

Рабочая программа дисциплины (модуля) принята:
Ученым советом математического факультета

Протокол заседания № 11 от «27» 07 2020 г.

Председатель Ученого совета
математического факультета _____  Е.А. Сбродова

Секретарь Ученого совета
математического факультета _____  С.А. Никитина

Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой
компьютерной безопасности и прикладной алгебры

Протокол заседания № 13 от «27» июля 2020 г.

Заведующий кафедрой _____  А.Н. Ручай

Автор (составитель):
Зав.кафедрой, канд.физ.-мат. наук, доцент _____  А.Н. Ручай

Структура рабочей программы соответствует приказу ректора
ФГБОУ ВО «ЧелГУ» от «05» декабря 2018 г. № 678-1

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре ОПОП
3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)
4. Объем дисциплины (модуля)
5. Структура и содержание дисциплины (модуля)
6. Фонд оценочных средств
 - 6.1. Перечень видов оценочных средств
 - 6.2. Типовые контрольные задания и иные материалы для текущей аттестации
 - 6.3. Типовые контрольные вопросы и задания для промежуточной аттестации
 - 6.4. Критерии оценивания
7. Учебно-методическое и информационное обеспечение дисциплины (модуля)
 - 7.1. Рекомендуемая литература
 - 7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"
 - 7.3. Перечень информационных технологий
8. Материально-техническое обеспечение дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Специальные условия освоения дисциплины обучающимися с инвалидностью и ограниченными возможностями здоровья

Рабочая программа дисциплины "Администрирование Windows" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»	стр. 4
1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
Целями изучения дисциплины являются:	
- ознакомление студентов с принципами построения и архитектурой современных сетевых операционных систем, принципами администрирования корпоративных сетевых информационных систем, с принципами обеспечения реализации типичных бизнес-процессов, характерных для большинства современных предприятий;	
- освоение студентами основ администрирования корпоративных сетевых операционных систем.	
Задачами изучения дисциплины являются:	
- формирование и развитие компетенций, знаний, практических навыков и умений по вопросам архитектуры современных сетевых операционных систем, настройки конкретной операционной системы для выполнения бизнес-задач, особенностей обеспечения безотказного режима работы системы 24/7.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Цикл (раздел) ОПОП:	Б1.Б.1.44
2.1 Требования к предварительной подготовке обучающегося:	
Освоение дисциплины опирается на знания по курсам	
Операционные системы	
Сети и системы передачи информации	
Компьютерные сети	
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Данная дисциплина является предшествующей для дисциплины «Защита в операционных системах».	
Защита в операционных системах	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-7: способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	
Знать:	
<ul style="list-style-type: none"> – понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации; – правовые акты в области защиты государственной тайны и информационной безопасности; – правовые основы организации защиты государственной тайны и конфиденциальной информации; – основные понятия компьютерной безопасности; – основные требования к системам криптографической защиты; – основные алгоритмы криптографической защиты; – основные алгоритмы передачи данных; – проблемы и направления развития операционных систем. 	
Уметь:	
<ul style="list-style-type: none"> – использовать программные и аппаратные средства персонального компьютера; – ориентироваться в современной системе источников информации; – использовать защищенные современные информационные технологии в своей профессиональной деятельности; – применять средства антивирусной защиты; – анализировать информационную безопасность многопользовательских систем; – пользоваться программными средствами, реализующими основные криптографические функции – системы публичных ключей, цифровую подпись, разделение доступа; – видеть и формулировать проблему защиты информации; видеть конкретную ситуацию; прогнозировать и предвидеть; – ставить цели и задачи по обеспечению информационной безопасности. 	
Владеть:	
<ul style="list-style-type: none"> – навыками самостоятельной исследовательской работы; – навыками обеспечения безопасной работы на компьютере; – навыками организации эффективной защиты от вирусов; – навыками обеспечения защиты информации от внешних угроз; – навыками использования инструментов криптографической защиты информации; – навыками использования современной терминологии в области компьютерной безопасности; – навыками применения методологии защиты в области информационной безопасности. 	

