МИНОБРНАУКИ РОССИИ

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

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра информационной безопасности

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

по направлению подготовки (специальности)
10.03.01 Информационная безопасность
по профилю:
Комплексная защита объектов информатизации
Уровень квалификация выпускника - бакалавр
Форма обучения очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2017*

Моделирование процессов и систем защиты информации
Рабочая программа дисциплины
Составитель:
Кандидат технических наук, доцент, доцент кафедры информационной безопасности Карпов Дмитрий Сергеевич

Ответственный редактор
к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры информационной безопасности
№ 5 от 24.01.2017

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

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.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Коды компетенции	**Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	1) Знать: - терминологию моделирования процессов и систем защиты информации; - основные методы моделирования процессов и систем защиты информации, основные принципы и приемы построения моделей; - основные нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах; - методологии и средства структурного моделирования процессов и систем 2) Уметь: - использовать нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах; - использовать принципы и методы моделирования процессов и систем защиты информации; - использовать методологии и средства моделирования процессов и систем, основные принципы и приемы построения моделей; - уметь анализировать результаты процесса моделирования, формулировать предложения по оптимизации и улучшению функционирования моделируемой системы или процесса. Владеть: - терминологией моделирования процессов и систем защиты информации; - навыками использования правовых и нормативных требований к определению и моделированию угроз безопасности информации в информационных системах; методологиями и средствами моделирования процессов и систем; - навыками анализа результатов процесса моделирования, формулирования предложений по оптимизации и
ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации	
ПСК-3.1	способностью проводить анализ функционального процесса объекта информатизации	

	с целью выявления вероятных угроз информационной безопасности, определения их источников и целей	улучшению функционирования моделируемой системы или процесса.

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Моделирование процессов и систем защиты информации» относится к вариативной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: Математический анализ, Информационные технологии, Сети и системы передачи информации, Программно-аппаратные средства защиты информации, Информационные процессы и системы. Вычислительные сети, Функциональный процесс и организация предприятия.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: Основы управления информационной безопасностью, Комплексное обеспечение безопасности объекта информатизации, Защита информационных процессов в автоматизированных системах, Проектирование систем защиты объектов информатизации, преддипломная практика.

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоемкость дисциплины составляет 4 з. е., 144 ч., в том числе контактная работа обучающихся с преподавателем 56 ч., самостоятельная работа обучающихся 88 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Основные понятия теории моделирования*	**6**	**4**		**2**			***8***	Опрос, участие в дискуссии на практическом занятии
2	*Значение моделирования процессов защиты информации. Группы моделей защиты*	**6**	**2**		**4**			***10***	Опрос, участие в дискуссии на практическом занятии
3	*Графовые модели*	**6**	**2**		**2**			***10***	Опрос, участие

	систем защиты информации								в дискуссии на практическом занятии
4	*Разработка модели угроз безопасности информации в информационных системах*	**6**	**4**		**4**			***10***	Опрос, участие в дискуссии на практическом занятии
5	*Разработка модели нарушителя, который может реализовать угрозы безопасности информации в информационной системе*	**6**	**4**		**4**			***10***	Опрос, участие в дискуссии на практическом занятии
6	*Модели управления доступом к информации*	**6**	**2**		**4**			***10***	Опрос, участие в дискуссии на практическом занятии, выступление с докладом
7	*Моделирование управления информационной безопасностью*	**6**	**2**		**4**			***10***	Опрос, участие в дискуссии на практическом занятии
8	*Организационные модели подразделений информационной безопасности*	**6**	**2**		**4**			***10***	Опрос, участие в дискуссии на практическом занятии, выступление с докладом
9	*Разработка функциональных моделей процессов и систем*	**6**	**2**		**4**			***10***	Опрос, участие в дискуссии на практическом занятии
	зачет с оценкой								
	итого:		**24**		**32**			**88**	

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

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	Основные понятия теории моделирования	*Лекция 1.* *Практическое занятие 1.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос.* *Консультирование и проверка домашних 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 функциональных моделей процессов и систем	*Лекция 9.* *Практическое занятие 9.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *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*	*3 балла*	*27 баллов*

