Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01 Защита информации в корпоративных информационных системах
(индекс, наименование дисциплины в соответствии с учебным планом)

09.04.03 Прикладная информатика
(код, наименование направления подготовки/специальности)

Корпоративные информационные системы
(наименование образовательной программы)

Очная форма обучения
(форма обучения)

Год набора – 2026

Донецк

Автор(ы)-составитель(и) РПД:

Тарусина Наталья Эмильяновна, канд. экон. наук, доцент, доцент кафедры информационных технологий

Заведующий кафедрой:

Брадул Наталья Валерьевна, канд. физ.-мат. наук, доцент, заведующий кафедрой информационных технологий

Рабочая программа дисциплины Б1.В.01 Защита информации в корпоративных информационных системах одобрена на заседании кафедры информационных технологий факультета государственной службы и управления Донецкого филиала РАНХиГС.

Протокол № 7 от «05» марта 2026 г.

СОДЕРЖАНИЕ

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

Дисциплина Б1.В.01 Защита информации в корпоративных информационных системах обеспечивает формирование у обучающихся следующих общепрофессиональных компетенций:

ОТФ/ТФ и реквизиты ПС *(при наличии)*	**Код компетенции**	**Наименование компетенции**	**Код индикатора достижения компетенций**	**Наименование индикатора достижения компетенций**	**Образовательный результат**
-	УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1	Формулирует основные принципы профессионального и личностного развития, способы совершенствования своей деятельности на основе самооценки; планирует решение задач собственного профессионального и личностного развития; использует способы управления своей познавательной деятельностью и ее совершенствования	УК-6.1. З-1 **Знает** основные принципы профессионального и личностного развития, способы совершенствования своей деятельности на основе самооценки, способы управления своей познавательной деятельностью. УК-6.1. У-1 **Умеет** решать задачи собственного профессионального и личностного развития, включая задачи изменения карьерной траектории, расставлять приоритеты.
С/16.6 Проектирование и дизайн ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС 06.015 «Специалист по информационным системам», утвержден	ПК-1	Способен проектировать и разрабатывать дизайн ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС	ПК-1.2	Верифицирует структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС	ПК-1.2. З-1 **Знает** Инструменты и методы проектирования и дизайна ИС ПК-1.2. У-2 **Умеет** Анализировать и структурировать входные данные в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС
			ПК-1.5	Устраняет обнаруженные несоответствия в программном коде и	ПК-1.5. З-1 **Знает** Возможности ИС ПК-1.5. У-2 **Умеет**

приказом Министерства труда и социальной защиты Российской Федерации от 13.07.2023 № 586н (зарегистрировано в Минюсте России 16 августа 2023 г. № 74817)				в дизайне ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС	Анализировать и структурировать входные данные в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС

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

Общий объем дисциплины:

4,00 з.е., 144 ак.час

Контактная работа обучающихся с преподавателем по видам учебных занятий: 36 ак. час на контактную работу с преподавателем, из них 18 ак.часа на лекции и 18 ак.часа на практические занятия. 79 ак. часа на самостоятельную работу обучающихся.

Б1.В.01 Защита информации в корпоративных информационных системах реализуется во 2-м семестре 1-го курса после изучения дисциплин:

- Управление проектами информатизации предприятий.

3. Содержание и структура дисциплины (модуля)

3.1. Структура дисциплины (модуля)

Очная форма обучения

№ п/п	Наименование тем и (или) разделов		Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
		ВСЕГО	Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Кат тэк	Контроль	СР кр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Раздел 1. Проблемы безопасности корпоративной информации. Технологии защиты корпоративных данных															
Тема 1.	Основные понятия и анализ угроз информационной безопасности. Политики безопасности	13	2	0	0	2	0	0	0	0	0	0	0	9	Устный опрос Контрольное задание Тестирование КТ №1

Тема 2.	Криптографическая защита информации.	13	2	0	0	2	0	0	0	0	0	0	0	9	Устный опрос Контрольное задание Тестирование КТ №1
Тема 3.	Идентификация, аутентификация и управление доступом	13	2	0	0	2	0	0	0	0	0	0	0	9	Устный опрос Контрольное задание КТ №1
Тема 4.	Защита электронного документооборота	13	2	0	0	2	0	0	0	0	0	0	0	9	Устный опрос Контрольное задание КТ №1
Раздел 2. Комплексная защита корпоративных информационных систем															
Тема 5.	Принципы комплексной защиты информации КИС	13	2	0	0	2	0	0	0	0	0	0	0	9	Устный опрос Контрольное задание КТ №2
Тема 6.	Защита от вредоносных программ. Обнаружение и предотвращение вторжений	13	2	0	0	2	0	0	0	0	0	0	0	9	Устный опрос Контрольное задание КТ №3
Тема 7.	Межсетевое экранирование. Виртуальные защищенные сети VPN	13	2	0	0	2	0	0	0	0	0	0	0	9	Устный опрос Контрольное задание

															КТ №3
Тема 8.	Управление средствами обеспечения информационной безопасности	12	2	0	0	2	0	0	0	0	0	0	0	8	Устный опрос КТ №3
Тема 9.	Стандарты информационной безопасности	12	2	0	0	2	0	0	0	0	0	0	0	8	Устный опрос КТ №3
	Промежуточная аттестация.	29	0	0	0	0	0	0	2	9	18	0	0	0	Экзамен
	Итого	144	18	0	0	18	0	0	2	9	18	0	0	79	

Используемые сокращения:

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

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

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

СРэк – самостоятельная работа на подготовку к экзамену.

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

3.2. Содержание дисциплины

Тема 1. Основные понятия и анализ угроз информационной безопасности. Политики безопасности. УК-6.1 ПК-1.2.

Основные понятия защиты информации и информационной безопасности

Анализ угроз информационной безопасности

Способы обеспечения безопасности информационных систем

Основные понятия политики безопасности

Структура политики безопасности организации

Разработка политики безопасности организации.

Тема 2. Криптографическая защита информации. УК-6.1 ПК-1.2.

Основные понятия криптографической защиты информации

Симметричные криптосистемы шифрования

Асимметричные криптосистемы шифрования

Функции хэширования

Электронная цифровая подпись

Управление криптоключами

Инфраструктура управления открытыми ключами PKI.

Тема 3. Идентификация, аутентификация и управление доступом. УК-6.1 ПК-1.2.

Аутентификация, авторизация и администрирование действий пользователей

Методы аутентификации, использующие пароли

Строгая аутентификация

Биометрическая аутентификация пользователя

Управление доступом по схеме однократного входа с авторизацией Single Sign-On.

Тема 4. Защита электронного документооборота. УК-6.1 ПК-1.2.

Концепция электронного документооборота

Особенности защиты электронного документооборота

Защита баз данных

Защита корпоративного почтового документооборота

Защита системы электронного документооборота DIRECTUM

Тема 5. Принципы комплексной защиты информации КИС. УК-6.1 ПК-1.2.

