**Федеральное государственное бюджетное**

**образовательное учреждение высшего образования**

**«Астраханский государственный университет имени В.Н. Татищева»**

|  |  |  |
| --- | --- | --- |
| СОГЛАСОВАНО  Руководитель программы аспирантуры  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.М. Ажмухамедов  «\_\_\_» \_\_\_\_\_\_\_\_\_ 2023 г. |  | УТВЕРЖДАЮ  Заведующий кафедрой ИТиК  *(наименование)*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Н. Марьенков  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

|  |  |
| --- | --- |
|  |  |
| Составитель(-и) | **Демина Р.Ю; к.т.н., доцент кафедры ИТиК; Ажмухамедов И.М., профессор, д.т.н., профессор кафедры ИТиК;** |
| Группа научных специальностей | **2. 3. 6 Информационные технологии и телекоммуникации** |
| Научная специальность | **Методы и системы защиты информации, информационная безопасность** |
| Форма обучения | **очная** |
| Год приема  Срок освоения | **2023**  **3 года** |

Астрахань – 2023

**1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

**1.1. Целями освоения дисциплины** **(модуля)** «Применение современных технологий в обеспечении информационной безопасности» являются освоение дисциплинарных компетенций, связанных с раскрытием базовых и расширенных технологий обеспечения информационной безопасности сложных технических объектов и систем.

**1.2. Задачи освоения дисциплины (модуля):** «Применение современных технологий в обеспечении информационной безопасности»

- изучение основных положений, понятий и категорий, относящихся к базовым и расширенным технологиям обеспечения информационной безопасности;

- изучение отечественных и международных стандартов и спецификаций информационной безопасности, их классификация и выявление взаимосвязей;

- изучение требований, предъявляемых к процессам защиты информации в современных информационных системах;

- изучение типовых подходов и методов противодействия наиболее распространенным угрозам информационной безопасности;

- изучение принципов организации, комплексного подхода к выбору средств и технологий обеспечения информационной безопасности объектов защиты;

- формирование умений, связанных с осуществлением классификации угроз и объектов защиты, применением концептуальных основ технической защиты информации, обеспечением требований и рекомендации по защите информации, обрабатываемой средствами вычислительной техники, созданию средств безопасности, отвечающим требованиям к архитектуре, казанных в соответствующих стандартах.

**2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Освоение дисциплины (модуля) «Применение современных технологий в обеспечении информационной безопасности» направлено на достижение следующих результатов, определенных программой подготовки научных и научно-педагогическим кадров в аспирантуре:

- самостоятельно осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты;

- разрабатывать методы и алгоритмы информационной безопасности компьютерных систем, организовать их тестирование и отладку;

- анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества.

**3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Общая трудоемкость дисциплины составляет – 4 зачетные единицы, 144 академических часов. На контактную работу обучающихся с преподавателем (по видам учебных занятий) – 28 часов и на самостоятельную работу обучающихся – 116 часов.

**Таблица 1.**

**Структура и содержание дисциплины (модуля)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Наименование радела (темы) | Семестр | Неделя семестра | Контактная работа  (в часах) | | | Самостоят. работа | Формы текущего контроля успеваемости *(по неделям семестра)*  Форма промежуточной аттестации *(по семестрам)* |
| Л | ПЗ | ЛР |
|  | Введение в экспертные информационные системы | 4 | 1-2 | 4 | 4 |  | 29 | Устный опрос |
|  | Концептуальные основы технической защиты информации. | 4 | 3-4 | 4 | 4 |  | 29 | Устный опрос |
|  | Архитектурные стандарты информационной безопасности. | 4 | 5-6 | 4 | 4 |  | 29 | Устный опрос. |
|  | Технические спецификации информационной безопасности. | 4 | 7 | 2 | 2 |  | 29 | Устный опрос. Итоговое тестирование |
| **ИТОГО** | |  |  | **14** | **14** |  | **116** | **ДИФФЕРЕНЦИРОВАННЫЙ ЗАЧЕТ** |

Условные обозначения:

Л – занятия лекционного типа; ПЗ – практические занятия, ЛР – лабораторные работы;

СР – самостоятельная работа по отдельным темам.

