Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.01.01Управление информационной безопасностью

(индекс, наименование дисциплины в соответствии с учебным планом)

38.04.05 «Бизнес-информатика»

(код, наименование направления подготовки/специальности)

«Бизнес-аналитика»

(наименование образовательной программы)

очная
(форма обучения)

Год набора - 2026

Санкт-Петербург,2026

Автор(ы)-составитель(и) РПД:

Сухостат Валентина Васильевна, кандидат технических наук, кандидат педагогических наук, доцент, доцент кафедры бизнес-информатики

Заведующий кафедрой:

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

Рабочая программа дисциплины Б1.В.ДВ.01.01 «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.ДЭ.01.01 Управление информационной безопасностью* 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 ****
06.015 СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННЫМ СИСТЕМАМ **D** Управление работами по сопровождению и проектами создания (модификации) ИС, автоматизирующих задачи организационного управления и бизнес-процессы **D/01/7** Организационное и технологическое обеспечение определения первоначальных требований заказчика к ИС и возможности их реализации в ИС	ПКс 2	Способен обосновывать подходы, используемые в бизнес-анализе, руководить и управлять бизнес-анализом с использованием информационно-коммуникационных технологий	ПКс 2.2	Решает задачи бизнес-аналитики с использованием современных инструментов ИТ-менеджмента	ПКс 2.2 Зн.15 **Знать** Основы менеджмента, в том числе менеджмента качества ПКс 2.2 -У2 **Уметь** Планировать работы в рамках управления работами по сопровождению и проектами создания (модификации) ИС

** 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.ДЭ.01.01 Управление информационной безопасностью* - 5 зачетных единиц – 180 акад.час; объем академических часов, выделенных на контактную работу обучающихся с преподавателем - 45 акад час, из них 12 акад.час – лекции, 22 час – практические занятия, 9 часов – контактная работа на аттестацию в период экзаменационных сессий, и 117 акад. час. выделяется на самостоятельную работу обучающихся.

Место дисциплины в структуре образовательной программы.
Дисциплина *Б1.В.ДЭ.01.01 Управление информационной безопасностью* относится к элективным дисциплинам части образовательной программы формируемой участниками образовательных отношений, преподается на 1 курсе во 2 семестре, когда у обучаемыми получены знания и сформированы навыки, полученные на таких дисциплинах как:
Б1.О.04 «Управленческий анализ», Б1.В.05 «Методы бизнес-аналитики», Б1.В.ДЭ.02.01 «Менеджмент данных» и является основой для подготовки к магистерским диссертациям.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная/очно-заочная/заочная форма обучения (оставить нужное)

№ 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	Основы управления информационной безопасностью предприятия.	60	4			6							6	39	Т
Тема 2	Система менеджмента информационной	60	4			8				4			6	39	Т

	безопасности.													
Тема 3	Управление рисками и оценка информационной безопасности компании	60	4			8				5		6	39	ПКЗ
Промежуточная аттестация									2					экзамен
Итого	180		12			22			2	9		18	117	

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. Основы управления информационной безопасностью предприятия

ПКс- 2.2

Основные направления обеспечения информационной безопасности организации. Риск-ориентированный подход. Понятие корпоративной политики безопасности. Основные требования и подходы к разработке политики безопасности. Многоуровневый подход.

Управления информационной безопасностью на основе соответствий требованиям (compliance management). Анализ упущений (gap-анализ). Модель непрерывного совершенствования (замкнутый цикл менеджмента PDCA).

Процессный подход к обеспечению информационной безопасности. Суть процессного подхода. Классификация и атрибуты процессов. Процессы управления и обеспечения информационной безопасности. Эталонная модель процесса для управления ИБ (ГОСТ Р 57640-2017, ISO/IEC TS 33052:2016). Проблемы внедрения процессного подхода.

Тема 2.

Система менеджмента информационной безопасности

ПКс- 2.2

Уровни организации деятельности по обеспечению информационной безопасности компании, и общая структура стандартов информационной безопасности. Оценочные стандарты информационной безопасности («Оранжевая книга», ITSEC, ISO/IEC 15408 «Общие критерии»). Статус стандартов ISO/IEC в РФ.

«Лучшие практики» информационной безопасности (стандарты BSI, BS 7799 / ISO/IEC 17799, 27002).

Стандарты менеджмента информационной безопасности. Состав и структура серии международных стандартов ISO/IEC 2700x. Российские гармонизированные стандарты.

Национальные стандарты и стандарты саморегулируемых организаций в сфере управления информационной безопасностью и информационными технологиями (BS-100, NIST 800, ITIL, ISM 3, Cobit). Сервис-ориентированный и процессно-ориентированный подходы к управлению ИБ и ИТ. Концепция корпоративного управления информационной безопасностью (IS Governance).

Эволюция модели информационной безопасности.

Построение системы менеджмента информационной безопасности (СМИБ) на основе ISO/IEC 27001. Организационная структура системы менеджмента информационной безопасности. Система частных менеджментов. Сертификация соответствия СМИБ ISO/IEC 27001.

Тема 3. Управление рисками и оценка информационной безопасности компании

ПКс – 2.2

Риск как объект управления. 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.

Виды и способы оценки информационной безопасности. Процесс оценки (аудита) ИБ. Метрики информационной безопасности (ISO/IEC 27004, NIST 800-55).

Оценка процессов информационной безопасности на основе моделей зрелости (ГОСТ Р ИСО/МЭК 33020-2017, ISO 21827, ISO 15504).

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	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.	Ответ считается верным, если правильно установлены все соответствия (позиции из

правильных ответов из нескольких вариантов предложенных		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).	одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в 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).	Ответ считается верным, если 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.	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа

		5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	
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. Основы управления информационной безопасностью предприятия. ПКс- 2.2

Тестовые задания с инструкцией по выполнению:

Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных.

Сценарий выполнения

1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько верных ответов.

4. Записать только номера (или буквы) выбранного варианта ответа (например, 3 или В).

Задание 1. Выберите правильный ответ, чтобы закончить фразу:

Стандартный подход ISO к построению СМИБ основан на модели PDCA. Какие элементы соответствуют модели PDCA?

Варианты ответов:

1) планирование (Plan);
2) изменение (Change);
3) выполнение (Do);
4) решение (Solution);
5) проверка (Check);
6) совершенствование (Akt).

Задание закрытого типа с выбором только 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 вариант-ты ответа.

3. Выбрать тот ответ, который считаете верными.

4. Запишите только один номер (или букву) выбранных вариантов ответа (например, 3 или В).

Задание 2. Задание 2. Выберите правильный ответ, чтобы продолжить

Международная организация по стандартизации (ISO) под словом «система» в системе менеджмента информационной безопасности понимает:

1) действующее устройство;
2) приложение;
3) процесс, программу действий или методологию.

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.

4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).

Задание 3. Установите соответствие между термином и его определением.

Термин	**Определение**
1 Управление доступом	А Обеспечение санкционированного доступа к активам в соответствии с бизнес-требованиями и требованиями безопасности..
2 Атака	В Попытка уничтожения раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования
3 Аудит	С Систематический, независимый и задокументированный процесс, предназначенный для получения свидетельств и объективной оценки.

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).

Задание 4.
Что из перечисленного НЕ является фундаментальным свойством безопасности при риск-ориентированном подходе к обеспечению информационной безопасности?
Выберите один вариант и обоснуйте ответ:

1) безопасность никогда не бывает абсолютной;
2) измерить уровень безопасности невозможно;
3) наступление рискового события в общем случае предотвратить невозможно;
4) можно снизить степень последствий (размер ущерба) от наступления рискового события;
5) при любом вмешательстве в систему в первую очередь страдает ее безопасность;
6) система документированных управленческих решений по обеспечению ИБ организации являет собой политику информационной безопасности.

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.
4.В случае расчетной задачи, записать решение и ответ

Задание 5.
Указать задачи, выполняемые ИБ-отделом

Задание закрытого типа на установление последовательности действий
1. Внимательно прочитать текст задания и понять, что в 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).

Задание 6. Укажите уровни общей структуры нормативно-методических документов компании в области информационной безопасности в порядке возрастания:

1) политика информационной безопасности;

2) процедуры, инструкции, стандарты конфигурации, журналы, записи;

3) частные политики, стандарты

Тема 2. Система менеджмента информационной безопасности ПКс- 2.2;

Задание открытого типа с развернутым ответом

Вопрос 1 Перечислите и дайте характеристику шагам этапа планирования СМИБ в соответствии с требованиями стандарта ISO/IEC 27001.

Вопрос 2

Сравните риск-ориентированный и процессный подходы к управлению ИБ.

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 ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько верных ответов.

4. Записать только номера (или буквы) выбранного варианта ответа (например, 3 или В).

Задание 1. Выберите, что включает в себя система менеджмента:

1) организационную структуру;
2) политики;
3) планирование;
4) оценку информационных рисков, планирование мер по обработке рисков;
5) должностные обязанности;
6) ресурсы.

Задание закрытого типа с выбором только 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 вариант-ты ответа.

3. Выбрать тот ответ, который считаете верными.

4. Запишите только один номер (или букву) выбранных вариантов ответа (например, 3 или В).

Задание 2. Граница СМИБ по отношению к системе управления непрерывностью бизнеса (Business continuity management - BCM) очерчивается выражением:

1) $СМИБ \subseteq ВСМ$;

2) $СМИБ \supset ВСМ$;

3) $СМИБ \cap ¿ ¿ ВСМ$ = защита критичных бизнес-процессов организации от крупных сбоев и аварий ИС.

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.
4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).

Задание 3. Соотнесите термин из левого столбца с его правильным определением из правого столбца. Каждому термину соответствует одно определение.

Термин	**Определение**
1. Обеспечение непрерывности информационной безопасности	А. Процессы и процедуры, гарантирующие непрерывность операций по обеспечению информационной безопасности
2. Событие информационной безопасности	В. Выявленное состояние системы, услуги или сети, указывающее на возможное нарушение политики обеспечения информационной безопасности
3. Инцидент информационной безопасности	С Одно или несколько нежелательных или неожиданных событий информационной безопасности, которые с высокой степенью вероятности могут привести к компрометации в бизнес- процессах и создают угрозы для информационной безопасности

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.Внимательно прочитать предложенные варианты ответа.
2.Выбрать один верный ответ.
3.Записать только номер (или букву) выбранного варианта ответа.
4.Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).

Задание 4. В систему менеджмента НЕ входит:

1) организационная структура;
2) политики;
3) оценка информационных рисков, планирование мер по обработке рисков;
4) ресурсы.

Тема 3. Управление рисками и оценка информационной безопасности компании

ПКс – 2.2

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	0,2	20
КТ 2	100	0,2	20
КТ 3	100	0,2	20
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:

КТ – 1.
Тема 1
Тестовые задания по теме 1
КТ – 1

Тема 2,
Тестовые задания по теме 3.
КТ – 2

Тема 3
Практическое контрольное задание (ПКЗ)
КТ – 3

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

Критерии оценки	Диапазон баллов	Описание критерия
Количество правильных ответов	*0*	*Количество правильных ответов менее 55%*
	25	*Количество правильных ответов от 55% до 64%*
	50	*Количество правильных ответов от 65% до 74%*
	75	*Количество правильных ответов от 75% до 84%*
	100	*Количество правильных ответов от 85% до 100%*
Итого максимально:	100	

НАПРИМЕР: из 20 вопросов правильных ответов составляет 75% - значит это значит, что за тест студент получит 75% от максимального балла, то есть 15 баллов вместо максимальных 20.

1. Критерии оценивания Практического контрольного задания:

Критерии оценки	Диапазон баллов	Описание критерия
Правильность выполнения задачи и содержание комментариев, наличие иллюстративных	*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. Отсутствуют скриншоты.* *Или задание выполнено не полностью* *Задание выложено с опозданием*
объектов – сриншотов *Возможность демонстрировать работу системы*	*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 экзамену:

1. Риск-ориентированный подход к управлению ИБ организации.
2. Понятие корпоративной политики безопасности. Многоуровневый подход.
3. Управления информационной безопасностью на основе соответствия требованиям (compliance management).
4. Анализ упущений (gap-анализ).
5. Модель непрерывного совершенствования (замкнутый цикл менеджмента PDCA).
6. Уровни организации деятельности по обеспечению ИБ компании и общая структура стандартов ИБ.
7. Стандарт «Оранжевая книга».
8. Стандарт ITSEC.
9. Стандарт ISO/IEC 15408 «Общие критерии».
10. «Лучшие практики» информационной безопасности ISO/IEC 27002. Статус стандартов ISO/IEC в РФ.
11. Стандарты менеджмента информационной безопасности. Состав и структура серии международных стандартов ISO/IEC 2700x.
12. Сервис-ориентированный и процессно-ориентированный подходы к управлению ИБ и ИТ.
13. Концепция корпоративного управления информационной безопасностью (IS Governance) в стандарте Cobit 5.
14. Эволюция модели информационной безопасности.
15. Свойства систем. Иерархические системы.
16. Понятие процесса. Свойства процессов. Суть управления процессом
17. Структурный (функциональный) и процессный подход к управлению.
18. Классификация и атрибуты процессов.
19. Эталонная модель процесса для управления ИБ.
20. Проблемы и ошибки при внедрении процессного подхода к управлению ИБ.
21. Понятие и состав системы менеджмента.

22. Принципы построения системы менеджмента ИБ на основе ISO/IEC 27001.
23. Этапы построения системы менеджмента ИБ на основе ISO/IEC 27001.
24. Организационная структура системы менеджмента ИБ.
25. Определение контекста и области действия системы менеджмента ИБ.
26. Процедура сертификации соответствия СМИБ требованиям ISO/IEC 27001.
27. Процесс управления рисками ИБ на основе ISO 27005.
28. Итерационная процедура оценки рисков ИБ.
29. Виды обработки рисков ИБ.
30. Методики оценки рисков ИБ.
31. Виды и способы оценки ИБ компании.
32. Этапы процесса оценки (аудита) ИБ.
33. Роли в процессе оценки (аудита) ИБ.
34. Измерения ИБ ISO/IEC 27004
35. Понятие зрелости и уровней возможности. Модели зрелости.
36. Оценка процессов ИБ на основе моделей уровней возможностей.
37. Оценка процессов разработки средств ЗИ на основе моделей зрелости

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	1. Укажите последовательность методов аутентификации по обеспечиваемому уровню защищенности (от наименее безопасного к наиболее защищенному)

	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).	1) аппаратная аутентификация 2) биометрическая аутентификация 3) парольная аутентификация 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,	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

	обосновывающие выбор ответа (например, 4 текст обоснования).	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. Елин, В. М., Организационное и правовое обеспечение информационной безопасности : учебное пособие / В. М. Елин, А. К. Жарова. — Москва : КноРус, 2025. — 207 с. — ISBN 978-5-406-14605-7. — URL: https://book.ru/book/958440 (дата обращения: 30.04.2026). — Текст : электронный.
2. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889 (дата обращения: 30.04.2026). — Режим доступа: для авториз. пользователей.
3. Козьминых, С. И., Управление информационной безопасностью : учебное пособие / С. И. Козьминых, С. А. Борисов. — Москва : КноРус, 2024. — 281 с. — ISBN 978-5-406-13773-4. — URL: https://book.ru/book/955744 (дата обращения: 30.04.2026). — Текст : электронный.
4. Крылов, Г. О., Базовые понятия информационной безопасности : учебное пособие / Г. О. Крылов, С. Л. Ларионова, В. Л. Никитина. — Москва : Русайнс, 2026. — 257 с. — ISBN 978-5-466-09255-4. — URL: https://book.ru/book/958467 (дата обращения: 30.04.2025). — Текст : электронный.

Все источники основной литературы взаимозаменяемы.

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/