Рабочая программа дисциплины "Администрирование Windows" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»	стр. 5
---	--------

ПК-5: способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
Знать: основные понятия защищенных операционных систем, баз данных и компьютерных сетей; понятие защиты информации, системы защиты; аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; средства аутентификации электронных данных и средства управления ключевой информацией; основные виды угроз безопасности информации и их классификацию; требования к криптографическим системам защиты информации; понятиями компьютерной безопасности в рамках администрирования и защиты публичных служб Windows.
Уметь: разрабатывать программно-аппаратных средств защиты информации, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; конфигурировать программно-аппаратных средств защиты информации, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.
Владеть: основами конфигурирования и разработки программно-аппаратных средств защиты информации, системы управления базами данных; компьютерных сетей, системы антивирусной защиты; средствами криптографической защиты информации в рамках администрирования и защиты публичных служб Windows.

В результате освоения дисциплины обучающийся должен

3.1 Знать:
3.1.1 – понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации;
3.1.2 - основные понятия защищенных операционных систем, баз данных и компьютерных сетей;
3.1.3 - понятиями компьютерной безопасности в рамках администрирования и защиты публичных служб Windows.
3.2 Уметь:
3.2.1 – пользоваться программными средствами, реализующими основные криптографические функции;
3.2.2 - разрабатывать программно-аппаратных средств защиты информации.
3.3 Владеть:
3.3.1 – навыками обеспечения безопасной работы на компьютере;
3.3.2 - средствами криптографической защиты информации в рамках администрирования и защиты публичных служб Windows.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)	
Общая трудоемкость	2 ЗЕТ
Часов по учебному плану : 72 в том числе : аудиторные занятия : 54 самостоятельная работа : 18 :	Виды контроля в семестрах: зачеты 7

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)				
Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. 1. Сетевые операционные системы. Установка и базовые настройки системы			
1.1	Модель OSI, модель TCP/IP. Базовые задачи, выполняемые сетевым администратором. Принципы работы сетевых операционных систем. Модель OSI, модель TCP/IP. Установка сетевой операционной системы на примере Microsoft Windows Server 2008 r2. Настройка базовой конфигурации. Протокол TCP/IP. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

Рабочая программа дисциплины "Администрирование Windows" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»				стр. 6
1.2	Настройка виртуальной машины с WindowsServer 2008. Выполнение базовой настройки виртуальной машины и настройка сети виртуальных машин. Знакомство с утилитами мониторинга работоспособности сети. /Лаб/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
Раздел 2. 2. Служба каталогов. Протокол LDAP				
2.1	Служба DNS. Протокол LDAP. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.2	Служба каталогов ActiveDirectory. Понятие домен, лес. Установка первого контроллера домена в лесу, создание резервного контроллера. Репликация между доменами. Хозяева операций. Управление пользователями, группами пользователей, компьютерами в домене. Групповые политики. Службы файлов и печати /Лек/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.3	Технология Raid. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.4	Установка и настройка службы DNS. Знакомство с работой службы DNS. Установка и базовая конфигурация службы. Проверка работоспособности полученной службы /Лаб/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.5	Служба каталогов Active Directory. Установка первого контроллера домена в лесу, создание резервного контроллера. Репликация между доменами. Хозяева операций. Управление пользователями, группами пользователей, компьютерами в домене. Групповые политики. /Лаб/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.6	Службы файлов и печати. Установка и настройка службы печати. /Лаб/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.7	Технология Raid. Изучение возможностей программной реализации RAID. /Лаб/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
Раздел 3. 3. Сетевые протоколы и службы				
3.1	Служба DHCP. Служба WINS и протокол NetBios. Протокол PPP. Служба маршрутизации и удаленного доступа (RRAS). Протокол DHCP. Установка и настройка DHCP-сервера. NetBios пространство имен. Установка и настройка WINS сервера: служба WINS, клиенты WINS, репликация. Протокол PPP. Служба маршрутизации и удаленного доступа (RRAS). Виртуальная частная сеть (VPN) средствами операционной системы. Маршрутизация, служба «Маршрутизация и удаленный доступ». RADIUS-сервер и RADIUS -клиенты. Сетевые политики. Удаленное подключение. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.2	Установка и настройка WINS сервера: служба WINS, клиенты WINS, репликация. Изучение технологии DHCP. Настройка базовых параметров DHCP. /Лаб/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.3	Служба маршрутизации и удаленного доступа (RRAS). Виртуальная частная сеть (VPN) средствами операционной системы. Маршрутизация, служба «Маршрутизация и удаленный доступ». RADIUS-сервер и RADIUS -клиенты. Сетевые политики. Удаленное подключение. Настройка службы маршрутизации. Настройка различных способов удаленного подключения к серверам по защищенному каналу (VPN доступ). /Лаб/	7	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
Раздел 4. 4. Управление сервером и мониторинг				
4.1	Резервное копирование и восстановление серверов. Основные принципы построения отказоустойчивых серверов. Встроенные средства резервного копирования WindowsServer. Консоли управления сервером. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.2	Удаленное управление сервером. Протокол RDP. Службы удаленного рабочего стола (RDS). Удаленный помощник. Мониторинг операционных систем. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

