Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Таныгин Максим Олегович
Должность: И.о. декана ФФиПИ
Дата подписания: 11.08.2026 08:15:12
Уникальный программный ключ:
9e5f67597080ec269645b995de68ced589046325

Аннотация к рабочей программе дисциплины «Защита информации»

1. Цель дисциплины

Целью дисциплины является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в системах искусственного интеллекта.

2. Задачи дисциплины

- изучение методов и инструментов защиты информации;
- формирование целостного представления об организации и содержании процессов управления информационной безопасностью;
- практическое применение изученных методов для реализации процессов управления информационной безопасностью в организации.

3. Индикаторы компетенций, формируемые в результате освоения дисциплины:

ПК-8.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях;

ПК-8.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях.

4. Разделы дисциплины

1. Понятие «информационная безопасность».
2. Сетевые и компьютерные угрозы.
3. Риски информационной безопасности.
4. Средства защиты информации.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета фундаментальной
и прикладной информатики
(наименование фото полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
«18» 02 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации
(наименование дисциплины)

ОПОП ВО 09.04.01Информатика и вычислительная техника
шифр и наименование направления подготовки (специальности)

программа «Киберфизические системы и искусственный интеллект»
направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта»
наименование направленности (профиля, специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника на основании учебного плана ОПОП ВО 09.04.01 Информатика и вычислительная техника, программа «Киберфизические системы и искусственный интеллект», направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта», одобренного Ученым советом университета (протокол № 5 от «27» декабря 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 09.04.01 Информатика и вычислительная техника, программа «Киберфизические системы и искусственный интеллект», направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта» на заседании кафедры вычислительной техники № 9 от «18» 02 2022 г.

Зав. кафедрой ВТ И.Е. Чернецкая
Разработчик программы
к.т.н., доцент О.О. Яночкина

Согласовано
Директор научной библиотеки В.Г. Макаровская

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.04.01 «Информатика и вычислительная техника», программа «Киберфизические системы и искусственный интеллект» направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта», одобренного Ученым советом университета, протокол № 9 «27» 02 2023 г., на заседании кафедры вычислительной техники протокол № 1 «30» 08 2024 г.

Зав. кафедрой ВТ И.Е. Чернецкая

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.04.01 «Информатика и вычислительная техника», программа «Киберфизические системы и искусственный интеллект» направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта», одобренного Ученым советом университета, протокол № 9 «27» 03 2024 г., на заседании кафедры вычислительной техники протокол № 1 «25» 08 2025 г.

Зав. кафедрой ВТ И.Е. Чернецкая

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.04.01 «Информатика и вычислительная техника», программа «Киберфизические системы и искусственный интеллект» направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта», одобренного Ученым советом университета, протокол № 9 «31» 03 2025 г., на заседании кафедры вычислительной техники протокол № 12 «02» 07 2026 г.

Зав. кафедрой ВТ И.Е. Чернецкая

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1. Цель дисциплины

Целью дисциплины является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в системах искусственного интеллекта

1.2. Задачи изучения дисциплины

- изучение методов и инструментов защиты информации;
- формирование целостного представления об организации и содержании процессов управления информационной безопасностью;
- практическое применение изученных методов для реализации процессов управления информационной безопасностью в организации.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-8	Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	ПК-8.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	***Знать:*** - новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ***Уметь:*** - разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях ***Владеть:*** - навыками планирования политик безопасности при разработке

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач
		ПК-8.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	***Знать:*** - особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ***Уметь:*** - модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях ***Владеть:*** - навыками планирования политик безопасности при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Защита информации» входит в часть, формируемую участниками образовательных отношений, основной профессиональной образовательной программы – программы магистратуры 09.04.01 Информатика и вычислительная техника, программа «Киберфизические системы и искусственный интеллект», направленность (профиль) «Облачная и сетевая инфраструктура систем искусственного интеллекта» в Модуль «Администрирование и Веб» Комплексного модуля профиля «Облачная и сетевая инфраструктура систем искусственного интеллекта». Дисциплина изучается в 4 семестре на 2 курсе

3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 4 зачетных единицы (з.е.) 144 часа.

Таблица 3 – Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	24,1
в том числе:	0
лекции	8
лабораторные занятия	12
практические занятия	12
Самостоятельная работа обучающихся (всего)	119,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего КоРа)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 - Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	**Понятие «информационная безопасность»**	Информационная безопасность (ИБ) в области искусственного интеллекта. Основные понятия. Основные стандарты в области обеспечения информационной безопасности систем искусственного интеллекта. Политика безопасности.
2	**Сетевые и компьютерные угрозы**	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.
3	**Риски информационной безопасности**	Методы анализа рисков. Понятие уязвимости. Классификация угроз. Методы оценки ущерба от реализации угроз информационной безопасности систем искусственного интеллекта
4	**Средства защиты информации**	Специализированные программно-аппаратные средства защиты информации для систем искусственного интеллекта. Основные направления применения криптографических технологий при защите систем искусственного интеллекта. Принципы организации и примеры систем обнаружения вторжений, мониторинга защищенности локальной и сетевой компьютерной среды

