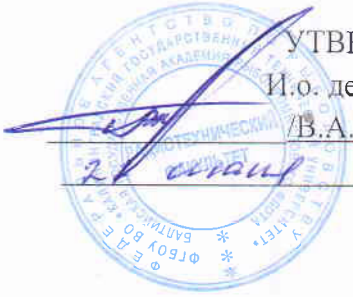
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
Балтийская государственная академия рыбопромыслового флота
ФГБОУ ВО «КГТУ»
БГАРФ



УТВЕРЖДАЮ
И.о. декана РТФ
/В.А. Баженов/
«21» апреля 2018 г.

Рабочая программа дисциплины
Безопасность операционных систем

базовой части образовательной программы
по специальности

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы
«Обеспечение информационной безопасности распределенных информационных систем»

Факультет/институт: Радиотехнический (РТФ)

Кафедра «Информационная безопасность»

Калининград 2018

Визирование РПД для исполнения в очередном учебном году

УТВЕРЖДАЮ:

и.о. декана РТФ_____ В.А.Баженов

«27» июня 2018 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2018 – 2019 учебном году на заседании кафедры «Информационная безопасность».

Протокол от «14» июня 2018 г. № 9

Заведующий кафедрой «Информационная безопасность» _____ /Великите Н.Я./

УТВЕРЖДАЮ:

и.о. декана РТФ_____ В.А.Баженов

«____» _____ 2019 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2019 – 2020 учебном году на заседании кафедры «Информационная безопасность».

Протокол от «___» _____2019 г. №

Заведующий кафедрой «Информационная безопасность» _____ /Великите Н.Я./

1. Цель освоения дисциплины.

1.1. Цель изучения дисциплины.

Теоретическая и практическая подготовка специалистов в области эксплуатации современных операционных систем (ОС) для обеспечения их эффективного применения с учетом требований информационной безопасности и привитие навыков в использовании методов обеспечения защиты информации в ОС.

1.2. Задачи изучения дисциплины.

К задачам дисциплины относятся ознакомление с основами ОС; изучение основ управления ОС; изучение средств обеспечения безопасности ОС.

1.3. Предметом изучения дисциплины являются следующие объекты:

Операционные системы, механизмы обеспечения безопасности операционных систем.

2. Результаты освоения дисциплины

Таблица 1 - Компетенции, формируемые в результате освоения дисциплины

Коды компетенций	Описание компетенций	Краткое содержание и структура компетенций.
ОПК-6	способностью применять нормативные правовые акты в профессиональной деятельности	знать: принципы моделирования поведения злоумышленника при осуществлении несанкционированного доступа в сети; классификация действий злоумышленника в соответствии с законодательством Российской Федерации; способы противодействия действиям злоумышленника допустимые нормами российского законодательства; структуру нормативно-технических и нормативно-методических документов по защите информации уметь: адаптировать функционирование служб безопасности распределенных систем обработки информации, параметры криптографической защиты передаваемых данных, определять сферы полномочий пользователей в соответствии с требованиями ФСТЭК и номами законодательства Российской Федерации, нормативными и методическими документы по технической защите информации, постановлениями правительства российской федерации; классифицировать злоумышленника в соответствии и определять степень их ответственности за нарушение работы и раскрытие конфиденциальных данных пользователей распределенных систем обработки информации; применять методы обеспечения информационной

		безопасности владеть: адаптировать функционирование служб безопасности распределенных систем обработки информации, параметры криптографической защиты передаваемых данных, определять сферы полномочий пользователей в соответствии с требованиями ФСТЭК и номами законодательства Российской Федерации, нормативными и методическими документы по технической защите информации, постановлениями правительства российской федерации; классифицировать злоумышленника в соответствии и определять степень их ответственности за нарушение работы и раскрытие конфиденциальных данных пользователей распределенных систем обработки информации; применять методы обеспечения информационной безопасности
ПК-1	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	знать: методики поиска, изучения, обобщения и систематизации научно-технической информации, виды нормативных и методических материалов в сфере профессиональной деятельности уметь: осуществлять поиск и обобщать, систематизировать научно-техническую информацию в области информационной защиты, использовать нормативные и методические материалы в сфере профессиональной деятельности владеть: методикой поиска, изучения, обобщения и систематизации научно-технической информации
ПК-3	способностью проводить анализ защищенности автоматизированных систем	знать: методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, методов оценки качества КСИБ, метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера уметь: определять риски информационной системы, возможные каналы НСД, применять экспертные структурные вопросники. Оценивать уяз-

