МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Рабочая программа дисциплины

Составитель:
Кандидат военных наук, доцент кафедры КЗИ *Д.Н. Баранников*

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ *Д.А. Митюшин*

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 23.03.2023

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – формирование основных знаний и умений в области технологий проектирования защищенных автоматизированных систем и соответствующими общепрофессиональными компетенциями в соответствии с ООП.
Задачи дисциплины:
– формирование знаний в области проектирования защищенных автоматизированных систем;
– уяснение основных понятий и определений, позволяющих осуществлять выбор и проектирование систем защиты;
– Рассмотреть особенности методов и средств проектирования, создания и сопровождения защищенных автоматизированных систем.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-4.1. Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.1 Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знать: • Нормативные и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
	ОПК-4.1.2 Умеет разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности)	Уметь: • Разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности)
	ОПК-4.1.3 Владеет навыками планирования мероприятий по обеспечению защиты информации и организацию работы персонала автоматизированной системы с учетом требований по защите информации	Владеть: • Навыками планирования мероприятий по обеспечению защиты информации и организацию работы персонала автоматизированной системы с учетом требований по защите информации
ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4.1 Знает критерии оценки защищенности автоматизированной системы, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Знать: • Критерии оценки защищенности автоматизированной системы, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	ОПК-4.4.2 Умеет контролировать уровень защищенности в автоматизированных системах, регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах	Уметь: • Контролировать уровень защищенности в автоматизировыанных системах, регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах
	ОПК-4.4.3 Владеет навыками проведения аудита защищенности информации	Владеть: • Навыками проведения аудита защищенности информации в автома-

	в автоматизированных системах	тизированных системах

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Проектирование защищенных автоматизированных систем» относится к обязательной части блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Электроника и схемотехника», «Аппаратные средства вычислительной техники», «Операционные системы», «Программно-аппаратные средства защиты информации», «Безопасность программного обеспечения автоматизированных систем».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: дисциплина является одной из завершающих обучение, «Преддипломная практика».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет _3_ з.е., 108академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
8	Лекции	**18**
8	Практическиезанятия	**24**
Всего:		**42**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _66_ академических часов.

3. Содержание дисциплины

Тема 1. Общая характеристика процесса проектирования защищенных автоматизированных систем

Базовые подходы к автоматизированному проектированию. Понятие системы автоматизированного проектирования. Определение процесса проектирования. Классификация систем автоматизированного проектирования. Подсистемы и виды обеспечения.
Требования к системам проектирования. Компоненты видов обеспечения. Современные системы проектирования защищенных автоматизированных систем, их возможности при проектировании. Использование систем автоматизированного проектирования на всех этапах проектирования систем.

Тема 2. Исходные данные для проектирования.

Обзор систем, возможности. Проблема выбора системы. Перспективы и направления развития. Возможности системы при проектировании автоматизированных систем. Интерфейс. Создание и оформление чертежей деталей и сборочных чертежей. Спецификации. Библиотеки элементов. Параметрические возможности. Возможности системы при проектировании автоматизированных систем. Параметрические возможности. Сложные элементы 3D-моделирования. Библиотеки элементов. Обмен данными между системами автоматизированного проектирования.

Тема 3. Организационные процессы создания автоматизированных систем

Организационные принципы. Этапы создания автоматизированных систем. Требования типизации проектных решений. Требования этапности создания автоматизированных систем. Экономические принципы создания автоматизированных систем. Дифференциация и интеграция.

Тема 4. Модели жизненного цикла автоматизированных систем

Понятие жизненного цикла. Стадии жизненного цикла. Формирование набора документов и технических решений, которые являются исходными для последующих решений.функциональные и информационные модели. Жизненный цикл программного обеспечения. Вспомогательные процессы жизненного цикла защищенных автоматизированных систем. Процесс управления проектами. Процесс создания инфраструктуры. Процесс усовершенствования. Процесс обучения. Эксплуатация и сопровождение.

Тема 5. Особенности проектирования комплексной системы информационной безопасности

Анализ рынка. Требования к качеству обмена информацией и уровню ее защиты. Принципы и подходы проектирования защищенных автоматизированных систем. Интегрирование средств, методов и мероприятий в единый, целостный механизм. Условиями обеспечения безопасности. Общие рекомендации по проектированию комплексной системы информационной безопасности.

