Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.07 Моделирование информационной безопасности. Управление рисками
(индекс, наименование дисциплины в соответствии с учебным планом)

38.04.05 Бизнес-информатика
(код, наименование направления подготовки/специальности)

«Аналитическое обеспечение информационной безопасности»
направлению подготовки «бизнес-информатика»

очная
(форма обучения)

Год набора 2026

Город
Санкт-Петербург, 2026 г.

Автор(ы)-составитель(и) РПД:

Сухостат Валентина Васильевна, кандидат техн. наук, кандидат пед. наук, доцент, доцент кафедры бизнес-информатика

Заведующий кафедрой:

Наумов Владимир Николаевич, доктор военных наук, кандидат технических наук, профессор, профессор кафедры бизнес-информатики

Рабочая программа дисциплины Б1.В.01 «Управление информационной безопасностью» одобрена на заседании кафедры бизнес-информатики, факультета экономики и финансов Северо-Западного института управления РАНХиГС.

протокол № 6 от «_26_» _марта_2026 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Дисциплина *Б1.В.07 «Моделирование информационной безопасности. Управление рисками»* обеспечивает формирование у обучающихся следующих универсальных, общепрофессиональных и профессиональных компетенций*:

ОТФ/ТФ и реквизиты ПС (при наличии)**	**Код компетенции ****	**Наименование Компетенции ****	**Код индикатора достижения компетенций ****	**Наименование индикатора достижения компетенций ****	**Образовательный результат ****
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, СВЯЗЬ 06 Связь, информационные и коммуникационные технологии **06.033** Специалист по защите информации в автоматизированных системах утв. приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н **С/С/02.7** Разработка систем защиты	ПКс 2	Способен обосновывать подходы и требования к системе обеспечения информационной безопасности, оценивать уровни безопасности компьютерных систем и сетей	ПКс-2.3.	Оценивает уровни безопасности компьютерных систем и сетей	ПКс.2.3.-Зн.6 **Знать** Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем ПКс.2.3-У-8 **Уметь** Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем

информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости					
Разработка проектных решений по защите информации в автоматизированных системах					

** Дисциплина может формировать компетенцию полностью или частично.*
***Должно соответствовать Приложению 1 к образовательной программе*

2. Объем и место дисциплины в структуре образовательной программы

Общий объем дисциплины *Б1.В.07 «Моделирование информационной безопасности. Управление рисками»* - 4 зачетных единицы – 144 акад.часа; объем академических часов, выделенных на контактную работу обучающихся с преподавателем - 43 акад часа, 83 акад. Часа выделяется на самостоятельную работу; из них

в 3-м семестре:

2 зачетных единицы –72 акад. часа;6 акад. часов – лекции, 8 час – практические занятия, 4 часа – контактная работа на аттестацию в период экзаменационных сессий, и 54 акад. час. выделяется на самостоятельную работу обучающихся;

в 4-м семестре:

2 зачетных единицы - 72 акад. часа, 6 акад. часов – лекции, 8 час – практические занятия, 9 часа – контактная работа на аттестацию в период экзаменационных сессий, и 29 акад. час. выделяется на самостоятельную работу обучающихся.

Место дисциплины в структуре образовательной программы.

Дисциплина изучается в 3-м и 4-м семестрах 2-го курса. Дисциплина Б1.В..07 «Моделирование информационной безопасности. Управление рисками» относится к части дисциплин, формируемых участниками образовательных отношений учебного плана по направлению «Бизнес-информатика» 38.04.05 образовательной программы «Аналитическое обеспечение информационной безопасности». Преподавание дисциплины опирается на дисциплины программы магистратуры Б1.О.04 «Средства информационной безопасности», Б1.О.07 «Аналитическая поддержка принятия решений».

Дисциплина закладывает теоретический и методологический фундамент для овладения умениям и навыками в ходе овладения дисциплинами (модулями) по выбору 3 (ДВ.3), Б2.О.01(У) «Проектно-аналитическая практика» и Б2.О.02 (Н) «Научно-исследовательская работа».

Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при выполнении магистерской диссертации.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов		Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
		ВСЕГО	Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Кат тэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Тема 1	Теоретические и методологические основы моделирования информационной безопасности	72	6			8				4				54	Реферат

Промежуточная аттестация														зачет
Тема 2	Управление рисками	72	6			8				9		18	29	ПКЗ
Промежуточная аттестация									2					экзамен
Итого	144		12			16			2	13		18	83	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения

СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.