		вимость информации. Анализировать пути проникновения в и нарушение работы в комплексных системах информационной безопасности (КСИБ). Создавать модель нарушителя. проводить вероятностный анализ методов и способов воздействия на КСИБ нарушителем владеть: методиками определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, средствами автоматизированного расчета рисков информационной системы, методами оценки уязвимости информации, средствами мониторинга и контроля состояния информационный среды КСИБ
ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать: классы угроз распределенной системы обработки информации; методику поиска актуальных уязвимостей распределенной системы; порядок создания модели нарушителя; определение базовой модели нарушителя; неформальной модели нарушителя; типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах; определение категории нарушителя; типологию нарушителей по характеру поведения Уметь: установить приоритеты целей безопасности для субъекта отношений; определить перечень актуальных источников угроз; определить перечень актуальных уязвимостей; оценить взаимосвязь угроз, источников угроз и уязвимостей; определить перечень возможных атак на объект; описать возможные последствия реализации угроз; создавать модель нарушителя; определять базовой модели нарушителя; определять категорию нарушителя; составлять содержательную модель нарушителей; создавать сценарии воздействия нарушителей; составлять математическая модель воздействия нарушителей на ресурсы распределенной системы обработки информации Владеть: навыками установки приоритетов целей безопасности для субъекта отношений; определить перечень актуальных источников

		угроз; определить перечень актуальных уязвимостей; оценить взаимосвязь угроз, источников угроз и уязвимостей; определить перечень возможных атак на объект; описать возможные последствия реализации угроз. создавать модель нарушителя; определять базовой модели нарушителя; определять категорию нарушителя; составлять содержательную модель нарушителей; создавать сценарии воздействия нарушителей; составлять математическая модель воздействия нарушителей на ресурсы распределенной системы обработки информации
ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	знать: Способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы. уметь: определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять целесообразность применения средств привязки программного обеспечения к аппаратному

		окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий; применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации. владеть: методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей; средствами защиты информации в процессе хранения и передачи данных и методами их тестирования; методикой определения эффективности предложенных решений с учетом снижения рисков
ПК-11	способностью разрабатывать политику информационной безопасности автоматизированной системы	знать: политику информационной безопасности автоматизированной системы уметь: разрабатывать политику информационной безопасности автоматизированной системы владеть: способностью разрабатывать политику информационной безопасности автоматизированной системы
ПК-13	способностью участвовать в проектировании средств защиты информации	знать: методы проектирования средств защиты информации уметь: разрабатывать и исследовать модели информационно-технологических ресурсов, проектировать средств защиты информации владеть: методами исследования информационно-технологических ресурсов, методами проектирования средств защиты информации

ПК-22	способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	знать: методы формирования политики информационной безопасности организации, методы формирования политики информационной безопасности информационных систем в организации, методы и способы контроля ее реализации уметь: формировать политику информационной безопасности организации, применять методы и способы контроля ее реализации, формировать политики информационной безопасности при эксплуатации информационных систем в организации. владеть: методами формирования политики информационной безопасности организации, методы и способы контроля ее реализации, методами формирования политики информационной безопасности информационных систем в организации,
ПК-24	способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	знать: методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности уметь: обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности владеть: методами обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности
ПК-25	способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и	знать: способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы; способы восстановление ресурсов автоматизированной системы работоспособности при возникновении нештатных ситуаций; методы и средства ограничения доступа к компонентам вычислитель-

	восстановление их работоспособности при возникновении нештатных ситуаций	ных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; способы защиты программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий. уметь: применять средства и системы защиты информационно-технологических ресурсов автоматизированной системы; восстанавливать ресурсы автоматизированной системы, их работоспособность при возникновении нештатных ситуаций; методы и средства ограничения доступа к компонентам вычислительных систем; применять методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; применять методы и средства хранения ключевой информации; осуществлять защиту программ от изучения, встраивать средства защиты в программное обеспечение; осуществлять защиту от разрушающих программных воздействий. владеть: методикой применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы; методикой восстановления ресурсов автоматизированной системы, их работоспособности при возникновении нештатных ситуаций; методами и средствами ограничения доступа к компонентам вычислительных систем; методикой применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; методикой применения методов и средств хранения ключевой информации; методикой защиты программ от изучения, методикой встраивания средств защиты в программное обеспечение; методикой защиты от разрушающих программных воздействий.
ПК-26	способностью администрировать подсистему информационной безопасности автоматизированной системы	знать: способы и механизмы администрирования подсистем информационной безопасности, критерии эффективности применения СЗИ уметь: администрировать подсистем информационной безопасности, применять критерии эффек-

