МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

Филиппович А.Ю.

"01" сентября 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Разработка и эксплуатация защищенных автоматизированных систем»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)
«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация (степень) выпускника
Специалист

Форма обучения
Очная
Год приема - 2019

Москва 2019 г.

1. Цели освоения дисциплины

К **основным целям** освоения дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» следует отнести:

- теоретическая и практическая подготовка к деятельности, связанной с проектированием и эксплуатации защищенных автоматизированных информационных систем в своей профессиональной деятельности.

К **основным задачам** освоения дисциплины «»Разработка и эксплуатация защищенных автоматизированных систем следует отнести:

- освоение методологии, анализа и выбора принципов и методов проектирования и эксплуатации безопасных информационных систем.

2. Место дисциплины в структуре ООП специалитета

Дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» относится к числу профессиональных учебных дисциплин базовой части цикла Б.1 основной образовательной программы специалитета (Б.1.ДС.2 - специализация).

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Криптографические методы защиты информации», «Организационное и правовое обеспечение информационной безопасности», «Безопасность вычислительных сетей», «Программно-аппаратные средства защиты информации», «Техническая защита информации».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ПК – 2	способностью создавать и исследовать модели автоматизированных систем	**знать:** - язык UML для создания моделей автоматизированных систем; **уметь:** - создавать и исследовать модели автоматизированных систем на языке UML; **владеть:** - инструментальными средствами для создания моделей автоматизированных систем на языке UML.

ПК - 4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	**уметь:** - разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.
ПК – 6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	**знать:** -информационные ресурсы, подлежащие защите; **уметь:** - выявлять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов;
ПК - 8	способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	**знать:** - средства обеспечения информационной безопасности; **уметь:** -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;
ПК - 9	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	**знать:** -стандарты в области информационной безопасности при проектировании безопасной информационной системы; **уметь:** -применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования при проектировании безопасных информационных систем;
ПК - 20	способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований	**знать:** - состав рабочей технической документации с учетом действующих нормативных и методических документов; **уметь:** -оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

	информационной безопасности	
ПК - 24	способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	**уметь:** - проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; - выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации;

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц, т.е. **144** академических часов (лабораторные занятия – 72 часа, самостоятельная работа - 72 часа, форма контроля – экзамен) в шестом семестре.

Структура и содержание дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Тема 1. Общие положения проектирования безопасных информационных систем.

Основы методологии проектирования информационных систем. Модели жизненного цикла. Методологии и технологии проектирования ИС.

Тема 2. Формирование требований к системе защиты информации информационной системы.

Определение актуальных угроз безопасности информации и разработка на их основе модели угроз. Классификация информационной системы.

Цель и задачи обеспечения защиты информации в информационной системе. Перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система. Перечень типов объектов защиты информационной системы. Требования к мерам и средствам защиты информации, применяемым в информационной системе.

Тема 3. Разработка системы защиты информации информационной системы.

Определение субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа).

Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы.

Организационные меры, виды и типы средств защиты информации.

Логическая структура, состав (количество) и места размещения элементов системы защиты информации информационной системы.

Выбор сертифицированных средств защиты информации с учетом их совместимости с информационными технологиями и техническими средствами обработки информации, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы.

Параметры настройки средств защиты информации, обеспечивающие реализацию мер по защите информации и блокирование (нейтрализацию) актуальных угроз безопасности информации, в том числе путем устранения возможных уязвимостей информационной системы.

Эксплуатационная документация на систему защиты информации информационной системы.

Тестирование системы защиты информации информационной системы.

Тема 4. Реализация системы защиты информации в информационной системе.

Установка и настройка средств защиты информации в информационной системе. Разработка документов, определяющих мероприятия, проводимые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.

Внедрение организационных мер в информационной системе. Предварительные испытания системы защиты информации информационной системы. Опытная эксплуатация системы защиты информации информационной системы. Анализ уязвимостей информационной системы. Приемочные испытания системы защиты информации информационной системы.

Тема 5. Аттестация информационной системы на соответствие требованиям о защите информации и ввод ее в действие.