Архитектура корпоративной информационной системы

Структура системы защиты информации в корпоративной информационной системе

Комплексный подход к обеспечению информационной безопасности

КИС

Подсистемы информационной безопасности КИС.

Тема 6. Защита от вредоносных программ. Обнаружение и предотвращение вторжений. УК-6.1 ПК-1.2.

Классификация вредоносных программ

Основы работы антивирусных программ

Средства защиты от нежелательной корреспонденции

Защита корпоративной сети от воздействия вредоносных программ и вирусов

Основные понятия

Обнаружение вторжений системой IPS

Предотвращение вторжений в КИС

Современные средства предотвращения вторжений.

Тема 7. Межсетевое экранирование. Виртуальные защищенные сети VPN. УК-6.1 ПК-1.5.

Функции межсетевых экранов

Особенности функционирования межсетевых экранов Схемы сетевой защиты на базе межсетевых экранов

Концепция построения виртуальных защищенных сетей VPN

-решения для построения защищенных сетей

Современные VPN-продукты.

Тема 8. Управление средствами обеспечения информационной безопасности. УК-6.1 ПК-1.5.

Задачи управления информационной безопасностью

Архитектура управления информационной безопасностью КИС

Функционирование системы управления информационной безопасностью КИС

Обзор современных систем управления безопасностью.

Тема 9. Стандарты информационной безопасности. УК-6.1 ПК-1.5.

Роль стандартов информационной безопасности

Международные стандарты информационной безопасности

Отечественные стандарты информационной безопасности.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.01 Защита информации в корпоративных информационных системах 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 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 Донецкого филиала РАНХиГС.

Итоговая балльная оценка	**Традиционная система**	**Бинарная система**	**ECTS**	
			Для традиционной системы	**Для бинарной системы**
90-100	Отлично	Зачтено	A	P/ Passed
80-89	Хорошо		B	P/ Passed
75-79			C	P/ Passed
70-74	Удовлетворительно		B	P/ Passed
60-69			E	P/ Passed
0-59	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
100 баллов	100 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.01 Защита информации в корпоративных информационных системах используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

доклад, устный опрос, тестирование, контрольные задания.

Распределение баллов по видам учебной деятельности (БРС)

Раздел/Темы	Формы текущего контроля			КТ
	УО	КЗ	ТЗ	
Р-1. / Т-1	3	3	4	15
Р-1. / Т-2	3	3	4	

Р-1. / Т-3	3	3		
Р-1. / Т-4	3	3		
Р-2. / Т-5	3	3		14
Р-2. / Т-6	3	3		15
Р-2. / Т-7	3	3		
Р-2. / Т-8	3			
Р-2. / Т-9	3			
Итого: 100 б	27	21	8	44

УО – устный опрос;
КЗ – контрольные задания;
ТЗ – тестовое задание;
КТ – контрольные точки.

Критерии оценивания опроса:

Балы	Описание критерия
3	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.
2	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.
1	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	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

0* - в журнал академической группы не выставляется

Критерии оценивания контрольных заданий:

Балы	Описание критерия
3	Обучающимся задание выполнено без ошибок и в полном объеме.
2	Обучающимся допущены отдельные ошибки при выполнении задания
1	У обучающегося отсутствуют ответы на большинство вопросов задачи, задание не выполнено или выполнено не верно.

0* - в журнал академической группы не выставляется

Критерии оценивания тестовых заданий:

Балы	Описание критерия	
4	Свыше 80% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
2-3	Свыше 70% правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
1	Свыше 50% правильных ответов.	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
0	Менее 50% правильных ответов.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

0* - в журнал академической группы не выставляется

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных заданий по разделу):

Тема 1. Основные понятия и анализ угроз информационной безопасности. Политики безопасности. УК-6.1 ПК-1.2.

Контрольные вопросы для проведения опроса:

1. Сформулируйте понятие информационной безопасности ИС.
2. Объясните понятия целостности, конфиденциальности и доступности информации.
3. Объясните понятия идентификации, аутентификации и авторизации пользователя. Как они взаимосвязаны?
4. Укажите отличия санкционированного доступа от несанкционированного доступа к информации.
5. Сформулируйте определение политики безопасности.
6. Сформулируйте особенности избирательной и полномочной политики безопасности.
7. Объясните понятие «угроза безопасности ИС».
8. Укажите основные признаки классификации возможных угроз безопасности ИС.
9. Каковы основные виды угроз безопасности ИС по цели и степени воздействия?
10. Дайте краткую характеристику угроз безопасности, обозначаемых терминами: «троянский конь»,
11. «вирус», «червь»?
12. Перечислите и дайте краткую характеристику основных методов реализации угроз информационной безопасности.
13. Объясните суть комплексного подхода к обеспечению информационной безопасности ИС.

14. Объясните понятие «политика безопасности организации».
15. Какие разделы должна содержать документально оформленная политика безопасности?
16. Какие проблемы решает верхний уровень политики безопасности?
17. Какие задачи решает средний уровень политики безопасности?
18. Каковы особенности нижнего уровня политики безопасности?
19. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.
20. Опишите структуру политики безопасности организации.
21. Что представляют собой специализированные политики безопасности?
22. Приведите несколько примеров специализированных политик безопасности с описанием их особенностей.
23. Что представляют собой процедуры безопасности?
24. Приведите несколько примеров процедур безопасности с описанием их особенностей.
25. Сформулируйте основные этапы разработки политики безопасности организации.

Тестирование

Задание закрытого типа на установление последовательности

Прочитайте текст и установите последовательность.

Главным компонентом политики безопасности организации является базовая политика безопасности. Базовая политика безопасности устанавливает, как организация обрабатывает информацию, кто может получить к ней доступ и как это можно сделать.

Укажите правильную последовательность этапов разработки базовой политики безопасности:

1. Составление программы обеспечения безопасности.
2. Назначение ответственных лиц и распределение ресурсов.
3. Анализ рисков и определение стратегии защиты.
4. Определение порядка контроля выполнения программы.

Запишите соответствующую последовательность цифр слева направо:

Контрольные задания

Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Под политикой безопасности организации понимают совокупность управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Задание:

1. Какие принципы необходимо учитывать при разработке политики безопасности организации?

2. Объясните, почему они важны для обеспечения информационной безопасности.

Ответ:

Тема 2. Криптографическая защита информации. УК-6.1 ПК-1.2.

