УТВЕРЖДАЮ
Проректор по научной работе
_____ И.В. Бычков
«_26_» _____06_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)*

2.1.1.3. Методы и системы защиты информации, информационная безопасность

Научная специальность – 2.3.6. Методы и системы защиты информации, информационная безопасность

Направленность (профиль) – Методы и системы защиты информации, информационная безопасность

Высшее образование – подготовка кадров высшей квалификации

Форма обучения
очная

Челябинск, 2023

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Программа по дисциплине «Методы и системы защиты информации, информационная безопасность» составлена в соответствии с паспортом научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность и федеральными государственными требованиями (уровень образования: высшее образование – подготовка кадров высшей квалификации), утвержденными приказом Министерства науки и высшего образования Российской Федерации от 20 октября 2021 года № 951.

Разработчик программы:

Зав. кафедрой компьютерной безопасности
и прикладной алгебры,
кандидат физико-математических наук, доцент А.Н. Ручай

Программа одобрена на заседании кафедры компьютерной безопасности и прикладной алгебры от «14» апреля 2023 г., протокол № 11.

Зав. кафедрой компьютерной безопасности
и прикладной алгебры А.Н. Ручай

Программа принята на заседании Ученого совета математического факультета от «25» мая 2023 г., протокол № 9.

Согласовано:

Декан математического факультета Е.А. Сбродова

Зав. отделом аспирантуры
и докторантуры Н.В. Бочкарева

Аннотация программы: Формирование системы теоретических знаний и умений, необходимых для успешной профессиональной деятельности в сфере науки, техники и технологии, охватывающие совокупность проблем, связанных с разработкой, совершенствованием и применением методов и средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения, а также обеспечением информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации.

1. Цели и задачи освоения дисциплины

Цели дисциплины:

– изучить российские и зарубежные методы и стандарты оценки защищенности компьютерных систем и уметь применять полученные знания на практике.

Задачи дисциплины:

– уметь разрабатывать модели угроз безопасности информационных систем;

– уметь проводить оценку защищенности компьютерных систем согласно российским и зарубежным стандартам.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Методы и системы защиты информации, информационная безопасность» по подготовке к кандидатскому экзамену является обязательной. Преподавание дисциплины осуществляется на втором курсе (в 4 семестре).

Общая трудоемкость дисциплины, в том числе и промежуточная аттестация, составляет 3 зачетных единиц/108 часа, из них: контактная работа с преподавателем составляет – 1 зачетных единиц/36 часов (лекционные занятия – 18 часов, практические занятия – 18 часов), самостоятельная работа – 1,78 зачетных единиц/64 часов, контроль – 0, 22 зачетных единиц/8 часов.

Освоение дисциплины опирается на знания информатики, операционных систем (ОС), аппаратных средств вычислительной техники, теории информации, моделей безопасности компьютерных систем, систем управления базами данных, сетей и систем передачи информации, компьютерных сетей и сетевых технологий, основ построения защищенных компьютерных сетей, защиты программ и данных.

Для освоения дисциплины обучаемый должен обладать навыками аналитической работы, а также владеть основными навыками владения современными вычислительными средствами.

Дисциплина «Методы и системы защиты информации, информационная безопасность» призвана помочь аспирантам овладеть навыками и знаниями, необходимыми для подготовки к кандидатскому экзамену, выполнения научно-исследовательской работы, включая выполнение кандидатской диссертации.

Требования к «входным» знаниям, умениям и опыту деятельности обучающегося, необходимые при изучении дисциплины

Знать	Уметь	Владеть
– основные современные тенденции развития информатики и вычислительной техники; – основные принципы создания программных средств и основные этапы процесса разработки программных средств.	– использовать существующие пакеты прикладных программ для решения конкретных задач.	– методами решения конкретных задач из области технологии; – методами работы с программно-техническими средствами.
– общее устройство, принципы работы, основные алгоритмы работы и служебные структуры данных современных операционных систем.	– выполнять установку, настройку и обслуживание ОС, разрабатывать программы, использующие возможности ОС.	– владеть начальными навыками администрирования ОС, настройки и реализации политики безопасности ОС.
– основные понятия и методы теории информации, используемых для обеспечения компьютерной безопасности.	– использовать математические методы и модели для решения прикладных задач.	– методами количественного анализа процессов обработки, поиска и передачи информации.
– основные формальные модели политик безопасности, модели дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности	– самостоятельно разрабатывать новые и дорабатывать типовые модели политик безопасности; – определять причины, обстоятельства и условия дестабилизирующего воздействия на	– методами разработки моделей политик безопасности, управления доступом и информационными потоками; – навыками определения угроз информации в зависимости от среды

информационных потоков; – виды и состав угроз информационной безопасности; – принципы и общие методы обеспечения информационной безопасности; – основы разработки систем защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы; – методы выявления уязвимостей.	защищаемую информацию; – определять возможные каналы и методы несанкционированного доступа; – организовывать системное обеспечение защиты информации; – самостоятельно разрабатывать системы защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы.	эксплуатации продуктов информационных технологий; – навыками разработки основных политик безопасности; – методами разработки системы защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы.
– характеристики и типы систем баз данных; – области применения систем управления базами данных; – порядок эксплуатации баз данных; – основные модели структур данных; – способы организации файловых систем; – основные предложения языка запросов SQL.	– разрабатывать программы на языках программирования четвертого поколения; – реализовывать на практике сложные структуры данных средствами реляционной СУБД; – использовать язык запросов SQL.	– навыками работы с системами управления базами данных на различных платформах; – навыками разработчика и администратора баз данных; – навыками поддержки и сопровождения баз данных.
– понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации; – задачи и цели администрирования сетевой инфраструктуры организации; – основы функционирования сетевых протоколов и служб.	– проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации; – пользоваться программными средствами, реализующими основные криптографические функции, системами публичных ключей, цифровой подписью, разделение доступа.	– навыками самостоятельной исследовательской работы; – инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования; – методами и средствами аудита и мониторинга сетевых устройств и служб.

– основы функционирования сетевых протоколов и служб; – принципы построения системы безопасности сетевой операционной системы; – понятия и технологии корпоративных сетей, сетей LAN, сетей WAN; – понятие инфраструктуры корпоративной сети; – сетевые протоколы.	– проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации; – администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности; – проектировать простую компьютерную сеть	– технологиями и навыками построения и администрирования службы каталогов информационной системы организации; – инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования; – навыками настройки коммутации в корпоративной сети.
– иметь представление о построения современной системы защиты вычислительной сети предприятия; – знать основы средств и методов реализации атак на сетевые ресурсы; – знать основы принципов использования межсетевых экранов (МЭ); – знать основы построения систем адаптивной безопасности в вычислительных сетях; – знать основы построения виртуальных частных сетей.	– строить системы адаптивной безопасности в вычислительных сетях.	– построения систем адаптивной безопасности в вычислительных сетях; – построения виртуальных частных сетей.
– методы исследования программного обеспечения без исходных кодов (в том числе вредоносного программного обеспечения).	– исследовать программное обеспечение без исходных кодов с использованием методов статического и динамического анализа; – реализовывать методы защиты программного обеспечения (в том числе отдельные функциональные компоненты вредоносного программного обеспечения).	– навыками исследования программного обеспечения с использованием средств статического и динамического анализа; – навыками реализации и исследования компонент вредоносного программного обеспечения.

3. Требования к результатам освоения содержания дисциплины

Результаты обучения по дисциплине	
знать	– методы и стандарты оценки защищенности;
	– российские и зарубежные стандарты в области информационной безопасности;
	– методику разработки и применения модели угроз безопасности информации.
уметь	– разрабатывать модели угроз безопасности информационных систем;
	– проводить оценку защищенности компьютерных систем согласно российским и зарубежным стандартам.
владеть	– практические навыки разработки модели угроз безопасности информации и проведение оценки защищенности компьютерных систем согласно стандартам информационной безопасности.

4. Структура и содержание дисциплины

4.1. Структура дисциплины

Вид работы	**Семестр**				**Всего**
	1	**2**	**3**	**4**	
Общая трудоёмкость, акад. часов				108	108
Контактная работа:				36	36
Лекции, акад. часов				18	18
Практические (семинары), акад. часов				18	18
Лабораторные работы, акад. часов					
Самостоятельная работа, акад. часов				64	64
Контроль				8	8
Вид контроля (зачёт, экзамен)				канд. экзамен	