Программа и методика аттестационных испытаний. Особенности аттестации информационной системы на основе результатов аттестационных испытаний выделенного набора ее сегментов.

Тема 6. Эксплуатация системы защиты информации информационной системы.

Обеспечение безопасности среды эксплуатации информационной системы. Администрирование системы защиты информации информационной системы. Реагирование на инциденты, связанные с нарушением требований о защите информации. Управление конфигурацией системы защиты информации информационной системы. Управление защитой информации в информационной системе.

Тема 7. Защита информации в ходе снятия с эксплуатации информационной системы.

Архивирование информации конфиденциального характера, содержащейся в информационной системе. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

5. Образовательные технологии

Методика преподавания дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» и реализация компетентностного подхода в изложении и

восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- подготовка к выполнению лабораторных работ с использованием видео уроков;
- проведение интерактивных лекционных занятий в форме видео уроков;
- обсуждение и защита домашних заданий по дисциплине;
- подготовка, представление и обсуждение презентаций на семинарских занятиях.

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 60 % аудиторных занятий. Занятия лекционного типа составляют 33 % от объема аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- домашние задания и их защита;
- экзамен.

Темы домашних заданий, контрольных вопросов и заданий для проведения текущего контроля, экзаменационных билетов, приведены в приложении 2.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ПК – 2	способностью создавать и исследовать модели автоматизированных систем
ПК - 4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы
ПК – 6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности
ПК - 8	способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем
ПК - 9	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности

ПК - 20	способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности
ПК - 24	способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю)

ПК – 2 способностью создавать и исследовать модели автоматизированных систем				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: - язык UML для создания моделей автоматизированных систем;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: язык UML для создания моделей автоматизированных систем.	Обучающийся демонстрирует неполное соответствие следующих знаний: язык UML для создания моделей автоматизированных систем. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: язык UML для создания моделей автоматизированных систем, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: язык UML для создания моделей автоматизированных систем. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.

уметь: - создавать и исследовать модели автоматизированных систем на языке UML;	Обучающийся не умеет или в недостаточной степени умеет создавать и исследовать модели автоматизированных систем на языке UML.	Обучающийся демонстрирует неполное соответствие следующих умений: создавать и исследовать модели автоматизированных систем на языке UML. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: создавать и исследовать модели автоматизированных систем на языке UML. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: создавать и исследовать модели автоматизированных систем на языке UML. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: - инструментальными средствами для создания моделей автоматизированных систем на языке UML.	Обучающийся не владеет или в недостаточной степени владеет инструментальными средствами для создания моделей автоматизированных систем на языке UML.	Обучающийся владеет инструментальными средствами для создания моделей автоматизированных систем на языке UM, допускаются значительные ошибки, проявляется недостаточность владения навыками.	Обучающийся частично владеет инструментальными средствами для создания моделей автоматизированных систем на языке UML, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет инструментальными средствами для создания моделей автоматизированных систем на языке UML, свободно применяет полученные навыки в ситуациях повышенной сложности.
ПК - 4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы				
уметь: - разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.	Обучающийся не умеет или в недостаточной степени умеет разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.	Обучающийся демонстрирует неполное соответствие следующих умений разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы. Допускаются значительные ошибки, проявляется	Обучающийся демонстрирует частичное соответствие следующих умений: разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.. Умения освоены, но	Обучающийся демонстрирует полное соответствие следующих умений: разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизирован

		недостаточность умений.	допускаются незначительные ошибки, неточности.	ной системы.. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
ПК – 6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности				
знать: - информационные ресурсы, подлежащие защите;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: информационные ресурсы, подлежащие защите.	Обучающийся демонстрирует неполное соответствие следующих знаний: информационные ресурсы, подлежащие защите. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: информационные ресурсы, подлежащие защите, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: информационные ресурсы, подлежащие защите. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
уметь: - выявлять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов;	Обучающийся не умеет или в недостаточной степени умеет выявлять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов.	Обучающийся демонстрирует неполное соответствие следующих умений Допускаются значительные ошибки, проявляется недостаточность умений выявлять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов.	Обучающийся демонстрирует частичное соответствие следующих умений: выявлять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: выявлять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов. Свободно оперирует приобретенными умениями,

