ЧАСТНОЕ УЧРЕЖДЕНИЕ
ОРГАНИЗАЦИЯ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «УЧЕБНЫЙ ЦЕНТР «ЗВЕЗДЫ И С»

УТВЕРЖДАЮ
Директор
ЧУ ОДПО «Учебный центр «Звезды и С»
Стародубцев В.Н. _____
«19» мая 2021г.

Дополнительная профессиональная образовательная программа
повышения квалификации
М20744 «Настройка безопасности в Windows Server 2016»

Москва, 2021г.

1. Целевая установка

В этом курсе объясняется, как использовать аудит и функцию расширенного анализа угроз в Windows Server 2016 для выявления проблем безопасности. Вы также узнаете, как минимизировать угрозы со стороны вредоносных программ, защищать платформу виртуализации и использовать параметры развертывания, такие как Nano-сервер и контейнеры, для повышения безопасности. В курсе также объясняется, как вы можете помочь защитить доступ к файлам с помощью шифрования и динамического контроля доступа, и как вы можете повысить безопасность вашей сети.

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".

Совершенствуемые компетенции

Администрирование сетевой подсистемы инфокоммуникационной системы организации

№	Компетенция	Код компетенции
1	Настройка сетевых элементов инфокоммуникационной системы	D/01.6
2	Контроль использования ресурсов сетевых устройств и программного обеспечения	D/02.6
3	Управление безопасностью сетевых устройств и программного обеспечения	D/03.6
4	Диагностика отказов и ошибок сетевых устройств и программного обеспечения	D/04.6
5	Контроль производительности сетевой инфраструктуры инфокоммуникационной системы	D/05.6
6	Проведение регламентных работ на сетевых устройствах и программном обеспечении	D/06.6

	инфокоммуникационной системы	

Приобретенные навыки

- Защита Windows Server.
- Защита учетных данных и реализация рабочих станций с привилегированным доступом.
- Ограничение прав администратора с помощью Just Enough Administration.
- Управление привилегированным доступом.
- Минимизация вреда от вредоносных программ и угроз.
- Анализ активности с помощью расширенного аудита и анализа журналов регистрации.
- Развертывание и настройка Advanced Threat Analytics и Microsoft Operations Management Suite.
- Настройка виртуальных машин (VM) защищенной структуры.
- Использование Security Compliance Toolkit (SCT) и контейнеров для повышения безопасности.
- Планирование и защита данных.
- Оптимизация и защита файловых служб.
- Обеспечение безопасности сетевого трафика с помощью брандмауэров и шифрования.
- Обеспечение безопасности сетевого трафика с использованием DNSSEC и Message Analyzer.

3. Учебный план.

№ п/п	Наименование модулей по программе	В том числе аудиторных			Форма контроля
		Всего	*Лекций*	*Практических занятий*	

1	Атаки, определение брешей и инструменты Sysinternals.	**2**	1	1	Прак. занятие
2	Защита учетных данных и привилегированных доступов.	**3**	2	1	Прак. занятие
3	Ограничение прав администратора при помощи Just Enough Administration (JEA).	**2**	1	1	Прак. занятие
4	Управление привилегированными доступами (PAM) и административные леса.	**3**	2	1	Прак. занятие
5	Противостояние вредоносному программному обеспечению и предотвращение угроз.	**4**	2	2	Прак. занятие
6	Анализ активности при помощи расширенного аудита и анализа журналов.	**4**	2	2	Прак. занятие
7	Развертывание и настройка Microsoft Advanced Threat Analytics (ATA) и Microsoft Operations Management Suite (OMS).	**2**	1	1	Прак. занятие
8	Обеспечение безопасности инфраструктуры виртуализации.	**4**	2	2	Прак. занятие
9	Обеспечение безопасности разработки приложений и серверных нагрузок инфраструктуры.	**4**	2	2	Прак. занятие

