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

УТВЕРЖДАЮ
И.о. декана радиотехнического факультета
_____ / В.А. Баженов /
27 июня 2018 г.

Рабочая программа дисциплины

Комплексное обеспечение информационной безопасности автоматизированных систем

вариативной 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 г.

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.

Цель изучения дисциплины "Комплексное обеспечение информационной безопасности автоматизированных систем" - заложить фундамент комплексного подхода к решению задач информационной безопасности, научить правильно проводить комплексный анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, приобрести навыки анализа угроз информационной безопасности, рассмотреть основные общеметодологические принципы комплексных систем обеспечения информационной безопасности; изучение методов и средств проектирования систем обеспечения информационной безопасности, методов оценки качества систем и моделей, аттестация средств.

1.2. Задачи изучения дисциплины.

- выявлять возможные способы нарушения информационной безопасности при работе автоматизированных систем обработки информации;
- в рамках задач обеспечения информационной безопасности решать вопросы использования радиоэлектронной аппаратуры и других технических средств;
- применять стандартные криптографические решения для зашиты информации и квалифицированно оценивать их качество;
- используя современные методы и средства разрабатывать и оценивать модели и политику безопасности;
- реализовывать системы зашиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем;
- практически решать задачи защиты программ и данных программно-аппаратными средствами: и давать оценку качества предлагаемых решений;
- определять и. измерять параметры опасных сигналов для технических каналов утечки информации и определять эффективность защиты от утечки информации;
- применять системный подход к обеспечению информационной безопасности в различных сферах деятельности, включая комплекс организационных мер, учитывающих особенности функционирования предприятия и решаемых им задач;
- проектировать и реализовывать комплексную систему защиты информации, оценивать ее качество.

1.3.Предметом изучения дисциплины являются следующие объекты:
обеспечение информационной безопасности автоматизированных систем

2. Результаты освоения дисциплины

Таблица 1 - Компетенции, формируемые в результате освоения дисциплины

Коды компетенций	Описание компетенций	Краткое содержание и структура компетенций.

ОК-4	способность использовать основы правовых знаний в различных сферах деятельности	знать: знать основные руководящие документы в области эксплуатации средств информационной безопасности, определения угроз и уязвимостей. уметь: применять основные руководящие документы в области эксплуатации средств информационной безопасности, определения угроз и уязвимостей. владеть: методикой основных руководящие документов в области эксплуатации средств информационной безопасности, определения угроз и уязвимостей.
ОПК-6	способностью применять нормативные правовые акты в профессиональной деятельности	знать: понятие и виды защищаемой информации по законодательству РФ правовые основы защиты информации с использованием технических средств законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации уметь: отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации применять действующую законодательную базу в области информационной безопасности разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и

		других организационно-распорядительных документов, анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития владеть: навыками разработки и использования нормативно-методическими материалами по регламентации вопросов информационной безопасности на предприятии (в организации)
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 уязвимость 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: 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 нарушите-

		лей; создавать сценарии воздействия нарушителей; составлять математическая модель воздействия нарушителей на ресурсы распределенной системы обработки информации
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-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	знать: методы инструментального мониторинга защищенности информации; способы и средства выявления каналов утечки информации уметь: проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации владеть: методами инструментального мо-

		ниторинга защищенности информации; способами и средствами выявления каналов утечки информации
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-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 эффективности применения СЗИ автоматизировать работу по административной настройке СЗИ от НСД владеть: способами, механизмами администрирования средств защиты информации и средств, встроенных в ОС

ПСК-7.2	способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	знать: методики анализа рисков информационной безопасности , способы и методы разработки, типы политики безопасности в распределенных информационных системах, методики разработки политики безопасности в распределенных информационных системах уметь: применять методики анализа рисков информационной безопасности , способы и методы разработки, определять типы политики безопасности в распределенных информационных системах, применять методики разработки политики безопасности в распределенных информационных системах владеть: владеть методиками анализа рисков информационной безопасности , способами и методы разработки, способами внедрения политики безопасности в распределенных информационных системах, методиками разработки политики безопасности в распределенных информационных системах

Таблица 2 - Этапы формирования компетенций

Коды компетенций	Этапы формирования компетенций (разделы программы)

ОК-4, ОПК-6, ПК-3, ПК-4, ПК-11, ПК-17, ПК-24, ПК-26, ПСК-7.2	Тема 1. Проблемы обеспечения комплексной защиты информации автоматизированных систем. Введение. Основные понятия, термины и определения. Предмет и задачи дисциплины. Введение. Цели и задачи обучения. Проблемы комплексного обеспечения информационной безопасности автоматизированных систем: состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ). Тема 2. Методология формирования задач защиты. Методология формирования задач защиты; интеграция средств и информационной безопасности в технологическую среду. Основные угрозы автоматизированным системам. Формирование целевой функции защиты информации. Тема 3. Этапы проектирования КСИБ и требования к ним Этапы проектирования КСИБ и требования к ним. Предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение. Функциональные и обеспечивающие подсистемы, технология, управление. Тема 4. Типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД). Типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД). Несанкционированный доступ к информации, возможные последствия. Классы каналов НСД АС и средств вычислительной техники. Тема 5. Мониторинг и контроль состояния окружающей среды. Параметры окружающей среды Мониторинг и контроль состояния окружающей среды; ведение специальной информационной базы данных КСИБ. Окружающая среда как потенциальный источник угроз автоматизированным системам и потенциальное повышение защиты АС. /Лек/ Параметры окружающей среды, шкалы, среды, воздействующие на технологический процесс и автоматизированную систему. Использование объединенной базы данных параметров окружающей среды для формирования особых функций защиты с элементами прогнозирования. Тема 6. Методы и методики проектирования. КСИБ. Моделирование как инструментарий проектирования, методика построения административного управления КСИБ. Целевая функция задач защиты информации. Критерии достижения требуемого уровня. Последовательность работ и особенности при проектировании системы защиты информации от НСД. Утечка информации за счет ПЭМИН. Типовые решения защиты от ПЭМИН. Моделирование процессов утечки информации, модели нарушителя, основные критерии, типовые этапы моделирования. Последователь-

	ность использования административного управления КСИБ. Методы и методики проектирования: методика выявления возможных каналов НСД, последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН. Тема 7. Методы и методики оценки качества КСИБ. Методы и методики оценки качества КСИБ: методы нормативного функционального наблюдения. Требования к эксплуатационной документации КСИБ. Метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера. Тема 8. Аттестация КСИБ по требованиям безопасности. Аттестация по требованиям безопасности; особенности эксплуатации КСИБ на объекте защиты. /Лек/ Организационно-функциональные задачи службы безопасности. /Лек/ Тема 9. Эксплуатационная документация КСИБ. Проведение аттестационных испытаний КСИБ. Требования к эксплуатационной документации КСИБ. Аттестация по требованиям безопасности; особенности эксплуатации КСИБ на объекте защиты, организационно-функциональные задачи службы безопасности. Состав и содержание эксплуатационной документации. Проведение аттестационных испытаний КСИБ. Заключение. Перспективы развития КСЗИ.

Таблица 3 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	содержание основных понятий по правовому обеспечению информационной безопасности; основы безопасности информационных систем; основы безопасности вычислительных сетей; основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; основные технические средства и методы защиты информации; основные программно-аппаратные средства обеспечения информационной безопасности.; способы расчета рисков информационной безопасности; особенности комплексного сочетания средств защиты информации; методы оценки качества КСИБ.
уметь	создавать необходимую информационную базу с использованием безопасных информационных технологий; эффективно использовать средства и способы безопасных информационных технологий в профессиональной деятельности.
владеть	навыками работы со средствами защиты информации, создавать и эксплуатировать системы защищенного электронного документооборота в организации; иметь навыки создавать необходи-

	мую информационную базу с использованием безопасных информационных технологий; эффективно использовать средства и способы безопасных информационных технологий в профессиональной деятельности.

