политик.

После окончания обучения слушатель будет уметь:

- Использовать групповые политики для управления компьютерами, учётными записями и настройками Windows
- Проектировать инфраструктуру для применения групповых политик
- Использовать команды PowerShell для управления групповыми политиками
- Настройка безопасности при помощи групповых политик
- Реализация AppLocker
- Настройка предпочтений групповых политик
- Использование административных шаблонов

2. Категория слушателей

Этот курс предназначен для ИТ-специалистов, имеющих опыт администрирование и поддержки клиентов и серверов Microsoft и желающих приобрести знания и навыки в вопросах управления OS Windows при помощи групповых политик.

2.1. Требования к предварительной подготовке:

Требуемая подготовка:
Знание и практический опыт администрирования клиентов и серверов семейства Windows. Знакомство с Active Directory. Английский язык.

Связь с другими курсами: Курс 20413C: Проектирование и реализация серверной инфраструктуры

1.7. Срок обучения: 60 академических часов, в том числе 40 аудиторных, **СРС -** 20 час.
1.8. Форма обучения: очная. По желанию слушателя форма обучения может быть изменена и/или дополнена.
1.9. Режим занятий: дневной, вечерний, группы выходного дня.

2.2. Учебный план курса

№	Наименование модулей	Академические часы	Форма

п/п	по программе	Общая трудоемкость	В том числе			ПА [1]
			Аудиторные		СРС	
			Лекций	Практических занятий		
1	**Модуль 1:** Введение в управление конфигурациями (Configuration Management).	**5**	2	2	1	Лабораторная работа
2	**Модуль 2:** Использование инструментов управления Групповыми политиками	**4**	1	2	1	Лабораторная работа
3	**Модуль 3:** Проектирование инфраструктуры групповых политик	**4**	1	2	1	Лабораторная работа
4	**Модуль 4:** Механизм обработки групповых политик	**4**	1	2	1	Лабораторная работа
5	**Модуль 5:** Устранение проблем и резервное копирование	**4**	1	2	1	Лабораторная работа
6	**Модуль 6:** Управление безопасностью при помощи групповых политик	**4**	1	2	1	Лабораторная работа
7	**Модуль 7:** Реализация безопасности приложений при помощи групповых политик.	**5**	1	2	2	Лабораторная работа
8	**Модуль 8:** Настройка рабочего стола при помощи групповых политик	**5**	1	2	2	Лабораторная работа
9	**Модуль 9:** Реализация виртуализации состояния пользователя (User State Virtualization).	**5**	1	2	2	Лабораторная работа
10	**Модуль 10:** Установка ПО при помощи групповых политик.	**5**	1	2	2	Лабораторная работа
11	**Модуль 11:** Использование PowerShell с групповыми политиками	**5**	1	2	2	Лабораторная работа
12	**Модуль 12:** Использование PowerShell DSC (Desired State Configuration)	**5**	1	2	2	Лабораторная работа
13	**Модуль 13:** Настройка предпочтений групповых политик (Group Policy Preferences)	**5**	1	2	2	Лабораторная работа

[1] ПА – промежуточная аттестация

	ИТОГО:	**60**	**14**	**26**	**20**	
10	Итоговая аттестация	Тест				

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Количество аудиторных занятий при очно-заочной форме обучения составляет 20-25% от общего количества часов.

Практические занятия включают в себя, в частности, анализ ситуаций, выполнение практических заданий.

3. Календарный учебный график

Календарный учебный график формируется при осуществлении обучения в течение всего календарного года. По мере набора групп слушателей по программе составляется календарный график, учитывающий объемы лекций, практики, самоподготовки, выезды на объекты.

Неделя обучения	1	2	3	4	5	6	7	Итого часов
	пн	вт	ср	чт	пт	сб	вс	
1 неделя	0	4	0	4	0	0	0	8
СРС	0	2	0	2	0	0	0	4
2 неделя	0	4	0	4	0	0	0	8
СРС	0	2	0	2	0	0	0	4
3 неделя	0	4	0	4	0	0	0	8
СРС	0	2	0	2	0	0	0	4
4 неделя	0	4	0	4	0	0	0	8
СРС	0	2	0	2	0	0	0	4
5 неделя	0	4	0	4 ИА	0	0	0	8
СРС	0	2	0	2	0	0	0	4
Итого:	**0**	**12**	**0**	**12**	**0**	**0**	**0**	**40/20**
Примечание: ИА – Итоговая аттестация (тест)								

4. Рабочая программа

Модуль 1. Введение в управление конфигурациями (Configuration Management).

- Управление Конфигурациями при помощи групповых политик.
- Новое в групповых политиках
- Использование Windows PowerShell в процессе управления конфигурациями

Модуль 2. Использование инструментов управления Групповыми политиками

- Локальные и доменные политики
- Использование GPMC (Group Policy Management Console)
- Обновление групповых политик

Модуль 3. Проектирование инфраструктуры групповых политик

- Планирование групповых политик
- Разработка решения по внедрению групповых политик
- Внедрение групповых политик
- Управление групповыми политиками

Модуль 4. Механизм обработки групповых политик

- Компоненты Active Directory для групповых политик
- Порядок применения групповых политик
- Изменение порядка применения политик

Модуль 5. Устранение проблем и резервное копирование

- Диагностические инструменты
- RSoP
- Журналирование групповых политик
- Резервное копирование и восстановление политик
- Построение Таблицы миграций

Модуль 6. Управление безопасностью при помощи групповых политик

- Инструменты обеспечения безопасности
- Защита учётных записей
- Обзор политик безопастности
- Политики безопасности для серверов и клиентских компьютеров.

Модуль 7. Реализация безопасности приложений при помощи групповых политик.

- Управление настройками UAC.
- Задание политики ограничения запуска программ
- Использование механизма AppLocker

Модуль 8. Настройка рабочего стола при помощи групповых политик

- Типы сценариев и управление исполнением сценария
- Конфигурирование настроек рабочего стола, стартового меню и панели задач
- Задание настроек панели управления
- Настройка компонентов Windows
- Управление настройками печати
- Задание сетевых настроек

Модуль 9. Реализация виртуализации состояния пользователя (User State Virtualization).

- Настройка перенаправления папок
- Управление автономными файлами.
- OneDrive for Business

Модуль 10. Установка ПО при помощи групповых политик.

- Использование пакетов MSI для установки программ
- Развёртывание ПО при помощи политик
- Настройка точек распространения
- Использование SCCM

Модуль 11. Использование PowerShell с групповыми политиками

- Введение в Windows PowerShell
- Использование Windows PowerShell
- Написание сценариев PowerShell
- Библиотека PowerShell для работы с групповыми политиками
- Сценарии входа на PowerShell

Модуль 12. Использование PowerShell DSC (Desired State Configuration)

- Обзор DSC
- Примеры сценариев DSC
- Использование DSC

Модуль 13. Настройка предпочтений групповых политик (Group Policy Preferences)

- Введение в Group Policy Preferences
- Настройка Group Policy Preferences
- Применение Group Policy Preferences

5. Организационно-педагогические условия

Соблюдение требований к кадровым условиям реализации дополнительной профессиональной программы:

а) преподавательский состав образовательной организации, обеспечивающий образовательный процесс, обладает высшим образованием и стажем преподавания по изучаемой тематике не менее 1 года и (или) практической работы в областях знаний, предусмотренных модулями программы, не менее 3 (трех) лет;

б) образовательной организацией наряду с традиционными лекционно-семинарскими занятиями применяются современные эффективные методики преподавания с применением интерактивных форм обучения, аудиовизуальных средств, информационно-телекоммуникационных ресурсов и наглядных учебных пособий.

Соблюдение требований к материально-техническому и учебно-методическому обеспечению дополнительной профессиональной программы:

а) образовательная организация располагает необходимой материально-технической базой, включая современные аудитории, библиотеку, аудиовизуальные средства обучения, мультимедийную аппаратуру, оргтехнику, копировальные аппараты. Материальная база соответствует санитарным и техническим нормам и правилам и обеспечивает проведение всех видов практической и дисциплинарной подготовки слушателей, предусмотренных учебным планом реализуемой дополнительной профессиональной программы.

б) в случае применения электронного обучения, дистанционных образовательных технологий каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационно-образовательной среде, содержащей все электронные образовательные ресурсы, перечисленные в модулях дополнительной профессиональной программы.

6. Формы аттестации и оценочные материалы

Образовательная организация несет ответственность за качество подготовки слушателей и реализацию дополнительной профессиональной программы в полном объеме в соответствии с учебным планом.

Оценка качества освоения дополнительной профессиональной программы слушателей включает текущий контроль успеваемости, промежуточную и итоговую аттестацию.

Промежуточная аттестация по данному курсу проводится в форме выполнения практических работ и устного опроса, к итоговой аттестации допускаются слушатели, выполнившие все практические работы.

Результаты итоговой аттестации слушателей ДПП в соответствии с формой итоговой аттестации, установленной учебным планом, выставляются по двух бальной шкале («зачтено»/«не зачтено»), правильное выполнение не менее 80% заданий – «зачтено».

Слушателям, успешно освоившим дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

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

Итоговая аттестация проводится по форме выполнения задания в соответствии с учебным планом. Результаты итоговой аттестации заносятся в соответствующие документы.

7. <u>Промежуточная аттестация:</u>

№п/п	***Тематика практического занятия***	***Форма ПА***
Модуль 1.	Configuration Management	

Модуль 2.	Использование инструментов управления Групповыми политиками	Лабораторная работа:
Модуль 3.	Проектирование инфраструктуры групповых политик	Лабораторная работа:
Модуль 4.	Механизм обработки групповых политик	Лабораторная работа:
Модуль 5.	Устранение проблем и резервное копирование	Лабораторная работа:
Модуль 6.	Управление безопасностью при помощи групповых политик	Лабораторная работа:
Модуль 7.	Реализация безопасности приложений при помощи групповых политик.	Лабораторная работа:
Модуль 8.	Настройка рабочего стола при помощи групповых политик	Лабораторная работа:
Модуль 9.	Реализация виртуализации состояния пользователя (User State Virtualization).	Лабораторная работа:
Модуль 10.	Установка ПО при помощи групповых политик.	Лабораторная работа:
Модуль 11.	Использование PowerShell с групповыми политиками	Лабораторная работа:
Модуль 12.	Использование PowerShell DSC (Desired State Configuration)	Лабораторная работа:
Модуль 13.	Настройка предпочтений групповых политик (Group Policy Preferences)	Лабораторная работа:

8. Итоговая аттестация (выполнение задания):

Задание: «Создание объекта групповой политики»

Алгоритм выполнения задания:

1. Чтобы создать объект групповой политики и настроить режимы BranchCache
2. Для настройки брандмауэра Windows с повышенной безопасности трафика правила для входящих подключений
3. Для настройки брандмауэра Windows с повышенной безопасности трафика правила для исходящих подключений

В следующей процедуре будет предложено создать объект групповой политики в политике домена по умолчанию, однако можно создать объект в организационную единицу (OU) или другой контейнер, соответствующие вашему развертыванию.

Необходимо быть членом "Администраторы домена", или аналогичные им для выполнения этих процедур.
Чтобы создать объект групповой политики и настроить режимы BranchCache

1. На компьютере, на котором установлена роль сервера доменных служб Active Directory, в диспетчере серверов щелкните средства, а затем нажмите кнопку Управление групповой политикой. Откроется консоль управления групповыми политиками.
2. В консоли управления групповыми политиками разверните следующий путь: леса: *example.com*, домены, *example.com*, объектов групповой политики,

где *example.com* — это имя домена, где расположены учетные записи компьютеров BranchCache клиента, которые вы хотите настроить.

3. Щелкните правой кнопкой мыши объектов групповой политики, а затем нажмите кнопку New. Новый объект групповой Политики откроется диалоговое окно. В имя, введите имя для нового объекта (Групповой).Например, если вы хотите указать объект клиентских компьютеров BranchCache, введите клиентских компьютеров BranchCache. Нажмите кнопку ОК.
4. Убедитесь, что в консоли управления групповыми политиками объектов групповой политики установлен и в области сведений щелкните правой кнопкой мыши только что созданный объект групповой Политики. Например, если имя объекта групповой Политики BranchCache клиентские компьютеры, щелкните правой кнопкой мыши клиентских компьютеров BranchCache.Нажмите кнопку изменить. Откроется консоль управления групповыми политиками.
5. В консоли управления групповыми политиками разверните следующий путь: Конфигурация компьютера, политики, административные шаблоны: определения политик (файлы ADMX), полученные из локального компьютера, сети, BranchCache.
6. Нажмите кнопку BranchCache, а затем в области сведений дважды щелкнитевключить BranchCache. Откроется диалоговое окно параметра политики.
7. В включить BranchCache диалоговом нажмите кнопку включено, а затем нажмите кнопку ОК.
8. Чтобы включить BranchCache в режиме распределенного кэша, в области сведений дважды щелкните режим распределенного кэша BranchCache задать. Откроется диалоговое окно параметра политики.
9. В режим задать распределенного кэша BranchCache диалоговом нажмите кнопку включено, а затем нажмите кнопку ОК.
10. Если у вас есть один или несколько филиалов вы развертываете BranchCache в режиме размещенного кэша, куда вы развернули серверов размещенного кэша в этих офисах, дважды щелкните включить автоматическое размещенного кэша обнаружения с использованием точки подключения службы. Откроется диалоговое окно параметра политики.
11. В включить автоматическое размещенного кэша обнаружения с использованием точки подключения службы диалоговом нажмите кнопку включено, а затем нажмите кнопку ОК.

    При включении оба режим распределенного кэша BranchCache задать и включить автоматическое размещенного кэша обнаружения с использованием точки подключения службы параметры политики работают клиентские компьютеры в режиме распределенного кэша BranchCache, если только они поиск сервера размещенного кэша в филиале, после чего они работают в режиме размещенного кэша.

12. Используйте описанные ниже процедуры для настройки брандмауэра на клиентских компьютерах с помощью групповой политики.

Для настройки брандмауэра Windows с повышенной безопасности трафика правила для входящих подключений

1. В консоли управления групповыми политиками разверните следующий путь: леса: *example.com*, домены, *example.com*, объектов групповой политики, где *example.com* — это имя домена, где расположены учетные записи компьютеров BranchCache клиента, которые вы хотите настроить.
2. Убедитесь, что в консоли управления групповыми политиками объектов групповой политики установлен и в области сведений щелкните правой кнопкой мыши объект

групповой Политики, который вы создали ранее BranchCache клиентские компьютеры. Например, если имя объекта групповой Политики BranchCache клиентские компьютеры, щелкните правой кнопкой мыши клиентских компьютеров BranchCache. Нажмите кнопку изменить.Откроется консоль управления групповыми политиками.

3. В консоли управления групповыми политиками разверните следующий путь:Конфигурация компьютера, политики, параметры Windows, параметры безопасности, брандмауэр Windows в режиме повышенной безопасности,брандмауэр Windows в режиме повышенной безопасности — LDAP, правила для входящих подключений.
4. Щелкните правой кнопкой мыши правила для входящих подключений, а затем нажмите кнопку новое правило. Откроется мастер создания правила для нового входящего подключения.
5. В тип правила, нажмите кнопку предопределенное, разверните список вариантов выбора и нажмите кнопку BranchCache — получение содержимого (использует HTTP). Нажмите кнопку Далее.
6. В предопределенные правила, нажмите кнопку Далее.
7. В действие, убедитесь, что разрешить подключение установлен, а затем нажмите кнопку Готово.

   Необходимо выбрать разрешить подключение для на клиенте BranchCache иметь возможность получать трафик через этот порт.

8. Чтобы создать исключения брандмауэра WS-Discovery, снова щелкните правой кнопкой мыши правила для входящих подключений, а затем нажмите кнопку новое правило. Откроется мастер создания правила для нового входящего подключения.
9. В тип правила, нажмите кнопку предопределенное, разверните список вариантов выбора и нажмите кнопку BranchCache — обнаружение кэширующих узлов (использует WSD). Нажмите кнопку Далее.
10. В предопределенные правила, нажмите кнопку Далее.
11. В действие, убедитесь, что разрешить подключение установлен, а затем нажмите кнопку Готово.

    Необходимо выбрать разрешить подключение для на клиенте BranchCache иметь возможность получать трафик через этот порт.

Для настройки брандмауэра Windows с повышенной безопасности трафика правила для исходящих подключений

1. В консоли управления групповыми политиками щелкните правой кнопкой мыши правила для исходящих подключений, а затем нажмите кнопку новое правило. Откроется мастер создания правила исходящих подключений.
2. В тип правила, нажмите кнопку предопределенное, разверните список вариантов выбора и нажмите кнопку BranchCache — получение содержимого (использует HTTP). Нажмите кнопку Далее.
3. В предопределенные правила, нажмите кнопку Далее.
4. В действие, убедитесь, что разрешить подключение установлен, а затем нажмите кнопку Готово.

   Необходимо выбрать разрешить подключение для клиента BranchCache может отправлять трафик через этот порт.

5. Чтобы создать исключения брандмауэра WS-Discovery, снова щелкните правой кнопкой мыши правила для исходящих подключений, а затем нажмите кнопку новое правило. Откроется мастер создания правила исходящих подключений.

6. В тип правила, нажмите кнопку предопределенное, разверните список вариантов выбора и нажмите кнопку BranchCache — обнаружение кэширующих узлов (использует WSD). Нажмите кнопку Далее.
7. В предопределенные правила, нажмите кнопку Далее.
8. В действие, убедитесь, что разрешить подключение установлен, а затем нажмите кнопку Готово.

   Необходимо выбрать разрешить подключение для клиента BranchCache может отправлять трафик через этот порт.