Таблица 4.1.2 – Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра)	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Понятие «информационная безопасность»	-	-	1,2	У1-У5, МУ1	ЗП (8)	ПК-8
2	Сетевые и компьютерные угрозы	-	-	3	У1-У5, МУ1	ЗП (11)	ПК-8
3	Риски информационной безопасности	-	1	-	У1-У5, МУ1	ЗП (4)	ПК-8
4	Средства защиты информации	-	2,3	-	У1-У5, МУ1	ЗП (11)	ПК-8

ЗП – защита практической работы, ЗЛ – защита лабораторной работы

4.2. Лабораторные работы и (или) практические занятия

4.2.1 – Практические занятия

Таблица 4.2.1 – Практические занятия

№	Наименование практического занятия	Объём, час.
1.	Информационная безопасность (ИБ) в области искусственного интеллекта.	4
2.	Основные стандарты в области обеспечения информационной безопасности систем искусственного интеллекта. Политика безопасности.	4
3.	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.	4
Итого		12

4.2.2 – Лабораторные занятия

Таблица 4.2.2 – Лабораторные занятия

№	Наименование практического занятия	Объём, час.
1.	Методы анализа рисков. Понятие уязвимости. Классификация угроз. Методы оценки ущерба от реализации угроз информационной безопасности систем искусственного интеллекта.	4
2.	Специализированные программно-аппаратные средства защиты информации для систем искусственного интеллекта. Основные направления применения криптографических технологий при защите систем искусственного интеллекта.	4
3.	Принципы организации и примеры систем обнаружения вторжений, мониторинга защищенности локальной и сетевой компьютерной среды	4
Итого		12

4.3. Самостоятельная работа студентов

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час
1	Понятие «информационная безопасность»	1-2	29,9
2	Сетевые и компьютерные угрозы	3-4	30
3	Риски информационной безопасности	5	30
4	Средства защиты информации	6-7	30
Итого			119,9

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;

– тем рефератов;

– вопросов к зачету;

–методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий.

№	Наименование	Интерактивные образовательные технологии	Объем в часах
1	Понятие «информационная безопасность»	Разбор конкретных ситуаций	2
2	Сетевые и компьютерные угрозы	Разбор конкретных ситуаций	2
3	Риски информационной безопасности	Разбор конкретных ситуаций	2
4	Средства защиты информации	Разбор конкретных ситуаций	2
		Всего	8

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения программы

Код и содержание дисциплины	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-8 Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	Технологии программирования и инструментальные средства разработки систем искусственного интеллекта, Технологии построения сетей нового поколения	Учебная технологическая (проектно-технологическая) практика	Производственная преддипломная практика, Мобильные и сетевые архитектуры комплексных систем искусственного интеллекта, Безопасность систем искусственного интеллекта, Отказоустойчивые и масштабируемые вычислительные системы, Методы и средства защиты облачной и сетевой инфраструктуры, Технологии широкополосной цифровой связи, Защита информации, Технологии беспроводной связи

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции / этап	Показатели оценивания компетенций *(индикаторы достижения компетенций,*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)

	закрепленные за дисциплиной)			
1	**2**	**3**	**4**	**5**
ПК-8 / завершающий	ПК-8.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	***Знать:*** - основные научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ***Уметь:*** - испытывая затруднения, разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях ***Владеть:*** элементарными навыками планирования политик безопасности при разработке программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач	***Знать:*** - достаточно хорошо новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ***Уметь:*** - недостаточно точно разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях ***Владеть:*** основными навыками планирования политик безопасности при разработке программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач	***Знать:*** - глубоко новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ***Уметь:*** - корректно разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях ***Владеть:*** развитыми навыками планирования политик безопасности при разработке программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач

	ПК-8.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	***Знать:*** - основные особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ***Уметь:*** - испытывая затруднения, модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях ***Владеть:*** - элементарными навыками планирования политик безопасности при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач	***Знать:*** - достаточно хорошо особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ***Уметь:*** - недостаточно точно модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях ***Владеть:*** - основными навыками планирования политик безопасности при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач	***Знать:*** - глубоко особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ***Уметь:*** - корректно модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях ***Владеть:*** - развитыми навыками планирования политик безопасности при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы

формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контро-лируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал
				наимено-вание	№№ заданий	
1	**2**	**3**	**4**	**5**	**6**	**7**
1	**Понятие «информационная безопасность»**	ПК-8	Прак.зан.	С	1-5	Согласно табл. п.7.4
2	**Сетевые и компьютерные угрозы**	ПК-8	Прак.зан.	С	1-5	Согласно табл. п.7.4
3	**Риски информационной безопасности**	ПК-8	Лабор. зан.	С	1-5	Согласно табл. п.7.4
4	**Средства защиты информации**	ПК-8	Лабор. зан.	С	1-5	Согласно табл. п.7.4

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования

Раздел (тема) дисциплины. Средства защиты информации

1. Какие основные принципы обеспечения ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
2. На какие направления можно декомпозировать задачу обеспечения ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
3. Каковы основные участники процесса обеспечения ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
4. Каковы основные стадии процесса обеспечения ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
5. Какие группы нормативной документации применяются при обеспечении ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде бланкового и компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

– закрытой (с выбором одного или нескольких правильных ответов),
– открытой (необходимо вписать правильный ответ),
– на установление правильной последовательности,
– на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения
промежуточной аттестации обучающихся

Задание в закрытой форме:

К какому уровню доступа к информации в автоматизированной системе относится перехват данных, передаваемых по каналам связи?