Рабочая программа дисциплины "Администрирование Windows" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»				стр. 7
4.3	Служба резервного копирования WindowsServer. Установка и настройка автоматического резервного копирования. /Лаб/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.4	Консоли управления сервером. Мониторинг работоспособности серверов. Знакомство с консолями управления и мониторинга работоспособности сервера. /Лаб/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.5	Протокол RDP. Служба RDS. Настройка работы с сервером по протоколу RDP и службы удаленного рабочего стола (RDS). /Лаб/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
Раздел 5. 5. Установка и настройка прикладных сервисов и служб				
5.1	Основные прикладные сервисы и службы. Сервер баз данных MicrosoftSQLServer. Веб-сервер IIS. FTP-сервер на базе IIS. Корпоративный портал на базе IIS и SharePoint. Протокол SNMP и установка SNMP-сервера. Сервер сертификации. Настройка надежной конфигурации для сервера сертификации. Протокол SMTP. Настройка SMTP-сервера. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.2	Настройка MSSQL. /Ср/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.3	Настройка IIS. Настройка FTP-сервера на IIS. /Ср/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.4	Настройка SNMP /Ср/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.5	Настройка SMTP /Ср/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.6	Настройка сервера сертификации /Ср/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.7	Конфигурация служб каталогов ActiveDirectory /Ср/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Лабораторная работа.
Вопросы для зачета.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Лабораторная работа № 1 - Парольная защита в Windows
В виртуальной машине установить клиентскую операционную систему Windows.
С использованием локальных политик безопасности установить ограничения:
- минимальная длина пароля пользователя Windows – 14 символов;
- требование сложности пароля;
- блокировка учетной записи пользователя на 30 минут после пяти неудачных попыток авторизации.
Создать учетную запись пользователя Windows с паролем, удовлетворяющим установленным требованиям.
Сбросить пароль пользователя Windows с использованием предоставленного специализированного программного обеспечения.
Установить предоставленное средство защиты от несанкционированного доступа.
Сбросить пароль пользователя Windows на виртуальной машине с установленным средством защиты от несанкционированного доступа.
Настроить средство защиты от несанкционированного доступа для блокировки попыток сброса пароля специализированным ПО.
*Дистрибутивы, лицензии и специализированное программное обеспечение предоставляются преподавателем.