**Содержание дисциплины**

**Введение в экспертные информационные системы**

Понятие экспертной системы. Основные особенности, архитектура и классификация ЭС. Этапы разработки и стадии жизненного цикла ЭС. Введение в экспертные информационные системы в комплексном анализе информационной безопасности автоматизированных систем.

**Концептуальные основы технической защиты информации.**

Базовые технологии защиты информации. Классификация угроз и объектов защиты. Методы оценки опасности угроз. Объект информатизации. Классификация объектов защиты. Классификация информации. Классификация АС. Классификация СВТ. Угрозы несанкционированного доступа к информации.

Основные классы атак в сетях на базе TCP/IP. Понятие несанкционированного доступа.

Модель потенциального нарушителя. Основные классы атак в сетях на основе TCP/IP. Программно-математическое воздействие. Вредоносные программы и их классификация.

Антивирусы. Межсетевой экран. Система обнаружения вторжений.

Базовые и расширенные требования и рекомендации по защите информации. Классификация технических каналов утечки информации. Система документов по технической защите информации. Концептуальные основы защиты информации.

Органы по технической защите информации в РФ. Государственные органы в области защиты информации. ФСТЭК России. Лицензирование деятельности в области ТЗИ. Сертификация средств защиты информации. Общий порядок сертификации средств защиты информации. Порядок сертификации во ФСТЭК России

**Архитектурные стандарты информационной безопасности.**

«Общие критерии». Основные понятия и идеи "Общих критериев". Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий". Классификация функциональных требований безопасности. Классы функциональных требований, описывающие производные сервисы безопасности/

Профили защиты, разработанные на основе "Общих критериев". Общие угрозы безопасности. Общие элементы политики и цели безопасности. Общие функциональные требования. Общие требования доверия безопасности. Биометрическая идентификация и аутентификация. Требования к произвольному (дискреционному) управлению доступом. Требования к принудительному (мандатному) управлению доступом. Ролевое управление доступом. Межсетевое экранирование. Системы активного аудита. Выпуск и управление сертификатами. Анализ защищенности. Операционные системы. Системы управления базами данных. Виртуальные частные сети. Виртуальные локальные сети. Обзор стандарта BS 7799. Регуляторы безопасности и реализуемые ими цели. Регуляторы общего характера. Регуляторы технического характера. Регуляторы безопасности и реализуемые ими цели. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия. Четырехфазная модель процесса управления информационной безопасностью.

FIPS 140-2 «Требования безопасности для криптографических модулей». Основные понятия и идеи стандарта FIPS 140-2 Требования безопасности. Спецификация, порты и интерфейсы, роли, сервисы и аутентификация. Модель в виде конечного автомата, физическая безопасность. Эксплуатационное окружение, управление криптографическими ключами. Самотестирование, доверие проектированию, сдерживание прочих атак, другие рекомендации.

**Технические спецификации информационной безопасности.**

Искусственный интеллект в экспертных системах. Архитектура средств безопасности IP-уровня. Контексты безопасности и управление ключами. Протокольные контексты и политика безопасности. Обеспечение аутентичности IP-пакетов. Обеспечение конфиденциальности сетевого трафика. Основные идеи и понятия протокола TLS. Протокол передачи записей. Протокол установления соединений и ассоциированные протоколы. Применение протокола HTTP над TLS.

**4. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ   
ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ**

**4.1. Указания по организации и проведению лекционных, практических (семинарских) и лабораторных занятий с перечнем учебно-методического обеспечения**

Обучающемся проводится лекция с коллективным исследованием. По ходу излагаемого материала обучающимся предлагается совместно вывести то или иное правило, комплекс требований, определить закономерность на основе имеющихся знаний. Подводя итог рассуждениям, предложениям аспирантов, преподаватель дает правильное решение путем постановки необходимого вопроса.

Цель семинарских и практических занятий углубить и закрепить соответствующие знания аспирантов по предмету, но и развить инициативу, творческую активность, вооружить будущего специалиста методами и средствами научного познания. С точки зрения методики проведения семинар представляет собой комбинированную, интегративную форму учебного занятия. Он предполагает возможность использования рефератов.