3. Место дисциплины в структуре образовательной программы

Место дисциплины в структуре ООП:

Б1.В.ОД.5 Вариативная часть. Изучение дисциплины производится в тесной взаимосвязи с базовыми и вариативными математическими и естественнонаучными дисциплинами.

Требования к предварительной подготовке обучающегося:

Для успешного освоения дисциплины студент должен иметь базовую подготовку по дисциплинам: Безопасность вычислительных сетей, Безопасность систем баз данных, Безопасность операционных систем, Теоретические основы информационной и компьютерной безопасности, Криптографические методы защиты информации.

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

Дисциплина необходима для написания выпускной квалификационной работы, для подготовки и сдачи междисциплинарного итогового экзамена.

4. Содержание дисциплины

Тема 1. Проблемы обеспечения комплексной защиты информации автоматизированных систем.

Введение. Основные понятия, термины и определения. Предмет и задачи дисциплины. Введение. Цели и задачи обучения.

Проблемы комплексного обеспечения информационной безопасности автоматизированных систем: состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ).

Тема 2. Методология формирования задач защиты.

Методология формирования задач защиты; интеграция средств и информационной безопасности в технологическую среду. Основные угрозы автоматизированным системам. Формирование целевой функции защиты информации.

Тема 3. Этапы проектирования КСИБ и требования к ним

Этапы проектирования КСИБ и требования к ним. Предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение.

Функциональные и обеспечивающие подсистемы, технология, управление.

Тема 4. Типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД).

Типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД).

Несанкционированный доступ к информации, возможные последствия. Классы каналов НСД АС и средств вычислительной техники.

Тема 5. Мониторинг и контроль состояния окружающей среды. Параметры окружающей среды

Мониторинг и контроль состояния окружающей среды; ведение специальной информа-

ционной базы данных КСИБ. Окружающая среда как потенциальный источник угроз автоматизированным системам и потенциальное повышение защиты АС.

Параметры окружающей среды, шкалы, среды, воздействующие на технологический процесс и автоматизированную систему. Использование объединенной базы данных параметров окружающей среды для формирования особых функций защиты с элементами прогнозирования.

Тема 6. Методы и методики проектирования. КСИБ.

Моделирование как инструментарий проектирования, методика построения административного управления КСИБ. Целевая функция задач защиты информации. Критерии достижения требуемого уровня.

Последовательность работ и особенности при проектировании системы защиты информации от НСД. Утечка информации за счет ПЭМИН. Типовые решения защиты от ПЭМИН. Моделирование процессов утечки информации, модели нарушителя, основные критерии, типовые этапы моделирования. Последовательность использования административного управления КСИБ.

Методы и методики проектирования: методика выявления возможных каналов НСД, последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН.

Тема 7. Методы и методики оценки качества КСИБ.

Методы и методики оценки качества КСИБ: методы нормативного функционального наблюдения. Требования к эксплуатационной документации КСИБ.

Метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера.

Тема 8. Аттестация КСИБ по требованиям безопасности.

Аттестация по требованиям безопасности; особенности эксплуатации КСИБ на объекте защиты. Организационно-функциональные задачи службы безопасности.

Тема 9. Эксплуатационная документация КСИБ. Проведение аттестационных испытаний КСИБ.

Требования к эксплуатационной документации КСИБ. Аттестация по требованиям безопасности; особенности эксплуатации КСИБ на объекте защиты, организационно-функциональные задачи службы безопасности. Состав и содержание эксплуатационной документации. Проведение аттестационных испытаний КСИБ.

Заключение. Перспективы развития КСЗИ.

