

**МИНОБРНАУКИ РОССИИ**



Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
**«Российский государственный гуманитарный университет»  
(ФГБОУ ВО «РГГУ»)**

**ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ**  
Кафедра информационной безопасности

**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В  
ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Специальность 45.05.01 Перевод и переводоведение  
Специализация: Лингвистическое обеспечение межгосударственных отношений

Форма обучения очная

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2020

Основы информационной безопасности в профессиональной деятельности  
Рабочая программа дисциплины

Составитель:

Кандидат технических наук, доцент, доцент, Н.В.Гришина

Ответственный редактор

канд. ист. наук, доц., зав.кафедрой ИБ Г.А. Шевцова

УТВЕРЖДЕНО

Протокол заседания кафедры

Информационной безопасности

№ 1 от 29.08.2020

## **ОГЛАВЛЕНИЕ**

### **1. Пояснительная записка**

1.1 Цель и задачи дисциплины

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине

1.3. Место дисциплины в структуре образовательной программы

### **2. Структура дисциплины**

### **3. Содержание дисциплины**

### **4. Образовательные технологии**

### **5. Оценка планируемых результатов обучения**

5.1. Система оценивания

5.2. Критерии выставления оценок

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

### **6. Учебно-методическое и информационное обеспечение дисциплины**

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

### **7. Материально-техническое обеспечение дисциплины**

### **8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов**

### **9. Методические материалы**

9.1. Планы семинарских занятий

## **Приложения**

Приложение 1. Аннотация дисциплины

Приложение 2. Лист изменений

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

Цель дисциплины - формирование знаний об основных принципах, методах и направлениях обеспечения информационной безопасности в профессиональной деятельности.

Задачи дисциплины:

- раскрытие базовых содержательных положений в области информационной безопасности и защиты информации;
- определение целей и принципов и методов защиты информации.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Коды компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОПК -1		
ОПК -2	способность соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности	Знать: основные понятия в области информационной безопасности и защиты информации. Уметь: соблюдать в профессиональной деятельности требования по информационной безопасности. Владеть: методами обеспечения режима секретности.

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности в профессиональной деятельности» относится к базовой части блока дисциплин учебного плана.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения дисциплины «Информатика и информационные технологии в лингвистике».

## 2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 ч., в том числе контактная работа обучающихся с преподавателем 42 ч., самостоятельная работа обучающихся 48 ч., промежуточная аттестация 18ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная							
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация			
1	Введение. Предмет, задачи и содержание курса	I	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы	
2	Значение обеспечения информационной безопасности	I	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы	
3	Сущность и понятие защиты информации	I	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы	
4	Критерии, условия и принципы отнесения информации к защищаемой	I	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы	
5	Объекты защиты информации	I	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы	
6	Классификация конфиденциальной информации по видам тайны	I	4	4				8	Заслушивание сообщений, дискуссия, ответы на вопросы	
7	Понятие и структура угроз защищаемой информации	I	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы	
8	Источники, причины обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию	I	2	2				8	Заслушивание сообщений, дискуссия, ответы на вопросы	

<b>9</b>	Классификация видов, методов и средств защиты информации	<i>1</i>	4	2				8	Заслушивание сообщений, дискуссия, ответы на вопросы
	Экзамен						18		экзамен по билетам
	<b>Итого:</b>	<b>108</b>	<b>22</b>	<b>20</b>			<b>18</b>	<b>48</b>	

### **3. Содержание дисциплины**

#### **ТЕМА 1. ВВЕДЕНИЕ. ПРЕДМЕТ, ЗАДАЧИ И СОДЕРЖАНИЕ КУРСА**

Основные понятия и термины дисциплины. Предмет и задачи курса. Значение и место курса в подготовке специалистов по лингвистическому обеспечению межгосударственных отношений. Становление и развитие понятия «информационная безопасность». Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества.

#### **ТЕМА 2. ЗНАЧЕНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**

Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации.

Понятие и современная концепция национальной безопасности. Место информационной безопасности в системе национальной безопасности.

Понятие и назначение доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере.

#### **ТЕМА 3. СУЩНОСТЬ И ПОНЯТИЕ ЗАЩИТЫ ИНФОРМАЦИИ.**

Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации. Понятие «утечка информации». Соотношение форм и видов уязвимости информации. Понятие «защита информации». Существующие подходы к определению целей защиты информации.

