

**Федеральное государственное образовательное бюджетное учреждение
высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

Ярославский филиал Финуниверситета

Кафедра «Экономика и финансы»

СОГЛАСОВАНО

Директор ООО Юридическая
компания «Константа»



Ю.В. Колесникова

«14» апреля 2026 г.

УТВЕРЖДАЮ

Директор
Ярославского филиала
Финуниверситета



В.А. Кваша

«21» апреля 2026 г.

Автор: И.А. Девятковская

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

Рабочая программа дисциплины

для студентов, обучающихся по направлению (ям) подготовки
40.03.01 «Юриспруденция»,
профиль «Экономическое право»
(очная форма обучения)

*Рекомендовано Ученым советом Ярославского филиала Финуниверситета
(протокол № 35 от 21.04.2026)*

*Одобрено кафедрой «Экономика и финансы»
(протокол № 8 от 06.04.2026)*

СОДЕРЖАНИЕ

1. Наименование дисциплины	3
2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	3
3. Место дисциплины в структуре образовательной программы	4
4. Объем дисциплины в зачетных единицах и академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся (в семестре, в сессию)	5
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	5
5.1. Содержание дисциплины	5
5.2. Учебно-тематический план	8
5.3. Содержание практических и семинарских занятий	9
6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине	11
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	11
6.2. Методическое обеспечение для аудиторной и внеаудиторной самостоятельной работы	14
7. Фонд оценочных средств для проведения промежуточной аттестации	19
7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы:	19
7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания	19
7.3. Соответствующие приказы, распоряжения ректората о контроле уровня освоения дисциплин и сформированности компетенций студентов	23
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	23
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	24
10. Методические указания для обучающихся по освоению дисциплины.	24
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	25
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	26

1. Наименование дисциплины

Дисциплина Б.1.2.2.2.2.2. «Правовое обеспечение кибербезопасности».

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Таблица 1 - Структура планируемых результатов обучения

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесённые с компетенциями/индикаторами достижения компетенции
ПКП-1	Способность использовать фундаментальные знания в области частного права и публичного права в современных условиях и оказывать помощь в реализации правовых норм субъектами гражданского оборота	1. Демонстрирует знания нормативных правовых актов, а также прогнозирует результат экономической деятельности для решения практических задач. 2. Использует фундаментальные знания в области частного и публичного права в современных условиях. 3. Оказывает помощь в реализации правовых норм субъектами гражданского оборота.	Знать: основные положения нормативных правовых актов в области обеспечения кибербезопасности; позиции высших судебных инстанций; Уметь: ориентироваться в проблематике обеспечения кибербезопасности и на данной основе прогнозировать результат экономической деятельности. Знать: фундаментальные частного и публичного права в современных условиях применительно к проблематике кибербезопасности Уметь: соотносить юридические факты с законодательством; систематизировать необходимый материал и анализировать практику правоприменения в информационно правовой сфере; осуществлять выбор оптимального варианта правомерного поведения в информационных правоотношениях с учетом фактических обстоятельств дела. Знать: основные положения нормативных правовых актов в области обеспечения кибербезопасности, угрозы кибербезопасности и правовые меры обеспечения информационной безопасности; Уметь: оказывать помощь в

			реализации правовых норм для обеспечения кибербезопасности субъектам гражданского оборота.
ПКП-2	Способность действовать с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера, анализировать проблемные ситуации на рынке товаров, работ, услуг, а также выявлять правонарушения при осуществлении предпринимательской деятельности и давать юридически обоснованные предложения по их преодолению и устранению.	1. Действует с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера. 2. Выявляет правонарушения при осуществлении предпринимательской деятельности. 3. Дает юридически обоснованные предложения по преодолению и устранению правонарушений при осуществлении предпринимательской деятельности.	Знать: кризисных ситуаций в экономике, вызываемых рисками нарушения кибербезопасности; Уметь: анализировать кризисные ситуации в экономике, вызываемых рисками нарушения кибербезопасности; противодействовать различным проявлениям информационных угроз. Знать: основные направления обеспечения кибербезопасности; требования нормативных правовых актов к субъектам предпринимательской деятельности по обеспечению кибербезопасности; Уметь: выявлять правонарушения в ходе обеспечения кибербезопасности при осуществлении предпринимательской деятельности. Знать: основные направления правового обеспечения кибербезопасности; Уметь: вырабатывать обоснованные предложения по преодолению и устранению правонарушений при обеспечении кибербезопасности при осуществлении предпринимательской деятельности.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Правовое обеспечение кибербезопасности» входит в цикл профиля (элективный) части, формируемой участниками образовательных отношений, в Модуль «Право цифровой экономики» профиля «Экономическое право» образовательной программы «Юриспруденция» по направлению подготовки 40.03.01 «Юриспруденция», очная форма обучения.

4. Объем дисциплины в зачетных единицах и академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся (в семестре, в сессию)

Таблица 2 - Объём учебной дисциплины

Вид учебной работы по дисциплине	Всего (в з.е. и часах)	Семестр 7
Общая трудоемкость дисциплины	3 / 108	108
Аудиторные занятия	34	34
Лекции (Л)	16	16
Практические и семинарные занятия, т.ч. занятия в интерактивных формах (С)	18	18
Самостоятельная работа	74	74
Текущий контроль	Контрольная работа	
Промежуточный контроль	Зачет	

5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Понятие кибербезопасности, место кибербезопасности в системе информационной безопасности РФ

Национальная безопасность. Информационная безопасность. Соотношение кибербезопасности и информационной безопасности.