10	Планирование и защита данных.	**2**	1	1	Прак. занятие
11	Оптимизация и обеспечение безопасности файловых служб.	**2**	1	1	Прак. занятие
12	Обеспечение безопасности сетевого трафика при помощи межсетевых экранов и шифрования.	**2**	1	1	Прак. занятие
13	Обеспечение безопасности сетевого трафика.	**2**	1	1	Прак. занятие
14	Обновление Windows Server.	**2**	1	1	Прак. занятие
15	**Итоговая аттестация:** (Лабораторная работа)	**2**	**-**	**2**	Прак. занятие
	Итого:	**40**	**20**	**20**	

4. Календарный учебный график

Календарный учебный график составляется в форме расписания занятий при наборе группы и прилагается к программе повышения квалификации.
Форма обучения: очная, очная с применением дистанционных технологий.
Трудоемкость программы: 40 часа.
Сроки освоения программы: 5 дней.
Режим занятий: дневной, вечерний.

5. Рабочие программы дисциплин

Модуль 1: Атаки, определение брешей и инструменты Sysinternals.

- Описание атак.
- Определение брешей.
- Проверка активности при помощи инструментов Sysinternals.
- **Лабораторная работа: Определение основных брешей и стратегии реакции на инциденты**
    - Определение типа атаки.

- Исследование инструментов Sysinternals.

Модуль 2: Защита учетных данных и привилегированных доступов.

- Описание пользовательских прав.
- Учетные записи компьютеров и служб.
- Защита учетных данных.
- Рабочие станции с привилегированным доступом и серверы доступа в выделенной зоне (Jump Servers).
- Решение для паролей локального администратора (LAPs).
- **Лабораторная работа: Применение пользовательских прав, опций безопасности и групповых управляемых учетных записей (MSA).**
  - Настройка опций безопасности.
  - Настройка ограниченных групп.
  - Делегирование привилегий.
  - Создание и управление групповыми управляемыми учетными записями (MSA).
  - Настройка компонента Credential Guard.
  - Обнаружение проблемных учетных записей.
- **Лабораторная работа: Настройка и развертывание LAPs.**
  - Установка и настройка LAPs.
  - Развертывание и тестирование LAPs.

Модуль 3: Ограничение прав администратора при помощи Just Enough Administration (JEA).

- Описание JEA.
- Проверка и развертывание JEA.
- **Лабораторная работа: Ограничение административных привилегий при помощи JEA.**
  - Создание файла возможностей роли.
  - Создание файла конфигурации сессии.
  - Создание конечной точки JEA.
  - Подключение и тестирование конечной точки JEA.

- Развертывание конфигурации JEA на сторонний компьютер.

Модуль 4: Управление привилегированными доступами (PAM) и административные леса.

- Леса Enhanced Security Administrative Environment (ESAE).
- Обзор Microsoft Identity Manager (MIM).
- Обзор администрирования JIT и PAM.
- **Лабораторная работа: Ограничение привилегий администратора при помощи PAM**
  - Многоуровневый подход к безопасности.
  - Настройка доверительных отношений.
  - Запрос привилегированного доступа.
  - Управление ролями PAM.

Модуль 5: Противостояние вредоносному программному обеспечению и предотвращение угроз.

- Настройка и управление Windows Defender.
- Ограничение программного обеспечения.
- Настройка и использование компонента Device Guard.
- Развертывание и использование Enhanced Mitigation Experience Toolkit (EMET).
- **Лабораторная работа: Обеспечение безопасности при помощи 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 при помощи расширенного аудита и анализа журналов.

- Обзор аудита.
- Расширенный аудит.
- Ведение журнала и аудит Windows PowerShell.

- **Лабораторная работа: Настройка расширенного аудита**
    - Настройка аудита доступа к файловой системе.
    - Аудит входов в домен.
    - Управление параметрами политики расширенного аудита.
    - Аудит и ведение журнала Windows PowerShell.

Модуль 7: Развертывание и настройка Microsoft Advanced Threat Analytics (ATA) и Microsoft Operations Management Suite (OMS).

- Развертывание и настройка Advanced Threat Analytics (ATA).
- Развертывание и настройка Operations Management Suite (OMS).
- **Лабораторная работа: Развертывание Advanced Threat Analytics (ATA) и Operations Management Suite (OMS).**
    - Подготовка и развертывание ATA.
    - Подготовка и развертывание OMS.

Модуль 8: Обеспечение безопасности инфраструктуры виртуализации.