Значение защиты информации для субъектов информационных отношений государства, общества, личности. Значение защиты информации в политической, военной, экономической и других областях деятельности.

#### **ТЕМА 4. КРИТЕРИИ, УСЛОВИЯ И ПРИНЦИПЫ ОТНЕСЕНИЯ ИНФОРМАЦИИ К ЗАЩИЩАЕМОЙ**

Основания для отнесения информации к защищаемой, категории информации, подпадающие под это. Понятия «конфиденциальная информация», «секретная информация», «открытая информация», параметры их защиты. Понятие защищаемой информации.

Критерии отнесения открытой информации к защищаемой, их обусловленность необходимостью защиты информации от утраты. Критерии отнесения конфиденциальной информации к защищаемой, их обусловленность необходимостью защиты информации от утраты и утечки.

Условия, необходимые для отнесения информации к защищаемой.

Правовые и организационные принципы отнесения информации к защищаемой.

#### **ТЕМА 5. ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ**

Понятие объекта защиты. Понятие «носитель защищаемой информации». Соотношение между носителем и источником информации. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты. Состав объектов хранения письменных и видовых носителей информации, подлежащих защите.

Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации.

Виды и способы дестабилизирующего воздействия на объекты защиты.

## ТЕМА 6. КЛАССИФИКАЦИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПО ВИДАМ ТАЙНЫ

Понятие «тайна информации». Виды тайны конфиденциальной информации. Показатели разделения конфиденциальной информации на виды тайны.

Становление и современное определение понятия «государственная тайна». Основания и организационно-правовые формы отнесения информации к государственной тайне.

Определение коммерческой тайны. Место коммерческой тайны в системе предпринимательской деятельности. Основания и методика отнесения сведений к коммерческой тайне. Функции государства в сфере защиты коммерческой тайны.

Понятия «личная тайна» и «персональные данные». Категории информации, отнесенной к персональным данным. Разновидности личной тайны. Функции государства и граждан в сфере защиты личной тайны и персональных данных.

Понятие и особенности профессиональной тайны. Сфера действия профессиональной тайны. Соотношение между профессиональной и другими видами тайны. Разновидности профессиональной тайны.

## ТЕМА 7. ПОНЯТИЕ И СТРУКТУРА УГРОЗ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации.

Структура явлений как существенных проявлений угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

## ТЕМА 8. ИСТОЧНИКИ, ПРИЧИНЫ ОБСТОЯТЕЛЬСТВА И УСЛОВИЯ ДЕСТАБИЛИЗИРУЮЩЕГО ВОЗДЕЙСТВИЯ НА ЗАЩИЩАЕМУЮ ИНФОРМАЦИЮ

Источники дестабилизирующего воздействия на защищаемую информацию как определяющая структурная часть угрозы. Состав и характеристика источников дестабилизирующего воздействия на информацию.

Виды и способы дестабилизирующего воздействия на информацию со стороны различных источников. Соотношение видов дестабилизирующего воздействия на защищаемую информацию с формами проявления уязвимости информации.

Соотношение между причинами, обстоятельствами и условиями дестабилизирующего воздействия на информацию, их обусловленность источниками и видами воздействия.

Причины, вызывающие преднамеренное и непреднамеренное дестабилизирующее воздействие на информацию со стороны людей. Обстоятельства (предпосылки), способствующие появлению этих причин. Условия, создающие возможность для дестабилизирующего воздействия на информацию.

Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны других источников воздействия.

Канал несанкционированного доступа к конфиденциальной информации как составная часть угрозы информации.

## ТЕМА 9. КЛАССИФИКАЦИЯ ВИДОВ, МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Виды защиты информации, сферы их действия.

Классификация методов защиты информации. Универсальные методы защиты информации, область их применения. Области применения организационных, криптографических и инженерно-технических методов защиты информации.

Понятие и классификация средств защиты информации. Назначение программных, криптографических и технических средств защиты.