СРэк – самостоятельная работа на подготовку к экзамену.

СР – самостоятельная работа в семестре на подготовку к учебным занятиям.

3.2. Содержание дисциплины

Тема 1. Теоретические и методологические основы моделирования информационной безопасности

Основы системного анализа и теории системного моделирования. Цели и задачи системного анализа. Модель как философская категория. Множественность моделей систем. Процедуры системного анализа. Понятие модели. Цели моделирования. Классификация моделей. Принципы системного моделирования. Общий порядок разработки моделей.

Эвристические методы моделирования. Классификация. Индивидуальные и коллективные методы. Инструментальные средства.

Натурные методы моделирования. Классификация. Испытание как метод моделирования систем. Инструментальные средства.

Аналитические методы моделирования. Классификация. Математическое и статическое моделирование. Порядок построения и анализа аналитических моделей.

Структурные технологии моделирования процессов и систем защиты информации. Концепция структурного моделирования процессов и систем защиты информации. Программные средства структурного моделирования, их возможности и особенности использования.

Объектно-ориентированные технологии моделирования процессов и систем защиты информации. Концепция объектно-ориентированного моделирования процессов и систем защиты информации. Программные средства объектно-ориентированного моделирования, их возможности и особенности использования.

Имитационные технологии моделирования процессов и систем защиты информации. Концепция имитационного моделирования процессов и систем защиты информации. Программные средства имитационного моделирования, их возможности и особенности использования.

Интегрированные технологии моделирования процессов и систем защиты информации. Концепция интеграции технологий процессов и систем защиты информации. Интегрированные программные средства моделирования, их возможности и особенности использования.

Тема 2. Управление рисками.

Риск как объект управления. Оценка риска. Идентификация и анализ риска. Методологические основы управления рисками на объекте. Система управления рисками на предприятии.

Стандарты в области управления рисками. Управление рисками информационной безопасности на основе ISO 27005. Управление рисками на основе ГОСТ Р ИСО 31000. Методы анализа риска ГОСТ Р ИСО/МЭК 31010. Процедуры оценки и обработки рисков. Методология оценки рисков ИБ.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1.Оценочныематериалыподисциплине(*наименование*)входятвсостав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа — это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа — это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)
Задание закрытого	Прочитайте	1. Внимательно прочитать текст задания и понять, что в	Ответ считается верным, если

типа на установление последовательности	текст и установите последовательность	качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	правильно указана вся последовательность цифр
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3.Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

Итоговая балльная оценка	**Традиционная система**	**Бинарная система**	**ECTS**	
			Для традиционной системы	**Для бинарной системы**
95-100	Отлично	Зачтено	A	P/ Passed
85-94			B	P/ Passed
75-84	Хорошо		C	P/ Passed
65-74			D	P/ Passed
55-64	Удовлетворительно		E	P/ Passed
0-54	Неудовлетворительно	Не зачтено	F	F/Failed

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

Максимальная сумма баллов за текущий контроль успеваемости	Максимальная сумма баллов за промежуточную аттестацию	Максимальная итоговая балльная оценка	Максимальная сумма баллов за повторную промежуточную аттестацию
60 баллов	40 баллов	100 баллов	100 баллов

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

тестирование, реферат, эссе, упражнения, опрос, контрольная работа, кейс и т.д. (должны совпадать с теми, что отражены в п. 3.1.)

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

Тема 1. Теоретические и методологические основы моделирования информационной безопасности

ПКс-2.3

Типовые темы рефератов с последующей защитой и обсуждением

1. Моделирование систем массового обслуживания в телекоммуникационных системах.
2. Модели принятия решений.
3. Модели взаимодействия двух популяций.
4. Модели безопасности на основе дискреционной политики.
5. Модели безопасности на основе мандатной политики.
6. Модели безопасности на основе тематической политики.
7. Модели безопасности на основе ролевой политики.
8. Автоматные и теоретико-вероятностные модели невлияния и невыводимости.
9. Построение математических моделей угроз ИБ, нарушителя ИБ, защиты ИБ в сетях и системах телекоммуникаций.
10. Модели и технологии обеспечения целостности данных.
11. Модели безопасности в распределенных системах.
12. Моделирование систем управления