Контрольные вопросы для проведения опроса:

1. Что такое криптография?
2. Дайте определения следующих понятий: криптограмма, криптоалгоритм, криптосистема.
3. В чем состоит коренное различие симметричных и асимметричных криптосистем?
4. Охарактеризуйте четыре основных режима работы блочного алгоритма.
5. Расскажите о способах комбинирования блочных алгоритмов для получения алгоритмов с более длинным ключом, сравните их между собой.
6. Каковы основные характеристики и режимы работы отечественного стандарта шифрования данных?
7. Сформулируйте концепцию криптосистемы с открытым ключом?
8. Дайте определение однонаправленной функции. Приведите примеры однонаправленных функций.
9. Каковы особенности однонаправленных функций с «потайным ходом»?
10. На чем основывается надежность криптоалгоритма шифрования RSA?
11. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.
12. Опишите отечественный стандарт цифровой подписи, укажите его преимущества по сравнению с алгоритмом цифровой подписи DSA.
13. Каково назначение хэш-функции и каким требованиям должна удовлетворять качественная хэш- функция?
14. Каким образом комбинированный метод шифрования позволяет сочетать достоинства асимметричных и симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования.
15. Опишите работу алгоритма Диффи - Хэллмана. Укажите достоинства этого алгоритма.
16. Каково назначение инфраструктуры открытых ключей PKI? Опишите функционирование инфраструктуры PKI.

Тестирование

Задание комбинированного типа с выбором одного верного ответа из предложенных и обоснованием выбора

Прочитайте текст, выберите один правильный ответ и запишите аргументы, обосновывающие выбор ответа.

Базовая политика безопасности устанавливает, как организация обрабатывает информацию, кто может получить к ней доступ и как это можно сделать. Обычно базовая политика безопасности организации поддерживается набором специализированных политик и процедур безопасности.

Какая из следующих политик предназначена для безопасного использования удаленного доступа?

А. Политика защиты паролей.

Б. Политика конфиденциальности.

В. Политика удаленного доступа к ресурсам сети.

Г. Политика по защите информации.

Ответ:

Обоснование выбора:

Контрольные задания

Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Комплексный подход к построению системы защиты информации позволяет организовать целостную систему защиты от угроз.

Задание:

Перечислить меры, которые эффективно управляют рисками в корпоративной информационной системе и предотвращают несанкционированный доступ.

Ответ:

Тема 3. Идентификация, аутентификация и управление доступом. УК-6.1 ПК-1.2.

Контрольные вопросы для проведения опроса:

1. Дайте определения понятий: идентификация, аутентификация, авторизация, администрирование. Что понимают под решением задач AAA?
2. Какие задачи решает подсистема управления идентификацией и доступом IAM (Identity and Access Management)?
3. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?
4. Перечислите основные атаки на протоколы аутентификации.

5. Опишите метод аутентификации на основе многоразовых паролей. Каковы недостатки этого метода?

6. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?

7. Сформулируйте принцип строгой аутентификации. Опишите типы процедур строгой аутентификации.

8. Объясните назначение PIN-кода и особенности его использования.

9. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используются для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?

10. Опишите функциональность и характеристики смарт-карт и USB-токенов.

11. Опишите методы биометрической аутентификации пользователя. Что означают коэффициент ошибочных отказов и коэффициент ошибочных подтверждений?

12. Поясните принцип управления доступом по схеме однократного входа с авторизацией Single Sign-On.

Контрольные задания

1. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Биометрическая аутентификация пользователя, позволяет уверенно аутентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.

Задание:

1. Опишите методы биометрической аутентификации пользователя.

2. Что означают коэффициент ошибочных отказов и коэффициент ошибочных подтверждений?

Ответ:

2. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает идентификацию и аутентификацию.

Задание:

1. Опишите метод аутентификации на основе многоразовых паролей.

2. Опишите метод аутентификации на основе одноразовых паролей.

3. Каковы их недостатки?

Ответ:

3. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Строгая аутентификация — это процесс проверки подлинности пользователя или системы с использованием не менее двух независимых факторов аутентификации, что существенно повышает уровень безопасности по сравнению с традиционными методами (например, простым паролем).

Задание:

1. Сформулируйте принципы строгой аутентификации.
2. Опишите типы процедур строгой аутентификации.

Ответ:

Тема 4. Защита электронного документооборота. УК-6.1 ПК-1.2.

Контрольные вопросы для проведения опроса:

1. Укажите особенности построения и функционирования системы распределенного электронного документооборота.
2. Назовите угрозы информационной безопасности для СЭД и охарактеризуйте источники этих угроз.
3. Какие функции должны быть реализованы средствами защиты информации СЭД?

Контрольные задания

1. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

С развитием локальных и глобальных сетей все шире используются системы электронного документооборота (СЭД). Такие системы существенно расширяют возможности как коммерческих компаний, так и государственных организаций.

Задание:

1. Укажите различия между понятиями «система электронного документооборота» (СЭД) и ECM (Enterprise Content Management).
2. Укажите преимущества электронного документооборота по сравнению с бумажным документооборотом.

Ответ:

2. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Корпоративная электронная почта — критически важный канал коммуникации, который требует комплексной защиты от утечек данных, мошенничества и кибератак.

Задание:

1. Охарактеризуйте методы и средства защиты корпоративного почтового документооборота.

Ответ:

Тема 5. Принципы комплексной защиты информации КИС. УК-6.1 ПК-1.2.

Контрольные вопросы для проведения опроса:

1. Сформулируйте основополагающие принципы построения современных КИС.
2. Охарактеризуйте четыре уровня управления КИС.
3. Укажите необходимые условия обеспечения санкционированного доступа к информационным ресурсам предприятия.
4. Какие важные системные функции может выполнять КИС при реализации в ней принципа централизованного управления?
5. Объясните значение управления рисками предприятия для создания системы эффективной защиты информации на этом предприятии.
6. Какие требования необходимо учитывать при разработке архитектуры КСЗИ?
7. Перечислите меры и средства защиты, применяемые при построении комплексной системы защиты информации КИС.
8. Укажите основные подсистемы информационной безопасности, входящие в состав КСЗИ.
9. Опишите особенности подсистемы защиты информации от несанкционированного доступа.
10. Опишите назначение и особенности подсистемы контроля эффективности защиты информации.
11. Опишите назначение и особенности подсистемы мониторинга и управления инцидентами ИБ.
12. Опишите назначение и особенности подсистемы обеспечения непрерывности функционирования средств защиты.

Контрольные задания

1. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Для обеспечения безопасности данных необходимо поддерживать три основные функции. Для реализации указанных функций используются

криптографические технологии шифрования и цифровой подписи, а также средства аутентификации.

Задание:

Опишите основные функции, обеспечивающие безопасность данных:

1. Защиту конфиденциальности передаваемых или хранимых в памяти данных.

2. Подтверждение целостности и подлинности данных.

3. Аутентификацию пользователей при входе в систему и установлении соединения.

Ответ:

Тема 6. Защита от вредоносных программ. Обнаружение и предотвращение вторжений. УК-6.1 ПК-1.2.