Тема 6. Проектирование системы защиты от НСД

Модель злоумышленника.Модель угроз. Определение направлений. Политика безопасности. Функции защиты информации. Программное решение. Сценарии настроек. Процедура входа в систему. Ценовая политика. Этапы проектирования. Обеспечение защиты информации на этапах проектирования системы защиты от НСД. Участники проектирования. Типовое содержание работ в части создания защищенной автоматизированной системы. Организационно-методическое руководство работами по созданию, изготовлению, обеспечению и эксплуатации. Контроль выполнения требований.

Тема 7. Аттестация автоматизированной системы по требованиям безопасности

Аттестация объектов информатизации.Состав нормативной и методической документации для аттестации конкретных автоматизированных систем. Государственный контроль и надзор, инспекционный контроль за проведением аттестации. Опыт зарубежных стран. Модель нарушителя. Анализ требований безопасности. Анализ состава исходных данных. Определение границ проведения аттестации и распределение работ. Области повышенного внимания. Документирование плана проведения аттестации. Документы, содержащие требования безопасности. Единые критерии оценки безопасности информационных технологий. Методологии реализации механизмов безопасности. Подготовка отчетных документов по результатам аттестации.

4. Образовательные технологии

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	Общая характеристика процесса проектирования защищенных автоматизированных систем	Лекция 1. Самостоятельная работа	Традиционная лекция с использованием презентаций, опрос Подготовка к занятиям с использованием ЭБС
2	Исходные данные для проектирования.	Лекция 2. Практическое занятие 1.	Традиционная лекция с использованием презентаций, опрос Занятия с использованием специализи-

			рованного ПО
		Самостоятельная работа	Подготовка к занятиям с использованием ЭБС
3	Организационные процессы создания автоматизированных систем	Лекция 3.	Традиционная лекция с использованием презентаций, опрос
		Практическое занятие 2.	Занятия с использованием специализированного ПО
		Самостоятельная работа	Подготовка к занятиям с использованием ЭБС
4	Модели жизненного цикла автоматизированных систем	Лекция 4.	Традиционная лекция с использованием презентаций Тестирование
		Практическое занятие 3.	Занятия с использованием специализированного ПО
		Самостоятельная работа	Подготовка к занятиям с использованием ЭБС
5	Особенности проектирования комплексной системы информационной безопасности	Лекция 5.	Традиционная лекция с использованием презентаций Тестирование
		Практическое занятие 4.	Занятия с использованием специализированного ПО
		Самостоятельная работа	Подготовка к занятиям с использованием ЭБС
6	Проектирование системы защиты от НСД	Лекция 6.	Традиционная лекция с использованием презентаций Тестирование
		Практическое занятие 5.	Занятия с использованием специализированного ПО
		Самостоятельная работа	Подготовка к занятиям с использованием ЭБС
7	Аттестация автоматизированной системы по требованиям безопасности	Лекция 7.	Традиционная лекция с использованием презентаций
		Практическое занятие 6.	Занятия с использованием специализированного ПО
		Самостоятельная работа	Подготовка к занятиям с использованием ЭБС

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
– опрос (темы 1-3)	*4 балла*	*12 баллов*
– тестирование (темы 4-7)	*3 балла*	*12 баллов*
– практическоезанятие(темы 1-6)	*6 баллов*	*36 баллов*
Промежуточная аттестация – экзамен (экзамен по билетам)		*40 баллов*
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 –67	удовлетворительно		D
50 –55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
82-68/ C	хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

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

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

1. Основные средства и способы обеспечения информационной безопасности в автоматизированных системах. Принципы построения систем защиты информации
2. Понятие и классификация угроз безопасности автоматизированных систем
3. Базовая модель угроз безопасности информации. Методика оценки угроз безопасности информации
4. Последовательность стадий и содержание этапов разработки автоматизированных систем в защищенном исполнении
5. Содержание этапов проектирования автоматизированных систем в защищенном ис-полнении. Требования по защите сведений о создаваемой АС.

