МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

/Д. Г. Демидов/

"30" августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы проектирования информационных систем»

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная
Год приема - 2021

Москва 2021 г.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.03.01 «Информационная безопасность»**.

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

Программа утверждена на заседании кафедры «Информационная безопасность»
«30» августа 2021 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Основы проектирования информационных систем» следует отнести:

• теоретическая и практическая подготовка к деятельности, связанной с исследованием, моделированием и проектированием защищенных автоматизированных информационных систем в области информационной безопасности.

К **основным задачам** освоения дисциплины «Основы проектирования информационных систем» следует отнести:

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

2. Место дисциплины в структуре ООП.

Дисциплина «Основы проектирования информационных систем» относится к числу профессиональных учебных дисциплин базовой части цикла (Б.1) основной образовательной программы (Б.1.15).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности».

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-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**знать:** •язык UML для создания моделей автоматизированных систем; **уметь:** применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования при проектировании безопасных информационных систем; **владеть:** •инструментальными средствами для исследования и моделирования моделей защищенных автоматизированных систем на языке UML.
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для	**знать:** -информационные ресурсы, подлежащие защите; **уметь:** -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; - выявлять угрозы безопасности информации и возможные пути их реализации на основе анализа

	технико-экономического обоснования соответствующих проектных решений	структуры и содержания информационных процессов;
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**знать:** -информационные ресурсы, подлежащие защите; **уметь:** -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; - выявлять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов;

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетные единицы, т.е. **144** академических часов (лабораторные занятия – 72 час, самостоятельная работа - 72 час., форма контроля – экзамен) в 2 семестре.

Структура и содержание дисциплины «Основы проектирования информационных систем» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Тема 1. Системный анализ информационных систем

Основные понятия CASE – технологий. Основы методологии проектирования информационных систем. Модели жизненного цикла ИС. Методологии и технологии проектирования ИС. Жизненный цикл системы защиты информации.

Тема 2. Структурный подход к проектированию информационных систем.

Сущность структурного подхода. Методология функционального моделирования SADT. Методология функционального моделирования IDEF0.

Тема 3. Характеристики CASE-средств.

Методология Silverrun. Методология JAM. Методология Vantage Team Builder (Westmount I-CASE). Методология Uniface. Методология Designer/2000 + Developer/2000. Локальные средства (ERwin, BPwin, S-Designor, CASE-Аналитик). Объектно-ориентированное CASE-средство Rational Rose. Вспомогательные средства поддержки жизненного цикла ПО. Примеры комплексов CASE-средств

Тема 4. Моделирование бизнес-процессов и структур в области информационной безопасности на основе языка UML

Диаграммы поведения. Диаграмма сценариев (Use case diagram). Диаграмма состояний (Statechart diagram). Диаграмма активности (Activity diagram). Диаграмма взаимодействия (Interaction diagram).

Структурные диаграммы. Диаграмма классов (Class diagram). Диаграмма топологии (Deployment diagram). Диаграмма компонент (Component diagram).

5. Образовательные технологии.

Методика преподавания дисциплины «Основы проектирования информационных 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;

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 20 % 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:

- Лабораторные работы 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-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

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-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

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 автоматизированны х 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 автоматизированны х 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 приобре-тенными знаниями.

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, инструментальные средства. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: : применять программные средства системного, прикладного и специального назначения, инструментальные средства. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: применять программные средства системного, прикладного и специального назначения, инструментальные средства. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: •инструментальными средствами для исследования и моделирования моделей защищенных автоматизированных систем на языке UML.	Обучающийся не владеет или в недостаточной степени владеет инструментальными средствами для исследования и моделирования моделей защищенных автоматизированных систем на языке UML.	Обучающийся владеет навыками использования инструментальными средствами для исследования и моделирования моделей защищенных автоматизированных систем на языке UML, допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей, Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет навыками использования инструментальными средствами для исследования и моделирования моделей защищенных автоматизированных систем на языке UM, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет навыками использования инструментальными средствами для исследования и моделирования моделей защищенных автоматизированных систем на языке UML, свободно применяет полученные навыки в ситуациях повышенной сложности.

ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**

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 приобре-тенными знаниями.
уметь: -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; - 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 в-проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности ; ыявлять угрозы безопасности информации.	Обучающийся демонстрирует неполное соответствие следующих умений: -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; выявлять угрозы безопасности информации и возможные пути их реализации. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; выявлять угрозы безопасности информации и возможные пути их реализации. 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» выявлять угрозы безопасности информации и возможные пути их реализации. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**

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 приобре-тенными знаниями.
уметь: -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; - 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 в-проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности ; ыявлять угрозы безопасности информации.	Обучающийся демонстрирует неполное соответствие следующих умений: -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; выявлять угрозы безопасности информации и возможные пути их реализации. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; выявлять угрозы безопасности информации и возможные пути их реализации. 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» выявлять угрозы безопасности информации и возможные пути их реализации. 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 средствпредставлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) основная литература:

1. Федоров Н.В. Основы проектирования информационных систем. Электронный образовательный ресурс. Московский Политех, 2020- https://lms.mospolytech.ru/course/view.php?id=5353

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.
3. Проектирование информационных систем на основе современных CASE-технологий : учеб. пособие Федоров Н.В. М.: МГИУ, 2007, 278 стр.
4. Проектирование информационных систем : лаб. практикум Федоров Н.В. М.: МГИУ, 2009, 122 стр.708
5. 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

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, экран) – 1 комплект.

Для проведения лабораторных 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, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

10. Методические рекомендации для преподавателя

При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

Приложение.

Структура и содержание дисциплины «Основы проектирования информационных систем»
по направлению подготовки
10.03.01 «Информационная безопасность»
(бакалавр)

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
	2 семестр														
1	Лекции														
1.1	Тема 1. Системный анализ информационных систем.	2	1-2				8								
1.2	Тема 2. Структурный подход к проектированию информационных систем.		3-8				24								
1.3	Тема 3. Характеристики CASE-средств.		9-10				8								
1.4	Тема 4. Моделирование бизнес-процессов и структур в области информационной безопасности на основе языка UML		11-18				24								
2	Лабораторные занятия														
2.1	Лабораторная работа № 1.		1-4			16									

	Разработка функциональной модели жизненного цикла системы защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.																
2.2	Лабораторная работа № 2. Разработка модели потока данных системы защиты информации.		5-6			8											
2.3	Лабораторная работа № 3. Разработка диаграммы сценариев (Use case diagram) системы защиты информации.		7-8			8											
2.4	Лабораторная работа № 4. Разработка диаграммы топологии (Deployment diagram) системы защиты информации		9			4											
2.5	Лабораторная работа № 5. Разработка диаграммы состояний (Statechart diagram) системы защиты информации.		10			4											
2.6	Лабораторная работа № 6. Разработка диаграммы активности (Activity diagram) системы защиты информации.		11-13			12											
2.7	Лабораторная работа № 7. Разработка диаграммы взаимодействия (Interaction diagram).		14-15			8											
2.8	Лабораторная работа № 8. Разработка диаграммы классов (Class diagram) системы защиты информации.		16-17			8											

2.9	Лабораторная работа № 9. Разработка диаграммы компонент (Component diagram) системы защиты информации		18			4									
	Форма аттестации		19-21											Э	
	Всего часов по дисциплине во втором семестре					72	72								
	Всего часов по дисциплине					72	72								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.03.01 «Информационная безопасность»

ОП (профиль): «Безопасность компьютерных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Основы проектирования информационных систем»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Экзамен

Составители: к.т.н., доцент Н.В. Федоров

Москва, 2021 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Основы проектирования информационных систем					
ФГОС ВО **10.03.01 «Информационная безопасность»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**знать:** •язык UML для создания моделей автоматизированных систем; **уметь:** -применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования при проектировании безопасных информационных систем; **владеть:** •инструментальными средствами для исследования и моделирования моделей защищенных автоматизированных систем на языке UML. на основе анализа структуры и содержания информационных процессов;	лекции, самостоятельная работа, лабораторные занятия	ДЗ, экзамен	Базовый уровень: **знать:** •язык UML для создания моделей автоматизированных систем; **уметь:** способен применять программные средства системного, прикладного и специального назначения **владеть:** •инструментальными средствами для исследования и моделирования моделей защищенных автоматизированных систем на языке UML. Повышенный уровень: **уметь:** способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	**знать:** -информационные ресурсы, подлежащие защите; **уметь:** проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; - выявлять угрозы безопасности информации и возможные пути их реализации	лекции, самостоятельная работа, лабораторные занятия	ДЗ, экзамен	Базовый уровень: **знать:** -информационные ресурсы, подлежащие защите; **уметь:** проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации Повышенный уровень: **уметь:** способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты участвовать в проведении технико-экономического обоснования соответствующих проектных решений

ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**знать:** -информационные ресурсы, подлежащие защите; **уметь:** проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; - выявлять угрозы безопасности информации и возможные пути их реализации	лекции, самостоятельная работа, лабораторные занятия	ДЗ, экзамен	Базовый уровень: **знать:** -информационные ресурсы, подлежащие защите; **уметь:** проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации Повышенный уровень: **уметь:** способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты участвовать в проведении технико-экономического обоснования соответствующих проектных решений

Приложение 2
к рабочей программе

Оценочные средства для текущей аттестации

Электронный тест

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. Основные понятия CASE – технологий.
2. Основы методологии проектирования информационных систем.
3. Модели жизненного цикла ИС.
4. Методологии и технологии проектирования ИС.
5. Жизненный цикл системы защиты информации.
6. Классификация информационной системы. Классы защищенности.
7. Сущность структурного подхода.
8. Методология функционального моделирования SADT.
9. Методология функционального моделирования IDEF0.
10. Методология Silverrun.
11. Методология JAM.
12. Методология Vantage Team Builder (Westmount I-CASE).
13. Методология Uniface.
14. Методология Designer/2000 + Developer/2000.
15. Локальные средства (ERwin, BPwin, S-Designor, CASE-Аналитик).
16. Объектно-ориентированное CASE-средство Rational Rose.

17. Вспомогательные средства поддержки жизненного цикла ПО.
18. Примеры комплексов CASE-средств
19. Диаграммы поведения.
20. Диаграмма сценариев (Use case diagram).
21. Диаграмма состояний (Statechart diagram).
22. Диаграмма активности (Activity diagram). Д
23. иаграмма взаимодействия (Interaction diagram).
24. Структурные диаграммы.
25. Диаграмма классов (Class diagram).
26. Диаграмма топологии (Deployment diagram).
27. Диаграмма компонент (Component diagram).

Пример билета.

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