1. Уровень средств взаимодействия с носителем.
2. Уровень носителей информации.
3. Уровень представления информации.
4. Уровень содержания информации.

Задание в открытой форме:

Основные этапы построения системы защиты

Задание на установление правильной последовательности:

Расположить параметры для группировки данных на сервере сбора информации об атаке:

1. Дата, время
2. Протокол
3. Порт получателя
4. Номер агента
5. IP-адрес атакующего
6. Тип атаки

Задание на установление соответствия:

Установить соответствие названия протокола его назначению

	FTP	А	Протокол передачи данных
	SMTP	Б	Протокол передачи файлов
	TCP/IP	В	Протокол передачи гипертекста
	HTTP	Г	Протокол передачи почты

Компетентностно-ориентированная задача:

Установите сервер виртуальной частной сети (VPN).

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;
- методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для текущего контроля успеваемости по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	Балл	Примечание	Балл	Примечание
Практическое занятие №1	3	Выполнил без ошибок, но «не защитил»	6	Выполнил без ошибок и «защитил», полностью ответил на вопросы
Практическое занятие №2	3	Выполнил без ошибок, но «не защитил»	6	Выполнил без ошибок и «защитил», полностью ответил на вопросы
Практическое занятие №3	3	Выполнил без ошибок, но «не защитил»	6	Выполнил без ошибок и «защитил», полностью ответил на вопросы
Лабораторное занятие №1	3	Выполнил без ошибок, но «не защитил»	6	Выполнил без ошибок и «защитил», полностью ответил на вопросы
Лабораторное занятие №2	3	Выполнил без ошибок, но «не защитил»	6	Выполнил без ошибок и «защитил», полностью ответил на вопросы
Лабораторное занятие №3	3	Выполнил без ошибок, но «не защитил»	6	Выполнил без ошибок и «защитил», полностью ответил на вопросы
СРС	6	Материал усвоен на 50%	12	Материал усвоен более чем на 90%
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
ИТОГО	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, уме-ний, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Прохорова, О. В.Информационная безопасность и защита информации :учебник / О. В. Прохорова. - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. - URL: http://biblioclub.ru/index.php?page=book&id=438331(дата обращения 02.03.2022) . – Режим доступа : по подписке. - Текст : электронный.

2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2020. – 156 с. – URL: https://biblioclub.ru/index.php?page=book&id=612591 (дата обращения: 02.03.2022). – Режим доступа: по подписке. – Текст : электронный.

3. Информационная безопасность в цифровом обществе : учебное пособие / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=611084 (дата обращения: 02.03.2022). – Режим доступа: по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

4. Информационная безопасность и защита информации : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с. - ISBN 978-5-94178-2 16-1 : 386.25 р. - Текст : непосредственный.

5. Родичев, Ю. А.Безопасность инфокоммуникаций: стандартизация, измерения соответствия и подготовка кадров : учебное пособие для студентов вузов, обучающихся по специальности 10.05.02 - "Информационная безопасность телекоммуникационных систем", по направлениям подготовки 11.00.00 - "Электроника, радиотехника и системы связи" и 10.00.00 - "Информационная безопасность" / Ю. А. Родичев, Ю. А. Кубанков, П. И. Симонов ; под ред. Ю. А. Родичева. - Москва : Горячая линия - Телеком, 2018. - 160 с. : ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр.: с. 149-156 (58 назв.). - ISBN 978-5-9912-0706-5 : 386.59 р. - Текст : непосредственный.

8.3 Перечень методических указаний

1. Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем : методические указания по выполнению самостоятельной работы для студентов направления подготовки 10.04.01 / Юго-Зап. гос. ун-т ; сост. В. П. Добрица. - Курск : ЮЗГУ, 2018. - 19 с. - Текст : электронный.

8.4 Другие учебно-методические материалы

Для расширения знаний по дисциплине рекомендуется использовать журналы в библиотеке университета:

- Датчики и системы,
- Телекоммуникации,
- Системы управления и информационные технологии,
- Приборостроение,
- Микропроцессорная техника.

9 Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. http://www.biblioclub.ru – ЭБС «Университетская библиотека онлайн».
2. http://www.lib.swsu.ru – Электронная библиотека ЮЗГУ.

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Защита информации» являются лабораторные и практические занятия. Студент не имеет права пропускать занятия без уважительных причин.

Практические и лабораторные занятия посвящены выполнению заданий, которые служат для закрепления изученного материала, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.

По согласованию с преподавателем или по его заданию студенты могут готовить рефераты по отдельным темам дисциплины, выступать на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

В процессе обучения преподаватели используют активные формы работы со студентами: привлечение студентов к творческому процессу на занятиях, текущий контроль путем отработки студентами пропущенных занятий, участие в групповых и индивидуальных консультациях. Эти формы способствуют выработке у студентов умения работать с учебником и литературой.