6. Модели данных, систем и процессов защиты информации в автоматизированных системах. Технологии автоматизированного проектирования автоматизированных информационных систем.
7. Понятие и архитектура распределенных автоматизированных систем. Особенности способов и средств защиты информации в распределенных автоматизированных системах.
8. Перечислить комплекс работ по созданию защищенных автоматизированных систем
9. Проектирование системы защиты информации
10. Где отражаются результаты проектирования?
11. Разрабатываемые организационно-распорядительные документы должны определять
12. Предварительные испытания и опытная эксплуатация
13. Сопровождение спроектированных защищенных автоматизированных систем в ходе эксплуатации объекта информатизации
14. Перечень информации, подлежащей защите, в ходе проектирования
15. Требования к качеству готового продукта. Оснащенность технологического процесса необходимыми средствами контроля параметров.
16. Стадии и этапы проектирования защищенных автоматизированных систем
17. Назначение технологического регламента процесса.
18. Порядок сбора данных, необходимых для проектирования защищенных автоматизированных систем
19. Алгоритм проектированиязащищенных автоматизированных систем
20. Требования, формулируемые в техническом задании при проектировании защищенных автоматизированных систем
21. Принципы и методы проектирования защищённых автоматизированных систем
22. Требования и рекомендации по защите конфиденциальной информации, обрабатываемой в автоматизированных системах
23. Алгоритм построения автоматизированной системы в защищенном исполнении
24. Специальное исследование, проводимое при проектировании защищенных автоматизированных систем
25. Техническое и эскизное проектирование защищенных автоматизированных систем
26. Разрешительная система доступа разработчиков, пользователей, эксплуатирующего персонала
27. Полномочия разработчиков, пользователей и эксплуатирующего персонала
28. Требования по предотвращению утечки защищаемой информации

Промежуточная аттестация (примерные вопросы к экзамену)

1. Системы автоматизированного проектирования
2. Этапы проектирования защищенных автоматизированных систем
3. Технические требования проектирования защищенных автоматизированных систем
4. Требования по защите информации к техническому обеспечению
5. Возможности системы при проектировании защищенных автоматизированных систем
6. Обмен данными между системами автоматизированного проектирования
7. Экономические принципы создания защищенных автоматизированных систем
8. Стадии жизненного цикла моделей при проектировании защищенных автоматизированных систем.
9. Вспомогательные процессы жизненного цикла защищенных автоматизированных систем
10. Процессы управления проектами
11. Принципы и подходы проектирования защищенных автоматизированных систем
12. Требования к качеству обмена информацией и уровню ее защиты
13. Принципы и подходы проектирования защищенных автоматизированных систем
14. Общие рекомендации по проектированию комплексной системы информационной безопасности

15. Обеспечение защиты информации на этапах проектирования системы защиты от НСД
16. Вспомогательные процессы жизненного цикла защищенных автоматизированных систем
17. Типовое содержание работ в части создания защищенной автоматизированной системы
18. Организационно-методическое руководство работами по созданию, изготовлению, обеспечению и эксплуатации
19. Государственный контроль и надзор, инспекционный контроль за проведением аттестации
20. Единые критерии оценки безопасности информационных технологий
21. Содержание разделов технического задания при проектировании защищенных автоматизированных систем
22. Стадии и этапы создания защищенных автоматизированных систем
23. Подготовительные этапы подготовки защищенных автоматизированных систем к проведению предварительным и приемочным испытаниям
24. Перечень организаций, участвующих в работах по созданию защищенных автоматизированных систем
25. Техническое задание на создание защищенной автоматизированной системы
26. Требования, предъявляемые к системе при проектировании защищенной автоматизированной системы
27. Порядок разработки, согласования и утверждения технического задания при проектировании защищенных автоматизированных систем
28. Особенности испытаний и применения автоматизированной системы в защищенном исполнении
29. Обслуживание средств защиты информации прикладного и системного программного обеспечения
30. Обслуживание систем защиты информации в автоматизированных системах

Примерные тестовые задания

1. Проектирование технологии представляет собой ...

a. информационный процесс, связанный с практической деятельностью менеджера по закупке сырья.

b. информационный процесс, связанный с интеллектуальной деятельностью менеджеров по продаже и характеризующейся различными видами связей: аналитическими выражениями, логическими и иерархическими связями.

c. информационный процесс, связанный с интеллектуальной деятельностью технолога и характеризующейся различными видами связей: аналитическими выражениями, логическими и иерархическими связями.

d. информационный процесс, связанный с интеллектуальной деятельностью маркетолога и характеризующейся различными видами связей: аналитическими выражениями, логическими и иерархическими связями.