### 4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Введение. Предмет, задачи и содержание курса	Лекция 1 Семинар 1	Вводная лекция с использованием видеоматериалов Дискуссия Консультирование и проверка домашних заданий посредством электронной почты
2	Значение обеспечения информационной безопасности	Лекция 2. Семинар 2	Проблемная лекция Консультирование и проверка домашних заданий посредством

			электронной почты
3	Сущность и понятие защиты информации	Лекция 3. Семинар 3	Лекция с разбором конкретных ситуаций Консультирование и проверка домашних заданий посредством электронной почты
4	Критерии, условия и принципы отнесения информации к защищаемой	Лекция 4. Семинар 4.	Проблемная лекция Консультирование и проверка домашних заданий посредством электронной почты
5	Объекты защиты информации	Лекция 5. Семинар5	Проблемная лекция Консультирование и проверка домашних заданий посредством электронной почты
6	Классификация конфиденциальной информации по видам тайны	Лекция 6. Семинар 6	Лекция с разбором конкретных ситуаций Консультирование и проверка домашних заданий посредством электронной почты
7	Понятие и структура угроз защищаемой информации	Лекция 7. Семинар 7.	Проблемная лекция Консультирование и проверка домашних заданий посредством электронной почты
8	Источники, причины обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию	Лекция 8. Семинар 8	Проблемная лекция Консультирование и проверка домашних заданий посредством электронной почты
9	Классификация видов, методов и средств защиты информации	Лекция 9. Семинар 9	Проблемная лекция Консультирование и проверка домашних заданий посредством электронной почты

## 5. Оценка планируемых результатов обучения

### 5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль: - подготовка сообщения - ответы на вопросы на семинаре - участие в дискуссии (темы 1-9)	15 баллов 2 балла 3 баллов	15 баллов 18 баллов 27 баллов
Промежуточная аттестация экзамен		40 баллов
<b>Итого за семестр</b>		<b>100 баллов</b>

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

## 5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A, B	«отлично»/ «зачтено (отлично)»/ «зачтено»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		<p>обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	«неудовлетворительно»/ не зачтено	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

**Примерные темы сообщений:**

1. Виды и состав угроз информационной безопасности.
2. Задачи, принципы и методы обеспечения информационной безопасности.

3. Понятие, сущность, цели и значение защиты информации.
4. Критерии, условия, принципы и формы отнесения информации к защищаемой.
5. Информационные войны и информационное оружие.
6. Анализ существующих подходов к классификации конфиденциальной информации по видам тайны.
7. Виды и характеристика носителей защищаемой информации.
8. Структура и характеристика угроз защищаемой информации.
9. Соотношение угроз защищаемой информации с видами носителей и формами проявления уязвимости информации.
10. Соотношение видов разведывательной деятельности с каналами и методами несанкционированного доступа к конфиденциальной информации.
11. Классификация и характеристика объектов защиты информации.
12. Классификация и характеристика видов, методов и средств защиты информации и их соотношение с объектами защиты.
13. Сущность, назначение и структура систем защиты информации.
14. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность».
15. Общее и различия между видами тайны.
16. Соотношение угроз безопасности информации с источниками и видами уязвимости информации.
17. Соотношение видов и способов дестабилизирующего воздействия на информацию с каналами и методами несанкционированного доступа к конфиденциальной информации.
18. Организация защиты коммерческой тайны.
19. Организация защиты государственной тайны.
20. Организация защиты персональных данных.
21. Методы аналитической разведки.
22. Использование криптографических методов защиты информации.
23. Наказания за нарушение требований по защите конфиденциальной информации.

#### **Перечень вопросов к экзамену:**

1. Становление и развитие понятия «информационная безопасность».
2. Связь информационной безопасности с информатизацией общества.
3. Сущность информационной безопасности. Объекты информационной безопасности.

4. Значение информационной безопасности для субъектов информационных отношений.
5. Связь между информационной безопасностью и безопасностью информации.
6. Понятие и назначение доктрины информационной безопасности.
7. Интересы личности, общества и государства в информационной сфере.
8. Понятие уязвимости информации. Формы проявления уязвимости информации.
9. Виды уязвимости информации. Соотношение форм и видов уязвимости информации.
10. Понятие “защита информации”. Существующие подходы к определению целей защиты информации.
11. Значение защиты информации для субъектов информационных отношений государства, общества, личности.
12. Значение защиты информации в политической, военной, экономической и других областях деятельности.
13. Основа для отнесения информации к защищаемой, категории информации, подпадающие под эту основу.
14. Понятия «конфиденциальная информация», «секретная информация», «открытая информация», параметры их защиты. Понятие защищаемой информации.
15. Критерии отнесения открытой информации к защищаемой, их обусловленность необходимостью защиты информации от утраты.
16. Критерии отнесения конфиденциальной информации к защищаемой, их обусловленность необходимостью защиты информации от утраты и утечки.
17. Правовые и организационные принципы отнесения информации к защищаемой.
18. Понятие «носитель защищаемой информации».
19. Особенности отдельных видов носителей как объектов защиты.
20. Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации.
21. Виды и способы дестабилизирующего воздействия на объекты защиты.
22. Понятие «тайна информации». Виды тайны конфиденциальной информации. Показатели разделения конфиденциальной информации на виды тайны.
23. Определение понятия «государственная тайна». Основания и организационно-правовые формы отнесения информации к государственной тайне.
24. Определение коммерческой тайны. Основания и методика отнесения сведений к коммерческой тайне.

25. Понятия «личная тайна» и «персональные данные». Категории информации, отнесенной к персональным данным.
26. Понятие и особенности профессиональной тайны. Соотношение между профессиональной и другими видами тайны.
27. Подходы к понятию угрозы защищаемой информации. Признаки и составляющие угрозы: явления, факторы, условия.
28. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.
29. Источники дестабилизирующего воздействия на защищаемую информацию как определяющая структурная часть угрозы.
30. Состав и характеристика источников дестабилизирующего воздействия на информацию.
31. Виды и способы дестабилизирующего воздействия на информацию со стороны различных источников.
32. Соотношение между причинами, обстоятельствами и условиями дестабилизирующего воздействия на информацию, их обусловленность источниками и видами воздействия.
33. Причины, вызывающие преднамеренное и непреднамеренное дестабилизирующее воздействие на информацию со стороны людей.
34. Условия, создающие возможность для дестабилизирующего воздействия на информацию.
35. Канал несанкционированного доступа к конфиденциальной информации как составная часть угрозы информации.
36. Виды защиты информации, сферы их действия.
37. Классификация методов защиты информации.
38. Понятие и классификация средств защиты информации. Назначение программных, криптографических и технических средств защиты.

## **6. Учебно-методическое и информационное обеспечение дисциплины**

### **6.1. Список источников и литературы**

Источники:

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/)

2. Федеральный закон РФ «О коммерческой тайне» от 29 июля 2004 года №98-ФЗ, Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_48699/](http://www.consultant.ru/document/cons_doc_LAW_48699/)
3. Закон РФ от 21.07.1993 N 5485-I «О государственной тайне», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_2481/](http://www.consultant.ru/document/cons_doc_LAW_2481/)

Литература:

Основная:

1. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/612572>
2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — [www.dx.doi.org/10.12737/11380](http://www.dx.doi.org/10.12737/11380). - Режим доступа: <http://znanium.com/catalog/product/1009606>

Дополнительная:

3. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 120 с. - ISBN 978-5-9275-2742-7. - Режим доступа: <http://znanium.com/catalog/product/1021744>
- 6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».
1. Материалы сайта «Нормативные документы» – <http://www.consultant.ru/>
2. Журнал «Защита информации. Инсайд»: журнал посвящен вопросам безопасности и защиты информации. <http://www.inside-zi.ru/>

## 7. Материально-техническое обеспечение дисциплины/модуля

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен

### Перечень ПО

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

#### Перечень БД и ИСС

№п /п	Наименование
1	Компьютерные справочные правовые системы Консультант Плюс, Гарант

### 8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:
  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
  - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
  - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
  - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
  - письменные задания оформляются увеличенным шрифтом;
  - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих:
  - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
  - письменные задания выполняются на компьютере в письменной форме;
  - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата:
  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
  - письменные задания выполняются на компьютере со специализированным программным обеспечением;
  - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными

особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
  - в печатной форме увеличенным шрифтом;
  - в форме электронного документа;
  - в форме аудиофайла.
- для глухих и слабослышащих:
  - в печатной форме;
  - в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - в печатной форме;
  - в форме электронного документа;
  - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
  - устройством для сканирования и чтения с камерой SARA CE;
  - дисплеем Брайля PAC Mate 20;
  - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
  - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - передвижными, регулируемые эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

## **9. Методические материалы**

### **9.1. Планы семинарских занятий**

#### **Занятие 1.**

Тема 1(2ч.) ВВЕДЕНИЕ. ПРЕДМЕТ, ЗАДАЧИ И СОДЕРЖАНИЕ КУРСА

Вопросы для обсуждения:

- 1.Значение дисциплины «Основы информационной безопасности в профессиональной деятельности» для подготовки кадров по лингвистическому обеспечению межгосударственных отношений.
2. Становление и развитие понятия «информационная безопасность».
- 3.Сущность информационной безопасности. Объекты информационной безопасности.
- 4.Связь информационной безопасности с информатизацией общества.

Занятие проводится в форме непрерывного диалога между преподавателем и студентами, в ходе которого студенты отвечают на поставленные вопросы. В процессе

занятия возможны выступления студентов с заранее подготовленными сообщениями, раскрывающими в том или ином аспекте тематику занятия.

Список литературы:

1. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/612572>
2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — [www.dx.doi.org/10.12737/11380](http://www.dx.doi.org/10.12737/11380). - Режим доступа: <http://znanium.com/catalog/product/1009606>

### **Занятие 2.**

Тема 2(2 ч.) ЗНАЧЕНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Вопросы для обсуждения:

- 1.Значение информационной безопасности для субъектов информационных отношений.
- 2.Связь между информационной безопасностью и безопасностью информации.
- 3.Понятие и современная концепция национальной безопасности. Место информационной безопасности в системе национальной безопасности.
- 4.Понятие и назначение доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере.

Занятие проводится в форме обсуждения подготовленных сообщений по вопросам темы. Обсуждение сообщений дополняется проведением дискуссии в форме ответов на поставленные вопросы.

Список литературы:

1. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/612572>
2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — [www.dx.doi.org/10.12737/11380](http://www.dx.doi.org/10.12737/11380). - Режим доступа: <http://znanium.com/catalog/product/1009606>

### **Занятие 3.**

Тема 2(2 ч.) СУЩНОСТЬ И ПОНЯТИЕ ЗАЩИТЫ ИНФОРМАЦИИ.

Вопросы для обсуждения:

- 1.Понятие уязвимости информации. Формы проявления уязвимости информации.
- 2.Виды уязвимости информации. Понятие “утечка информации”.

3.Соотношение форм и видов уязвимости информации.

4.Понятие “защита информации”. Существующие подходы к определению целей защиты информации.

Значение защиты информации для субъектов информационных отношений государства, общества, личности. Значение защиты информации в политической, военной, экономической и других областях деятельности.

Занятие проводится в форме обсуждения подготовленных сообщений по вопросам темы. Обсуждение сообщений дополняется проведением дискуссии в форме ответов на поставленные вопросы.

Список литературы:

1.Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/612572>

2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — [www.dx.doi.org/10.12737/11380](http://www.dx.doi.org/10.12737/11380). - Режим доступа: <http://znanium.com/catalog/product/1009606>

#### **Занятие 4.**

Тема 2(2 ч.) КРИТЕРИИ, УСЛОВИЯ И ПРИНЦИПЫ ОТНЕСЕНИЯ ИНФОРМАЦИИ К ЗАЩИЩАЕМОЙ.

Вопросы для обсуждения:

1.Основания для отнесения информации к защищаемой, категории информации, подпадающие под это.

2.Понятия «конфиденциальная информация», «секретная информация», «открытая информация», параметры их защиты. Понятие защищаемой информации.

3.Критерии отнесения открытой информации к защищаемой.

4.Критерии отнесения конфиденциальной информации к защищаемой. Условия, необходимые для отнесения информации к защищаемой.

Занятие проводится в форме обсуждения подготовленных сообщений по вопросам темы. Обсуждение сообщений дополняется проведением дискуссии в форме ответов на поставленные вопросы.

Список литературы:

1.Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/612572>

2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — [www.dx.doi.org/10.12737/11380](http://www.dx.doi.org/10.12737/11380). - Режим доступа: <http://znanium.com/catalog/product/1009606>

### **Занятие 5.**

Тема 2(2 ч.) ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ.

Вопросы для обсуждения:

1. Понятие объекта защиты. Понятие «носитель защищаемой информации».
2. Соотношение между носителем и источником информации. Носители информации как конечные объекты защиты.
3. Особенности отдельных видов носителей как объектов защиты. Состав объектов хранения письменных и видовых носителей информации, подлежащих защите.
4. Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации.
5. Виды и способы дестабилизирующего воздействия на объекты защиты.

Занятие проводится в форме обсуждения подготовленных сообщений по вопросам темы. Обсуждение сообщений дополняется проведением дискуссии в форме ответов на поставленные вопросы.

Список литературы:

1. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/612572>
2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — [www.dx.doi.org/10.12737/11380](http://www.dx.doi.org/10.12737/11380). - Режим доступа: <http://znanium.com/catalog/product/1009606>

### **Занятие 6.**

Тема 2(4 ч.) КЛАССИФИКАЦИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПО ВИДАМ ТАЙНЫ.

Вопросы для обсуждения:

1. Понятие «тайна информации». Виды тайны конфиденциальной информации.
2. Показатели разделения конфиденциальной информации на виды тайны.
3. Становление и современное определение понятия «государственная тайна».
4. Основания и организационно-правовые формы отнесения информации к государственной тайне.

5.Определение коммерческой тайны. Методика отнесения сведений к коммерческой тайне.

6.Понятия «личная тайна» и «персональные данные».

7.Понятие и особенности профессиональной тайны.

Занятие проводится в форме обсуждения подготовленных сообщений по вопросам темы. Обсуждение сообщений дополняется проведением дискуссии в форме ответов на поставленные вопросы.

Список литературы:

1.Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/612572>

2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — [www.dx.doi.org/10.12737/11380](http://www.dx.doi.org/10.12737/11380). - Режим доступа: <http://znanium.com/catalog/product/1009606>

### **Занятие 7.**

Тема 2(2 ч.) ПОНЯТИЕ И СТРУКТУРА УГРОЗ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ.

Вопросы для обсуждения:

1.Подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации.

2. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации.

3.Структура явлений как сущностных проявлений угрозы защищаемой информации.

4.Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

Занятие проводится в форме обсуждения подготовленных сообщений по вопросам темы. Обсуждение сообщений дополняется проведением дискуссии в форме ответов на поставленные вопросы.

Список литературы:

1.Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/612572>

2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 322 с. —

(Высшее образование). — [www.dx.doi.org/10.12737/11380](http://www.dx.doi.org/10.12737/11380). - Режим доступа: <http://znanium.com/catalog/product/1009606>

### **Занятие 8.**

Тема 2(2 ч.) ИСТОЧНИКИ, ПРИЧИНЫ ОБСТОЯТЕЛЬСТВА И УСЛОВИЯ ДЕСТАБИЛИЗИРУЮЩЕГО ВОЗДЕЙСТВИЯ НА ЗАЩИЩАЕМУЮ ИНФОРМАЦИЮ.

Вопросы для обсуждения:

1. Источники дестабилизирующего воздействия на защищаемую информацию как определяющая структурная часть угрозы.
2. Виды и способы дестабилизирующего воздействия на информацию со стороны различных источников.
3. Соотношение между причинами, обстоятельствами и условиями дестабилизирующего воздействия на информацию.
4. Условия, создающие возможность для дестабилизирующего воздействия на информацию.
5. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны других источников воздействия.

Занятие проводится в форме обсуждения подготовленных сообщений по вопросам темы. Обсуждение сообщений дополняется проведением дискуссии в форме ответов на поставленные вопросы.

Список литературы:

1. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/612572>
2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — [www.dx.doi.org/10.12737/11380](http://www.dx.doi.org/10.12737/11380). - Режим доступа: <http://znanium.com/catalog/product/1009606>

### **Занятие 9.**

Тема 2(2 ч.) КЛАССИФИКАЦИЯ ВИДОВ, МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Вопросы для обсуждения:

1. Виды защиты информации, сферы их действия.
2. Классификация методов защиты информации. Универсальные методы защиты информации, область их применения.

3.Области применения организационных, криптографических и инженерно-технических методов защиты информации.

4.Понятие и классификация средств защиты информации. Назначение программных, криптографических и технических средств защиты.

Занятие проводится в форме обсуждения подготовленных сообщений по вопросам темы. Обсуждение сообщений дополняется проведением дискуссии в форме ответов на поставленные вопросы.

Список литературы:

- 1.Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/612572>
2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — [www.dx.doi.org/10.12737/11380](http://www.dx.doi.org/10.12737/11380). - Режим доступа: <http://znanium.com/catalog/product/1009606>

## АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Основы информационной безопасности в профессиональной деятельности» реализуется кафедрой Информационной безопасности для студентов 1 курса, относится к базовой части блока дисциплин учебного плана.

Цель дисциплины - формирование знаний об основных принципах, методах и направлениях обеспечения информационной безопасности в профессиональной деятельности.

Задачи дисциплины:

- раскрытие базовых содержательных положений в области информационной безопасности и защиты информации;
- определение целей и принципов и методов защиты информации.

Дисциплина направлена на формирование следующих компетенций:

ОПК -2 способность соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Дисциплина «Основы информационной безопасности в профессиональной деятельности» изучается в 1 семестре, предназначается для студентов 1 курса Специальность 45.05.01 «Перевод и переводоведение» специализация: Лингвистическое обеспечение межгосударственных отношений

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы.

**ЛИСТ ИЗМЕНЕНИЙ**

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	<i>Обновлена основная и дополнительная литература</i>	21.06.2017	<b>6</b>
2	Приложение №1		
3	<i>Обновлена основная и дополнительная литература</i>	20.06.2018	<b>6</b>
4	Приложение №2		
5	<i>Обновлена основная и дополнительная литература</i>	22.06.2019	<b>6</b>
6	Приложение №3		
7	<i>Обновлены структура дисциплины, образовательные технологии, основная и дополнительная литература</i>	26.06.2020	<b>6</b>
8	Приложение №4		

**Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2017 г.)**

**1. Перечень ПО**

Таблица 1

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
5	Archicad 19 Rus Student	Graphisoft	свободно распространяемое
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Kaspersky Endpoint Security	Kaspersky	лицензионное

*\* Оставить используемое ПО в рамках учебной дисциплины*

**2. Перечень БД и ИСС**

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

**Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2018 г.)**

**1. Перечень ПО**

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

*\* Оставить используемое ПО в рамках учебной дисциплины*

**2. Перечень БД и ИСС**

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

**Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)**

**1. Перечень ПО**

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

**2. Перечень БД и ИСС**

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

## 1. Структура дисциплины (к п. 2 РПД на 2020 )

## Структура дисциплины (модуля) для очной формы обучения

Общая трудоёмкость дисциплины составляет 3 з.е., 114 ч., в том числе контактная работа обучающихся с преподавателем 42 ч., самостоятельная работа обучающихся 54 ч., промежуточная аттестация 18ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Введение. Предмет, задачи и содержание курса	1	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы
2	Значение обеспечения информационной безопасности	1	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы
3	Сущность и понятие защиты информации	1	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы
4	Критерии, условия и принципы отнесения информации к защищаемой	1	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы
5	Объекты защиты информации	1	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы
6	Классификация конфиденциальной информации по видам тайны	1	4	4				8	Заслушивание сообщений, дискуссия, ответы на вопросы
7	Понятие и структура угроз защищаемой информации	1	2	2				4	Заслушивание сообщений, дискуссия, ответы на вопросы
8	Источники, причины обстоятельства и условия дестабилизирующего воздействия на	1	2	2				8	Заслушивание сообщений, дискуссия, ответы на вопросы

	защищаемую информацию								
<b>9</b>	Классификация видов, методов и средств защиты информации	<i>1</i>	4	2				8	Заслушивание сообщений, дискуссия, ответы на вопросы
	Экзамен						18	6	экзамен по билетам
	<b>Итого:</b>	<b>114</b>	<b>22</b>	<b>20</b>			<b>18</b>	<b>54</b>	

## 2. Образовательные технологии (к п.4 на 2020 г.)

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

## 3. Перечень БД и ИСС (к п. 6.2 на 2020 г.)

№п /п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

## 4. Состав программного обеспечения (ПО) (к п. 7 на 2020 г.)

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное

8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное