Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.01 Средства информационной безопасности

(индекс, наименование дисциплины в соответствии с учебным планом)

38.04.05 «Бизнес-информатика»

(код, наименование направления подготовки/специальности)

«Аналитическое обеспечение информационной безопасности»

(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 ФТД.01 «Средства информационной безопасности» 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 ФТД.01 Средства информационной безопасности 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 ****
06.033/ СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ **С/02.7** Разработка проектных решений по защите информации в автоматизированных системах	ПКс 2	Способен обосновывать подходы и требования к системе обеспечения информационной безопасности, оценивать уровни безопасности компьютерных систем и сетей	ПКс 2.3	Оценивает уровни безопасности компьютерных систем и сетей	ПКс-2.3. З-6. **Знает** Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем ПКс-2.3. У-8 **Умеет** Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем
06.014 МЕНЕДЖЕР ПО ИНФОРМАЦИО	ПКс-4	Способен управлять информационн	ПКс-4.2	Управляет ИАС в защищенн	ПКс-4.2 Зн-3 **Знает**

ННЫМ ТЕХНОЛОГИЯМ **В/06.7/** Управление непрерывностью ИТ-сервисов		ыми сервисами, ресурсами ИТ и ИТ-инновациями. Управлять ИАС в защищенном исполнении, обслуживать системы защиты		ом исполнении	Методы контроля непрерывности ИТ-сервисов ПКс-4.2 У-3 **Умеет** Осуществлять мониторинг и контроль управления непрерывностью ИТ-сервисов

** 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 ФТД.01 Средства информационной безопасности – 1 зачетная единица – 36 акад.час; объем академических часов, выделенных на контактную работу обучающихся с преподавателем - 36 акад час, из них 4 акад.час – лекции, 4 час – практические занятия, 4 акад.час – контактная работа на аттестацию в период экзаменационных сессий, и 24 акад. час. выделяется на самостоятельную работу обучающихся.

Место дисциплины в структуре образовательной программы.

Дисциплина ФТД.01 Средства информационной безопасности относится к факультативным 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

№ 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 безопасности автоматизированных систем предприятия. Средства защиты информации от несанкционированного доступа	18	2			2				2				12	опрос
Тема 2	Методы защиты сетевых	18	2			2				2				12	Т, ПКЗ

	информационных технологий													
Промежуточная аттестация														зачет
Итого	36		4			4				4			24	

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 безопасности автоматизированных систем предприятия. Средства защиты информации от несанкционированного доступа

ПКс- 2.3

Проблема обеспечения безопасности АС. Место и роль АС в управлении бизнес-процессами. Основные понятия в области безопасности АС. Понятие безопасности автоматизированной информационной системы. Понятие защиты информации. Конфиденциальность, целостность, доступность. Субъекты, заинтересованные в обеспечении информационной безопасности. Уровни обеспечения информационной безопасности.

Понятие угрозы безопасности информации, АС и субъектов информационных отношений. Системная классификация угроз информационной безопасности. Понятие уязвимости АС, атаки на систему. Классификация каналов проникновения в АС и утечки информации. Неформальная модель нарушителя. Информационные риски. Управление рисками. Качественный и количественный анализ риска. Противодействие инсайдерской деятельности.

Основные принципы, меры обеспечения безопасности АС. Классификация мер и методов защиты информации. Правовые основы обеспечения безопасности АС: защищаемая информация, лицензирование, сертификация средств ЗИ и аттестация объектов информатизации. Ответственность за нарушения в сфере ЗИ.

Государственная система ЗИ. Главные направления работ по ЗИ. Структура государственной системы ЗИ. Политика безопасности организации. Способы защиты конфиденциальности, целостности и доступности в КС. Руководящие документы ФСТЭК РФ по оценке защищенности от НСД.

Понятие доступа, субъект и объект доступа. Понятие НСД. Классы и виды НСД. Несанкционированное копирование программ как особый вид НСД. Понятие злоумышленника при решении проблем компьютерной безопасности (КБ). Назначение и возможности средств защиты информации от НСД. Основные средства и механизмы защиты АС. Компьютерные сети и управление механизмами защиты.

Тема 2. Методы защиты сетевых информационных технологий
ПКс- 4.2

Аппаратно-программные средства защиты информации от НСД. Средства аппаратной поддержки, способы аутентификации. Штатные и дополнительные средства ЗИ от НСД. Системы идентификации и аутентификации: основные определения, типы, область применения, классификация. Задача идентификации пользователя. Идентификация

субъекта. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами. Парольные системы и парольная защита. Общие подходы к построению парольных систем. Выбор паролей. Методы взлома паролей. Методы выбора паролей.

Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.

Типовая корпоративная сеть. Основные принципы организации сетевой защиты. Уровни информационной инфраструктуры корпоративной сети. Типичные угрозы безопасности и уязвимости сетевых информационных систем. Классификация способов несанкционированного доступа и жизненный цикл атак. Средства защиты компьютерных сетей.

Защита периметра корпоративной сети. Угрозы, связанные с периметром корпоративной сети. Способы противодействия несанкционированному сетевому и межсетевому доступу. Аутентификация пользователя локальной сети. Разграничение доступа к локальной сети. Противодействие несанкционированному межсетевому доступу. Использование межсетевых экранов (Firewall). Критерии их оценки. Туннелирование. Технология виртуальных частных сетей. Защищенные сетевые протоколы. Безопасность работы в сети Интернет. Безопасная доставка e-mail сообщений. Обнаружение и устранение уязвимостей. Сканеры безопасности. Средства анализа защищенности системного уровня.

Мониторинг событий безопасности. Классификация систем обнаружения атак.

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 безопасности автоматизированных систем (АС) предприятия. Средства защиты информации от несанкционированного доступа (НСД)

ПКс- 2.3

Типовые вопросы для опроса по теме 1

1. Охарактеризуйте место и роль автоматизированных систем в управлении бизнес-процессами.

2. Что понимается под риском информационной безопасности? Каковы составляющие
3. риска?
4. В чем заключается анализ рисков и управление ими? Перечислите этапы анализа
5. и управления.
6. Каковы требования к методам оценки целесообразности затрат на обеспечение
7. безопасности АС?
8. Назовите категории затрат, связанных с безопасностью АС; кратко охарактеризуйте каждую категорию и перечислите статьи расходов для каждой из них.
9. Дайте определение АС и безопасности АС.
10. Приведите определения информации и информационных ресурсов.
11. Перечислите категории субъектов информационных отношений.
12. Охарактеризуйте три свойства информации: конфиденциальность, целостность и доступность.
13. Сформулируйте цели защиты АС и циркулирующей в ней информации.
14. Дайте определение понятий «угроза», «уязвимость» и «атака».
15. Перечислите источники угроз ИБ.
16. Назовите каналы проникновения в автоматизированную систему и утечки информации.
17. Какие факторы лежат в основе формирования модели нарушителя?
18. Каковы цели разработки моделей угроз и нарушителей?
19. В чем разница между нарушителем и злоумышленником?
20. Перечислите основные виды мер противодействия угрозам безопасности АС. Охарактеризуйте каждую меру противодействия.
21. Перечислите достоинства и недостатки различных мер защиты.
22. Возможно ли создание идеально надежной системы защиты и почему?
23. Какие основные принципы построения систем защиты?
24. Приведите классификацию информации по достуmюсти с точки зрения Федерального закона «Об информации, информационных технологиях и о защите информации».
25. Дайте определения обладателя информации и оператора информационной системы. Перечислите права и обязанности обладателя информации.
26. Что такое лицензирование? Какие виды лицензирования вам известны?
27. Для кого аттестация АИС по требованиям безопасности информации ФСТЭК России является обязательной?
28. Когда проводится аттестация АИС по требованиям безопасности информации ФСТЭК России?

29. Перечислите классы защищенности АС в соответствии с руководящими документами ФСТЭК России.
30. Какие подсистемы включает в себя комплекс программно-технических средств защиты информации от НСД в АС?
31. Перечислите основные организационно-технические мероприятия в области защиты информации.
32. В чем заключаются основные задачи государственной системы защиты информации?
33. Какова структура государственной системы защиты информации? Каковы цели защиты информации?
34. В чем заключается контроль состояния защиты информации?
35. Каковы источники финансирования мероприятий по защите информации?

Тема 2. Методы защиты сетевых информационных технологий
ПКс- 4.2

Задание открытого типа с развернутым ответом

Вопрос 1 Перечислите основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты.

Вопрос 2

Опишите процедуру внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций системы

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. Правила парольной защиты:

1) регламентируют контроль над действиями пользователей при работе с паролями;

2) определяют требования к организации защиты автоматизированной системы от разрушающего воздействия вредоносного ПО;

3) регламентируют организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в автоматизированной системе.

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 категорию защищаемой информации из левого столбца с его правильным свойством из правого столбца. Каждой категории соответствует одно свойство.

Категория	**Свойство защищаемой информации**
1. Открытая	А. Конфиденциальность защищаемой информации
2. Высокая	В. Целостность защищаемой информации
3. Средняя	С Доступность защищаемой информации

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. Авторизация пользователей осуществляется с применением следующих механизмов реализации разграничения доступа:

1) избирателъного управлеиия доступом с помощью атрибутивных схем, списков разрешений и т. п.;
2) полномочиого управлеиия доступом с помощью меток конфиденциальности ресурсов и уровней допуска пользователей;
3) регистрации факта попытки доступа и его параметров в системном журнале (в том числе НСД с превышением полномочий).

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 3 КТ в течение периода освоения дисциплины.

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

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

Расчет по контрольным точкам дисциплины

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

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

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

Тема 1
Опрос по теме 1
КТ – 1

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

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

Критерии оценивания опроса

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*
Защита и обсуждение	*30*	*Активное участие в обсуждении после защиты от 85% до 100%*
	15	*Частичное участие в обсуждении после защиты от 55% до 84%*
	0	*Не участвовал в обсуждении менее 55%*
Итого максимально:	100	

Критерии оценивания тестирования

Критерии оценки	Диапазон баллов	Описание критерия
Количество	*0*	*Количество правильных ответов*

		менее 55%
правильных ответов	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 объектов – сриншотов	*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*
Возможность демонстрировать работу системы	*5-29*	*Задание выложено с опозданием 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		*Четкое изложение хода выполнения задания*
	10- 15	*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 *зачета.*

Вопросы для подготовки к зачету:

1. Актуальность решения проблемы обеспечения безопасности автоматизированных систем.
2. Вредоносное программное обеспечение. Классификация вредоносных программ.
3. Методы и средства антивирусной защиты.
4. Парольная защита. Общие подходы к построению парольных систем.
5. Системы идентификации и аутентификации: основные определения, типы, область применения, классификация.
6. Конфиденциальность, целостность, доступность. Ролевое управление доступом.
7. Дискреционное и мандатное управление доступом.
8. Понятие угрозы информационной безопасности. Основные виды и источники угроз информационной безопасности.
9. Понятие уязвимости информационной системы, атаки на систему.
10. Цифровая стеганография. Определения и методы цифровой стеганографии.
11. Стегосистема. Области применения компьютерной стеганографии.
12. Понятия и определения современной криптографии. Стойкость криптоалгоритмов.
13. Классификация криптографических алгоритмов.
14. Персональные данные. Защита персональных данных
15. Алгоритмы электронной подписи. Хеширование.
16. Государственное регулирование в сфере информационной безопасности.
17. Защищенная электронная подпись. Цифровые сертификаты.
18. Компьютерные преступления.
19. Этапы процесса осуществления атаки на информационную систему. Классификация систем обнаружения атак.
20. Способы противодействия несанкционированному сетевому и межсетевому доступу.
21. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
22. Безопасность работы в сети Интернет. Основные угрозы при работе в Интернет.
23. Безопасная доставка e-mail сообщений.
24. Обеспечение информационной безопасности на государственном уровне.
25. .Обеспечение информационной безопасности на уровне предприятия.
26. Классификация тайн.
27. Правовые основания отнесения сведений к категории ограниченного доступа.
28. Институт стандартизации сферы информационной безопасности.
29. Национальные стандарты в области информационной безопасности и защиты информации.

30. Международные стандарты в области информационной безопасности и защиты информации.
31. Электромагнитный спектр как источник воздействия на информацию.
32. Каналы силового деструктивного воздействия (СДВ) на информацию.
33. Рекомендации по защите компьютерных систем от СДВ.
34. Классификация технических каналов утечки информации.
35. Модель и способы утечки по радиоканалу.
36. Модель и способы утечки по электрическому каналу.
37. Модель и способы утечки по акустическому (вибрационному, акустоэлектрическому) каналу.
38. Модель и способы утечки по оптическому (оптико-электронному) каналу.
39. Модель и способы утечки по каналу ПЭМИН.
40. Классификация угроз несанкционированного доступа (НСД) к информации.
41. Категории нарушителей безопасности информации и их возможности.
42. Общая характеристика уязвимостей.
43. Способы реализации угрозы НСД к информации.
44. Понятие и обобщенная модель нетрадиционного информационного канала.
45. Методы сокрытия информации в текстовых файлах.
46. Методы сокрытия информации в графических файлах.
47. Методы сокрытия информации в звуковых файлах.
48. Методы сокрытия информации в сетевых пакетах и исполняемых файлах.
49. Историография и классификация шифров.
50. Примеры криптографических алгоритмов.
51. Криптосистема с симметричными и несимметричными ключами.
52. Электронная цифровая подпись.
53. Мандатная и дискреционная модели доступа.
54. Процедура идентификации, аутентификации и авторизации.
55. Система паролирования.
56. Системы контроля и управления доступом.
57. Система охраны периметра.
58. Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети.
59. Понятие и функционал DLP-систем.
60. Объем и структура данных защищаемых DLP-системами.

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. 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. 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.

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.

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/