Дискуссионные вопросы определения кибербезопасности.

Необходимость правового регулирования кибербезопасности. Методы обеспечения кибербезопасности. Цель обеспечения кибербезопасности. Принципы обеспечения кибербезопасности.

Понятия информационного пространства и киберпространства. Национальная киберинфраструктура: система передачи данных, в том числе телекоммуникационной сети Интернет, и услугах, направленных на расширение использования киберпространства; система основных услуг, включающая национальную систему распределения доменных имен, национальную систему идентификации аутентификации (цифрового профиля); услуги и приложения в области информационных технологий, включая онлайн-сервисы; электронное правительство, электронная коммерция, сайты сети «Интернет» с общественно значимой информацией, онлайн-форумы, социальные сети, блоги; искусственный интеллект; инфраструктура информационных технологий умного города, система виртуальной реальности, облачные вычисления, система больших данных, системы мгновенной передачи данных и иные интеллектуальные системы.

Тема 2. Основные направления правового регулирования информационных отношений в Российской Федерации

Понятие и виды источников информационного права. Структура, состав и особенности информационного законодательства. Конституционные основы информационного законодательства.

Базовый закон информационной сферы. Базовые законодательные акты, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, федеральных органов исполнительной власти, регулирующие отношения в информационной сфере.

Понятие, содержание, структура информационных правоотношений.

Классификация информационных правоотношений. Объекты и субъекты информационных правоотношений.

Тема 3. Основные виды киберугроз и проблема защиты конечных пользователей

Киберпреступность.

Компьютерные атаки и инциденты (кибератаки)

Кибертерроризм.

Вредоносное программное обеспечение: вирусы, троянские программы, шпионское ПО, программы-вымогатели, рекламное ПО в Интернет, ботнеты.

Булинг.

Фишинг.

DDos – атаки.

Защита пользователей

Тема 4. Международно-правовое регулирование кибербезопасности

Международный стандарт ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности» (ISO/ IEC 27032 Information technology. Security techniques. Guidelines for cybersecurity)

Будапештская Конвенция Совета Европы по киберпреступлениям ETS 185 от 23 ноября 2001 г. Общие правила ЕС по защите данных (GDPR) от 14 апреля 2016 года. Регламент 2019/881 Об Агентстве ЕС по кибербезопасности (ENISA) и сертификации по кибербезопасности информационных и коммуникационных технологий (Cybersecurity Act) 2019 г.

Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (подготовлен РФ).

Международные стандарты NIST, IEC 62443.

Тема 5. Правовое обеспечение кибербезопасности в РФ

Стратегия развития информационного общества в Российской Федерации об обеспечении кибербезопасности. Проблемы разработки Стратегии кибербезопасности Российской Федерации. Доктрина информационной безопасности. Указ Президента от 01 мая 2022 года №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и нормативные правовые акты, принятые для его реализации.

Государственные (национальные) стандарты РФ и руководящие документы по кибербезопасности. Правовое обеспечение безопасности критической информационной инфраструктуры Российской Федерации. Создание ГосСОПКА (государственной системы обнаружения,

предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации).

Критерии и методы оценки эффективности систем и средств обеспечения информационной безопасности и кибербезопасности. Оценка защищенности государственных информационных ресурсов и систем.

Создание механизма мониторинга киберугроз и реагирования на них. Повышение информированности общества в сфере кибербезопасности.

Тема 6. Правовое обеспечение кибербезопасности критической информационной инфраструктуры

Органы ответственные за обеспечение кибербезопасности критической информационной инфраструктуры. Полномочия ФСТЭК, ФСБ и иных государственных органов в сфере обеспечения кибербезопасности.

Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». ФСБ РФ рекомендации №149/2/7-200 от 24 декабря 2016 г. «Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Категорирование объектов. Внедрение и поддержка технических средств и решений для осуществления деятельности по мониторингу информационной безопасности средств и систем мониторинга.

Осуществление взаимодействия при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Тема 7. Правовое обеспечение кибербезопасности конечных пользователей в информационно-телекоммуникационной сети «Интернет»

Особенности правового регулирования общественных отношений в сети «Интернет». Требования к информационным ресурсам в сети «Интернет».

Распространение информации в сети «Интернет». Правовое регулирование социальных сетей.

Защита персональных данных в сети «Интернет»

Деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет».

Актуальные вопросы ограничения доступа к сайтам в сети «Интернет» с информацией, распространяемой с нарушением законодательства РФ.

Тема 8. Юридическая ответственность за правонарушения в сфере кибербезопасности

Понятие киберпреступления и правонарушения в сфере кибербезопасности.

Уголовная ответственность за киберпреступления: создание, распространение и использование программ для неправомерного воздействия; неправомерный доступ к информации с последующим

причинением вреда; нарушение правил эксплуатации средств хранения, обработки, передачи информации; распространение заведомо недостоверной информации; несанкционированный доступ к персональным данным; преступления, связанные с экстремистской и террористической деятельностью.

Административная ответственность за противоправные деяния в киберпространстве.