**4.2. Указания для обучающихся по освоению дисциплины (модулю)**

**Таблица 2.**

**Содержание самостоятельной работы обучающихся**

|  |  |  |  |
| --- | --- | --- | --- |
| Номер радела (темы) | Темы/вопросы, выносимые на самостоятельное изучение | Кол-во  часов | Формы работы |
| Введение в экспертные информационные системы | Специфика информационных технологий, используемых в правовой сфере. | 29 | Внеаудиторная,  изучение учебных пособий |
| Концептуальные основы технической защиты информации. | Законодательные и иные правовые акты в области технической защиты информации. | 29 | Внеаудиторная,  изучение учебных пособий |
| Архитектурные стандарты информационной безопасности. | Общие принципы выработки официальной политики предприятия в области информационной безопасности. | 29 | Внеаудиторная,  изучение учебных пособий |
| Технические спецификации информационной безопасности. | Подход к выработке процедур для предупреждения нарушений безопасности. | 29 | Внеаудиторная,  изучение учебных пособий |

**4.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно** – не предусмотрено .

**5. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

**5.1. Образовательные технологии**

В рамках изучения дисциплины «Применение современных технологий в обеспечении информационной безопасности» предусмотрено использование в учебном процессе следующих активных и интерактивных форм проведения занятий:

| Название образовательной технологии | Темы, разделы дисциплины | Краткое описание применяемой технологии |
| --- | --- | --- |
| Анализ проблемных ситуаций | По всем темам | Анализ проблемных ситуаций, выбор наиболее рациональных математических методов и моделей для обеспечения информационно-аналитической поддержки соответствующих решений, запись математических моделей на бумаге или в электронной форме, определение целесообразных численных методов для реализации разработанных математических моделей |
| Проведение сеансов видеоконференцсвязи | По всем темам | Использования сеансов видеоконференцсвязи для оперативного обсуждения с аспирантами вопросов, относящихся к теме курса |
| Изучение «свежих» статей, публикуемых в научных журналах университета | По всем темам | Используются свежие статьи, опубликованные в журналах Астраханского государственного университета (с целью анализа содержащейся в них информации, изучения новых методов и подходов к анализу данных) |
| Подготовка научных публикаций | По всем темам | С помощью преподавателя подготавливаются тексты научных публикаций, связанные с темой кандидатской диссертации |
| Решение практических задач расчетного характера с использованием штатных средств электронных таблиц и разработки программ для ЭВМ | По всем темам | Используются индивидуализированные постановки задач для решения на аудиторных занятиях |

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line и/или off-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др)

**5.2. Информационные технологии**

Информационные технологии, используемые при реализации различных видов учебной и внеучебной работы:

- использование возможностей Интернета в учебном процессе (использование информационного сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление учащихся с оценками и т.д.));

- использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источников информации;

- использование возможностей электронной почты преподавателя;

- использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т.д.);

- использование интерактивных средств взаимодействия участников образовательного процесса (технологии дистанционного или открытого обучения в глобальной сети (веб-конференции, форумы, учебно-методические материалы и др.));

- использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс)

- использование виртуальной обучающей среды (или системы управления обучением LМS Moodle) или иных информационных систем, сервисов и мессенджеров.

|  |  |  |
| --- | --- | --- |
| Название информационной технологии | Темы, разделы дисциплины | Краткое описание  применяемой технологии |
| Использование возможностей Интернета в учебном процессе | По всем темам | Проведение входного, текущего и рейтингового контроля знаний учащихся (в системах электронного обучения) |
| Использование средств представления учебной информации | По всем темам | Использование мультимедийной презентации |

**5.3. Перечень программного обеспечения и информационных справочных систем**

***Лицензионное программное обеспечение***

|  |  |
| --- | --- |
| Наименование программного обеспечения | Назначение |
| Adobe Reader | Программа для просмотра электронных документов |
| Mozilla FireFox | Браузер |
| Microsoft Office 2013,  Microsoft Office Project 2013, Microsoft Office Visio 2013 | Пакет офисных программ |
| 7-zip | Архиватор |
| Microsoft Windows 7 Professional | Операционная система |
| Kaspersky Endpoint Security | Средство антивирусной защиты |
| Платформа дистанционного обучения LМS Moodle | Виртуальная обучающая среда |