4.2. Содержание разделов дисциплины

№ раздела	**Наименование раздела**	**Количество часов**						**Форма текущего контроля**
		Всего	**Контактная работа**				**Самостоятельная работа**	
			Лекции	**Практические, семинары**	**Лаб. работы**	**Контроль**		
1.	Оценка угроз информационной безопасности	32	10	10			12	Устный опрос на практических занятиях
2.	Стандарты оценки угроз информационной безопасности	28	8	8			12	
3.	Реферат по диссертационному исследованию	12					12	Собеседование
	Контроль	36				8	28	Канд. экзамен
	Итого:	**108**	**18**	**18**		**8**	**64**	

№ раздела	Наименование раздела	Содержание раздела
1.	Оценка угроз информационной безопасности	**Лекционные занятия:** Определения угроз безопасности информации в информационной системе Модель нарушителя по реализации угроз безопасности информации Способы реализации угроз безопасности информации. Определение актуальных угроз безопасности информации в информационной системе Определение потенциала нарушителя Модель угроз безопасности информации **Практические занятия:** Оценка угроз информационной безопасности. Актуальные угрозы. Способы реализации угроз информационной безопасности. Действия по реализации угроз информационной безопасности. **Самостоятельная работа:** Разработка модели нарушителя Разработка модели угроз безопасности
2.	Стандарты оценки угроз информационной безопасности	**Лекционные занятия:** Стандарты информационной безопасности Стандарты оценки защищенности Методы и стандарты оценки защищенности информационных систем в банковской сфере **Практические занятия:** Стандарты оценки угроз информационной безопасности. **Самостоятельная работа:** Методика определения угроз безопасности информации в информационных системах Российские стандарты информационной безопасности

5. Образовательные технологии

- информационно-коммуникационные технологии;
- исследовательские методы в обучении;
- интерактивные технологии;
- применение новых методов обучения, связанных с использованием возможностей виртуальной информационной среды (мультимедийные технологии).

В соответствии с утвержденной основной образовательной программой по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (направленность (профиль) - Методы и системы защиты информации, информационная безопасность) программа дисциплины «Методы и системы защиты информации, информационная безопасность» предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков у обучающихся. Эффективность применения интерактивных форм обучения обеспечивается реализацией следующих условий:

– создание диалогического пространства в организации учебного процесса;

– использование принципов социально-психологического обучения в учебной и научной деятельности;

– формирование психологической готовности преподавателей к использованию интерактивных форм обучения, направленных на развитие внутренней активности аспиранта и достижения ряда важнейших образовательных целей: стимулирование мотивации и интереса в области защиты информации; повышение уровня активности и самостоятельности научно-исследовательской работы; развитие навыков анализа, критичности мышления, научной коммуникации.

6. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

6.1. Паспорт фонда оценочных средств по дисциплине «Методы и системы защиты информации, информационная безопасность»

№	Контролируемые разделы дисциплины	Результаты обучения	Наименование оценочного средства
1.	Оценка угроз информационной безопасности	**знать:** – современные тенденции развития информатики и вычислительной техники, компьютерных технологий; – методику составления результатов исследований по оценке защищенности компьютерных систем; **уметь:** – использовать программные средства общего и специального назначения в своей профессиональной деятельности; –исследовать защищенность компьютерных систем; **владеть:** – практическими навыками использования программных средств общего специального назначения в своей профессиональной деятельности с учетом современных тенденций развития информационных технологий	Устный опрос на практических занятиях
2.	Стандарты оценки угроз информационной безопасности	**знать:** – российские и зарубежные стандарты в области информационной безопасности; – регламентирующие порядок проведения сертификации	Устный опрос на практических занятиях

		средств защиты информации в компьютерных системах; – современные критерии и стандарты для анализа безопасности компьютерных систем; **уметь:** –оценивать соответствие проектной и эксплуатационной документации информационной системы на соответствие стандарту в области информационной безопасности; – применять современные критерии и стандарты для анализа безопасности компьютерных систем; **владеть:** – практическими навыками работы с современными критериями и стандартами для анализа безопасности компьютерных систем	

