Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

СЕВЕРО-ЗАПАДНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ-филиал РАНХИГС
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

УТВЕРЖДЕНО
Директор Северо-Западного
института управления – филиала
РАНХиГС
Хлутков А.Д.

ПРОГРАММА СПЕЦИАЛИТЕТА

Гражданско-правовая
(*специализация)*

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,
реализуемой без применения электронного (онлайн) курса

Б1.В.02.05 «Правовое обеспечение информационной безопасности»

40.05.01. Правовое обеспечение национальной безопасности
по специальности

очная, заочная
формы обучения

Год набора - 2024 г.

Санкт-Петербург, 2024

Автор–составитель:
к.э.н., доцент С.Е. Елкин

Руководитель образовательной программы
Смирнов С.Н.

РП одобрена на заседании кафедры Протокол от 24.04.2024 № 4

СОДЕРЖАНИЕ

1.Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Дисциплина Б1.В.02.05. «Правовое обеспечение информационной безопасности» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
ПКр ОС-1	Способность обеспечивать безопасность личности, общества, государства правовыми средствами	ПКр ОС-1.2	ПКр ОС-1.2. Способность обеспечивать безопасность личности, общества, государства правовыми средствами

1.1. **В результате освоения дисциплины у студентов должны быть сформированы**

ОТФ/ТФ/трудовые /профессиональные действия	Код компонента освоения компетенции	Результаты обучения
Деятельность по обеспечению безопасности в составе подразделения (службы).	ПКр ОС 1.2.	на уровне знаний: основных понятий, категорий функционирования систем хозяйствующих субъектов;
		на уровне умений: оценка рисков объекта анализ и оценка информации,
		на уровне навыков: идентификации и оценки рисков объекта.
Текущий контроль выполнения требований национальной безопасности в организации. Организация и координация работ по соблюдению требований национальной безопасности в организации.	ПКр ОС 1.2.	на уровне знаний: - специфики применения принципов функционирования систем безопасности хозяйствующих субъектов.
		на уровне умений: выявление причинно-следственных связей, делать выводы.
		на уровне навыков: - оценкой схемы построения (эффективности) контрольных процедур объекта (бизнес-процесса, проекта, программы, подразделения).
Разработка и внедрение организационных, технологических и технических мероприятий по обеспечению национальной безопасности в организации.	ПКр ОС 1.2.	на уровне знаний: основных понятий, категорий функционирования систем хозяйствующих субъектов; специфики применения принципов функционирования систем безопасности хозяйствующих субъектов;
		на уровне умений: оценки рисков объекта; анализа и оценка информации; выявления причинно-следственных связей и формулирования выводов;
		на уровне навыков: идентификации и оценки рисков объекта
Управление системой национальной безопасности в организации; руководство комплексом работ по обеспечению защиты основных ресурсов.	ПКр ОС 1.2.	на уровне знаний: способов выявления экономических и налоговых преступлений в базовых отраслях экономики; методов выявления экономических и налоговых преступлений в базовых отраслях экономики;
		на уровне умений: использовать знания о экономических и налоговых преступлениях в базовых отраслях экономики; выявлять экономические и налоговые преступления в базовых отраслях экономики;
		на уровне навыков: оценки схемы построения (эффективности) контрольных процедур объекта (бизнес-процесса, проекта, программы, подразделения)

2.Объем и место дисциплины в структуре образовательной программы

Объем дисциплины

Общая трудоемкость дисциплины (очная/заочная) составляет 3 зачетные единицы или

108 академических часов. Дисциплина реализуется с применением дистанционных образовательных технологий (*далее – ДОТ)*

Очная форма обучения

Вид работы	**Трудоемкость** (в акад. часах/астрон. часах)
Общая трудоемкость	108/81
Контактная работа с преподавателем	48/36
Лекции	24/18
Практические занятия	24/18
Самостоятельная работа	60/45
Контроль	
Формы текущего контроля	устный опрос, тестирование
Форма промежуточной аттестации	Зачет

Заочная форма обучения

Вид работы	**Трудоемкость** (в акад. часах/астрон. часах)
Общая трудоемкость	108/81
Контактная работа с преподавателем	12/9
Лекции	4/3
Практические занятия	8/6
Самостоятельная работа	92/69
Контроль	4/3
Формы текущего контроля	устный опрос, тестирование
Форма промежуточной аттестации	Зачет

Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.02.05. «Правовое обеспечение информационной безопасности» включена в состав дисциплин по выбору учебного плана подготовки специалистов по специальности 45.05.01 «Правовое обеспечение национальной безопасности».

Дисциплина относится к блоку 1 (Б1), (Б1.В).

Дисциплина для очной формы обучения изучается на 4 курсе в 7 семестре.

Дисциплина для заочной формы обучения изучается на 4 курсе в 7 семестре.

Форма промежуточной аттестации в соответствии с учебным планом: зачет.

Доступ к системе дистанционных образовательных технологий осуществляется каждым обучающимся самостоятельно с любого устройства на портале: https://lms.ranepa.ru/. Пароль и логин к личному кабинету / профилю предоставляется студенту в деканате.