2. Оптимальное проектирование нацелено на ...

a. удовлетворение разных, порой противоречивых потребностей людей.

b. создание эффективно работающего объекта.

c. базируется на системном подходе.

d. разработку функциональных показателей качества и показателей надёжности.

3. В российской практике проектирование ведётся ...

a. Поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-68.

b. в соответствии со стадиями, регламентированными ГОСТ 2.103-98.

c. поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-78.

d. поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-98.

4. Техническое задание ...

a. исходный документ для разработки изделия.

b. исходный документ для испытания изделия.

c. ничего из перечисленного.

d. исходный документ для разработки и испытания изделия.

9. Системное проектирование ...

a. Обоснованный выбор окончательного варианта.

b. Удовлетворение разных, порой противоречивых потребностей людей.

c. Базируется на системном подходе.

d. Создание эффективно работающего объекта.

5. По подходу к проектированию различают ...

a. Оптимальное проектирование.

b. Все перечисленное.

c. Функциональное проектирование.

d. Системное проектирование.

6. Эскизный проект -это ...

a. совокупность конструкторских документов, содержащих технические и технико-экономические обоснования целесообразности дальнейшей разработки проекта.

b. совокупность конструкторских документов, которые должны содержать принципиальные конструктивные решения, дающие общее представление об устройстве и принципе работы изделия, данные, определяющие назначение, основные параметры и габаритные размеры проектируемого изделия.

c. программный продукт, вырабатываемый в ходе бизнес-планирования.

d. нормативно-техническая информация (справочники, каталоги и т.п.).

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

основные

1. *Руководящий докумен*т. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3, свободный. – Загл. с экрана.

2. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.

3. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.

4. *Руководящий документ*. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный

ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.
5. Выписка из Приказа ФСТЭК России №76 от 02.06.2020 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к СТЗИ и СОБИТ» [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty/2126-vypiska-iz-trebovanij-po-bezopasnosti-informatsii-utverzhdennykh-prikazom-fstek-rossii-ot-2-iyunya-2020-g-n-76, свободный. – Загл. с экрана.
6. Приказ ФСТЭК России от 29.04.2021 г. № 77 [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/normotvorcheskaya/akty/53-prikazy/2270-prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77, свободный. – Загл. с экрана.
7. ГОСТ Р 58189–2018 Защита информации. Требования к органам по аттестации объектов информатизации [Электронный ресурс]. – Режим доступа : https://internet-law.ru/gosts/gost/69566/, свободный. – Загл. с экрана.
8. Нормативные требования к аттестации АС/ИС по ГОСТ–РО 0043-003-2012 года [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://safe-surf.ru/specialists/article/5255/642827/, свободный. – Загл. с экрана.
9. Приказ Минцифры России от 17.03.2020 №114 «Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/ , свободный. – Загл. с экрана.
10. Приказ Минцифры России от 28.12.2020 №777 «Об утверждении Рекомендаций по проведению сертификации оборудования связи, используемого в составе сети связи общего пользования, обеспечивающей функционирование значимых объектов критической информационной инфраструктуры» [Электронный ресурс] : Режим доступа : https://digital.gov.ru/ru/documents/7446/, свободный. – Загл. с экрана.
11. Приказ Минцифры России от 28.12.2020 №779 «Об утверждении организационно-технических мер по обеспечению информационной безопасности ресурсов сети связи общего пользования, используемых значимыми объектами критической информационной инфраструктуры» [Электронный ресурс] : Режим доступа : https://digital.gov.ru/ru/documents/7442/, свободный. – Загл. с экрана.
12. Приказ ФСТЭК России №106 о внесении изменений в требования о защите информации, содержащейся в государственных информационных системах (ГИС), от 28 мая 2019 года. [Электронный ресурс] : Режим доступа : https://fstec.ru/normotvorcheskaya/eksportnyj-kontrol/100-prikazy/2430-prikaz-fstek-rossii-ot-21-iyunya-2022-g-n-106, свободный. – Загл. с экрана.

