Приложение 4
к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДЭ.01.02 Средства защиты информации
(индекс, наименование дисциплины в соответствии с учебным планом)

38.04.05 Бизнес-информатика
(код, наименование направления подготовки)

Бизнес-информатика
(наименование образовательной программы)

очная форма обучения
(форма обучения)

Год набора – 2026

Санкт-Петербург, 2026

Автор(ы)-составитель(и) РПД:

Сухостат Валентина Васильевна, к.п.н., к.т.н., доцент, доцент кафедры бизнес-информатики

Заведующий кафедрой бизнес-информатики:

Наумов Владимир Николаевич, доктор военных наук, профессор

Рабочая программа дисциплины Б1.В.ДЭ.01.02 Средства защиты информации одобрена на заседании кафедры бизнес-информатики
СЗИУ РАНХиГС

протокол № 6 от «26» марта 2026 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.....4

2. Объем и место дисциплины в структуре образовательной программы.....5

3. Содержание и структура дисциплины (модуля).....6

4. Типы оценочных материалов, показатели и критерии оценивания.....10

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам 14

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине.....22

7. Методические материалы по освоению дисциплины.....29

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет.....31

9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы.....33

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

Дисциплина Б1.В.ДЭ.01.02 Средства защиты информации 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**
06.015 СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННЫМ СИСТЕМАМ Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 13.07.2023 № 586н D/01.7 Организационное и технологическое обеспечение определения первоначальных требований заказчика к ИС и возможности их реализации в ИС	ПКс-2	Способен обосновывать подходы, используемые в бизнес-анализе, руководить и управлять бизнес-анализом с использованием информационно-коммуникационных технологий	ПКс- 2.2	Решает задачи бизнес-аналитики с использованием современных инструментов ИТ-менеджмента	ПКс-2.2. З-1. **Знает** Инструменты и методы управления требованиями ПКс-2.2. З-6. **Знает** Программные средства и платформы инфраструктуры информационных технологий организаций ПКс-2.2. У-1. **Умеет.** Проводить переговоры в рамках управления работами по сопровождению и проектами создания (модификации) ИС

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

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

Общий объем дисциплины

5,00 з.е., 180 ак. час.

Контактная работа обучающихся с преподавателем по видам учебных занятий: 45 ак. час на контактную работу с преподавателем, из них 12 ак. часов на лекции и 22 ак. часа на практические занятия, 2 ак.часа на консультацию, 117 ак. часов на самостоятельную работу обучающихся (9 ак. час каттэк).

Дисциплина Б1.В.ДЭ.01.02 Средства защиты информации относится к дисциплинам по выбору учебного плана по направлению «Бизнес-информатика» 38.03.05, дисциплина изучается во 2-м семестре 1-го курса. Преподавание дисциплины опирается на дисциплины программы бакалавриата «Информационная безопасность», «Анализ данных», «Теория вероятностей», «Теория систем». В свою очередь она создаёт необходимые предпосылки для освоения программ таких дисциплин, как Б1.О.05 «Управление жизненным циклом информационных систем», Б1.В.03 «Цифровая трансформация бизнеса. Инфономика», Б1.В.09 «Интеллектуальный анализ текстов и изображений».

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

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

Формой промежуточной аттестации в соответствии с учебным планом является экзамен.

3. Содержание и структура дисциплины (модуля)

3.1. Структура дисциплины (модуля)

Очная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
			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	Каттэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Тема 1.	Основы безопасности автоматизированных систем предприятия	42	4			8								30	Т
Тема 2.	Средства защиты информации от несанкционированного доступа	40	4			6								30	О
Тема 3.	Методы защиты сетевых информационных технологий	69	4			8								57	Т
Промежуточная аттестация		29							2	9			18		Экзамен
Итого		180	12			22				9			18	117	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами,

привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

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.

Т – тестирование.

О – опрос.

3.2. Содержание дисциплины

Тема 1. Основы безопасности автоматизированных систем (АС) предприятия. ПКс-2.2.