3Содержание и структура дисциплины
структура дисциплины

Очная форма обучения

№ п/п	**Наименование тем и/или разделов**	**Объем дисциплины (модуля), час.**					**Форма текущего контроля успеваемости, промежуточной аттестации**
		Всего	**Контактная работа обучающихся с преподавателем по видам учебных занятий**			**СР**	
			Л/ЭО ДОТ	**ЛР/ЭО ДОТ**	**ПЗ/ЭО ДОТ**	**КСР/ЭО ДОТ**	
Тема 1	Информационная безопасность (ИБ) РФ и задачи по ее обеспечению	9	2		2		5	*О*

Тема 2	Нормативно-правовая база обеспечения ИБ в России	9	2		2		5	*О*
Тема 3	Информация как объект правового регулирования и защиты	9	2		2		5	*О, Т*
Тема 4	Система субъектов обеспечения ИБ в России и их правовой статус	9	2		2		5	*О, Т*
Тема 5	Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика	9	2		2		5	*О*
Тема 6	Правовая защита личности в информационной сфере	9	2		2		5	*О*
Тема 7	Правовой режим государственной тайны и меры по ее обеспечению	9	2		2		5	*О*
Тема 8	Правовые и организационные способы защиты информации в сфере высоких технологий	9	2		2		5	*О*
Тема 9	Правовое обеспечение права интеллектуальной собственности (ПИС)	9	2		2		5	*О*
Тема 10	Правовая защита коммерческой тайны (КТ)	9	2		2		5	*О*
Тема 11	Правовое регулирование отношений в сфере лицензирования и сертификации	6	2		2		2	*О*
Тема 12	Предупреждение преступлений в информационной сфере в современной России	6	-		2		4	*О*
Тема 13	Юридическая ответственность за правонарушения в сфере ИБ	6	2		-		4	*О*
	Промежуточная аттестация	-						**Зачет**
	Всего:	**108**	**24**	**-**	**24**	**-**	**60**	

О – опрос; Т – тестирование

Заочная форма обучения

№ п/п	**Наименование тем и/или разделов**	**Объем дисциплины (модуля), час.**						**Форма текущего контроля успеваемости, промежуточной аттестации**
		Всего	**Контактная работа обучающихся с преподавателем по видам учебных занятий**				**СР**	
			Л/ЭО ДОТ	**ЛР/ЭО ДОТ**	**ПЗ/ЭО ДОТ**	**КСР/ЭО ДОТ**		
Тема 1	Информационная безопасность (ИБ) РФ и задачи по ее обеспечению	10	1		1		8	*О*
Тема 2	Нормативно-правовая база обеспечения ИБ в России	10	1		1		8	*О*
Тема 3	Информация как объект правового регулирования и защиты	10	1		1		8	*О, Т*
Тема 4	Система субъектов обеспечения ИБ в России и их правовой статус	10	1		1		8	*О, Т*

Тема 5	Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика	9			1		8	*О*
Тема 6	Правовая защита личности в информационной сфере	9			1		8	*О*
Тема 7	Правовой режим государственной тайны и меры по ее обеспечению	9			1		8	*О*
Тема 8	Правовые и организационные способы защиты информации в сфере высоких технологий	9			1		8	*О*
Тема 9	Правовое обеспечение права интеллектуальной собственности (ПИС)	8					8	*О*
Тема 10	Правовая защита коммерческой тайны (КТ)	8					8	*О*
Тема 11	Правовое регулирование отношений в сфере лицензирования и сертификации	6					6	*О*
Тема 12	Предупреждение преступлений в информационной сфере в современной России	6					6	*О*
Тема 13	Юридическая ответственность за правонарушения в сфере ИБ	6					6	*О*
	Промежуточная аттестация	**4**						**Зачет**
	Всего:	**108**	**4**	**-**	**8**	**-**	**92**	

О – опрос; Т – тестирование

Содержание учебной дисциплины

Тема 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.

Понятие ИБ и информационного общества. Цели, задачи и принципы обеспечения ИБ. Угроза национальной безопасности и их виды. Информационные войны и информационное оружие. Информационный терроризм. Информационное общество в РФ и его характеристики. Информационная сфера и ее области. Национальные интересы России в информационной сфере. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.

Тема 2. Нормативно-правовая база обеспечения ИБ в России.

Понятие правового обеспечения и правовой защиты. История формирования законодательства РФ об информации и ее защите. Система нормативно-правовых актов России, регулирующих отношения в сфере ИБ. Международно-правовые нормы и стандарты в сфере ИБ. Место Окинавской Хартии глобального информационного общества в системе международно-правовых актов обеспечения ИБ. Предмет и метод правового регулирования в сфере ИБ страны. Информационное право. Информационные отношения. Виды ведомственных и корпоративных норм и их место в системе правового регулирования ИБ в РФ. Правовое регулирование деятельности средств массовой информации. Основные тенденции развития законодательства РФ в сфере ИБ. Особенности стандартизации нормативной базы в сфере ИБ в современном мире.

Тема 3. Информация как объект правового регулирования и защиты.

Информация, ее виды и признаки. Информация как объект юридической защиты. Информационная сфера общества и ее характеристики. Информационные ресурсы. Понятие и виды. Виды и источники информации, подлежащие защите. Правовой режим защиты государ-

ственной тайны. Способы обеспечения сохранности информации, составляющей государственную тайну и система контроля за состоянием ее защиты. Основные принципы засекречивания информации. Конфиденциальная информация и возможные каналы ее утечки. Информационная инфраструктура и информационная среда. Их структура и характеристики. Международный опыт деятельности по правовому обеспечению ИБ и основные направления его развития. Государственная политика РФ в сфере правового обеспечения ИБ.

Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус.

Понятие государственного управления в сфере обеспечения ИБ. Система органов государственной власти, обеспечивающая ИБ и особенности их компетентности. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами. Служба Специальной связи и информации Федеральной службы охраны РФ, ее задачи и правовой статус.

Тема 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.