Лабораторная работа № 2 - Аудит в операционных системах Windows
Настроить журналирование событий Windows – создать систему разграничения доступа (минимум два пользователя Windows с разным уровнем полномочий: полный доступ и доступ только для чтения) и настроить аудит

использования привилегий для каталога на локальном диске и вложенных в него файлов, обеспечивающий регистрацию сведений:

- метод доступа к контролируемым файлам и каталогу;
- результат (успех, отказ) попытки использования привилегий;
- учетная запись пользователя, использующего привилегии;
- время события;
- регистрация сведений об удалённых файлах.

Воссоздать структуру сети, сценарии использования компьютеров в локальной сети по результатам анализа предоставленных журналов безопасности, содержащую следующую информацию:

- сетевые имена компьютеров, входящих в локальную сеть;
- учётные записи пользователей и их соответствие сетевым именам компьютеров, на которых эти учетные записи используются;
- режим эксплуатации (время, дни недели) компьютеров;
- наличие сетевого программного обеспечения;
- определение наличия и типа контроллера домена Windows;
- используемые сетевые протоколы;
- используемое прикладное программное обеспечение;
- приблизительная схема локальной сети.

*специально подготовленные журналы, содержащие исходные события, предоставляются преподавателем

Лабораторная работа № 3 - Microsoft Active Directory

На двух виртуальных машинах установить соответственно серверную (Windows 2008 Server или более новая) и клиентскую (Windows 7 или более новая) операционные системы.

Клонировать виртуальную машину с серверной операционной системой, изменив идентификатор (SID) операционной системы и сетевое имя.

Между созданными виртуальными машинами настроить виртуальную сеть, соответствующую требованиям:

- все виртуальные машины находятся в одном virtual lan;
- все виртуальные машины имеют различные сетевые имена и ip-адреса;
- все виртуальные машины доступны друг другу по широковещательным рассылкам (находятся в одной подсети);
- основным шлюзом и сервером имён является виртуальная машина с исходной (по отношению к клонированной виртуальной машине с серверной операционной системой).

Серверной операционной системе добавить роль контроллера домена Active Directory.

Сконфигурировать контроллер домена с настройками по умолчанию, ввести клиентскую операционную систему в состав контроллера домена (показатель успешности настройки – на клиентской машине появляется возможность авторизоваться с доменной учетной записью).

На клонированной виртуальной машине с серверной операционной системой настроить роль резервного контроллера домена (показатель успешности настройки – изменение структуры Active Directory на основном контроллере домена (добавление пользователей, компьютеров и т.д.) влечёт изменение структуры Active Directory на резервном контроллере домена).

Лабораторная работа № 4 - Microsoft Active Directory. Коллектор журналов

На двух виртуальных машинах установить соответственно серверную (Windows 2008 Server или более новая) и клиентскую (Windows 7 или более новая) операционные системы.

Настроить журналирование событий Windows – создать систему разграничения доступа (минимум два пользователя Windows с разным уровнем полномочий: полный доступ и доступ только для чтения) и настроить аудит использования привилегий для каталога на локальном диске и вложенных в него файлов, обеспечивающий регистрацию сведений:

- метод доступа к контролируемым файлам и каталогу;
- результат (успех, отказ) попытки использования привилегий;
- учетная запись пользователя, использующего привилегии;
- время события;
- регистрация сведений об удалённых файлах.

Между созданными виртуальными машинами настроить виртуальную сеть, соответствующую требованиям:

- все виртуальные машины находятся в одном virtual lan;
- все виртуальные машины имеют различные сетевые имена и ip-адреса;
- все виртуальные машины доступны друг другу по широковещательным рассылкам (находятся в одной подсети);
- основным шлюзом и сервером имён является виртуальная машина с серверной операционной системой.

Серверной операционной системе добавить роль контроллера домена Active Directory.

Сконфигурировать контроллер домена с настройками по-умолчанию, ввести клиентскую операционную систему в состав контроллера домена (показатель успешности настройки – на клиентской машине появляется возможность авторизоваться с доменной учетной записью).

Настроить коллектор (сборщик) журналов безопасности в серверной операционной системе для сбора событий из

<p>Рабочая программа дисциплины "Администрирование Windows" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»</p>	<p>стр. 9</p>								
<p>журнала безопасности клиентской операционной системы (показатель успешности выполнения задания - события по результатам аудита (в клиентской операционной системе, в журнале безопасности) доступа к каталогу, на основе созданной системы разграничения доступа, появляются в серверной операционной системе, в журнале коллектора (сборщика) журналов).</p> <p>Лабораторная работа № 5 - Positive Technologies MP SIEM. Активация, основные функции, сбор событий Подключиться к удалённому стенду с установленным Positive Technologies MP SIEM. Активировать предоставленную лицензию, в соответствии с предоставленной документацией на Positive Technologies MP SIEM. Создать задачу по сбору журналов из коллектора (сборщика) журналов Windows. Создать задачу по сбору событий из базы данных Kaspersky Security Center. Создать задачу по сбору событий по стандарту syslog.</p> <p>Лабораторная работа № 6 - Positive Technologies MP SIEM. Анализ защищенности Подключиться к удалённому стенду с установленным Positive Technologies MP SIEM. Провести поиск доступных хостов в сети. Выполнить задачу по сканированию доступных хостов на наличие уязвимостей в режиме PenTest (показатель успешности – обнаруженные уязвимости в результатах сканирования доступных хостов). Проанализировать выявленные уязвимости рассмотреть, описать и принять меры по их устранению стандартными средствами Windows (закрытие портов, установка обновлений и т.д.).</p> <p>Лабораторная работа № 7 - Positive Technologies MP SIEM. Обработка событий Подключиться к удалённому стенду с установленным Positive Technologies MP SIEM. Написать произвольное правило нормализации. Написать произвольное правило агрегации. Написать произвольное правило обогащения. Написать произвольное правило корреляции. Написать произвольное правило локализации.</p>									
<p>6.3. Типовые контрольные вопросы и задания для промежуточной аттестации</p>									
<p>Вопросы к зачёту</p> <ol style="list-style-type: none"> 1. Модель OSI 2. Модель TCP/IP 3. Архитектура DNS 4. Протокол LDAP 5. MS Windows Server. Роли 6. MS Active Directory. Архитектура 7. MS Active Directory. Средства управления 8. Коллектор журналов событий Windows Server 9. Построение VPN сети средствами MS Windows Server 10. Настройка сервера удалённых рабочих столов RDP 11. Парольная защита Windows (локальная) 12. Система аудита Windows 13. RAID 14. UEFI/Legacy режимы загрузки Windows 15. SIEM-системы. Принципы построения и назначение 16. SIEM-системы. Формирование инцидентов и управление ими 17. SIEM-системы. Обработка событий 18. SIEM-системы. Настройка сбора событий 									
<p>6.4. Критерии оценивания</p>									
<p>Порядок проведения промежуточной аттестации</p> <p>На зачёте студент получает билет. В билете два теоретических вопроса. Написание ответа дается 1 час. После этого происходит оценка ответа. Преподаватель может задавать вопросы по тексту ответа. Студент должен на них ответить. Максимальный балл за ответ на теоретический вопрос - 10. Максимальный балл за лабораторную работу - 10. Посещаемость и активная работа на занятиях - 10 баллов.</p> <p>Сводная таблица рейтинга успеваемости</p> <table border="0" style="width: 100%;"> <tr> <td>Наименование оценочного средства</td> <td>Максимальное кол-во баллов</td> </tr> <tr> <td>Билеты для зачета</td> <td>2x10=20</td> </tr> <tr> <td>Лабораторная работа</td> <td>7x10=70</td> </tr> <tr> <td>Посещаемость и активная работа на занятиях</td> <td>10</td> </tr> </table>		Наименование оценочного средства	Максимальное кол-во баллов	Билеты для зачета	2x10=20	Лабораторная работа	7x10=70	Посещаемость и активная работа на занятиях	10
Наименование оценочного средства	Максимальное кол-во баллов								
Билеты для зачета	2x10=20								
Лабораторная работа	7x10=70								
Посещаемость и активная работа на занятиях	10								