***Современные профессиональные базы данных, информационные справочные системы***

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: [https://library.asu.edu.ru](https://library.asu.edu.ru/).
2. Электронный каталог «Научные журналы АГУ»: <http://journal.asu.edu.ru/>.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: <http://dlib.eastview.com/>
4. Электронно-библиотечная система elibrary. <http://elibrary.ru>
5. Корпоративный проект Ассоциации региональных библиотечных консорциумов (АРБИКОН) «Межрегиональная аналитическая роспись статей» (МАРС) [http://mars.arbicon.ru](http://mars.arbicon.ru/)
6. Электронные версии периодических изданий, размещенные на сайте информационных ресурсов [www.polpred.com](http://www.polpred.com)
7. Справочная правовая система КонсультантПлюс: [http://www.consultant.ru](http://www.consultant.ru/)
8. Информационно-правовое обеспечение «Система ГАРАНТ»: [http://garant-astrakhan.ru](http://garant-astrakhan.ru/)

***Перечень международных реферативных баз данных научных изданий*** – не используются.

**6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ   
И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

**6.1. Паспорт фонда оценочных средств**

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Применение современных технологий в обеспечении информационной безопасности» проверяется сформированность у обучающихся планируемых результатов обучения,указанных в разделе 2 настоящей программы*.*

**Таблица 3.**

**Соответствие разделов, тем дисциплины (модуля),**

**результатов обучения по дисциплине (модулю) и оценочных средств**

|  |  |  |
| --- | --- | --- |
| № п/п | Контролируемые разделы (этапы) | Наименование  оценочного средства |
| 1 | Введение в экспертные информационные системы | Вопросы для обсуждения |
| 2 | Концептуальные основы технической защиты информации. | Вопросы для обсуждения |
| 3 | Архитектурные стандарты информационной безопасности. | Вопросы для обсуждения |
| 4 | Технические спецификации информационной безопасности. | Вопросы для обсуждения. Итоговый тест. Вопросы к зачету |

**6.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания**

**Таблица 4**

**Показатели оценивания результатов обучения**

|  |  |
| --- | --- |
| Шкала оценивания | Критерии оценивания |
| 5  «отлично» | демонстрирует глубокое знание теоретического материала при выполнении заданий; последовательно и правильно выполняет задания;  обоснованно излагает свои мысли и делает необходимые выводы;  правильно и аргументированно отвечает на вопросы, приводит примеры. |
| 4  «хорошо» | демонстрирует знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания;  обоснованно излагает свои мысли и делает необходимые выводы;  допускает единичные ошибки, исправляемые после замечания преподавателя. |
| 3  «удовлетворительно» | демонстрирует отдельные, несистематизированные знания, не способен применить знание теоретического материала при выполнении заданий; испытывает затруднения и допускает ошибки при выполнении заданий; выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов. |
| 2  «неудовлетворительно» | демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры |

**6.3. Контрольные задания или иные материалы, необходимые для оценки результатов обучения**

**Введение в экспертные информационные системы**

***1. Вопросы для обсуждения***

1. Понятие экспертной системы.
2. Основные особенности, архитектура и классификация ЭС.
3. Этапы разработки и стадии жизненного цикла ЭС.
4. Введение в экспертные информационные системы в комплексном анализе информационной безопасности автоматизированных систем.

**Концептуальные основы технической защиты информации.**

***1. Вопросы для обсуждения***

1. Базовые технологии защиты информации. Классификация угроз и объектов защиты.
2. Методы оценки опасности угроз. Объект информатизации. Классификация объектов защиты.
3. Классификация информации. Классификация АС.
4. Классификация СВТ. Угрозы несанкционированного доступа к информации.
5. Основные классы атак в сетях на базе TCP/IP. Понятие несанкционированного доступа.
6. Модель потенциального нарушителя. Основные классы атак в сетях на основе TCP/IP. Программно-математическое воздействие. Вредоносные программы и их классификация.
7. Антивирусы. Межсетевой экран. Система обнаружения вторжений.
8. Базовые и расширенные требования и рекомендации по защите информации.
9. Классификация технических каналов утечки информации.
10. Система документов по технической защите информации.
11. Концептуальные основы защиты информации.
12. Органы по технической защите информации в РФ. Государственные органы в области защиты информации.
13. ФСТЭК России. Лицензирование деятельности в области ТЗИ.
14. Сертификация средств защиты информации. Общий порядок сертификации средств защиты информации. Порядок сертификации во ФСТЭК России

**Архитектурные стандарты информационной безопасности.**

***1. Вопросы для обсуждения***

1. «Общие критерии». Основные понятия и идеи "Общих критериев".
2. Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий".
3. Классификация функциональных требований безопасности. Классы функциональных требований, описывающие производные сервисы безопасности.
4. Профили защиты, разработанные на основе "Общих критериев". Общие угрозы безопасности.
5. Общие элементы политики и цели безопасности. Общие функциональные требования.
6. Общие требования доверия безопасности. Биометрическая идентификация и аутентификация.
7. Требования к произвольному (дискреционному) управлению доступом. Требования к принудительному (мандатному) управлению доступом. Ролевое управление доступом.
8. Межсетевое экранирование.
9. Системы активного аудита. Выпуск и управление сертификатами. Анализ защищенности.
10. Операционные системы. Системы управления базами данных. Виртуальные частные сети. Виртуальные локальные сети.
11. Обзор стандарта BS 7799. Регуляторы безопасности и реализуемые ими цели. Регуляторы общего характера. Регуляторы технического характера. Регуляторы безопасности и реализуемые ими цели. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия. Четырехфазная модель процесса управления информационной безопасностью.
12. FIPS 140-2 «Требования безопасности для криптографических модулей». Основные понятия и идеи стандарта FIPS 140-2 Требования безопасности. Спецификация, порты и интерфейсы, роли, сервисы и аутентификация.
13. Модель в виде конечного автомата, физическая безопасность. Эксплуатационное окружение, управление криптографическими ключами. Самотестирование, доверие проектированию, сдерживание прочих атак, другие рекомендации.

**Технические спецификации информационной безопасности.**

***1. Вопросы для обсуждения***

1. Искусственный интеллект в экспертных системах.
2. Архитектура средств безопасности IP-уровня.
3. Контексты безопасности и управление ключами.
4. Протокольные контексты и политика безопасности.
5. Обеспечение аутентичности IP-пакетов.
6. Обеспечение конфиденциальности сетевого трафика.
7. Основные идеи и понятия протокола TLS.
8. Протокол передачи записей.
9. Протокол установления соединений и ассоциированные протоколы. Применение протокола HTTP над TLS.

***2. Итоговый тест***

***Примерные вопросы***

1. Аспекты ИБ в соответствии со стандартом BS 7799.

2. Основные отличительные черты «Общих критериев».

3. Какие шаги рекомендуется проделать для определения последствий нарушения безопасности?

4. Какой ТКУИ обладает следующими особенностями: высокая достоверность добываемой информации, большой объем добываемой информации, оперативность получения информации, скрытность перехвата сигнала?

а) Радиоэлектронные каналы утечки информации;

б) Оптические каналы утечки информации;

в) Акустические канала утечки информации;

г) Материально-вещественные каналы утечки информации.

5. Структура канала утечки информации:

а) источник сигнала

б) среда распространения

в) приемник сигнала

г) ПЭМИН

д) человек

е) скорость распространения.

6. Принципы проектирования систем технической защиты.