- Защищенная фабрика (Guarded Fabric).
- Экранирование виртуальные машины и виртуальные машины с поддержкой шифрования.
- **Лабораторная работа: Защищенная фабрика (Guarded Fabric) с проверкой доверия администратору и экранированными виртуальными машинами.**
    - Развертывание защищенной фабрики (Guarded Fabric) с проверкой доверия администратору.
    - Развертывание экранированных виртуальных машин.

Модуль 9: Обеспечение безопасности разработки приложений и серверных нагрузок инфраструктуры.

- Использование Security Compliance Manager (SCM).
- Введение в Nano Server.
- Описание контейнеров
- **Лабораторная работа: Использование Security Compliance Manager (SCM)**

    - Настройка набора параметров безопасности (Security Baseline) для Windows Server 2016.
    - Развертывание набора параметров безопасности (Security Baseline) для Windows Server 2016.
- **Лабораторная работа: Развертывание и настройка Nano Server.**
    - Развертывание, управление и обеспечение безопасности Nano Server.
    - Развертывание, управление и обеспечение безопасности контейнеров

Модуль 10: Планирование и защита данных.

- Планирование и внедрение шифрования.
- Планирование и внедрение BitLocker.
- **Лабораторная работа: Защита данных при помощи шифрования и BitLocker**
    - Шифрование и восстановление доступа к зашифрованным файлам.
    - Использование BitLocker для защиты данных.

Модуль 11: Оптимизация и обеспечение безопасности файловых служб.

- Диспетчер ресурсов файлового сервера (FSRM).
- Применение управления классификацией и задач управления файлами.
- Динамическое управление доступом (DAC).
- **Лабораторная работа: Настройка квот и проверки файлов (File Screening).**
    - Настройка квот FSRM.
    - Настройка проверки файлов и отчетов хранилища.
- **Лабораторная работа: Применение динамического управления доступом (DAC).**
    - Подготовка к внедрению динамического управления доступом (DAC).
    - Внедрение динамического управления доступом (DAC).
    - Проверка и приведение в соответствие динамического управления доступом (DAC).

Модуль 12: Обеспечение безопасности сетевого трафика при помощи межсетевых экранов и шифрования.

- Описание сетевых угроз безопасности.
- Описание Windows Firewall with Advanced Security (WFAS).
- Настройка IPSec.
- Datacenter Firewall.
- **Лабораторная работа: Настройка Windows Firewall with Advanced Security (WFAS).**
    - Создание и проверка входящих правил.
    - Создание и проверка исходящих правил.
    - Создание и проверка правил безопасности подключений.

Модуль 13: Обеспечение безопасности сетевого трафика.

- Угрозы безопасности сети и правила безопасности подключений.
- Настройка расширенных параметров DNS.
- Проверка сетевого трафика при помощи Microsoft Message Analyzer.
- Обеспечение безопасности трафика SMB и анализ трафика SMB.
- **Лабораторная работа: Обеспечение безопасности DNS.**
    - Настройка и проверка DNSSEC.
    - Настройка политик DNS и RRL.
- **Лабораторная работа: Microsoft Message Analyzer и шифрование SMB.**
    - Использование Microsoft Message Analyzer.
    - Настройка и проверка шифрования SMB на общих ресурсах SMB.

Модуль 14: Обновление Windows Server.

- Обзор WSUS.
- Развертывание обновлений при помощи WSUS.
- **Лабораторная работа: Внедрение управления обновлениями.**
    - Применение серверной роли WSUS.
    - Настройка параметров обновления.

Подтверждение и развертывание обновлений при помощи WSUS.

6. Организационно-педагогические условия реализации программы

6.1. Материально-технические условия реализации программы

Исполнитель 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 3,1 ГГц;
- оперативная память - 32 Гб;
- SSD + 2 HDD в RAID0 не менее 500Гб;
- два монитора (24' + 22' FullHD);
- комплект клавиатура и мышь.

6.2. Учебно-методическое обеспечение программы

Каждый Слушатель обеспечивается авторизованным учебным пособием на английском языке.

