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

«Проектирование систем информационной безопасности»

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 «Проектирование систем информационной безопасности» 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 «Проектирование систем информационной безопасности» следует отнести:

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

2. Место дисциплины в структуре ООП.

Дисциплина «Проектирование систем информационной безопасности» относится к числу профессиональных учебных дисциплин по выбору студента части цикла (Б.1.ДВ) основной образовательной программы (Б.1.ДВ.5).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности», «Криптографические методы защиты информации», Программно-аппаратные средства обеспечения информационной безопасности, Организационное и правовое обеспечение 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-9	Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	**знать:** • информационные ресурсы, подлежащие защите; • язык UML для создания моделей автоматизированных систем; **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; • 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.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лекции – 36 час, лабораторные занятия – 36 час, самостоятельная работа - 72 часа, форма контроля – экзамен) в 6 семестре.

Структура и содержание дисциплины «Проектирование систем информационной безопасности» 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.

5. Образовательные технологии.

Методика преподавания дисциплины «Проектирование систем информационной безопасности» 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:

- экзамен.

Образцы тестовых заданий, экзаменационных билетов, приведены в приложении.

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-9	Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности

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-9 Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности

Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: информационные ресурсы, подлежащие защите; язык UML для создания моделей автоматизированных систем;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: информационные ресурсы, подлежащие защите; язык UML для создания моделей автоматизированных систем;	Обучающийся демонстрирует неполное соответствие следующих знаний: информационные ресурсы, подлежащие защите; 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: информационные ресурсы, подлежащие защите; язык UML для создания моделей автоматизированных систем; но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний**:** информационные ресурсы, подлежащие защите; язык UML для создания моделей автоматизированных систем;: 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; 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 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; применять программные средства системного, прикладного и специального назначения.	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 на основе анализа структуры и содержания информационных процессов; применять программные средства системного, прикладного и специального назначения, инструментальные средства. 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 на основе анализа структуры и содержания информационных процессов; применять программные средства системного, прикладного и специального назначения, инструментальные средства. 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 на основе анализа структуры и содержания информационных процессов; 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	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,	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.

		новых ситуациях.	нестандартные ситуации.	

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. 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, 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

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

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

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 «Проектирование систем информационной безопасности»
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
	6 семестр														
1.1	Основы методологии проектирования информационных систем. Модели жизненного цикла. Методологии и технологии проектирования ИС.	6	1	2											
1.2	Функциональная модель IDEF0 информационной системы. Основы проектирования.		1			2					+				
1.3	Определение актуальных угроз безопасности информации и разработка на их основе модели угроз. Классификация информационной системы.		2-3	4											
1.4	Функциональная модель IDEF0 информационной системы. AS-IS.		2-3			4	8				+				

1.5	Требования к мерам и средствам защиты информации, применяемым в информационной системе.		4-5	4													
1.6	Функциональная модель IDEF0 информационной системы. TO-BE.		4-5			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	2													
1.8	Функциональная модель IDEF0 безопасной информационной системы. TO-BE.		6			2	8				+						
1.9	Эксплуатационная документация на систему защиты информации информационной системы. Тестирование системы защиты информации информационной системы.		7-8	4													
1.10	Диаграммы поведения Use Case безопасной информационной системы.		7-8			4	6				+						
1.11	Установка и настройка средств защиты информации в информационной системе. Разработка документов, определяющих мероприятия, проводимые оператором для обеспечения защиты информации в		9	2													

	информационной системе в ходе ее эксплуатации.																
1.12	Диаграммы поведения Statechart безопасной информационной системы.		9			2	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.		10-11	4													
1.14	Диаграммы поведения Activity безопасной информационной системы.		10-11			4	8				+						
1.15	Программа и методика аттестационных испытаний. Особенности аттестации информационной системы на основе результатов аттестационных испытаний выделенного набора ее сегментов.		12	2													
1.16	Диаграммы поведения. Collaboration & Sequence.		12			2	8				+						
1.17	Обеспечение безопасности среды		13-14	4													

	эксплуатации информационной системы. Администрирование системы защиты информации информационной системы.														
1.18	Структурные диаграммы. Диаграммы классов.		13-14			4	8								
1.19	Структурные диаграммы. Диаграммы развёртывания.	6	15	2		2	8				+				
1.20	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	6	2		2	2								
1.21	Структурные диаграммы. Диаграммы компонентов.	6	17-	2		2	4				+				
1.22	Управление проектом.	6	18	2		2									
	Форма аттестации		19-21											Э	
	Всего часов по дисциплине во шестом семестре			36		36	72								
	Всего часов по дисциплине			36		36	72								

Приложение 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: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая

.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Проектирование систем информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Экзамен

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

Москва, 2019 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Проектирование систем информационной безопасности					
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 компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК-9	Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	**знать:** -информационные ресурсы, подлежащие защите; •язык UML для создания моделей автоматизированных систем; **уметь:** проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; - выявлять угрозы безопасности информации и возможные пути их реализации -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:** -информационные ресурсы, подлежащие защите; •язык UML для создания моделей автоматизированных систем; **уметь:** проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; - выявлять угрозы безопасности информации и возможные пути их реализации 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

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.