Понятие и виды преступности в информационной сфере. Основные этапы и тенденции развития компьютерной преступности в России. Особенности детерминации преступлений, совершаемых в информационной сфере. Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет. Понятие преступления в сфере компьютерной информации. Виды преступлений в сфере компьютерной информации. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Особенности объективных признаков компьютерных преступлений. Основные способы их совершения. Субъективные признаки компьютерных преступлений. Характерные мотивы и цели их совершения. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.

Тема 6. Правовая защита личности в информационной сфере.

Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере. Конституционные гарантии правовой охраны прав личности в информационной сфере. Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни. Правовой механизм защиты права на неприкосновенность частной жизни. Врачебная тайна как институт защиты интересов личности. Защита права на личную информацию с ограниченным доступом. Персональная тайна и ее виды. Обработка и правовая охрана персональных данных. Правовая база обеспечения защиты личности от воздействия «вредной» информации. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.

Тема 7. Правовой режим государственной тайны и меры по ее обеспечению.

Понятие государственной тайны и правового режима ее обеспечения. Принципы и механизм отнесения сведений к государственной тайне (ГТ). Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну. Субъекты обеспечения режима государственной тайны и их правовой статус. Организационно-правовые меры защиты ГТ. Допуск и доступ к ГТ. Обеспечение ИБ при международном обмене информацией. Система контроля за режимом обеспечения ГТ. Особенности юридической ответственности за нарушение режима обеспечения ГТ.

Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий.

Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям. Организационно-управленческие меры обеспечения

защиты информации в сфере высоких технологий. Компьютерные преступления и особенности их идентификации и предупреждения. Правовые основы применения «электронной цифровой подписи» (ЭЦП). Криптографическая защита информации (КЗИ). Правовые и организационные способы обеспечения КЗИ в России и других странах современного мира. Контроль за разработкой, производством и применением криптографических средств. КЗИ и их правовая основа. Органы лицензирования и сертификации и их правовой статус.

Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС).

Понятие интеллектуальной собственности и ее правовой статус. Законодательство РФ об авторских и смежных правах. Особенности правоотношений, обеспечивающих ПИС. Объекты и субъекты ПИС. Правовой механизм обеспечения защиты авторских и смежных прав. Государственная регистрация ПИС. Особенности правовой защиты программ для электронных вычислительных машин и баз данных. Патентное право и патентные правоотношения. Правовой статус участников. Сфера действия патентного законодательства. Показатели и условия патентоспособности. Правовой статус автора и патентообладателя. Механизм правовой защиты прав автора и патентообладателей. Товарный знак и механизм его правовой защиты. Государственная регистрация товарного знака. Прекращение права на товарный знак. Программы для ЭВМ и механизм их правовой защиты. Правовое регулирование договорных отношений в сфере ПИС.

Тема 10. Правовая защита коммерческой тайны (КТ).

Понятие КТ и ее правовой статус. Признаки КТ. Защита КТ и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель. Объекты защиты КТ. Особенности правового обеспечения режима КТ. Промышленный шпионаж и его объекты. Критерии определения секретности при определении режима КТ. Организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений. Режим представления информации, составляющей КТ органам государственной власти. Юридическая ответственность за нарушения режима обеспечения КТ.

Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации.

Правовое обеспечение деятельности организаций по лицензированию и сертификации в сфере ИБ. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию в сфере ИБ. Система государственного лицензирования в сфере ИБ и ее функции. Субъекты лицензирования в сфере ИБ и их правовой статус. Порядок лицензирования, приостановления или аннулирования действия лицензии. Специальная экспертиза предприятия и государственная аттестация их руководителей. Контроль за условиями обеспечения ИБ лицензиатами. Понятие сертификации средств защиты информации (ССЗИ) и ее правовая основа в РФ. Цели создания системы ССЗИ. Организационная структура системы ССЗИ и особенности правового статуса ее субъектов. Объекты сертификационной деятельности и режимы сертификации. Особенности аттестации и контроля за деятельностью объектов обработки особо важной информации. Юридическая ответственность за нарушением правил лицензирования и сертификации.

Тема 12. Предупреждение преступлений в информационной сфере в современной России.

Информационная безопасность России и задачи по ее обеспечению. Система детерминант преступности в информационной сфере. Уровневый подход. Мотивационная сфера лиц, совершающих правонарушения в сфере ИБ. Субъекты деятельности по обеспечению противодействия правонарушениям в сфере ИБ и их правовой статус. Оперативно-розыскные и крими-

налистические мероприятия по борьбе с преступлениями в сфере ИБ. Особенности расследования преступлений в сфере ИБ. Совершенствование правовых норм как средство обеспечения профилактического воздействия на отношения в сфере ИБ. Зарубежный опыт борьбы с преступностью в сфере ИБ.

Тема 13. Юридическая ответственность за правонарушения в сфере ИБ.

Понятие и виды юридической ответственности (ЮО) за правонарушения в сфере ИБ. Уголовная ответственность за правонарушения в сфере ИБ и ее особенности. Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны. Уголовная ответственность за компьютерные преступления и особенности их реализации в современной России. Правовое регулирование отношений, связанных с привлечением к ответственности лиц, совершивших административные правонарушения в сфере ИБ. Составы административных правонарушений, посягающих на ИБ страны. Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

4.Материалы текущего контроля успеваемости обучающихся

4.1.В ходе реализации дисциплины **Б1.В.02.05. «Правовое обеспечение информационной безопасности» используются следующие методы текущего контроля успеваемости обучающихся:**

