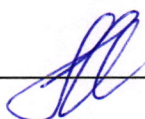


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной
образовательной программы

_____  Осипов Г.С.

"22" мая 2025 г

РАБОЧАЯ ПРОГРАММА

Дисциплины

Б1.В.08 «Основы информационной безопасности»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

01.03.02 Прикладная математика и информатика

профиль

Системное программирование и компьютерные технологии

Квалификация

Бакалавр

Форма обучения

очная

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск
2025

Рабочая программа дисциплины «Основы информационной безопасности» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.03.02 Прикладная математика и информатика.


Программу составил(и):

И. К. Мазур, доцент кафедры информатики



Рабочая программа дисциплины «Основы информационной безопасности» утверждена на заседании кафедры информатики, протокол № 9 от 22 мая 2025 г.

Исполняющий обязанности
заведующего кафедрой информатики

 Осипов Г.С.

1. Цель и задачи дисциплины

Цель дисциплины

Целью дисциплины является изучение принципов обеспечения информационной безопасности государства и организаций, подходов к анализу угроз его информационной инфраструктуры и освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах, а также формирование фундаментальных знаний в области информационной безопасности.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
- изучение видов защищаемой информации, угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных войн;
- изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;
- приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации, использовании современной научно-технической литературой для решения задач по вопросам защиты информации;
- приобретение навыков анализа информационной инфраструктуры государства с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к разделу вариативных дисциплин подготовки студентов по направлению подготовки бакалавров 01.03.02 «Прикладная математика и информатика».

Пререквизиты дисциплины:

Для освоения данной дисциплины студент должен владеть основными понятиями дисциплин Теоретические основы информатики, Компьютерные сети и телекоммуникации.

Постреквизиты дисциплины:

Освоение данной дисциплины должно подготовить студентов к профессиональной деятельности в области информационной безопасности, а также подготовить к прохождению технологической практики, написанию выпускной квалификационной работы, ведению научно-исследовательской работы.

3. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-1	Способен разрабатывать, изменять и согласовывать архитектуры программного обеспечения с системным аналитиком и архитектором программного обеспечения	ПКС-1.1. Знать существующие архитектуры программного обеспечения; ПКС-1.2. Уметь использовать существующие архитектуры программного обеспечения;

		ПКС-1.3. Иметь навыки разработки и программного обеспечения различных архитектур
--	--	--

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет **3** зачетные единицы (**108** академических часов).

Вид работы	Трудоемкость, акад. часов	
	семестр	всего
	7	
Общая трудоемкость	108	108
Контактная работа:	52	52
Лекции (Лек)	16	16
Лабораторные работы (Лаб)	32	32
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	0	0
Самостоятельная работа:	56	56
- самостоятельное изучение разделов (перечислить);	0	0
- самоподготовка (проработка и повторение лекционного материала, материала учебников и учебных пособий);	16	16
- подготовка к лабораторным занятиям;	32	32
- подготовка к коллоквиумам;	0	0
- подготовка к промежуточной аттестации и т.п.)	8	8

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
		семестр	контактная			Самостоятельная работа	
			Лекции	Практические занятия	Лабораторные занятия		
1.	Информационная безопасность в системе национальной безопасности Российской Федерации	7	2		2	4	Устный опрос по теме лекции. Проверка домашнего задания.

2.	Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации. Государственная тайна. Государственная система защиты информации.		2		6	8	Устный опрос по теме лекции. Проверка домашнего задания.
3.	Методологические основы защиты информации		2		6	10	Устный опрос по теме лекции. Проверка домашнего задания.
4.	Угрозы информационной безопасности		4		8	10	Устный опрос по теме лекции. Проверка домашнего задания.
5.	Построение систем защиты информации		4		6	10	Устный опрос по теме лекции. Проверка домашнего задания.
6.	Нормативно правовое регулирование защиты информации		2		4	6	Устный опрос по теме лекции. Проверка домашнего задания.
7.	<i>зачет</i>					8	
	<i>итого</i>		16		32	56	

4.3. Содержание разделов дисциплины

Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации

Понятие информационной безопасности. Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Информационная безопасность и информационное противоборство. Общие методы обеспечения информационной безопасности Российской Федерации. Методы и средства обеспечения безопасности компьютерных систем. Основные направления обеспечения информационной безопасности объектов информационной сферы государства.

Тема 2. Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации. Государственная тайна. Государственная система защиты информации.

Информация как объект правовых отношений. Общедоступная информация. Информация ограниченного доступа. Конфиденциальная информация: коммерческая тайна; служебная тайна; профессиональная тайна; личная тайна; семейная тайна; персональные данные. Государственная тайна.

Тема 3. Методологические основы защиты информации

Методы и технологии защиты информации. Классификация методов и средств защиты информации. Антивирусная защита. Системы идентификации и аутентификации. Системы разграничения доступа. Стенографические и криптографические методы. Технология электронной подписи. Методы обнаружения и блокирования угроз информационной безопасности. Методы защиты в операционных системах. Сетевые технологии защиты.

Тема 4. Угрозы информационной безопасности

Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.

Тема 5. Построение систем защиты информации

Определение и основные способы несанкционированного доступа. Методы защиты от несанкционированного доступа: организационные методы защиты; инженерно-технические методы защиты; построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Использование криптографических методов. Защита целостности информации при хранении; обработке; транспортировке. Построение систем защиты от угрозы отказа доступа к информации.

Тема 6. Нормативно правовое регулирование защиты информации

Нормативно-правовые документы в области информационной безопасности в РФ. Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации.

4.4. Темы и планы практических занятий

Лабораторное занятие №1 (2 ч.)

Тема Информационная безопасность в системе национальной безопасности Российской Федерации

Вопросы для обсуждения:

1. Понятие информационной безопасности.
2. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.
3. Виды угроз информационной безопасности Российской Федерации.
4. Источники угроз информационной безопасности Российской Федерации.
5. Информационная безопасность и информационное противоборство.
6. Основные направления обеспечения информационной безопасности объектов информационной сферы государства
7. Общие методы обеспечения информационной безопасности Российской Федерации.

Лабораторное занятие №2 (6 ч.)

Тема Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации. Государственная тайна. Государственная система защиты информации.

Вопросы для обсуждения:

1. Как разделяется информация в зависимости от порядка ее предоставления или распространения в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации»?
2. Как разделяется информация в зависимости от категории доступа в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации»?
3. Какова цель Федерального закона «О персональных данных»? Дайте определение понятию «персональные данные».
4. Определите понятия «доступ к информации» и «конфиденциальность информации»; «предоставление информации» и «распространение информации».
5. Какие отношения регулируются в Федеральном законе «О коммерческой тайне»? Дайте определение понятию «коммерческая тайна».
6. Какие виды информации можно отнести к основным объектам служебной тайны?
7. Каким требованиям должна отвечать информация, чтобы считаться профессиональной тайной?
8. Какие отношения регулирует Закон РФ «О государственной тайне»?

Лабораторное занятие №3 (6 ч.)

Тема Методологические основы защиты информации

Вопросы для обсуждения:

1. Какие методы защиты информации относятся к организационным?
2. Перечислите известные Вам технологические методы защиты информации.
3. Перечислите уровни защиты ИС.
4. Типовые методы защиты информации для различных направлений защиты.
5. Компьютерные вирусы: основные типы, фазы существования.
6. Классификация компьютерных вирусов
7. Организационные меры антивирусной защиты.
8. Типы методов аутентификации
9. Криптографические методы защиты информации. Классификация криптографических алгоритмов.
10. Сетевые технологии защиты.

Лабораторное занятие №4 (8 ч.)

Тема Угрозы информационной безопасности

Вопросы для обсуждения:

1. На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности).
2. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.
3. Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?
4. В каких системах на первом месте стоит обеспечение доступности информации?
5. В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?
6. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.

Лабораторное занятие №5 (6 ч.)

Тема Построение систем защиты информации

Вопросы для обсуждения:

1. В чем отличие терминов «Несанкционированный доступ» и «Нарушение конфиденциальности информации»?
2. Что понимается под утечкой информации?
3. Каким образом классифицируются каналы утечки информации?
4. Каким образом следует выбирать меры защиты конфиденциальности информации?
5. Дайте определение идентификации и аутентификации пользователя. В чем разница между этими понятиями?
6. Перечислите основные способы аутентификации. Какой, на Ваш взгляд, является наиболее эффективным?
7. Дайте определение шифра и сформулируйте основные требования к нему.
8. Поясните, что понимается под совершенным шифром.
9. Каким образом государство регулирует использование средств криптозащиты?
10. Каковы способы контроля целостности потока сообщений?
11. Как контролировать целостность сообщений при высоком уровне помех в каналах связи?
12. Как организован обмен документами, заверенными цифровой подписью?
13. В чем отличие и сходство обычной и цифровой подписей?
14. Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?
15. Почему проблемы контроля целостности данных относятся к проблемам информационной безопасности?

16. Что означает контроль целостности данных на уровне содержания? Приведите примеры.
17. Как обеспечить целостность данных при их хранении?
18. Что такое надежность и чем отличается надежность аппаратуры от надежности программного обеспечения?
19. Как изменяется надежность аппаратуры с течением времени?
20. Каковы способы повышения надежности аппаратуры и линий связи?

Лабораторное занятие №6 (4 ч.)

Тема Нормативно правовое регулирование защиты информации

Вопросы для обсуждения:

1. Нормативно-правовые документы в области информационной безопасности в РФ.
2. Акты федерального законодательства
3. Методические документы государственных органов России
4. Законе «Об информации, информационных технологиях и о защите информации»
5. Законодательные акты в области защиты информации.
6. Ответственность за нарушения в сфере информационной безопасности
7. Российские и международные стандарты, определяющие требования к защите информации.
8. Цели применения стандартов информационной безопасности.
9. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?
10. Для организаций какой сферы применимы стандарты серии ISO/IEC 27000?
11. Каковы отличительные черты стандартов серии ISO/IEC 27000?
12. Система сертификации РФ в области защиты информации.
13. Основные правила и документы системы сертификации РФ в области защиты информации.

5. Темы дисциплины (модуля) для самостоятельного изучения

Не предусмотрены

6. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1.	Информационная безопасность в системе национальной безопасности Российской Федерации	Лекция 1-2	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
2.	Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации. Государственная тайна. Государственная система защиты информации.	Лекция 3-4	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
3.	Методологические основы защиты информации	Лекции 5-6	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
4.	Угрозы информационной безопасности	Лекции 7-8	Традиционная лекция в ауд. с мультимедиа проектором

		Лабораторные занятия	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
5.	Построение систем защиты информации	Лекции 9-10	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
6.	Нормативно правовое регулирование защиты информации	Лекция 11	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия	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 дисциплины	Наименование практических работ
1.	«Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Виды угроз информационной безопасности Российской Федерации».
2.	«Источники угроз информационной безопасности Российской Федерации. Анализ информационной инфраструктуры государства».
3.	«Методы защиты от компьютерных вирусов» «Криптографические методы защиты. Электронная подпись.»
4.	«Классификация угроз информационной безопасности»
5.	«Построение систем защиты от угрозы нарушения конфиденциальности»
6.	«Обзор международных стандартов информационной безопасности» «Обзор отечественных стандартов информационной безопасности»

Примерные темы самостоятельной работы

1. Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
2. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности.
3. Интересы личности, общества и государства в информационной сфере.
4. Угрозы информационной безопасности Российской Федерации.
5. Внешние и внутренние источники угроз информационной безопасности государства.

6. Проблемы региональной информационной безопасности.
7. Информационное оружие, его классификация и возможности.
8. Методы нарушения конфиденциальности, целостности и доступности информации.
9. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
10. Компьютерная система как объект информационной безопасности.
11. Особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну.
12. Анализ современных подходов к построению систем защиты информации.
13. Общая характеристика средств видеонаблюдения и обнаружения оптических приборов.

Примерные темы рефератов:

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Правовая база обеспечения информационной безопасности личности (общества, государства).
3. Виды защищаемой информации.
4. Интересы личности (общества, государства) в информационной сфере.
5. Угрозы информационной безопасности Российской Федерации.
6. Внешние (внутренние) источники угроз информационной безопасности государства.
7. Проблемы региональной информационной безопасности.
8. Информационное оружие, его классификация и возможности.
9. Методы нарушения конфиденциальности (целостности, доступности) информации.
10. Правовые (организационно-технические, экономические) методы обеспечения информационной безопасности.
11. Компьютерная система как объект информационной безопасности.
12. Обеспечение информационной безопасности компьютерных систем.
13. Классификация и способы нейтрализации вредоносных программ;
14. Инфраструктура открытых ключей;
15. Криптографические способы защиты информации;
16. Защита информации в мобильных устройствах;
17. Источники угроз информационной безопасности РФ;
18. Доктрина информационной безопасности;
19. Виды угроз информационной безопасности Российской Федерации;
20. Понятие информационной безопасности;
21. Основы информационной безопасности;
22. Конфиденциальные документы;
23. Общие методы обеспечения информационной безопасности Российской Федерации;
24. Противодействие техническим каналам утечки информации;
25. Средства защиты информации. Генераторы акустического и электромагнитного шума.

Примерные вопросы к зачету.

1. Национальная безопасность.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.
3. Виды защищаемой информации.
4. Основные понятия и общеметодологические принципы теории информационной безопасности.
5. Роль информационной безопасности в обеспечении национальной безопасности государства.
6. Интересы личности в информационной сфере.
7. Интересы государства в информационной сфере.

8. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.
9. Угрозы информационному обеспечению государственной политики Российской Федерации.
10. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.
11. Угрозы безопасности информационных систем, как уже развернутых, так и создаваемых на территории России.
12. Внешние источники угроз.
13. Внутренние источники угроз.
14. Направления обеспечения информационной безопасности государства.
15. Проблемы региональной информационной безопасности.
16. Субъекты информационного противоборства.
17. Составные части и методы информационного противоборства.
18. Информационное оружие, его классификация и возможности.
19. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации.
20. Классификация и способы нейтрализации вредоносных программ;
21. Инфраструктура открытых ключей;
22. Криптографические способы защиты информации;
23. Защита информации в мобильных устройствах;
24. Источники угроз информационной безопасности РФ;
25. Доктрина информационной безопасности;
26. Виды угроз информационной безопасности Российской Федерации;
27. Понятие информационной безопасности;
28. Основы информационной безопасности;
29. Конфиденциальные документы;
30. Общие методы обеспечения информационной безопасности Российской Федерации;
31. Противодействие техническим каналам утечки информации;
32. Средства защиты информации.
33. Охарактеризуйте угрозы доступности информации.
34. Основные угрозы целостности информации.
35. Компьютерные вирусы и ИБ.
36. Назовите классификационные признаки и характерные черты компьютерных вирусов.
37. Перечислите виды антивирусных программ.
38. Назовите факторы, которые определяют качество антивирусных программ.
39. Уровни ИБ. Основные задачи и положения, решаемые на каждом уровне.
40. Методы определения требований к защите информации
41. Классификация требований к средствам защиты информации

8. 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 «зачтено» 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.
- 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.
- 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, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания

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

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература:

1. Мирошников, А. И. Основы 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>
2. Основы информационной безопасности : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2017. — 287 с. — ISBN 978-5-238-02857-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/72444.html>.
3. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/512268>
4. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю.
5. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/>
6. Галатенко, В. А. Основы 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>

9.2. Дополнительная литература:

1. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519079>
2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 с. — 978-5-4488-0091-7. — Режим доступа: <http://www.iprbookshop.ru/63800.html>
3. 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. — 978-5-94774-708-9. — Режим доступа: <http://www.iprbookshop.ru/62827.html>

9.3. 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 & Acceleration Server Standard Edition 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. ABBYY FineReader 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).
- 1.

9.4. 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>)

10. 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.

11. 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).