Контрольные вопросы для проведения опроса:

1. Что такое вредоносная программа? Охарактеризуйте основные типы вредоносных программ.
2. Укажите существенные отличия компьютерных вирусов от сетевых «червей». Опишите основные особенности «троянских» программ.
3. Опишите два основных подхода к обнаружению вредоносных программ.
4. Как выполняется сигнатурный анализ? Каковы его достоинства и недостатки?
5. Что представляют собой проактивные методы обнаружения?
6. Опишите принцип действия, достоинства и недостатки эвристических анализаторов.
7. Опишите принцип действия, достоинства и недостатки поведенческих блокираторов.
8. Назовите и опишите дополнительные модули антивирусных средств.
9. Каковы дополнительные меры и средства защиты от вредоносных программ, расширяющие возможности антивирусных программ?
10. Опишите меры и средства защиты от спама (нежелательной корреспонденции).

Каковы особенности реализации подсистемы защиты корпоративной информации от вредоносных программ и вирусов?

11. Сформулируйте понятия: обнаружение вторжений и предотвращение вторжений.
12. Укажите четыре признака системы IPS, отличающие ее от системы IDS.
13. Дайте определения понятий: сетевая система NIPS (network-based IPS) и хостовая система HIPS (host- based IPS).

14. Сформулируйте назначение и особенности применения специализированных средств - сканеров уязвимости (vulnerability assessment).

15. Какие методы анализа событий используются в процессе выявления вторжений?

16. В чем суть метода обнаружения аномального поведения?

17. В чем суть метода обнаружения злоупотреблений?

Контрольные задания

1. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

В современных антивирусных продуктах используются два основных подхода к обнаружению вредоносных программ: сигнатурный и проактивный/эвристический. Сигнатурные методы - точные методы обнаружения вирусов. Эвристические методы - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

Задание:

1. Опишите эвристический и сигнатурный методы обнаружения вредоносных программ.

2. Укажите и опишите преимущества и недостатки эвристических методов по сравнению с сигнатурным методом.

Ответ:

Тема 7. Межсетевое экранирование. Виртуальные защищенные сети VPN. УК-6.1 ПК-1.5.

Контрольные вопросы для проведения опроса:

1. Опишите функциональность средств предотвращения вторжений системного (хостового) уровня

2. HIPS (Host-based IPS).

3. Опишите функциональность средств предотвращения вторжений сетевого уровня NIPS (network- based IPS).

4. Сформулируйте подход к защите от распределенных атак типа «отказ в обслуживании» DDoS (Distributed Denial of Service).

5. Какими свойствами и функциями должна обладать современная IPS для успешного обнаружения и предотвращения вторжений?

6. Опишите структуру и функционирование подсистемы предотвращения вторжений в КИС.

7. Что такое виртуальные защищенные сети VPN (Virtual Private Network)?

8. Сформулируйте концепцию построения виртуальных защищенных

сетей VPN.

9. Объясните понятия «виртуальный защищенный туннель», «туннелирование» и «инкапсуляция».

10. Дайте развернутые определения таких устройств VPN, как VPN-клиент, VPN-сервер и VPN-шлюз безопасности.

11. Поясните особенности структуры и функционирования двух основных схем виртуальных защищенных каналов.

12. Каковы функции инициатора туннеля и терминатора туннеля?

13. Какие методы используют для обеспечения безопасности сетей VPN?

14. Опишите классификацию сетей VPN по рабочему уровню модели взаимодействия открытых систем

15. OSI (Open Systems Interconnection).

16. Каковы основные варианты архитектуры сетей VPN? Дайте пояснение для каждого из трех основных вариантов.

17. Укажите основные виды технической реализации VPN и дайте пояснения для каждого из них.

18. Какие российские компании выпускают VPN-продукты в настоящее время?

19. Опишите возможности и основные характеристики семейства VPN-продуктов CSP VPN 3.0 российской компании «С-Терра СиЭсПи».

Контрольные задания

1. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Для эффективного противодействия сетевым атакам и обеспечения возможности активного и безопасного использования в бизнесе открытых сетей активно применяются виртуальные защищенные сети VPN (Virtual Private Network).

Задание:

Какую основную цель преследует использование виртуальных защищенных сетей (VPN) для обеспечения безопасности защищенных данных?

Ответ:

Тема 8. Управление средствами обеспечения информационной безопасности. УК-6.1 ПК-1.5.

Контрольные вопросы для проведения опроса:

1. Назовите задачи системы управления информационной безопасностью КИС.

2. Как осуществляется управление учетными записями и правами доступа к рабочим станциям, серверам и другим активным устройствам КИС?

3. В чем суть концепции глобального управления безопасностью GSM (Global Security Management)?

4. Объясните понятия «глобальная и локальная политики безопасности».

5. Опишите функционирование системы управления информационной безопасностью GSM.

6. Как осуществляется защита ресурсов в системе управления информационной безопасностью GSM?

7. Как осуществляется управление средствами информационной безопасности масштаба предприятия в системе GSM?

8. Опишите централизованное управление безопасностью, реализованное в продуктах Застава.

9. Опишите возможности системы управления Cisco Security Manager и программно-аппаратного комплекса управления Cisco MARS.

10. Какие функции реализуют продукты IBM Tivoli для обеспечения информационной безопасности КИС?

11. Назовите основные продукты IBM Tivoli и опишите их возможности.

12. Какие задачи решает система управления безопасностью IBM Proventia Management SiteProtector?

Тема 9. Стандарты информационной безопасности. УК-6.1 ПК-1.5.

Контрольные вопросы для проведения опроса:

1. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.

2. Назовите основные международные стандарты информационной безопасности.

3. Дайте краткую характеристику международного стандарта ISO/IEC 17799:2000 (BS 7799-1:2000).

4. Каковы основные особенности германского стандарта BSI «Руководство по защите информационных технологий для базового уровня защищенности»?

5. Опишите содержание и укажите значение международного стандарта ISO 15408 «Общие критерии безопасности информационных технологий.

6. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.

7. Назовите стандарты информационной безопасности для Интернета.

8. Каковы назначение и особенности функционирования протокола SET (Security Electronics Transaction)?

9. Каковы назначение и функциональность протоколов SSL (Secure Socket Layer) и IPSec? В чем эти протоколы существенно различаются?

10. Каковы назначение и функциональность инфраструктуры управления открытыми ключами PKI?

11. Перечислите российские стандарты безопасности информационных технологий.

12. Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408? Назовите и охарактеризуйте три основные части этого стандарта.

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

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

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

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать обучающийся	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,15	15
КТ 2	100	0,14	14
КТ 3	100	0,15	15
Итого:	х	0,44	44

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 1-4.