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 - 9 (216 час; 6 ЗЕТ).						
Тема 1. Проблемы обеспечения комплексной защиты информации автоматизированных систем.	4					4
Тема 2 Методология формирования задач защиты.	2	8		12		22
Тема 3. Этапы проектирования КСИБ и требования к ним.	2			12		14

Тема 4. Типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД).	2				6	8
Тема 4. Типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД).	4	4		12	6	26
Тема 5. Мониторинг и контроль состояния окружающей среды. Параметры окружающей среды.	4	10		24	6	44
Тема 6. Методы и методики проектирования. КСИБ	6	4		2	6	18
Тема 7. Методы и методики оценки качества КСИБ.	12	18		2	6	38
Тема 8. Аттестация КСИБ по требованиям безопасности.	4				6	10
Тема 9. Эксплуатационная документация КСИБ. Проведение аттестационных испытаний КСИБ.	4			28		14
Подготовка к сдаче и сдача экзамена						
Всего в семестре	44	44		92	36	216
Итого по дисциплине	44	44		92	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 – 9 (44 час.).			
1.	**Тема 2**	Формирования задач защиты. Табличные оценки рисков	8
2.	**Тема 4**	Определения каналов НСД АС и ущерба от реализации действий злоумышленника по найденным каналам.	4
3.	**Тема 5**	Расчет и анализ рисков информационной безопасности	10
4.	**Тема 6**	Моделирование процессов утечки информации, модели нарушителя, основные критерии, типовые этапы моделирования.	4
5.	**Тема 7**	Оценка эффективности СЗИ.	8
6.	**Тема 7**	Метод оценки уязвимости информации.	6
7.	**Тема 7**	Модель угроз и уязвимостей.	4
Всего за семестр:			44
Итого по дисциплине			44

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 – 9 (92 час.)			
1.	Методы защиты информации.	12	Текущий контроль: опрос, тест
2.	Особенности проектирования на современном уровне и синтез КСИБ.	12	
3.	Последствия от НСД для информационных систем различных типов.	12	
4.	Стандарты проектирования.	12	
5.	Построение административного управления КСИБ.	12	
6.	Нечеткие множества. Способы выявления и оценки уязвимостей	4	
7	Состав и содержание эксплуатационной документации. Регламентные документы службы безопасности.	28	
Всего за семестр:		92	
Итого по дисциплине		92	

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

9.1. Основная учебная литература

1. Кузнецов, А.В. Основы защиты информации : учеб. пособие для студентов специальности – КОИБАС/ В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с. (наличие в библиотеке БГАРФ - 110 экз.)
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М. : ИД «Форум», 2013. – 416 с. (наличие в библиотеке БГАРФ - 20 экз.)

9.2. Дополнительная учебная литература

1. Милославская, Н. Г. Управление рисками информационной безопасности : учебное пособие для студентов вузов, обучающихся по направлению подготовки 090900 «Информационная безопасность» (уровень - магистр) / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - М. : Горячая линия - Телеком, 2017. - 130 с. (наличие в библиотеке БГАРФ - 2 экз.)
2. Мельников, В. П. Информационная безопасность и защита информации: учеб. посо-бие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А. Клейменов. – Москва: Академия, 2008. – 336 с. (наличие в библиотеке БГАРФ - 31 экз.

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

Ресурсы информационно-телекоммуникационной сети «Интернет»:
- «Консультант Плюс» (www.consultant.ru);
- «Гарант» (www.garant.ru);
- http://www.rg.ru/dok/ [On-line] – опубликованные нормативные-правовые акты РФ;
- http://fstec.ru;
- http://www.confident.ru;
- http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/;
- http://eLIBRARY.RU (Научная лицензионная библиотека eLIBRARY.RU договор №673-03/2017К от 23. 03.207г., бессрочно)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем: программное обеспечение Microsoft Desktop Education.

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 № 440.

Состав оборудования: столы учебные – 10 шт., стол преподавательский – 1 шт., стулья учебные – 20 шт., стул преподавательский – 1 шт., доска маркерная – 1 шт.; мультимедийный проектор TOSHIBA – 1 шт.; ноутбук Acer Extensa – 1 шт.

Стенды охранно-пожарной сигнализации – 3 шт.

Стенды со специализированным оборудованием по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок и контроля эффективности защиты (подавитель микрофонов «Шаман», детектор поля ST 007, портативный измеритель частоты и мощности MPF-8000).

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.

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 специали-

ста):

• 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.