



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
«Б1.О.19.08 МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ
ИНФОРМАЦИИ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Москва, 2024

Разработчики:

Декан факультета кафедры Информационно-измерительных систем, д.т.н. Матерухин А. В.

Преподаватель кафедры Информационно-измерительных систем
Калмыков С. А.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Минобрнауки от 17.11.2020 № 1427

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

Содержание

1. Цель и задачи освоения дисциплины (модуля)
2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы
3. Место дисциплины в структуре ОП
4. Объем дисциплины и виды учебной работы
5. Содержание дисциплины
 - 5.1. Разделы, темы дисциплины и виды занятий
 - 5.2. Содержание разделов, тем дисциплины и формы текущего контроля
6. Оценочные материалы текущего контроля
7. Оценочные материалы промежуточной аттестации
8. Порядок проведения промежуточной аттестации
9. Материально-техническое и учебно-методическое обеспечение дисциплины
 - 9.1. Перечень основной и дополнительной учебной литературы
 - 9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
 - 9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
 - 9.4. Оборудование и технические средства обучения
10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучающихся системы знаний, умений и навыков в области построения моделей процессов и систем защиты информации в будущей профессиональной деятельности.

Задачи изучения дисциплины:

- изучение принципов структурно-функционального анализа и моделирования систем защиты информации;;
- формирование умений использовать на практике языки моделирования, принципы и методы информационного, функционального и поведенческого моделирования систем и технологий защиты информации;;
- формирование навыков использования компьютерных технологий, позволяющих разрабатывать модели систем защиты информации..

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ОПК-2.2 Способен формировать предложения по оптимизации структуры и функциональных процессов защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы

ОПК-2.2.1 Выявляет достоинства и недостатки структуры и функциональных процессов защиты, его информационных составляющих

Знать:

ОПК-2.2.1/Зн1 современные нотации языков моделирования, российские государственные стандарты и методические документы в области оценки и моделирования безопасности информационных систем

Уметь:

ОПК-2.2.1/Ум1 использовать элементы языков моделирования для построения структурных, функциональных и информационных моделей систем и процессов защиты информации

Владеть:

ОПК-2.2.1/Нв1 методикой оценки угроз безопасности информации и методикой моделирования угроз

ОПК-2.2.2 Выявляет возможные деструктивные воздействия на информационные ресурсы

Знать:

ОПК-2.2.2/Зн1 основные виды деструктивных воздействий на информационные ресурсы

Уметь:

ОПК-2.2.2/Ум1 проводить анализ рисков и выявлять потенциальные угрозы для информационных ресурсов

Владеть:

ОПК-2.2.2/Нв1 навыками работы с программным обеспечением для мониторинга и оценки безопасности информационных систем

ОПК-2.2.3 Формулирует конструктивные предложения по оптимизации структуры и функциональных процессов защиты объекта

Знать:

ОПК-2.2.3/Зн1 принципы проектирования систем защиты информации и их компонентов

Уметь:

ОПК-2.2.3/Ум1 анализировать существующие процессы защиты информации и выявлять их недостатки

Владеть:

ОПК-2.2.3/Нв1 навыками разработки технических заданий на оптимизацию систем защиты информации

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.19.08 «Моделирование процессов и систем защиты информации» относится к обязательной части образовательной программы и изучается в семестре(ах): 3.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
3 семестр	108	3	17	34	21	Экзамен (36)
Всего	108	3	17	34	21	36

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотношенные с результатами освоения программы
Раздел 1. Основные представления о моделировании процессов и систем защиты информации	5	2		3	ОПК-2.2. 2