		тивности применения СЗИ, автоматизировать работу по административной настройке СЗИ от НСД владеть: способами, механизмами администрирования средств защиты информации и средств, встроенных в ОС
ПК-28	способностью управлять информационной безопасностью автоматизированной системы	знать: способы и механизмы управления информационной безопасностью автоматизированной системы уметь: примять способы и механизмы управления информационной безопасностью автоматизированной системы владеть: способами, средствами и механизмами способы и механизмы управления информационной безопасностью автоматизированной системы
ПСК-7.4	способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	Знать: знать способы, правила и задачи удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах Уметь: применять способы и правила удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах владеть: способами удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах

Таблица 2 - Этапы формирования компетенций

Коды компетенций	Этапы формирования компетенций (разделы программы)
ПК-3	Назначение и функции операционных систем
ПК-11 ПК-13 ПК-22 ПК-24 ПК-25 ПК-26 ПК-28 ПСК-7.4	Автоматизация решения задач администрирования в ОС с использованием языков сценариев Управление задачами и ресурсами в ОС Аудит в ОС Разграничение доступа в ОС.

ОПК-6 ПК-1 ПК-4 ПК-6	Разграничение доступа в ОС. Требования к защите ОС

Таблица 3 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	принципы построения и функционирования, примеры реализаций современных операционных систем; функции ОС, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; критерии оценки эффективности и надежности средств защиты ОС; принципы организации и структуру подсистем защиты ОС семейств UNIX и Windows;
уметь	использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надежность защиты операционных систем; планировать политику безопасности операционных систем;
владеть	навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев; навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности.

3. Место дисциплины в структуре образовательной программы

Место дисциплины в структуре ООП:

Дисциплина относится к базовой части. Изучение дисциплины производится в тесной взаимосвязи с базовыми и вариативными математическими и естественнонаучными дисциплинами.

Требования к предварительной подготовке обучающегося:

«Информатика» - знать формы и способы представления данных в персональном компьютере, классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; уметь применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, дефрагментации и очистки диска и т.п.), пользоваться сетевыми средствами и внешними носителяи информаци для обмена данными; владеть навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией и т.п.), навыками поиска и обмена информацией в глобальной информационной сети Интернет;

«Языки программирования» - знать общие принципы построения и использования современных языков программирования высокого уровня, язык программирования высокого уровня (объектно-ориентированное программирование); уметь работать с интегрированной средой разработки программного обеспечения, использовать динамически подключаемые библиотеки; владеть навыками разработки, документирования, тестирования и отладки программ-

ного обеспечения в соответствии с современными технологиями и методами программирования.

«Основы информационной безопасности» - знать основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; владеть профессиональной терминологией в области информационной безопасности.

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее:

«Безопасность систем баз данных», «Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности».

4. Содержание дисциплины

Тема 1. Назначение и функции операционных систем
Тема 2. Управление задачами и ресурсами в ОС
Тема 3. Автоматизация решения задач администрирования в ОС с использованием языков сценариев
Тема 4. Требования к защите ОС
Тема 5. Разграничение доступа в ОС.
Тема 6. Аудит в ОС
Подготовка к сдаче и сдача экзамена Курсовой работы /КР

5. Объем (трудоемкость освоения) и структура дисциплины, формы аттестации

Таблица 1 - Объем (трудоемкость освоения) и структура дисциплины, формы аттестации **для очной формы обучения**

Номер и наименование разделов и тем	Объем учебной работы (час.)					
	Лекции	ЛЗ	ПЗ	СРС	Контроль	Всего
Семестр - шестой (216 час; 6 ЗЕТ).						
Тема 1. Назначение и функции операционных систем	6	12		8	6	32
Тема 2. Управление задачами и ресурсами в ОС	6	12		8	6	32
Тема 3. Автоматизация решения задач администрирования в ОС с использованием языков сценариев	6	12		8	6	32
Тема 4. Требования к защите ОС	6	12		10	6	34
Тема 5. Разграничение доступа в ОС.	6	12		10	6	34
Тема 6. Аудит в ОС	6	12		8	6	32
Подготовка к сдаче и сдача экзамена						
Подготовка КР				**20**		**20**
Всего в семестре	36	72		72	36	216
Итого по дисциплине	36	72		72	36	216

ЛЗ – лабораторные занятия,

ПЗ – практические занятия,
СРС – самостоятельная работа студента,
КР – курсовая работа,
КП – курсовой проект.

6. Лабораторные занятия (работы)

Таблица 2 - Лабораторные по **очной форме обучения**

№ ЛЗ	Тема дисциплины	Тема и содержание ЛЗ	Кол-во часов ЛЗ
Семестр – 6 (72 час.).			
1.	Тема 1.	Лабораторная работа №1. Работа с файлами и дисками в ОС Windows XP	6
2.	Тема 1	Лабораторная работа № 2. Работа с протоколом TCP/IP в ОС Windows XP	6
3.	Тема 2.	Лабораторная работа №3. Организация пакетных файлов и сценариев в ОС Windows XP	6
4.	Тема 2.	Лабораторная работа №4. Организация консоли администрирования в ОС Windows XP	6
5.	Тема 3.	Лабораторная работа №5. Мониторинг, оптимизация и аудит ОС WINDOWS XP	6
6.	Тема 3.	Лабораторная работа № 6. Работа с подсистемой безопасности в ОС WINDOWS XP	6
7.	Тема 4.	Лабораторная работа №7. Средства обеспечения безопасности ос семейства WINDOWS	6
8.	Тема 4	Лабораторная работа №8. Модель безопасности ОС Windows	6
9.	Тема 5	Лабораторная работа №9 ОС семейства unix. работа с файлами и каталогами. Управление пользователями. Защита файлов. резервное копирование данных	6
10.	Тема 5	Лабораторная работа №10. Создание и управление доменной политикой	6
11	Тема 5	Лабораторная работа №11. Конфигурирование доменной политики	6
12	Тема 6	Лабораторная работа №12. Конфигурирование и использование EFS. Восстановление данных	6
Всего за семестр:			72
Итого по дисциплине			72

7. Практические занятия

Практические занятия по дисциплине учебным планом не предусмотрены.

8. Самостоятельная работа студента

Таблица 3 - Самостоятельная работа студента по **очной форме обучения**

№	Вид (содержание) СРС	Кол-во часов СРС	Форма контроля, аттестации
Семестр – 6 (72 час.)			
1.	Парольные системы, аутентификация пользователей в ОС семейства Unix. Раз-	8	Текущий контроль: опрос, тест

	граничение доступа в ОС семейства Unix		
2.	Защита от программных вирусов в среде ОС семейства Unix	8	
3.	Парольные системы, аутентификация пользователей в ОС семейства Windows. Разграничение доступа в ОС семейства Windows	8	
4.	Аудит безопасности в ОС семейства Windows. Защита реестра ресурсов ОС семейства Windows	5	
5.	Защита от НСД к информации в доменах ОС семейства Windows	5	
6.	Системы обнаружения вторжений и виртуальные ловушки	5	
7.	Защита от НСД на рабочей станции с использованием программно-аппаратных комплексов	5	
8.	Системы поиска и уничтожения остаточной информации	4	
9.	Защита программного обеспечения от анализа	4	
10	Подготовка КР	20	
Всего за семестр:		72	
Итого по дисциплине		72	

9. Учебная литература и учебно-методическое обеспечение самостоятельной работы студента

Таблица 4 – Основная учебная литература

№ п/п	Автор(ы)	Заглавие	Город, издательство, год издания,	Кол-во в библ.
1.	Гордеев А.В.	Операционные системы: учебник для вузов	Спб.: Питер, 2009	50
2.	Иртегов Д.В.	Введение в операционные системы	Спб.: БХВ-Петербург, 2008	35
3.	Запечников С.В., Милославская Н.Г.	Информационная безопасность открытых систем: учебник для вузов. Т.2 : Средства защиты в сетях.	М.: Горячая линия-Телеком, 2008	15
4.	Назаров С.В.	Операционные среды, системы и оболочки. Основы структурной и функциональной организации: учебное пособие	М.: КУДИЦ-ПРЕСС, 2007	15

Таблица 5 – Дополнительная учебная литература

№ п/п	Автор(ы)	Заглавие	Город, издательство, год издания, кол-во стр.	Кол-во в библ.
1.	Мартемьянов, Ю. Ф.	Операционные системы. Концепции построения и обеспечения безопасности : учебное пособие	М. : Горячая линия - Телеком, 2017.	2
2.	Партыка Т.Л., Попов И.И.	Операционные системы, среды и оболочки	М.: Форум, 2009	5
3.	Мартемьянов, Ю. Ф.	Операционные системы. Концепции построения и обеспечения безопасности : учебное пособие для студентов, обучающихся по направлению «Информационные системы и технологии» / Ю. Ф. Мартемьянов, А. В. Яковлев, А. В. Яковлев . - 2-е изд.	М. : Горячая линия - Телеком, 2017. - 332 с.	2

10. Информационные технологии, программное обеспечение и Интернет-ресурсы дисциплины.

Электронная информационная образовательная среда БГАРФ ФГБОУ ВО «КГТУ»: http://83.171.112.16/login/index.php

Программное обеспечение

1.Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription (срок действия: три года)

2.Программное обеспечение распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU , по которой автор передаёт программное обеспечение в общественную собственность):

- Linux Ubuntu(Программы перехвата и анализа сетевых пакетов);
- VirtualBox (система виртуальных машин);

Интернет-ресурсы

Интернет-ресурсы, применяемые при изучении:

1. http://www.intuit.ru/
2. http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/
3. http://eLIBRARY.RU (Научная лицензионная библиотека eLIBRARY.RU договор №673-03/2017К от 23. 03.207г., бессрочно)

11. Материально-техническое обеспечение дисциплины

11.1. Общие требования к материально-техническому обеспечению дисциплины

11.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется учебная аудитория № 441.

Состав оборудования: столы учебные – 15 шт., стол преподавательский – 1 шт., стулья учебные – 30 шт., стул преподавательский – 1 шт., трибуна – 1 шт., экран раздвижной PROJECTA – 1 шт.; доска магнитно-маркерная – 1 шт.; мультимедийный проектор TOSHIBA – 1 шт.; ноутбук Acer Extensa – 1 шт.

Стенды: «Комплекс средств автоматизации деятельности оперативного персонала пункта централизованной охраны», «Требования и нормы проектирования по защите объектов от преступных посягательств». Специализированные стенды: СКУД «Стилпост»; «СИНЕРГЕТ» (цифровая система видеонаблюдения и аудиорегистрации).

Используется лицензионное программное обеспечение Microsoft Desktop Education, Microsoft Office 2016, Kaspersky Total Space Security Russian Edition.

11.1.2. Материально-техническое обеспечение для лабораторных занятий

Для проведения лабораторных занятий используется лаборатория технической защиты информации № 439.

Состав оборудования: столы учебные – 12 шт., стол преподавательский – 1 шт., стулья учебные – 17 шт., стул преподавательский – 1 шт., доска маркерная – 1 шт.

Компьютеры (системный блок, монитор, мышка, клавиатура), с установленным лицензионным программным обеспечением:

1.Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription (срок действия: три года)

2.Программное обеспечение распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU , по которой автор передаёт программное обеспечение в общественную собственность):

- Linux Ubuntu(Программы перехвата и анализа сетевых пакетов);
- VirtualBox (система виртуальных машин);

Для проведения лабораторных занятий используются компьютерный класс № 248.

Состав оборудования: столы учебные – 19 шт., стол преподавательский – 1 шт., стулья учебные – 23 шт., стул преподавательский – 1 шт., шкаф для учебных пособий – 1 шт., доска маркерная – 1 шт.; мультимедийный проектор ViewSonic – 1 шт.; ноутбук Acer Extensa – 1 шт.; проекционный экран Redleaf – 1 шт.

Компьютеры (системный блок, монитор ASUS, мышка, клавиатура), с установленным лицензионным программным обеспечением:

1.Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription (срок действия: три года)

11.1.3. Материально-техническое обеспечение для самостоятельной работы

Для организации самостоятельной работы обучающихся используется библиотечный фонд вуза, библиотека.

Помещение для самостоятельной работы – читальный зал, оснащенный компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза.

11.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов с нарушениями слуха предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована

компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов с нарушениями зрениями предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов с нарушениями опорно-двигательного аппарата используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

12 Фонд оценочных средств для проведения аттестации по дисциплине.

Аттестация по дисциплине (итоговая аттестация по дисциплине является промежуточной аттестацией по образовательной программе). Для рабочей программы разработано и утверждено приложение «Фонд оценочных средств для аттестации по дисциплине «Языки программирования».

13. Особенности преподавания и освоения дисциплины

13.1 Под образовательными технологиями будем понимать пути и способы формирования компетенций. В рамках дисциплины предусмотрены:

- лекции;
- лабораторные занятия, во время которых отрабатываются практические навыки, обсуждаются вопросы лекций, домашних заданий, проводятся контрольные и самостоятельные работы и т.д.;
- самостоятельная работа студентов, включающая усвоение теоретического материала, подготовку к практическим занятиям, выполнение индивидуальных заданий, курсовой работы, работа с учебниками, иной учебной и учебно-методической литературой, подготовка к текущему контролю успеваемости, к экзамену;
- тестирование по отдельным темам дисциплины;
- консультирование студентов по вопросам учебного материала.

13.2 Реализация программы предполагает использование интерактивных форм проведения лабораторных занятий. Проведение лабораторных занятий подразумевает обучение, построенное на групповой совместной деятельности студентов, в том числе с использованием персонального компьютера.

14. Методические указания по освоению дисциплины

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста):
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники:
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы:
- решить предложенные задачи, кейсы, ситуации;
- выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам:
2. Выполнение письменных контрольных и курсовых работ;
3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов:
4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) - важный элемент в работе студента по расширению и закреплению знаний;
- конспектирование лекций;
- получение консультаций для разъяснений по вопросам изучаемой дисциплины;
- подготовка ответов на вопросы тестов;
- подготовка к экзамену;
- выполнение контрольных, курсовых и дипломных работ;
- подготовка научных докладов, рефератов, эссе;
- анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с рабочей программой учебной дисциплины. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента не регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

Для овладения знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы);
- составление плана текста;
- конспектирование текста;
- выписки из текста;

• работа со словарями и справочниками;
• исследовательская работа;
• использование аудио- и видеозаписи;
• работа с электронными информационными ресурсами и ресурсами Internet:

Для закрепления и систематизации знании:

• работа с конспектом лекции (обработка текста);
• повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио-видеозаписей):
• составление плана и тезисов ответа;
• выполнение тестовых заданий;
• ответы на контрольные вопросы;
• аннотирование, реферирование, рецензирование текста;
• подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;
• работа с компьютерными программами;
• подготовка к сдаче экзамена;

Для формирования умений:

• решение задач и упражнений по образцу;
• решение вариативных задач и упражнений:
• выполнение расчетно-графических работ;
• решение ситуационных производственных (профессиональных) задач;
• участие в научных и практических конференциях;
• проектирование и моделирование разных видов и компонентов профессиональной деятельности;
• создание проспектов, проектов, моделей;
• экспериментальная работа, участие в НИР;
• рефлексивный анализ профессиональных умений с использованием аудио- видеотехники и компьютерных расчетных программ и электронных практикумов;
• подготовка курсовых и дипломных работ;

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

15. Сведения о рабочей программе и ее согласовании

Рабочая программа дисциплины представляет собой компонент образовательной программы специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и соответствует учебному плану, утвержденному «31» января 2018 г. и действующему для студентов, принятых на первый курс, начиная с 2014 года.

Автор(ы) программы:
ст. преподаватель кафедры информационной безопасности _____ /В.В.Подтопельный/

Программа дисциплины рассмотрена и одобрена на заседании кафедры «Информационная безопасность» (протокол № 9 от 14 июня 2018 г.)

Зав. кафедрой информационной безопасности _____ /Н.Я. Великите/

Рабочая программа дисциплины рассмотрена и одобрена на заседании методической комиссии радиотехнического факультета (протокол № 6 от 27 июня 2018 г.)

Председатель методической комиссии _____ / Жестовский А.Г.