				применяет их в ситуациях повышенной сложности.
ПК - 8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем				
знать: - средства обеспечения информационной безопасности;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: средства обеспечения информационной безопасности	Обучающийся демонстрирует неполное соответствие следующих знаний: средства обеспечения информационной безопасности. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: средства обеспечения информационной безопасности, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: средства обеспечения информационной безопасности. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
уметь: -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;	Обучающийся не умеет или в недостаточной степени умеет проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.	Обучающийся демонстрирует неполное соответствие следующих умений: проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности. Свободно оперирует приобретенными умениями, применяет их в

				ситуациях повышенной сложности.
ПК - 9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности				
знать: -стандарты в области информационной безопасности при проектировании безопасной информационной системы;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: стандарты в области информационной безопасности при проектировании безопасной информационной системы.	Обучающийся демонстрирует неполное соответствие следующих знаний: стандарты в области информационной безопасности при проектировании безопасной информационной системы. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: стандарты в области информационной безопасности при проектировании безопасной информационной системы, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: стандарты в области информационной безопасности при проектировании безопасной информационной системы. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
уметь: -применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования при проектировании безопасных информационных систем;	Обучающийся не умеет или в недостаточной степени умеет применять программные средства системного, прикладного и специального назначения.	Обучающийся демонстрирует неполное соответствие следующих умений применять программные средства системного, прикладного и специального назначения. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: применять программные средства системного, прикладного и специального назначения. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: применять программные средства системного, прикладного и специального назначения. Свободно оперирует приобретенными умениями,

				применяет их в ситуациях повышенной сложности.
ПК - 20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности				
знать: - состав рабочей технической документации с учетом действующих нормативных и методических документов;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: состав рабочей технической документации с учетом действующих нормативных и методических документов.	Обучающийся демонстрирует неполное соответствие следующих знаний: состав рабочей технической документации с учетом действующих нормативных и методических документов. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: состав рабочей технической документации с учетом действующих нормативных и методических документов, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: состав рабочей технической документации с учетом действующих нормативных и методических документов. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
уметь: -оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Обучающийся не умеет или в недостаточной степени умеет оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.	Обучающийся демонстрирует неполное соответствие следующих умений: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов. Свободно оперирует приобретенными умениями, применяет их в

				ситуациях повышенной сложности.
ПК - 24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности				
уметь: - проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; - выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации;	Обучающийся не умеет или в недостаточной степени умеет проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	Обучающийся демонстрирует неполное соответствие следующих умений: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации.. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации.. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств представлены в приложении 2 к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Проектирование информационных систем на основе современных CASE-технологий : учеб. пособие Федоров Н.В. М.: МГИУ, 2007, 278 стр.
2. Проектирование информационных систем : лаб. практикум Федоров Н.В. М.: МГИУ, 2009, 122 стр.708

3. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. N 17

б) дополнительная литература:

1. Ручкин В.С., Семенов И.О., Черемных С.В. Структурный анализ систем. IDEF-технологии М.: Финансы и статистика, 2001
2. Вендров А.М. CASE – технологии. Современные методы и средства проектирования информационных систем. – М.: Финансы и статистика, 1998.- 176 с.

в) программное обеспечение и интернет-ресурсы:

1. Видеокурс «CASE-технологии». Электронный ресурс. Свидетельство ОФЭРНиО о регистрации электронного ресурса № 16340 от 28.10.2010
2. Ramus Educational
3. StarUML 5.0

8. Материально-техническое обеспечение дисциплины.

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, ноутбук, экран) – 1 комплект.

Для проведения практических занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются *лекции.*

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Самостоятельная работа по дисциплине предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др..

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;

- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на лабораторных занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:
- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.05.03 «Информационная безопасность автоматизированных систем».**

Программу составил: проф., к.т.н. Федоров Н.В.

Программа утверждена на заседании кафедры “Информационная безопасность” «29» августа 2019 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение.

**Структура и содержание дисциплины «Разработка и эксплуатация защищенных автоматизированных систем»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалист)**

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	Шестой семестр														
1.1	Основы методологии проектирования информационных систем. Модели жизненного цикла. Методологии и технологии проектирования ИС.	6	1			4									
1.2	Функциональная модель IDEF0 информационной системы. Основы проектирования.	6	2			4	12				+				
1.3	Определение актуальных угроз безопасности информации и разработка на их основе модели угроз. Классификация информационной системы.	6	3			4									
1.4	Функциональная модель IDEF0	6	4			4	8				+				

	информационной системы. AS-IS.														
1.5	Требования к мерам и средствам защиты информации, применяемым в информационной системе.	6	5			4									
1.6	Функциональная модель IDEF0 информационной системы. TO-BE.	6	6			4	8				+				
1.7	Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы.	6	7			4									
1.8	Функциональная модель IDEF0 безопасной информационной системы. TO-BE.	6	8			4	8				+				
1.9	Эксплуатационная документация на систему защиты информации информационной системы. Тестирование системы защиты информации информационной системы.	6	9			4									
1.10	Диаграммы поведения Use Case безопасной информационной системы.	6	10			4	8				+				
1.11	Установка и настройка средств защиты информации в	6	11			4									

	информационной системе. Разработка документов, определяющих мероприятия, проводимые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.														
1.12	Диаграммы поведения Statechart безопасной информационной системы.	6	12			4	8				+				
1.13	Внедрение организационных мер в информационной системе. Предварительные испытания системы защиты информации информационной системы. Опытная эксплуатация системы защиты информации информационной системы. Анализ уязвимостей информационной системы. Приемочные испытания системы защиты информации информационной системы.	6	13			4									
1.14	Диаграммы поведения Activity безопасной информационной системы.	6	14			4	8				+				
1.15	Программа и методика аттестационных испытаний. Особенности аттестации информационной системы на основе результатов аттестационных испытаний выделенного набора ее	6	15			4									

	сегментов.														
1.16	Диаграммы поведения. Collaboration & Sequence.	6	16			4	6				+				
1.17	Обеспечение безопасности среды эксплуатации информационной системы. Администрирование системы защиты информации информационной системы.	6	17			2									
1.18	Структурные диаграммы. Диаграммы классов. Диаграммы развёртывания.	6	17			2	4				+				
1.19	Архивирование информации конфиденциального характера, содержащейся в информационной системе. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.	6	18			2									
1.20	Структурные диаграммы. Диаграммы компонентов. Управление проектом.	6	18			2	2				+				
	Форма аттестации		19-22											Э	
	Всего часов по дисциплине в шестом семестре					72	72								
	Всего часов по дисциплине					72	72								

Приложение 1 к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): «Обеспечение информационной безопасности распределенных информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: научно-исследовательская; проектно-конструкторская; контрольно-аналитическая; организационно-управленческая; эксплуатационная

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Разработка и эксплуатация защищенных автоматизированных систем»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Домашние задания

Экзамен

Составители:

Проф., к.т.н. Н.В. Федоров

Москва, 2019 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Разработка и эксплуатация защищенных автоматизированных систем					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценоч-ного средств**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				
ПК – 2	способностью создавать и исследовать модели автоматизированных систем	**знать:** - язык UML для создания моделей автоматизированных систем; **уметь:** - создавать и исследовать модели автоматизированных систем на языке UML; **владеть:** - инструментальными средствами для создания моделей автоматизированных систем на языке UML.	лекции, самостоятельная работа, практические занятия	ДЗ, экзамен	Базовый уровень: уметь создавать и исследовать модели автоматизированных систем на языке UML Повышенный уровень: владеть инструментальными средствами для создания моделей автоматизированных систем на языке UML.

ПК - 4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	**уметь:** - разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.	лекции, самостоятельная работа, практические занятия	ДЗ, экзамен	Базовый уровень: уметь разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.
ПК – 6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	**знать:** -информационные ресурсы, подлежащие защите; **уметь:** - выявлять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов;	лекции, самостоятельная работа, практические занятия	ДЗ, экзамен	Базовый уровень: уметь выявлять угрозы безопасности информации Повышенный уровень: уметь выявлять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов

ПК - 8	способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	**знать:** - средства обеспечения информационной безопасности; **уметь:** -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;	лекции, самостоятельная работа, практические занятия	ДЗ, экзамен	Базовый уровень: уметь проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
ПК - 9	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	**знать:** -стандарты в области информационной безопасности при проектировании безопасной информационной системы; **уметь:** -применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования при проектировании безопасных информационных систем;	лекции, самостоятельная работа, практические занятия	ДЗ, экзамен	Базовый уровень: знать стандарты в области информационной безопасности при проектировании безопасной информационной системы Повышенный уровень: уметь применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования при проектировании безопасных информационных систем

ПК - 20	способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	**знать:** - состав рабочей технической документации с учетом действующих нормативных и методических документов; **уметь:** -оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;	лекции, самостоятельная работа, практические занятия	ДЗ, экзамен	Базовый уровень: уметь оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.
ПК - 24	способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	**уметь:** - проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; - выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации;	лекции, самостоятельная работа, практические занятия	ДЗ, экзамен	Базовый уровень: уметь проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности Повышенный уровень: уметь выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации

Приложение 2
к рабочей программе

Оценочные средства для текущей аттестации

Домашние задания.

Домашнее задание 1. Разработка функциональной модели IDEF0 безопасной информационной системы.
Домашнее задание 2. Разработка диаграммы поведения Use Case безопасной информационной системы.
Домашнее задание 3. Разработка диаграммы поведения Statechart безопасной информационной системы.
Домашнее задание 4. Разработка диаграммы поведения Activity безопасной информационной системы.
Домашнее задание 5. Разработка диаграммы поведения Collaboration & Sequence безопасной информационной системы.
Домашнее задание 6. Разработка структурной диаграммы развертывания безопасной информационной системы.
Домашнее задание 7. Разработка структурной диаграммы компонентов безопасной информационной системы.

Информационная система для защиты определяется индивидуально для каждого студента.

Оценочные средства для промежуточной аттестации

Экзамен

Список вопросов для экзамена по дисциплине

1. Основы методологии проектирования информационных систем.
2. Модели жизненного цикла.
3. Методологии и технологии проектирования ИС.
4. Определение актуальных угроз безопасности информации и разработка на их основе модели угроз.
5. Классификация информационной системы.
6. Цель и задачи обеспечения защиты информации в информационной системе.
7. Перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система.
8. Перечень типов объектов защиты информационной системы.

9. Требования к мерам и средствам защиты информации, применяемым в информационной системе.

10. Определение субъектов доступа и объектов доступа.

11. Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы.

12. Организационные меры, виды и типы средств защиты информации.

13. Логическая структура, состав (количество) и места размещения элементов системы защиты информации информационной системы.

14. Выбор сертифицированных средств защиты информации.

15. Эксплуатационная документация на систему защиты информации информационной системы.

16. Тестирование системы защиты информации информационной системы.

17. Установка и настройка средств защиты информации в информационной системе.

18. Разработка документов, определяющих мероприятия, проводимые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.

19. Внедрение организационных мер в информационной системе.

20. Предварительные испытания системы защиты информации информационной системы.

21. Опытная эксплуатация системы защиты информации информационной системы.

22. Анализ уязвимостей информационной системы.

23. Приемочные испытания системы защиты информации информационной системы.

24. Программа и методика аттестационных испытаний.

25. Особенности аттестации информационной системы на основе результатов аттестационных испытаний выделенного набора ее сегментов.

26. Обеспечение безопасности среды эксплуатации информационной системы.

27. Администрирование системы защиты информации информационной системы.

28. Реагирование на инциденты, связанные с нарушением требований о защите информации.

29. Управление конфигурацией системы защиты информации информационной системы.

30. Управление защитой информации в информационной системе.
31. Архивирование информации конфиденциального характера, содержащейся в информационной системе.
32. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

Пример билета.

1. Классификация информационной системы. Классы защищенности.
2. Практическая разработка модели системы безопасности ИС на среде IDEF 3.7 и StarUML.