Тема 2. Управление рисками
ПКс – 2.3

Практческие контрольные задания

1. *Задание.* «Построение модели угроз ИБ».
Провести идентификацию, анализ и описание основных угроз ИБ для конкретного объекта защиты по выбору обучающегося. Выбор объекта защиты согласовывается с преподавателем. Для каждой угрозы должны быть указаны активы, которым может быть нанесен ущерб в случае ее реализации, источник угрозы, факторы, способствующие возникновению и реализации угрозы ИБ, возможные последствия. Результаты анализа должны быть структурированы и оформлены в виде отчета в среде MS Word.
Выполненное задание защищается преподавателю.
2. *Задание*. «Оценка риска ИБ».
Для объекта защиты, выбранного в контрольном задании 1, провести анализ и оценивание рисков ИБ, соответствующих описанным угрозам. Для каждой угрозы ИБ должны быть определены (качественно или количественно) уровень угрозы (вероятность реализации угрозы) и размер возможного ущерба (уровень негативных последствий). На основании этих значений производится определение уровня риска, ранжирование рисков и выявление критических рисков. Должны быть представлены используемые при оценке шкалы. Результаты оценки рисков оформляются в виде отчета в среде MS Word. Выполненное задание защищается преподавателю.
Вариант организаций
1. Отделение коммерческого банка

2. Поликлиника
3. Колледж
4. Офис страховой компании
5. Рекрутинговое агентство
6. Интернет-магазин
7. Центр оказания государственных услуг
8. Отделение полиции
9. Аудиторская компания
10. Дизайнерская фирма

5.3. Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает 2 КТ в течение периода освоения дисциплины.

Максимальное количество баллов за любой тип работ в рамках КТ составляет 100 (сто) баллов.

Распределение весовых коэффициентов по КТ в рамках текущего контроля успеваемости по дисциплине и формулы расчета:

Расчет по контрольным точкам дисциплины

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать студент	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,3	30
КТ 2	100	0,3	30
Итого:	х	0,6	60

Формула расчета результата контрольной точки:
Результат контрольной точки = Количество баллов за работу в рамках КТ х Коэффициент веса контрольной точки.

5.4. Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

Тема 1
Реферат по теме 1
КТ – 1

Тема 2
Практическое контрольное задание (ПКЗ)
КТ – 2

1. Для каждой формы текущего контроля успеваемости обучающихся в рамках КТ определены критерии оценивания результатов выполнения задания.

Критерии оценивания реферата

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и полнота раскрытия темы *Защита и участие в обсуждении*	*41-70*	*Полное раскрытие темы, представляемая информация систематизирована и логически связана, даны ответы на все вопросы*
	21-40	*Тема раскрыта, представляемая информация не систематизирована даны ответы на все вопросы*
	0-20	*Содержание темы не раскрыто полностью, информация не систематизирована*
	30	*Активное участие в обсуждении от 85% до 100%*
	15	*Частичное участие в обсуждении от 55% до 84%*
	0	*Не участвовал в обсуждении менее 55%*

Критерии оценивания Практического контрольного задания:

Критерии оценки	Диапазон баллов	Описание критерия
Правильность выполнения задачи и содержание комментариев, наличие иллюстративных объектов –	*50-60*	*Правильные решения и последовательность выполнения и. Задание выполнено полностью, сделаны выводы*
	40-49	*Допущены незначительные недочеты, отсутствуют выводы*
	30-40	*Допущены некоторые ошибки.*

сриншотов *Возможность демонстрировать работу системы*		*Отсутствуют скриншоты.* *Или задание выполнено не полностью* *Задание выложено с опозданием*
	5-29	*Не выполнена и половина задания, результаты не получены, много ошибок. Но выложено во-время*
Грамотность изложения и оформления работы	***10***	*Соблюдены все правила грамматики, орфографии, форматирования и представления визуальной части. Баллы не снижаются*
	6-10	*Не все правила оформления соблюдены*
	0-5	*Многочисленные ошибки, нечитаемые или непонятные скриншоты, затрудняющие восприятие текста. Или отсутствие в содержании демонстрационной части*
Идентификация объектов	***15***	*Существование идентификации объектов*
	0	*Нет идентификации*
Защита работы	***10- 15***	*Четкое изложение хода выполнения задания* *Способность пояснить, что будет если какие-то параметры будут изменены или рассказать, как можно другой ответ получить*
	5-10	*Изложение – неуверенное и затруднения ответов при правильном решении.*
	0-5	*Неспособность пояснить как получены результаты, для чего выполнялись задания*

Итого максимально:	100	

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (*при необходимости*).

Для решения заданий (ПКЗ) студенту разрешается использование разных средств; программ для работы с электронными таблицами для обработки, анализа и визуализации данных, онлайновых инструментов.

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Промежуточная аттестация проводится в форме *экзамена.*
Вопросы для подготовки к зачету:

1) Понятие модели. Цели, задачи и принципы моделирования.
2) Структурные технологии моделирования. Синтаксис и семантика IDEF0-диаграмм.
3) Классификация моделей по признаку физической сущности моделирующих объектов.
4) Основные этапы имитационного моделирования. Технология моделирования в ARENA/
5) Общая характеристика эвристических методов моделирования.
6) Структурные технологии моделирования. Принципы моделирования в IDEF0. Декомпозиция.
7) Общая характеристика аналитических методов моделирования.
8) Структурные технологии моделирования. Синтаксис и семантика IDEF0 – диаграмм.
9) Математические модели. Формы записи математических моделей.
10) Структурные технологии моделирования. Основные правила построения IDEF0 – диаграмм.
11) Натурное моделирование. Типовые схемы испытаний.
12) Структурные технологии моделирования. Туннелирование стрелок в IDEF0-диаграммах.
13) Общий порядок разработки моделей. Типовые этапы и стадии моделирования.
14) Иерархическая структура модельных представлений в объектно-ориентированном моделировании.
15) Признаки классификации моделей.
16) Объектно-ориентированное моделирование. Использование языка UML.
17) Назначение и содержание экспериментального этапа моделирования.

18) Диаграммы языка UML. Виды и назначение.

19) Назначение и содержание экспериментального этапа моделирования.

20) Интегрированные методы моделирования. Сущность интеграции.

21) Компьютерные технологии моделирования. Обзор.

Вопросы для подготовки к экзамену:

1) Сущность методологии АРИС.
2) Методы экспертных оценок. Проблемы применения.
3) Понятие имитационного моделирования. Целесообразность применения имитационного моделирования.
4) Диаграммы языка UML. Виды диаграмм.
5) Методология АРИС. Особенности.
6) Методы экспертных оценок. Способы устранения недостатков методов.
7) UML. Диаграмма вариантов использования.
8) Имитационное моделирование. Способы продвижения модельного времени.
9) Экспертные оценки. Особенности использования метода.
10) Целесообразность и особенности применения иммитационного моделирования.
11) Ключевые принципы использования UML.
12) Эвристические методы моделирования. Мозговой штурм. Особенности использования.
13) Сущности в языке UML. Типы сущностей.
14) Принцип системности интеграции. Системообразующие свойства сложной системы.
15) Отношения в языке UML. Типы отношений.
16) Преимущества методологии АРИС.
17) Диаграммы поведения в зыке UML. Назначение и использование.
18) Основные типы представлений в методологии АРИС.
19) UML. Концептуальная модель.
20) Уровни детализации моделей в АРИС.
21) Виды методов типа «мозговой атаки».
22) Разновидности имитационных моделей.
23) Практическое применение КГИ (коллективной генерации идей).
24) Моделирование систем массового обслуживания.
25) Методы экспертных оценок. Виды шкал, используемых для обработки ответов экспертов.
26) ARENA. Язык моделирования и анимационная система.
27) Методики анализа рисков ИБ. Инвентаризация активов.
28) Понятие актива. Типы активов. Источники информации об активах организации.

29) Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками.
30) Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов.
31) Оценка рисков ИБ. Идентификация и анализ риска.
32) Планирование мер по обработке выявленных рисков ИБ.
33) Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.
34) Система управления рисками на предприятии.

6.2. Типовые оценочные материалы промежуточной аттестации.

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

ТИП ЗАДАНИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	ТИПОВЫЕ ЗАДАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	1.К органам защиты государственной тайны НЕ относится: 1) Федеральная служба безопасности; 2) Служба внешней разведки; 3) Министерство внутренних дел; 4) Федеральная служба по техническому и экспортному контролю; 5) Министерство обороны (неверное зачеркнуть).
		2.По виду защищаемой информации НЕ различаются угрозы НСД к: 1) речевой информации; 2) видовой информации; 3) сигнальной информации; 4) логической информации; 5) тестовой информации
Задание закрытого типа на установление последовательности	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты	1. Укажите последовательность методов аутентификации по обеспечиваемому уровню защищенности (от наименее безопасного к наиболее защищенному) 1) аппаратная аутентификация 2) биометрическая аутентификация 3) парольная аутентификация

	ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	2. Расположите уровни обеспечения информационной безопасности в РФ от высшего к низшему (последовательность номеров через запятую): 1) морально-этический; 2) организационно-технический; 3) нормативно-правовой; 4) программно-аппаратный; 5) духовно-нравственный.
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	1.При отсутствии трудовых договоров охрана КТ должна включать в себя: 1) определение перечня сведений; 2) ограничение доступа; 3) учет лиц, получивших доступ; 4) регулирование отношений с контрагентами; 5) нанесение грифа «Коммерческая тайна» (неверное зачеркнуть). 2.Процесс оценивания рисков содержит этапы: 1) оценивание угроз 2) установка межсетевых экранов 3) установка антивирусных средств 4) оценивание рисков
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	1.Выбрать верный ответ и обосновать свой выбор. Коммерческая тайна – это: 1) общее понятие для тайн профессиональной, личной, семейной; 2) то же самое, что и интеллектуальная собственность; 3) то же самое, что и профессиональная тайна; 4) то же самое, что и банковская тайна; 5) частный случай государственной тайны; 6) частный случай конфиденциальной информации. 2.Выбрать верный ответ и обосновать свой выбор. Захват всех ресурсов компьютера одним приложением или процессом в многозадачной операционной системе является угрозой 1) нарушения конфиденциальности; 2) нарушения целостности; отказа служб

Задание открытого типа с развернутым ответом	1. Внимательно прочитать текст задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки.	1.Прочитайте вопрос и запишите развернутый обоснованный ответ Актив: определение согласно нормативно-правовому акту или стандарту. 2.Прочитайте вопрос и запишите развернутый обоснованный ответ Угроза: определение согласно нормативно-правовому акту или стандарту.
Задание закрытого типа на установление соответствия	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов.	1.Установите соответствие характеристикой государственного органа и аббревиатурой: А)… – федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры; Б)… – федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки ПДн требованиям законодательства РФ в области персональных данных; В)… – государственный орган, на который возложены функции по лицензированию и сертификации в сфере криптографической защиты и защиты государственной тайны. 1.ФСБ; 2.ФСТЭК; 3.Роскомнадзор.

6.3. Критерии и шкала оценивания на основе БРС.

Критерии и балльная шкала определяются преподавателем

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок	40
Дан развернутый ответ на поставленный вопрос, где обучающийся демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.	30-39
Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.	20-29
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. обучающийся не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	0-19

6.4. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (*при необходимости*).

Для выполнения тестовых заданий требуется кабинет с компьютерами и электронная образовательная система вуза ЭОС Moodle. Если необходимо, студент может использовать калькулятор, бумагу, ручку. В исключительных случаях допустимо проведение экзамена в СДО, для чего необходима система электронного взаимодействия, например, МТС-Link Yandex.telemost,

7. Методические материалы по освоению дисциплины (модуля)

Для изучения основных вопросов дисциплины необходимо конспектировать материалы лекций, работать с рекомендованной преподавателем литературой, а также ресурсами информационно-телекоммуникационной сети «Интернет». Для приобретения навыков активного использования знаний полезно обсуждать плановые и возникающие вопросы, а также решаемые задачи на практических занятиях. Чтобы легче и прочнее усвоить материал следует постоянно использовать конкретные примеры, сравнения из уже полученных областей наук.

Методические материалы по дисциплине находятся в электронной образовательной системе Moodle. Структура курса представлена отдельными темами, в которых можно найти Лекционные материалы, практические задания и методические рекомендации по их выполнению, а также тестовые вопросы по каждой теме и список вопросов для подготовки к опросам и тестированию.

Важной составной частью учебного процесса в вузе являются практические занятия, которые закрепляют теоретические знания, полученные на лекциях и изученные в дополнительной литературе. Практические занятия помогают глубже усвоить учебный материал, приобрести умения применять принципы решения разнообразных проблем, определять и оценивать ресурсы и существующие ограничения разного рода проектов.

При подготовке к практическим занятиям необходимо проанализировать конспект лекции, ознакомиться с рекомендованной литературой по соответствующей теме, осуществить подготовку по рекомендованным в рабочей программе вопросам для обсуждения темы, выполнить домашнее задание (при необходимости).

Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. Особое внимание, работая самостоятельно, необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы нужно стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь, также

благоприятно действует на результаты. При необходимости следует обращаться за консультацией к преподавателю (в том числе по электронной почте). Для самостоятельной работы имеют значение записи. Они помогают понять построение изучаемого материала, выделить основные положения, проследить их логику. Ведение записей способствует активизации и мобилизации мышления наряду со зрительной, и моторную память. Полезно записывать идеи.

После изучения базовых тем курса проводится текущий контроль знаний студентов в виде опроса или письменного тестирования. Типовые тесты и задания по темам дисциплины приведены в специальном разделе данной рабочей программы.

Подготовка к текущему и промежуточному контролю предполагает изучение представленных вопросов к зачету, работу над тестами, представленными в данной рабочей программе, выполнение семестровой проектной работы по применению системного подхода и методов системного анализа к выбранной системе.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998 .

2. Панарина, М. М. Корпоративная безопасность: система управления рисками и комплаенс в компании: учебное пособие для вузов / М. М. Панарина. — Москва: Издательство Юрайт, 2023. — 158 с. — (Высшее образование). — ISBN 978-5-534-15342-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520423 .

3. Моделирование процессов и систем: учебник и практикум для вузов / Е. В. Стельмашонок, В. Л. Стельмашонок, Л. А. Еникеева, С. А. Соколовская; под редакцией Е. В. Стельмашонок. — Москва: Издательство Юрайт, 2023. — 289 с. — (Высшее образование). — ISBN 978-5-534-04653-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511904 .

4. Воронцовский, А. В. Управление рисками: учебник и практикум для вузов / А. В. Воронцовский. — 2-е изд. — Москва: Издательство Юрайт, 2023. — 485 с. — (Высшее образование). —

ISBN 978-5-534-12206-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511534 .

8.2 Дополнительная литература

1. Дронов В.Ю. Международные и отечественные стандарты по информационной Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 120 с. - ISBN 978-5-9275-2742-7. - Текст: электронный. - URL: https://znanium.com/catalog/product/1021744

2. Веселов Г.Е. Менеджмент риска информационной безопасности: учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. — Электрон. дан. - Таганрог:Южный федеральный университет, 2016. - 107 с.

3. Основы управления информационной безопасностью : учебное пособие : Допущено УМО ... / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - Москва : Горячая линия-Телеком, 2016. - 244 с. - (Вопросы управления информационной безопасностью. Вып. 1). - Библиогр.: с. 234-239. - ISBN 978-5-9912-0361-6.

8.3.Нормативные правовые документы и иная правовая информация

Не используются

Интернет-ресурсы

Обучающимся обеспечен доступ к материалам курса в СДО Академии http://lms.ranepa.ru, а так же через сайт научной библиотеки к следующим подписным электронным ресурсам:

Русскоязычные ресурсы

1. Электронные учебники электронно-библиотечной системы (ЭБС) *«Айбукс»*
2. Электронные учебники электронно-библиотечной системы (ЭБС) *«Юрайт»*
3. Электронные учебники электронно-библиотечной системы (ЭБС) *«Лань»*
4. Электронные учебники электронно-библиотечной системы (ЭБС) «*ZNANIUM.COM*»
5. Электронные учебники электронно-библиотечной системы (ЭБС) «BOOK.RU»
6. Оценка качества информационной инфраструктуры организации. http://www.dir-consulting.ru/ocenka-kachestva-informacionnoj-infrastruktury-organizacii.html

7. Управление инцидентами и проблемами – понятия и принципы / ИнфраМенеджер, Электронный ресурс URL: [https://www.inframanager.ru/library/about-methodology/upravlenie-incidentami/]
8. Колесов А. HP ITSM и эффективность обслуживания информационных систем предприятий / http://www.bytemag.ru/?ID=602758
9. Управление ИТ-услугами / http://www.itexpert.ru/rus/articles/200406222006/200406222044

9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

№ п/п	Наименование
1.	Специализированные залы для проведения лекций, оснащенные персональным компьютером/ноутбуком и мультимедийным проектором
2.	Аудитории и компьютерные классы, оборудованные посадочными местами и персональными компьютерами с выходом в Интернет для проведения практических занятий
3.	«МТС Линк» — российская платформа для онлайн-коммуникаций и совместной работы команд ; «Яндекс Телемост» — сервис для видеоконференций от Яндекса; Я-мессенджер
4.	Технические средства обучения: персональные компьютеры; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV; программы для работы с электронными таблицами для обработки, анализа и визуализации данных; соответствующие онлайн-инструменты для построения интеллект-карты и моделей в различных нотациях
5.	Научная библиотека (в т.ч. электронные информационные ресурсы научной библиотеки)
6.	СДО Академии https://lms.ranepa.ru/