Литература

Основная

1. Флоу, С. Занимайсяхакингом как невидимка. Искусство взлома облачных инфраструктур : руководство / С. Флоу ; перевод с английского В. С. Яценкова. — Москва : ДМК Пресс, 2023. — 272 с. — ISBN 978-5-97060-977-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/314924
2. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/288974
3. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. —

Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009
4. Музипов, Х. Н. Программно-технические комплексы автоматизированных систем управления : учебное пособие / Х. Н. Музипов. — Санкт-Петербург : Лань, 2022. — 164 с. — ISBN 978-5-8114-3133-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/213098
5. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837
6. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237770
7. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/

Дополнительная

1. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
2. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. http://rkn.gov.ru/ Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

2. Официальный сайт компании Microsoft [Электронный ресурс] : Режим доступа: http://www.microsoft.com/, свободный. – Загл. с экрана.

3. Центр разработки Microsoft [Электронный ресурс] : Режим доступа: http://www.msdn.microsoft.com/, свободный. – Загл. с экрана.

6.3. Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. Microsoft Office

3. Kaspersky Endpoint Security

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. CiscoPacketTracer v.7.2

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительныеметоды обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- 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:устройством для сканирования и чтения с камерой SARA CE;дисплеем Брайля PAC Mate 20;принтером Брайля EmBrailleViewPlus;
- 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.

9. Методические материалы

9.1 Планы практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.
Цельюпрактических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.
Тематикапрактических занятий соответствует программе дисциплины.

Практическая работа № 1. (6 ч)*Разработка технического задания*
Задания:
1. Определить требования к составу работ.
2. Определить показатели надежности и режимы функционирования.
3. Определить перспективы развития и модернизации системы

Практическая работа № 2 (6 ч)*Моделирование информационного обеспечения*
Задания:
1. Спроектировать логическую модель баз данных.
2. Задать атрибуты для каждой определенной сущности.
3. Ввести связи между сущностями.
4. Присвойте связям уникальные имена.

Практические работы № 3 (6 ч)*Сравнение и выбор проектов*
Задания:
1. Выделить критерии отбора оптимального варианта и целевую функцию.
2. Сформулируйть задачу выбора проекта в общем виде.

Практическая работа № 4 (6 ч)*Технико-экономическийанализпроекта*
Задания:
1. Провести оценку ианализизмененийтехнико- экономическихпоказателей.
2. Сформировать выводы по результатам анализа.
3. Составить отчет.

Практическая работа № 5 (6 ч) *Проектирование системы защиты от НСД*
Задания:
1. Осуществить защиту информации используя программные средства защиты.
2. Подготовить отчет полученных результатов.

Практическая работа № 6. (6 ч)*Аттестация автоматизированной системы по требованиям безопасности*
Задания:
1. Оценить объем входной и анализируемой информации.
2. Определить категории получаемых и обрабатываемых сведений.
3. Подготовить отчет

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Проектирование защищенных автоматизированных систем» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины – формирование основных знаний и умений в области технологий проектирования защищенных автоматизированных систем и соответствующими общепрофессиональными компетенциями в соответствии с ООП.

Задачи дисциплины:

– формирование знаний в области проектирования защищенных автоматизированных систем;
– уяснение основных понятий и определений, позволяющих осуществлять выбор и проектирование систем защиты;
– рассмотреть особенности методов и средств проектирования, создания и сопровождения защищенных автоматизированных систем.

Дисциплина направлена на формирование следующих компетенций:

- ОПК-4.1 - Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах
- ОПК-4.1.1 - Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- ОПК-4.1.2 - Умеет разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности)
- ОПК-4.1.3 - Владеет навыками планирования мероприятий по обеспечению защиты информации и организацию работы персонала автоматизированной системы с учетом требований по защите информации
- ОПК-4.4 - Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем
- ОПК-4.4.1 - Знает критерии оценки защищенности автоматизированной системы, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
- ОПК-4.4.2 - Умеет контролировать уровень защищенности в автоматизированных системах, регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах
- ОПК-4.4.3 - Владеет навыками проведения аудита защищенности информации в автоматизированных системах

В результате освоения дисциплиныобучающийся должен:

Знать: основные законы и закономерности функционирования экономики;основы экономической теории, необходимые для решения профессиональных и социальных задач; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации;нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.

Уметь: применять экономические знания при выполнении практических задач;принимать обоснованные экономические решения в различных областях жизнедеятельности; обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных

прав;разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации.
Владеть: методами выбора инструментальных средств для обработки экономических данных при решении социальных и профессиональных задач; навыками разрабатывать проекты локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации; навыками по разработке политики безопасности объекта информатизации.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.
Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.