Рабочая программа дисциплины "Администрирование Windows" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»	стр. 10
Итого	100
<p>Критерии оценивания теоретического вопроса и лабораторной работы</p> <p>Отлично/зачтено/9-10 баллов - Обучающийся отлично знает материал, понимает терминологию на языке программирования PERL или Python . Обучающийся практически не допускает ошибок.</p> <p>Хорошо/зачтено/7-8 баллов - Обучающийся хорошо знает материал, понимает терминологию на языке программирования PERL или Python. Обучающийся допускает незначительные ошибки.</p> <p>Удовлетворительно/зачтено/5-6 баллов - Обучающийся знаком с материалом, владеет терминологией объектно-ориентированного программирования. Обучающийся допускает фактические ошибки.</p> <p>Неудовлетворительно/незачтено/0-4 балла - Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.</p>	

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)				
7.1. Рекомендуемая литература				
7.1.1. Основная литература				
	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Власов Ю. В., Рицкова Т. И.	Администрирование сетей на платформе MS Windows Server: учебное пособие (http://biblioclub.ru/index.php?page=book&id=233291)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) Бином. Лаборатория знаний, 2008	ЭБС
Л1.2	Айвенс К.	Администрирование Microsoft Windows Server 2003: практическое пособие (http://biblioclub.ru/index.php?page=book&id=233685)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2008	ЭБС
Л1.3	Элсенпитер Р., Велт Тоби Дж.	Администрирование сетей Microsoft Windows XP Professional (http://biblioclub.ru/index.php?page=book&id=428821)	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
7.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Айвенс К.	Внедрение, управление и поддержка сетевой инфраструктуры MS Windows Server 2003: практическое пособие (http://biblioclub.ru/index.php?page=book&id=233686)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2008	ЭБС
Л2.2	Таненбаум Э., Леонтьев А.	Современные операционные системы	СПб.: Питер, 2005	
Л2.3	Хоружников С. Э., Прыгун В. В.	Администрирование сетей Windows: учебное пособие (http://e.lanbook.com/books/element.php?p11_id=40727)	Санкт-Петербург : НИУ ИТМО, 2012	ЭБС
7.3 Перечень информационных технологий				
7.3.1 Программное обеспечение				
Adobe Reader				
Notepad++				
VirtualBox				
MS Office365				

Рабочая программа дисциплины "Администрирование Windows" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»	стр. 11
7.3.2 Профессиональные базы данных и информационно-справочные системы	
1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.	
2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.	
3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp .	
4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php .	
5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.	
6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/	

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.
Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; рабочими станциями с установленным ПО (п. 7.3.1.).
Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.
Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)
<p>При изучении данной дисциплины используются лекционные, лабораторные занятия и самостоятельная работа студента. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.</p> <p>На лабораторных занятиях рассматриваются установка и настройка служб и базовых параметров. Рекомендуется перед каждым лабораторным занятием выполнить домашнее задание, что позволит лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на лабораторных и лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни.</p> <p>В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, видеохостинг YouTube, форумы, электронная почта и др.).</p> <p>Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.</p> <p>Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.</p> <p>При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.</p> <p>Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с</p>

применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.

1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «EIBraile-W14J G2»; ноутбуки с программой экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.

2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-PCM» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.

3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.

При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации NVDA, речевые синтезаторы, экранные лупы).

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.

Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).

Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:

Рабочая программа дисциплины "Администрирование Windows" по направлению подготовки (специальности) "Компьютерная безопасность" направленности (профилю) специализация N 1 "Анализ безопасности компьютерных систем": ФГБОУ ВО «ЧелГУ»	стр. 13
<p>а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);</p> <p>б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);</p> <p>в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).</p> <p>При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.</p> <p>Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.</p>	