Важное место в образовательном процессе занимает самостоятельная работа студентов. Она необходима как для подготовки к практическим занятиям, так и к собеседованиям. Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю. Основная цель самостоятельной работы студента - закрепить теоретические знания, полученные в процессе аудиторных занятий.

Качество учебной работы студентов оценивается по результатам выполнения практических заданий, собеседования, а также по результатам рефератов.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Операционная система Windows, браузер Google Chrome, Adobe Reader. Отчет оформляется в Open Office / Libre Office.

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудитория 300

1. Мультимедиа центр:

Ноутбук ASUS X50VL PMD – T2330/14”/1024 Mb/160 Gb/ сумка

Проектор in Focus IN24+ (39945,45)

2. Стойка для интерактивной доски Hitachi.
3. Интерактивная доска Hitachi EX-82: StazBourd с аксессуарами.

Аудитория 303 – компьютерный класс

ПЭВМ INTEL Gore i3-7100/H110M-R C/SI White Box LGA1151.mATX/8Gb/1TB/DVDRW/LCD 21.5’’/k+m/ – 10 шт.

Аудитория 301– компьютерный класс

Многопроцессорный вычислительный комплекс: 10 шт.

Процессор, монитор, жесткий диск, клавиатура, мышь, опер. память, корпус, матер. плата.

Аудитория 202– компьютерный класс

1. Стойка открытая
2. Рабочая станция Core 2 Duo 1863/2*DDR2 1024 Mb/2*HDD 200G/SVGA/DVD-RW/20’LCD*2/Secret Net – 10 шт.

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу

Номер изме-нения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	заменен ных	аннулиро ванных	новых			

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Волгоградский государственный технический университет»

Факультет электроники и вычислительной техники

УТВЕРЖДАЮ

Декан

_____ / Авдеюк О. А. /

ФИО

29.09.2021

МОДУЛЬ "АДМИНИСТРИРОВАНИЕ И ВЕБ"
Защита информации

рабочая программа дисциплины (модуля, практики)

Закреплена за кафедрой	**Электронно-вычислительные машины и системы**
Учебный план	Направление 09.04.01 Информатика и вычислительная техника Программа "Киберфизические системы и искусственный интеллект"
Профиль	**Облачная и сетевая инфраструктура систем искусственного интеллекта**
Квалификация	**Магистр**
Срок обучения	**2**
Форма обучения	**очная**
Виды контроля в семестрах:	зачеты 4

Семестр(Курс.Номер семестра на курсе)	4(2.2)		Итого	
	УП	ПП	УП	ПП
Практические	12	12	12	12
Лабораторные	12	12	12	12
Итого ауд.	24	24	24	24
Контактная работа	24,25	24,25	24,25	24,25
Сам. работа	119,75	119,75	119,75	119,75
Часы на контроль	0	0	0	0
Практическая подготовка	0	0	0	0
Итого трудоемкость в часах	144	144	0	0

ЛИСТ ОДОБРЕНИЯ И СОГЛАСОВАНИЯ РАБОЧЕЙ ПРОГРАММЫ

Разработчик(и) программы:

доцент Быков Дмитрий Владимирович ктн _____

Рецензент(ы):
(при наличии)
_____

Рабочая программа дисциплины (модуля, практики)
Защита информации

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 918)

составлена на основании учебного плана:

Направление 09.04.01 Информатика и вычислительная техника
Программа "Киберфизические системы и искусственный интеллект"

Профиль: Облачная и сетевая инфраструктура систем искусственного интеллекта

утвержденного учёным советом вуза от 29.09.2021 протокол № 2.

Рабочая программа одобрена на заседании кафедры
Электронно-вычислительные машины и системы

Протокол от 16 сентября 2021 г. № 2

Зав. кафедрой Андреев Андрей Евгеньевич _____

СОГЛАСОВАНО:

Председатель НМС _____/Авдеюк О.А./

Протокол заседания НМС от 27 сентября 2021 г. № 2

ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

№ п/п	Виды дополнений и изменений (или иная информация)	Дата и номер протокола заседания кафедры	Визирование актуализации РПД председателем НМС факультета
1.		Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры Электронно-вычислительные машины и системы Протокол от __ _____ 2022 г. № __ Зав. кафедрой Андреев Андрей Евгеньевич _____	Председатель НМС _____/_____/ Протокол заседания НМС от __ _____ 2022 г. №__
2.		Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры Электронно-вычислительные машины и системы Протокол от __ _____ 2023 г. № __ Зав. кафедрой Андреев Андрей Евгеньевич _____	Председатель НМС _____/_____/ Протокол заседания НМС от __ _____ 2023 г. №__
3.		Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры Электронно-вычислительные машины и системы Протокол от __ _____ 2024 г. № __ Зав. кафедрой Андреев Андрей Евгеньевич _____	Председатель НМС _____/_____/ Протокол заседания НМС от __ _____ 2024 г. №__

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ). ВИД, ТИП ПРАКТИКИ, СПОСОБ И ФОРМА (ФОРМЫ) ЕЕ ПРОВЕДЕНИЯ.

Изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в системах искусственного интеллекта

Основными задачами дисциплины являются:

- изучение методов и инструментов защиты информации;

- формирование целостного представления об организации и содержании процессов управления информационной безопасностью;

- практическое применение изученных методов для реализации процессов управления информационной безопасностью в организации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОП:	К.М.01.ДВ.01.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Администрирование операционных систем
2.1.2	Методы и средства защиты облачной и сетевой инфраструктуры
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная практика: Преддипломная практика
2.2.2	Выполнение и защита выпускной квалификационной работы
2.2.3	Отказоустойчивые и масштабируемые вычислительные системы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)

ПК-8: Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях

ПК-8.1: Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

Результаты обучения: ПК-8.1. З-1. Знает новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях
ПК-8.1. У-1. Умеет разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

ПК-8.2: Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

Результаты обучения: ПК-8.2. З-1. Знает особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях
ПК-8.2. У-1. Умеет модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Форма контроля
1	**Раздел 1. Обучение**			
1.1	Защита информации в системах искусственного интеллекта /Тема/	4	0	
1.1.1	Информационная безопасность (ИБ) в области искусственного интеллекта. Основные понятия. /Пр/	4	4	К, З
1.1.2	Основные стандарты в области обеспечения информационной безопасности систем искусственного интеллекта. Политика безопасности. /Пр/	4	4	К, З
1.1.3	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. /Пр/	4	4	К, З
1.1.4	Методы анализа рисков. Понятие уязвимости. Классификация угроз. Методы оценки ущерба от реализации угроз информационной безопасности систем искусственного интеллекта. /Лаб/	4	4	Ко, К
1.1.5	Специализированные программно-аппаратные средства защиты информации для систем искусственного интеллекта. Основные направления применения криптографических технологий при защите систем искусственного интеллекта. /Лаб/	4	4	Ко, К

1.1.6	Принципы организации и примеры систем обнаружения вторжений, мониторинга защищенности локальной и сетевой компьютерной среды /Лаб/	4	4	Ко, К
2	**Раздел 2. Самостоятельная работа студентов**			
2.1	в том числе /Тема/	4	0	
2.1.1	Подготовка к отчету лабораторных работ и практическим занятиям /Ср/	4	60	
2.1.2	Выполнение контрольной работы /Ср/	4	59,75	
3	**Раздел 3. Промежуточная аттестация**			
3.1	в том числе /Тема/	4	0	
3.1.1	/Зачет/ /Зачёт/	4	0	З
3.1.2	Контактная работа с ППС /КоРа/	4	0,25	З

Примечание. Формы контроля: Эк – экзамен, К- контрольная работа, Ко- контрольный опрос, Сз- семестровое задание, З-зачет, ОП- отчет по практике.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Оценочные средства планируемых результатов обучения представлены в виде фондов оценочных средств (ФОС), разработанных в соответствии с локальным нормативным актом университета. ФОС может быть представлен в Приложении к рабочей программе.

5.1 Контрольные вопросы и задания

ПК-8: Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях

ПК-8.1: Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

Студент должен знать новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Какие основные принципы обеспечения ИБ?
2. На какие направления можно декомпозировать задачу обеспечения ИБ?
3. Каковы основные участники процесса обеспечения ИБ при разработке программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
4. Каковы основные стадии процесса обеспечения ИБ при разработке программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
5. Какие группы нормативной документации применяются при обеспечении ИБ?

Студент должен уметь разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Приведите пример анализа угроз ИБ по методике ФСТЭК России
2. Опишите структуру карточек в Банке данных угроз ФСТЭК России
3. Поясните связь между уязвимостью и угрозой ИБ
4. Приведите пример связки техники и тактики, согласно методике моделирования угроз ФСТЭК России
5. Опишите основные категории нарушителей применяются при анализе угроз ИБ

ПК-8.2: Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

Студент должен знать особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Какие основные принципы обеспечения ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
2. На какие направления можно декомпозировать задачу обеспечения ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
3. Каковы основные участники процесса обеспечения ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
4. Каковы основные стадии процесса обеспечения ИБ при модернизации программного и аппаратного обеспечения

технологий и систем искусственного интеллекта?
5. Какие группы нормативной документации применяются при обеспечении ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?

Студент должен уметь модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

Вопросы, задания:
1. Опишите структура документа «Модели угроз и нарушителя безопасности»
2. Приведите пример определения актуальных нарушителей ИБ
3. Приведите пример определения актуальные угрозы ИБ
4. Приведите пример моделирования угроз влияют на требования по обеспечению ИБ
5. Опишите основные подходы по выбору средств защиты для нивелирования актуальных угроз ИБ

5.2 Темы письменных работ (контрольная работа)
На контрольную работу студенту выдается индивидуальное задание (по вариантам), заключающееся в разработке документа «Модель угроз и нарушителя безопасности».
Работа выполняется в письменной форме в течение 10 недель с момента выдачи задания. Контрольный срок сдачи – последний месяц семестра.

Примерное содержание контрольной работы
1. Титульный лист.
2. Формулировка варианта задания.
3. Основная часть, включающая:
1) Описание объекта защиты, для которого производится моделирование угроз.
2) Определение негативных последствий от реализации (возникновения) угроз безопасности информации.
3) Определение возможных объектов воздействия угроз безопасности информации.
4) Определение источников угроз безопасности информации.
5) Оценка способов реализации (возникновения) угроз безопасности информации.
6) Оценка актуальности угроз безопасности информации.

Правила оформления контрольной работы
- контрольная работа оформляется в редакторе MS Word / OpenOffice (*.doc, *.docx, *.odt);
- листы формата А4, ориентация книжная;
- поля: левое – 2 см, остальные – по 1 см;
- шрифт – Times New Roman;
- размер шрифта 14 pt;
- междустрочный интервал – 1,5;
- абзацный отступ – 1,25 см;
- нумерация страниц сквозная, номер на первой странице не ставится;
- в конце работы необходим список использованной литературы согласно ГОСТ Р 7.0.5 – 2008;
- объем работы зависит от степени раскрытия основных пунктов контрольной работы.

Примерный список вариантов контрольной работы:

1. Разработка модели угроз и нарушителя для системы фильтрации электронной почты
2. Разработка модели угроз и нарушителя для системы чат-бота
3. Разработка модели угроз и нарушителя для системы голосового помощника
4. Разработка модели угроз и нарушителя для поисковой системы
5.3 Показатели и критерии оценивания компетенций, шкалы оценивания
В рамках изучаемой дисциплины студент может демонстрировать следующие уровни овладения компетенциями.

Повышенный уровень: обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий. Оценка промежуточной аттестации (зачет): 90 баллов и более.

Базовый уровень: обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий. Оценка промежуточной аттестации (зачет): 76-89 баллов.

Пороговый уровень: обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне. Оценка промежуточной аттестации (зачет): 61-75 баллов.

Уровень ниже порогового: система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности.
Оценка промежуточной аттестации (зачет): ниже 61 балла, не зачтено.

В рамках данной дисциплины используются следующие критерии оценки знаний студентов.

90 баллов и более.
Обучающийся демонстрирует:
- систематизированные, глубокие и полные знания по всем разделам учебной дисциплины, а также по основным вопросам, выходящим за ее пределы;
- точное использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы;
- безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач;
- выраженную способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации;
- полное и глубокое усвоение основной, и дополнительной литературы, по изучаемой учебной дисциплине;
- умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин;
- творческую самостоятельную работу на учебных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

76-89 баллов.
Обучающийся демонстрирует:
- систематизированные, глубокие и полные знания по всем разделам учебной дисциплины;
- использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения;
- владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач;
- способность решать сложные проблемы в рамках учебной дисциплины;
- свободное владение типовыми решениями;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой по учебной дисциплине;
- умение ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку;
- активную самостоятельную работу на учебных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

61-75 баллов.
Обучающийся демонстрирует:
- достаточные знания в объеме рабочей программы по учебной дисциплине;
- использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать выводы без существенных ошибок;
- владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно применять типовые решения в рамках изучаемой дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой по дисциплине;
- умение ориентироваться в базовых теориях, концепциях и направлениях по дисциплине;
- работу на учебных занятиях под руководством преподавателя, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Не зачтено.
Обучающийся демонстрирует:
- фрагментарные знания в рамках изучаемой дисциплины; знания отдельных литературных источников, рекомендованных рабочей программой по учебной дисциплине;
- неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок;
- пассивность на занятиях или отказ от ответа, низкий уровень культуры исполнения заданий.

5.4. Вопросы промежуточной аттестации
1. Какие основные принципы обеспечения ИБ при разработке программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
2. На какие направления можно декомпозировать задачу обеспечения ИБ при разработке программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
3. Каковы основные участники процесса обеспечения ИБ при разработке программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
4. Каковы основные стадии процесса обеспечения ИБ при разработке программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
5. Какие группы нормативной документации применяются при обеспечении ИБ при разработке программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
6. Каков порядок анализа угроз ИБ по методике ФСТЭК России?

7. Какова структура карточек в Банке данных угроз ФСТЭК России?
8. Какова связь между уязвимостью и угрозой ИБ?
9. Как связаны техники и тактики, согласно методике моделирования угроз ФСТЭК России?
10. Какие основные категории нарушителей применяются при анализе угроз ИБ?
11. Какие основные принципы обеспечения ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
12. На какие направления можно декомпозировать задачу обеспечения ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
13. Каковы основные участники процесса обеспечения ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
14. Каковы основные стадии процесса обеспечения ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
15. Какие группы нормативной документации применяются при обеспечении ИБ при модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта?
16. Какова структура документа «Модели угроз и нарушителя безопасности»?
17. Как определяются актуальные нарушители ИБ?
18. Как определяются актуальные угрозы ИБ?
19. Как результаты моделирования угроз влияют на требования по обеспечению ИБ?
20. Каковы основные подходы по выбору средств защиты для нивелирования актуальных угроз ИБ?
5.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности
Промежуточная аттестация обучающихся ведется непрерывно и включает в себя текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине) и семестровую аттестацию (зачет) – оценивание окончательных результатов обучения по дисциплине.

По данной дисциплине, завершающейся зачетом, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 60 баллов. Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля и количества баллов, набранных на семестровой аттестации (зачете).

Система оценивания

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля можно отнести устный опрос, письменные задания, лабораторные работы, контрольные работы.

Контрольная работа
Контрольная работа представляет собой законченную работу, включающую в себя разработку документа «Модель угроз и нарушителя безопасности». Данная работа позволяет оценить умения учащихся решать практические задачи моделирования угроз, умения ориентироваться в информационном пространстве по данной тематике, оценить уровень сформированности аналитических навыков. Полностью выполненная контрольная работа оценивается в 30 баллов.

Лабораторная работа.
Лабораторная работа является формой контроля и средством применения и реализации полученных обучающимися знаний, умений и навыков в ходе выполнения учебно-практической задачи, связанной с получением значимого результата с помощью реальных средств деятельности. Рекомендуются для проведения в рамках тем (разделов), наиболее значимых в формировании компетенций. За каждое полностью выполненное лабораторное задание начисляется 10 баллов. В рамках данной дисциплины планируется 3 лабораторные работы. Темы лабораторных работ указаны в разделе “4. Структура и содержание дисциплины (модуля, практики)”.

Устный опрос, собеседование.
Устный опрос, собеседование являются формой оценки знаний и предполагают специальную беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной. Процедуры направлены на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Устный ответ или собеседование может практиковаться преподавателем для уточнения знаний на практических и лабораторных занятиях.

Устный опрос включает 1 вопрос из группы вопросов “5.1 Контрольные вопросы и задания”, собеседование может включать более 1-го вопроса того же списка. Ответ оценивается от 0 до 3 баллов следующим образом:
3 балла - полный, логически безупречный ответ;
2 балла - ответ в целом полный, но могут иметь место несущественные пробелы в знаниях; логика ответа правильная, но некоторые моменты в своих рассуждениях студент обосновать затрудняется;
1 балл - ответ частичный, содержит значительные изъяны; нарушений логики ответа нет, но имеется ряд логических переходов в рассуждениях, которые студент обосновать затрудняется.

Промежуточная аттестация. Зачет.
Промежуточная аттестация осуществляется в конце семестра и завершает изучение дисциплины. Промежуточная аттестация помогает оценить более крупные совокупности знаний, умений и навыков, в некоторых случаях – даже формирование определенных компетенций. В рамках данного предмета к форме промежуточного контроля относится зачет.

Зачет имеет цель оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач. Зачет проводится в устной форме. В ходе зачета студент готовит ответы на вопросы билета. Билет включает два вопроса из списка "5.4. Вопросы промежуточной аттестации", оцениваемых по 20 баллов. Дополнительные баллы, помимо баллов, полученных за контрольную и лабораторные работы, могут быть заработаны за правильные ответы в ходе опросов и собеседований.

Если суммарное число баллов набранных в семестре по результатам модулей и полученных на зачете
- от 61 до 100 , то ставится итоговая оценка "Зачтено",
- менее 61 балла, то ставится оценка "Не зачтено".
Если суммарное число баллов, набранных студентом не менее 60 баллов, то студент может согласиться с соответствующей итоговой оценкой без зачета.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)

6.1. Рекомендуемая литература

	Авторы, составители	Заглавие	Издательство, год.	Электронный адрес
Л.1	Лукьянов В. С., Черковский И. В., Скакунов А. В., Быков Д. В.	Модели компьютерных сетей с удостоверяющими центрами: монография	Волгоград: ВолгГТУ, 2009	
Л.2	Лукьянов В. С., Быков Д. В.	Методы обеспечения безопасности в сетях с публичными ключами: учеб. пособие	Волгоград: ВолгГТУ, 2015	
Л.3	Олифер В. Г., Олифер Н. А.	Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие для студ. вузов	СПб.: Питер, 2004	
Л.4	Шевченко В. П.	Вычислительные системы, сети и телекоммуникации: учебник	Москва: КноРус, 2021	https://www.book.ru/book/936930
Л.5	Нестеров С. А.	Основы информационной безопасности: учеб. пособие	Санкт-Петербург: Лань, 2018	
Л.6	Бизяев А. А., Куратов К. А.	Сети связи и системы коммутации: учебное пособие	Новосибирск: НГТУ, 2016	https://e.lanbook.com/book/118257
Л.7	Ли П., Райтман М. А.	Архитектура интернета вещей	Москва: ДМК Пресс, 2019	https://e.lanbook.com/reader/book/112923/#5

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Кутузов, О. И. Инфокоммуникационные системы и сети : учебник для вузов / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 244 с. — ISBN 978-5-8114-8051-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171410 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э2	Голиков, А. М. Тестирование и диагностика в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2016. — 436 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110274 (дата обращения: 19.09.2021). — Режим доступа: для авториз. пользователей.
Э3	Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 392 с. — ISBN 978-5-8114-8514-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176657 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э4	Журавлев, А. Е. Инфокоммуникационные системы. Программное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 376 с. — ISBN 978-5-8114-8515-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176658 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э5	Лукша, М. Kubernetes в действии / М. Лукша ; перевод с английского А. В. Логунов. — Москва : ДМК Пресс, 2019. — 672 с. — ISBN 978-5-97060-657-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131688 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э6	Кутузов, О. И. Инфокоммуникационные системы и сети : учебник для вузов / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 244 с. — ISBN 978-5-8114-8051-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171410 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э7	Федеральный портал «Российское образование» [Электронный ресурс] – Режим доступа: www.edu.ru
Э8	Национальный Открытый Университет «ИНТУИТ» [Электронный ресурс] – Режим доступа: www.intuit.ru
Э9	Документация по технической защите конфиденциальной информации [Электронный ресурс] – Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty

Э10	Защита информации в центрах обработки данных : учебно-методическое пособие / И. А. Ушаков, В. А. Десницкий, А. А. Чечулин, Т. Е. Захарова. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2019. — 44 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180094 (дата обращения: 10.09.2021). — Режим доступа: для авториз. пользователей.
Э11	Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. — 644 с. — ISBN 978-5-9729-0512-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148386 (дата обращения: 10.09.2021). — Режим доступа: для авториз. пользователей.
6.3 Перечень программного обеспечения	
6.3.1.1	OpenOffice, LibreOffice – офисные пакеты
6.3.1.2	Microsoft Visual Studio Community – среда разработки
6.3.1.3	Яндекс.Браузер - веб-браузер.
6.4 Перечень информационных справочных систем	
6.3.2.1	Библиотека (НТБ), http://library.vstu.ru/sci-nci
6.3.2.2	Электронная информационно-образовательная среда университета, http://eos2.vstu.ru
6.3.2.3	ЭБС "Лань", https://e.lanbook.com/
6.3.2.4	ЭБС "Book.ru", https://www.book.ru/
6.3.2.5	Электронная библиотека "Grebennikon", https://grebennikon.ru/
6.3.2.6	Библиографическая и реферативная база данных статей, опубликованных в научных изданиях “Scopus”,
6.3.2.7	https://www.scopus.com/
6.3.2.8	Российская научная электронная библиотека, интегрированная с РИНЦ “eLIBRARY.ru”, https://www.elibrary.ru/
6.3.2.9	Поисковая интернет-платформа, объединяющая реферативные базы данных публикаций в научных журналах и
6.3.2.10	патентов “Web of Science”, https://webofknowledge.com/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ) /ОБОРУДОВАНИЕ	
7.1	1. Лаборатория сетевых технологий / Мультимедийный класс для проведения занятий лекционного и семинарского
7.2	типа, лабораторных занятий
7.3	1) ПЭВМ Intel DualCore 2ГГц / 2Гб RAM / LCD 19" - 8 шт.; 2) экран EliteScreens; 3) проектор Acer 1200; 4) Коммутаторы CISCO
7.4	2. Учебная лаборатория / комьютерный класс
7.5	1) Ноутбуки HP Elitebook 8460p – 4 шт., 2) Ноутбуки HP EliteBook 8570p - 4 шт. 3) Ноутбук Lenovo ThinkPad T420 – 4 шт. 4) экран EliteScreens; 5) проектор Acer 1203;
7.6	6) доступ в Интернет и к наукометрическим базам данных
7.7	3. Аудитория для самостоятельной работы обучающихся./Учебная мебель, компьютерная техника с возможностью
7.8	подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду
7.9	университета (читальный зал информационно-библиотечного центра)

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)

Организация образовательного процесса по данной дисциплине регламентируется учебным планом и расписанием учебных занятий. При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет дисциплины (переаттестации ее части), если она была освоена в процессе предшествующего обучения. Перезачёт (переаттестации ее части) освобождает обучающегося от необходимости повторного освоения дисциплины (полностью или частично).

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены практическими занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в электронной информационной образовательной среде.

Практические занятия проводятся в целях рассмотрения основных вопросов курса и охватывают основные разделы дисциплины.

Основной формой проведения практических занятий является решение конкретных задач, аналогичные которым будут выполнять студенты на лабораторных работах.

Лабораторные работы предполагают выполнение и отчет заданий по темам, рассмотренным на практических занятиях. Каждому лабораторному занятию предшествует самостоятельная подготовка студента, включающая: ознакомление с содержанием лабораторной работы по методическим указаниям; проработку теоретической части по учебникам, рекомендованным в методических указаниях;

Самостоятельная работа студентов включает изучение законспектированного материала, дополнение его с учетом

рекомендованной по данной теме литературы, самостоятельную подготовку к лабораторным работам, самостоятельное выполнение и оформление заданий контрольной работы, аналогичных выполненным на занятиях.
В течении семестра для студентов проводятся групповые текущие консультации по учебной дисциплине.

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов
Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ), индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.
В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн), в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.
Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ (при необходимости).
Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств. Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания.
При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Учебно-методическое пособие :
Быков, Д.В. Защита информации: учебно-методическое пособие. Волгоград : ВолгГТУ, 2021