6.2. Оценочные средства

6.2.1. Текущий контроль

Вопросы для устного опроса

1. Информация.
2. Информационная система.
3. Угроза безопасности информации.
4. Определение области применения оценки угроз информационной безопасности.
5. Характеристика угрозы информационной безопасности.
6. Источники угроз безопасности и их классификация.
7. Факторы, обуславливающие техногенные угрозы безопасности информации.
8. Идентификация угрозы безопасности информации в информационной системе.
9. Мониторинг и переоценка угроз безопасности информации.
10. Определение угроз безопасности информации в информационной системе.
11. Нарушитель информационной безопасности.
12. Оценка возможностей нарушителей.
13. Типы нарушителей.
14. Мотивации реализации нарушителями угроз безопасности информации в информационной системе.
15. Связи нарушителей.
16. Нарушители с базовым (низким) потенциалом.
17. Нарушители с базовым повышенным (средним) потенциалом.
18. Нарушители с высоким потенциалом.
19. Модель нарушителя по реализации угроз безопасности информации.
20. Способы реализации угроз безопасности информации.
21. Действия по реализации угроз информационной безопасности.
22. Реализация преднамеренных угроз безопасности информации.
23. Условия определения способов реализации угроз безопасности информационной системы.
24. Актуальная угроза безопасности информации.
25. Показатель актуальности угрозы.
26. Вероятность реализации угрозы.

27. Вербальные градации показателя вероятности реализации угрозы.
28. Возможность реализации угрозы безопасности информации.
29. Показатели, характеризующие проектную защищенность информационной системы.
30. Уровень проектной защищенности.
31. Уровень защищенности в ходе эксплуатации информационной системы.
32. Возможность реализации угрозы безопасности информации.
33. Исходные данные об угрозах безопасности информации.
34. Условия определения способов реализации угроз безопасности информационной системы.
35. Оценка степени возможного ущерба от реализации угрозы безопасности информации.
36. Определение актуальных угроз безопасности информации в информационной системе.
37. Потенциал нарушителя.
38. Классификация и виды нарушителей информационной безопасности.
39. Определение потенциала нарушителя.
40. Параметры экспертной оценки.
41. Техническая компетентность нарушителя.
42. Возможности нарушителя по доступу к информационной системе.
43. Оснащенность нарушителя.
44. Оценка потенциала нарушителя.
45. Модель угроз безопасности информации.
46. Структура модели нарушителя.
47. Структура модели угроз безопасности.
48. Стандарты информационной безопасности.
49. Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (1983).
50. Политика безопасности.
51. Классы безопасности.
52. Распределение функций безопасности по уровням модели OSI.
53. Стандарт ISO/IEC 15408.
54. Классы функциональных требований.
55. Международный стандарт ISO 17799.
56. Международные стандарты информационной безопасности.
57. Российские стандарты информационной безопасности.

58. Стандарты оценки защищенности.
59. Методы и стандарты оценки защищенности информационных систем в банковской сфере.
60. Minimum Security Requirements for Federal Information and Information Systems
61. Методика определения угроз безопасности информации в информационных системах.
62. Банковские стандарты информационной безопасности.
63. Обеспечение информационной безопасности организаций банковской системы Российской Федерации.

6.2.2. Перечень самостоятельных работ

1. Разработка модели нарушителя.
2. Разработка модели угроз безопасности.
3. Применение методики определения угроз безопасности информации в информационных системах.
4. Применение российских стандартов информационной безопасности.
5. Применение банковских стандарты информационной безопасности.

6.2.3. Промежуточная аттестация

Видом контроля по данной дисциплине является кандидатский экзамен.

Вопросы к экзамену формируются в соответствии с программой кандидатского экзамена и паспортом научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» (за каждый вопрос выставляется оценка).

Экзамен по дисциплине проводится по билетам, каждый из которых содержит 3 вопроса. За каждый ответ на вопрос выставляется оценка. По результатам ответов за экзамен выводится единая оценка по пятибалльной системе.

Реферат (на экзамене проводится собеседование и выставляется оценка).

Пишется в соответствии с общими требованиями к реферативным работам, представляет собой обзор мнений, точек зрения, научных положений по тематике диссертации.

Вопросы к кандидатскому экзамену

1. Понятие нарушителя. Исходные предположения о возможностях нарушителя. Цели информационной безопасности.
2. Законы Российской Федерации, составляющие основу информации в стране.
3. Особенности российского законодательства в части защиты государственной тайны, коммерческой тайны и авторских прав.
4. Порядок лицензирования и сертификации деятельности в области защиты информации.
5. Математические модели формальной теории защиты информации.
6. Угрозы информации и политика безопасности.
7. Классификация систем защиты.
8. Международные и отечественные стандарты в области защиты информации.
9. Криптографические стандарты Российской Федерации, стандартизации.
10. Понятия теоретической, практической и временной стойкость. Методы получения оценок стойкости.
11. Понятие надежности. Методология обоснования надежности криптографической защиты.
12. Автоматное определение шифра. Криптографические параметры узлов и блоков шифрующих автоматов.
13. Методы получения псевдослучайных последовательностей.
14. Генераторы псевдослучайных последовательностей и их свойства.
15. Блочные и поточные шифры.
16. Режимы использования блочных шифров.
17. Алгоритмы выработки имитовставки. Методы оценки имитозащищенности.
18. Режимы аутентифицированного шифрования. Современные стандартизированные решения.
19. Ключевые системы, методы распределения ключей.
20. Методы выработки производных ключей, принципы оценки качества производной ключевой информации.
21. Асимметричные криптографические схемы.
22. Гибридные схемы шифрования. Практические примеры реализации гибридных схем.

23. Электронная подпись, инфраструктура открытых ключей. Удостоверяющие центры. Методы обеспечения подлинности физических лиц.
24. Атаки на криптографические алгоритмы: алгоритмические, статистические.
25. Свойства безопасности криптографических протоколов.
26. Методы и средства обеспечения заданных свойств безопасности криптографических протоколов.
27. Протоколы выработки общего ключа.
28. Протоколы распределения ключей.
29. Протоколы с разделением секрета.
30. Протоколы с подписью в слепую и протоколы электронного голосования.
31. Протоколы семейства TLS, область их применения, методы оценки безопасности.
32. Протокол SSH, область его применения, реализуемые методы аутентифицированного удаленного доступа.
33. Протокол SESPAKE выработки общего ключа на основе пароля, область его применения, принципы обоснования сложности перебора паролей.
34. Протокол защищенного взаимодействия SP-FIOT. Обоснование свойств безопасности, отличия от других протоколов.
35. Криптографические механизмы протокола IPSec. Обеспечиваемые безопасности.
36. Принципы организации виртуальных частных сетей (VPN). Обеспечиваемые свойства безопасности. Программные средства реализации VPN.
37. Анонимизирующие сети. Принципы их построения, обеспечиваемые безопасности. Криптографические механизмы, используемые в анонимизитрующих сетях.
38. Методы разграничения доступа.
39. Программные и аппаратные средства разграничения доступа.
40. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
41. Методы и средства хранения ключевой информации.
42. Средства обеспечения безопасности в ОС семейств Windows и UNIX, критерии защищенности ОС.
43. Средства обеспечения безопасности в сетях.

44. Принципы и протоколы аутентификации при удаленном доступе. Отличия от криптографических протоколов.
45. Средства защиты серверов и рабочих станций.
46. Средства защиты локальных сетей при подключении к Internet.
47. Межсетевые экраны, электронные замки, криптофильтры, криптороутеры.
48. Области применения, достоинства, недостатки, реализуемые политики безопасности.
49. Методы оценки качества применяемых средств защиты.
50. Методы и средства защиты информации в СУБД.
51. Средства идентификации и аутентификации, управление доступом, средства контроля, аудит безопасности.
52. Критерии защищенности БД и АИС.
53. Методы и системы обнаружения компьютерных атак.
54. Основные физические каналы утечки информации информационной системы.
55. Узлы и блоки оборудования информационной системы, уязвимые для технической разведки.
56. Примеры современных атак на средства защиты информации, основанные на изучении побочных сигналов.
57. Технические параметры современных средств перехвата побочных сигналов.
58. Математические модели побочных каналов утечки.
59. Выделение полезных сигналов на фоне помех.
60. Методы и средства защиты от инженерно-технической разведки.
61. Алгоритмические средства защиты ключевой и криптографически опасной информации от утечек по побочным каналам информации.
62. Методика оценки качества инженерно-технической защиты.
63. Определение компьютерного вируса. Классификация компьютерных вирусов.
64. Методы выявления и защиты от вирусов.
65. Определение понятия изолированной программной среды. Примеры.
66. Методы защиты от изменения, контроль целостности.
67. Криптографический контроль целостности программных средств при их распространении и эксплуатации.
68. Методы защиты от изучения программных средств.