Тема занятия	Вид занятия / Оценочное средство
Информационная безопасность (ИБ) РФ и задачи по ее обеспечению	ПЗ / опрос
Нормативно-правовая база обеспечения ИБ в России	ПЗ / опрос
Информация как объект правового регулирования и защиты	ПЗ / опрос
Система субъектов обеспечения ИБ в России и их правовой статус	ПЗ / опрос
Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика	ПЗ / опрос
Правовая защита личности в информационной сфере	ПЗ / опрос
Правовой режим государственной тайны и меры по ее обеспечению	ПЗ / опрос
Правовые и организационные способы защиты информации в сфере высоких технологий	ПЗ / опрос
Правовое обеспечение права интеллектуальной собственности (ПИС)	ПЗ / опрос
Правовая защита коммерческой тайны (КТ)	ПЗ / опрос
Правовое регулирование отношений в сфере лицензирования и сертификации	ПЗ / опрос
Предупреждение преступлений в информационной сфере в современной России	ПЗ / опрос
Юридическая ответственность за правонарушения в сфере ИБ	ПЗ / опрос

Полный перечень типовых оценочных материалов находится в фонде оценочных средств по дисциплине.

Вопросы для обсуждения

1. Какими факторами обусловлена актуальность проблемы обеспечения защиты информации?
2. Каковы основные задачи информационной безопасности?
3. Какие классы угроз информационной безопасности можно выделить?
4. Каковы основные методы реализации угроз информационной безопасности?
5. Какие существуют средства и методы обеспечения целостности информации?
6. Какие существуют средства и методы обеспечения конфиденциальности информации?
7. Каковы особенности защиты информации при работе с сетевыми сервисами?
8. Какова цель резервного копирования данных?
9. Каковы место и роль системы обеспечения информационной безопасности в национальной безопасности РФ?

10. Каково состояние системы защиты информации в России и в ведущих зарубежных странах?
11. Какие Международные стандарты в области информационного обмена Вам известны?
12. Какие основные понятия и определения защиты информации Вы можете привести?
13. Какие уровни обеспечения информационной безопасности Вам известны?
14. В чем заключается особенность государственной политики в области информационной безопасности?
15. Когда была принята Доктрина информационной безопасности РФ?
16. Какие нормативные руководящие документы, касающиеся государственной тайны Вам известны?
17. Какие преступления можно отнести к компьютерным?
18. Как классифицируются компьютерные преступления?
19. Что такое угроза информационной безопасности?
20. По каким признакам можно классифицировать угрозы информационной безопасности?
21. Каковы причины успешной реализации угроз информационной безопасности?
22. Какие каналы утечки и искажения информации Вам известны?
23. Каковы основные методы реализации угроз информационной безопасности?
24. Какое влияние на состояние информационной безопасности оказывает развитие глобальных сетей?
25. Какие виды нарушения информационной системы Вам известны?

Задание (тип 1):

Разработать нормативную документацию организации (государственного органа/хозяйствующего субъекта) в сфере информационной безопасности:

1. Политика информационной безопасности
2. Концепция обеспечения информационной безопасности
3. Положение о службе информационной безопасности
4. План защиты информационных активов от несанкционированного доступа
5. Правила обеспечения безопасности при работе пользователей в корпоративной сети
6. Политика управления доступом к ресурсам корпоративной сети
7. Политика управления инцидентами информационной безопасности
8. Политика обеспечения безопасности при взаимодействии с сетью Интернет
9. Политика антивирусной защиты
10. Парольная политика
11. Политика обеспечения безопасности платежных систем организации
12. Руководство по защите конфиденциальной информации
13. Регламент работы с цифровыми носителями конфиденциальной информации
14. Политика предотвращения утечки информации по каналам связи
15. Политика обеспечения безопасности электронного документооборота

и другие.

Задание (тип 2):

Выполнить задания по использованию информационных ресурсов (справочно-правовые системы, электронный документооборот, электронные торговые площадки).

Компоненты:

- определение объектов безопасности личности, общества, государства и их жизненно важных интересов;

- прогнозирование, выявление, анализ и оценка угроз и рисков безопасности личности, общества, государства, в том числе с применением риск-ориентированного подхода;

- принятие правовых мер по нейтрализации угроз безопасности личности, общества, государства.

Описание критериев оценивания компетенции

Критерий оценивания	**Характеристика критерия оценивания**
системность	системный подход к определению объектов безопасности личности, общества, государства и их жизненно важных интересов
объективность	выявление объективных обстоятельств, способствующих возникновению угроз и рисков безопасности личности, общества, государства;
оперативность	система правовых мер, позволяющая осуществить нейтрализацию угроз безопасности личности, общества, государства кратчайшие сроки

Схема расчета рейтинговых баллов по дисциплине
Б1.В.02.05. «Правовое обеспечение информационной безопасности»
по специальности 45.05.01 «Правовое обеспечение национальной безопасности»

Недели	Виды учебных занятий (лекции/семинары)	Посещение учебных занятий	Письменные работы			Устные выступления		Компенсирующие задания (сверх расчетных 100 баллов)	Промежуточная аттестация	Итого (максимально-расчетное количество баллов)
			Контрольные	Решение ситуационной задачи	Тестирование	Ролевые игры	Опрос			
Кол-во баллов за 1 вид мероприятия										
1	лекция	1								
2	семинар	1		4/5			2	1 (эссе)		
3	лекция	1								
4	лекция	1								Σ за 4 недели =8/9
5	семинар	1		4/5			2	1 (эссе)		
6	семинар	1		4/5			2	1 (эссе)		
7	лекция	1								
8	лекция	1								Σ за 8 недель =25/29
9	семинар	1		4/5			2	1 (эссе)		
	Текущий* контроль 1									29
10	семинар	1		4/5			2	1 (эссе)		
11	лекция	1								
12	лекция	1								Σ за 12 недель = 37/42
13	лекция	1		4/5			2	1 (эссе)		
14		1		4/5			3	1 (эссе)		
15	лекция	1								
16	семинар	1		4/5***			5	1 (эссе)		Σ за 16 недель
										64/76
	Текущий** контроль 2								24	24
Всего за семестр (баллов)		16		32/40			20	8	24	100

