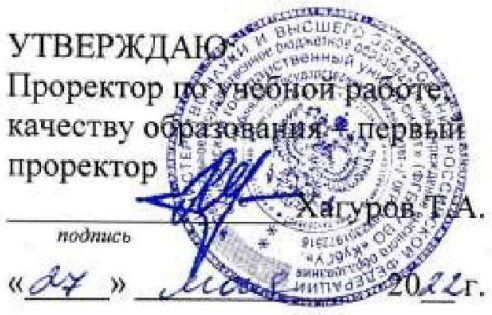
Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»
Факультет компьютерных технологий и прикладной математики



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.09 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Специальность **45.05.01 Перевод и переводоведение**

Специализация: Лингвистическое обеспечение межгосударственных отношений

Программа подготовки академическая

Форма обучения очная

Квалификация (степень) выпускника лингвист-переводчик

Краснодар 2022

Рабочая программа дисциплины «Основы информационной безопасности в профессиональной деятельности» составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по специальности **45.05.01 Перевод и переводоведение**.

Программу составили:

Зацепин М.Н., ст. преподаватель кафедры математического моделирования КубГУ _____

Рабочая программа дисциплины «Основы информационной безопасности в профессиональной деятельности» утверждена на заседании кафедры математического моделирования
протокол № 8 « 22 » апреля 2022 г.

Заведующий кафедрой математического моделирования акад. РАН, д-р физ.-мат. наук, проф. Бабешко В.А. _____

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики
протокол № 6 «25» мая 2022 г.

Председатель УМК факультета
д. техн. наук, доцент Коваленко А.В _____

Рецензенты:
Канд. физ.-мат. наук, доцент Каф. вычислительных технологий КубГУ
Кособуцкая Е.В.
Заместитель директора ООО «ИнитЛаб»
Синица С.Г.

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Дисциплина «Основы информационной безопасности в профессиональной деятельности» ставит своей целью освоение основ информационной безопасности. Цели дисциплины соответствуют следующим формируемым компетенциям: ОПК-2, ОПК-5.

Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера является залогом успешной деятельности при работе с информационными ресурсами. Информационная безопасность является составляющей компьютерной грамотности и основными задачами дисциплины являются: ознакомить студентов с базовыми понятиями информационной безопасности, сформировать представление о принципах защиты от несанкционированного доступа и навыки работы с защищенными программами.

1.2 Задачи дисциплины

Основные **задачи** дисциплины:

– ознакомить студентов с базовыми понятиями информационной безопасности;

– сформировать представление о принципах защиты от несанкционированного доступа и навыки работы с защищенными программами.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности в профессиональной деятельности» относится к обязательной части Блока 1 "Дисциплины" учебного плана для специальности 45.05.01 Перевод и переводоведение ФГОС ВО.

Данная дисциплина призвана обучить студентов соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, при необходимости обеспечивать соблюдение режима секретности, понимать виды и назначение различных мер обеспечения информационной безопасности.

Необходимым требованием к «входным» знаниям, умениям и опыту деятельности обучающегося при освоении данной дисциплины является знакомство с основами и практикой использования средств информационно-коммуникационных технологий, а также сведения предшествующего курса «Информатика и информационные технологии в профессиональной деятельности».

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

Программа определяет общий объем знаний, позволяющий сформировать у студента знания по проблемам правового, административного, технического и программного обеспечения информационной безопасности. Кроме того, освоение дисциплины «Основы информационной безопасности в профессиональной деятельности» способствует повышению информационной культуры обучающихся.

В результате изучения дисциплины студент должен

-знать терминологию в области информационной безопасности, источники возникновения информационных угроз, методы и средства обеспечения информационной безопасности, средства защиты от нарушения конфиденциальности, целостности и доступности информации;

-уметь проводить анализ угроз информационной безопасности, применять на практике основные принципы теории информационной безопасности;

-владеть информацией о современных направлениях развития систем безопасности, об основных типах угроз информационной безопасности.

Изучение данной учебной дисциплины направлено на формирование у обучающихся общепрофессиональных и профессиональных компетенций:

- ОПК-2 – способность соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;
- ОПК-5 – способность самостоятельно осуществлять поиск профессиональной информации в печатных и электронных источниках, включая электронные базы данных.

Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
		знать	**уметь**	**владеть**
ОПК-2	способностью соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	– терминологию в области информационной безопасности; – источники возникновения информационных угроз; – методы и средства обеспечения информационной безопасности; – средства защиты от нарушения конфиденциальности, целостности и доступности информации; – нормативные акты об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи; – тематические электронные ресурсы	– проводить анализ угроз информационной безопасности; – компетентно довести до окружающих информацию об обеспечении безопасности хранения, обработки и передачи информации; – применять на практике основные принципы теории информационной безопасности	– информацией о современных направлениях развития систем безопасности; – информацией об основных типах угроз информационной безопасности; – навыками безопасного сбора и обработки информации
ОПК-5	способностью самостоятельно осуществлять	– способы и средства получения, перера-	– организовывать процессы	– коммуникационными сетевыми навыками;

Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
		знать	**уметь**	**владеть**
	поиск профессиональной информации в печатных и электронных источниках, включая электронные базы данных	ботки и представления информации с помощью информационно-коммуникационных технологий	поиска информации на основе IT-технологий; – использовать базы данных и знаний и тематические информационные ресурсы; – использовать электронные тематические ресурсы для углубления знаний о предметной области.	– навыками тематического поиска анализа информации

Процесс освоения дисциплины «Основы информационной безопасности в профессиональной деятельности» направлен на получения необходимого объема знаний, отвечающих требованиями ФГОС и обеспечивающих успешное ведение специалистом производственной и научно-исследовательской деятельности, владение навыками обеспечения информационной безопасности, средствами защиты от нарушения конфиденциальности, целостности и доступности информации.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 академических часа. Курс «Основы информационной безопасности в профессиональной деятельности» состоит из лекционных и лабораторных занятий, сопровождаемых регулярной индивидуальной работой преподавателя со студентами в процессе самостоятельной работы. В конце семестра проводится экзамен. Программой дисциплины предусмотрены 18 часов лекционных, 18 часов лабораторных занятий.

Виды работ	Всего часов	Форма обучения			
		очная		очно-заочная	заочная
		6 семестр (часы)	семестр (часы)	семестр (часы)	курс (часы)
Контактная работа, в том числе:	**42,3**	**42,3**			
Аудиторные занятия (всего):	**36**	**36**			
занятия лекционного типа	18	18			
лабораторные занятия	18	18			
практические занятия					
семинарские занятия					

Иная контактная работа:		**6,3**	**6,3**			
Контроль самостоятельной работы (КСР)		6	6			
Промежуточная аттестация (ИКР)		0,3	0,3			
Самостоятельная работа, в том числе:		**66**	**66**			
Проработка учебного (теоретического) материала		66	66			
Подготовка к текущему контролю		35,7	35,7			
Контроль:						
Подготовка к экзамену						
Общая трудоемкость	**час.**	**144**	**144**			
	в том числе контактная работа	**42,3**	**42,3**			
	зач. ед	**4**	**4**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Итого акад. часов	Аудиторная работа			СР
			Всего	Л	ЛР	
1.	Введение в информационную безопасность	28	4	4		12
2.	Способы обработки информации	56	18	6	12	26
3.	Основные направления защиты информации	53,7	14	8	6	28
	Контроль самостоятельной работы (КСР)	6				
	Промежуточная аттестация (ИКР)	0,3				
	Подготовка к текущему контролю	35,7				
	Итого	**144**	**36**	**18**	**18**	**66**

Примечание: Л – лекции, ЛР – лабораторные занятия, СРС – самостоятельная работа студента.

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1.	Введение в информационную безопасность	Основные понятия: задачи, объект, предмет, методы информационной безопасности. Официальные органы, обеспечивающие информационную безопасность в Российской Федерации. Обзор российского законодательства в сфере информационных технологий. Федеральный закон «Об информации, информационных технологиях и о защите информации», законодательство РФ в сфере СМИ. Правовое обеспечение информационной безопасности. Доктрина информационной безопасности РФ и Стратегия национальной безопасности Российской Федерации до 2020 года. Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности. Составляющие концептуальной модели информационной безопасности. Понятие угроз безопасности. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации	Опрос по результатам лабораторного задания
2.	Способы обработки информации	Понятие информации. Понятие конфиденциальной информации. Понятие государственной тайны. Степени грифа секретности. Виды сведений составляющих государственную тайну. Перечень информации, не подлежащей к засекречиванию. Классификация видов профессиональной тайны и объекты их приложения. Федеральный закон «О государственной тайне». Федеральный закон «О персональных данных». Федеральный закон «Об электронной подписи». Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Определение требований к уровню обеспечения информационной безопасности. Офисные технологии. Текстовые процессоры. Электронные таблицы. Обработка результатов экспериментов в электронных таблицах. Основные структуры данных. Базы и банки данных. Системы управления базами данных. Способы защиты персональных данных. Электронный документ. Электронный документооборот. Электронная подпись. Информационное облако. Понятие, структура, предназначение, перспективы применения	Опрос по результатам лабораторного задания
3.	Основные направления	Понятие, методы защиты информации. Уровни защиты информации. Угрозы информационным системам и их	Опрос по результатам лабораторного

№	Наименование раздела	Содержание раздела	Форма текущего контроля
	защиты информации	виды. Виды мер обеспечения информационной безопасности: законодательные, морально-этические, организационные, технические, программно-математические. Система защиты информации. Техническое и программное обеспечение информационной безопасности. Основные защитные механизмы: идентификация и аутентификация. Разграничение доступа. Контроль целостности. Защита информации при работе в сети Интернет. Признаки незаконного проникновения в компьютерную систему. Дальнейшие действия в случае обнаружения незаконного проникновения в компьютерную систему. Компьютерные вирусы: понятие, пути распространения, проявление действия вируса. Модели поведения вирусов, деструктивные действия вируса, разрушение программы защиты, изменение состояния программной среды; воздействия на программно-аппаратные средства защиты информации. Программы-шпионы. Взлом парольной защиты. Защита от воздействия вирусов. Использование антивирусных программы. Программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры. Профилактика заражения вирусом. Информационные войны. Компьютерные преступления. Киберпреследование. Переговорный процесс и обеспечение информационной безопасности. Переговорный процесс как способ разрешения конфликтных ситуаций. Виды переговоров. Стратегии переговоров. Роль переводчика в переговорном процессе.	задания

Раздел 1. Основные понятия: задачи, объект, предмет, методы информационной безопасности. Официальные органы, обеспечивающие информационную безопасность в Российской Федерации. Обзор российского законодательства в сфере информационных технологий. Федеральный закон «Об информации, информационных технологиях и о защите информации», законодательство РФ в сфере СМИ. Правовое обеспечение информационной безопасности. Доктрина информационной безопасности РФ и Стратегия национальной безопасности Российской Федерации до 2020 года (**2** ч.)

Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности. Составляющие концептуальной модели информационной безопасности. Понятие угроз безопасности. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации (**2** ч.).

Раздел 2. Понятие информации. Понятие конфиденциальной информации. Понятие государственной тайны. Степени грифа секретности. Виды сведений составляющих государственную тайну. Перечень информации, не подлежащей к засекречиванию. Классификация видов профессиональной тайны и объекты их приложения. Федеральный закон «О государственной тайне». Федеральный закон «О персональных данных». Федеральный закон «Об электронной подписи» (**2** ч.).

Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Угрозы информационной безопасности: классификация, источники возникновения и пути реализации**.** Определение требований к уровню обеспечения информационной безопасности (**2** ч.).

Офисные технологии. Текстовые процессоры. Электронные таблицы. Обработка результатов экспериментов в электронных таблицах. Основные структуры данных. Базы и банки данных. Системы управления базами данных. Способы защиты персональных данных. Электронный документ. Электронный документооборот. Электронная подпись. Информационное облако. Понятие, структура, предназначение, перспективы применения (**2** ч.).

Раздел 3. Понятие, методы защиты информации. Уровни защиты информации. Угрозы информационным системам и их виды. Виды мер обеспечения информационной безопасности: законодательные, морально-этические, организационные, технические, программно-математические. Система защиты информации. Техническое и программное обеспечение информационной безопасности. Основные защитные механизмы: идентификация и аутентификация. Разграничение доступа. Контроль целостности. (**2** ч.).

Защита информации при работе в сети Интернет. Признаки незаконного проникновения в компьютерную систему. Дальнейшие действия в случае обнаружения незаконного проникновения в компьютерную систему. Компьютерные вирусы: понятие, пути распространения, проявление действия вируса. Модели поведения вирусов, деструктивные действия вируса, разрушение программы защиты, изменение состояния программной среды; воздействия на программно-аппаратные средства защиты информации. Программы-шпионы. Взлом парольной защиты (**2** ч.).

Защита от воздействия вирусов. Использование антивирусных программы. Программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры. Профилактика заражения вирусом. Информационные войны. Компьютерные преступления. Киберпреследование (**2** ч.).

Переговорный процесс и обеспечение информационной безопасности. Переговорный процесс как способ разрешения конфликтных ситуаций. Виды переговоров. Стратегии переговоров. Роль переводчика в переговорном процессе. (**2** ч.).

2.3.2 Занятия семинарского типа

Учебный план не предусматривает занятий семинарского типа по дисциплине «основы информационной безопасности в профессиональной деятельности».

2.3.3 Лабораторные занятия

№ п/п	Наименование лабораторных занятий	Форма текущего контроля
1.	Офисные пакеты. Пакет программ Microsoft Office. Редактор Word. Шаблоны и стили. Форматирование документа. Стили. Формы и макросы. Настройка среды Word. Возможности антивирусной защиты, защита доступа и редактирования	Инд. проверка (защита)
2.	Электронные таблицы: назначение и принцип работы программы Excel. Форматы данных. Возможности обработка экспериментальных данных. Настройка табличного процессора Excel.	Инд. проверка (защита)
3.		

	Макросы. Совместное использование приложений MS Office. Возможности антивирусной защиты, защита доступа и редактирования.	
4.	Программа Power Point. Настройка и демонстрация презентаций. Защита доступа и редактирования	Инд. проверка (защита)
5. 6.	Работа с базами данных. СУБД Microsoft Access. Создание структуры базы данных. Таблицы. Формы. Запросы по образцу (Query By Example). Отчеты. Макросы. Создание и обработка базы данных персональной информации	Инд. проверка (защита)
7. 8.	Сетевые сервисы и механизмы безопасности. Основные типы браузеров и их особенности. Структура адресов. Поиск информации в Интернет. Поисковые системы. Электронная почта. Механизмы управления доступом. Средства аутентификации.	Инд. проверка (защита)
9.	Создание архивов. Архивирование с паролем. Вирусы и антивирусы. Защита от вирусных атак. Работа с антивирусными программами	Инд. проверка (защита)

2.3.4 Примерная тематика курсовых работ (проектов)

Учебный план не предусматривает курсовых работ по дисциплине «основы информационной безопасности в профессиональной деятельности».

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплин

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Подготовка к текущему контролю	1. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114688 . 2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469866. 3. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470131. 4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для

		вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469235. 5. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348 (дата обращения: 17.05.2021). – Библиогр. в кн. – ISBN 978-5-238-02857-6.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Темы для самостоятельной работы

1. Опыт законодательного регулирования информатизации в России и за рубежом.

2. Международные правовые акты по защите информации.

3. Объекты, цели и задачи защиты информации.

4. Модели безопасности и их применение.

5. Пакеты антивирусных программ.

6. Криптографические методы защиты информации.

7. Информационная безопасность при подключении к Internet. Межсетевые экраны.

8. Информационная безопасность при подключении к Internet. Сетевые фильтры.

9. Классификация угроз информационной безопасности. Угрозы, не зависящие от человека.

10. Атака. Локальная и удаленная атака. Хакер. Кракер. Фрикер.

11. Атаки на средства аутентификации. Биометрические средства аутентификации.

12. Компьютерные преступления. Киберпреследование. Способы защиты от киберпреследования.

3. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки специалистов программа по дисциплине «Основы информационной безопасности в профессиональной деятельности» предусматривает использование в учебном процессе следующих

образовательных технологий и методов формирования компетенций: применение технических и аудиовизуальных средств обучения, выполнение конкретных технических упражнений, поисковых задач, знакомство с конкретными программными продуктами.

Интерактивные формы лабораторных занятий: использование специализированных и прикладных программ; решение конкретных профессиональных ситуаций, используя методы и подходы информационной безопасности; компьютерное моделирование ситуаций; моделирование переговорного процесса, используя технологии информационной безопасности; групповая дискуссия.

	Вид занятия	Используемые интерактивные образовательные технологии	Общее количество часов
Семестр 6	ЛР	Выполнение групповых и индивидуальных заданий в компьютерном классе: решение конкретных профессиональных ситуаций, используя методы и подходы информационной безопасности; компьютерное моделирование ситуаций; моделирование переговорного процесса, используя технологии информационной безопасности; групповая дискуссия	18
Итого:			18

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Основы информационной безопасности в профессиональной деятельности».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме разноуровневых заданий и **промежуточной аттестации** в форме вопросов и заданий к экзамену.

№ п/п	**Контролируемые разделы (темы) дисциплины**	**Код контролируемой компетенции (или ее части)**	**Наименование оценочного средства**	
			Текущий контроль	**Промежуточная аттестация**
1	Введение в информационную безопасность	ОПК-2	*УО*	*ЭкВ (1-5)*
2	Способы обработки информации.	ОПК-2, ОПК-5	*УО, ЗР*	*ЭкВ(6-8)*
3	Основные направления защиты информации.	ОПК-2, ОПК-5	*УО*	*ЭкВ (9-22)*

Сокращения: *УО* – опрос по результатам лабораторного задания, *ЗП* – защита проекта, *ТР* – типовой расчет, *ВкЗ* – экзаменационные вопросы.

Показатели, критерии и шкала оценки сформированных компетенций

Код и наименование компетенции	Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания		
	пороговый	**базовый**	**продвинутый**
	Оценка		
	удовлетворительно	**хорошо**	**отлично**
ОПК-2 способностью соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	*Знать*: базовую терминологию в области информационной безопасности; основные источники возникновения информационных угроз; базовые методы обеспечения информационной безопасности; основные средства защиты от нарушения конфиденциальности; основные нормативные акты об организации и обеспечении безопасности хранения, и передачи по каналам связи *Уметь*: проводить анализ угроз информационной безопасности; применять на практике основные принципы теории информационной безопасности. *Владеть*: информацией об основных типах угроз информационной безопасности; базовыми навыками безопасного сбора и обработки информации. *Студент показывает* не достаточный уровень знаний учебного материала, не в полном объеме владеет практическими	*Знать*: терминологию в области информационной безопасности; источники возникновения информационных угроз; методы и средства обеспечения информационной безопасности; средства защиты от нарушения конфиденциальности, целостности и доступности информации; нормативные акты об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи; тематические электронные ресурсы *Уметь*: проводить анализ угроз информационной безопасности; компетентно довести до окружающих информацию об обеспечении безопасности хранения, обработки и передачи информации; применять на практике основные принципы теории информационной безопасности. *Владеть*: информацией об основных типах угроз информационной безопасности;	*Знать*: терминологию в области информационной безопасности; источники возникновения информационных угроз; методы и средства обеспечения информационной безопасности; средства защиты от нарушения конфиденциальности, целостности и доступности информации; нормативные акты об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи; тематические электронные ресурсы *Уметь*: уверенно проводить анализ угроз информационной безопасности; компетентно довести до окружающих информацию об обеспечении безопасности хранения, обработки и передачи информации; применять на практике основные принципы теории информационной безопасности. *Владеть*: информацией о современных направлениях

Код и наименование компетенции	Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания		
	пороговый	**базовый**	**продвинутый**
	Оценка		
	удовлетворительно	**хорошо**	**отлично**
	навыками, чувствует себя неуверенно при анализе междисциплинарных связей. В ответе не всегда присутствует логика, аргументы привлекаются недостаточно веские. На поставленные вопросы затрудняется с ответами, показывает недостаточно глубокие знания.	навыками безопасного сбора и обработки информации. *Студент показывает* достаточный уровень профессиональных знаний, свободно оперирует понятиями, методами оценки принятия решений, имеет представление о междисциплинарных связях, увязывает знания, полученные при изучении различных дисциплин, умеет анализировать практические ситуации, но допускает некоторые погрешности. Ответ построен логично, материал излагается хорошим языком, привлекается информативный и иллюстрированный материал, но при ответе допускает некоторые погрешности. Вопросы, задаваемые преподавателем, не вызывают существенных затруднений	развития систем безопасности; информацией об основных типах угроз информационной безопасности; навыками безопасного сбора и обработки информации. *Студент показывает* не только высокий уровень теоретических знаний по дисциплине, но и прослеживает междисциплинарные связи. Умеет увязывать знания, полученные при изучении различных дисциплин, анализировать практические ситуации, принимать соответствующие решения. Ответ, построен логично, материал излагается четко, ясно, хорошим языком, аргументировано. На вопросы отвечает кратко, аргументировано, уверенно, по существу
ОПК-5 способностью самостоятельно осуществлять поиск профессиональной информации в	*Знать:* способы и средства получения, переработки и представления информации с помощью информационно-	*Знать*: способы и средства получения, переработки и представления информации с помощью информационно-коммуникационных технологий	*Знать*: способы и средства получения, переработки и представления информации с помощью информационно-коммуникационных технологий

Код и наименование компетенции	Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания		
	пороговый	**базовый**	**продвинутый**
	Оценка		
	удовлетворительно	**хорошо**	**отлично**
печатных и электронных источниках, включая электронные базы данных.	коммуникационных технологий; *Уметь:* применять на практике основные принципы теории информационной безопасности; *Владеть:* навыками сбора и обработки информации; *Студент показывает* не достаточный уровень знаний учебного материала, не в полном объеме владеет практическими навыками, чувствует себя неуверенно при анализе междисциплинарных связей. В ответе не всегда присутствует логика, аргументы привлекаются недостаточно веские. На поставленные вопросы затрудняется с ответами, показывает недостаточно глубокие знания.	*Уметь:* организовывать процессы поиска информации на основе IT-технологий; использовать базы данных и знаний и тематические информационные ресурсы; использовать электронные тематические ресурсы для углубления знаний о предметной области. *Владеть*: коммуникационными сетевыми навыками; навыками тематического поиска анализа информации. *Студент показывает* достаточный уровень профессиональных знаний, свободно оперирует понятиями, методами оценки принятия решений, имеет представление о междисциплинарных связях, увязывает знания, полученные при изучении различных дисциплин, умеет анализировать практические ситуации, но допускает некоторые погрешности. Ответ построен логично, материал излагается хорошим языком, привлекается	*Уметь:* организовывать процессы поиска информации на основе IT-технологий; использовать базы данных и знаний и тематические информационные ресурсы; использовать электронные тематические ресурсы для углубления знаний о предметной области. *Владеть*: уверенными коммуникационными сетевыми навыками; устойчивыми навыками тематического поиска анализа информации. *Студент показывает* не только высокий уровень теоретических знаний по дисциплине, но и прослеживает междисциплинарные связи. Умеет увязывать знания, полученные при изучении различных дисциплин, анализировать практические ситуации, принимать соответствующие решения. Ответ, построен логично, материал излагается четко, ясно, хорошим языком, аргументировано. На вопросы отвечает кратко, аргументировано,

Код и наименование компетенции	Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания		
	пороговый	**базовый**	**продвинутый**
	Оценка		
	удовлетворительно	**хорошо**	**отлично**
		информативный и иллюстрированный материал, но при ответе допускает некоторые погрешности. Вопросы, задаваемые преподавателем, не вызывают существенных затруднений	уверенно, по существу

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

Примерный перечень вопросов, выносимых на экзамен

1. Понятие информации. Признаки информации.
2. Информация по структуре и по уровню доступа.
3. Объекты, цели и задачи защиты информации.
4. Нормативно-правовые, морально-этические, организационные и физические (технические) механизмы защиты.
5. Угрозы информационной безопасности: классификация, источники возникновения и пути реализации.
6. Конфиденциальная информация и ее разновидности.
7. Понятие электронного документа и электронного документооборота. Электронная подпись.
8. Понятие защиты информации. Уровни защиты информации.
9. Угрозы информационным системам и их виды. Программы-шпионы. Методы защиты информации.
10. Техническое и программное обеспечение информационной безопасности.
11. Система защиты информации. Информационное оружие.
12. Компьютерные вирусы.
13. Компьютерная система как объект информационной безопасности.
14. Информационные процессы как объект информационной безопасности
15. Влияние человеческого фактора на обеспечение информационной безопасности
16. Виды и назначение различных мер обеспечения информационной безопасности
17. Программно-аппаратные средства обеспечения информационной безопасности
18. Классификация программно-аппаратных средств обеспечения информационной безопасности
19. Защита от несанкционированного доступа
20. Антивирусная защита.
21. Защита информации при работе в сети Интернет.
22. Признаки незаконного проникновения в компьютерную систему.

Критерии оценивания результатов обучения

Оценка	Критерии оценивания по экзамену
Высокий уровень «5» (отлично)	оценку «отлично» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку «хорошо» заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку «удовлетворительно» заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Основные требования к результатам освоения дисциплины представлены в таблице в виде признаков сформированности компетенций. Требования формулируются по двум

уровням: пороговый и повышенный и в соответствии со структурой, принятой в ФГОС ВО: знать, уметь, владеть.

№ п/п	Раздел дисциплины, тема	Виды работ		Код компетенции	Конкретизация компетенции
		Аудит	СРС		
1	Введение в информационную безопасность	*ЛР*	*ДР*	ОПК-2, ОПК-5	*знает:* основные термины и понятия *умеет:* определять информацию по структуре и по уровню доступа *владеет:* знаниями о концептуальной модели информационной безопасности
		ЛЗ	*ТЕОР*		
2	Способы обработки информации.	*ЛР*	*ТЕОР*	ОПК-2, ОПК-5	*знает:* разновидности конфиденциальной информации *умеет:* создавать электронные таблицы и документы *владеет:* знаниями об электронной подписи и информационном облаке
		ЛЗ	*ДР*		
3	Основные направления защиты информации.	*ЛЗ*	*ТЕОР*	ОПК-2, ОПК-5	*знает:* понятие, методы защиты информации *умеет:* использовать антивирусные программы *владеет:* знаниями о роли переговорного процесса
		ЛР	*ДР*		

Методические рекомендации к сдаче экзамена

В ходе проводимых занятий предлагаемые студентам задания, упражнения и т.п. Экзамен является заключительным этапом процесса формирования компетенции студента при изучении дисциплины или ее части и имеет целью проверку и оценку знаний студентов по теории и применению полученных знаний, умений и навыков при решении практических задач. Экзамены проводятся по расписанию в сроки, предусмотренные календарным графиком учебного процесса. Расписание экзаменов доводится до сведения студентов не менее чем за две недели до начала экзаменационной сессии.

Результаты экзамена оцениваются по четырехбалльной системе («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») и заносятся в экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1 Учебная литература:

1. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114688 .
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469866.
3. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470131.
4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469235.
5. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348 (дата обращения: 17.05.2021). – Библиогр. в кн. – ISBN 978-5-238-02857-6.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах.

Нормативные источники

1. Конституция РФ.
2. Федеральный закон «О безопасности» от 28.12.2010 N 390-ФЗ.

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Закон РФ от 27.12.1991 N 2124-1 «О средствах массовой информации».
5. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
6. Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1.
7. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
8. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
9. Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации».
10. Доктрина информационной безопасности Российской Федерации.
11. Указ Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
12. Постановление Правительства РФ от 16.04.2012 N 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».
13. Постановление Правительства РФ от 24.11.2009 N 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» (вместе с «Требованиями к технологическим, программным и лингвистическим средствам обеспечения пользования официальным сайтом Правительства Российской Федерации в сети Интернет»).
14. Приказ ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (с изменениями и дополнениями) (Положение ПКЗ-2005)».
15. Приказ ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

5.2. Периодическая литература.

Не используются

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

1. http://www.kremlin.ru
2. http://www.government.ru
3. http://www.council.gov.ru
4. http://www.duma.gov.ru
5. http://consultant.ru
6. http://elibrary.ru
7. ЭБС «ЮРАЙТ» https://urait.ru/
8. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
9. ЭБС «BOOK.ru» https://www.book.ru
10. ЭБС «ZNANIUM.COM» www.znanium.com
11. ЭБС «ЛАНЬ» https://e.lanbook.com

6. Методические указания для обучающихся по освоению дисциплины

В ходе проводимых занятий предлагаемые студентам задания, упражнения и т.п. должны быть ориентированы на расширение спектра функциональных возможностей, используемых в образовательных учреждениях информационных технологий.

Для приобщения обучаемых к поиску, к исследовательской работе, для развития их творческого потенциала следует по возможности избегать прямого руководства работой обучающихся при выполнении ими тех или иных заданий, чаще выступать в роли консультанта, эксперта.

Важнейшим этапом курса является самостоятельная работа по дисциплине. Поиск информации для ответов на вопросы для самостоятельной работы и выполнения заданий в некоторых случаях предполагает не только изучение основной учебной литературы, но и привлечение дополнительной литературы, а также использование ресурсов сети Интернет.

Примерные варианты тем для самостоятельных работ и индивидуальных заданий

1. Современные стратегии доступа к информации.
2. Безопасный сетевой поиск информации.
3. Программный инструментарий, применяемый для защиты информации.
4. Новейшие компьютерные технологии в защите информации.
5. Наиболее распространенные угрозы информационной безопасности.
6. Стандарты и спецификации в области информационной безопасности.
7. Идентификация и аутентификация, управление доступом к информации.
8. Протоколирование и аудит, шифрование, контроль целостности.
9. Обеспечение высокой доступности.
10. Обеспечение высокой защищенности.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7. Материально-техническое обеспечение по дисциплине

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа (ауд. 313, 312, 324)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Операционная система MS Windows. Интегрированное офисное приложение MS Office, Программное обеспечение для организации управляемого коллективного и безопасного доступа в Интернет

Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (105, 107)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Операционная система MS Windows. Интегрированное офисное приложение MS Office, Программное обеспечение для организации управляемого коллективного и безопасного доступа в Интернет, Справочно-правовая система «Консультант Плюс»
Учебные аудитории для проведения лабораторных работ. Лаборатория информационных технологий – компьютерные залы 105, 107	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Операционная система MS Windows. Интегрированное офисное приложение MS Office, Программное обеспечение для организации управляемого коллективного и безопасного доступа в Интернет, Справочно-правовая система «Консультант Плюс»

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное	

	оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Помещение для самостоятельной работы обучающихся (ауд. 102а)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	