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.

Тема 2. Средства защиты информации от несанкционированного доступа (НСД). ПКс-2.2.

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.

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.

Тема 3. Методы защиты сетевых информационных технологий. ПКс-2.2.

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. Оценочные материалы по дисциплине Б1.В.ДЭ.01.02 Средства защиты информации 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, 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 варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.	Ответ считается верным, если правильно указана вся последовательность цифр

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

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

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

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

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

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

5.1. В ходе реализации дисциплины Б1.В.ДЭ.01.02 Средства защиты информации используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Т – тестирование, О – опрос.

Тема 1. Основы безопасности автоматизированных систем (АС) предприятия. ПКс-2.2.

Опрос по теме 1:

1. Назовите категории затрат, связанных с безопасностью, АС; кратко охарактеризуйте каждую категорию и перечислите статьи расходов для каждой из них.
2. Дайте определение АС и безопасности АС.
3. Приведите определения информации и информационных ресурсов.
4. Перечислите категории субъектов информационных отношений.

5. Охарактеризуйте три свойства информации: конфиденциальность, целостность и доступность.

Тестирование по теме 1:

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

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

Задание закрытого типа 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 вариант-ты ответа.

3. Выбрать один верный ответ.

4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).

2. Связь между индивидуальными особенностями, целями и задачами бизнеса организации при построении СМИБ обеспечивается особенным корпоративным документом:

1) руководством BABOK;
2) центральной концептуальной моделью по бизнес-анализу (BACCM);
3) политикой информационной безопасности.

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 вариант-ты ответа.

3. Выбрать один верный ответ.

4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).

3.Политика информационной безопасности:

1) это система документированных управленческих решений по обеспечению ИБ организации;
2) это система документированных управленческих решений по обеспечению бизнес-процессов организации;
3) это исходный документ для разработки информационной системы организации.

Тема 2. Средства защиты информации от несанкционированного доступа (НСД). ПКс-2.2.

Опрос по теме 2:

1. Перечислите основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты.
2. В чем заключается политика безопасности организации?
3. Что такое явная и неявная компрометация ключей шифрования?
4. Какие действия должен предпринять сотрудник при компрометации ключей?
5. Каков порядок уничтожения ключей шифрования?

Тестирование по теме 2:

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 вариант-ты ответа.

3. Выбрать один верный ответ.

4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).

1. Какие угрозы, основанные на ошибках сотрудников структурных подразделений, могут быть использованы злоумышленниками для нанесения вреда организации и ее сотрудникам?
   1) Разглашение конфиденциальной информации (сведений, составляющих коммерческую тайну организации, персональных данных, паролей и др.).

2) Заражение рабочих станций вирусами, «троянскими» и другими вредоносными программами (внедрение шпионских кодов).
3) Потеря конкурентных преимуществ в результате разглашения сведений, составляющих коммерческую тайну.

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 вариант-ты ответа.

3. Выбрать один верный ответ.

4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).

2. К обеспечению безопасности информационных технологий организации должны привлекаться:
   1) все сотрудники, участвующие в процессах автоматизированной обработки информации;
   2) все категории обслуживающего АС персонала;
   3) все категории посторонних лиц.

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 вариант-ты ответа.

3. Выбрать один верный ответ.

4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).

3. 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.

Тема 3. Методы защиты сетевых информационных технологий. ПКс-2.2.

Опрос по теме 3:

1. Охарактеризуйте уровни информационной инфраструктуры корпоративной сети.
2. Дайте определения угрозы, уязвимости и атаки. Охарактеризуйте на примерах взаимосвязь между этими понятиями.
3. Приведите классификационные схемы уязвимостей и атак.
4. Какой из механизмов реализации сетевых атак наиболее сложен с точки зрения обнаружения?
5. Какой из механизмов реализации сетевых атак не подразумевает использования какой-либо уязвимости?

Тестирование по теме 3:

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 вариант-ты ответа.

3. Выбрать один верный ответ.

4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).

1. Аналитик оценки:
   1) измеряет и оценивает свидетельства оценки, предоставленными владельцами активов;
   2) выбирает способ, модель оценки и определяет методику оценки ИБ;
   3) проводит анализ результатов оценки и формирует отчет и рекомендации по результатам оценки.

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 вариант-ты ответа.

3. Выбрать один верный ответ.

4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).

2. Биометрические методы идентификации подразделяют на группы:
   1) статические;
   2) мобильные;
   3) динамические.

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 вариант-ты ответа.

3. Выбрать один верный ответ.

4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).

3. К статическим биометрическим методам идентификации относится распознавание:
   1) по отпечаткам пальцев;
   2) по радужной оболочке глаз;
   3) по клавиатурному почерку.

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.

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

2. 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	0,2	20
КТ-2	100	0,2	20
КТ-3	100	0,2	20
Итого:	х	0,6	60

Формула расчета результата контрольной точки:

Результат контрольной точки = Количество баллов за работу в рамках КТ Х Коэффициент веса контрольной точки.

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

КТ – 1.
Тема 1.
Опрос по теме 1.
Тестирование (Т) по теме 1.

КТ-2
Тема 2.
Опрос по теме 2.
Тестирование (Т) по теме 2.

КТ-3
Тема 3.
Опрос по теме 3.
Тестирование (Т) по теме 3.

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

1. *Критерии оценивания тестирования:*

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

2. *Критерии оценивания опроса:*

Диапазон баллов	Описание критерия
85-100	*Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.*
65-84	*Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом*

	оформлении излагаемого.
55-64	*Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.*
0-54	*Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.*

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

Для решения задач открытого типа (кейсов), тестовых заданий студенту разрешается использование программ для работы с электронными таблицами для обработки, анализа и визуализации данных. Для построения графиков, диаграмм, моделей в различных нотациях студенту можно использовать любой соответствующий онлайн-инструмент.

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

6.1. Промежуточная аттестация (экзамен) проводится в компьютерном классе в форме устного ответа на теоретические вопросы и выполнения заданий по темам учебных дисциплин.

Во время экзамена проверяется уровень знаний по дисциплине Средства защиты информации, а также уровень умений решать учебные задачи с использованием программных приложений.

Обучение по дисциплине «Средства защиты информации» предполагает изучение курса на аудиторных занятиях (лекции, практические работы) и самостоятельной работы обучающихся. Семинарские занятия дисциплины «Средства защиты информации» предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий. С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

- знакомит с новым учебным материалом;
- разъясняет учебные элементы, трудные для понимания;
- систематизирует учебный материал;
- ориентирует в учебном процессе.

Подготовка к лекции заключается в следующем:

- внимательно прочитайте материал предыдущей лекции;

– узнайте тему предстоящей лекции (по тематическому плану, по информации лектора);

– ознакомьтесь с учебным материалом по рекомендуемой литературе;

– постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;

– запишите возможные вопросы, которые вы зададите лектору на лекции.

Подготовка к практическим занятиям:

– внимательно прочитайте материал лекций, относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом;

– ответьте на контрольные вопросы по семинарским занятиям, готовьтесь дать развернутый ответ на каждый из вопросов;

– уясните, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до семинарского занятия) во время текущих консультаций преподавателя;

– готовиться можно индивидуально, парами или в составе малой группы, последние являются эффективными формами работы;

– рабочая программа дисциплины в части целей, перечню знаний, умений, терминов и учебных вопросов может быть использована вами в качестве ориентира в организации обучения.

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

6.2. Типовые оценочные материалы промежуточной аттестации

Вопросы для подготовки к экзамену

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.

Типовые задания для экзамена

Задание. Построение модели угроз ИБ

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 B).	1. Что из перечисленного относится к программно-аппаратным средствам идентификации и аутентификации пользователя для защиты от НСД? Варианты ответов: A) Установка кондиционера в серверной комнате B) Использование антивируса для проверки флешки C) Сканер отпечатка пальца (биометрический датчик) D) Регулярное резервное копирование баз данных
		2. Какой метод защиты информации от несанкционированного доступа основан на преобразовании данных в нечитаемую форму с использованием ключа? Вариант ответов: A) Межсетевое экранирование (Firewall) B) Криптографическое шифрование C) Мандатное управление доступом D) Экранирование электромагнитного излучения
Задание закрытого типа на установление	1.Внимательно прочитать текст задания и понять, что в качестве	1.Установите соответствие между средством защиты информации и принципом (или типом) его

<table>
<tr>
<td>соответствия</td>
<td>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).</td>
<td>работы:
<table>
<tr><td>Средство защиты от НСД</td><td>Принцип работы / Тип</td></tr>
<tr><td>1. Межсетевой экран (Firewall)</td><td>A) Преобразование информации в нечитаемую форму с помощью ключа для предотвращения перехвата</td></tr>
<tr><td>2. Система обнаружения вторжений (СОВ/IDS)</td><td>B) Разграничение доступа на основе меток конфиденциальности объектов и уровня допуска субъектов</td></tr>
<tr><td>3. Криптографическое шифрование диска</td><td>C) Анализ сетевого трафика или системных вызовов для выявления и регистрации аномальной активности</td></tr>
<tr><td>4. Мандатная модель доступа (например, в ОС с контролем потоков)</td><td>D) Фильтрация сетевых пакетов по правилам (IP-адресам, портам, протоколам)</td></tr>
</table>
<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
2.Установите соответствие между угрозами и их методом защиты:
<table>
<tr><td>Угроза</td><td>Метод защиты</td></tr>
<tr><td>1. Перехват пароля при входе на сайт через открытый Wi-Fi</td><td>A) Использование IDS/IPS для анализа аномалий трафика</td></tr>
<tr><td>2. сканирование портов и попытка подбора SSH-ключей из внешней сети</td><td>B) Настройка списков контроля доступа (ACL) на маршрутизаторе</td></tr>
<tr><td>3. Распространение сетевого червя между серверами внутри сегмента</td><td>C) Применение HTTPS (TLS/SSL) или WPA3 на уровне канала</td></tr>
<tr><td>4. DDoS-атака с флудом SYN-пакетов</td><td>D) Микросегментация с политиками zero-trust и изоляция хостов</td></tr>
</table>
<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
</td>
</tr>
<tr>
<td>Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных</td>
<td>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).</td>
<td>1. Какие из перечисленных методов относятся к криптографическим методам защиты сетевых информационных технологий? (Выберите три правильных ответа.)
A) Использование протокола TLS/SSL для защиты HTTPS-соединений
B) Настройка списков доступа ACL на маршрутизаторе
C) Шифрование трафика в VPN-туннеле (IPsec, OpenVPN)
D) Обнаружение аномалий поведения пользователей с помощью SIEM
E) Электронная подпись (ЭП) для</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td>аутентификации сетевых пакетов
F) Разделение сети на VLAN для изоляции трафика</td></tr>
<tr><td></td><td></td><td>2. Какие методы эффективны для защиты сетевых информационных технологий от атак типа «человек посередине» (Man-in-the-Middle, MITM) в корпоративной сети? (Выберите три правильных ответа.)
A) Принудительное использование HTTPS с валидными сертификатами
B) Применение протокола SSH вместо Telnet для удалённого управления
C) Отключение всех межсетевых экранов для увеличения скорости
D) Использование DNSSEC для проверки подлинности DNS-ответов
E) Отправка паролей в открытом виде в заголовках HTTP
F) Реализация 802.1X (например, EAP-TLS) для аутентификации устройств при подключении к коммутатору</td></tr>
<tr><td>Задание закрытого типа на установление последовательности</td><td>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).</td><td>1. Установите правильную последовательность этапов обработки сетевого пакета при прохождении через современный межсетевой экран с анализом состояния соединений (Stateful Firewall) и функцией IPS (системы предотвращения вторжений).
<table>
<tr><td>Буква</td><td>Этап</td></tr>
<tr><td>A</td><td>Проверка пакета на соответствие сигнатурам атак (IPS)</td></tr>
<tr><td>B</td><td>Приём пакета с сетевого интерфейса</td></tr>
<tr><td>C</td><td>Логирование разрешённого пакета и передача его получателю</td></tr>
<tr><td>D</td><td>Проверка состояния соединения (есть ли уже открытая сессия)</td></tr>
<tr><td>E</td><td>Отбрасывание пакета или сброс соединения в случае обнаружения атаки</td></tr>
<tr><td>F</td><td>Применение правил фильтрации (ACL) по IP-адресам и портам</td></tr>
</table>
2. Установите правильную последовательность действий администратора при организации защищённого VPN-соединения между удалённым офисом и головным офисом (технология IPsec в режиме туннеля).
<table>
<tr><td>Буква</td><td>Действие</td></tr>
<tr><td>A</td><td>Настройка правил межсетевого экрана для разрешения протоколов ESP/AH и UDP-порта 500 (IKE)</td></tr>
<tr><td>B</td><td>Проверка работы туннеля (ping, трассировка через VPN-шлюз)</td></tr>
<tr><td>C</td><td>Настройка политик шифрования и аутентификации (алгоритмы, ключи)</td></tr>
<tr><td>D</td><td>Генерация и обмен предварительными ключами (PSK) или сертификатами</td></tr>
<tr><td>E</td><td>Настройка фаз IKE: Phase 1 (аутентификация и защищённый канал) и Phase 2 (собственно, IPsec SA)</td></tr>
<tr><td>F</td><td>Определение защищаемых сетей</td></tr>
</table>
</td></tr>
</table>

		(локальная сеть офиса A и локальная сеть офиса B)
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, текст обоснования).	1. Какой метод защиты наиболее эффективен против ARP-spoofing в данной сети? A) Фильтрация MAC-адресов на коммутаторах (port-security) B) Использование статических ARP-записей на всех рабочих станциях C) Включение защиты DHCP Snooping + ARP Inspection (DAI) на коммутаторах D) Полное отключение протокола ARP и настройка статических маршрутов
		2. Какой метод защиты сетевых информационных технологий следует применить в первую очередь? A) NAT (Network Address Translation) B) Технология VPN в режиме туннеля (например, IPsec) C) Межсетевое экранирование с глубокой фильтрацией пакетов (NGFW) D) Использование VLAN с изоляцией трафика
Задание открытого типа с развернутым ответом	1. Внимательно прочитать текст задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи записать решение и ответ	1. Какие программные средства достаточно установить (не менее двух).
		2. Какое аппаратное или программно-аппаратное средство является обязательным даже при ограниченном бюджете?

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,	20-29

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.	
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 решения задач открытого типа (кейсов), тестовых заданий студенту разрешается использование программ для работы с электронными таблицами для обработки, анализа и визуализации данных. Для построения графиков, диаграмм, моделей в различных нотациях студенту можно использовать любой соответствующий онлайн-инструмент.

7. Методические материалы по освоению дисциплины (модуля)

Для изучения основных вопросов образовательной программы предусмотрены следующие виды аудиторных занятий: лекции, практические занятия, контрольные работы. На лекциях рассматриваются наиболее сложный материал дисциплины. Лекция сопровождается презентациями, компьютерными текстами лекции, что позволяет студенту самостоятельно работать над повторением и закреплением лекционного материала. Для этого студенту должно быть предоставлено право самостоятельно работать в компьютерных классах в сети Интернет.

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 принципы системного подхода к решению разнообразных задач, 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 предназначены для самостоятельной работы студентов по решении конкретных задач проектного семинара. Все практические занятия проводятся в компьютерных классах. Также в компьютерных классах или с использованием мультимедийных средств проводятся лекции. В ходе лекций теоретические положения поясняются возможностями программных пакетов реализовать данные положения. Так, например, при рассмотрении моделировании бизнес-процессов и работы с данными.

Каждое практическое занятие сопровождается заданиями, выдаваемыми студентам для решения внеаудиторное время. Для оказания помощи в решении задач имеются тексты практических заданий с условиями задач и вариантами их решения.

Подготовка к текущему и промежуточному контролю предполагает изучение представленных вопросов к зачету, работу над тестами, представленными в данной рабочей программе, выполнение проектной работы.

Для активизации работы студентов во время контактной работы с преподавателем отдельные занятия проводятся в интерактивной форме. В основном интерактивная форма занятий обеспечивается при проведении занятий в компьютерном классе. Интерактивная форма обеспечивается наличием разработанных файлом с заданиями, наличием контрольных вопросов, возможностью доступа к системе дистанционного обучения, использованием канала MTS-Link, а также Яндекс.Мессенджер.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Зенков, Андрей Вячеславович. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. - 2-е изд., перераб. и доп. - Москва : Юрайт, 2023. - 107 с. - Текст: электронный. - URL: https://urait.ru/book/informacionnaya-bezopasnost-i-zaschita-informacii-530927. - Режим доступа: для авторизир. пользователей..
2. Корабельников, Сергей Маркович. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М.

Корабельников. - Москва : Юрайт, 2022. - 111 с. - Текст: электронный. - URL: https://urait.ru/book/prestupleniya-v-sfere-informacionnoy-bezopasnosti-496492. - Режим доступа: для авторизир. пользователей.
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. Золотарев, В. В. Управление информационной безопасностью. Ч. 1: Анализ информационных рисков : учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463037 (дата обращения: 03.08.2021). – Режим доступа: по подписке.
2. Дронов В.Ю. Международные и отечественные стандарты по информационной безопасности : учебно-методическое пособие / Дронов В.Ю.. — Новосибирск : Новосибирский государственный технический университет, 2016. — 34 с. — ISBN 978-5-7782-3112-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91395.html (дата обращения: 03.08.2021). — Режим доступа: для авторизир. Пользователей
3. Гасанов Э.С. Самарина Е.А. Управление информационной безопасностью в корпоративной предпринимательской среде в условиях киберугроз цифровой экономики [Электронный ресурс] – URL: https://cyberleninka.ru/article/n/

8.3. Нормативные правовые документы и иная правовая информация
Не используются

8.4. Интернет-ресурсы

Система организации конкурсов по исследованию данных, а также социальная сеть специалистов по обработке данных и машинному обучению. http://kaggle.com

Обучающимся обеспечен доступ к материалам курса в СДО Академии http://lms.ranepa.ru, а также через сайт научной библиотеки https://sziu-lib.ranepa.ru к следующим подписным электронным ресурсам:

- Электронные учебники электронно-библиотечной системы (ЭБС) «Айбукс».
- Электронные учебники электронно-библиотечной системы (ЭБС) «Лань».
- Электронные учебники электронно-библиотечной системы (ЭБС) «Юрайт».

− Электронные учебники электронно-библиотечной системы (ЭБС) «*ZNANIUM.COM*».
− Электронные учебники электронно-библиотечной системы (ЭБС) «BOOK.RU».
− Электронные учебники электронно-библиотечной системы (ЭБС) *«IPRSMART».*
Возможно использование, кроме вышеперечисленных ресурсов, и других электронных ресурсов сети Интернет.

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

№ п/п	Наименование
1.	Компьютерные классы с персональными ЭВМ, объединенными в локальные сети с выходом в Интернет
2.	Текстовый редактор и табличный процессор
3.	Мультимедийные средства в каждом компьютерном классе и в лекционной аудитории
4.	Браузер, сетевые коммуникационные средства для выхода в Интернет
5.	СДО Академии http://lms.ranepa.ru