*Количество баллов, достаточное для аттестации текущего контроля

**Количество баллов, достаточное для возможного освобождения от промежуточной аттестации

*** возможна замена на результаты тестирования

Условия выполнения задания:

1. Место выполнения: в учебной аудитории
2. Каждый критерий оценки доклада оценивается в 1 балл, максимум 4 балла за доклад. Допускается не более трех докладов в семестр (всего 12 баллов)
3. За полноту и правильность ответа на вопрос при устном опросе в соответствии со сложностью вопроса присваиваются баллы от 5 до 10 баллов. Всего необходимо получить до 30 баллов в семестр.
4. Тестирование проходит два раза за семестр и оценивается по критерию оценки – правильность ответов на тестовые задания в баллах от 0 до 5, всего необходимо набрать до 10 баллов.

5.Оценочные материалы промежуточной аттестации по дисциплине

5.1. Промежуточная аттестация проводится с применением следующих методов:

Зачет проводится на основе компьютерного тестирования в ДОТ/устно/письменно

Промежуточная аттестация проводятся устно в ДОТ/письменно с прокторингом / тестирование с прокторингом. Для успешного освоения курса учащемуся рекомендуется ознакомиться с литературой, размещенной в разделе 6, и материалами, выложенными в ДОТ.

5.2.Оценочные материалы промежуточной аттестации

Компонент компетенции	Промежуточный/ключевой индикатор оценивания	Критерий оценивания
ПКр ОС-1.2. Способность обеспечивать безопасность личности, общества, государства правовыми средствами;	Обеспечивает безопасность личности, общества, государства правовыми средствами;	**30-40 баллов** Обучающийся показывает высокий уровень компетентности, знания программного материала, учебной литературы, раскрывает и анализирует проблему с точки зрения различных авторов. Обучающийся показывает не только высокий уровень теоретических знаний, но и видит междисциплинарные связи. Профессионально, грамотно, последовательно, хорошим языком четко излагает материал, аргументированно формулирует выводы. Знает в рамках требований к направлению и профилю подготовки нормативную и практическую базу. На вопросы отвечает кратко, аргументировано, уверенно, по существу. Способен принимать быстрые и нестандартные решения. **19-29 баллов** Обучающийся показывает достаточный уровень компетентности, знания материалов занятий, учебной и методической литературы, нормативов и практики его применения. Уверенно и профессионально, грамотным языком, ясно, четко и понятно излагает состояние и суть вопроса. Знает теоретическую и практическую базу, но при ответе допускает несущественные погрешности. Обучающийся показывает достаточный уровень профессиональных знаний, свободно оперирует понятиями, методами оценки принятия решений, имеет представление: о междисциплинарных связях, увязывает знания, полученные при изучении

		различных дисциплин, умеет анализировать практические ситуации, но допускает некоторые погрешности. Ответ построен логично, материал излагается хорошим языком, привлекается информативный и иллюстрированный материал, но при ответе допускает незначительные ошибки, неточности по названным критериям, которые не искажают сути ответа; **1-18 баллов** Обучающийся показывает слабое знание материалов занятий, отсутствует должная связь между анализом, аргументацией и выводами. На поставленные вопросы отвечает неуверенно, допускает погрешности. Обучающийся владеет практическими навыками, привлекает иллюстративный материал, но чувствует себя неуверенно при анализе междисциплинарных связей. В ответе не всегда присутствует логика, аргументы привлекаются недостаточно веские. На поставленные вопросы затрудняется с ответами, показывает недостаточно глубокие знания. **0 баллов** Обучающийся показывает слабые знания материалов занятий, учебной литературы, теории и практики применения изучаемого вопроса, низкий уровень компетентности, неуверенное изложение вопроса. Обучающийся показывает слабый уровень профессиональных знаний, затрудняется при анализе практических ситуаций. Не может привести примеры из реальной практики. Неуверенно и логически непоследовательно излагает материал. Неправильно отвечает на вопросы или затрудняется с ответом.

5.3. Показатели и критерии оценивания текущих и промежуточных форм контроля

Оценочные средства	Показатели оценки	Критерии оценки
Доклад	Соблюдение регламента (15 мин.); характер источников (более трех источников); подача материала (презентация); ответы на вопросы (владение материалом).	Каждый критерий оценки доклада оценивается в 0,25 балла, максимум 1 балл за доклад. Допускается не более одного доклада в семестр, десяти докладов в год (всего до 10 баллов)
Тестирование	Процент правильных ответов на вопросы теста	Менее 60% – 0 баллов; 61 - 75% – 6 баллов; 76 - 90% – 8 баллов; 91 - 100% – 10 баллов.
Зачет	В соответствии с балльно-рейтинговой системой на промежуточную аттестацию отводится 30 баллов. Зачет проводится по тестам.	Менее 60% – 0 баллов; 61 - 75% – 10 баллов; 76 - 90% – 20 баллов; 91 - 100% – 30 баллов.
Устный опрос	Корректность и полнота ответов	Сложный вопрос: полный, развернутый, обоснованный ответ – 10 баллов Правильный, но не аргументированный ответ – 5 баллов Неверный ответ – 0 баллов Обычный вопрос: полный, развернутый, обоснованный ответ – 4 балла Правильный, но не аргументированный ответ – 2 балла

		Неверный ответ – 0 баллов. Простой вопрос: Правильный ответ – 1 балл; Неправильный ответ – 0 баллов
Выполнение проблемных заданий	Правильность решения; корректность выводов обоснованность решений	баллы начисляются от 1 до 3 в зависимости от сложности задачи/вопроса (не более 38 баллов за семестр)

Типовые оценочные материалы промежуточной аттестации

Вопросы к зачету

1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению
2. Нормативно-правовая база обеспечения ИБ в России
3. Информация как объект правового регулирования и защиты
4. Система субъектов обеспечения ИБ в России и их правовой статус
5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика
6. Правовая защита личности в информационной сфере
7. Правовой режим государственной тайны и меры по ее обеспечению
8. Правовые и организационные способы защиты информации в сфере высоких технологий
9. Правовое обеспечение права интеллектуальной собственности (ПИС)
10. Правовая защита коммерческой тайны (КТ)
11. Правовое регулирование отношений в сфере лицензирования и сертификации
12. Предупреждение преступлений в информационной сфере в современной России
13. Юридическая ответственность за правонарушения в сфере ИБ

Критерии оценки ответа на зачетное тестирование:

Процент правильных ответов на вопросы теста.

Шкала оценивания

Применение балльно-рейтинговой системы оценки знаний студентов

При оценивании используется балльно-рейтинговая система. Баллы начисляются за посещаемость (максимум 20 баллов), выступления с докладами (максимум 12 баллов), полный и правильный ответ на вопрос при устном опросе (максимум 30 баллов), результаты выполнения тестовых заданий, ответ на экзамене (максимум 30 баллов). Дисциплина считается освоенной, если экзаменуемый набрал не менее 51 балла в результате выполнения всех типов заданий, включая ответ на экзамене. Минимальное количество баллов для допуска к экзамену – 45.

На основании п. 14 Положения о балльно-рейтинговой системе оценки знаний обучающихся в РАНХиГС в институте принята следующая шкала перевода оценки из многобалльной системы в пятибалльную:

Оценка результатов производится на основе балльно-рейтинговой системы (БРС). Использование БРС осуществляется в соответствии с приказом от 06 сентября 2019 г. №306 «О применении балльно-рейтинговой системы оценки знаний обучающихся».

Схема расчетов сформирована в соответствии с учебным планом направления, согласована с руководителем научно-образовательного направления, утверждена деканом факультета.

Схема расчетов доводится до сведения студентов на первом занятии по данной дисциплине, является составной частью рабочей программы дисциплины и содержит информацию по изучению дисциплины, указанную в Положении о балльно-рейтинговой системе оценки знаний обучающихся в РАНХиГС.

В соответствии с балльно-рейтинговой системой максимально-расчетное количество баллов за семестр составляет 100, из них в рамках дисциплины отводится:

40 баллов - на промежуточную аттестацию

40 баллов - на работу на семинарских занятиях

20 баллов - на посещаемость занятий

В случае если студент в течение семестра не набирает минимальное число баллов, необходимое для сдачи промежуточной аттестации, то он может заработать дополнительные баллы, отработав соответствующие разделы дисциплины, получив от преподавателя компенсирующие задания.

В случае получения на промежуточной аттестации неудовлетворительной оценки студенту предоставляется право повторной аттестации в срок, установленный для ликвидации академической задолженности по итогам соответствующей сессии.

Обучающийся, набравший в ходе текущего контроля в семестре от 51 до 60 баллов, по его желанию может быть освобожден от промежуточной аттестации.

Шкала перевода оценки из многобалльной в систему «зачтено»/«не зачтено»:

от 0 по 50 баллов	«не зачтено»
от 51 по 100 баллов	«зачтено»

6. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов включает подготовку к практическим занятиям, которая предусматривает подготовку докладов и презентаций. Учебно-методическое обеспечение самостоятельной работы студентов представлено в данной программе. Контроль за качеством самостоятельно подготовленных материалов осуществляется в процессе проведения практических занятий с помощью соответствующих оценочных средств, также представленных в данной программе.

Вид учебных занятий, промежуточная аттестация	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, формулы, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, сложный материал, формулы, которые вызывают трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации или при выполнении лабораторной работы.
Лабораторные работы	Лабораторные работы направлены на экспериментальное подтверждение теоретических положений и формирование учебных и профессиональных практических умений. В процессе лабораторного занятия обучающиеся выполняют задания под руководством преподавателя в соответствии с изучаемым содержанием учебного материала. Все студенты, находящиеся в лаборатории, должны соблюдать инструкцию по охране труда при проведении лабораторных занятий в аудиториях кафедры. Перед выполнением лабораторной работы необходимо познакомиться с теоретическим материалом и описанием соответствующей работы, используя методическую литературу по данной теме.
Практические занятия	Практические занятия направлены на формирование учебных и профессиональных практических умений, выполнение расчетов и задач.
Научно-исследовательская работа	При выполнении НИР студенты должны решать задачи практической направленности на основании теоретических положений, получая реальные результаты на основе обоснованного анализа данных.
Подготовка к экзамену	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

При проведении учебных занятий предусмотрено применение разных форм учебных занятий, развивающих у обучающихся навыки командной работы, межличностной коммуникации, включая проведение интерактивных лекций, групповых дискуссий.

В процессе лекционного занятия обучающийся ведет свой конспект лекций, делая записи, касающиеся основных тезисов лектора. Это могут быть исходные проблемы и вопросы, ключевые понятия и их определения, важнейшие положения и выводы, существенные оценки и т.д.