69. Методы восстановления алгоритмов защиты в программных продуктах.
70. Метод черного ящика при исследовании программных реализаций средств защиты информации.
71. Метод оценки уровня криптографической защиты типовых программных продуктов.
72. Анализ особенностей выработки и распределения ключей.
73. Анализ возможности и способы внедрения криптографических закладок.
74. Методы удаленного исследования компьютеров и средств защиты информации.
75. Проведение экспресс-анализа защищенности сетевого компьютера.
76. Сетевые атаки. Классификация атак.
77. Методы и технические средства защиты от сетевых атак.
78. Принципы реализации средств криптографической защиты информации.
79. Требования к ключевой системе средств защиты информации.
80. Требования к криптографическим и инженерно-криптографическим методам защиты, реализуемым в средствах защиты информации.
81. Механизмы документирования исходных текстов программ.
82. Методы анализа исходных текстов с целью поиска уязвимостей.
83. Инструментальные средства для проведения статистического и динамического анализа исходных текстов.
84. Методы и инструментальные средства тестирования программного обеспечения.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене/зачете.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа,
– в форме аудиофайла,
– в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа,
– в форме аудиофайла.

6.3. Критерии оценивания результатов обучения

Оценивание результатов обучения проводится по пятибалльной шкале:

Оценка **«Отлично» (5 баллов)** ставится при соблюдении следующих условий:

- обучающимся дан полный, в логической последовательности развернутый ответ на поставленный вопрос, в котором он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса;
- обучающимся верно определены границы оценки защищенности компьютерной системы, верно выбрана и применена методика оценки.

Оценка **«Хорошо» (4 балла)** ставится при соблюдении следующих условий:

- обучающимся дан развернутый ответ на поставленный вопрос, в котором аспирант демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, логичность и последовательно выстраивает ответ. Однако, допускает неточность в ответе;
- обучающимся верно определены границы оценки защищенности компьютерной системы, выбрана и применена методика оценки с небольшими неточностями.

Оценка «**Удовлетворительно» (3 балла)** ставится, если:

- обучающимся дан ответ, свидетельствующий, в основном, о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточной логичностью и последовательностью ответа;
- обучающимся верно определены границы оценки защищенности компьютерной системы, неверно выбрана и применена методика оценки.

Оценка **«Неудовлетворительно» (1-2 балла)** ставится, если:

- обучающимся дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, отсутствием логичности и последовательности. Выводы поверхностны. Обучающийся не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя;
- обучающимся подготовлен ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме на языке Брайля, устно с использованием услуг сурдопереводчика);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно на языке Брайля, с использованием услуг ассистента, устно).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине (модулю) может проводиться в несколько этапов.

7. Учебно-методическое обеспечение дисциплины

Самостоятельная работа аспирантов проводится в форме изучения отдельных теоретических вопросов по предлагаемой литературе и самостоятельного решения задач с дальнейшим их разбором или обсуждением на аудиторных занятиях. Во время самостоятельной подготовки обучающиеся обеспечены доступом к базам данных и библиотечным фондам и доступом к сети Интернет.

Самостоятельная работа способствует:

– углублению и расширению знаний;

– формированию интереса к самостоятельной научно-исследовательской деятельности;

– овладению приемами процесса познания и развитию познавательных способностей.

Самостоятельная работа аспирантов имеет основную цель – обеспечить качество подготовки выпускаемых специалистов.

Самостоятельная работа аспиранта является показателем научного потенциала, умения работы с литературными источниками и нормативными актами, материалами экономической и педагогической практики, способности аспиранта к самостоятельному анализу проблемных вопросов. Она состоит в изучении учебной и научной литературы, в выполнении заданий для самостоятельной работы.

Аспиранты очной, а также и заочной форм обучения изучают и нарабатывают теоретический и практический материал по большей части самостоятельно. На кафедре компьютерной безопасности и прикладной алгебры в списке рекомендованной литературы предложен объем учебной и научной литературы, следовательно, аспиранту необходимо как можно чаще обращаться к фондам научных библиотек, а также и к периодической литературе, следить за новыми изданиями в области защиты информации и информационной безопасности. При изучении научной, учебной литературы необходимо сопоставить содержание имеющейся в наличии литературы с программой кандидатского экзамена по специальности. В случае отсутствия того или иного источника литературы, необходимо обратиться к фондам Российской государственной библиотеки (г. Москва). Аспирант должен провести тщательную подготовительную работу с научной литературой по своей специальности, освоить различные методы поиска информации.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями

здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,
– в форме электронного документа,
– в форме аудиофайла,
– в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:

– в печатной форме,
– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,
– в форме электронного документа,
– в форме аудиофайла.

Рекомендованная литература

Основная литература				
	Авторы, составители	Заглавие	Издательство, год	Ресурс
1	Галатенко В. А., Бетелин В. Б.	Стандарты информационной безопасности: курс лекций (https://biblioclub.ru/index.php?page=book&id=233065)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2006	ЭБС
2	Бекетнова Ю. М., Крылов Г. О., Ларионова С. Л.	Международные основы и стандарты информационной безопасности финансово-экономических систем: учебное пособие (https://biblioclub.ru/index.php?page=book&id=494850)	Москва : Прометей, 2018	ЭБС
3	Аверченков В. И.	Аудит информационной безопасности: учебное пособие (https://biblioclub.ru/index.php?page=book&id=93245)	Москва : ФЛИНТА, 2021	ЭБС
Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Ресурс
1	Громов Ю. Ю., Мартемьянов Ю. Ф., Букурако Ю. К., Иванова О. Г., Однолько В. Г.	Организация безопасной работы информационных систем: учебное пособие (https://biblioclub.ru/index.php?page=book&id=277794)	Тамбов : Тамбовский государственный технический университет (ТГТУ), 2014	ЭБС
2	Кияев В., Граничин О.	Безопасность информационных систем: курс: учебное пособие (https://biblioclub.ru/index.php?page=book&id=429032)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС

Электронные фонды и ресурсы

Профессиональные базы данных и информационно-справочные системы
1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.
2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.
3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp.
4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php.
5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.
6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/

Лицензионное программное обеспечение по дисциплине (модулю)

Adobe Reader
Notepad++
VirtualBox
Visual Studio

8. Материально-техническое обеспечение

Для реализации дисциплины «Методы и системы защиты информации, информационная безопасность» используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

Практические занятия проходят в учебных лабораториях технических средств защиты информации и «Сетевой полигон» (ауд. 421, 423, учебный корпус №1). Материально-техническое обеспечение приведено в паспортах лабораторий.

Для проведения занятий по дисциплинам, предусмотренным учебным планом подготовки аспирантов, имеется необходимая материально-техническая база, соответствующая действующим санитарным и

противопожарным правилам и нормам, обеспечивающей проведение всех видов теоретической и практической подготовки, а также эффективное выполнение выпускной квалификационной работы (диссертации):

– лекционные аудитории, оснащенные мультимедийными комплексами на основе антивандальной трибуны;

– специализированные компьютерные классы с подключенным к ним периферийным устройством и оборудованием;

– методические материалы для проведения самостоятельной работы по дисциплине.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Университет располагает компьютерными классами, объединенными в локальную сеть, выходом в Интернет, оснащенными современными высокопроизводительными компьютерами. Поддерживается собственный сайт: http://csu.ru.

Для получения высшего образования по программам аспирантуры инвалидами и лицами с ограниченными возможностями здоровья в университете имеются аудитории, оснащенные следующим оборудованием:

Название кабинета	Оборудование
Тифлотехническая аудитория, кабинет А-28 первого учебного корпуса	Тифлотехнические средства: брайлевский компьютер с дисплеем и принтером, тифлокомплекс «Читающая машина», телевизионное увеличивающее устройство, тифломагнитолы кассетные (3 шт.) и цифровые диктофоны (6 шт.). Специальное программное обеспечение: программа речевой навигации JAWS, речевые синтезаторы («говорящая мышь»), экранные лупы.
Сурдотехническая аудитория, кабинет А-27 первого учебного корпуса	Радиокласс «Сонет-Р» (на 6 человек), программируемые слуховые аппараты (6 шт.) индивидуального пользования с устройством задания режима работы на компьютере, аудиотехника.
Аудитория адаптивных информационных технологий, кабинет А-27 первого учебного корпуса	Компьютерный класс на 2 мест, интерактивная доска ActiveBoard с системой голосования, акустический усилитель и колонки, мультимедийный проектор, телевизор, видеомагнитофон, устройство видеоконференцсвязи VCON HD3000.

Все указанные в настоящей рабочей программе дисциплины методическое и техническое обеспечение учебного процесса для инвалидов и лиц с ограниченными возможностями здоровья предоставляется Региональным учебно-научным центром инклюзивного образования ЧелГУ.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

При изучении данной дисциплины используются лекционные и практические занятия, а также самостоятельная работа аспиранта. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала обучающемуся желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.

Рекомендуется перед каждым лекционным занятием выполнить домашнее задание, что позволит лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Обучающемуся желательно проявлять активное участие в лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, форумы, электронная почта и др.).

Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Обучающиеся имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.

Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии

предусматривают возможность приема-передачи информации в доступных для них формах.

Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.