

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

К.т.н., доцент, доцент, Н.В.Гришина

## **ОГЛАВЛЕНИЕ**

### **1. Пояснительная записка**

1.1 Цель и задачи дисциплины

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

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**

### **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 - изучение теоретических и прикладных вопросов информационной безопасности и использование их в сфере лингвистического обеспечения межгосударственных отношений.

Задачи дисциплины:

- освоить терминологию и понятийный аппарат в области информационной безопасности и защиты информации;
- изучить нормативно-правовую базу, регулирующую сферу информационной безопасности и защиты информации;
- изучить основные средства и методы обеспечения информационной безопасности;
- научиться применять полученные знания и навыки по информационной безопасности и защите информации в сфере лингвистического обеспечения межгосударственных отношений.

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций  
ОПК-3.2; ОПК-4.1; ОПК-4.2

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

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Перечень планируемых результатов обучения по дисциплине
ОПК-3 Способен осуществлять межъязыковое и межкультурное взаимодействие на основе знаний в области географии, истории, политической, экономической, социальной, религиозной и культурной жизни стран изучаемых языков, а также знания об их роли в региональных и глобальных политических	ОПК-3.2 Учитывает роль страноведческих знаний о региональных и глобальных политических процессах при переводе	<i>Знать:</i> географию, историю, политику, экономику, религию и культуру страны изучаемого языка; <i>Уметь:</i> осуществлять межъязыковое и межкультурное взаимодействие на основе знаний в области географии, истории, политической, экономической, социальной, религиозной и культурной жизни стран изучаемых языков; <i>Владеть:</i> навыком использования страноведческих знаний о региональных и глобальных политических процессах при переводе

<p>процессах</p> <p><b>ОПК-4</b> Способен работать с электронными словарями, различными источниками информации, осуществлять поиск, хранение, обработку и анализ информации, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий</p>	<p><b>ОПК-4.1</b> Демонстрирует умение работы с электронными носителями информации, поиском в сети необходимой для перевода информации</p> <p><b>ОПК-4.2</b> Владеет навыками применения справочно-информационных баз данных, тематических глоссариев и сетевых технологий</p>	<p><i>Знать:</i> методы работы с электронными носителями информации, поиском в сети необходимой для перевода информации</p> <p><i>Уметь:</i> работать с электронными словарями, различными источниками информации</p> <p><i>Владеть:</i> навыками применения справочно-информационных баз данных, тематических глоссариев и сетевых технологий</p>
<p><b>ОПК-5</b> Способен понимать принципы работы современных информационных технологий и использовать их при решении задач профессиональной деятельности</p>	<p><b>ОПК-5.1.</b> Понимает содержание, структуру и принципы работы современных информационных технологий, применяемых для решения задач профессиональной деятельности.</p> <p><b>ОПК-5.2.</b> Использует современные информационные технологии при решении задач профессиональной деятельности.</p>	<p><i>Знать:</i> принципы работы современных информационных технологий.</p> <p><i>Уметь:</i> Применять информационные технологии для решения задач профессиональной деятельности;</p> <p><i>Владеть:</i> методами и способами использования информационных технологий для оказания первой помощи при ЧС.</p>

### 1.3. Место дисциплины в структуре образовательной программы

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

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе обучения в школе.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для прохождения практик и государственной итоговой аттестации.

## 2. Структура дисциплины

### Структура дисциплины 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., экзамен 18 ч.

№ 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. Терминологический и понятийный аппарат информационной безопасности и защиты информации	2	2	4				4	Дискуссия, ответы на вопросы, защита лабораторных работ, самостоятельная работа
2	Понятие защиты информации	2	2					6	Дискуссия, ответы на вопросы, самостоятельная работа
3	Порядок отнесения информации к защищаемой	2	4	6				6	Дискуссия, ответы на вопросы, самостоятельная работа
4	Объекты защиты информации	2	2					6	Дискуссия, ответы на вопросы, самостоятельная работа
5	Классификация конфиденциальной информации по видам тайны	2	4	4				6	Дискуссия, ответы на вопросы, защита лабораторных работ, самостоятельная работа
6	Понятие и структура угроз защищаемой информации	2	4					6	Дискуссия, ответы на вопросы
7	Источники, причины обстоятельства и условия дестабилизирующего	2	4					6	Дискуссия, ответы на вопросы, самостоятельная работа

	воздействия на защищаемую информацию								работа.
<b>8</b>	Классификация видов, методов и средств защиты информации	2	2	6				6	Дискуссия, ответы на вопросы, защита лабораторных работ
	Экзамен							<b>18</b>	
	<b>Итого:</b>		<b>22</b>	<b>20</b>				<b>18</b>	<b>54</b>

### 3. Содержание дисциплины

#### ТЕМА 1. ВВЕДЕНИЕ. ТЕРМИНОЛОГИЧЕСКИЙ И ПОНЯТИЙНЫЙ АППАРАТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ.

Основные понятия и термины дисциплины. Предмет и задачи курса. Значение и место курса в подготовке специалистов в сфере лингвистического обеспечения межгосударственных отношений.

Становление и развитие понятия «информационная безопасность».

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

Понятие и назначение доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Документационное обеспечение информационной безопасности и защиты информации

#### ТЕМА 2. 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 3. ПОРЯДОК 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 4. 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 5. 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 6. 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 сущностных проявлений угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

#### ТЕМА 7. 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 8. 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

№	Наименование	Виды учебных	Образовательные технологии
---	--------------	--------------	----------------------------

п/п	раздела	занятий	
1	2	3	4
1	Введение. Терминологический и понятийный аппарат информационной безопасности и защиты информации	Лекция 1 Семинар 1.	Вводная лекция с использованием видеоматериалов Дискуссия Консультирование и проверка домашних заданий посредством электронной почты
2	Понятие защиты информации	Лекция 2.	Проблемная лекция Консультирование и проверка домашних заданий посредством электронной почты
3	Порядок отнесения информации к защищаемой	Лекция 3. Семинар 2.	Лекция с разбором конкретных ситуаций Консультирование и проверка домашних заданий посредством электронной почты
4	Объекты защиты информации	Лекция 4.	Проблемная лекция Консультирование и проверка домашних заданий посредством электронной почты
5	Классификация конфиденциальной информации по видам тайны	Лекция 5. Семинар 3.	Проблемная лекция Консультирование и проверка домашних заданий посредством электронной почты
6	Понятие и структура угроз защищаемой информации	Лекция 6.	Лекция с разбором конкретных ситуаций Консультирование и проверка домашних заданий посредством электронной почты
7	Источники, причины обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию	Лекция 7.	Проблемная лекция Консультирование и проверка домашних заданий посредством электронной почты
8	Классификация видов, методов и средств защиты информации	Лекция 8. Семинар 4.	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:		
-выполнение заданий	12 баллов	48
-сообщение	12баллов	12
		60 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
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»	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. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	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. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		<p>навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. 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. 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. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. 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. 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. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

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

**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/)
4. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. N 646, Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/](http://www.consultant.ru/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/)

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.complexdoc.ru>
2. Журнал «Защита информации. Инсайд»: журнал посвящен вопросам безопасности и защиты информации. <http://www.inside-zi.ru/>
3. <http://www.consultant.ru/>
4. <http://base.garant.ru/>

## 7. Материально-техническое обеспечение дисциплины

Лекционные занятия проводятся в аудитории, оборудованной экраном со стойкой, ноутбуком и мультимедийным проектором. Семинарские занятия проводятся в компьютерном классе с доступом в интернет, оборудованным экраном со стойкой, ноутбуком и мультимедийным проектором.

**Состав программного обеспечения:**

1. Microsoft Office 2010, производитель Microsoft, лицензионное.
2. Windows 7 Pro, производитель Microsoft, лицензионное.

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

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса лицам с ограниченными возможностями здоровья. Для этого от студента требуется представить заключение психолого-медико-педагогической комиссии (ПМПК) и личное заявление (заявление законного представителя).

В заключении ПМПК должно быть прописано:

- рекомендуемая учебная нагрузка на обучающегося (количество дней в неделю, часов в день);
- оборудование технических условий (при необходимости);
- сопровождение и (или) присутствие родителей (законных представителей) во время учебного процесса (при необходимости);
- организация психолого-педагогического сопровождение обучающегося с указанием специалистов и допустимой нагрузки (количества часов в неделю).

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся при необходимости могут быть созданы фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе.

Форма проведения текущей и итоговой аттестации для лиц с ограниченными возможностями здоровья устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно (на бумаге, на компьютере), в форме тестирования и т.п.). При необходимости студенту предоставляется дополнительное время для подготовки ответа на экзамене.

**9. Методические материалы**



## 9.1. Планы семинарских занятий.

### **Занятие 1.**

Тема 1(4ч.) Анализ Доктрины информационной безопасности Российской Федерации.

**ЦЕЛЬ ЗАНЯТИЯ:** Изучение Доктрины информационной безопасности как системы официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения Стратегии национальной безопасности Российской Федерации.

**Задания:**

1. Пользуясь справочно-правовыми базами в сети Интернет, найти Доктрину Информационной безопасности РФ.
2. Проанализировать Доктрину Информационной безопасности.
3. Выявить: национальные интересы Российской Федерации в информационной сфере; угрозы информационной безопасности Российской Федерации; стратегические цели и основные направления обеспечения информационной безопасности.

**ИТОГ ЗАНЯТИЯ:** Письменно сформулировать вывод по итогам изучения материала.

**Список литературы:**

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. N 646, Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/](http://www.consultant.ru/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/)

### **Занятие 2.**

Тема 5 (6ч.) Порядок отнесения информации к защищаемой.

**ЦЕЛЬ ЗАНЯТИЯ:** ознакомление с нормативно-правовой базой в сфере информационной безопасности.

**Задания:**

1. Проанализировать состав законодательных и нормативно-правовых документов в сфере информационной безопасности.
2. Пользуясь справочно-правовыми базами в сети Интернет, найти документы, регламентирующие деятельность по защите информации. Проанализировать найденные документы и ответить на вопросы:
  - наименование документа;
  - актуальность документа;
  - сведения о введении в действие
  - цели и задачи принятия;

- основные термины и определения, используемые в документе;
- основные положения документа.

**ИТОГ ЗАНЯТИЯ:** Письменно сформулировать вывод по итогам изучения материала. В конце работы указать все сайты, использованные при подготовке лабораторной работы. Можно составить сравнительные таблицы и, при необходимости, иллюстрировать скриншотами.

Список источников:

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/)

### **Занятие 3.**

Тема 5 (4ч.) Классификация конфиденциальной информации по видам тайны.

**ЦЕЛЬ ЗАНЯТИЯ:** Выявить наказания за нарушение конфиденциальности для различных видов тайны.

Задания:

1. Проанализировать законодательные и нормативно-правовые документы в сфере информационной безопасности.
2. Пользуясь справочно-правовыми базами в сети Интернет, найти документы, регламентирующие деятельность по защите информации. Проанализировать найденные документы и ответить на вопросы:
  - наименование документа;
  - наказания следует за нарушение.

**ИТОГ ЗАНЯТИЯ:** Письменно сформулировать вывод по итогам изучения материала. В конце работы указать все сайты, использованные при подготовке работы. Можно составить сравнительные таблицы и, при необходимости, иллюстрировать скриншотами.

Список источников:

1. 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/)
2. 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/)

### **Занятие 4.**

## Тема 8 (бч.) Криптографические методы защиты информации.

ЦЕЛЬ ЗАНЯТИЯ: Исследование методов криптографической защиты информации.

Введение.

Наиболее простой тип криптограмм – это так называемые подстановочные криптограммы. Составляя их, каждой букве алфавита сопоставляют определенный символ (чаще тоже букву) и при кодировании всякую букву текста заменяют на соответствующий ей символ.

Расшифровка (криптоанализ) подобных криптограмм не составляет большой проблемы. Все основывается на том, что различные буквы естественного языка – русского, английского или какого-либо другого встречаются в осмысленных текстах неодинаково часто. Следовательно, тоже самое верно и для сопоставляемых им знаков. В еще большей мере это относится к буквосочетаниям из двух или нескольких букв. Лишь некоторые из них часто употребляются, многие же вообще не употребляются.

Анализируя частоту появления тех или иных знаков и их сочетаний можно с большой уверенностью восстановить буквы зашифрованного текста. Этот метод называется частотным анализом. Он основывается на подсчете частоты появления зашифрованных знаков. В таблице 1 указаны относительные частоты букв русского языка. Буквы Е и Ё, а также Ъ и Ы кодируются обычно одинаково, поэтому в таблице они не различаются. Как следует из таблицы наиболее часто встречающаяся буква русского алфавита – это О. Ее относительная частота, равная 0,090, означает, что на 1000 букв русского текста приходится в среднем 90 букв О. В таком же смысле понимаются относительные частоты и остальных букв. В таблицу 1 не включен символ пробел. Его относительная частота наибольшая и равна 0,175.

**Таблица 1.**

№	буква	Отн.частота	№	буква	Отн.частота	№	буква	Отн.частота
0	А	0.062	10	К	0.028	20	Ф	0.002
1	Б	0.014	11	Л	0.035	21	Х	0.009
2	В	0.038	12	М	0.026	22	Ц	0.004
3	Г	0.013	13	Н	0.053	23	Ч	0.012
4	Д	0.025	14	О	0.090	24	Ш	0.006
5	Е	0.072	15	П	0.023	25	Щ	0.003
6	Ж	0.007	16	Р	0.040	26	Ы	0.016
7	З	0.016	17	С	0.045	27	Ь,Ъ	0.014
8	И	0.062	18	Т	0.053	28	Э	0.003
9	Й	0.010	19	У	0.021	29	Ю	0.006
						30	Я	0.018

Рассмотрим криптограмму:

ЦЯРСНСМЩИ ЯМЯКЗЖ ОНКДЖДМ МД СНКЫЙН ГКЮ ОНГРСЯМНБНЦМЩФ  
ЙПЗОСНВПЯЛЛ МН Б ГПТВЗФ РКТЦЯЮФ НМ РКНЕМДД Для расшифровки  
подсчитаем сколько раз в криптограмме встречается каждая буква. Результаты подсчета  
приведены в таблице 2.

**Таблица 2.**

Н	Б	Я	К	Д	С	Р	Г	О	П	З	Ф	Ц	Б	В	Ж	Й	Л	Т	Щ	Ю	Е	И	Ы
11	9	6	6	5	5	4	3	3	3	3	3	3	2	2	2	2	2	2	2	2	1	1	1

Наиболее часто встречающийся символ Н скорее всего означает букву О. Сделав такое предположение, рассмотрим следующий по частоте символ М. В криптограмме имеется двубуквенное сочетание МН. Так как Н – это О, то символ М соответствует согласной. Среди согласных в русском языке выделяются по частоте буквы Т и Н. Разберем случай, когда М означает Н. Если М – это Н, то в сочетании МД, встречающемся в криптограмме, Д скорее всего означает гласную. Из наиболее вероятных для Д вариантов А, Е, И выбираем Е, потому что лишь в этом случае имеющееся в криптограмме слово РКНЕМДД допускает осмысленную расшифровку.

Теперь обратимся к сочетанию ЯМЯКЗЖ. В нем Я может означать лишь гласную А или И. Любые другие возможности заведомо не допускают разумного прочтения слова ЯМЯКЗЖ. Испытаем букву А. Подставляя вместо Я букву А, вместо М – Н, вместо других знаков точки, получим недописанное слово АНА... . В словаре имеется всего лишь несколько слов из 6 букв с таким началом: АНАЛИЗ, АНАЛОГ, АНАНАС, АНАТОМ. Из них годится лишь первое. Если вместо Я подставить букву И, то получится шестибуквенное сочетание с началом ИНИ, но в словаре нет ни одного такого слова. Расшифрованы еще четыре буквы: Я, К, З, Ж. Они означают соответственно А, Л, И, З. В слове ОНКЖДМ известны все символы кроме первого. Заменяя их буквами, получаем: . ОЛЕЗЕН. Ясно, что неизвестная буква – это П.

Значит О расшифровывается как П. Рассмотрим сочетание РКНЕМДД, означающее .ЛО.НЕЕ. Имеется несколько вариантов его прочтения, один из них – СЛОЖНЕЕ. Следовательно, скорее всего Р – это С, Е - это Ж. Из нерасшифрованных знаков чаще всего встречается С. В соответствии с таблицей 1 среди оставшихся согласных наибольшую частоту имеет Т. Естественно предположить, что С означает Т. Попробуем восстановить зашифрованный текст, подставляя вместо разгаданных знаков соответствующие им буквы:

.АСТОТН.. АНАЛИЗ ПОЛЕЗЕН НЕ ТОЛ..О .Л. ПО.СТАНО.О.Н.. ..ИПТО..А.. НО .  
...И. СЛ..А.. ОН СЛОЖНЕЕ

Ясны по контексту, по крайней мере три слова:

.АСТОТН.. означает ЧАСТОТНЫЙ, ТОЛ..О – ТОЛЬКО, .Л. – ДЛЯ.

С учетом новой информации текст примет следующую форму:

ЧАСТОТНЫЙ АНАЛИЗ ПОЛЕЗЕН НЕ ТОЛЬКО ДЛЯ ПОДСТАНО.ОЧНЫ.  
К.ИПТО..А.. НО . Д...И. СЛ.ЧАЯ. ОН СЛОЖНЕЕ

Окончательная расшифровка не представляет труда.

Текст таков:

ЧАСТОТНЫЙ АНАЛИЗ ПОЛЕЗЕН НЕ ТОЛЬКО ДЛЯ ПОДСТАНОВОЧНЫХ  
КРИПТОГРАММ, НО В ДРУГИХ СЛУЧАЯХ ОН СЛОЖНЕЕ.

Задания:

1. Зашифровать любой текст с помощью подстановочного шифра Цезаря (Он состоит в том, что весь алфавит циклически сдвигается вправо на определенное число букв.) Предложить метод расшифровки более простой, чем частотный анализ.
2. Расшифровать заданный преподавателем текст зашифрованный шифром Цезаря.
3. Зашифровать любой текст с помощью шифра замены.
4. Расшифровать заданный преподавателем шифртекст с помощью таблицы Виженера.

ИСХОДНЫЕ ДАННЫЕ: Файлы с шифртекстами.

СОДЕРЖАНИЕ ОТЧЕТА: Отчет должен содержать:

1. Описание алгоритма шифрования.
2. Описание алгоритма криптоанализа.
3. Программы шифрования и дешифрования.
4. Расшифрованные тексты.
5. Выводы по работе.

Н.В.Гришина

### **АННОТАЦИЯ ДИСЦИПЛИНЫ**

Дисциплина реализуется в Институте лингвистики кафедрой Информационной безопасности Института информационных наук и технологий безопасности РГГУ.

Цель дисциплины - изучение теоретических и прикладных вопросов информационной безопасности и использование их в сфере лингвистического обеспечения межгосударственных отношений.

Задачи:

- освоить терминологию и понятийный аппарат в области информационной безопасности и защиты информации;
- изучить нормативно-правовую базу, регулирующую сферу информационной безопасности и защиты информации;
- изучить основные средства и методы обеспечения информационной безопасности;
- научиться применять полученные знания и навыки по информационной безопасности и защите информации в сфере лингвистического обеспечения межгосударственных отношений.

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

<b>Компетенция</b> (код и наименование)	<b>Индикаторы компетенций</b> (код и наименование)	<b>Перечень планируемых результатов обучения по дисциплине</b>
ОПК-3 Способен осуществлять межъязыковое и межкультурное взаимодействие на основе знаний в области географии, истории, политической, экономической, социальной, религиозной и культурной жизни стран изучаемых языков, а также знания об их роли в региональных и глобальных политических процессах	ОПК-3.2 Учитывает роль страноведческих знаний о региональных и глобальных политических процессах при переводе	<i>Знать:</i> географию, историю, политику, экономику, религию и культуру страны изучаемого языка; <i>Уметь:</i> осуществлять межъязыковое и межкультурное взаимодействие на основе знаний в области географии, истории, политической, экономической, социальной, религиозной и культурной жизни стран изучаемых языков; <i>Владеть:</i> навыком использования страноведческих знаний о региональных и глобальных политических процессах при переводе
ОПК-4 Способен работать с электронными словарями, различными источниками информации, осуществлять поиск, хранение, обработку и анализ информации,	ОПК-4.1 Демонстрирует умение работы с электронными носителями информации, поиском в сети необходимой для перевода информации ОПК-4.2 Владеет навыками применения справочно-информационных баз данных, тематических	<i>Знать:</i> методы работы с электронными носителями информации, поиском в сети необходимой для перевода информации <i>Уметь:</i> работать с электронными словарями, различными источниками информации <i>Владеть:</i> навыками применения справочно-информационных баз данных, тематических глоссариев и сетевых технологий

представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	гlossариев и сетевых технологий	
ОПК-5 Способен понимать принципы работы современных информационных технологий и использовать их при решении задач профессиональной деятельности	ОПК-5.1. Понимает содержание, структуру и принципы работы современных информационных технологий, применяемых для решения задач профессиональной деятельности. ОПК-5.2. Использует современные информационные технологии при решении задач профессиональной деятельности.	<i>Знать:</i> принципы работы современных информационных технологий. <i>Уметь:</i> Применять информационные технологии для решения задач профессиональной деятельности; <i>Владеть:</i> методами и способами использования информационных технологий для оказания первой помощи при ЧС.

В результате освоения дисциплины обучающийся должен:

*Знать:* основные понятия в области информационной безопасности и защиты информации; как подобрать нормативные документы используя поисковые системы.

*Уметь:* соблюдать в профессиональной деятельности требования по информационной безопасности; использовать нормативные документы для обеспечения информационной безопасности.

*Владеть:* навыками подбора, изучения и обобщения нормативных материалов по вопросам обеспечения информационной безопасности и методами обеспечения режима конфиденциальности.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы.