В заключительной части лекции обучающийся может задать вопросы преподавателю по содержанию лекции, уточняя и уясняя для себя теоретические моменты, которые остались ему непонятными.

Самостоятельная работа обучающегося, прежде всего, подразумевает изучение им учебной литературы, рекомендуемой рабочей программой дисциплины.

Значительную роль в изучении данной дисциплины выполняют семинарские занятия, которые призваны, прежде всего, закреплять теоретические знания, полученные в ходе прослушивания и запоминания лекционного материала, изучения источников, ознакомления с учебной и научной литературой. Тем самым семинары способствуют получению студентами наиболее качественных знаний, а также позволяют осуществлять со стороны преподавателя текущий контроль над успеваемостью студентов.

Семинарские занятия преподаватель может проводить в форме обсуждения вопросов темы, заслушивания докладов по отдельным вопросам и их обсуждения, рекомендуется выполнение письменных работ, тестирование и решение практических задач.

В процессе подготовки к семинару студент самостоятельно аккумулирует знания путем изучения конспекта лекций и соответствующих разделов учебника, ознакомления с дополнительной литературой и источниками, рекомендованными к этому практическому занятию.

Отвечать на тот или иной вопрос обучающимся рекомендуется формулировать наиболее полно и точно, при этом нужно уметь логически грамотно выражать и обосновывать свою точку зрения, свободно оперировать юридическими понятиями и терминами.

Предусмотрена работа слушателей на практических занятиях (семинарах) по рассмотрению основных тенденций мировой экономики и международных экономических отношений. Есть часы лабораторной работы с практической оценкой мировых тенденций по изучаемым вопросам.

Таким образом, посещение обучающимся лекционных занятий, активная самостоятельная работа, а также участие на семинарских занятиях необходимы для подготовки и успешной сдачи экзамена как формы итогового контроля.

При подготовке к зачету необходимо исходить из перечня контрольных вопросов. зачет, как правило, проводится в устной форме.

При оценивании знаний студентов экзаменатор руководствуется, прежде всего, следующими критериями:

- правильность ответов на вопросы;
- полнота и лаконичность ответа;
- логика и аргументированность изложения.

Более подробную информацию о методике подготовки и сдачи зачета обучающийся может получить у преподавателя.

Учебно-методическое обеспечение самостоятельной работы

Для успешного овладения учебным материалом и методами системного анализа студент обязан не менее 4-х часов в неделю уделять самостоятельной работе: подготовке к семинарским занятиям, нахождению в учебнике ответов на тестовые задания к каждой теме дисциплины, организации учебно-исследовательской деятельности.

В самостоятельной работе студентов могут также найти свое применение специально созданные научно-просветительские и образовательные мультимедиа продукты с ориентацией на историко-культурные и историко-политические сюжеты, изданные на CD-R.

Положительной стороной образовательной технологии является ее гибкость, адаптация к индивидуальным особенностям студентов за счет исходной диагностики уровня и объема знаний, варьирования темпа усвоения учебного материала.

В компьютерном классе организована система предварительной записи студентов.

Тестовые задания ориентированы на альтернативный, простой выборочный, выборочно-конструируемый и свободно-конструируемый ответы. При компьютерном тестировании эти задания группируются в фреймы, где последовательность вопросов генерируется в диалоговом режиме и может включать в себя цепочки уточняющих вопросов (вопросы с продолжением), а

в некоторых случаях и обучающие комментарии.

Каждый вопрос, при правильном ответе на него, имеет свою экспертную весовую оценку, которая учитывается при сборе статистической информации и заносится в индивидуальный файл тестируемого. Затем эти данные обрабатываются и группируются в сводные статистические таблицы для учебных (семинарских) групп. Таким образом, создается объективная картина учебных достижений каждого студента на всех этапах обучения. Время, отводимое на компьютерное тестирование, ограничено. По окончании тестирования студенту выдается объективная информация, позволяющая выявить имеющиеся у него пробелы в знаниях и принять меры по их устранению.

На центральном компьютере тестирующей сети с точностью до вводимого символа фиксируются протоколы диалогов и хронометраж каждого тестируемого по всем сеансам его работы. Протоколы используются для разрешения конфликтных ситуаций и совершенствования компьютерного анализатора ответов на тестовые задания.

Методические рекомендации по изучению дисциплины

Для изучения основных вопросов образовательной программы необходимо конспектировать материалы лекций, работать с рекомендованной преподавателем литературой. Для приобретения навыков активного использования знаний полезно обсуждать решаемые задачи на практических занятиях. При разучивании формул полезно записывать их на бумаге. Чтобы легче и прочнее усвоить материал следует постоянно использовать конкретные примеры, сравнения из уже полученных областей наук.

Для закрепления изученного материала даны вопросы по каждой теме дисциплины, на которые следует самостоятельно найти ответы.

При подготовке к практическим занятиям необходимо ознакомиться с методическими указаниями по соответствующей теме и осуществить подготовку по рекомендованным в учебно-методическом комплексе вопросам для обсуждения темы.

После изучения базовых тем курса проводится оперативный контроль знаний студентов в виде опроса или письменного тестирования. Тестовые задания по темам дисциплины приведены в специальном разделе данного учебно-методического комплекса.

Подготовка к рубежному и итоговому контролю предполагает изучение представленных вопросов к экзамену, а также работу над тестами, представленными в данном учебно-методическом комплексе.

Для решения задач целесообразно широко использовать современные информационные технологии.