5.2. Учебно-тематический план

Таблица 3 - Учебно-тематический план

№ п/п	Наименование темы (раздела) дисциплины	Трудоемкость						Формы текущего контроля успеваемости и
		Всего	Аудиторная работа				Само стоят ельна я работ а	
			Общая	Лекции и	Практ . и семин. занят ия	В т. ч. занят ия в интер акт. форме		
1.	Понятие кибербезопасности, место кибербезопасности в системе информационной безопасности РФ	17	6	2	4	2	11	Научная дискуссия, доклады, учебные презентации, письменные работы, фронтальный опрос-рефлексия, круглый стол, коллоквиум, ДТЗ
2.	Основные направления правового регулирования информационных отношений в Российской Федерации	13	4	2	2	1	9	
3.	Основные виды киберугроз и проблема защиты конечных пользователей	13	4	2	2	1	9	
4.	Международно-правовое регулирование кибербезопасности	13	4	2	2	1	9	
5	Правовое обеспечение кибербезопасности в РФ	13	4	2	2	1	9	
6	Правовое обеспечение кибербезопасности критической информационной инфраструктуры	13	4	2	2	1	9	

7	Правовое обеспечение кибербезопасности конечных пользователей в информационно-телекоммуникационной сети «Интернет»	13	4	2	2	1	9	
8	Юридическая ответственность за правонарушения в сфере кибербезопасности	13	4	2	2	1	9	
	Итого	108	34	16	18	9	74	
	Итого в %		100			50		

5.3. Содержание практических и семинарских занятий

Таблица 3 - Семинарские занятия

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
Тема 1. Понятие кибербезопасности, место кибербезопасности в системе информационной безопасности РФ	1. Понятия Национальная безопасность и Информационная безопасность. 2. Определения киберпространства и кибербезопасности. 3. Необходимость правового регулирования кибербезопасности. 4. Методы обеспечения кибербезопасности. 5. Принципы обеспечения кибербезопасности. 6. Национальная киберинфраструктура Рекомендуемые источники из разделов 8 (А-1,6,7,8; Б-11, 12); 9 (2,3,4)	опрос, групповая дискуссия
Тема 2. Основные направления правового регулирования информационных отношений в Российской Федерации	1. Понятие и виды источников информационного права. 2. Структура, состав и особенности информационного законодательства. 3. Конституционные основы информационного законодательства. 4. Базовый закон информационной сферы. 5. Объекты и субъекты информационных правоотношений. 6. Права и обязанности обладателя информации. 7. Государство как субъект информационных отношений. Рекомендуемые источники из разделов 8 (А-1,2; Б-11; В-14); 9 (1,2,3,4)	опрос, тестирование, групповая дискуссия, презентация докладов
Тема 3. Основные виды	1. Субъекты кибербезопасности. 2. Киберпреступность.	опрос, групповая

киберугроз и проблема защиты конечных пользователей	3. Компьютерные атаки и инциденты. 4. Защита конечных пользователей. Рекомендуемые источники из разделов 8 (А-7; Б-12,13; В-14); 9 (4,5,6)	дискуссия, решение практических ситуационных задач, презентация докладов
Тема 4. Международно-правовое регулирование кибербезопасности	1. Международные стандарты кибербезопасности. 2. Конвенция о киберпреступности. 3. Cybersecurity Act. 4. Проблемы международно-правового обеспечения кибербезопасности. Рекомендуемые источники из разделов 8 (А-1; Б-12; В-14,15); 9 (2,3,4,5)	опрос, решение практико-ориентированных задач, групповая дискуссия, презентация докладов
Тема 5. Правовое обеспечение кибербезопасности в РФ	1. Нормативно правовая база Российской Федерации об обеспечении кибербезопасности. 2. Проблемы разработки Стратегии кибербезопасности Российской Федерации. 3. Государственные (национальные) стандарты РФ и руководящие документы по кибербезопасности. 4. Критерии и методы оценки эффективности систем и средств обеспечения информационной безопасности и кибербезопасности. 5. Мониторинг киберугроз и система реагирования на них. Рекомендуемые источники из разделов 8 (А-1,2,3,4,6; Б-11,12,13); 9 (1,2,3,4,6)	решение практико-ориентированных задач, групповая дискуссия, презентация докладов
Тема 6. Правовое обеспечение кибербезопасности критической информационной инфраструктуры	1. Понятие критической информационной инфраструктуры. 2. Принципы, задачи, функции и стандарты обеспечения безопасности критической информационной инфраструктуры. 3. ГосСОПКА. 4. Полномочия ФСТЭК, ФСБ и иных государственных органов в сфере обеспечения кибербезопасности. Рекомендуемые источники из разделов 8 (А-1,4,5,7,8; Б-11,12); 9 (2,3,6)	опрос, групповая дискуссия, тестирование, презентация докладов
Тема 7. Правовое обеспечение кибербезопасности конечных пользователей в информационно-телекоммуникационной сети «Интернет»	1. Особенности правового регулирования общественных отношений в сети «Интернет». 2. Актуальные вопросы ограничения доступа к сайтам в сети «Интернет» с информацией, распространяемой с нарушением законодательства РФ. 3. Правовой статус организатора распространения информации в сети "Интернет". 4. Регулирование социальных сетей	Опрос, ситуационные и практические задачи, дискуссия

	5. Особенности распространения информации в сети интернет. 6. Особенности распространения информации иностранными субъектами. Рекомендуемые источники из разделов 8 (А-1,2,3,10; Б-11,12,13; В-14); 9 (1,2,3,4)	
Тема 8. Юридическая ответственность за правонарушения в сфере кибербезопасности	1. Понятия киберпреступности, киберпреступления и административного правонарушения в сфере кибербезопасности. 2. Уголовная ответственность за киберпреступления. 3. Административная ответственность за правонарушения в сфере кибербезопасности. Рекомендуемые источники из разделов 8 (А-1,9,10; Б-11,12,13; В-15); 9 (1,2,3,4,5)	опрос, групповая дискуссия, анализ нормативно-правовых документов и судебной практики

6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

К внеаудиторным формам самостоятельной работы студентов относятся:

- подготовка к семинарским занятиям;
- выполнение контрольной работы;
- подготовка к зачету.

На семинарских занятиях все студенты должны принимать активное участие в обсуждении изучаемых вопросов и уметь демонстрировать знание практического материала. При выступлении, студентам необходимо аргументировано излагать свою позицию, подкреплять ее конкретными данными, уметь обобщать, аргументировать и систематизировать статистические данные.

На семинарских занятиях преподаватель проверяет выполнение самостоятельных заданий и качество усвоения знаний.

Таблица 5 – Темы дисциплины, изучаемые вопросы и формы внеаудиторной самостоятельной работы

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Тема 1. Понятие кибербезопасности место кибербезопасности в системе	1. Общеметодологические проблемы обеспечения информационной безопасности и кибербезопасности. 2. Стратегия развития	Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, работа со справочно-правовыми системами, подбор

информационной безопасности РФ	информационного общества в Российской Федерации. 3. Проблемы формирования понятийного (терминологического) аппарата в области кибербезопасности. 4. Проблемы развития информационной сферы как системообразующего фактора жизни общества.	материала к групповой дискуссии, изучение рекомендованных к занятию нормативных правовых актов, литературных источников.
Тема 2. Основные направления правового регулирования информационных отношений в Российской Федерации	1. Информационное право как наука, учебная дисциплина, система правового регулирования общественных отношений в информационном обществе. 2. Система информационного права. 3. Законодательные акты, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, федеральных органов исполнительной власти, регулирующие отношения в информационной сфере. 4. Правовой статус государственных организаций и учреждений в области обеспечения кибербезопасности	Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, изучение рекомендованных к занятию нормативных правовых актов и литературных источников, подготовка к решению практических и ситуационных задач.
Тема 3. Основные виды киберугроз и проблема защиты конечных пользователей	1. Проблемы выявления, идентификации, классификации, оценки угроз информационной безопасности. 2. Проблемы создания, совершенствования и обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. 3. Научно-технические проблемы развития современных информационных технологий, индустрии средств	Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, изучение рекомендованных к занятию нормативных правовых актов, судебной практики и литературных источников, подготовка к решению практических и ситуационных задач.

	информатизации, телекоммуникации и связи. 4. Проблемы защиты личности в ходе трансграничного использования информационных технологий	
Тема 4. Международно-правовое регулирование кибербезопасности	1. Кибербезопасность как компонент международных отношений. 2. Правовые гарантии свободы коммуникации. 3. Закона о кибербезопасности Европейского союза (ЕС). 4. Международные стандарты кибербезопасности. 5. Проблемы обеспечения снижения риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.	Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, изучение рекомендованных к занятию нормативных правовых актов, судебной практики и литературных источников, подготовка к решению практических и ситуационных задач.
Тема 5. Правовое обеспечение кибербезопасности в РФ	1. Проблемы противодействия угрозам и вызовам информационной безопасности личности, общества, государства и международного сообщества. 2. Проблемы развития системы обеспечения кибербезопасности Российской Федерации. 3. Проблемы влияния информационной сферы на конкурентоспособность России на современном этапе. 4. Проблемы оценки информационной безопасности личности, общества и государства. 5. Проблемы развития нормативного правового и нормативного технического обеспечения кибербезопасности	Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, изучение рекомендованных к занятию нормативных правовых актов, судебной практики и литературных источников, подбор материала к групповой дискуссии, подготовка к решению практических и ситуационных задач.

Тема 6. Правовое обеспечение кибербезопасности критической информационной инфраструктуры	1. Критическая информационная инфраструктура России. 2. Проблемы нормативного правового обеспечения устойчивости функционирования и безопасности использования информационных систем и телекоммуникационных сетей, в том числе в составе глобальной информационной инфраструктуры. 3. Проблемы противодействия использованию информационных технологий в террористических целях для оказания деструктивного воздействия на элементы критической информационной инфраструктуры.	Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, работа со справочно-правовыми системами, изучение рекомендованных к занятию нормативных правовых актов, судебной практики, литературных источников.
Тема 7. Правовое обеспечение кибербезопасности конечных пользователей в информационно-телекоммуникационной сети «Интернет»	1. Особенности правового регулирования общественных отношений в сети «Интернет». 2. Государственный сегмент сети «Интернет». 3. Требования к информационным ресурсам в сети «Интернет». 4. Противодействие киберугрозам в социальных сетях	Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, изучение рекомендованных к занятию нормативных правовых актов, судебной практики и литературных источников, подбор материала к групповой дискуссии.
Тема 8. Юридическая ответственность за правонарушения в сфере кибербезопасности	1. Субъекты юридической ответственности за нарушения в информационном пространстве. 2. Уголовная ответственность за киберпреступления. 3. Иные виды юридической ответственности за нарушения в информационном пространстве.	Подготовка ответов на вопросы по теме занятия из рабочей программы дисциплины, работа со справочно-правовыми системами, изучение рекомендованных к занятию нормативных правовых актов, судебной практики, литературных источников.

6.2. Методическое обеспечение для аудиторной и внеаудиторной самостоятельной работы

Перечень примерных тем Контрольной работы:

1. Основные угрозы кибербезопасности, влияющие на темпы роста информационного общества в Российской Федерации.
2. Соотношение кибербезопасности и информационной безопасности.
3. Дискуссионные вопросы определения кибербезопасности.
4. Понятия информационного пространства и киберпространства.

5. Структура, состав и особенности информационного законодательства.

6. Конституционные основы информационного законодательства.

7. Базовый закон информационной сферы.

8. Объекты и субъекты правоотношений в сфере кибербезопасности.

9. Киберпреступность: понятие и виды.

10. Компьютерные атаки и инциденты (кибератаки)

11. Кибертерроризм.

12. Вредоносное программное обеспечение: понятие и виды.

13. Проблемы КиберБулинга.

14. Фишинг и противодействие ему.

15. DDoS – атаки: понятие и противодействие.

16. Международный стандарт ISO/IEC 27032:2012: Основные положения.

17. Будапештская Конвенция Совета Европы по киберпреступлениям ETS 185 от 23 ноября 2001 г.

18. Регламент 2019/881 Об Агентстве ЕС по кибербезопасности (ENISA) и сертификации по кибербезопасности информационных и коммуникационных технологий (Cybersecurity Act) 2019 г.

19. Стратегия развития информационного общества в Российской Федерации об обеспечении кибербезопасности.

20. Проблемы разработки Стратегии кибербезопасности Российской Федерации.

21. Государственные (национальные) стандарты РФ и руководящие документы по кибербезопасности.

22. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

23. Повышение информированности общества в сфере кибербезопасности.

24. Органы, ответственные за обеспечение кибербезопасности критической информационной инфраструктуры.

25. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 : основные требования.

26. Особенности правового регулирования общественных отношений в сети «Интернет».

27. Требования к безопасности информационных ресурсов в сети «Интернет».

28. Правовое регулирование социальных сетей.

29. Защита персональных данных в сети «Интернет»

30. Деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет».

31. Актуальные вопросы ограничения доступа к сайтам в сети «Интернет» с информацией, распространяемой с нарушением законодательства РФ.

32. Понятие киберпреступления и правонарушения в сфере кибербезопасности.

33. Уголовная ответственность за киберпреступления.

34. Административная ответственность за нарушения в области обеспечения кибербезопасности.

Перечень примерных тем для докладов

35. Основные требования, по обеспечению кибербезопасности, предъявляемые государственным информационным ресурсам.

36. Основные препятствия, влияющие на темпы роста информационного общества в Российской Федерации.

37. Динамика разработки правовых актов информационного законодательства и ее обусловленность.

38. Проблематика международного правового противодействия киберугрозам.

39. Сравнительный анализ законодательства по обеспечению кибербезопасности Евросоюза и США.

40. Нормативное регулирование обеспечения кибербезопасности в Сбербанке.

41. Органы публичной власти как субъекты правоотношений по обеспечению кибербезопасности.

42. Конфликты в информационной сфере (споры, конфликты, войны) и формы их разрешения.

43. Кредитные организации как субъекты правоотношений по обеспечению кибербезопасности.

44. Государственные информационные ресурсы во всемирной сети: проблемы обеспечения безопасности.

45. Распространение ненадлежащей информации в сети «Интернет»: применение мер ответственности.

46. Проблемы обеспечения безопасности электронных средств массовой информации.

47. Влияние процесса обеспечения кибербезопасности на ограничение свободы СМИ.

48. Цифровая экономика: проблемы и риски.

49. Защита интеллектуальной собственности в сети «Интернет».

50. Принципы, задачи, функции и стандарты обеспечения информационной безопасности в публичном управлении.

51. Доктрина информационной безопасности: обзор основных особенностей.

52. Стратегия построения Информационного общества: проблемы реализации.

53. Обеспечение безопасности детей в сети «Интернет»

54. Анализ правоприменительной практики ограничения доступа к сайтам в сети «Интернет»

55. Глобальное сетевое управление посредством сети «Интернет».

56. Гармонизация национальных и международных стандартов кибербезопасности.

57. Обеспечение безопасности объектов критической информационной инфраструктуры.

58. Защита пользователей сети «Интернет» от киберугроз.

59. Международное сотрудничество в сфере обеспечения кибербезопасности.

Примеры типовых ситуационных заданий

1. Владелец и создатель информационного ресурса в сети «Интернет» на автомобильную тему на своем сайте разместил ссылку на сбор средств для закупки машин повышенной проходимости для незаконных вооруженных формирований. Законны ли такие действия?

2. В ходе категорирования объекта критической информационной инфраструктуры была допущена ошибка и определена категория ниже требуемой. Является ли данное деяние правонарушением? Если – да, то кто и какому виду ответственности будет привлечен? Какие возможны риски в случае, если по ошибке будет определена категория выше требуемой?

3. В ходе проверки было установлено, что информационная система федерального органа исполнительной власти использует ресурсы европейского провайдера хостинга.

Критерии балльной оценки реализации форм текущего контроля успеваемости

Оценка знаний студентов осуществляется в баллах с учетом оценки работы в семестре (написание контрольной работы, аудиторных и домашних заданий, подготовка докладов и участие в обсуждениях на практических занятиях), оценки итоговых знаний (по результатам зачета) и в соответствии с критериями Финансового университета реализуется следующим образом:

№ п/п	Вид отчетности	Баллы
1.	Работа в семестре	40
2.	Зачёт	60
3.	Итого:	100

Таблица 6 - Формы текущего контроля успеваемости и их балльная оценка

Критерий оценки	Баллы	Методика оценки
Посещение аудиторных занятий	10	Математический расчет: $Оц = Кз \times Кб$ Где Оц – сумма баллов; Кз – количество занятий, посещенных студентом (max 10 занятий); Кб – количество баллов за одно занятие (max 1 балла)
Активность при проведении аудиторных занятий	18	По выбору студента: Доклад, презентация – 3 балла Активное участие в обсуждении – 3 балла

		Решение заданий – 3 балла
Активность при проведении внеаудиторной работы	12	Подготовка материалов и выступление на студенческих научных конференциях, в печатных изданиях, в том числе Университета - 6 баллов

С целью стимулирования систематической подготовки студентов к практическим и семинарским занятиям по дисциплине в течение семестра вводится комплексный подход к оценке, получаемой студентами по итогам изучения дисциплины. На основании положения о системе оценки знаний студентов в Финансовом университете действует 100-балльная система оценки знаний. Это означает, что оценка, получаемая на зачёте, состоит из двух частей: текущего контроля студентов в семестре — максимальная оценка 40 баллов и результатов промежуточной аттестации — максимальная оценка 60 баллов.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения самостоятельных работ. Основными формами текущего контроля знаний являются:

решение тестов, ситуационных задач и их обсуждение с точки зрения умения формулировать выводы, вносить рекомендации и принимать адекватные управленческие решения;

выполнение контрольных заданий и обсуждение результатов.

Вторая составляющая оценивает письменный ответ на зачёте и не может превышать 60 баллов.

40 баллов, полученные студентом в течение семестра, должны означать самую высокую характеристику его работы. Такой балл получают студенты, которые на практических занятиях систематически показывают высокие результаты при опросах, проявляют активность при обсуждении изучаемых проблем, в полном объеме выполняют учебную программу, не имеют пропусков.

Максимальная оценка ответа на зачёте оценивается в 60 баллов. Каждый вопрос в билете имеет свою долю в общей оценке в зависимости от сложности. Теоретический вопрос максимально оценивается в 30 баллов.

Балльная система аттестации:

- студент, получивший от 50 до 100 баллов, считается аттестованным, получивший от 0 до 49 баллов - не аттестованным;

- студент, получивший от 50 до 69 баллов, считается аттестованным на «удовлетворительно»;

- студент, получивший от 70 до 85 баллов, считается аттестованным на «хорошо»;

- студент, получивший от 86 до 100 баллов, считается аттестованным на «отлично».

Таким образом, если студент по итогам работы в семестре набирает 21 балл, а по итогам зачёта — 60 баллов, то общая сумма 81 балл соответствует окончательной оценке 4 «хорошо».

Если студент подошел к зачёту с оценкой 0 баллов, то при безупречном качестве ответов на теоретические вопросы он может получить итоговую оценку по данной дисциплине только 60 баллов.

О данном подходе к оценке знаний студентов преподаватель информирует студентов на первом семинарском (практическом) занятии. На последнем семинарском занятии студентам сообщается оценка, которую они получают по итогам работы в семестре.

Студенты могут улучшить свою оценку по итогам работы в семестре за счет отработки пропущенных занятий или полученных неудовлетворительных оценок на семинарах. Вместе с тем все отработки могут быть осуществлены в консультационные дни в период не более двух консультаций с момента получения оценки «неудовлетворительно» или пропуска занятий. Только в случае болезни студент может отрабатывать пропуски в более поздние сроки.

Отработка пропусков, имевших место по причине работы студентов во время занятий, не допускается.

7. Фонд оценочных средств для проведения промежуточной аттестации

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы:

Перечень компетенций, формируемых в процессе освоения дисциплины, содержится в разделе 2 «Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы».

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Таблица 7 - Типовые контрольные задания, необходимые для оценки индикаторов достижения компетенций

Компетенция	Типовые задания
ПКП-1 Способность использовать фундаментальные знания в области частного права и публичного права в современных условиях и оказывать помощь в реализации правовых норм субъектами гражданского оборота	1. Демонстрирует знания нормативных правовых актов, а также прогнозирует результат экономической деятельности для решения практических задач. Задание. Возможно ли разместить в сети «Интернет» схему водоснабжения города Смоленска? 2. Использует фундаментальные знания в области частного и публичного права в современных условиях. Задание. Охарактеризуйте взаимосвязь процессов обеспечения национальной безопасности с обеспечением информационной безопасности и кибербезопасности. 3. Оказывает помощь в реализации правовых норм субъектами гражданского оборота. Укажите, с какими государственными органами должен взаимодействовать юрист организации, выполняющий указание руководителя по разработке положения о кибербезопасности предприятия.

ПКП-2 Способность действовать с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера, анализировать проблемные ситуации на рынке товаров, работ, услуг, а также выявлять правонарушения при осуществлении предпринимательской деятельности и давать юридически обоснованные предложения по их преодолению и устранению	1. Действует с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера. Задание. Каким образом осуществить взаимодействие в случае обнаружения факта компьютерной атаки на ресурсы субъекта хозяйственной деятельности и как минимизировать причиненный ущерб? 2. Выявляет правонарушения при осуществлении предпринимательской деятельности. Задание. Правомерно ли требование, что индивидуальный предприниматель должен: - иметь круглосуточный выход в сеть «Интернет»; - создать официальный электронный адрес и официальный сайт; - обеспечивать кибербезопасность своих информационных ресурсов. 3. Дает юридически обоснованные предложения по преодолению и устранению правонарушений при осуществлении предпринимательской деятельности. Задание. В ходе проверки было установлено, что информационная система российского банка «РоСаБанк» располагается на ресурсах израильского провайдера хостинга. Является ли выявленный факт правонарушением?
--	--

Перечень вопросов для подготовки к зачету:

1. Понятия Национальная безопасность и Информационная безопасность.
2. Определения киберпространства и кибербезопасности.
3. Необходимость правового регулирования кибербезопасности.
4. Методы обеспечения кибербезопасности.
5. Принципы обеспечения кибербезопасности.
6. Национальная киберинфраструктура.
7. Стратегия развития информационного общества в Российской Федерации.
8. Проблемы формирования понятийного (терминологического) аппарата в области кибербезопасности.
9. Проблемы развития информационной сферы как системообразующего фактора жизни общества.
10. Понятие и виды источников информационного права.
11. Структура, состав и особенности информационного законодательства.
12. Конституционные основы информационного законодательства.
13. Базовый закон информационной сферы.
14. Объекты и субъекты информационных правоотношений.
15. Права и обязанности обладателя информации.
16. Государство как субъект информационных отношений.