7. Требования к профессорско-преподавательскому составу

Высшее профессиональное образование и стаж работы в образовательном учреждение не менее 1 года. Статус Microsoft Certified Trainer.

8. Форма 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.

Аттестация считается пройденной в случае успешного завершения лабораторной работы, а именно:
выполнения поставленной задачи: «Развертывание и настройка Operations Management Suite (OMS).».

Время выполнения итоговой аттестации – 2 ак. часа.

9. Оценочные материалы к итоговой аттестации

Итоговая аттестация проводится в форме выполнения задания. Результаты итоговой аттестации слушателей выставляются по двух бальной шкале («зачтено\не зачтено»). Итоговая аттестация считается пройденной («зачтено»), если слушатель выполнил все лабораторные работы и итоговое задание.

Пример решения задач (Официальное учебное пособие Microsoft, язык – английский):

Quotas and file screening

Scenario

Adatum Corporation is a medical research company with approximately 5,000 employees worldwide that

has specific needs for ensuring that medical data and records remain private. The company has a

headquarters location and multiple worldwide sites. Adatum has recently deployed a Windows Server

2016 server and Windows 10 client infrastructure.

Each network client within the Adatum domain is provided with a server-based home folder that is used

for storing personal documents or files that are works in progress. It has come to your attention that

home folders are becoming very large, and might contain file types such as MP3 files that are not

approved under corporate policy. You decide to implement FSRM quotas and file screening to help

address this issue.

Objectives

After completing this lab, you will be able to:

• Configure FSRM quotas.

• Configure file screening and generate a storage report.

Lab Setup

Estimated Time: 30 minutes

Virtual machines: **20744C-LON-DC1**, **20744C-LON-SVR1**

User name: **Adatum\Administrator**

Password: **Pa55w.rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must

complete the following steps:

1. On the host computer, start **Hyper-V Manager**.

2. In Hyper-V Manager, click **20744C-LON-DC1**, and, in the **Actions** pane, click **Start**.

3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.

4. Sign in using the following credentials:

5. User name: **Adatum\Administrator**

o Password: **Pa55w.rd**

o Perform steps 2 through 4 for **20744C-LON-SVR1**.

Exercise 1: Configuring File Server Resource Manager quotas

Scenario

To control the size of home folders, you are implementing FSRM quotas. Each home folder is limited to

100 MB. To ensure that users are not surprised by their home folders running out of space, a notification

is emailed to them when they exceed 85 percent of their quota. An event is also written to the event log

so that administrators can track it.

The main tasks for this exercise are as follows:

1. Create a quota template.

2. Configure a quota based on the quota template.

3. Test that the quota is functional.

- Task 1: Create a quota template

1. If not already signed in, sign in **LON-SVR1**, from Server Manager, install the **File Server Resource**

Manager.

2. In the **File Server Resource Manager** console, use the **Quota Templates** node to configure a

template that sets a hard limit of **100 MB** as the maximum folder size.

3. Configure the template to record an event in the Event Log when the folder reaches 85 percent

capacity and 100 percent capacity.

- Task 2: Configure a quota based on the quota template

1. Use the **File Server Resource Manager** console and the **Quotas** node to create a quota on the

D:\Labfiles\Mod11\Data folder by using the quota template that you created in Task 1.

2. Configure the quota to auto apply on existing and new subfolders.

3. Create an additional folder named **Max** in the **D:\Labfiles\Mod11\Data** folder, and ensure that the

new folder is listed in the quotas list in **File Server Resource Manager**.

- Task 3: Test that the quota is functional

1. Open a **Windows PowerShell** window, and use the following commands to create a file in the

D:\Labfiles\Mod11\Data\Max folder. Press Enter after each of the three commands:

D:

cd \Labfiles\Mod11\data\Max

fsutil file createnew file1.txt 89400000

2. Check the Event Viewer for an **Event ID** of **12325**.

3. Test that the quota works by attempting to create a file that is **16,400,000 bytes**, and then press

Enter:

fsutil file createnew file2.txt 16400000

Note: Notice that the file cannot be created. The message returned from Windows

references disk space, but the file creation fails because it would exceed the quota limit.

4. Close the Windows PowerShell window.

5. Close all open windows on LON-SVR1.