Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.18 Информационная безопасность
(индекс, наименование дисциплины в соответствии с учебным планом)

38.05.01 Экономическая безопасность
(код, наименование направления подготовки)

Экономико-правовое обеспечение экономической безопасности
(наименование образовательной программы)

очная форма обучения
(форма обучения)

Год набора – 2025

Санкт-Петербург

Автор(ы)-составитель(и) РПД:

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

Заведующий кафедрой бизнес-информатики:
Наумов Владимир Николаевич доктор военных наук, профессор

Рабочая программа дисциплины Б1.В.18 Информационная безопасность одобрена на заседании кафедры бизнес-информатики СЗИУ РАНХиГС.

протокол № 10 от «27» августа 2025 г.

СОДЕРЖАНИЕ

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

Дисциплина Б1.В.18 Информационная безопасность обеспечивает формирование у обучающихся следующих профессиональных компетенций:

ОТФ/ТФ и реквизиты ПС *(при наличии)*	**Код компетенции**	**Наименование компетенции**	**Код индикатора достижения компетенций**	**Наименование индикатора достижения компетенций**	**Образовательный результат**
E/02.7 Организация работы по выполнению заданий (поручений) и предоставление отчетов акционерам (собственникам), совету директоров и руководителям организации E/03.8 Создание организационно-управленческой и информационной структуры интегральной системы управления рисками E/04.8 Координация работ по	ПКс-16	Способен защитить информацию и информационную инфраструктуру организации от негативных воздействий	ПКс-16.1	Формирует представление о мерах организационного и технического характера, направленных на сохранение и защиту информации и ее инфраструктуры от негативных воздействий	ПКс-16.1-З-1 Знает: понятие и сущность экономической безопасности, ее место в системе национальной безопасности РФ; объекты и субъекты экономической безопасности; концепцию экономической безопасности Российской Федерации; экономические риски, природу и сущность угроз экономической безопасности; методы оценки уровня рисков и угроз экономической безопасности; критерии и показатели экономической безопасности; организационно-правовые основы, принципы, факторы, механизмы,

технико-информационному обеспечению системы стратегического управления рисками					методы и средства обеспечения экономической безопасности; принципы построения и элементы системы безопасности ПКс-16.1-У-1 Умеет: определять критерии и рассчитывать пороговые значения показателей уровня экономической безопасности; выявлять угрозы экономической безопасности, проводить их ранжирование по вероятности реализации и величине ущерба; разрабатывать и проводить мероприятия по противодействию коррупции, легализации криминальных доходов.

2. Объем и место дисциплины (модуля) в структуре образовательной программы

Общий объем дисциплины (очная форма обучения):

4 з.е., 144 ак.час

Контактная работа обучающихся с преподавателем по видам учебных занятий: 56 ак. час на контактную работу с преподавателем, из них 26 ак.час на лекции и 28 ак.час на практические занятия. 88 ак. час на самостоятельную работу обучающихся.

Общий объем дисциплины (заочная форма обучения):

4 з.е., 144 ак.час

Контактная работа обучающихся с преподавателем по видам учебных занятий: 26 ак. час на контактную работу с преподавателем, из них 6 ак.час на лекции и 8 ак.час на практические занятия. 124 ак. час на самостоятельную работу обучающихся.

Б1.В.18 «Информационная безопасность» реализуется в 9-м семестре очной формы обучения, в 7 и 8 семестрах заочной формы обучения. Преподавание дисциплины «Информационная безопасность» основано на дисциплинах «Информатика» «Экономика организации», «Бухгалтерский учет», «Экономический анализ», «Экономическая безопасность» и др. Завершение изучения дисциплины происходит одновременно с изучением таких дисциплин как «Правовое обеспечение экономической безопасности», что обеспечивает успешное освоение профессиональных компетенций.

Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при выполнении выпускных квалификационных работ.

3. Содержание и структура дисциплины (модуля)

3.1. Структура дисциплины (модуля)

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.	Нормативная база и стандарты в области ИБ и защиты информации. Компьютерная преступность	46	8	0		8	0	0	0	0		0	0	30	Деловая игра «Проблемы и приоритеты в сфере информационной безопасности»/ Тестирование
Тема 2.	Угрозы	46	10	0	0	8	0	0	0	0		0	0	28	Тестирование ,

	безопасности информации.													кейс
Тема 3.	Методы и средства защиты информации от несанкционированного доступа	46	8	0	0	12	0	0	0	0	0	0	30	Кейс
Промежуточная аттестация		46		0	0		0	0	2		0	0		Зачет с оценкой
Итого		144	26	0	0	28	0	0	2		0	0	88	

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

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.

3.1. Структура дисциплины (модуля)

Заочная форма обучения

№ п/п	**Наименование**		**Объем дисциплины, ак.час**	**Форма**

	тем и (или) разделов	ВСЕГО	Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			текущего контроля успеваемости, промежуточной аттестации
			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.	Нормативная база и стандарты в области ИБ и защиты информации. Компьютерная преступность	41	2	0		2	0	0	0	0		0	0	37	Деловая игра «Проблемы и приоритеты в сфере информационной безопасности»/ Тестирование
Тема 2.	Угрозы безопасности информации.	47	2	0	0	2	0	0	0	0		0	0	43	Тестирование , кейс
Тема 3.	Методы и средства защиты информации от	50	2	0	0	4	0	0	0	0		0	0	44	Кейс

	несанкционированного доступа													
Промежуточная аттестация		6		0	0		0	0	2	4	0	0		Зачет с оценкой
Итого		144	6	0	0	8	0	0	2	4	0	0	124	

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

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. Нормативная база и стандарты в области информационной безопасности и защиты информации. ПКс-16.1

Нормативная база информационной безопасности и защиты информации. Государственная политика в сфере информационной безопасности и защиты информации. Правовое обеспечение информационной безопасности. Конституция РФ об «информационных правах и обязанностях». Основные нормативные документы, регулирующие отношения в сфере информационной безопасности. Виды «тайн» по Российскому законодательству. Классификация тайн.

Обобщенная модель информационной безопасности. Национальные стандарты в области информационной безопасности и защиты информации. Международные стандарты в области информационной безопасности и защиты информации.

Понятие компьютерной преступности. Масштабы и общественная опасность компьютерной преступности. Виды и субъекты компьютерных преступлений. Специфика расследования компьютерных преступлений. Предупреждение компьютерных преступлений. Кодификатор Интерпола. Ответственность за нарушения и преступления в сфере информационной безопасности. Дисциплинарная ответственность за разглашение охраняемой законом тайны. Административная ответственность за нарушения в сфере информационной безопасности и защиты информации. Уголовная ответственность за преступления в сфере компьютерной информации. Уголовная ответственность за нарушение закона о государственной тайне.

Тема 2. Угрозы безопасности информации. ПКс-16.1

Каналы силового деструктивного воздействия на информацию. Электромагнитный спектр как источник воздействия на информацию. Каналы силового деструктивного воздействия (СДВ) на информацию. Классификация средств СДВ. Рекомендации по защите компьютерных систем от СДВ. Технические каналы утечки информации. Классификация технических каналов утечки информации. Модели и способы утечки информации по техническим каналам.

Угрозы несанкционированного доступа к информации. Классификация угроз несанкционированного доступа (НСД) к информации. Категории нарушителей безопасности информации и их возможности. Общая характеристика уязвимостей. Способы реализации угрозы НСД к информации.

Нетрадиционные информационные каналы. Понятие и обобщенная модель нетрадиционного информационного канала. Методы сокрытия информации в текстовых файлах. Методы сокрытия информации в

графических файлах. Методы сокрытия информации в звуковых файлах. Методы сокрытия информации в сетевых пакетах и исполняемых файлах.

Тема 3. Методы и средства защиты информации от НСД. ПКс-16.1

Криптографическая защита информации. Модель криптосистемы. Историография и классификация шифров. Примеры криптографических алгоритмов. Криптосистема с симметричными и несимметричными ключами. Электронная цифровая подпись.

Методы и средства разграничения и контроля доступа к информации. Мандатная и дискреционная модели доступа. Процедура идентификации, аутентификации и авторизации. Система паролирования. Системы контроля и управления доступом. Система охраны периметра.

Системы предотвращения утечки информации из корпоративной сети. Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети. Понятие и функционал DLP-систем. Объем и структура данных защищаемых DLP-системами. Каналы коммуникаций, контролируемые DLP-системами. Критерии оценки программных продуктов, реализующих функциональность DLP.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.18 «Информационная безопасность» входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляют 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 закрытого 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 предложенных вариантов	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 Б1.В.18 «Информационная безопасность» используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Деловая игра, письменный опрос, тестирование, кейсы.

Тема 1. Нормативная база и стандарты в области информационной безопасности и защиты информации

Деловая (ролевая игра)

Тема (проблема): Определение проблем и приоритетов в области обеспечения информационной безопасности

Вопросы, требующие разработки:

1) Что необходимо сохранить в области обеспечения ИБ в современных условиях?

2) Что необходимо модернизировать в области обеспечения ИБ в современных условиях?

