МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

07.12.2020 г.

протокол № 9

Зав. кафедрой Назаров Д.М.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

20 января 2021 г.

протокол № 6

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Управление антивирусной защитой
Направление подготовки	10.03.01 Информационная безопасность
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2021

Разработана:
Доцент, к.т.н.
Стаин Д.А.

Екатеринбург
2021 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г.
ПС	

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины является формирование у студентов теоретических и практических знаний в области информационной безопасности, принципам обеспечения информационной безопасности государства, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности предприятия.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к вариативной части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточный контроль	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Практические занятия, включая курсовое проектирование		
Семестр 5						
Экзамен	216	56	28	28	124	6

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Профессиональные компетенции (ПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
эксплуатационный	

ПК-1 Администрирование подсистем защиты информации в операционных системах	ИД-1.ПК-1 Знать: Архитектура и принципы построения операционных систем Программные интерфейсы операционных систем Виды политик управления доступом и информационными потоками применительно к операционным системам Архитектура подсистем защиты информации в операционных системах Принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы Состав типовых конфигураций программно-аппаратных средств защиты информации Требования по составу и характеристикам подсистем защиты информации применительно к операционным системам Порядок реализации методов и средств антивирусной защиты в операционных системах Программно-аппаратные средства и методы защиты информации в операционных системах Принципы работы и правила эксплуатации программно-аппаратных средств защиты информации Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации
	ИД-2.ПК-1 Уметь: Формулировать политики безопасности операционных систем Настраивать политики безопасности операционных систем Оценивать угрозы безопасности информации операционных систем Противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах Настраивать антивирусные средства защиты информации в операционных системах Устанавливать обновления программного обеспечения и средств антивирусной защиты Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

ПК-1 Администрирование подсистем защиты информации в операционных системах	ИД-3.ПК-1 Иметь практический опыт: Определение состава применяемых программно-аппаратных средств защиты информации в операционных системах Разработка порядка применения программно-аппаратных средств защиты информации в операционных системах Формирование шаблонов установки программно-аппаратных средств защиты информации в операционных системах Установка программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации Конфигурирование программно-аппаратных средств защиты информации в операционных системах Контроль корректности функционирования программно-аппаратных средств защиты информации в операционных системах Управление антивирусной защитой операционных систем в соответствии с действующими требованиями
ПК-2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	ИД-1.ПК-2 Знать: Принципы построения компьютерных сетей Стек сетевых протоколов операционных систем Стек протоколов сетевого оборудования Порядок реализации методов и средств межсетевого экранирования Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы Виды политик управления доступом и информационными потоками в компьютерных сетях Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению Состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации Принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации Программно-аппаратные средства и методы защиты информации в компьютерных сетях Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации

ПК-2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	ИД-2.ПК-2 Уметь: Оценивать угрозы безопасности информации в компьютерных сетях Настраивать правила фильтрации пакетов в компьютерных сетях Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях
	ИД-3.ПК-2 Иметь практический опыт: Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях Разработка порядка применения программно-аппаратных средств защиты информации в компьютерных сетях Формирование шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях Настройка программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации Управление функционированием программно-аппаратных средств защиты информации в компьютерных сетях Контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях Управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-1.ПК-3 Знать: Архитектура подсистем защиты информации в операционных системах Принципы построения систем управления базами данных Основные средства и методы анализа программных реализаций Принципы построения антивирусного программного обеспечения Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению Уязвимости используемого программного обеспечения и методы их эксплуатации Виды и формы функционирования вредоносного программного обеспечения Характерные признаки наличия вредоносного программного обеспечения Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения Принципы функционирования программных средств криптографической защиты информации Порядок обеспечения безопасности информации при эксплуатации программного обеспечения Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации
	ИД-2.ПК-3 Уметь: Анализировать угрозы безопасности информации программного обеспечения Формулировать правила безопасной эксплуатации программного обеспечения Обосновывать правила безопасной эксплуатации программного обеспечения Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-3.ПК-3 Иметь практический опыт: Определение порядка установки программного обеспечения с целью соблюдения требований по защите информации Контроль над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение Формулирование требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения Выполнение работ по обнаружению вредоносного программного обеспечения Ликвидация обнаруженного вредоносного программного обеспечения и последствий его функционирования Формулирование требований к встроенным средствам защиты информации программного обеспечения

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 5		180					
Тема 1.	Общие сведения о компьютерных вирусах	38	3			35	
Тема 2.	Загрузочные вирусы	4	3		1		
Тема 3.	Файловые вирусы в Windows	4	3		1		
Тема 4.	Макровирусы	4	3		1		
Тема 5.	Сетевые и почтовые вирусы и черви	28	4		24		
Тема 6.	Распространение вирусов	54	4			50	
Тема 7.	Обнаружение вирусов	5	4		1		
Тема 8.	Структура антивирусного решения	28	4			24	
Тема 9.	Применение типового антивирусного решения	15				15	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Тема 1. Общие сведения о компьютерных вирусах	Тест	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 2. Загрузочные вирусы	Тест	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 3. Файловые вирусы в Windows	Тест	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5

Тема 4. Макровирусы	Тест	Состоит из 9 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 5. Сетевые и почтовые вирусы и черви	Тест	Состоит из 10 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 6. Распространение вирусов	Тест	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 7. Обнаружение вирусов	Тест	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 8. Структура антивирусного решения	Тест	Состоит из 10 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 9. Применение типового антивирусного решения	Тест	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Промежуточный контроль (Приложение 5)			
5 семестр (Эк)	Экзаменационные билеты (приложение 5)	В билете 2 теоретических вопроса и 1 практический	100 баллов

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущей и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущая аттестация. Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущей аттестации, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Общие сведения о компьютерных вирусах Введение в компьютерную вирусологию. Основные понятия о компьютерных вирусах.

Тема 2. Загрузочные вирусы Общая информация о загрузочных компьютерных вирусов. Загрузка с винчестера. Загрузочные вирусы в Windows. Методы борьбы с загрузочными вирусами
Тема 3. Файловые вирусы в Windows Системная организация Windows. Специфика вирусов для Windows. Полиморфные вирусы.
Тема 4. Макровирусы Вирусы в MS Word и MS Excel. Общие сведения о макросах. Полиморфные макровирусы.
Тема 5. Сетевые и почтовые вирусы и черви Архитектуру современных сетей. Типовая структура и поведение программы-червя. Механизм заражения ЭВМ программой-червем.
Тема 6. Распространение вирусов Методы обнаружения программ деструктивного воздействия
Тема 7. Обнаружение вирусов Методы защиты от программ деструктивного воздействия
Тема 8. Структура антивирусного решения Архитектура современного антивирусного пакета

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Загрузочные вирусы Изучение принципа работы загрузочного вируса
Тема 3. Файловые вирусы в Windows Анализ и нейтрализация конкретного вирусы
Тема 4. Макровирусы Анализ и удаление конкретного макровируса
Тема 5. Сетевые и почтовые вирусы и черви Обнаружение, исследование и удаление программы-червя
Тема 7. Обнаружение вирусов Обнаружение вирусной активности, лечение зараженного компьютера, ликвидация вредоносного кода

7.3. Содержание самостоятельной работы

Тема 1. Общие сведения о компьютерных вирусах Изучение принципов работы компьютерных вирусов
Тема 6. Распространение вирусов Изучение принципов инфекции файлов
Тема 8. Структура антивирусного решения Выбор антивирусного комплекса методом функциональной полноты
Тема 9. Применение типового антивирусного решения Установка и использование антивирусного программного пакета

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
не предусмотрено

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
не предусмотрено

7.6 Методические рекомендации по выполнению курсовой работы
Материалы не предусмотрены

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

1. Трофимов В. В., Ильина О. П., Трофимова Е. В., Кияев В. И., Приходченко А. П. Информационные системы и технологии в экономике и управлении. [Электронный ресурс]:учебник для академического бакалавриата : для студентов вузов, обучающихся по экономическим направлениям и специальностям. - Москва: Юрайт, 2018. - 542 – Режим доступа: https://urait.ru/bcode/412460

2. Гагарина Л.Г., Петров А. А. Современные проблемы информатики и вычислительной техники. [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2011. - 368 с. – Режим доступа: https://znanium.com/catalog/product/203313

3. Коноплева И.А., Богданов И. А. Управление безопасностью и безопасность бизнеса. [Электронный ресурс]:Учебное пособие для вузов. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2012. - 448 с. – Режим доступа: https://znanium.com/catalog/product/352467

4. Маркова В.Д. Цифровая экономика. [Электронный ресурс]:Учебник. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2018. - 186 с. – Режим доступа: https://znanium.com/catalog/product/959818

5. Клименко И.С. Информационная безопасность и защита информации: модели и методы управления. [Электронный ресурс]:Монография. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2020. - 180 с. – Режим доступа: https://znanium.com/catalog/product/1018665

Дополнительная литература:

1. Каратунова Н. Г. Защита информации. Курс лекций. [Электронный ресурс]:учебно-методическое пособие. - Краснодар: Кубанский социально-экономический институт, 2014. - 188 – Режим доступа: https://znanium.com/catalog/product/503511

2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2017. - 416 с. – Режим доступа: https://znanium.com/catalog/product/775200

3. Баранова Е.К., Бабаш А.В. Основы информационной безопасности. [Электронный ресурс]:учебник. - Москва: РИОР: ИНФРА-М, 2019. - 202 – Режим доступа: https://znanium.com/catalog/product/1014830

4. Полякова Т. А., Чубукова С. Г., Ниесов В. А. Организационное и правовое обеспечение информационной безопасности. [Электронный ресурс]:Учебник и практикум для вузов. - Москва: Юрайт, 2020. - 325 – Режим доступа: https://urait.ru/bcode/450371

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии 30.09.2023.

МойОфис стандартный. Соглашение № СК-281 от 7 июня 2017. Дата заключения - 07.06.2017. Срок действия лицензии - без ограничения срока.

ОС "Альт Образование" 8. Договор № ДС-010-2018 от 12.04.2018, Акт к договору от 07.05.2018. Срок действия лицензии - без ограничения срока.

Microsoft Visual Studio Community. Лицензия для образовательных учреждений. Срок действия лицензии - без ограничения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Консультант +. Договор № 163/223-У/2020 от 14.12.2020. Срок действия лицензии до 31.12.2021

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.