МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы проектирования информационных систем»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

Преподаватель / В.А. Пиков /

Согласовано:

И.о. заведующего кафедрой «Информационная безопасность»,  А.Ю. Гневшев

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 5
3 Структура и содержание дисциплины 5
3.1 Виды учебной работы и трудоемкость 5
3.2 Тематический план изучения дисциплины 6
3.3 Содержание дисциплины 7
4 Учебно-методическое и информационное обеспечение 7
4.1 Основная литература 7
4.2 Дополнительная литература 8
4.3 Электронные образовательные ресурсы 8
4.4 Лицензионное и свободно распространяемое программное обеспечение 8
5 Материально-техническое обеспечение 9
6 Методические рекомендации 9
6.1 Методические рекомендации для преподавателя по организации обучения 9
6.2 Методические указания для обучающихся по освоению дисциплины 9
7 Фонд оценочных средств 9
7.1 Методы контроля и оценивания результатов обучения 9
7.2 Шкала и критерии оценивания результатов обучения 9
7.3 Оценочные средства 14
7.3.1. Электронный тест 14
7.3.2. Список вопросов для экзамена 14

1 Цели, задачи и планируемые результаты обучения по дисциплине

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.

Обучение по дисциплине **«Основы проектирования информационных систем»** направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
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 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 на основе анализа структуры и содержания информационных процессов;
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными	**знать:** ● информационные ресурсы, подлежащие защите;

правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**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;

2 Место дисциплины в структуре образовательной программы

Дисциплина «Основы проектирования информационных систем» относится к числу профессиональных учебных дисциплин обязательной части цикла (Б1.1) основной образовательной программы (Б1.1.19).

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

3 Структура и содержание дисциплины

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

3.1 Виды учебной работы и трудоемкость (по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	2	1-18
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	2	1-18
2	**Самостоятельная работа**	**72**	2	1-18
3	**Промежуточная аттестация**		2	19-21
	Диф.зачет			
	Итого:	**144**		

3.2 Тематический план изучения дисциплины (по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Лекции						
1.1	Тема 1. Системный анализ информационных систем.	8					8
1.2	Тема 2. Структурный подход к проектированию информационных систем.	24					24
1.3	Тема 3. Характеристики CASE-средств.	8					8
1.4	Тема 4. Моделирование бизнес-процессов и структур в области информационной безопасности на основе языка UML	24					24
2	Лабораторные занятия						
2.1	Лабораторная работа № 1. Разработка функциональной модели жизненного цикла системы защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.	16			16		
2.2	Лабораторная работа № 2. Разработка модели потока данных системы защиты информации.	8			8		
2.3	Лабораторная работа № 3. Разработка диаграммы сценариев (Use case diagram) системы защиты информации.	8			8		
2.4	Лабораторная работа № 4. Разработка диаграммы топологии (Deployment diagram) системы защиты информации	4			4		
2.5	Лабораторная работа № 5. Разработка диаграммы состояний (Statechart diagram) системы защиты информации.	4			4		

2.6	Лабораторная работа № 6. Разработка диаграммы активности (Activity diagram) системы защиты информации.	12			12		
2.7	Лабораторная работа № 7. Разработка диаграммы взаимодействия (Interaction diagram).	8			8		
2.8	Лабораторная работа № 8. Разработка диаграммы классов (Class diagram) системы защиты информации.	8			8		
2.9	Лабораторная работа № 9. Разработка диаграммы компонент (Component diagram) системы защиты информации	4			4		
Итого		**144**			**72**		**72**

3.3 Содержание 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. 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).

4 Учебно-методическое и информационное обеспечение

4.1 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
2. Проектирование информационных систем : учебник и практикум для среднего профессионального образования / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк,

Н. Б. Ничепорук. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 293 с. — (Профессиональное образование). — ISBN 978-5-534-16217-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530635

3. Грекул, В. И. Проектирование информационных систем : учебник и практикум для среднего профессионального образования / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина. — 2-е изд. — Москва : Издательство Юрайт, 2023. — 423 с. — (Профессиональное образование). — ISBN 978-5-534-17836-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/533817
4. Григорьев, М. В. Проектирование информационных систем : учебное пособие для среднего профессионального образования / М. В. Григорьев, И. И. Григорьева. — Москва : Издательство Юрайт, 2023. — 318 с. — (Профессиональное образование). — ISBN 978-5-534-12105-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518751.

4.2 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

4.3 Электронные образовательные ресурсы

1. Основы проектирования информационных систем. Электронный образовательный ресурс. Московский Политех, 2020- https://lms.mospolytech.ru/course/view.php?id=5353
2. Видеокурс «CASE-технологии». Электронный ресурс. Свидетельство ОФЭРНиО о регистрации электронного ресурса № 16340 от 28.10.2010

4.4 Лицензионное и свободно распространяемое программное обеспечение

1. Ramus Educational
2. StarUML 5.0

5 Материально-техническое обеспечение

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.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

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.

6.2 Методические указания для обучающихся по освоению дисциплины

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.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

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

- Лабораторные работы и их защита;
- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

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: •инструментальным и средствами для исследования и моделирования моделей защищенных автоматизированных систем на языке UML.	Обучающийся не владеет или в недостаточной степени владеет инструментальным и средствами для исследования и моделирования моделей защищенных	Обучающийся владеет навыками использования инструментальными средствами для исследования и моделирования моделей защищенных автоматизированных систем на языке UML,	Обучающийся частично владеет навыками использования инструментальными средствами для исследования и моделирования моделей защищенных	Обучающийся в полном объеме владеет навыками использования инструментальными средствами для исследования и моделирования моделей защищенных

	автоматизированны х систем на языке UML.	допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей, Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	автоматизированны х систем на языке UM, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	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	Обучающийся не умеет или в недостаточной степени умеет в-проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности ; выявлять угрозы	Обучающийся демонстрирует неполное соответствие следующих умений: -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; выявлять угрозы	Обучающийся демонстрирует частичное соответствие следующих умений: -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;	Обучающийся демонстрирует полное соответствие следующих умений: -проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности» выявлять угрозы

реализации на основе анализа структуры и содержания информационных процессов;	безопасности информации.	безопасности информации и возможные пути их реализации. Допускаются значительные ошибки, проявляется недостаточность умений.	выявлять угрозы безопасности информации и возможные пути их реализации. Умения освоены, но допускаются незначительные ошибки, неточности.	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	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	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.	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

процессов;		значительные ошибки, проявляется недостаточность умений.	Умения освоены, но допускаются незначительные ошибки, неточности.	приобретенными умениями, применяет их в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: дифференцированный зачет .

Промежуточная аттестация обучающихся в форме экзамена (зачета) 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.

7.3 Оценочные средства

7.3.1. Электронный тест

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.

7.3.2. Список вопросов для экзамена

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. Диаграмма взаимодействия (Interaction diagram).

24. Структурные диаграммы.
25. Диаграмма классов (Class diagram).
26. Диаграмма топологии (Deployment diagram).
27. Диаграмма компонент (Component diagram).