- участие в дискуссии на пр. занятии	*2 балла*	*18 баллов*
- выступление с докладом	*5 баллов*	*15 баллов*
Промежуточная аттестация *(зачет с оценкой)*		*40 баллов*
Итого за семестр *(дисциплину)*		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	1-5	ОПК-7, ПК-12	- оценка по итогам опроса на пр. занятии - оценка по итогам участия в дискуссии на пр. занятии - оценка выступления с докладом
2.	6-9	ПК-12, ПСК-3.1	

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»/ «зачтено (отлично)»/ «зачтено»	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»/ «зачтено (хорошо)»/ «зачтено»	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»/ «зачтено (удовлетвори-тельно)»/ «зачтено»	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. Оценка по дисциплине выставляются обучающемуся

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		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 **- *проверка сформированности компетенций ОПК-7, ПК-12, ПСК-3.1***

1. Концептуальные модели. - *ОПК-7, ПК-12*
2. Модели управления безопасностью. - *ПК-12, ПСК-3.1*
3. Модели отношений доступа и действий. - *ОПК-7, ПК-12*
4. Потоковые модели - *ПК-12, ПСК-3.1*
5. Графовые модели компьютерных атак. State Enumeration graph. - *ОПК-7, ПК-12*
6. Графовые модели компьютерных атак. Condition-oriented dependency graph. - *ПК-12, ПСК-3.1*
7. Графовые модели компьютерных атак. Exploit dependency graph. - *ОПК-7, ПК-12*
8. Национальная база данных уязвимостей (NIST США). - *ПК-12, ПСК-3.1*
9. Банк данных угроз безопасности информации. - *ОПК-7, ПК-12*
10. Процессный подход в серии стандартов ГОСТ Р ИСО 27000. - *ПК-12, ПСК-3.1*

Перечень вопросов для проведения опроса на практическом занятии: - ***проверка сформированности компетенций ОПК-7, ПК-12, ПСК-3.1***

1. Определение модели, моделирования. - *ОПК-7, ПК-12*
2. Требования, предъявляемые к моделям. - *ПК-12, ПСК-3.1*
3. Что такое процесс? - *ОПК-7, ПК-12*
4. В чем суть процессного подхода? - *ОПК-7, ПК-12*
5. Дайте определение системы. - *ПК-12, ПСК-3.1*
6. В чем суть системного подхода? - *ОПК-7, ПК-12*
7. Классификация моделей. - *ПК-12, ПСК-3.1*

8. Назовите этапы моделирования- *ОПК-7, ПК-12*
9. Что такое матрица смежности? - *ОПК-7, ПК-12*
10. Что такое матрица инцидентности? - *ПК-12, ПСК-3.1*

Промежуточная аттестация (примерные контрольные вопросы по курсу) - проверка сформированности компетенций - ОПК-7, ПК-12, ПСК-3.1

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

35. Линейная (иерархическая, бюрократическая) структура органов управления организации
36. Функциональная структура органов управления организации
37. Линейно-функциональная структура органов управления организации
38. Линейно-штабная структура органов управления организации
39. Дивизиональная структура органов управления организации.
40. Матричная структура органов управления организации.
41. Множественная структура органов управления организации.
42. Организационная структура и функции службы ИБ предприятия.
43. Организационная структура и функции департамента информационных технологий.
44. Методологии и средства структурного моделирования процессов и систем. Методология SADT.
45. Семейство методологий моделирования IDEF.
46. Раскрашенные сети Петри.
47. Методология функционального моделирования IDEF0.
48. Методология событийного моделирования IDEF3

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Основная литература

а) основная:

1. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/612572, свободный. — Загл. с экрана. — Яз. рус.

2. Моделирование информационных систем: Учебное пособие для вузов / О.И. Шелухин. - 2-е изд., перераб. и доп. - М.: Гор. линия-Телеком, 2012. - 536 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/366067, свободный. — Загл. с экрана. — Яз. рус.

б) Дополнительная литература

3. Моделирование информационных ресурсов: теория и решение задач: учебное пособие / Г.Н. Исаев. - М.: Альфа-М: ИНФРА-М, 2010. - 224 с.[Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/193771, свободный. — Загл. с экрана. — Яз. рус.

4. Моделирование систем и процессов: Учебное пособие / Н.Г. Чикуров. - М.: ИЦ РИОР: НИЦ Инфра-М, 2013. - 398 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/392652, свободный. — Загл. с экрана. — Яз. рус.

5. Моделирование систем управления с применением Matlab : учеб. пособие / А.Н. Тимохин, Ю.Д. Румянцев ; под ред. А.Н. Тимохина. — М. : ИНФРА-М, 2017. — 256 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/590240, свободный. — Загл. с экрана. — Яз. рус.

в) Информационно-справочная литература

6. Вопросы управления информационной безопасностью: Учебное пособие для вузов. Основы управления информационной безопасностью / Курило А.П., Милославская Н.Г., Сенаторов М.Ю. - М.: Гор. линия-Телеком, 2013. - 244 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/author/74047029-373f-11e4-b05e-00237dd2fde2, свободный. — Загл. с экрана. — Яз. рус.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Федеральный портал по научной и инновационной деятельности [Электронный ресурс] — Режим доступа: http://www.sci-innov.ru, свободный. — Загл. с экрана. — Яз. рус., англ.
2. Научная электронная библиотека eLibrary [Электронный ресурс] — Режим доступа: http://www.elibrary.ru, свободный. — Загл. с экрана. — Яз. рус., англ.
3. Росстандарт. Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс] — Режим доступа: http://www.gost.ru, свободный. — Загл. с экрана. — Яз. рус., англ.
4. Консультант плюс [Электронный ресурс] — Режим доступа: http://www.consultant.ru, свободный. — Загл. с экрана. — Яз. рус., англ.

7. Материально-техническое обеспечение дисциплины/модуля

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

Современный компьютерный класс оснащен Microsoft Office 2010, включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

Перечень ПО

№ п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

Перечень БД и ИСС

№п/п	Наименование
1	Компьютерные справочные правовые системы Консультант Плюс, Гарант

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

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 - ***проверка сформированности компетенций - ОПК-7, ПК-12, ПСК-3.1***

Практическое занятие:

Тема 1 (2 ч.) (Основные понятия теории моделирования) - ***проверка сформированности компетенций - ОПК-7, 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 (2 ч.) (Значение моделирования процессов защиты информации. Группы моделей защиты) - ***проверка сформированности компетенций - ПК-12, ПСК-3.1***

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 (2 ч.) (Графовые модели систем защиты информации) - ***проверка сформированности компетенций - ОПК-7, 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 (2 ч.) (Разработка модели угроз безопасности информации в информационных системах) - ***проверка сформированности компетенций - ОПК-7, ПСК-3.1***
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 (2 ч.) (Разработка модели нарушителя, который может реализовать угрозы безопасности информации в информационной системе) - ***проверка сформированности компетенций - ОПК-7, ПК-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 (2 ч.) (Модели управления доступом к информации) - ***проверка сформированности компетенций - ПК-12, ПСК-3.1***

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 (2 ч.) (Моделирование управления информационной безопасностью) - ***проверка сформированности компетенций - ОПК-7, ПСК-3.1***

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 (2 ч.) (Организационные модели подразделений информационной безопасности) - ***проверка сформированности компетенций - ОПК-7, ПСК-3.1***

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 (2 ч.) (Разработка функциональных моделей процессов и систем) - ***проверка сформированности компетенций - ПК-12, ПСК-3.1***

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 (модуль) направлена на формирование следующих компетенций:

ОПК-7 (*способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты*);

ПК-12 (*способность принимать участие в проведении экспериментальных исследований системы защиты информации*);

ПСК-3.1 (*способностью проводить анализ функционального процесса объекта информатизации с целью выявления вероятных угроз информационной безопасности, определения их источников и целей*).

В результате освоения дисциплины (модуля) обучающийся должен:

1) Знать:

- терминологию моделирования процессов и систем защиты информации;
- основные методы моделирования процессов и систем защиты информации, основные принципы и приемы построения моделей;
- основные нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах.
- методологии и средства структурного моделирования процессов и систем

2) Уметь:

- использовать нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах;
- использовать принципы и методы моделирования процессов и систем защиты информации;
- использовать методологии и средства моделирования процессов и систем, основные принципы и приемы построения моделей;
- анализировать результаты процесса моделирования, формулировать предложения по оптимизации и улучшению функционирования моделируемой системы или процесса.

Владеть:

- терминологией моделирования процессов и систем защиты информации;
- навыками использования правовых и нормативных требований к определению и моделированию угроз безопасности информации в информационных системах;
- методологиями и средствами моделирования процессов и систем;

- навыками анализа результатов процесса моделирования, формулирования предложений по оптимизации и улучшению функционирования моделируемой системы или процесса.

По дисциплине предусмотрена промежуточная аттестация в форме *зачета с оценкой*.

Общая трудоемкость освоения дисциплины (модуля) составляет 4 зачетные единицы, 144 часа.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.06.2017г.*	***10***
2	*Обновлена основная и дополнительная литература*	*26.06.2018 г.*	***20***
3	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*26.06.2018 г.*	***20***
4	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.08.2019*	***1***
5	*Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)*	*23.06.2020*	***14***
6	*Обновлена основная и дополнительная литература*	*23.06.2020*	***14***
7	*Обновлен раздел п.4 Образовательные технологии*	*23.06.2020*	***14***
8	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*23.06.2020*	***14***

Приложение 1
к листу изменений

Обновление

1. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2017 г.)

Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2013	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:
Кандидат технических наук, доцент,
доцент кафедры информационной безопасности Д.С. Карпов

Приложение 2
к листу изменений

2. Обновление основной и дополнительной литературы (2018 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

Дополнить раздел ***Основная литература***

Моделирование системы защиты информации. Практикум : учеб. пособие / Е.К. Баранова, А.В. Бабаш. — 2-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2018. — 224 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/916068, свободный. — Загл. с экрана. — Яз. рус.

3. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2018 г.)

Перечень ПО

Таблица 1

№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

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г.

	Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:
Кандидат технических наук, доцент,
доцент кафедры информационной безопасности Д.С. Карпов

Приложение 3
к листу изменений

Обновление

4.Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)

Перечень 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

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 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

Составитель:
Кандидат технических наук, доцент,
доцент кафедры информационной безопасности Д.С. Карпов

Приложение 4
к листу изменений

5. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)

Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 4 з. е., 152 ч., в том числе контактная работа обучающихся с преподавателем 56 ч., самостоятельная работа обучающихся 96 ч., промежуточная аттестация- - ч.

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

	системе									
6	*Модели управления доступом к информации*	**6**	**2**		**4**			***10***		Опрос, участие в дискуссии на практическом занятии, выступление с докладом
7	*Моделирование управления информационной безопасностью*	**6**	**2**		**4**			***10***		Опрос, участие в дискуссии на практическом занятии
8	*Организационные модели подразделений информационной безопасности*	**6**	**2**		**4**			***10***		Опрос, участие в дискуссии на практическом занятии, выступление с докладом
9	*Разработка функциональных моделей процессов и систем*	**6**	**2**		**4**			***16***		Опрос, участие в дискуссии на практическом занятии
	Зачет с оценкой									Зачет с оценкой по билетам
	итого:		**24**		**32**			**96**	**152**	

6. Обновление основной и дополнительной литературы (2020 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

Дополнить раздел **Дополнительная литература**

Жидко, Е. Концепция системного математического моделирования информационной безопасности [Интернет-журнал "Науковедение", Вып. 2 (21), 2014, стр. -]. - Текст : электронный. - URL: https://znanium.com/catalog/product/485597

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

7. В элемент рабочей программы **п.4 Образовательные технологии** вносятся следующие изменения:

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции;

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

8. В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

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

В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

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

Составитель:
К.и.н, доцент, Г.А. Шевцова