3) От чего следует отказаться в области обеспечения ИБ в современных условиях?

4) Что нового необходимо внести в обеспечение ИБ в современных условиях?

Роли:

Ведущий: независимый эксперт.

4 учебных команды

Учебная команда №1 отвечает за ответы на вопрос 1); учебная команда №2 – за ответы на вопрос 2); учебная команда №3 – за ответы на вопрос 3); учебная команда №4 – за ответы на вопрос 4).

Тестовые задания:

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

2. Внимательно прочитать предложенные вариант-ты ответа.

3. Записать последовательность номеров ответов из предложенных вариантов.

1. 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.

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 выбранного варианта ответа.

2. Что (кто) НЕ является элементом системы обеспечения информационной безопасности РФ (номер по порядку)?

1) Палаты Федерального собрания;

2) Президент;

3) Органы местного самоуправления;

4) Общественная Палата;

5) Органы исполнительной власти;

6) Совет безопасности?

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 выбранного варианта ответа.

3. Кто НЕ наделен полномочиями по отнесению сведений к государственной тайне?

1) Министр сельского хозяйства;

2) Председатель Банка РФ;

3) Руководитель Росгидромета;

4) Руководитель Федеральной таможенной службы

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 выбранного варианта ответа.

4. Служба безопасности на предприятии призвана:

1) постепенно заменить государственные правоохранительные органы и специальные службы;

2) помочь олигархическим группам в борьбе за власть;

3) обеспечить безопасность в тех областях, которые находятся вне компетенции правоохранительных органов;

4) осуществлять все, что указано в предыдущих пунктах?

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 выбранного варианта ответа.

5. 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.

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 выбранных вариантов ответа

6. 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)

Тема 2. Угрозы безопасности информации.

Тестовые задания:

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 выбранного варианта ответа.

1. Включение кейса с электролитическими конденсаторами в сетевую розетку офисной ЛВС является следующим каналом силового деструктивного воздействия:

1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

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 выбранного варианта ответа.

2. Включение кейса с электролитическими конденсаторами в офисную розетку сети электропитания является следующим каналом силового деструктивного воздействия:

1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

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 выбранного варианта ответа.

3. Включение электрошокера в сетевой разъем маршрутизатора является следующим каналом силового деструктивного воздействия:

1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

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 выбранного варианта ответа.

4. Мощный разряд молнии в непосредственной близости является следующим каналом силового деструктивного воздействия:

1) КСДВ – 2;
2) КСДВ – 1;

3) КСДВ – 3.

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 выбранного варианта ответа.

5. Внедрение программной закладки в источник бесперебойного питания. является следующим каналом силового деструктивного воздействия:

1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

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 выбранного варианта ответа.

6. Перехват побочных электромагнитных излучений от работы ПЭВМ и ВТСС является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:

1) электромагнитный;
2) воздушный (акустический);
3) электрический;
4) радиоканал;
5) параметрический.

Кейс «Уязвимости. Методы расчёта степени критичности уязвимостей»:

Задание: Использовать метод CVSSv3 (сайт ФСТЭК URI: https://bdu.fstec.ru/calc3) для анализа уязвимости, определения ее критичности и принятия решения о дальнейших шагах по устранению. Этот процесс позволяет организациям эффективно управлять рисками информационной безопасности и обеспечить надежную защиту информационных систем и данных.

Варианты заданий:

1. Уязвимость: Удаленное выполнение кода через уязвимость в Apache Struts 2
    - Описание: Уязвимость позволяет злоумышленнику удаленно выполнить произвольный код на сервере, используя уязвимость в Apache Struts 2. Это может привести к полному контролю над системой и потенциальному нарушению конфиденциальности и доступности данных.
    - CVSSv3 Score: 9.8 (Critical)
2. Уязвимость: SQL Injection в веб-приложении с недостаточной фильтрацией пользовательского ввода
    - Описание: Уязвимость представляет собой SQL инъекцию в веб-приложении из-за недостаточной фильтрации пользовательского ввода. Это позволяет атакующему выполнять произвольные SQL запросы к базе данных, что может привести к утечке данных или нарушению целостности данных.
    - CVSSv3 Score: 7.5 (High)
3. Уязвимость: Утечка информации через несанкционированный доступ к базе данных
    - Описание: Уязвимость позволяет злоумышленнику получить несанкционированный доступ к базе данных, что приводит к утечке конфиденциальной информации. Это может включать в себя персональные данные пользователей, финансовую информацию и другие конфиденциальные сведения.
    - CVSSv3 Score: 7.2 (High)
4. Уязвимость: Уязвимость в браузере, позволяющая XSS-атаки через вредоносный скрипт на странице
    - Описание: Уязвимость в браузере позволяет атакующему выполнить скрипт на стороне клиента (XSS), используя вредоносный код на странице. Это может привести к компрометации сессии пользователя, укрощению данных сессии и другим атакам на пользовательский браузер.
    - CVSSv3 Score: 8.1 (High)
5. Уязвимость: Недостаточное ограничение доступа к файлам на сервере, позволяющее получение конфиденциальной информации