7.Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

7.1. Основная литература:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469235

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470131

7.2. Дополнительная учебная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470131

2. Баранова, Е.К. Информационная безопасность и защита информации : учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. – Москва : РИОР, ИНФРА-М, 2018. - 336 с.

7.3. Нормативные правовые документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс»

2. Федеральный конституционный закон от 06 ноября 2020 г. № 4-ФКЗ «О Правительстве Российской Федерации» // СПС «КонсультантПлюс».

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс».

4. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // СПС

5. Закон Российской Федерации от 1 апреля 1993 г. № 4730-1 «О Государственной границе Российской Федерации» // СПС «КонсультантПлюс».

6. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» // СПС «КонсультантПлюс».

7. Федеральный закон от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» // СПС «КонсультантПлюс».

8. Федеральный закон от 21 декабря 1994 г. № 69-ФЗ «О пожарной безопасности» // СПС «КонсультантПлюс».

9. Федеральный закон от 10 декабря 1995 г. № 196-ФЗ «О безопасности дорожного движения» // СПС «КонсультантПлюс».

10. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // СПС «КонсультантПлюс».

11. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» // СПС «КонсультантПлюс».

12. Федеральный закон от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности» // СПС «КонсультантПлюс».

13. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» // СПС «КонсультантПлюс».

14. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // СПС «КонсультантПлюс»

15. Федеральный закон от 2 апреля 2014 г. № 44-ФЗ «Об участии граждан в охране общественного порядка» // СПС «КонсультантПлюс».

16. Федеральный закон от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации» // СПС «КонсультантПлюс».

17. Указ Президента Российской Федерации от 18 апреля 1996 г. № 567 «О координации деятельности правоохранительных органов по борьбе с преступностью» // СПС «КонсультантПлюс».

18. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс».

7.5. Интернет-ресурсы

Доступ к подписным электронным информационным ресурсам осуществляется с любого рабочего места СЗИУ по локальной сети, а также с любого компьютера или мобильного устройства, подключенного к сети Интернет, через сайт научной библиотеки СЗИУ http://nwapa.spb.ru/ по индивидуальному логину и паролю.

Русскоязычные ресурсы: - учебники, учебные пособия, монографии, сборники статей, практикумы, статьи из периодических изданий из электронно-библиотечных систем: (ЭБС) Айбукс; (ЭБС) Лань; (ЭБС) ЮРАЙТ; (ЭБС) Book.ru; (ЭБС) IPRbook.- East View Information Services, Inc. (Ист-Вью) - статьи из периодических изданий (журналы, газеты) по общественным и гуманитарным наукам.

- Электронная библиотека ИД «Гребенников» - научно-практические статьи по финансам, менеджменту, маркетингу, логистике, управлению персоналом.

Англоязычные ресурсы:EBSCO Discovery +A-to-Z. Система поиска по электронной подписке института;
Ebook Central –Полнотекстовая база данных электронных книг по всем отраслям знаний; Springer Link - полнотекстовые политематические базы академических книг; WILEY - более 1600 монографий и сборников по юриспруденции, криминологии, экономике, финансам и др.; Cambridge University Press – полнотекстовые издания; EBSCO Publishing - мультидисциплинарные и тематические базы данных научных журналов; Emerald eJournals Premier - электронное собрание рецензируемых журналов; SAGE Premier – база рецензируемых полнотекстовых электронных журналов; Springer Link - полнотекстовые политематические базы академических журналов; WILEY - доступны выпуски 1500 академических журналов разных профилей; Архивы НЭИКОН - полные тексты научных журналов до 2012 года авторитетных издательств: Annual Reviews, Cambridge University Press, Oxford University Press, Sage Publications, Taylor & Francis

7.6.Иные источники

1. Правовая система «Гарант-Интернет» [Электронный ресурс]. – Режим доступа: http: // www.garweb.ru.
2. Правовая система «КонсультантПлюс» [Электронный ресурс]. – Режим доступа: http: // www.consultant.
3. Центр профессиональной подготовки [Электронный ресурс]. – Режим доступа: http: // www.c-pp.ru.

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Курс включает использование программного обеспечения Microsoft Excel, Microsoft Word, Microsoft Power Point для подготовки текстового и табличного материала, графических иллюстраций; Ramus – для моделирования бизнес-процессов. Методы обучения с использованием информационных технологий (компьютерное тестирование, демонстрация мультимедийных материалов) Интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии, справочники, библиотеки, электронные учебные и учебно-методические материалы) Системы дистанционного обучения. В процессе освоения дисциплины используются следующие образовательные технологии, способы и методы формирования компетенций:

- лекционные занятия проводятся с использование интерактивных методик обучения в форме лекции-беседы, лекции с разбором микроситуаций, лекций с интенсивной обратной связью, лекции-конференции и др.;
- при проведении практических занятий используются такие интерактивные методики как, ролевые и деловые игры, выполнение творческих заданий, работа в малых группах, дискуссии и другие.
- внеаудиторная работа с использованием правовой системы Консультант Плюс в целях оптимизации поиска нормативно-правовых актов.

Компьютерные технологии и программные продукты, необходимые для сбора и систематизации информации, разработки планов и т.д. Интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии, справочники, библиотеки, электронные учебные и учебно-методические материалы). Кроме вышеперечисленных ресурсов, используются следующие информационные справочные системы: http://uristy.ucoz.ru/; http://www.garant.ru/; http://www.kodeks.ru/ и другие.

№ п/п	Наименование
1.	Специализированные залы для проведения лекций:
2.	Специализированная мебель и оргсредства: аудитории и компьютерные классы, оборудованные посадочными местами
3.	Технические средства обучения: Персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов