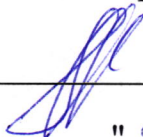


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной
образовательной программы

 _____ Осипов Г.С.
" 20 " 09 2024 г.

РАБОЧАЯ ПРОГРАММА

Дисциплины

Б1.В.01 Безопасные информационные технологии и системы

Уровень высшего образования

МАГИСТРАТУРА

Направление подготовки

09.04.03 Прикладная информатика

профиль

Искусственный интеллект и анализ данных

Квалификация

Магистр

Форма обучения

очная

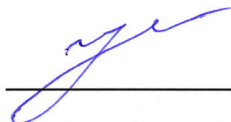
РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск
2024

Рабочая программа дисциплины Безопасные информационные технологии и системы составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 09.04.03 Прикладная информатика.

Программу составил:

Мазур И.К., доцент кафедры информатики



Рабочая программа дисциплины Безопасные информационные технологии и системы утверждена на заседании кафедры иностранного языка и страноведения протокол № 1 «20» сентября 2024 г.

Исполняющий обязанности
заведующего кафедрой информатики



Осипов Г.С.

1. Цель и задачи дисциплины

Цель дисциплины

Целью освоения дисциплины «Безопасные информационные технологии и системы» является формирование у студентов целостного представления о структуре и составе информационных систем, освоения технологии проектирования информационных систем, овладение навыками управления проектами создания информационных систем на всех стадиях жизненного цикла.

Задачи дисциплины

- освоение технологии проектирования и построения информационных систем;
- изучение программного и аппаратного обеспечения процессов моделирования и проектирования информационных систем;
- ознакомление с основами моделирования бизнес-процессов предметной области с помощью CASE-систем.

2. Место дисциплины в структуре образовательной программы

Дисциплина Безопасные информационные технологии и системы относится к вариативной части Блока 1 Дисциплины (модули) направления подготовки магистров подготовки 09.04.03 Прикладная информатика.

Пререквизиты дисциплины: Содержание дисциплины является логическим продолжением содержания дисциплин, изученных на этапе бакалавриата.

Постреквизиты дисциплины: знания и умения, полученные студентами при изучении дисциплины, применяются ими для последующего изучения дисциплин Интеграция информационных систем, Экономическое обоснование инвестиционных проектов, организация научного исследования, технологические (проектно-технологические) практики, подготовка к процедуре защиты и защита выпускной квалификационной работы и в их профессиональной деятельности.

3. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-1	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий	ПКС-1.1 - Знает виды моделей бизнес-процессов, требования к информационной системе, виды архитектур ИС; технологии программирования, тестирования и внедрения ИС; ПКС-1.2 - Умеет разрабатывать модели бизнес-процессов, требования к информационной системе, архитектуру ИС, применять технологии программирования, тестирования и внедрения ИС; ПКС-1.3 – Владеет методами разработки модели бизнес-процессов, требований к информационной системе, архитектур ИС, технологиями программирования, тестирования и внедрения ИС
ПКС-2	Способен управлять проектированием, процессом, разработки компьютерного программного обеспечения,	ПКС-2.1 - Знает методы управления проектированием, процессом, разработки компьютерного программного обеспечения, конфигурациями и выпусками

	конфигурациями и выпусками программного продукта	программного продукта ПКС-2.2 – Умеет применять методы управления проектированием, процессом, разработки компьютерного программного обеспечения, конфигурациями и выпусками программного продукта; ПКС-2.3 – Владеет методами управления проектированием, процессом, разработки компьютерного программного обеспечения, конфигурациями и выпусками программного продукта.
ПКС-3	Способен осуществлять организацию взаимодействия с заказчиком, планирования проекта ИС; руководить разработкой программного кода, верификацией и тестированием ИС	ПКС-3.1 - Знает методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.2 - Умеет применять методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.3 - Владеет методами организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС.

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет 6 зачетных единиц (216 академических часов).

Очная форма

Вид работы	Трудоемкость, акад. часов		
	семестр		всего
	1	2	
Общая трудоемкость	108	108	216
Контактная работа:	32	28	60
Лекции (Лек)	16	14	30
Лабораторные работы (Лаб)	16	14	30
Контактная работа в период теоретического обучения (КонтТО) (<i>Проведение текущих консультаций и индивидуальная работа со студентами</i>)	0		
Контактная работа в период промежуточной аттестации (КонтПА)	0		
Промежуточная аттестация (экзамен)	36	27	63
Самостоятельная работа:	40	53	93
- <i>самоподготовка (проработка и повторение лекционного материала, материала учебников и учебных пособий);</i>	20	20	40
- <i>подготовка к лабораторным занятиям;</i>	10	23	33
- <i>подготовка к промежуточной аттестации.</i>	10	10	20

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

№ п/п	Раздел дисциплины/ темы	Семестр	Виды учебной работы (в часах)				Формы текущего контроля успеваемости, промежуточной аттестации
			контактная			Самостоятель ная работа	
			Лекции	Практические занятия	Лабораторные занятия		
1.	Общая характеристика информационных систем Классификация информационных систем	1	2	-	2	6	Лабораторный практикум, контрольные вопросы, проверка домашнего задания
2.	Структура информационных систем. Модели жизненного цикла информационных систем		2	-	2	7	Лабораторный практикум, контрольные вопросы, проверка домашнего задания
3.	Безопасность информационных систем Информационное обеспечение информационной системы		2	-	2	7	Лабораторный практикум, контрольные вопросы, проверка домашнего задания
4.	Проектирование и совершенствование технологии обеспечения ин формационной безопасности.		4	-	4	13	Лабораторный практикум, контрольные вопросы, проверка домашнего задания
5.	Автоматизированные системы. Методология обеспечения информационной безопасности автоматизированных систем		6	-	6	7	Лабораторный практикум, контрольные вопросы, проверка домашнего задания
Экзамен							Вопросы к экзамену
Итого:			16	-	16	40	
6.	Анализ характеристик системы управления на основе информационного графа. Технология создания защищенных систем.	2	4	-	8	24	Лабораторный практикум, контрольные вопросы, проверка домашнего задания
7.	Анализ требований, угроз, уязвимостей объекта защиты. Особенности построения защищенных информационных систем»		4	-	4	14	Лабораторный практикум, контрольные вопросы, проверка домашнего задания
8.	Вычисление числовых		6	-	6	15	Лабораторный

	характеристик системы управления с помощью задания числовой функции на структурном графе системы						практикум, контрольные вопросы, проверка домашнего задания Защита индивидуальных учебных проектов
Экзамен							Вопросы к экзамену
Итого:		14	-	14	53		

4.4. Содержание разделов дисциплины

Раздел 1. Основные понятия информационных систем

Тема 1. Общая характеристика информационных систем Классификация информационных систем

Понятие экономической информационной системы. Структура однопользовательской и многопользовательской, малой и корпоративной ИС, локальной и распределенной ИС, состав и назначение подсистем. Основные особенности современных проектов ИС. Этапы создания ИС: формирование требований, концептуальное проектирование, спецификация приложений, разработка моделей, интеграция и тестирование информационной системы. Методы программной инженерии в проектировании ИС. Классификация информационных систем по масштабу, по сфере применения, по способу организации. История эволюции информационных систем. Этапы развития информационных систем. Развитие функциональности ИС и управления процессами предприятия.

Тема 2. Структура информационных систем Модели жизненного цикла информационных систем.

Информационное обеспечение ИС. Техническое обеспечение ИС. Математическое обеспечение ИС. Программное обеспечение ИС. Правовое обеспечение ИС. Организационное обеспечение ИС.

Понятие жизненного цикла ПО ИС. Процессы жизненного цикла: основные, вспомогательные, организационные. Содержание и взаимосвязь процессов жизненного цикла ПО ИС. Модели жизненного цикла: каскадная, модель с промежуточным контролем, спиральная. Стадии жизненного цикла ПО ИС. Регламентация процессов проектирования в отечественных и международных стандартах.

Тема 3. Безопасность информационных систем. Информационное обеспечение ИС.

Принципы и средства построения систем информационной безопасности в ИС. Этапы создания систем защиты информации в ИС. Моделирование системы защиты информации. Общая модель защиты информации в ИС. Внемашинное информационное обеспечение. Основные понятия классификации информации. Понятия и основные системы кодирования информации. Состав и содержание операций проектирования классификаторов. Система документации. Внутримашинное информационное обеспечение. Проектирование экраных форм электронных документов. Информационная база и способы ее организации.

Тема 4. Проектирование и совершенствование технологии обеспечения информационной безопасности

Этапы. Цели и задачи. Требования. Методы и способы. Проектирования. Дискуссия по теме «Проектирование и совершенствование технологии обеспечения информационной безопасности. Этапы. Цели и задачи.

Тема 5 Автоматизированные системы. Методология обеспечения информационной безопасности автоматизированных систем

Комплекс технических средств, обеспечивающих ввод, обработку, преобразование, хранение и передачу данных (различное техническое оборудование). Программное обеспечение (программы и программная документация). Специалисты, обслуживающие автоматизированные системы. Информация, размещенная на носителе

Тема 6 Анализ характеристик системы управления на основе информационного графа

Анализ требований, угроз, уязвимостей объекта защиты. Особенности построения защищенных информационных систем.

Тема 7 Анализ объекта автоматизации информационной системы

Основные этапы организационного анализа. Модели функции и функциональной области. Анализ функций организации. Этапы проектирования функциональной модели. Обследование организационной структуры организации.

Тема 8 Вычисление числовых характеристик системы управления с помощью задания числовой функции на структурном графе системы

4.4 Темы и планы лабораторных занятий

Тема 1. Общая характеристика информационных систем. Классификация информационных систем

Вопросы:

1. Понятие экономической информационной системы.
2. Структура однопользовательской и многопользовательской ИС
3. Структура локальной и распределенной ИС
4. Состав и назначение подсистем ИС.
5. Основные особенности современных проектов ИС.
6. Этапы создания информационной системы.
7. Методы программной инженерии в проектировании ИС.
8. История эволюции информационных систем. Этапы развития информационных систем.
9. Развитие функциональности ИС и управления процессами предприятия.
10. Классификация информационных систем.

Тема 2. Структура информационных систем. Модели жизненного цикла информационных систем.

Вопросы:

1. Информационное обеспечение ИС.
2. Техническое обеспечение ИС.
3. Математическое обеспечение ИС.
4. Программное обеспечение ИС.
5. Правовое обеспечение ИС.
6. Организационное обеспечение ИС.
1. Понятие жизненного цикла ПО ИС.
2. Процессы жизненного цикла: основные, вспомогательные, организационные.
3. Содержание и взаимосвязь процессов жизненного цикла ПО ИС.
4. Каскадная модель жизненного цикла ИС
5. Модель с промежуточным контролем
6. Спиральная модель жизненного цикла ИС.
7. Стадии жизненного цикла ПО ИС.
8. Регламентация процессов проектирования в отечественных и международных стандартах.

Тема 3. Безопасность информационных систем. Информационное обеспечение ИС

Вопросы:

1. Принципы и средства построения систем информационной безопасности в ИС.

2. Этапы создания систем защиты информации в ИС.
3. Моделирование системы защиты информации.
1. Общая модель защиты информации в ИС.
2. Внемашинное информационное обеспечение.
3. Основные понятия классификации информации.
4. Понятия и основные системы кодирования информации.
5. Состав и содержание операций проектирования классификаторов.
6. Система документации ИС.
7. Внутримашинное информационное обеспечение.
8. Проектирование экранных форм электронных документов.
9. Информационная база и способы ее организации.

Тема 4 Проектирование и совершенствование технологии обеспечения информационной безопасности

Вопросы:

1. Подходы к технико-экономическому обоснованию проектов.
2. Финансовые, капитальные и операционные затраты на разработку ИС.
3. Принципы выбора и использования ИТ в организации.
4. Гибкость и производительность ИТ.
5. Оптимизация затрат на ИС.
6. Управление рисками при создании ИС.
7. Разработка технического проекта.

Тема 5 Автоматизированные системы. Методология обеспечения информационной безопасности автоматизированных систем

Вопросы:

1. Архитектура предприятия и ее слои.
2. Информационные системы в управлении предприятием.
3. Структура и функции информационных систем, состав и назначение подсистем.
4. Архитектура корпоративных информационных систем.

Тема 6 Анализ характеристик системы управления на основе информационного графа. Технология создания защищенных систем.

Вопросы:

1. Регламентация процессов проектирования в отечественных и международных стандартах.
2. Процессы жизненного цикла ИС.
3. Содержание и взаимосвязь процессов жизненного цикла ПО ИС.
4. Стадии и этапы процесса канонического проектирования ИС.
5. Цели и задачи предпроектной стадии создания ИС.
6. Организация сбора материалов обследования.
7. Объекты обследования.
8. Методы организации обследования и сбора материалов обследования.
9. Понятие типового проекта, предпосылки типизации.
10. Методы типового проектирования.
11. Состав и содержание операций типового элементного проектирования ИС.
12. Функциональные пакеты прикладных программ ППП как основа ТПР.
13. Адаптация типовой ИС.
14. Методы и средства прототипного проектирования ИС.

Тема 7 Анализ требований, угроз, уязвимостей объекта защиты. Особенности построения защищенных информационных систем»

Вопросы:

1. Основные этапы организационного анализа.
2. Модели функции и функциональной области.
3. Анализ функций организации.
4. Этапы проектирования функциональной модели.

5. Обследование организационной структуры организации.
6. Динамическое описание компании.
7. Процессные потоковые модели.
8. Модели структур данных.

Тема 8 Вычисление числовых характеристик системы управления с помощью задания числовой функции на структурном графе системы

Вопросы:

1. Основные элементы процессного подхода.
2. Дерево целей.
3. Дерево функций.
4. Классификация бизнес-процессов.
5. Сравнение структурного и процессного подходов управления деятельностью предприятия.
6. Методология структурного моделирования.
7. Функциональные диаграммы.
8. Диаграммы потоков данных DFD.

5. Темы дисциплины для самостоятельного изучения

Контрольные задания

1. Что такое информация, субъекты информационных отношений?
2. Дайте определение Информационной технологии.
3. Компьютерная система-это...
4. Раскройте термин информационная безопасность
5. Что такое уязвимость?
6. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?
7. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?
8. Укажите модель управления доступом, к которой относится основная теорема безопасности.
9. Какие виды информации существуют в зависимости от категории доступа к ней?
10. Основные принципы системного подхода при создании сложных систем.
11. Перечислите основные объекты информационной безопасности. Дайте их определения.
12. Понятия ущерба, риска и угрозы.
13. Для чего нужна стандартизация в сфере информационной безопасности?
14. Какую информацию относят к секретной, конфиденциальной?
15. Перечислите основные риски ИБ. Дайте их определения.
16. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
17. Охарактеризуйте понятие большие данные.
18. Какую информацию относят к секретной, конфиденциальной?
19. Какие характеристики сотрудников и почему косвенно могут указывать на них как на потенциальных злоумышленников или нарушителей политики обеспечения информационной безопасности?
20. Какие применяются методы защиты информации от промышленного шпионажа?
21. Какие цели и задачи проведения тренингов по безопасности для сотрудников организации?
22. Какие организационные меры обеспечения безопасности Вы знаете?

23. Какие технические меры обеспечения безопасности Вы знаете?
24. Основные принципы обеспечения ИБ
25. Основные функции системы безопасности.
26. Защищаемая информация – это..

6. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие средства и формы обучения: мультимедийные лекции, компьютерный практикум, информационное моделирование, учебные проекты, имитация профессиональной деятельности.

При организации самостоятельной работы студентов используются средства и формы обучения: работа с учебной и научной литературой в электронных библиотеках, информационный поиск в интернете, выполнение учебных проектов, использование аудио и видео материалов для подготовки к лекционным и практическим занятиям, контроль знаний в тренинго-тестирующей системе.

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

Примерный перечень вопросов к экзамену за 1 семестр

1. Перечислите основные риски ИБ. Дайте их определения.
2. Какие требования предъявляются к комплексной системе безопасности объекта?
3. В чем суть гарантированного уничтожения?
4. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
5. Охарактеризуйте понятие большие данные.
6. Какую информацию относят к секретной, конфиденциальной?
7. Какие характеристики сотрудников и почему косвенно могут указывать на них как на потенциальных злоумышленников или нарушителей политики обеспечения информационной безопасности?
8. Какие применяются методы защиты информации от промышленного шпионажа?
9. Какие цели и задачи проведения тренингов по безопасности для сотрудников организации?
10. Какие организационные меры обеспечения безопасности Вы знаете?
11. Какие технические меры обеспечения безопасности Вы знаете?
12. Основные принципы обеспечения ИБ
13. Основные функции системы безопасности.
14. Основные принципы политики ИБ.
15. Какое свойство информации является наиболее актуальным при обеспечении ИБ? Дайте его определение.
16. Свойство информации при котором невозможно ее искажение...
17. Охарактеризуйте ИТ поиска информации.
18. Охарактеризуйте ИТ обработки данных.
19. Охарактеризуйте эмерджентные технологии.
20. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой

информации под угрозой материальной, административной и уголовной ответственности?

Примерный перечень вопросов к экзамену за 2 семестр

1. Элементы и подсистемы, управление и информация, самоорганизация.
2. Основные угрозы безопасности информации АС и их классификация.
3. Какие требования предъявляются к комплексной системе безопасности объекта?
4. В чем суть гарантированного уничтожения?
5. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
6. Охарактеризуйте понятие большие данные.
7. Какую информацию относят к секретной, конфиденциальной?
8. Какие характеристики сотрудников и почему косвенно могут указывать на них как на потенциальных злоумышленников или нарушителей политики обеспечения информационной безопасности?
9. Какие применяются методы защиты информации от промышленного шпионажа?
10. Какие цели и задачи проведения тренингов по безопасности для сотрудников организации?
11. Какие организационные меры обеспечения безопасности Вы знаете?
12. Какие технические меры обеспечения безопасности Вы знаете?
13. Основные принципы обеспечения ИБ
14. Основные функции системы безопасности.
15. Правовые методы обеспечения ИБ
16. Способы представления информации о правах доступа.
17. Характеристика качества
18. Показатели и критерии эффективности
19. Методические вопросы оценки эффективности сложных систем.
20. Дайте определение понятию «ядро безопасности»
21. Кратко опишите архитектуру защищенной системы.

8 Система оценивания планируемых результатов обучения

Основными критериями оценивания являются показатели выполнения самостоятельных заданий и лабораторных работ. Самостоятельные задания 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.

Критерии оценивания для экзамена:

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

– Оценка **«хорошо»** выставляется студенту, твердо знающему учебный 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 учебный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

– Оценка «**неудовлетворительно**» выставляется студенту, который не знает значительной части учебного 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
Текущее тестирование	1	3	3	9
Промежуточная аттестация (зачет, экзамен)			12	43
Итого за семестр			52	100

9 Учебно-методическое и информационное обеспечение дисциплины

9.1 Основная литература

1. Грекул, В. И. Проектирование информационных систем : учебник и практикум для вузов / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 423 с. — (Высшее образование). — ISBN 978-5-534-17841-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536901>

2. Зараменских, Е. П. Информационные системы: управление жизненным циклом : учебник и практикум для вузов / Е. П. Зараменских. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 497 с. — (Профессиональное образование). — ISBN 978-5-534-16179-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542807>

3. Брюхомицкий, Ю. А. Безопасность информационных технологий. В 2 частях. Ч.1 : учебное пособие / Ю. А. Брюхомицкий. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 171 с. — ISBN 978-5-9275-3571-2 (ч.1), 978-5-9275-3526-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/107943.html>

9.2 Дополнительная литература

1. Учебно-методическое пособие по дисциплине Методы и средства защиты компьютерной информации / составители А. Г. Симонян. — Москва : Московский технический университет связи и информатики, 2016. — 32 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/61498.html>

2. Кирпичников, А. П. Криптографические методы защиты компьютерной информации : учебное пособие / А. П. Кирпичников, З. М. Хайбуллина. — Казань : Казанский национальный исследовательский технологический университет, 2016. — 100 с. — ISBN 978-5-7882-2052-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/79313.html>

3. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/87992.html>

9.3 Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);

2. Microsoft VisualFoxPro Professional 9/0 Win32 Single Academic OPEN (бессрочная), (лицензия 49512935);
3. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661);
4. Microsoft Exchange Small Business CAL Russian Software Assurance Academic OPEN Level Device CAL Device CaL (бессрочная), (лицензия 60465661);
5. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351);
6. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351);
7. Microsoft Windows Professional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351);
8. Microsoft Windows Vista Business Russian Upgrade Academic OPEN, (бессрочная), (лицензия 41684549);
9. Microsoft Windows Server Datacenter 2003 R2 English Academic OPEN, (бессрочная), (лицензия 41684549);
10. Microsoft Internet Security & Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549);
11. Microsoft Windows Professional 7 Russian Upgrade Academic OPEN, (бессрочная), (лицензия 60939880);
12. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880);
13. Microsoft Windows Server Standart 2008 R2 Russian Academic OPEN, (бессрочная), (лицензия 60939880);
14. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880);
15. Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 1000-1499 Node 2 year Educational Renewal License (лицензия 2022-190513- 020932-503-526);
16. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD);
17. CorelDRAW Graphics Suite X5Education License ML (1-60), (бессрочная), (лицензия 4088083);
18. Ред ОС Рабочая станция
19. Ред ОС Сервер
20. СУБД Ред База Данных
21. Ред Виртуализация
22. Ред Адм
23. Справочно-правовая система "Консультант Плюс", сетевая студенческая версия версия «проф». В составе базы: «Судебная практика», «Сахалинский выпуск», «Законопроекты», «деловые бумаги», «международное право», «финансист», «эксперт-приложение», «документы СССР», «комментарии законодательства», «консультации для бюджетных организаций»;
24. Справочно-правовая система "Консультант Плюс", сетевая версия «Проф». В составе базы: «документы СССР», «бюджетные организации», «строительство», «суды общей юрисдикции», «сахалинский выпуск», «деловые бумаги», «корреспонденция счетов», «международное право», «эксперт-приложение»;
25. 1С-Бухгалтерия: 8.1. Регистрационный номер 801274453;
26. 1С-Университет. Регистрационный номер 8100238488;
27. «Антиплагиат. ВУЗ». Лицензионный договор №837;
28. 1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях. Сублицензионный договор № 180/2017;
29. Visual Studio Professional
30. СУБД MS SQL Server
31. Erwin Data Modeler

9.4 Профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- (<https://github.com/>)
2. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.nt.ru>)
3. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
4. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)
5. Интернет-университет информационных технологий (www.intuit.ru)
6. Онлайн среда разработки приложений (ideone.com)
7. Журнал «КомпьютерПресс» (www.compress.ru)
8. Издательство «Открытые системы» (www.osp.ru)
9. Издание о высоких технологиях (www.cnews.ru)
10. Справочно-правовая система «Консультант Плюс» (<http://www.consultant.ru>)
11. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
12. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
13. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
14. 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 проведения всех видов занятий (лекционных и практических) используются специально оборудованные кабинеты и аудитории, соответствующие действующим противопожарным правилам, средства для видеопросмотра, класс компьютерной техники. Для ведения занятий в достаточном количестве имеются компьютеры и офисная техника, учебники и учебные пособия в фондах университетской библиотеки. Имеется доступ к нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета.

Для самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями, справочно-правовой системой и возможностью доступа в глобальную сеть. Компьютерный класс оснащён аудиовизуальной техникой для показа лекционного материала и презентаций студенческих работ.

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).