Доклад:

Тематика докладов:

1. Основные понятия защиты информации и информационной безопасности
2. Анализ угроз информационной безопасности
3. Способы обеспечения безопасности информационных систем
4. Основные понятия политики безопасности
5. Структура политики безопасности организации
6. Разработка политики безопасности организации.
7. Основные понятия криптографической защиты информации
8. Симметричные криптосистемы шифрования
9. Асимметричные криптосистемы шифрования
10. Функции хэширования
11. Электронная цифровая подпись
12. Управление криптоключами
13. Инфраструктура управления открытыми ключами PKI.
14. Аутентификация, авторизация и администрирование действий пользователей
15. Методы аутентификации, использующие пароли
16. Строгая аутентификация
17. Биометрическая аутентификация пользователя
18. Управление доступом по схеме однократного входа с авторизацией Single Sign-On.
19. Концепция электронного документооборота
20. Особенности защиты электронного документооборота
21. Защита баз данных
22. Защита корпоративного почтового документооборота
23. Защита системы электронного документооборота DIRECTUM.

Методические рекомендации по подготовке доклада.

Подготовка доклада способствует формированию навыков исследовательской работы, расширяет познавательные интересы, приучает критически мыслить. При написании доклада по заданной теме составляется план, подбираются основные источники. В процессе работы с источниками, систематизируют полученные сведения, делают выводы и обобщения.

Подготовка доклада требует от обучающегося большой самостоятельности и серьезной интеллектуальной работы, которая принесет наибольшую пользу, если будет включать с себя следующие этапы: изучение наиболее важных научных работ по данной теме, перечень которых дает сам преподаватель; анализ изученного материала, выделение наиболее значимых для раскрытия темы фактов, мнений разных ученых и научных положений; обобщение и логическое построение материала доклада, например, в форме развернутого плана; написание текста доклада с соблюдением требований научного стиля.

Построение доклада включает три части: вступление, основную часть и заключение. Во вступлении указывается тема доклада, устанавливается логическая связь ее с другими темами или место рассматриваемой проблемы среди других проблем, дается краткий обзор источников, на материале которых раскрывается тема и т. п. Основная часть должна иметь четкое логическое построение, в ней должна быть раскрыта тема доклада. В заключении обычно подводятся итоги, формулируются выводы, подчеркивается значение рассмотренной проблемы и т. п.

Критерии оценивания доклада:

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и раскрытие темы	0-20	Детальное, последовательное описание всех этапов с конкретными примерами
Грамотность изложения	0-20	Соблюдены все правила грамматики, орфографии и пунктуации
Стилистика	0-20	Единый стиль изложения, точные формулировки, уместное использование терминов, лаконичность
Логика изложения	0-20	Чёткая последовательность изложения, логические связи между частями текста, аргументы подтверждают выводы
Оригинальность	0-20	Уникальный подход к теме, нестандартные решения, инновационные идеи, собственная позиция автора
Итого максимально:	100	

КТ – 2.

Тема 5.

Контрольное задание:

Методология проведения аудита информационной безопасности объекта

Актуальность. При построении систем информационной безопасности (ИБ) важное значение имеют процессы контроля адекватность мер и средств защиты, а также выявление уязвимостей в существующей информационной системе. Аудит ИБ позволяет провести такой контроль и выявить новые уязвимости.

Целью работы является систематизация основных сведений об этапах, теоретических и практических подходах к аудиту ИБ, классификации мероприятий аудита.

Определение аудита информационной безопасности

В настоящее время нет сложившегося определения аудита применяемого для анализа уровня ИБ. В различных источниках можно встретить различные определения. Приведем некоторые из них.

Аудит – форма независимого, нейтрального контроля какого-либо направления деятельности организации.

Аудит – совокупность специальных приемов (методов), используемых для обработки исходной информации для достижения поставленных целей.

Многообразные приемы аудита проверок обычно объединяют в четыре группы: определение реального состояния объектов, анализ, оценка, формирование технических предложений.

Аудит – систематический, независимый и документированный процесс получения записей, фиксирования фактов или другой соответствующей информации и их объективного оценивания с целью установления степени выполнения заданных требований.

Аудит информационных систем – проверка используемых компанией информационных систем, систем безопасности, систем связи с внешней средой, корпоративной сети на предмет их соответствия бизнес-процессам, протекающим в компании, а также соответствия международным стандартам, с последующей оценкой рисков сбоев в их функционировании.

Аудит информационной безопасности – системный процесс получения объективных качественных и количественных оценок о текущем состоянии ИБ компании в соответствии с определенными критериями и показателями без опасности.

Аудит, является наиболее общим и в максимальной степени отражающим процесс проведения аудита, а также гармонизирующем ISO 19011 – 2011, является следующее.

Цели и задачи аудита

Анализируя вышеуказанные определения можно сделать вывод, об общей и частных задачах аудита.

Общей задачей аудита является проверка и оценивание ИС на соответствие критериям, которые определяют требования к уровню ИБ.

Частными задачами аудита является:

- анализ рисков, связанных с возможностью реализации угроз безопасности;
- оценка текущего уровня защищенности;
- выявление уязвимостей в подсистеме защиты и «узких мест» системы;
- оценка соответствия системы и ее защиты существующим стандартам в области ИБ, а также политике безопасности;
- формирование рекомендаций по комплексу мер, направленных на повышение эффективности существующей системы защиты.

Цели аудита можно подразделить на:

- превентивные – направленные на превентивное выявление угроз и уязвимостей и предотвращение инцидентов ИБ;

- детектирующие – направленные на обнаружение новых или уточнение особенностей уже имеющихся угроз и уязвимостей системы защиты вовремя или после инцидентов ИБ;
- корректирующие – направленные на формирование комплекса мер повышения эффективности существующей системы защиты после инцидентов ИБ с учетом вновь выявленных угроз и уязвимостей.

В настоящее время аудит ИБ проводят по отношению к следующим объектам:

- организации;
- бизнес-процессы;
- системы управления (менеджмента);
- информационные системы;
- технические системы.

По форме аудит может быть:

- организационно-нормативным – когда анализируется организационные мероприятия обеспечения ИБ и нормативные акты в данной сфере;
- техническим – когда анализируется технические средства и способы обеспечения ИБ.

Аудит является наиболее общей формой оценки состояния ИБ объекта аудита. Аудит проводиться на соответствие любым требованиям, сформулированным как заинтересованными лицами, так и нормативными документами. Аудит может включать в себя проведение различных способов тестирования подсистем и процессов объекта аудита, анализ документации и других информационных источников, интервьюирование специалистов и т. д.

Этапы проведения аудита

Для решение этих этапов необходимо придумать организацию, которая осуществляет бизнес процесс и после этого можно приступить к аудиту придуманной организации.

При проведении аудита ИБ необходимо провести следующую последовательность мероприятий:

1 этап – подготовительный:

- выбор объекта аудита;
- выбор критериев и методов аудита;
- выбор средств и способов аудита;
- формирование команды аудиторов;
- определение объема и масштаба аудита, установление его сроков.

2 этап – основной:

- анализ состояния ИБ объекта аудита;
- регистрация, сбор и проверка статистических данных и результатов инструментальных измерений уязвимостей и угроз;
- оценка результатов проверки;
- формирование отчета о результатах проверки по отдельным элементам объекта аудита и различным аспектам ИБ.

3 этап – заключительный:

- составление итогового отчета;
- формирование рекомендаций по комплексу мер, направленных на повышение эффективности существующей системы защиты;
- разработка плана мероприятий по устранению уязвимостей и недостатков в обеспечении ИБ.

2.1.2. Рекомендации по оцениванию устных ответов обучающихся

5 баллов (отлично) - ставится, если обучающийся:

1) полно и аргументировано отвечает по содержанию вопроса;

2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике;

3) умеет достаточно глубоко и доказательно обосновать свои суждения и применяемый инструментарий для решения задания;

4 балла (хорошо) - ставится, если обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «5», но допускает 1-2 ошибки, которые сам же исправляет.

3 балла (удовлетворительно) - ставится, если обучающийся обнаруживает знание и понимание основных положений данного задания, но:

1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил;

2) не умеет достаточно глубоко и доказательно обосновать свои суждения и применяемый инструментарий для решения задания;

3) излагает материал непоследовательно и допускает ошибки.

1-2 баллов (неудовлетворительно) - ставится, если обучающийся обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает применяемый инструментарий для решения задания. Отмечаются такие недостатки в подготовке обучающегося, которые являются серьезным препятствием к успешному овладению последующим материалом.

Критерии оценивания контрольных заданий:

Диапазон баллов	Описание критерия
85-100	Обучающимся задание выполнено без ошибок и в полном объеме.
65-84	Обучающимся в целом задание выполнено, имеются отдельные неточности или недостаточно полные ответы, не содержащие ошибок.
55-64	Обучающимся допущены отдельные ошибки при выполнении задания
0-54	У обучающегося отсутствуют ответы на большинство вопросов задачи, задание не выполнено или выполнено не верно.

КТ – 3.

Тема 6-9.

Доклад:
Тематика докладов:

1. Классификация вредоносных программ
2. Основы работы антивирусных программ
3. Средства защиты от нежелательной корреспонденции
4. Защита корпоративной сети от воздействия вредоносных программ и вирусов
5. Обнаружение вторжений системой IPS
6. Предотвращение вторжений в КИС
7. Современные средства предотвращения вторжений.
8. Функции межсетевых экранов
9. Особенности функционирования межсетевых экранов Схемы сетевой защиты на базе межсетевых экранов
10. Концепция построения виртуальных защищенных сетей VPN -решения для построения защищенных сетей
12. Современные VPN-продукты.
13. Задачи управления информационной безопасностью
14. Архитектура управления информационной безопасностью КИС
15. Функционирование системы управления информационной безопасностью КИС
16. Обзор современных систем управления безопасностью.
17. Роль стандартов информационной безопасности
18. Международные стандарты информационной безопасности
19. Отечественные стандарты информационной безопасности.

Методические рекомендации по подготовке доклада.

Подготовка доклада способствует формированию навыков исследовательской работы, расширяет познавательные интересы, приучает критически мыслить. При написании доклада по заданной теме составляется план, подбираются основные источники. В процессе работы с источниками, систематизируют полученные сведения, делают выводы и обобщения.

Подготовка доклада требует от обучающегося большой самостоятельности и серьезной интеллектуальной работы, которая принесет наибольшую пользу, если будет включать с себя следующие этапы: изучение наиболее важных научных работ по данной теме, перечень которых дает сам преподаватель; анализ изученного материала, выделение наиболее значимых для раскрытия темы фактов, мнений разных ученых и научных положений; обобщение и логическое построение материала доклада, например, в форме

развернутого плана; написание текста доклада с соблюдением требований научного стиля.

Построение доклада включает три части: вступление, основную часть и заключение. Во вступлении указывается тема доклада, устанавливается логическая связь ее с другими темами или место рассматриваемой проблемы среди других проблем, дается краткий обзор источников, на материале которых раскрывается тема и т. п. Основная часть должна иметь четкое логическое построение, в ней должна быть раскрыта тема доклада. В заключении обычно подводятся итоги, формулируются выводы, подчеркивается значение рассмотренной проблемы и т. п.

Критерии оценивания доклада:

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и раскрытие темы	0-20	Детальное, последовательное описание всех этапов с конкретными примерами
Грамотность изложения	0-20	Соблюдены все правила грамматики, орфографии и пунктуации
Стилистика	0-20	Единый стиль изложения, точные формулировки, уместное использование терминов, лаконичность
Логика изложения	0-20	Чёткая последовательность изложения, логические связи между частями текста, аргументы подтверждают выводы
Оригинальность	0-20	Уникальный подход к теме, нестандартные решения, инновационные идеи, собственная позиция автора
Итого максимально:	100	

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

Для решения контрольных заданий обучающийся использует компьютер.

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

6.1. Промежуточная аттестация (экзамен) проводится в письменной форме. Обучающийся получает задания. Обучающийся получает чистые маркированные листы бумаги для записей. Необходимо дать ответ в письменном виде.

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к

промежуточной аттестации:

Тема 1. Основные понятия и анализ угроз информационной безопасности. Политики безопасности. УК-6.1 ПК-1.2.

1. Задание закрытого типа на установление последовательности

Прочитайте текст и установите последовательность.

Под политикой безопасности организации понимают совокупность управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Вообще политика безопасности определяется используемой компьютерной средой и отражает специфические потребности организации.

Расставьте по порядку действия при создании структуры многоуровневой политики безопасности:

1. Определение средних уровней политики.
2. Разработка специализированных политик безопасности.
3. Формирование высокоуровневой политики безопасности.
4. Создание процедур безопасности для каждой функциональной области.

Запишите соответствующую последовательность цифр слева направо:

Ответ:

2. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Инфраструктура открытых ключей PKI (Public Key Infrastructure) предназначена для надежного функционирования корпоративных информационных систем и позволяет как внутренним, так и внешним пользователям безопасно обмениваться информацией с помощью цепочки доверительных отношений.

Задание:

1. Опишите на чем основывается инфраструктура открытых ключей PKI.
2. Как вы могли бы применить эти знания в своей профессиональной практике?

Ответ:

Тема 2. Криптографическая защита информации. УК-6.1 ПК-1.2.

1. Задание закрытого типа на установление соответствия

Прочитайте текст и установите соответствие.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда проведен анализ рисков и определена стратегия защиты, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца (в соответствиях может быть несколько правильных ответов).

Установите соответствие между ролями сотрудников и их обязанностями в системе информационной безопасности:

Роль		Обязанность	
А.	Руководители подразделения	1.	Обеспечение комплексной работы систем и внедрение технических мер защиты
Б.	Администраторы ИС	2.	Ответственность за соблюдение службами общей политики безопасности
В.	Пользователи	3.	Соблюдение правил политической безопасности
Г.	Администраторы сервисов	4.	Доведение положений о политике безопасности для сотрудников и взаимодействии с ними
		5.	Информирование о подозрительных инцидентах

Запишите выбранные цифры под соответствующими буквами:

А.	Б.	В.	Г.

2. Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор.

Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Основой большинства криптографических средств защиты информации является шифрование данных.

Принципиальное отличие асимметричной криптосистемы от симметричной состоит в:

А. Использование одного и того же ключа для шифрования и расшифрования.

Б. Применение различных ключей для шифрования и расшифрования.

В. Использование секретного ключа для обмена информацией.

Г. Невозможности вычислить секретный ключ из открытого доступа.

Д. Требование одинаковых алгоритмов шифрования для второй стороны.

Ответ:

Обоснование выбора:

Тема 3. Идентификация, аутентификация и управление доступом. УК-6.1 ПК-1.2.

1. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора

Прочитайте текст, выберите один правильный ответ и запишите аргументы, обосновывающие выбор.

Главной целью мер, предпринимаемых на управленческом уровне, является формирование программы работ в области информационной безопасности и обеспечение ее выполнения путем выделения необходимых ресурсов и осуществления регулярного контроля состояния дел. Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать.

Каким образом политика безопасности организации помогает формулировать принципы профессионального и личностного развития сотрудников?

А. Она устанавливает, кто может получить доступ к каким данным и какие меры безопасности должны соблюдаться.

Б. Она представляет собой перечень карьерных возможностей и определяет зоны ответственности сотрудников.

В. Она описывает методы увеличения зарплаты в зависимости от вклада сотрудника.

Г. Она формулирует принципы корпоративной культуры, включая особенности поведения сотрудников на совещаниях.

Ответ:

Обоснование выбора:

2. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу.

Задание:

Как выстроить взаимодействие между подсистемой управления средствами защиты информации и подсистемой управления идентификацией и доступом для повышения эффективности управления информационной безопасностью?

Тема 4. Защита электронного документооборота. УК-6.1 ПК-1.2.

1. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора

Прочитайте текст, выберите один правильный ответ и запишите аргументы, обосновывающие выбор ответа.

Политика безопасности определяет стратегию управления в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую считает целесообразным выделить руководство.

Каким образом политика безопасности организации планирует решение задач по обеспечению защиты информации?

А. Через создание рабочего плана по обучению сотрудников новым технологиям.

Б. Через проведение анализа рисков и выделение ресурсов для реализации стратегии защиты.

В. Через сбор данных о производительности сотрудников и их вовлеченности в рабочие процессы.

Г. Через установление мотивационных премий за соблюдение политики безопасности.

Ответ:

Обоснование выбора:

2. Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор.

Риск информационной безопасности – это потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации.

Какие из следующих функций должна выполнять система управления рисками на предприятии для обеспечения информационной безопасности?

А. Идентификация различных типов угроз.

Б. Реализация средств защиты от повреждений физического оборудования.

В. Служба поддержки принятия решений для минимизации рисков.

Г. Ретроактивная уязвимость системы через внешних аудиторов.

Д. Автоматическое переконфигурирование межсетевых экранов при атаке.

Ответ:

Обоснование выбора:

Тема 5. Принципы комплексной защиты информации КИС. УК-6.1 ПК-1.2.

1. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора

Прочитайте текст, выберите один правильный ответ и запишите аргументы, обосновывающие выбор ответа.

На основе политики безопасности организации устанавливаются необходимые средства и процедуры безопасности, а также определяются роли и ответственность сотрудников организации в обеспечении безопасности.

Как планируется решение задач личностного развития сотрудников в рамках политики безопасности организации?

А. Через обучение сотрудников навыкам работы в сети и установки антивирусного ПО.

Б. Через делегирование полномочий каждому сотруднику для самостоятельного принятия решений.

В. Через предоставление персональных данных, необходимых для профессионального роста.

Г. Через определения ролей и обязанностей сотрудников, обеспечивающих безопасность ИС.

Ответ:

Обоснование выбора:

2. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

В современных антивирусных продуктах используются два основных подхода к обнаружению вредоносных программ: сигнатурный и проактивный/эвристический. Сигнатурные методы - точные методы обнаружения вирусов. Эвристические методы - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

Задание:

1. Опишите основные различия между статическим и динамическим эвристическим анализом.

2. Какие из них более эффективны в предотвращении ложных инициатив?

Ответ:

Тема 6. Защита от вредоносных программ. Обнаружение и предотвращение вторжений. УК-6.1 ПК-1.2.

1. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора

Прочитайте текст, выберите один правильный ответ и запишите аргументы, обосновывающие выбор.

Комплексный подход к построению системы защиты информации позволяет организовать целостную систему защиты от угроз.

Для обеспечения безопасности информационных ресурсов предприятия средства защиты информации размещаются:

А. В корпоративной сети, с активным межсетевым экраном и VPN.

Б. В локальной сети, с активным межсетевым экраном и антивирусным оборудованием.

В. В корпоративной сети с активным VPN.

Г. В локальной сети, с активной системой обнаружения и предотвращения вторжений IPS.

Ответ:

Обоснование выбора:

2. Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор.

Информационные системы повышенной сложности, такие, как корпоративные информационные системы (КИС), как правило, состоят из нескольких подсистем, решающих конкретные задачи. При построении КИС следует увязывать подсистемы в единый комплекс, придерживаясь ряда основополагающих принципов.

Какие принципы необходимо соблюдать при построении КИС?

А. Использование общепринятых стандартов.

Б. Применение программного обеспечения с высокой производительностью.

В. Принцип аппаратно-платформенной независимости.

Г. Применение конфиденциальных технологий.

Д. Принцип масштабируемости программного обеспечения.

Ответ:

Обоснование выбора:

Тема 7. Межсетевое экранирование. Виртуальные защищенные сети VPN. УК-6.1 ПК-1.5.

1. Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор.

При создании системы защиты корпоративной информации необходимо использовать принцип глубоко эшелонированной обороны от внешних и внутренних угроз.

На какие аспекты следует обратить внимание при создании комплексной системы защиты информации в КИС?

А. Система защиты должна быть многозвенной и масштабируемой.

Б. Меры безопасности должны применяться только на уровне серверов.

В. Система должна обеспечивать защиту на всех этапах жизненного цикла информации.

Г. Внедрение защиты должно быть выборочным, только для критических ресурсов.

Д. Интеграция систем защиты с операционными и прикладными системами обязательна.

Ответ:

Обоснование выбора:

2. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Для обеспечения безопасности информационных ресурсов предприятия средства защиты информации обычно размещаются непосредственно в корпоративной сети.

Задание:

Каковы уровни защиты от конкурентных программ, встроенных в корпоративную сеть, и каковы их особенности?

Ответ:

Тема 8. Управление средствами обеспечения информационной безопасности. УК-6.1 ПК-1.5.

1. Задание комбинированного типа с выбором одного верного ответа из предложенных и обоснованием выбора

Прочитайте текст, выберите один правильный ответ и запишите аргументы, обосновывающие выбор ответа.

Под политикой безопасности организации понимают совокупность управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Каким образом сотрудники могут совершенствовать свою познавательную деятельность, следуя политикам безопасности?

А. Путем увеличения времени на работу в сети.

Б. Путем соблюдения политик безопасности и выполнения инструкций по защите информации.

В. Путем повышения уровня доверия между коллегами.

Г. Путем выполнения стандартных процедур, не связанных с обеспечением безопасности.

Ответ:

Обоснование выбора:

2. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

Нижний уровень политики безопасности организации относится к конкретным сервисам. Эта политика включает в себя два аспекта - цели и правила их достижения Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать.

Задание:

1. Почему важно учитывать роль и обязанности сотрудников при изменении политики безопасности?

2. Как это влияет на эффективность защиты информации?

Ответ:

Тема 9. Стандарты информационной безопасности. УК-6.1 ПК-1.5.

1. Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор.

Информационные системы повышенной сложности, такие, как корпоративные информационные системы (КИС), как правило, состоят из нескольких подсистем, решающих конкретные задачи. При построении КИС следует увязывать подсистемы в единый комплекс.

Какие уровни управления могут быть выделены в корпоративной информационной системе (КИС)?

А. Управление конечными пользователями.

Б. Управление только сетевой инфраструктурой.

В. Централизованное управление всей системой предприятия.

Г. Управление только приложениями и серверами.

Д. Управление только пользователями.

Ответ:

Обоснование выбора:

2. Задание открытого типа с развернутым ответом

Прочитайте текст и запишите развернутый обоснованный ответ.

После проведения анализа рисков и определения стратегии защиты, составляется программа, реализация которой должна обеспечить информационную безопасность организации.

Задание:

1. Опишите этапы планирования внедрения программы информационной безопасности в организации.

2. Какие аспекты необходимо учитывать для эффективного выполнения плана?

Ответ:

6.3. Критерии и шкала оценивания на основе БРС.

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	90-100
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.	75-89
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.	60-74
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	1-59

поверхностны. Решение практических заданий не выполнено, т.е. обучающийся не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	

6.4. Для решения контрольных заданий обучающемуся разрешается использование компьютера.

7. Методические материалы по освоению дисциплины (модуля)

Подготовка к лекциям.

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин. Каждому обучающемуся следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Самостоятельная работа на лекции.

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лекции лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось просить их у однокурсников и тем самым не отвлекать их во время лекции. Целесообразно

разработать собственную «маркографию» (значки, символы), сокращения слов. Не лишним будет и изучение основ стенографии. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями.

Подготовка к практическим занятиям.

Подготовку к каждому практическому занятию каждый обучающийся должен начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (за компьютером). Все новые понятия по изучаемой теме необходимо выучить. Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы, правильном выполнении практических заданий и контрольных работ.

Структура практического занятия:

В зависимости от содержания и количества отведенного времени на изучение каждой темы может практическое занятие состоять из четырех-пяти частей:

1. Обсуждение теоретических вопросов, определенных программой дисциплины.
2. Доклад и/ или выступление с презентациями по проблеме практического занятия.
3. Обсуждение выступлений по теме – дискуссия.
4. Выполнение практического задания с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома, если это предусмотрено программой.
5. Подведение итогов занятия.

Первая часть – обсуждение теоретических вопросов - проводится в виде фронтальной беседы со всей группой и включает выборочную проверку преподавателем теоретических знаний обучающихся. Примерная продолжительность — до 15 минут. Вторая часть — выступление обучающихся с докладами, которые должны сопровождаться презентациями с целью усиления наглядности восприятия, по одному из вопросов практического занятия. Обязательный элемент доклада – представление и анализ статистических данных, обоснование социальных последствий любого экономического факта, явления или процесса. Примерная продолжительность — 20-25 минут. После докладов следует их обсуждение – дискуссия. В ходе этого этапа практического занятия могут быть заданы уточняющие вопросы к докладчикам. Примерная

продолжительность – до 15-20 минут. Если программой предусмотрено выполнение практического задания в рамках конкретной темы, то преподавателями определяется его содержание и дается время на его выполнение, а затем идет обсуждение результатов. Если практическое задание должно было быть выполнено дома, то на практическом занятии преподаватель проверяет его выполнение (устно или письменно). Примерная продолжительность – 15-20 минут. Подведением итогов заканчивается практическое занятие. Обучающимся должны быть объявлены оценки за работу и даны их четкие обоснования. Примерная продолжительность — 5 минут.

Работа с литературными источниками.

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на занятиях, выявить широкий спектр мнений по изучаемой проблеме.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Козьминых С.И. Обеспечение комплексной защиты объектов информатизации : учебное пособие для студентов вузов, обучающихся по направлению «Информационная безопасность», квалификация «магистр». - Москва : ЮНИТИ-ДАНА, 2020 г. - 543 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1359079

2. Галимов Р.Р. Основы разработки прикладных программ для защиты информации : учебное пособие. - Оренбург : Оренбургский государственный университет, 2023 г. - 164 с. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2164224

8.2. Дополнительная литература

1. Григорьев А.А. и др. Интегрированные информационные системы управления объектами. Корпоративные информационные системы : учебное пособие. - Москва : ИНФРА-М, 2024 г. - 273 с. - Текст : электронный.- URL:

https://znanium.ru/catalog/product/1911031

8.3. Нормативные правовые документы и иная правовая информация

Не используются

8.4. Интернет-ресурсы

1. Электронно-библиотечная система «ЗНАНИУМ» – URL: https://znanium.ru
2. Информационно-правовой портал ГАРАНТ.РУ. – URL: https://www.garant.ru/
3. Информационно-правовой портал «КонсультантПлюс». – URL: https://www.consultant.ru/about/
4. Научная электронная библиотека eLIBRARY.RU. – URL: https://elibrary.ru/
5. Научная электронная библиотека «КиберЛенинка». – URL: https://cyberleninka.ru
6. Электронно-библиотечная система «Лань». – URL: http://e.lanbook.com

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

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: - Libre Office (лицензия Mozilla Public License v2.0.) - 7-Zip (лицензия GNU Lesser General Public License) - AIMP (лицензия LGPL v.2.1) - STDU Viewer (freeware for private non-commercial or educational use) - GIMP (лицензия GNU General Public License) - Inkscape (лицензия GNU General Public License).

Для проведения учебных занятий, предусмотренных образовательной программой, закреплены аудитории согласно расписанию учебных занятий: рабочее место преподавателя, посадочные места по количеству обучающихся, доска меловая, персональный компьютер с лицензированным программным обеспечением общего назначения, мультимедийный проектор, экран, интерактивная панель.