Тема 1.1. Основные представления о моделировании процессов и систем защиты информации	2	2			
Тема 1.2. Проработка лекционного материала	3			3	
Раздел 2. Модель безопасности с полным перекрытием множества угроз	14	2	8	4	ОПК-2.2. 1 ОПК-2.2. 2
Тема 2.1. Модель безопасности с полным перекрытием множества угроз	2	2			
Тема 2.2. Разработка модели функционально-структурного моделирования для выбранного объекта исследования с использованием методологии IDEF0	8		8		
Тема 2.3. Проработка лекционного материала. Подготовка к практическим занятиям.	4			4	
Раздел 3. Модели нарушителя и модели угроз	12	2	6	4	ОПК-2.2. 2 ОПК-2.2. 3
Тема 3.1. Модели нарушителя и модели угроз	2	2			
Тема 3.2. Разработка диаграммы потоков данных для выбранного объекта исследования с использованием нотации DFD	6		6		
Тема 3.3. Проработка лекционного материала. Подготовка к практическим занятиям.	4			4	
Раздел 4. Моделирование риска	8	4		4	ОПК-2.2. 1 ОПК-2.2. 2 ОПК-2.2. 3
Тема 4.1. Моделирование риска	4	4			
Тема 4.2. Проработка лекционного материала. Подготовка к практическим занятиям.	4			4	
Раздел 5. Использование языка UML для создания моделей процессов и систем защиты информации	28	4	20	4	ОПК-2.2. 1 ОПК-2.2. 2 ОПК-2.2. 3
Тема 5.1. Использование языка UML для создания моделей процессов и систем защиты информации	4	4			

Тема 5.2. Разработка модели требований к системе или подсистеме к выбранному объекту исследования с использованием UML диаграммы вариантов использования	6		6		
Тема 5.3. Разработка модели сценариев взаимодействия, включающих действия злоумышленника и ответные шаги системы защиты и/или отдела информационной безопасности, на выбранном объекте исследования с использованием нотации UML диаграммы деятельности	6		6		
Тема 5.4. Разработка модели структурных аспектов системы выбранного объекта исследования с использованием нотации UML диаграммы компонентов	8		8		
Тема 5.5. Проработка лекционного материала. Подготовка к практическим занятиям.	4			4	
Раздел 6. Процесс формирования требований к защите информации, содержащейся в государственной информационной системе	5	3		2	ОПК-2.2. 1 ОПК-2.2. 2 ОПК-2.2. 3
Тема 6.1. Процесс формирования требований к защите информации, содержащейся в государственной информационной системе	3	3			
Тема 6.2. Проработка лекционного материала. Подготовка к практическим занятиям.	2			2	
Итого	72	17	34	21	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Основные представления о моделировании процессов и систем защиты информации

Тема 1.1. Основные представления о моделировании процессов и систем защиты информации

Понятие «модель», «моделирование» и «системный подход». Понятие «информационной безопасности». Задачи моделирования процессов и систем защиты информации. Теоретические основы моделирования процессов и систем защиты информации. Определение архитектуры системы. Графические нотации для моделирования.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 1.2. Проработка лекционного материала

Понятие «модель», «моделирование» и «системный подход». Понятие «информационной безопасности». Задачи моделирования процессов и систем защиты информации. Теоретические основы моделирования процессов и систем защиты информации. Определение архитектуры системы. Графические нотации для моделирования.

Раздел 2. Модель безопасности с полным перекрытием множества угроз

Тема 2.1. Модель безопасности с полным перекрытием множества угроз

Множество отношений «объект-угроза». Полная модель системы обеспечения безопасности. Проект инженерно-технической системы информационной безопасности. Методология функционального моделирования IDEF0. Семантические правила функционального моделирования IDEF0. Функциональное моделирование процесса анализа рисков информационной безопасности на базе модели с полным перекрытием множества угроз.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 2.2. Разработка модели функционально-структурного моделирования для выбранного объекта исследования с использованием методологии IDEF0

Разработка модели функционально-структурного моделирования для выбранного объекта исследования с использованием методологии IDEF0

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 2.3. Проработка лекционного материала. Подготовка к практическим занятиям.

Множество отношений «объект-угроза». Полная модель системы обеспечения безопасности. Проект инженерно-технической системы информационной безопасности. Методология функционального моделирования IDEF0. Семантические правила функционального моделирования IDEF0. Функциональное моделирование процесса анализа рисков информационной безопасности на базе модели с полным перекрытием множества угроз.

Раздел 3. Модели нарушителя и модели угроз

Тема 3.1. Модели нарушителя и модели угроз

Модели угроз информационной безопасности согласно российским государственным и ведомственным стандартам. Определение модели нарушителя: категории нарушителей, цели, типовые сценарии. Стандартная модель безопасности. Гексада Паркера. Модель угроз безопасности информации STRIDE. Использование методологии DFD для построения модели угроз.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 3.2. Разработка диаграммы потоков данных для выбранного объекта исследования с использованием нотации DFD

Разработка диаграммы потоков данных для выбранного объекта исследования с использованием нотации DFD

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 3.3. Проработка лекционного материала. Подготовка к практическим занятиям.

Модели угроз информационной безопасности согласно российским государственным и ведомственным стандартам. Определение модели нарушителя: категории нарушителей, цели, типовые сценарии. Стандартная модель безопасности. Гексада Паркера. Модель угроз безопасности информации STRIDE. Использование методологии DFD для построения модели угроз.

Раздел 4. Моделирование риска

Тема 4.1. Моделирование риска

Понятие риска. Требования к системе менеджмента информационной безопасности согласно российским и международным стандартам. Методика DREAD. Связь между моделью угроз безопасности STRIDE и методикой DREAD.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 4.2. Проработка лекционного материала. Подготовка к практическим занятиям.

Понятие риска. Требования к системе менеджмента информационной безопасности согласно российским и международным стандартам. Методика DREAD. Связь между моделью угроз безопасности STRIDE и методикой DREAD.

Раздел 5. Использование языка UML для создания моделей процессов и систем защиты информации

Тема 5.1. Использование языка UML для создания моделей процессов и систем защиты информации

Основы унифицированного языка моделирования (UML). Концептуальная модель UML. Типы сущностей и типы отношений. Структура UML. Семантика и синтаксис языка UML. Элементы модели UML. Классификация, назначение и содержание диаграмм UML. Последовательность использования различных методов для проектирования защищённой системы.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 5.2. Разработка модели требований к системе или подсистеме к выбранному объекту исследования с использованием UML диаграммы вариантов использования

Разработка модели требований к системе или подсистеме к выбранному объекту исследования с использованием UML диаграммы вариантов использования и их расширения "Вариантов злонамеренного использования"

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 5.3. Разработка модели сценариев взаимодействия, включающих действия злоумышленника и ответные шаги системы защиты и/или отдела информационной безопасности, на выбранном объекте исследования с использованием нотации UML диаграммы деятельности

Разработка модели сценариев взаимодействия, включающих действия злоумышленника и ответные шаги системы защиты и/или отдела информационной безопасности, на выбранном объекте исследования с использованием нотации UML диаграммы деятельности

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 5.4. Разработка модели структурных аспектов системы выбранного объекта исследования с использованием нотации UML диаграммы компонентов

Разработка модели структурных аспектов системы с отображением их ключевых компонентов, интерфейсов и взаимосвязей с использованием нотации UML диаграммы компонентов

Тема 5.5. Проработка лекционного материала. Подготовка к практическим занятиям.

Основы унифицированного языка моделирования (UML). Концептуальная модель UML. Типы сущностей и типы отношений. Структура UML. Семантика и синтаксис языка UML. Элементы модели UML. Классификация, назначение и содержание диаграмм UML. Последовательность использования различных методов для проектирования защищённой системы.

Раздел 6. Процесс формирования требований к защите информации, содержащейся в государственной информационной системе

Тема 6.1. Процесс формирования требований к защите информации, содержащейся в государственной информационной системе

Определение государственной информационной системы согласно российскому законодательству. Требования к защите информации, содержащейся в государственной информационной системе, согласно документам ФСТЭК России. Процесс формирования требований. Алгоритм принятия решения о необходимости защиты информации, содержащейся в информационной системе. Классификация информационной системы по требованиям защиты информации. Определение угроз безопасности информации и разработка модели угроз. Определение требований к системе защиты информации информационной системы.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 6.2. Проработка лекционного материала. Подготовка к практическим занятиям.

Определение государственной информационной системы согласно российскому законодательству. Требования к защите информации, содержащейся в государственной информационной системе, согласно документам ФСТЭК России. Процесс формирования требований. Алгоритм принятия решения о необходимости защиты информации, содержащейся в информационной системе. Классификация информационной системы по требованиям защиты информации. Определение угроз безопасности информации и разработка модели угроз. Определение требований к системе защиты информации информационной системы.

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Экзамен, 3 семестр.

Допуском к экзамену является успешная сдача всех предусмотренных практических работ. Сдача работ происходит через платформу lms.miigaik.ru в соответствующем курсе обучения. Экзамен оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие,

исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;

- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;

- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;

- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

7. Оценочные материалы текущего контроля

Раздел 1. Основные представления о моделировании процессов и систем защиты информации

Контролируемые ИДК: ОПК-2.2.2

Тема 1.1. Основные представления о моделировании процессов и систем защиты информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что понимается под моделированием системы?

1. Процесс написания программного кода системы
2. Построение образа системы, соответствующего ей с точностью до целей исследования, и получение с его помощью характеристик реальной системы
3. Процесс физического создания макета системы из конструкционных материалов
4. Полное копирование всех свойств оригинала без исключения

2. Что такое архитектура системы согласно определению Software Engineering Institute?

1. Набор аппаратных средств, используемых в системе
2. Структура системы, включающая программные элементы, их наблюдаемые свойства и взаимодействие между ними
3. Схема базы данных системы
4. Совокупность нормативных документов, регулирующих работу системы

3. В системах, интенсивно использующих программное обеспечение Software-Intensive Systems, функциональный потенциал:

1. Определяется исключительно аппаратной частью
2. Не зависит от программного обеспечения
3. Определяется программным обеспечением или зависит от него в существенной мере
4. Зависит только от квалификации пользователей

Раздел 2. Модель безопасности с полным перекрытием множества угроз

Контролируемые ИДК: ОПК-2.2.1 ОПК-2.2.2

Тема 2.1. Модель безопасности с полным перекрытием множества угроз

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. В модели безопасности с полным перекрытием множества угроз исходное множество отношений «объект-угроза» образует:

1. Дерево атак

2. Двудольный граф
3. Полный граф
4. Сеть Петри

2. Какова основная цель защиты в модели с полным перекрытием множества угроз?

1. Уничтожить всех нарушителей
2. Максимально увеличить стоимость системы защиты
3. «Перекрыть» каждое ребро графа отношений «объект-угроза» средством защиты
4. Уменьшить количество защищаемых объектов до нуля

3. Что обозначает элемент «В» в наборе $S = \{O, Y, M, V, B\}$, описывающем полную модель безопасности?

1. Базы данных
2. Набор барьеров
3. Бюджет защиты
4. Поведенческие факторы

Тема 2.2. Разработка модели функционально-структурного моделирования для выбранного объекта исследования с использованием методологии IDEF0

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется сторона функционального блока IDEF0, к которой присоединяются стрелки «Управления»?

1. Левая сторона
2. Правая сторона
3. Верхняя сторона
4. Нижняя сторона

2. Какой частью речи должно быть выражено имя функционального блока в IDEF0?

1. Существительным (например, «Проверка»)
2. Глаголом или глагольным оборотом (например, «Выполнить проверку»)
3. Прилагательным (например, «Проверенный»)
4. Любой частью речи

3. Что обозначают стрелки, выходящие из нижней стороны блока в нотации IDEF0 (стрелки вызова)?

1. Механизмы выполнения функции
2. Результаты выполнения функции
3. Обращение к другой модели или части модели
4. Управляющие воздействия

4. Как называется диаграмма верхнего уровня в IDEF0, представляющая объект моделирования одним блоком?

1. A-0
2. A-1
3. Root Diagram
4. Context Diagram Level 1

Раздел 3. Модели нарушителя и модели угроз

Контролируемые ИДК: ОПК-2.2.2 ОПК-2.2.3

Тема 3.1. Модели нарушителя и модели угроз

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какое свойство НЕ входит в стандартную триаду безопасности CIA?

1. Конфиденциальность
2. Целостность

3. Неотказуемость

4. Доступность

2. Что означает буква «Т» в модели угроз STRIDE?

1. Testing (Тестирование)

2. Tampering (Нарушение целостности/Подделка)

3. Termination (Прекращение работы)

4. Timing (Временные атаки)

3. Какой элемент гексады Паркера описывает, что данные были созданы заявленным источником?

1. Полезность (Utility)

2. Владение (Possession)

3. Подлинность (Authenticity)

4. Конфиденциальность (Confidentiality)

4. Согласно определению ФСТЭК (ГОСТ Р 50922), модель угроз — это:

1. Список сотрудников, имеющих доступ к системе

2. Перечень установленных антивирусов

3. Физическое, математическое или описательное представление свойств или характеристик угроз безопасности информации

4. Программный код эксплойта

Тема 3.2. Разработка диаграммы потоков данных для выбранного объекта исследования с использованием нотации DFD

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой элемент нотации DFD обозначается прямоугольником?

1. Процесс

2. Внешняя сущность

3. Хранилище данных

4. Поток данных

2. Что в методологии DFD обозначает «Граница доверия»?

1. Границу между аппаратной и программной частью

2. Линию, где заканчивается ответственность системного администратора

3. Место, где изменяется уровень доверия или привилегий

4. Физический периметр здания

3. Верно ли утверждение: «В DFD потоки данных могут передаваться от хранилища к хранилищу напрямую»?

1. Да, всегда

2. Нет, передача возможна только через процессы

3. Да, но только если хранилища одного типа

4. Зависит от используемого программного обеспечения

Раздел 4. Моделирование риска

Контролируемые ИДК: ОПК-2.2.1 ОПК-2.2.2 ОПК-2.2.3

Тема 4.1. Моделирование риска

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой показатель в методике DREAD оценивает количество пользователей, которых затронет атака?

1. Damage potential

2. Reproducibility

3. Affected Users

4. Discoverability

2. Что означает «Е» в методике DREAD?

1. Уровень экономического ущерба
2. Квалификация и усилия, необходимые для проведения атаки
3. Возможность расширения привилегий
4. Эффективность средств защиты

3. Если уязвимость позволяет злоумышленнику гарантированно провести атаку, какой показатель DREAD будет максимальным?

1. Damage potential
2. Reproducibility
3. Discoverability
4. Affected Users

Раздел 5. Использование языка UML для создания моделей процессов и систем защиты информации

Контролируемые ИДК: ОПК-2.2.1 ОПК-2.2.2 ОПК-2.2.3

Тема 5.1. Использование языка UML для создания моделей процессов и систем защиты информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Язык UML — это:

1. Язык программирования
2. Методология разработки ПО
3. Язык графического моделирования
4. Стандарт шифрования данных

2. К какому типу диаграмм UML относится диаграмма вариантов использования (Use Case)?

1. Структурные диаграммы
2. Поведенческие диаграммы
3. Диаграммы взаимодействия
4. Диаграммы развертывания

Тема 5.2. Разработка модели требований к системе или подсистеме к выбранному объекту исследования с использованием UML диаграммы вариантов использования

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как на диаграмме Use Case обозначается злоумышленник?

1. Красным квадратом
2. Черной фигуркой человечка
3. Перечеркнутым кругом
4. Пунктирной линией

2. Какое отношение показывает, что один вариант использования является расширением базового сценария при выполнении определенных условий?

1. <<include>>
2. '<<extend>>'
3. <<use>>
4. <<realize>>

Тема 5.3. Разработка модели сценариев взаимодействия, включающих действия злоумышленника и ответные шаги системы защиты и/или отдела информационной безопасности, на выбранном объекте исследования с использованием нотации UML диаграммы деятельности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой элемент диаграммы деятельности (Activity Diagram) используется для обозначения параллельного выполнения действий?

1. Ромб (Decision Node)
2. Жирная черта разделения/слияния (Fork/Join)
3. Черный круг (Initial Node)
4. Прямоугольник с закругленными углами

2. Что на диаграмме деятельности обозначают «Дорожки»?

1. Последовательность действий во времени
2. Альтернативные потоки данных
3. Зоны ответственности
4. Типы передаваемых данных

Раздел 6. Процесс формирования требований к защите информации, содержащейся в государственной информационной системе

Контролируемые ИДК: ОПК-2.2.1 ОПК-2.2.2 ОПК-2.2.3

Тема 6.1. Процесс формирования требований к защите информации, содержащейся в государственной информационной системе

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой документ является основным при определении требований к защите информации в государственных информационных системах на момент 2025 года?

1. Приказ ФСБ № 21
2. Приказ ФСТЭК России № 17
3. Доктрина информационной безопасности РФ
4. Гражданский кодекс РФ

2. Сколько классов защищенности установлено для ГИС?

1. Три (K1, K2, K3)
2. Четыре (K1, K2, K3, K4)
3. Пять (1Г, 1В, 1Б, 2А, 3А)
4. Семь (по модели OSI)

3. Кто обязан формировать требования к защите информации в ГИС?

1. Разработчик программного обеспечения
2. ФСТЭК России
3. Владелец информации
4. Интернет-провайдер

4. При классификации ГИС учитываются:

1. Стоимость оборудования и ПО
2. Уровень значимости информации и масштаб системы
3. Количество системных администраторов
4. Скорость интернет-соединения

8. Оценочные материалы промежуточной аттестации

Вопросы/Задания:

1. Понятие модели, системный подход и моделирование как способ снижения сложности. Цели и задачи моделирования процессов и систем защиты информации.
2. Обзор возможных теоретических основ, на которых могут быть основаны модели процессов и систем защиты информации.
3. Понятие системы, интенсивно использующей программное обеспечение. Связь этого понятия и понятия «информационная система». Понятие архитектуры системы, интенсивно использующей программное обеспечение. Примеры систем, интенсивно использующих программное обеспечение.
4. Использование математического аппарата теории графов для построения моделей безопасности систем. Модель безопасности с полным перекрытием множества угроз.
5. Методология функционального моделирования и графическая нотация IDEF0.
6. Методология моделирования, основанная на построении диаграмм потоков данных. Графическая нотация диаграмм потоков данных.
7. Понятия модели угроз и модели нарушителя.
8. Различные варианты моделей безопасности информации (стандартная модель безопасности, гексада Паркера, модель 5A, модель STRIDE).
9. Использование диаграмм потоков данных для разработки модели угроз.
10. Моделирование рисков информационной безопасности. Оценка рисков с помощью методики DREAD.
11. Пример использования нотации IDEF0 для моделирования процесса анализа рисков информационной безопасности на базе модели с полным перекрытием множества угроз.
12. Язык UML (история, базовые идеи, сферы применения). Концептуальная модель языка UML.
13. Диаграммы использования UML. Графическая нотация и область применения.
14. Диаграммы деятельности UML. Графическая нотация и область применения.
15. Диаграммы компонентов UML. Графическая нотация и область применения.
16. Понятие государственной информационной системы. Требования законодательства РФ к процессу формирования требований к защите информации, содержащейся в государственной информационной системе, использование моделирования в этом процессе.

17. Место и роль изученных методологий моделирования в процессах определения угроз безопасности информации и разработке модели угроз для информационных систем. Требования ФСТЭК к определению угроз безопасности информации и разработке модели угроз для государственных информационных систем.

18. Концепция Misuse Case и ее использование для моделирования атак.

19. Процесс формирования требований к защите информации в ГИС согласно Приказу ФСТЭК № 17.

20. Роль моделирования в создании системы защиты информации ГИС.

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации: учебное пособие: учебное пособие / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков [и др.] - Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации - Саратов: Вузовское образование, 2024. - 265 с. - 978-5-4487-0942-5. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/134999.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Голембиовская О. М. Формализация подходов к обеспечению защиты персональных данных: монография: монография / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков. - Формализация подходов к обеспечению защиты персональных данных - Саратов: Ай Пи Эр Медиа, 2019. - 198 с. - 978-5-4486-0726-4. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/81851.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Богульская Н. А. Модели безопасности компьютерных систем: учебное пособие: учебное пособие / Н. А. Богульская, М. М. Кучеров. - Модели безопасности компьютерных систем - Красноярск: Сибирский федеральный университет, 2019. - 206 с. - 978-5-7638-4008-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/100055.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

4. Методы и средства комплексной защиты информации в технических системах: учебное пособие: учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.] - Методы и средства комплексной защиты информации в технических системах - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2019. - 224 с. - 978-5-9515-0429-6. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/101925.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

5. Петров А. В. Моделирование процессов и систем / А. В. Петров. - Санкт-Петербург: Лань, 2022. - 288 с. - 978-5-8114-1886-2. - Текст: электронный. // Издательство Лань: [сайт]. - URL: <https://e.lanbook.com/img/cover/book/212213.jpg> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Морозова В. И. Функциональное и объектное проектирование информационных систем: учебно-методическое пособие к выполнению практических работ: учебно-методическое пособие к выполнению практических работ / В. И. Морозова, К. Э. Врублевский. - Функциональное и объектное проектирование информационных систем - Москва: Российский университет транспорта (МИИТ), 2021. - 58 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/122064.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Иванова О. Г. Методы и средства проектирования информационных систем и технологий. Основы UML: учебное пособие: учебное пособие / О. Г. Иванова, Ю. Ю. Громов. - Методы и средства проектирования информационных систем и технологий. Основы UML - Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2020. - 80 с. - 978-5-8265-2308-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/115768.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Михайлов В. В. Администрирование информационных систем: учебное пособие: учебное пособие / В. В. Михайлов. - Администрирование информационных систем - Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2017. - 112 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/80407.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

4. Белаш В. Ю. Моделирование потоков данных в информационных системах: учебное пособие: учебное пособие / В. Ю. Белаш, Н. В. Тимошина. - Моделирование потоков данных в информационных системах - Саратов: Вузовское образование, 2024. - 58 с. - 978-5-4487-1014-8. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/142500.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

5. Сунгатуллина А. Т. Системный анализ и проектирование информационных систем на основе объектно-ориентированного подхода: учебно-методическое пособие по дисциплине «методы и средства проектирования информационных систем»: учебно-методическое пособие по дисциплине «методы и средства проектирования информационных систем» / А. Т. Сунгатуллина. - Системный анализ и проектирование информационных систем на основе объектно-ориентированного подхода - Москва: Российский университет транспорта (МИИТ), 2020. - 118 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/115990.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. <https://www.iprbookshop.ru/> - IPR BOOKS
2. <https://e.lanbook.com/> - Электронная библиотечная система "Лань"
3. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

Не используется.

*Перечень информационно-справочных систем
(обновление выполняется еженедельно)*

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс

Маркерная доска - 0 шт.

Моноблок - 64 шт.

Проектор - 4 шт.

Смешанный тип

Автоматизированное рабочее место (АРМ) - 1 шт.

Доска настенная одноэлементная - 2 шт.

Интерактивная панель - 1 шт.

Проектор - 1 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.