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

Кафедра информатики

УТВЕРЖДАЮ
Проректор по учебной работе
_____ С.Ю. Рубцова
(подпись, расшифровка подписи)
" 16 " мая 2020 г.

РАБОЧАЯ ПРОГРАММА

Дисциплины

Б1.В.ДВ.09.01 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
2020 г.

Рабочая программа дисциплины Б1.В.ДВ.09.01 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):

Е.Н. Козлов, старший преподаватель кафедры информатики

Рабочая программа дисциплины Б1.В.ДВ.09.01 Основы информационной безопасности утверждена на заседании кафедры информатики, протокол № 10 от 12 мая 2020 г.

Заведующий кафедрой Г.С. Осипов

Рецензент:
А.В. Лоскутов,
ведущий научный сотрудник лаборатории цунами Института морской геологии и геофизики Дальневосточного отделения Российской академии наук, к.ф.-м.н.

1. Цель и задачи дисциплины

Цель дисциплины

Целью дисциплины является изучение принципов информационной безопасности предприятия, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- изучение основных принципов информационной безопасности предприятия;
- ознакомление с техническими и технологическими решениями, используемыми в данной области;
- выработка практических навыков аналитического и экспериментального исследования основных методов и средств, используемых в области, изучаемой в рамках данной дисциплины.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к части по выбору Блока 1 Дисциплины (модули) (Б1.В.ДВ.09.01) подготовки студентов по направлению подготовки бакалавров 01.03.02 «Прикладная математика и информатика».

Пререквизиты дисциплины:

Изучение данной дисциплины базируется на знании следующих дисциплин: Теоретические основы информатики; Операционные системы.

Постреквизиты дисциплины:

Основные положения данной дисциплины выступают опорой для подготовки к прохождению учебной, производственной и преддипломной практик, к научно-исследовательской работе.

3. Формируемые компетенции и индикаторы их достижения по дисциплине

Коды компетенции	Содержание компетенций	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.
ПКС-4	Способен проектировать программные интерфейсы	ПКС-4.1 Знать основные принципы проектирования программных интерфейсов.

		ПКС -4.2 Уметь использовать принципы проектирования программных интерфейсов. ПКС-4.3 Иметь навыки проектирования программных интерфейсов.

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет ***2*** зачетные единицы (***72*** академических часа).

Вид работы	Трудоемкость, акад. часов	
	семестр 8	всего
Общая трудоемкость	**72**	**72**
Контактная работа:	**52**	**52**
Лекции (Лек)	24	**24**
Лабораторные работы (Лаб)	24	**24**
Контактная работа в период теоретического обучения (КонтТО) *(Проведение текущих консультаций и индивидуальная работа со студентами)*	4	**4**
Контактная работа в период промежуточной аттестации (КонтПА)		
Промежуточная аттестация зачет		
Самостоятельная работа:	20	**20**
- самостоятельное изучение разделов (перечислить); *- самоподготовка (проработка и повторение лекционного материала, материала учебников и учебных пособий);* *- подготовка к лабораторным занятиям;* *- подготовка к промежуточной аттестации и т.п.)*	**20** 2 6 8 4	**20** **2** **6** **8** **4**

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

Очная форма обучения

№ 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		
8 семестр							
1.	Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации	**8**	2	0	2	2	Устный опрос по теме лекции. Проверка домашнего задания.
2.	Тема 2. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны		4	0	2	2	Устный опрос по теме лекции. Проверка домашнего задания.
3.	Тема 3. Общая характеристика КЗИ		4	0	4	2	Устный опрос по теме лекции. Проверка домашнего задания.
4.	Тема 4. Конфиденциальный документ		4	0	4	2	Устный опрос по теме лекции. Проверка домашнего задания.
5.	Тема 5. Испытание программного и аппаратного уровней КЗИ		4		4	2	Устный опрос по теме лекции. Проверка домашнего задания.
6.	Тема 6. Система физической защиты в КЗИ		4		4	2	Устный опрос по теме лекции. Проверка домашнего задания.
7.	Тема 7. Организация и аудит КЗИ		2		4	4	Устный опрос по теме лекции. Проверка домашнего задания.
	зачет					4	*Устный зачет*
	итого:	**104**	**24**	**0**	**24**	**20**	

4.3. Содержание разделов дисциплины

7 семестр

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.

Тема 2. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны

Основные направления обеспечения информационной безопасности объектов информационной сферы государства. Общие методы обеспечения информационной безопасности Российской Федерации. Методы и средства обеспечения безопасности компьютерных систем.

Тема 3. Общая характеристика КЗИ

Комплексная защита информации - сущность и задачи Стратегии комплексной защиты информации, стадии их создания Структура, характеристики принципы построения и этапы разработки комплексной защиты информации объекта.

Тема 4. Конфиденциальный документ

Критерии ценности информации и направления ее формирования. Выявление конфиденциальных сведений. Перечень конфиденциальных сведений. Носители

конфиденциальных данных. Конфиденциальные документы: состав, сроки, реквизиты. Угрозы конфиденциальному документу. Жизненный цикл открытого и конфиденциального документа. Документированная система защиты информации.

Тема 5. Испытание программного и аппаратного уровней КЗИ

Тестовые испытания программных средств защиты. Анализ сетевой топологии и установленных сервисов. Сетевое сканирование. Анализ трафика и сбор критичной информации программами пассивного анализа. Обнаружение уязвимостей по сигнатурам.

Тема 6. Система физической защиты в КЗИ

Система физической защиты - типовые задачи и способы ее реализации. Связь между функциями и основные характеристики системы физической защиты. Принципы обеспечения эффективности системы физической защиты, путь и стратегии нарушителя. Количественный и качественный анализ системы физической защиты. Диаграмма последовательности действий нарушителя. Применение технических, инженерных средств и сооружений охраны. Силы реагирования системы физической защиты, основные принципы их организации.

Тема 7. Организация и аудит КЗИ

Жизненный цикл организации работ по комплексной защите информации на объекте. Система анализа угроз и рисков комплексной защиты информации на объекте «Гриф». Система анализа и управления политикой информационной безопасности на объекте «Кондор» ISO 17799. Содержание и последовательность работ по комплексной защите информации на объекте ГОСТ 15408.

4.4 Темы и планы лабораторных занятий

8 семестр

Лабораторное занятие №1 (2 ч.)

Тема **Источники угроз информационной безопасности Российской Федерации**

Вопросы для обсуждения:

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
2. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.

Лабораторное занятие №2 (4 ч.)

Тема **Анализ информационной инфраструктуры государства**

Вопросы для обсуждения:

1. Документооборот государственных органов.
2. Электронно-цифровая подпись.

Лабораторное занятие №3 (4 ч.)

Тема **Технические средства и методы защиты информации**

Вопросы для обсуждения:

1. Межсетевые экраны.
2. Средства глушения сигнала.

Лабораторное занятие №4 (4 ч.)

Тема **Программно-аппаратные средства обеспечения информационной безопасности.**

Вопросы для обсуждения:

1. Использование брандмауэра в качестве базовой защиты информации.
2. VipNET.

Лабораторное занятие №5 (4 ч.)

Тема **Анализ сетевой топологии и установленных сервисов.**

Вопросы для обсуждения:

1. Программные средства анализа сетевой активности.
2. Технические средства анализа сети.

Лабораторное занятие №6 (4 ч.)

Тема **Оценка уязвимости коммутируемого доступа.**

Вопросы для обсуждения:

1. Уязвимости сетевого оборудования.
2. Уязвимости сетевых протоколов.

Лабораторное занятие №7 (2 ч.)

Тема **Аудит комплексной защиты информации предприятия.**

Вопросы для обсуждения:

1. Аудит помещения обработки данных.
2. Аттестация средств обработки персональных данных.

5. Темы дисциплины (модуля) для самостоятельного изучения

8 семестр (2 ч.)

№	Название темы	Количество часов
1.	Анализ современных подходов к построению систем защиты информации.	2

Вопросы для самоконтроля:

1. Перечислите современные способы борьбы с вредоносными программами.
2. Опишите алгоритм обнаружения вторжения в систему обработки данных.
3. Назовите законы, регулирующие защиту персональных данных в сети интернет.

6. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
	8 семестр		
	Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
	Тема 2. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
	Тема 3. Общая характеристика КЗИ	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
	Тема 4. Конфиденциальный документ	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
	Тема 5. Испытание программного и аппаратного уровней КЗИ	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
	Тема 6. Система физической защиты в КЗИ	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
	Тема 7. Организация и аудит КЗИ	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	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)

Примерный вариант контроля знаний по различным темам

1) Кто является основным ответственным за определение уровня классификации информации?

- Руководитель среднего звена
- Высшее руководство
- Владелец
- Пользователь

2) Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

- Сотрудники
- Хакеры
- Атакующие
- Контрагенты (лица, работающие по договору)

3) Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

- Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- Улучшить контроль за безопасностью этой информации
- Снизить уровень классификации этой информации

4) Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- Владельцы данных
- Пользователи
- Администраторы
- Руководство

5) Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

- Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
- Когда риски не могут быть приняты во внимание по политическим соображениям
- Когда необходимые защитные меры слишком сложны
- Когда стоимость контрмер превышает ценность актива и потенциальные потери

6) Что такое политики безопасности?

- Пошаговые инструкции по выполнению задач безопасности
- Общие руководящие требования по достижению определенного уровня безопасности
- Широкие, высокоуровневые заявления руководства
- Детализированные документы по обработке инцидентов безопасности

7) Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

- Анализ рисков
- Анализ затрат / выгоды
- Результаты ALE
- Выявление уязвимостей и угроз, являющихся причиной риска

8) Эффективная программа безопасности требует сбалансированного применения:

- Технических и нетехнических методов
- Контрмер и защитных механизмов
- Физической безопасности и технических средств защиты
- Процедур безопасности и шифрования

9) Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

- Внедрение управления механизмами безопасности
- Классификацию данных после внедрения механизмов безопасности
- Уровень доверия, обеспечиваемый механизмом безопасности
- Соотношение затрат / выгод

10) Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

- Только военные имеют настоящую безопасность
- Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
- Военным требуется больший уровень безопасности, т.к. их риски существенно выше
- Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

Форма контроля (8 семестр) **– *зачет***

Примерные вопросы к зачету (8 семестр)

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. Правовые, организационные и технические методы обеспечения информационной безопасности РФ.
21. Компьютерная система как объект информационной безопасности.
22. Общая характеристика методов и средств защиты информации.
23. Технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности КС.
24. Предмет, задачи и структура комплексной защиты информации.
25. Определение стратегии комплексной защиты информации. Виды стратегии: оборонительная, наступательная, упреждающая.
26. Определение структуры КЗИ. Основные характеристики КЗИ.
27. Этапы построения КЗИ по видам стратегий. Жизненный цикл построения КЗИ.
28. Основные критерии ценности информации.
29. Критерии анализа информационных ресурсов. Ущерб от утраты.
30. Определение Перечня конфиденциальных сведений. Основа и главная задача Перечня конфиденциальных сведений.
31. Документирование конфиденциальных сведений.
32. Состав и сроки хранения конфиденциального документа.
33. Действия службы безопасности по защите конфиденциальных документов
34. Основные этапы создания, исполнения, передачи, хранения и уничтожения документа. Отличия конфиденциального документооборота.
35. Документированная система защиты информации.
36. Способы защиты: сдерживание, обнаружение, задержка и реагирование. Показатели их эффективности.
37. Частота ложных тревог. Особенности восприятия информации обнаружения человеком.
38. Путь и стратегии нарушителя.
39. Критическая точка обнаружения нарушителя.
40. Модель территории объекта охраны.
41. Определение уровней защиты, параметров обнаружения и задержки.
42. Определения и область применения ИТСО. Виды и основные характеристики средств охраны.
43. Организация и структура охраны в Российской Федерации. Нормативные документы обеспечения охраны.
44. Жизненный цикл организации работ по комплексной защите информации на объекте**.**
45. Система анализа угроз и рисков комплексной защиты информации на объекте «Гриф»**.**
46. Система анализа и управления политикой информационной безопасности на объекте «Кондор» ISO 17799**.**
47. Содержание и последовательность работ по комплексной защите информации на объекте ГОСТ 15408

8. Система оценивания планируемых результатов обучения

Критерии оценивания

Критерием оценивания является выполнение 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.

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

– оценка «зачтено» выставляется студенту, который твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.

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*	4	12
Промежуточная аттестация (зачет)			*20*	*43*
Итого за семестр */зачет*			*60*	*100*

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература

1. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. – Электрон. текстовые данные. – М. : Евразийский открытый институт, 2012. – 311 c. – 978-5-374-00301-7. – Режим доступа: http://www.iprbookshop.ru/10677.html
2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 446 c. – 978-5-4488-0091-7. – Режим доступа: http://www.iprbookshop.ru/63800.html
3. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. – Электрон. текстовые данные. – Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. – 113 c. – 978-5-9585-0603-3. – Режим доступа: http://www.iprbookshop.ru/43183.html

9.2. Дополнительная литература

1. Гребенюк Е.И. Технические средства информатизации: учеб. для студентов сред. профес. образования /Е.И. Гребенюк, Н.А. Гребенюк. - 5-е изд., стер. - М.: Академия, 2009. - 267 с. - (Среднее профессиональное образование).
2. Куприянов А.И. Основы защиты информации: учебное пособие для студентов вузов /А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. - 2-е изд., стереотип. - М.: Академия, 2007. – 254 с. - (Высшее профессиональное образование).

3. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для студентов вузов /П.Б. Хорев. - 3-е изд., стереотип. - М.: Академия, 2007. – 255 с. - (Высшее профессиональное образование).
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 c. – 978-5-94774-708-9. – Режим доступа: http://www.iprbookshop.ru/62827.html
5. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В.Г. Спицын. – Электрон. текстовые данные. – Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011. – 148 c. – 978-5-4332-0020-3. – Режим доступа: http://www.iprbookshop.ru/13936.htm

Интернет-ресурсы:

1. https://www.securitylab.ru/
2. https://xakep.ru/
3. https://securelist.ru/

9.3. Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsift 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 Proffesional 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. Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 1000-1499 Node 2 year Educational Renewal License (лицензия 2022-190513-020932-503-526), срок пользования с 2019-05-13 по 2021-04-13
10. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
11. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
12. «Антиплагиат. ВУЗ». Лицензионный договор №194 от 22.03. 2018 года;

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. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)
14. Polpred.com Обзор СМИ (http://polpred.com/)
15. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)
16. Электронная библиотечная система IPRbooks (http://www.iprbookshop.ru)
17. Электронная библиотечная система Национальная электронная библиотека (https://нэб.рф)
18. 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, регулируемыми 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).

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

(Изменения и дополнения в РПД вносятся ежегодно и оформляются в данной форме. Изменения вносятся заменой отдельных листов (старый лист при этом цветным маркером перечеркивается, а новый лист с изменением степлером прикалывается к рабочей программе (хранится на кафедре), в электронной форме РПД должна быть актуализированной всегда, т.е. с внесенными изменениями.

При наличии большого количества изменений и поправок, затрудняющих понимание, возникших в связи с изменением нормативной базы ВО и другим причинам, проводится полный пересмотр РПД (т.е. выпускается новая РПД), которая проходит все стадии проверки и утверждения).

в рабочей программе *(модуле)* дисциплины_____
(название дисциплины)
по направлению подготовки *(специальности)*_____

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель подпись расшифровка подписи
дата

Зав. кафедрой подпись расшифровка подписи