МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ

Кафедра информационной безопасности

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 10.03.01 Информационная безопасность
Наименование направленности: Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Уровень квалификации выпускника (бакалавр)

Форма обучения (очная)

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2021*

Моделирование процессов и систем защиты информации
Рабочая программа дисциплины
Составитель:
К.т.н, доцент, доцент, Н.В.Гришина

Ответственный редактор
К.и.н., доцент, зав.кафедрой, Г.А.Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры ИБ
№10 от 20.05.2021

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины - формирование у студентов достаточно полного представления о существующих методах, средствах, методологиях и технологиях моделирования процессов и систем защиты информации.

Задачи дисциплины: ознакомить студентов с основными понятиями и подходами моделирования процессов и систем защиты информации; научить разрабатывать модели систем и процессов, проводить эксперименты на моделях, анализировать результаты моделирования.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1Анализирует имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач	Знать: как определить имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач
	УК-2.2 Способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения	Уметь: использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1 Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта	Знать: принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта
	ОПК-12.2 Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и	Уметь: определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и

	отдельных методов и средств защиты информации	отдельных методов и средств защиты информации
	ОПК-12.3 Владеет навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений	Владеть: навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений
ПК-12 Способен принимать участие в проведении экспериментальных исследований системы защиты информации	ПК-12.1 Знает методы и технологии проектирования, моделирования, исследования систем защиты информации	Знать: основные методы моделирования процессов и систем защиты информации, основные принципы и приемы построения моделей
	ПК-12.2 Умеет выполнять сбор, обработку, анализ и систематизацию информации в области защиты информации	Уметь: анализировать результаты процесса моделирования, формулировать предложения по оптимизации и улучшению функционирования моделируемой системы или процесса
	ПК-12.3 Владеет навыками по разработке и исследованию конкретных явлений и процессов для решения расчетных и исследовательских задач	Владеть: навыками анализа результатов процесса моделирования, формулирования предложений по оптимизации и улучшению функционирования моделируемой системы или процесса

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Моделирование процессов и систем защиты информации» относится к обязательной части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: Методы принятия организационно-технических решений, Математические основы защиты информации.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: Управление информационными рисками, Преддипломная практика.

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет 152 з.е., 4 ч., в том числе контактная работа обучающихся с преподавателем 80 ч., промежуточная аттестация 18ч., самостоятельная работа обучающихся 54 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации
			Контактная				Промежуточная аттестация	Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия			
1	Основные понятия теории моделирования	6	4		4			2	Опрос, участие в дискуссии на практическом занятии
2	Значение моделирования процессов защиты информации. Группы моделей защиты	6	2		4			4	Опрос, участие в дискуссии на практическом занятии
3	Графовые модели систем защиты информации	6	2		4			4	Опрос, участие в дискуссии на практическом занятии
4	Разработка модели угроз безопасности информации в информационных системах	6	4		6			10	Опрос, участие в дискуссии на практическом занятии
5	Разработка модели нарушителя, который может реализовать угрозы безопасности информации в информационной системе	6	4		8			10	Опрос, участие в дискуссии на практическом занятии
6	Модели управления доступом к информации	6	4		6			6	Опрос, участие в дискуссии на практическом занятии,

