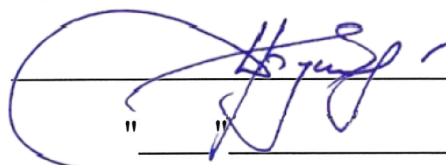


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной
образовательной программы



Буинцев Д.Н.

2024 г

РАБОЧАЯ ПРОГРАММА

Дисциплины

*Б1.О.15 «Организационное и правовое обеспечение информационной
безопасности»*

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 Информационная безопасность

профиль

*Безопасность автоматизированных систем (по отрасли или в сфере
профессиональной деятельности)*

Квалификация

Бакалавр

Форма обучения

очная

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск
2024

Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

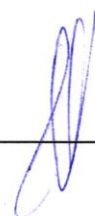
Программу составил:

Мазур И.К., доцент кафедры информатики



Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» утверждена на заседании кафедры информатики, протокол № 8 от 19 марта 2024 г.

Исполняющий обязанности
заведующего кафедрой информатики



Осипов Г.С.

1. Цель и задачи дисциплины

Цель дисциплины

Формирование понятий профессиональной деятельности у студентов, овладение системой знаний в области применения организационного и правового обеспечения информационной безопасности

Задачи дисциплины

- сформировать способность использовать основы правовых знаний в различных сферах деятельности;
- сформировать умения и навыки использования нормативных правовых актов в профессиональной деятельности;
- познакомить с организационными методами реализации политики безопасности предприятия при проектировании системы информационной безопасности.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к разделу обязательных дисциплин подготовки студентов по направлению подготовки бакалавров 10.03.01 Информационная безопасность.

Пререквизиты дисциплины:

Для освоения данной дисциплины студент должен владеть основными понятиями дисциплины «Основы информационной безопасности».

Постреквизиты дисциплины:

Знания, умения и навыки, полученные в процессе изучения данного курса, могут быть использованы студентами при изучении дисциплины «Комплексное обеспечение защиты информации объекта информатизации», «Организационное и правовое обеспечение информационной безопасности». Освоение данной дисциплины должно подготовить студентов к профессиональной деятельности в области информационной безопасности, призваны подготовить к прохождению преддипломной практики, написанию выпускной квалификационной работы.

3. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Знать: виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность. УК-2.2. Умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты решений для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности. УК-2.3.

		Владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией.
УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1 Знать задачи и направления государственной политики в сфере противодействия коррупции. УК-10.2 Уметь определять содержание полномочий государственных органов в сфере противодействия коррупции, объяснять отрицательное влияние коррупции на общество и воспитывать нетерпимость к коррупции УК-10.3 Иметь необходимые навыки в сфере противодействия коррупции
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1 - Знает основные виды и порядок применения нормативных и методических документов, а также порядок соблюдения законодательных ограничений в сфере профессиональной деятельности; ОПК-5.2 - Умеет использовать основные методы правовой оценки различных подходов решения задач в сфере профессиональной деятельности; ОПК-5.3 - Владеет навыками разработки текстовой документации в области профессиональной деятельности в соответствии с нормативными требованиями, регламентирующими деятельность по защите информации.
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.1 - Знает принципы поиска, обработки, обобщения и представления информации для решения задач профессиональной деятельности; ОПК-8.2 - Умеет работать с источниками информации, базами данных и нормативной документацией при решении профессиональных задач; ОПК-8.3 - Владеет практическими навыками поиска необходимой информации и обеспечения информационной безопасности при решении задач в области профессиональной деятельности.
ОПК-4.1	Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.1 - Знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; ОПК-4.1.2 - Умеет определять подлежащие защите информационные ресурсы, определять параметры настройки программного обеспечения, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; ОПК-4.1.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем.

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет **4** зачетные единицы (**144** академических часа).

Вид работы	Трудоемкость, акад. часов	
	семестр	всего
	5	
Общая трудоемкость	144	144
Контактная работа:	58	58
Лекции (Лек)	18	18
Лабораторные работы (Лаб)	36	36
Контактная работа в период теоретического обучения (КонтТО) (Проведение текущих консультаций и индивидуальная работа со студентами)	4	4
Контактная работа в период промежуточной аттестации (КонтПА)	0	0
Промежуточная аттестация зачет с оценкой	0	0
Самостоятельная работа:	86	86
- самостоятельное изучение разделов; - самоподготовка (проработка и повторение лекционного материала, материала учебников и учебных пособий); - подготовка к практическим занятиям; - подготовка к коллоквиумам; - подготовка к промежуточной аттестации и т.п.)	0 40 29 8 9	0 40 29 8 9

4.2. Распределение видов работы и их трудоемкости по разделам дисциплины (модуля)

№ п/п	Раздел дисциплины/ темы		Виды учебной работы (в часах)				Формы текущего контроля успеваемости, промежуточной аттестации
			контактная			Самостоятельная работа	
		семестр	Лекции	Практические занятия	Лабораторные занятия		
1.	Нормативно- правовая основа концепции ИБ	8	6	10		30	Устный опрос по теме лекции. Проверка домашнего задания.
2.	Правовое обеспечение информационной безопасности		6	14		25	Устный опрос по теме лекции. Проверка домашнего задания.
3.	Организационное обеспечение информационной безопасности		6	12		21	Устный опрос по теме лекции. Проверка домашнего задания.

4.	<i>Зачет с оценкой</i>		0	0		10	
	<i>итого</i>		18	36		86	

4.3. Содержание разделов дисциплины

Тема 1. Нормативно-правовая основа концепции ИБ

Правовые, нормативные и организационно-распорядительные документы. Обзор Российского законодательства в области информационной безопасности. Обзор Международного законодательства в области информационной безопасности. Модель процесса управления ИБ в разрезе различных стандартов. Требования стандарта ISO/ IEC 27000 к системам информационной безопасности. Требования нормативных стандартов к оценке рисков ИБ.

Тема 2 Правовое обеспечение информационной безопасности

Основные понятия о нормах, правах и правовых отношениях. Содержание и структура правового обеспечения. Правовая база защиты информации. Правовая база защиты персональных данных. Законодательная база в области интеллектуальной собственности. Законодательная база в области электронной подписи. Законодательная база в области технического регулирования.

Тема 3. Организационное обеспечение информационной безопасности

Основные принципы и условия организационной защиты информации. Основные подходы и требования к организации системы защиты информации. Основные силы и средства, используемые для организации защиты информации. Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений. Отнесение сведений к различным видам конфиденциальной информации. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей. Основания и порядок рассекречивания сведений и их носителей. Отнесение сведений к коммерческой тайне. Организация допуска и доступа персонала к конфиденциальной информации. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.

4.4. Темы и планы лабораторных занятий

Практическое занятие №1 (10 ч.)

Тема Нормативно-правовая основа концепции ИБ

Вопросы для обсуждения:

1. Понятие и цель организационного и правового обеспечения защиты информации
2. Структура организационного и правового обеспечения защиты информации
3. Принципы и методы организационного и правового обеспечения защиты информации

Практическое занятие №2 (14 ч.)

Тема Правовое обеспечение информационной безопасности

Вопросы для обсуждения:

1. Понятие информационной безопасности Российской Федерации
2. Методы обеспечения информационной безопасности Российской Федерации
3. Организация обеспечения информационной безопасности Российской Федерации
4. Классификация информации по возможности доступа
5. Классификация информации с точки зрения возможности распространения
6. Законодательство об электронной цифровой подписи
7. Стандарты и Технические регламенты

Практическое занятие №3 (12 ч.)

Тема **Организационное обеспечение информационной безопасности**

Вопросы для обсуждения:

1. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти
2. Организационные структуры системы обеспечения информационной безопасности предприятия (организации)
3. Нормативные требования к составу и содержанию системы организационного обеспечения информационной безопасности
4. Корпоративное нормативное регулирование
5. Организация объектовых режимов безопасности
6. Управление персоналом на предприятиях и в организациях

5. Темы дисциплины (модуля) для самостоятельного изучения

Не предусмотрены

6. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1.	Нормативно-правовая основа концепции ИБ	Лекция 1-3	Традиционная лекция в ауд. с мультимедиа проектором
		Практические занятия 1-5	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
2.	Правовое обеспечение информационной безопасности	Лекции 4-6	Традиционная лекция в ауд. с мультимедиа проектором
		Практические занятия 6-12	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
3	Организационное обеспечение информационной безопасности	Лекция 7-9	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 13-18	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.

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

Оценочные средства составляются преподавателем самостоятельно при ежегодном обновлении банка средств. Количество вариантов зависит от числа обучающихся.

Задания для текущего контроля

№ раздела дисципли ны	Наименование практических работ
1.	«Введение в правовые и организационные основы обеспечения информационной безопасности» «Правовые и организационные основы защиты охраняемой законом тайны» «Правовой режим коммерческой тайны» «Организационные и правовые основы обеспечения безопасности персональных данных» «Юридическая, административная, дисциплинарная, уголовная ответственность за правонарушения в сфере информационной безопасности»
2.	«Правовые основы информационной безопасности Российской Федерации» «Особенности организационно-правового обеспечения процессов создания автоматизированных систем» «Практика разработки и реализации политики информационной безопасности корпоративных информационных систем» «Правовое регулирование распространения информации и доступа к информации» «Особенности правового регулирования общественных отношений при использовании современных технических средств обработки информации и при разработке шифровальных средств» «Законодательство о техническом регулировании» «Правовые основы защиты компьютерной информации»
3.	«Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти» «Организационные структуры системы обеспечения информационной безопасности предприятия (организации)» «Нормативные требования к составу и содержанию системы организационного обеспечения информационной безопасности». «Корпоративное нормативное регулирование» «Организация объектовых режимов безопасности» «Управление персоналом на предприятиях и в организациях».

Примерные темы самостоятельной работы

1. Понятие коммерческой тайны
2. Правовой режим коммерческой тайны
3. Понятие служебной тайны
4. Особенности защиты профессиональной тайны
5. Уголовная ответственность за разглашение государственной тайны
6. Уголовная ответственность за разглашение коммерческой, налоговой и банковской тайны
7. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
8. Гражданская и дисциплинарная ответственность за разглашение коммерческой тайны, банковской тайны, за нарушение правового режима ноу-хау
9. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)
10. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи
11. Конституционные гарантии прав граждан на информацию

12. Структура государственной системы правового регулирования информационной безопасности в Российской Федерации
13. Корпоративная нормативная база по защите информации. Политика безопасности.
14. Организация пропускного режима.

Примерные темы рефератов:

1. Понятие служебной тайны в российском законодательстве.
2. Виды различных тайн в российском законодательстве (адвокатская, медицинская, личная, следствия, переговоров, переписки и т. д.).
3. Коммерческая тайна как разновидность способов защиты информации.
4. Ноу-хау - вид защищаемой информации в российском праве.
5. Конституция РФ как правовая основа защиты информации.
6. Гражданский кодекс РФ как правовая основа защиты информации.
7. Федеральный закон «О персональных данных» как правовая основа защиты информации.
8. Правовые основы защиты личной тайны в России.
9. Конституция РФ как основа закрепления прав на личную тайну.
10. Защита персональных данных: право или обязанность?
11. Виды защищаемых персональных данных.
12. Процесс восстановления нарушенных прав на различные виды тайн и персональные данные.
13. Уголовно-правовая политика России в области защиты информации на современном этапе.
14. Виды гражданско-правовых и дисциплинарных норм, применяемых при наступлении ответственности за разглашение защищаемой информации
15. Административная ответственность за разглашение защищаемой информации.
16. Виды административных норм в российском административном праве, устанавливающих ответственность за разглашение защищаемой информации.
17. Правовое регулирование отношений, связанных с доступом к персональным данным и их обработкой
18. Основные положения концепции и программы правовой информатизации как инструмента правового регулирования информационной безопасности личности, общества, государства
19. Организация внутри объектового режима.
20. Порядок проведения служебных расследований
21. Управление персоналом на предприятиях и в организациях

Примерные вопросы к зачёту.