7. Основными источниками угроз информационной безопасности являются:

а. Хищение жестких дисков, подключение к сети, инсайдерство

б. Перехват данных, хищение данных, изменение архитектуры системы

в. Хищение данных, подкуп системных администраторов, нарушение регламента работы

8. Основными рисками информационной безопасности являются:

а. Искажение, уменьшение объема, перекодировка информации

б. Техническое вмешательство, выведение из строя оборудования сети

в. Потеря, искажение, утечка информации

9. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации:

а. Источник информации

б. Потребитель информации

в. Уничтожитель информации

г. Носитель информации

д. Обладатель информации

10. Возможность получения информации и ее использования это:

а. Сохранение информации

б. Распространение информации

в. Предоставление информации

г. Конфиденциальность информации

д. Доступ к информации

**Вопросы для зачета:**

1. Введение в экспертные информационные системы в комплексном анализе информационной безопасности автоматизированных систем.
2. Концептуальные основы технической защиты информации.
3. Базовые технологии защиты информации.
4. Классификация угроз и объектов защиты.
5. Базовые и расширенные требования и рекомендации по защите информации.
6. Классификация технических каналов утечки информации.
7. Архитектурные стандарты информационной безопасности.
8. Стандарт «Общие критерии». Профили защиты, разработанные на их основе.
9. Стандарт BS7799.
10. FIPS 140-2 «Требования безопасности для криптографических модулей».
11. Технические спецификации информационной безопасности.
12. Искусственный интеллект в экспертных системах.

**6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности**

Оценивание аспирантов осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Зачет основан на итоговой оценке, включающий в себя следующее: суммы баллов по результатам текущего контроля (устные опросы, контрольные задания, комплексное задание творческого (проблемного) характера; результаты работы на занятиях в процессе обучения (инициативность, качество выполнения текущих заданий и пр.); результаты итогового тестирования; количества пропусков занятий; публикационная активность по теме учебного курса.

Преподаватель, реализующий дисциплину, в зависимости от уровня подготовленности, обучающихся может использовать иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

**7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ   
ДИСЦИПЛИНЫ (МОДУЛЯ)**

**а) Основная литература:**

1. Маглинец, Ю. А. Анализ требований к автоматизированным информационным системам : учебное пособие / Ю. А. Маглинец. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 191 c. — ISBN 978-5-4497-0301-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/89417.html>
2. Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин. - Москва : ДМК Пресс, 2017. Режим доступа: <https://www.studentlibrary.ru/book/ISBN9785970604397.html>
3. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 267 c. — ISBN 978-5-9515-0426-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/101929.html

**б) Дополнительная литература**

1. Барский, А. Б. Искусственный интеллект и логические нейронные сети : учебное пособие / А. Б. Барский. — Санкт-Петербург : Интермедия, 2019. — 360 c. — ISBN 978-5-4383-0155-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/95270.html (дата обращения: 21.12.2022). — Режим доступа: для авторизир. Пользователей
2. Долженко, А. И. Управление информационными системами : учебное пособие / А. И. Долженко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 180 c. — ISBN 978-5-4497-0911-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/102074.html>
3. Защита информации в компьютерных системах и сетях [Электронный ресурс] / В. Ф. Шаньгин. - Москва : ДМК Пресс, 2012. Режим доступа: <https://www.studentlibrary.ru/book/ISBN9785940748335.html>
4. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю. Н. Рагозин ; под редакцией Т. С. Кулакова. — Санкт-Петербург : Интермедия, 2018. — 168 c. — ISBN 978-5-4383-0161-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/73641.html

**в) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимый для освоения дисциплины (модуля)**

1. ЭБС "КОНСУЛЬТАНТ СТУДЕНТА" <http://www.studentlibrary.ru/>
2. Электронно-библиотечная система IPR BOOKS <http://www.iprbookshop.ru/>

**8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Вуз располагает необходимыми материально-техническими условиями для качественного проведения учебного процесса по реализуемой ОПОП ВО. Материально-техническое обеспечение включает необходимые учебные и вспомогательные площади для учебного процесса, достаточную инфраструктуру, обеспечение учебного процесса вычислительной и оргтехникой, достаточным количеством учебных материалов. Все учебные помещения оборудованы соответствующей мебелью, досками, техническими средствами обучения, что позволяет качественно осуществлять учебный процесс.

При необходимости рабочая программа дисциплины (модуля) может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе в том числе для обучения с применением дистанционных образовательных технологий. Для этого требуется заявление аспиранта (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).