- Описание: Уязвимость заключается в недостаточном ограничении доступа к файлам на сервере, что позволяет несанкционированному пользователю получить доступ к конфиденциальной информации. Это может привести к утечке конфиденциальных данных и нарушению приватности пользователей.
- CVSSv3 Score: 6.5 (Medium)

Тема 3. Методы и средства защиты информации от НСД

Кейс «Анализ индикаторов компрометации»

Задание.

Изучить понятие кибербразведки и индикаторов компрометации с целью идентификации, анализа и проверки индикаторов компрометации (IoC) из отчетов других аналитиков.

Освоить инструменты для верификации «айóков» (IoC'ов, индикаторов компрометации).

Оформить результаты работы в структурированном и понятном для смежных специалистов формате

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

приведены в п.6.2.

5.3. Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает не менее 2 (двух) и не более 10 (десяти) 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:

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать обучающийся	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,45	45
КТ 2	100	0,15	15
Итого:	x	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:

1 семестр

КТ – 1.

Тема 1-2:

Деловая игра,
тестирование по теме 1,
тестирование по теме 2,
кейс по теме 2

КТ-2.

Тема 3.

Кейс по теме 3

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

1. *Критерии оценивания деловой игры*

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и полнота раскрытия темы	*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*
Работа в команде и защита	*30*	*Участие в команде на всех этапах деловой игры от 85% до 100%*
	15	*Частичное участие в деловой игре от 55% до 84%*
	0	*Не являлся участником команды менее 55%*
Итого максимально:	100	

2. *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	

3. *Критерии оценивания кейса:*

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

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

Для решения тестовых заданий студенту разрешается использование сети Интернет; программ для работы с электронными таблицами для обработки, анализа и визуализации данных.

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

6.1. Промежуточная аттестация проводится в форме зачета с оценкой:

Зачет поводится в устной форме опроса. Обучающемуся даётся время на подготовку.

Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.

При реализации промежуточной аттестации в ЭО/ДОТ могут быть использованы следующие формы: устно в ДОТ - в форме обоснованных ответов на задания различного типа; письменно в СДО - в форме письменного отчета заданий различного типа; тестирование в СДО.

6.2. Типовые оценочные материалы промежуточной аттестации.

Вопросы для подготовки к зачету с оценкой:

1) Государственная политика в сфере информационной безопасности и защиты информации.
2) Правовое обеспечение информационной безопасности.
3) Конституция РФ об «информационных правах и обязанностях».
4) Основные нормативные документы, регулирующие отношения в сфере информационной безопасности.
5) Акты регуляторов в сфере защиты информации.
6) Институт «тайны» в Российском законодательстве.
7) Классификация тайн.
8) Правовые основания отнесения сведений к категории ограниченного доступа.
9) Краткая история защиты информации в России.
10) Обобщенная модель информационной безопасности.
11) Институт стандартизации сферы информационной безопасности.
12) Национальные стандарты в области информационной безопасности и защиты информации.
13) Международные стандарты в области информационной безопасности и защиты информации.
14) Проблемы гармонизации стандартов информационной безопасности.
15) «Ландшафт» стандартов информационной безопасности.
16) Электромагнитный спектр как источник воздействия на информацию.
17) Каналы силового деструктивного воздействия (СДВ) на информацию.
18) Рекомендации по защите компьютерных систем от СДВ.
19) Классификация технических каналов утечки информации.
20) Модель и способы утечки по радиоканалу.
21) Модель и способы утечки по электрическому каналу.
22) Модель и способы утечки по акустическому (вибрационному, акустоэлектрическому) каналу.
23) Модель и способы утечки по оптическому (оптико-электронному) каналу.
24) Модель и способы утечки по каналу ПЭМИН.
25) Классификация угроз несанкционированного доступа (НСД) к информации.
26) Категории нарушителей безопасности информации и их возможности.
27) Общая характеристика уязвимостей.
28) Способы реализации угрозы НСД к информации.
29) Понятие и обобщенная модель нетрадиционного информационного канала.
30) Методы сокрытия информации в текстовых файлах.
31) Методы сокрытия информации в графических файлах.
32) Методы сокрытия информации в звуковых файлах.
33) Методы сокрытия информации в сетевых пакетах и исполняемых файлах.
34) Историография и классификация шифров.
35) Примеры криптографических алгоритмов.
36) Криптосистема с симметричными и несимметричными ключами.
37) Электронная цифровая подпись.
38) Мандатная и дискреционная модели доступа.

39) Процедура идентификации, аутентификации и авторизации.
40) Система паролирования.
41) Системы контроля и управления доступом.
42) Система охраны периметра.
43) Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети.
44) Понятие и функционал DLP-систем.
45) Объем и структура данных защищаемых DLP-системами.
46) Каналы коммуникаций, контролируемые DLP-системами.
47) Критерии оценки программных продуктов, реализующих функциональность DLP.
48) Понятие компьютерной преступности.
49) Масштабы и общественная опасность компьютерной преступности.
50) Виды и субъекты компьютерных преступлений.
51) Специфика расследования компьютерных преступлений.
52) Предупреждение компьютерных преступлений.
53) Дисциплинарная ответственность за разглашение охраняемой законом тайны.
54) Административная ответственность за нарушения в сфере информационной безопасности и защиты информации.
55) Уголовная ответственность за преступления в сфере компьютерной информации.

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).	К органам защиты государственной тайны относятся: 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).
		По виду защищаемой информации 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.	1. Укажите последовательность методов аутентификации по обеспечиваемому уровню защищенности (от наименее безопасного к наиболее защищенному) 1) аппаратная аутентификация 2) биометрическая аутентификация 3) парольная аутентификация

	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).	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).	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).
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	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.

	обоснования).	

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.	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.	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.	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.	0-19

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

Для решения задач открытого типа (контрольных работ), тестовых заданий студенту разрешается использование калькулятора; программ для работы с электронными таблицами для обработки, анализа и визуализации данных.

7. Методические материалы по освоению дисциплины (модуля)

Для изучения основных вопросов образовательной программы необходимо конспектировать материалы лекций, работать с рекомендованной преподавателем литературой, а также ресурсами информационно-телекоммуникационной сети «Интернет».

Для закрепления изученного материала даны вопросы по каждой теме дисциплины, на которые следует самостоятельно найти ответы.

Важной составной частью учебного процесса в вузе являются практические занятия. Практические занятия проводятся главным образом по дисциплинам, требующим закрепления навыков решения задач, и помогают студентам глубже усвоить учебный материал, приобрести умения применять методы информационно-аналитической работы к решению разнообразных задач, определять и оценивать ресурсы и существующие ограничения разного рода проектов. Практические занятия предназначены для самостоятельной работы студентов по решению конкретных задач. Каждое практическое занятие сопровождается домашними заданиями, выдаваемыми студентам для решения во внеаудиторное время.

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. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю (в том числе по электронной почте). Планируя консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам. Записи имеют первостепенное значение для

самостоятельной работы студентов. Они помогают понять построение изучаемого материала, выделить основные положения, проследить их логику. Кроме того, ведение записей способствует превращению чтения в активный процесс, мобилизует, наряду со зрительной, и моторную память. Следует помнить: у студента, систематически ведущего записи, создается свой индивидуальный фонд методических материалов для быстрого повторения изученных вопросов, для мобилизации накопленных знаний. Особенно важны и полезны записи тогда, когда в них находят отражение мысли, возникшие при самостоятельной работе.

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. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2082642. – Режим доступа: по подписке.

2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/477968.

3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/469235.

Все источники основной литературы взаимозаменяемы.

8.2. Дополнительная литература

1. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL:

https://znanium.com/catalog/product/1167736 (дата обращения: 10.07.2024). – Режим доступа: по подписке.

2. Попов, И. В. Информационная безопасность: практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/2016193 (дата обращения: 10.07.2024). – Режим доступа: по подписке.

3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/467370.

4. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2021. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/476798.

8.3. Нормативные правовые документы и иная правовая информация

Не используются

8.4 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

- Электронные учебники электронно-библиотечной системы (ЭБС) *«Айбукс»*
- Электронные учебники электронно-библиотечной системы (ЭБС) *«Юрайт»*
- Электронные учебники электронно-библиотечной системы (ЭБС) *«Лань»*
- Электронные учебники электронно-библиотечной системы (ЭБС) «*ZNANIUM.COM*»
- Электронные учебники электронно-библиотечной системы (ЭБС) «BOOK.RU»
- Электронные учебники электронно-библиотечной системы (ЭБС) *«IPRSMART»*

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/