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

45.05.01 - Перевод и переводоведение
Лингвистическое обеспечение межгосударственных отношений

Уровень высшего образования: специалитет
Форма обучения очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

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 теории и практики перевода
№ 10 от 13.05.2021

Оглавление

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины - формирование знаний об основных принципах, методах и направлений 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. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы достижения компетенций	Результаты обучения
ОПК-4 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.	ОПК-4.1 Владеет навыками работы с различными источниками лингвистической информации, в том числе с электронными ресурсами	Знать: принципы работы с электронными изданиями и источниками информации. Уметь: получать, передавать и хранить информацию с помощью информационных, компьютерных и сетевых технологий. Владеть: навыками использования лингвистической информации, содержащейся в электронных источниках информации, при осуществлении переводческой деятельности
	ОПК-4.2 Способен использовать специальную лингвистическую информацию в переводческой работе	

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «» входит в обязательную часть учебного плана по специальности № 45.05.01 «Перевод и переводоведение». Дисциплина реализуется кафедрой теории и практики перевода Института филологии и истории в 1 семестре.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Практический курс первого иностранного языка».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Лексикология первого иностранного языка»; «Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности»; «Перевод текстов международной новостной публицистики - первый иностранный язык»; «Перевод финансово-экономических текстов международной тематики - первый иностранный язык»; «Перевод финансово-экономических текстов международной тематики - первый иностранный язык».

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

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Введение в специальность», «Введение в древние языки и культуры», «Адаптация к профессиональной деятельности», «Адаптивные информационно-коммуникационные технологии в профессиональной деятельности».

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

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часа (ов).

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
1	Лекции	22
1	Семинарские занятия	20
	Всего:	**42**

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 48 академических часа(ов), промежуточная аттестация (экзамен) 18 академических часов.

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 сущностных 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	Лекция 8. Семинар 8	Проблемная лекция Консультирование и проверка домашних заданий посредством

	дестабилизирующего воздействия на защищаемую информацию		электронной почты
9	Классификация видов, методов и средств защиты информации	Лекция 9. Семинар 9	Проблемная лекция Консультирование и проверка домашних заданий посредством электронной почты

Для проведения учебных занятий по дисциплине используются различные образовательные технологии. Для организации учебного процесса может быть использовано электронное обучение и (или) дистанционные образовательные технологии.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Текущий контроль осуществляется в виде устного опроса на семинарских занятиях и суммируется с баллами за промежуточную аттестацию (рецензию).

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос* *- контрольная работа*	 *5 баллов* *10 баллов*	 *30 баллов* *30 баллов*
Промежуточная аттестация *(экзамен)*		*40 баллов*

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	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

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		обосновывает принятые решения. Свободно 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 – «высокий».
82-68/ C	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 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».
67-50/ D,E	удовлетво-рительно/ зачтено	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».
49-0/ F,FX	неудовлет-ворительно/ не зачтено	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.

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/
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/
3. Закон РФ от 21.07.1993 N 5485-I «О государственной тайне», Режим доступа: 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). — ww.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. www.financialenglish.org
2. www.economist.com
3. www.guardian.co.uk
4. www.mirror.co.uk
5. www.news.com.au/dailytelegraph
6. www.washingftonpost.com
7. http//www/.canberra.edu. au/ studyskills /writing/ literature

8. Лингвистика XXI века [Электронный ресурс] : сборник научных статей : к 65-летнему юбилею профессора В. А. Масловой / соред. В. В. Колесов, М. В. Пименова, В. И. Теркулов. - 3-е изд., стер. – М.: ФЛИНТА, 2019. - 943 с. (Серия «Концептуальный и лингвальный миры». Вып. 3). - ISBN 978-5-9765-1818-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1048298 (дата обращения: 14.03.2020

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru
Cambridge University Press
ProQuest Dissertation & Theses Global
SAGE Journals
Taylor and Francis
JSTOR

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые компьютером и проектором для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows

2. Microsoft Office
3. Kaspersky Endpoint Security

Профессиональные полнотекстовые базы данных:
1. Национальная электронная библиотека (НЭБ) www.rusneb.ru
2. ELibrary.ru Научная электронная библиотека www.elibrary.ru
3. Электронная библиотека Grebennikon.ru www.grebennikon.ru
4. Cambridge University Press
5. ProQuest Dissertation & Theses Global
6. SAGE Journals
7. Taylor and Francis
8. JSTOR

Информационные справочные системы:
3. Консультант Плюс
4. Гарант

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

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, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических 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 приготовленными 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). — ww.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). — ww.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). — ww.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). — ww.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). — ww.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). — ww.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). — ww.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). — ww.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). — ww.dx.doi.org/10.12737/11380. - Режим доступа: http://znanium.com/catalog/product/1009606

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Основы информационной безопасности в профессиональной деятельности» реализуется кафедрой информационной безопасности в 1 семестре.

Цель дисциплины - формирование знаний об основных принципах, методах и направлений 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:

Компетенция	**Индикаторы достижения компетенций**	**Результаты обучения**
ОПК-4 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.	ОПК-4.1 Владеет навыками работы с различными источниками лингвистической информации, в том числе с электронными ресурсами	Знать: принципы работы с электронными изданиями и источниками информации. Уметь: получать, передавать и хранить информацию с помощью информационных, компьютерных и сетевых технологий. Владеть: навыками использования лингвистической информации, содержащейся в электронных источниках информации, при осуществлении переводческой деятельности

Программой дисциплины предусмотрены следующие **виды контроля**: промежуточный контроль в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.