1. Государственная система защиты информации в РФ от иностранных технических разведок и от ее утечки по техническим каналам.
2. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа.
3. Оценка соответствия объектов информатизации требованиям безопасности информации.
4. Классификация автоматизированных систем и требования по защите информации.
5. Организационные средства защиты информации. Место организационных средств в систем комплексной защиты информации объектов информатизации.
6. Классификация и основное содержание направлений организационной деятельности по обеспечению информационной безопасностью
7. Архитектура систем защиты информации. Классификация требований к СЗИ. Принципы построения систем защиты.
8. Служба защиты информации. Нормативная база создания служб защиты информации.
9. Принципы организации службы. Основные задачи службы.
10. Функции службы защиты информации. Порядок взаимодействия службы защиты информации с другими структурными подразделениями объекта.

11. Общее содержание организации и обеспечения работ по защите информации.
12. Основные мероприятия по подготовке лиц, ответственных за обеспечение информационной безопасности.
13. Управление процессами функционирования систем защиты информации.
14. Организационное и документальное обеспечение работ по защите информации.
15. Основное назначение документационного обеспечения информационной безопасности. Структура и состав системы документационного обеспечения защиты информации.
16. Организация пропускного и внутриобъектового режима. Понятие "пропускной режим".
17. Основные мероприятия по обеспечению пропускного режима на объекте.
18. Средства технического контроля и управления доступом.
19. Понятия государственной, профессиональной, служебной тайны.
20. Конфиденциальная информация. Признаки информации, составляющей коммерческую тайну.
21. Понятие политики информационной безопасности, принципы разработки и внедрения эффективных политик.
22. Организация и поддержание конфиденциального документооборота.
23. Программные, аппаратные и организационные средства его обеспечения.
24. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации.
25. Задачи, решаемые службой безопасности объекта. Структура и состав службы безопасности объекта.
26. Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне.
27. Требования к помещениям и хранилищам, в которых ведутся закрытые работы.
28. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей.
29. Защита информации в экстремальных ситуациях. Дайте определение понятию «информация».
30. Перечислите виды охраноспособной информации.
31. Опишите методы охраны информации.
32. Обоснуйте необходимость защиты информации.
33. Объясните, в чём разница между охраной и защитой информации.
34. Каковы существенные особенности информации?
35. Чем вызвана необходимость правового регулирования в информационной сфере?
36. Приведите пример правовой охраны информации.
37. Составьте перечень известных вам нормативных актов, посвящённых охране информации.
38. Каково назначение коммерческой тайны?
39. Чем вызвана необходимость защиты служебной тайны?
40. Оцените надёжность защиты при помощи права различных видов тайн.
41. Перечислите виды защищаемых персональных данных
42. В чём заключается сущность правовой защиты различных видов тайн?
43. Оцените надёжность правовой защиты различных видов тайн.
44. Укажите принципиальные различия между различными видами тайн и персональными данными.
45. Сравните различные виды персональных данных с точки зрения правовой защиты.
46. Дайте характеристику уголовно-правовым способам борьбы с разглашением защищаемой информации.
47. От чего зависит применение уголовно-правовых норм в борьбе с разглашением защищаемой информации?
48. Дайте характеристику гражданско-правовому способу защиты охраняемой информации.
49. Перечислите виды гражданско-правовых норм, направленных на защиту охраняемой информации.
50. Дайте определение понятию «разглашение защищаемой информации».
51. Перечислите виды разглашаемой информации.

52. Обоснуйте значение административно-правовых способов борьбы с разглашением защищаемой информации.
53. Какие положения, связанные с вопросами обработки информации, закреплены в Конституции Российской Федерации?
54. Какие виды информации обязательно требуется защищать в соответствии с законодательством Российской Федерации?
55. К какой информации не может быть ограничен доступ?
56. Какую ответственность может повлечь нарушение требований Федеральных законов?

Система оценивания планируемых результатов обучения

Критерии оценивания:

Критерием оценивания является выполнение самостоятельных заданий, контрольных и лабораторных работ.

Самостоятельные задания, контрольные и лабораторные работы по результатам выполнения и защиты оцениваются с учетом следующих основных параметров:

- своевременное выполнение работы;
- полнота и правильность ответов на вопросы, заданные в ходе защиты работы.

В случае выполнения данных условий, студент имеет возможность сдавать теоретический зачет по вопросам.

Оценка «отлично» выставляется студенту, глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.

Оценка «хорошо» выставляется студенту, твердо знающему программный материал, грамотно и по существу излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.

Оценка «удовлетворительно» выставляется студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

Оценка «не зачтено» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, допускающему в ответе или в решении задач грубые ошибки.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
коллоквиум	1	3	3	9
Промежуточная аттестация (зачет)			20	43
Итого за семестр			60	100

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Основная литература:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. —

Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/511239>

2. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 415 с. — (Высшее образование). — ISBN 978-5-534-14327-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/510644>
3. Кубанков, А. Н. Система обеспечения информационной безопасности Российской Федерации: организационно- правовой аспект : учебное пособие / А. Н. Кубанков, Н.Н. Куняев ; под редакцией А. В. Морозов. — Москва : Всероссийский государственный университет юстиции (РПА Минюста России), 2014. — 78 с. — ISBN 978-5-89172-850-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/47262.html>
4. Кожуханов, Н. М. Правовые основы информационной безопасности : учебное пособие / Н. М. Кожуханов, Е. С. Недосекова. — Москва : Российская таможенная академия, 2013. — 88 с. — ISBN 978-5-9590-0725-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/69749>.
5. Мирошников, А. И. Организационное и правовое обеспечение информационной безопасности и защита информации : учебное пособие / А. И. Мирошников, А. С. Сысоев. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2022. — 107 с. — ISBN 978-5-00175-160-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/128718.html>
6. Галатенко, В. А. Организационное и правовое обеспечение информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/97562.html>

8.2.дополнительная литература:

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/497002>.
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/490019>.
3. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/490277>.
4. Семенов Ю.А. Процедуры, диагностики и безопасность в Интернет [Электронный ресурс] / Ю.А. Семенов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 581 с. — ISBN 978-5-94774-708-9. — Режим доступа: <http://www.iprbookshop.ru/62827.html>

8.3.Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Professional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),

7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Microsoft Windows 10 Pro, 64 bit, Rus, OEM, Операционная система
10. Неисключительное право на использование ПО Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition.
11. Неисключительное право на использование ПО Kaspersky Security для виртуальных и облачных сред, Server, VirtSvr, License, Education Renewal
12. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
13. Microsoft Volume Licensing Service, (бессрочная), (лицензия 62824441),
14. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
15. Visual Studio Professional
16. «Антиплагиат. ВУЗ». Лицензионный договор № 5044 от 14.05. 2022 года (ежегодное продление).

8.4. Профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии» (<https://habr.com/>)
2. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- (<https://github.com/>)
3. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.n-t.ru>)
4. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии (http://window.edu.ru/catalog/?p_rubr=2.2.75.6)
5. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
6. Цифровая коллекция электронных версий изданий (учебники, учебные пособия, учебно-методические документы, монографии) по экономическим, естественным, техническим и гуманитарным наукам, сгруппированных по тематическим и целевым признакам.
7. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)
8. Интернет-университет информационных технологий (www.intuit.ru)
9. Онлайн среда разработки приложений (ideone.com)
10. Журнал «КомпьютерПресс» (www.compress.ru)
11. Издательство «Открытые системы» (www.osp.ru)
12. Издание о высоких технологиях (www.cnews.ru)
13. Polpred.com Обзор СМИ (<http://polpred.com/>)
14. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
15. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
16. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
17. Электронная библиотечная система Юрайт (<http://www.biblio-online.ru>)

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

Учебные и 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 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:

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

для обучающихся с нарушениями опорно-двигательного аппарата:

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

10. Материально-техническое обеспечение дисциплины (модуля)

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

К рабочей программе прилагаются:

Приложение 1 – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю);

Приложение 2 – Методические указания для обучающихся по освоению дисциплины (модуля).