17. Правовой статус государственных организаций и учреждений в области обеспечения кибербезопасности.
18. Субъекты кибербезопасности.
19. Киберпреступность.
20. Компьютерные атаки и инциденты.
21. Защита конечных пользователей.
22. Проблемы выявления, идентификации, классификации, оценки угроз информационной безопасности.
23. Научно-технические проблемы развития современных информационных технологий, индустрии средств информатизации, телекоммуникации и связи.
24. Проблемы защиты личности в ходе трансграничного использования информационных технологий.
25. Международные стандарты кибербезопасности.
26. Конвенция о киберпреступности.
27. Cybersecurity Act.
28. Проблемы международно-правового обеспечения кибербезопасности.
29. Кибербезопасность как компонент международных отношений.
30. Правовые гарантии свободы коммуникации.
31. Нормативно правовая база Российской Федерации об обеспечении кибербезопасности.
32. Проблемы разработки Стратегии кибербезопасности Российской Федерации.
33. Государственные (национальные) стандарты РФ и руководящие документы по кибербезопасности.
34. Критерии и методы оценки эффективности систем и средств обеспечения информационной безопасности и кибербезопасности.
35. Мониторинг киберугроз и система реагирования на них
36. Проблемы влияния информационной сферы на конкурентоспособность России на современном этапе.
37. Проблемы оценки информационной безопасности личности, общества и государства.
38. Проблемы развития нормативного правового и нормативного технического обеспечения кибербезопасности.
39. Понятие критической информационной инфраструктуры.
40. Принципы, задачи, функции и стандарты обеспечения безопасности критической информационной инфраструктуры.
41. ГосСОПКА.
42. Полномочия ФСТЭК, ФСБ и иных государственных органов в сфере обеспечения кибербезопасности.
43. Проблемы нормативного правового обеспечения устойчивости функционирования и безопасности использования информационных систем и телекоммуникационных сетей, в том числе в составе глобальной информационной инфраструктуры.

44. Проблемы противодействия использованию информационных технологий в террористических целях для оказания деструктивного воздействия на элементы критической информационной инфраструктуры.

45. Особенности правового регулирования общественных отношений в сети «Интернет».

46. Актуальные вопросы ограничения доступа к сайтам в сети «Интернет» с информацией, распространяемой с нарушением законодательства РФ.

47. Правовой статус организатора распространения информации в сети "Интернет".

48. Регулирование социальных сетей

49. Особенности распространения информации в сети "Интернет".

50. Особенности распространения информации иностранными субъектами.

51. Понятия киберпреступности, киберпреступления и административного правонарушения в сфере кибербезопасности.

52. Уголовная ответственность за киберпреступления.

53. Административная ответственность за правонарушения в сфере кибербезопасности.

Пример билета для проведения зачёта

**Федеральное государственное образовательное бюджетное учреждение
высшего образования**

**«Финансовый университет при Правительстве Российской Федерации»
(Ярославский филиал Финуниверситета)**

Кафедра «Экономика и финансы»

Дисциплина «Правовое обеспечение кибербезопасности»

Филиал Ярославский

Форма обучения Очная

Семестр 7 Направление 40.03.01 «Юриспруденция», профиль «Экономическое право»

БИЛЕТ ДЛЯ ЗАЧЁТА № 1

№ п/п	Вопросы билета	Максимальный балл
1	Особенности распространения информации иностранными субъектами.	30 баллов
2	Понятия киберпреступности, киберпреступления и административного правонарушения в сфере кибербезопасности.	30 баллов

Подготовил

(подпись и ФИО преподавателя)

Утверждаю:

Заведующий кафедрой

«Экономика и финансы»

Сироткин С.А.

Дата _____ 20__ г.

7.3. Соответствующие приказы, распоряжения ректората о контроле уровня освоения дисциплин и сформированности компетенций студентов

Приказ от 01 октября 2024 года №2187/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации студентов, обучающихся по образовательным программам высшего образования в Финансовом университете», размещенный по ссылке: https://www.fa.ru/upload/iblock/845/yqw4vi0gi21glvu9775bfm4rz6p19b0z/Prikaz-2187_o-ot-01.10.2024.pdf

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

А). Нормативные правовые акты

1. Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 (в действ. ред.).
2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ (в действ. ред.).
3. Федеральный закона "О персональных данных" от 27.07.2006 № 152-ФЗ (в действ. ред.).
4. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (в действ. ред.).
5. Приказ ФСТЭК России от 25.12.2017 N 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" (в действ. ред.).
6. Федеральный закон от 28.12.2010 N 390-ФЗ "О безопасности» (в действ. ред.).
7. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"
8. Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" (в действ. ред.).
9. УК РФ (в действ. ред.).
10. КоАП РФ (в действ. ред.).

Б). Основная литература

11. Информационное право : учебник для вузов / М. А. Федотов [и др.]; под редакцией М. А. Федотова. — Москва: Юрайт, 2021. — 497 с. — (Высшее образование).— Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/469790> (дата обращения: 17.10.2022). — Текст: электронный.
12. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху: монография / О. А. Степанов. — Москва : Юрайт, 2022. — 103 с. — (Актуальные монографии). — ISBN 978-5-534-12775-1. Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496448> (дата обращения: 17.10.2022).— Текст: электронный
13. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А.

Поляковой, А. А. Стрельцова. — Москва: Юрайт, 2022. — 325 с. — (Высшее образование). — Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/498844> (дата обращения: 17.10.2022). — Текст: электронный.

В). Дополнительная литература

14. Актуальные проблемы информационного права : учебник / РАН, Ин-т государства и права ; под ред. И. Л. Бачило, М. А. Лапиной. - Москва: Юстиция, 2016. - 534 с.— Текст: непосредственный. Актуальные проблемы информационного права: учебник / под ред. И. Л. Бачило, М. А. Лапиной. — Москва: Юстиция, 2020. — 592 с. — (магистратура, аспирантура). — ЭБС BOOK.ru. - URL: <https://book.ru/book/935207> (дата обращения: 17.10.2022)

15. Жарова, А. К. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации: монография / А. К. Жарова. — Москва : Юрайт, 2022. — 301 с. — (Актуальные монографии). — Текст : электронный—Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496939> (дата обращения: 17.10.2022).

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Официальный интернет-портал правовой информации. Государственная система правовой информации: <http://www.pravo.gov.ru>
2. Официальный сайт Совета Безопасности РФ <http://www.scrf.gov.ru/security/information/>
3. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
4. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
5. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
6. Электронно-библиотечная система Znanium <http://www.znaniy.com>
7. Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>
8. Электронно-библиотечная система издательства Проспект <http://ebs.prospekt.org/books>
9. Электронно-библиотечная система издательства «Лань» <https://e.lanbook.com/>
10. Электронная библиотека Издательского дома «Гребенников» <https://grebennikon.ru/>
11. Деловая онлайн-библиотека Alpina Digital <https://finunivers.alpinadigital.ru/>
12. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
13. Национальная электронная библиотека <http://нэб.рф/>
14. Справочно-правовая система "КонсультантПлюс". <http://www.library.fa.ru/resource.asp?id=351>
15. Справочно-правовая система по законодательству Российской Федерации "ГАРАНТ" <http://www.library.fa.ru/resource.asp?id=350>

10. Методические указания для обучающихся по освоению дисциплины.

Наименование методических материалов для обучающихся	Год утверждения	Местонахождение материала (ссылка на сайт филиала)
Девятковская И.А. Методические	2025	https://cloud.mail.ru/public/CnoV/

рекомендации по выполнению контрольной работы по дисциплине «Правовое обеспечение кибербезопасности» для студентов, обучающихся по направлению подготовки 40.03.01 «Юриспруденция», профиль «Экономическое право»		сYBRvyAHR
Приказ Финуниверситета от 14.05.2021 № 1040/о «Об утверждении методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры Финансовом университете»		https://www.fa.ru/upload/iblock/dc2/a5qpi6qb0k0l6jz01c4g9y1cv5x35ey3/Prikaz_-1040_o-ot-11.05.2021.PDF

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

11.1. Комплект лицензионного программного обеспечения:

1. Компьютерные программы общего назначения Windows, MicrosoftOffice
2. Антивирусная программа.

11.2. Современные профессиональные базы данных и информационные справочные системы:

Таблица 8 – Используемые профессиональные базы данных и информационные справочные системы

№п/п	Название рекомендуемых технических и компьютерных средств обучения	Наименование разделов и тем
1	Правовая база данных «КонсультантПлюс»	Все темы
2	Справочно-правовая система «Гарант»	Все темы

11.3. Сертифицированные программные и аппаратные средства защиты информации: не предусмотрены.

11.4. Доступ к электронно-библиотечным системам:

При освоении дисциплины каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде Финансового университета. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность доступа обучающегося из любой точки, в которой имеется доступ к

информационно-телекоммуникационной сети «Интернет», как на территории филиала, так и вне ее.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения учебных занятий, предусмотренных программой бакалавриата, оснащённая оборудованием и техническими средствами обучения

Специализированная мебель:

Стол студенческий двухместный— 12 шт.

Стулья студенческие— 24 шт.

Стол (учительский) – 2 шт.

Стул (учительский) — 1 шт.

Доска (меловая) — 1 шт.

Трибуна напольная – 1шт.

Технические средства обучения:

Интерактивная панель со встроенным компьютером - 1 шт.

Подключение к сети «Интернет» и обеспечение доступа к электронной информационно-образовательной среде Финансового университета

Специализированная аудитория, оборудованная для проведения занятий по информационным технологиям, оснащённая оборудованием и техническими средствами обучения

Специализированная мебель:

Стол студенческий двухместный— 12 шт.

Стулья студенческие— 12 шт.

Стол (учительский) – 1 шт.

Стул (учительский) — 1 шт.

Доска (меловая) — 1 шт.

Технические средства обучения:

Мультимедиа-проектор со встроенными колонками - 1 шт.

Экран — 1 шт.

Компьютер преподавателя — 1 шт.

Компьютер ученика — 12 шт.

Помещение для самостоятельной работы

Читальный зал библиотеки

Специализированная мебель:

Стол студенческий одноместный – 10 шт.
Стулья – 10 шт.
Кресла – 7 шт.
Стол большой – 1 шт.
Диван – 1 шт.
Кресла мягкие – 7 шт.
Пуфы – 6 шт.

Технические средства обучения:

Интерактивная панель со встроенными колонками - 1 шт.
Компьютер ученика — 11 шт.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде Финансового университета

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья. При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки России (утверждены 08.04.2014 № АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на

контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.