									выступление с докладом
7	Моделирование управления информационной безопасностью	6	4		6			6	Опрос, участие в дискуссии на практическом занятии
8	Организационные модели подразделений информационной безопасности	6	4		6			6	Опрос, участие в дискуссии на практическом занятии, выступление с докладом
9	Разработка функциональных моделей процессов и систем	6	4		4			6	Опрос, участие в дискуссии на практическом занятии
	экзамен						18		экзамен по билетам.
	итого: 152		**32**		**48**		**18**	**54**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1.	Основные понятия теории моделирования	Терминология в области моделирования процессов и систем. Модель. Моделирование. Процесс и процессный подход. Система и системный подход. Классификация моделей. Требования, предъявляемые к моделям. Этапы моделирования
2.	Значение моделирования процессов защиты информации. Группы моделей защиты	Концептуальные модели. Модели управления безопасностью. Модели отношений доступа и действий. Потоковые модели
3.	Графовые модели систем защиты информации	Краткие сведения из теории графов. Матричное представление. Матрица смежности. Матрица инцидентности. Список смежности. Список ребер. Графовые модели компьютерных атак. State Enumeration graph, condition-oriented dependency graph, exploit dependency graph. Национальная база данных уязвимостей (NIST США). Риск-ориентированные графовые модели систем защиты информации
4.	Разработка модели угроз безопасности информации в информационных системах	Порядок определения и моделирования угроз безопасности информации. Основные нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах. Банк данных угроз безопасности информации. Классификация факторов, воздействующих на информацию. Разработка модели угроз. Классификация угроз безопасности персональных данных. Угрозы утечки информации по техническим каналам. Угрозы несанкционированного доступа к информации в информационной системе персональных данных. Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Методика определения актуальных угроз. Последовательность действий по определению требований по защите ИСПДн и выбору орг. и технич. мер по обеспечению безопасности Пдн. Требования к разработке модели угроз безопасности информации, не содержащей гос. тайну в государственных информационных системах.
5.	Разработка модели нарушителя, который может реализовать угрозы безопасности информации в информационной системе	Основные нормативно-правовые акты, регламентирующие вопросы разработки моделирования нарушителя. Требования ФСТЭК к разработке модели нарушителя. Требования ФСБ к разработке модели нарушителя. Разработка модели нарушителя на основе комбинирования подходов ФСБ и ФСТЭК.

6.	Модели управления доступом к информации	Несанкционированный доступ к информации и полномочия ФСТЭК по его предотвращению. Дискреционная модель управления доступом. Мандатная (многоуровневая) модель управления доступом. Ролевая модель управления доступом
7.	Моделирование управления информационной безопасностью	Терминология в области управления информационной безопасностью. Процессный подход в серии стандартов ГОСТ Р ИСО 9000. Цикл Шухарта-Деминга PDCA Основы управления информационной безопасностью. Иерархия процессов управления внутренними ИТ и ИБ. Признаки эффективного управления ИБ. Модель системы управления информационной безопасностью. Этапы разработки и внедрения СУИБ.
8.	Организационные модели подразделений информационной безопасности	Организационные структуры органов управления организации. Иерархия управления. Линейная (иерархическая, бюрократическая), функциональная, линейно-функциональная, линейно-штабная, дивизиональная, матричная, множественная. Организационные структуры подразделений ИБ организации. Организационная структура и функции службы ИБ предприятия. Организационная структура и функции департамента информационных технологий. Рекомендации экспертов Института программирования Университета Карнеги-Меллон по организационной структуре подразделений ИБ. Ключевые позиции, отвечающие за ИБ: CISO, BISO. Организационная модель управления подразделениями ИБ на основе лучших мировых практик
9.	Разработка функциональных моделей процессов и систем	Методологии и средства структурного моделирования процессов и систем. Методология SADT. Семейство методологий моделирования IDEF. Раскрашенные сети Петри. Методология функционального моделирования IDEF0. Методология событийного моделирования IDEF3

4. Образовательные технологии

Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	Основные понятия теории моделирования	Лекция 1. Практическое занятие 1. Самостоятельная	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Консультирование и проверка домашних

		работа	заданий посредством электронной почты
2.	Значение моделирования процессов защиты информации. Группы моделей защиты	Лекция 2. Практическое занятие 2. Самостоятельная работа	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Консультирование и проверка домашних заданий посредством электронной почты
3.	Графовые модели систем защиты информации	Лекция 3. Практическое занятие 3. Самостоятельная работа	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Консультирование и проверка домашних заданий посредством электронной почты
4.	Разработка модели угроз безопасности информации в информационных системах	Лекция 4. Практическое занятие 4. Самостоятельная работа	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Консультирование и проверка домашних заданий посредством электронной почты
5.	Разработка модели нарушителя, который может реализовать угрозы безопасности информации в информационной системе	Лекция 5. Практическое занятие 5. Самостоятельная работа	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Выступления с докладами. Консультирование и проверка домашних заданий посредством электронной почты
6.	Модели управления доступом к информации	Лекция 6. Практическое занятие 6. Самостоятельная работа	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Выступления с докладами. Консультирование и проверка домашних заданий посредством электронной почты
7	Моделирование управления информационной безопасностью	Лекция 7. Практическое занятие 7. Самостоятельная работа	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Консультирование и проверка домашних заданий посредством электронной почты
8	Организационные модели подразделений информационной безопасности	Лекция 8. Практическое занятие 8. Самостоятельная работа	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Выступления с докладами. Консультирование и проверка домашних заданий посредством электронной почты
9	Разработка	Лекция 9.	Лекция с использованием видеоматериалов

	функциональных моделей процессов и систем	Практическое занятие 9. Самостоятельная работа	Развернутая беседа с обсуждением лекции. Опрос. Консультирование и проверка домашних заданий посредством электронной почты

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос на пр. занятии* *- участие в дискуссии на пр. занятии* *- выступление с докладом*	 *3 балла* *2 балла* *5 баллов*	 *27 баллов* *18 баллов* *15 баллов*
Промежуточная аттестация *экзамен*		*40 баллов*
Итого за семестр *экзамен*		*100 баллов*

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	*«отлично»*	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	*«хорошо»*	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	*«удовлетвори-тельно»*	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине.

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Примерные темы докладов:

1. Концептуальные модели. УК-2
2. Модели управления безопасностью. ОПК-12
3. Модели отношений доступа и действий. УК-2
4. Потоковые модели ОПК-12
5. Графовые модели компьютерных атак. State Enumeration graph. ОПК-12
6. Графовые модели компьютерных атак. ОПК-12
7. Графовые модели компьютерных атак. ПК-12
8. Национальная база данных уязвимостей ПК-12
9. Банк данных угроз безопасности информации. ПК-12
10. Процессный подход в серии стандартов ГОСТ Р ИСО 27000. ПК-12

Перечень вопросов для проведения опроса на практическом занятии:

1. Определение модели, моделирования. ПК-12
2. Требования, предъявляемые к моделям. ОПК-12
3. Что такое процесс? УК-2
4. В чем суть процессного подхода? ОПК-12
5. Дайте определение системы. ОПК-12
6. В чем суть системного подхода? ПК-12
7. Классификация моделей. УК-2
8. Назовите этапы моделирования. УК-2
9. Что такое матрица смежности? УК-2
10. Что такое матрица инцидентности? ПК-12

Промежуточная аттестация (примерные контрольные вопросы по курсу)

1. Определение модели, моделирования. Требования, предъявляемые к моделям. УК-2
2. Процесс и процессный подход. ОПК-12
3. Система и системный подход. ПК-12
4. Модель. Классификация моделей. Этапы моделирования. ПК-12
5. Матричное представление графа. Матрица смежности. ОПК-12
6. Матричное представление графа. Матрица инцидентности. УК-2
7. Графовые модели компьютерных атак. УК-2
8. Риск-ориентированные графовые модели систем защиты информации. ОПК-12
9. Порядок определения и моделирования угроз безопасности информации. ПК-12
10. Основные нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах. УК-2
11. Классификация факторов, воздействующих на информацию. ОПК-12
12. Разработка модели угроз. УК-2
13. Классификация угроз безопасности персональных данных. УК-2
14. Угрозы утечки информации по техническим каналам. ОПК-12
15. Угрозы несанкционированного доступа к информации в информационной системе персональных данных. ПК-12
16. Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных. УК-2
17. Методика определения актуальных угроз. УК-2
18. Последовательность действий по определению требований по защите ИСПДн и выбору организационных и технических мер по обеспечению безопасности Пдн. УК-2
19. Требования к разработке модели угроз безопасности информации, не содержащей государственную тайну в государственных информационных системах. ПК-12
20. Основные нормативно-правовые акты, регламентирующие вопросы разработки моделирования нарушителя. ОПК-12
21. Требования ФСТЭК к разработке модели нарушителя. УК-2
22. Требования ФСБ к разработке модели нарушителя. УК-2
23. Разработка модели нарушителя на основе комбинирования подходов ФСБ и ФСТЭК. ПК-12
24. Несанкционированный доступ к информации и полномочия ФСТЭК по его предотвращению. ОПК-12
25. Дискреционная модель управления доступом. ПК-12
26. Мандатная (многоуровневая) модель управления доступом. ОПК-12
27. Ролевая модель управления доступом. УК-2
28. Терминология в области управления информационной безопасностью. ОПК-12
29. Процессный подход в серии стандартов ГОСТ Р ИСО 9000. Цикл Шухарта-Деминга PDCA ОПК-12
30. Основы управления информационной безопасностью. Иерархия процессов управления внутренними ИТ и ИБ. УК-2
31. Признаки эффективного управления ИБ. ОПК-12
32. Модель системы управления информационной безопасностью. ПК-12
33. Этапы разработки и внедрения СУИБ. ПК-12
34. Организационные структуры органов управления организации. Иерархия управления.
35. Линейная (иерархическая, бюрократическая) структура органов управления организации. ПК-12
36. Функциональная структура органов управления организации. УК-2
37. Линейно-функциональная структура органов управления организации. ОПК-12
38. Линейно-штабная структура органов управления организации. ПК-12
39. Дивизиональная структура органов управления организации. ОПК-12
40. Матричная структура органов управления организации. ПК-12

41. Множественная структура органов управления организации. УК-2
42. Организационная структура и функции службы ИБ предприятия. ПК-12
43. Организационная структура и функции департамента информационных технологий. ПК-12
44. Методологии и средства структурного моделирования процессов и систем. Методология SADT. УК-2
45. Семейство методологий моделирования IDEF. ПК-12
46. Раскрашенные сети Петри. ОПК-12
47. Методология функционального моделирования IDEF0. ОПК-12
48. Методология событийного моделирования IDEF3. УК-2

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Литература

Основная

1. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина. - Москва : ИНФРА-М, 2021. - 216 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178150 (дата обращения: 12.05.2021). – Режим доступа: по подписке.
2. Шелухин, О.И. Моделирование информационных систем. Учебное пособие для вузов. - 2-е изд., перераб. и доп. - М.: Горячая линия-Телеком, 2012. - 516 с.: ил. ISBN 978-5-9912-0193-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/366067 (дата обращения: 12.05.2021). – Режим доступа: по подписке.

дополнительная

3. Исаев, Г. Н. Моделирование информационных ресурсов: теория и решение задач: учебное пособие / Г.Н. Исаев. - Москва : Альфа-М: ИНФРА-М, 2010. - 224 с.: ил.; . ISBN 978-5-98281-211-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/193771 (дата обращения: 12.05.2021). – Режим доступа: по подписке.
4. Чикуров, Н. Г. Моделирование систем и процессов: Учебное пособие / Н.Г. Чикуров. - М.: ИЦ РИОР: НИЦ Инфра-М, 2019. - 398 с.:- (Высшее образование: Бакалавриат). - ISBN 978-5-369-01167-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1010810 (дата обращения: 12.05.2021). – Режим доступа: по подписке.
5. Тимохин, А. Н. Моделирование систем управления с применением MatLab : учебное пособие / А. Н. Тимохин, Ю. Д. Румянцев ; под ред. А. Н. Тимохина. — Москва : ИНФРА-М, 2020. — 256 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-010185-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1117213 (дата обращения: 12.05.2021). – Режим доступа: по подписке.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной

	подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Состав программного обеспечения (ПО)

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
  - устройством для сканирования и чтения с камерой SARA CE;
  - дисплеем Брайля PAC Mate 20;
  - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
  - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - передвижными, регулируемыми эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий .

Практическое занятие:

Тема 1 (Основные понятия теории моделирования) ПК-12

Задания:

1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.

Указания по выполнению заданий:

1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.

Список литературы:

[3, 4, 5] (см. Подраздел 6.1)

Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:

Тема 2 (Значение моделирования процессов защиты информации. Группы моделей защиты) УК-2

Задания:

1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.

Указания по выполнению заданий:

1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.

Список литературы:

[1, 2] (см. Подраздел 6.1)

Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:

Тема 3 (Графовые модели систем защиты информации) ПК-12

Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
Список литературы:
[1, 2, 3] (см. Подраздел 6.1)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:
Тема 4 (Разработка модели угроз безопасности информации в информационных системах) УК-2
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя.
2. Ответить на вопросы по теме занятия и ранее изученному материалу
Список литературы:
[1, 2] (см. Подраздел 6.1), [4] (см. Подраздел 6.2)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:
Тема 5 (Разработка модели нарушителя, который может реализовать угрозы безопасности информации в информационной системе) ОПК-12
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
3. Выступления с докладами.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя.
2. Ответить на вопросы по теме занятия и ранее изученному материалу
3. Выступить с докладом с использованием презентации. Ответить на заданные вопросы.
Список литературы:
[1, 2] (см. Подраздел 6.1), [4] (см. Подраздел 6.2)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:
Тема 6 (Модели управления доступом к информации) УК-2
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
3. Выступления с докладами.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя.
2. Ответить на вопросы по теме занятия и ранее изученному материалу
3. Выступить с докладом с использованием презентации. Ответить на заданные вопросы.
Список литературы:
[1, 2] (см. Подраздел 6.1)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски, раздаточный материал для тестирования.

Практическое занятие:
Тема 7 (Моделирование управления информационной безопасностью) ОПК-12
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
Список литературы:
[1, 4, 7] (см. Подраздел 6.1), [4] (см. Подраздел 6.2)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски, раздаточный материал для тестирования.

Практическое занятие:
Тема 8 (Организационные модели подразделений информационной безопасности)
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
3. Выступления с докладами.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя.
2. Ответить на вопросы по теме занятия и ранее изученному материалу
3. Выступить с докладом с использованием презентации. Ответить на заданные вопросы.
Список литературы:

[1, 2, 6] (см. Подраздел 6.1), [4] (см. Подраздел 6.2)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски, раздаточный материал для тестирования.

Практическое занятие:
Тема 9 (Разработка функциональных моделей процессов и систем)
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
Список литературы:
[1, 2] (см. Подраздел 6.1), [4] (см. Подраздел 6.2)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски, раздаточный материал для тестирования.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Моделирование процессов и систем защиты информации» реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.

Цели дисциплины: формирование у студентов достаточно полного представления о существующих методах, средствах, методологиях и технологиях моделирования процессов и систем защиты информации.

Задачи дисциплины: ознакомить студентов с основными понятиями и подходами моделирования процессов и систем защиты информации; научить разрабатывать модели систем и процессов, проводить эксперименты на моделях, анализировать результаты моделирования.

Дисциплина направлена на формирование следующих компетенций:

- УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;

В результате освоения дисциплины (модуля) обучающийся должен:

- Анализирует имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач
- Способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения

- ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта
- Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации
- Владеет навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений

- ПК-12 Способен принимать участие в проведении экспериментальных исследований системы защиты информации.

В результате освоения дисциплины обучающийся должен:

- Знает методы и технологии проектирования, моделирования, исследования систем защиты информации
- Умеет выполнять сбор, обработку, анализ и систематизацию информации в области защиты информации
- Владеет навыками по разработке и исследованию конкретных явлений и процессов для решения расчетных и исследовательских задач

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы.