МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
имени И.Т. ТРУБИЛИНА»

Экономический факультет
Компьютерных технологий и систем

УТВЕРЖДЕНО:
Декан, Руководитель подразделения
Тюпаков К.Э.
(протокол от 17.05.2024 № 9)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) « ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Уровень высшего образования: специалитет

Специальность: 38.05.01 Экономическая безопасность

Направленность (профиль): Экономико-правовое обеспечение экономической безопасности
Квалификация (степень) выпускника: Экономист

Формы обучения: очная, очно-заочная

Год набора: 2024

Срок получения образования: Очная форма обучения – 5 лет
Очно-заочная форма обучения – 5 лет 8 месяца(-ев)

Объем: в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

2024

Разработчики:
Доцент, кафедра компьютерных технологий и систем
Алашеев В.В.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по специальности Специальность: 38.05.01 Экономическая безопасность, утвержденного приказом Минобрнауки России от 14.04.2021 №293, с учетом трудовых функций профессиональных стандартов: "Специалист по управлению рисками", утвержден приказом Минтруда России от 30.08.2018 № 564н; "Специалист по финансовому мониторингу (в сфере противодействия легализации доходов, полученных преступным путем, и финансированию терроризма)", утвержден приказом Минтруда России от 24.07.2015 № 512н; "Экономист предприятия", утвержден приказом Минтруда России от 30.03.2021 № 161н; "Внутренний аудитор", утвержден приказом Минтруда России от 24.06.2015 № 398н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Компьютерных технологий и систем	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Лукьяненко Т.В.	Согласовано	22.03.2024, № 9
2	Экономический факультет	Председатель методической комиссии/совета	Толмачев А.В.	Согласовано	16.05.2024, № 11

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - Целью освоения дисциплины «Информационная безопасность» является формирование комплекса знаний об организационных, научных и методических основах информационной безопасности (ИБ), освоение методов анализа процессов, происходящих в сфере ИБ; изучение принципов ее функционирования и развития и использование полученных результатов в экономико-правовом обеспечении экономической безопасности (ЭБ) предприятий и отраслей.

Задачи изучения дисциплины:

- Раскрыть особенности функционирования ИБ экономических систем, ¶их структур и динамики развития;;
- Ознакомить обучающихся с основными видами и структурами связей ¶элементов систем ИБ, механизмами ее устойчивого функционирования и ¶развития;;
- Раскрыть факторы, воздействующие на функционирование и развитие ¶ИБ в экономико-правовое обеспечение экономической безопасности предприятий, национальных и мировой экономик в целом, при их взаимодействиях и интеграции.¶.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-П6 Способен осуществлять информационно-аналитическое обеспечение предупреждения, выявления, пресечения, раскрытия и расследования экономических и финансовых преступлений, применять технико-криминалистические средства и методы, формы организации и методику раскрытия и расследования преступлений в сфере экономики

ПК-П6.1 Собирает, проверяет и анализирует полученную информацию о финансовых операциях и сделках с признаками ОД/ФТ, полученную в результате мониторинга средств массовой информации, информационно-телекоммуникационной сети «Интернет», а также в рамках сотрудничества участников профессиональных объединений

Знать:

ПК-П6.1/Зн1 о признаках ОД/ФТ

Уметь:

ПК-П6.1/Ум1 собирать, проверять и анализировать полученную информацию о финансовых операциях и сделках с признаками ОД/ФТ, полученную в результате мониторинга средств массовой информации, информационно-телекоммуникационной сети «Интернет», а также в рамках сотрудничества участников профессиональных объединений

Владеть:

ПК-П6.1/Нв1 сбора, проверки и анализа полученной информации о финансовых операциях и сделках с признаками ОД/ФТ, полученную в результате мониторинга средств массовой информации, информационно-телекоммуникационной сети «Интернет», а также в рамках сотрудничества участников профессиональных объединений

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Информационная безопасность» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): Очная форма обучения - 7, Очно-заочная форма обучения - 7.

В процессе изучения дисциплины студент готовится к видам профессиональной деятельности и решению профессиональных задач, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины и виды учебной работы

Очно-заочная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Внеаудиторная контактная работа (часы)	Зачет (часы)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Седьмой семестр	108	3	23	1		12	10	85	Зачет
Всего	108	3	23	1		12	10	85	

Очная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Внеаудиторная контактная работа (часы)	Зачет (часы)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Седьмой семестр	108	3	37	1		16	20	71	Зачет
Всего	108	3	37	1		16	20	71	

5. Содержание дисциплины

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Очно-заочная форма обучения

Наименование раздела, темы	Всего	Внеаудиторная контактная работа	Лабораторные занятия	Лекционные занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы

Раздел 1. Основы информационной безопасности	**34**	**1**	**4**	**4**	**25**	ПК-П6.1
Тема 1.1. Основы информационной безопасности. Основные понятия и определения.	11		1	2	8	
Тема 1.2. Основные стандарты в области информационнойбезопасности	11		1	2	8	
Тема 1.3. Политика государства в области информационной безопасности.	12	1	2		9	
Раздел 2. Модель угроз информационной безопасности.	**21**		**2**	**2**	**17**	ПК-П6.1
Тема 2.1. Модель угроз информационной безопасности.	11		1	2	8	
Тема 2.2. Методы контроля и разграничения доступа.	10		1		9	
Раздел 3. Меры обеспечения защиты информации.	**53**		**6**	**4**	**43**	ПК-П6.1
Тема 3.1. Меры обеспечения защиты информации.	12		2	2	8	
Тема 3.2. Криптографические методы защиты информации.	11		1	2	8	
Тема 3.3. Техническая защита информации.	10		1		9	
Тема 3.4. Программно-технические меры защиты информации.	10		1		9	
Тема 3.5. Системы обнаружения и предотвращения компьютерных атак.	10		1		9	
Итого	**108**	**1**	**12**	**10**	**85**	

Очная форма обучения

Наименование раздела, темы	Всего	Внеаудиторная контактная работа	Лабораторные занятия	Лекционные занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Основы информационной безопасности	**31**		**4**	**6**	**21**	ПК-П6.1

Тема 1.1. Основы информационной безопасности. Основные понятия и определения.	9			2	7	
Тема 1.2. Основные стандарты в области информационнойбезопасности	11		2	2	7	
Тема 1.3. Политика государства в области информационной безопасности.	11		2	2	7	
Раздел 2. Модель угроз информационной безопасности.	**22**		**4**	**4**	**14**	ПК-П6.1
Тема 2.1. Модель угроз информационной безопасности.	11		2	2	7	
Тема 2.2. Методы контроля и разграничения доступа.	11		2	2	7	
Раздел 3. Меры обеспечения защиты информации.	**55**	**1**	**8**	**10**	**36**	ПК-П6.1
Тема 3.1. Меры обеспечения защиты информации.	11		2	2	7	
Тема 3.2. Криптографические методы защиты информации.	11		2	2	7	
Тема 3.3. Техническая защита информации.	11		2	2	7	
Тема 3.4. Программно-технические меры защиты информации.	11		2	2	7	
Тема 3.5. Системы обнаружения и предотвращения компьютерных атак.	11	1		2	8	
Итого	**108**	**1**	**16**	**20**	**71**	

5. Содержание разделов, тем дисциплин

Раздел 1. Основы информационной безопасности
(Очно-заочная: Внеаудиторная контактная работа - 1ч.; Лабораторные занятия - 4ч.; Лекционные занятия - 4ч.; Самостоятельная работа - 25ч.; Очная: Лабораторные занятия - 4ч.; Лекционные занятия - 6ч.; Самостоятельная работа - 21ч.)

Тема 1.1. Основы информационной безопасности. Основные понятия и определения.
(Очно-заочная: Лабораторные занятия - 1ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 8ч.; Очная: Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.)
1. Понятие информации.
2. Доступ, обработка и защита информации.
3. Информационные системы.
4. Информационная безопасность.

Тема 1.2. Основные стандарты в области информационнойбезопасности
(Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.; Очно-заочная: Лабораторные занятия - 1ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 8ч.)

1. Категории стандартов Российской Федерации.
2. Основные действующие стандарты РФ в области информационной безопасности.
3. Группа стандартов Р ИСО/МЭК 27000.
4. Стандарты в области криптографической защиты.
5. Стандарты Р ИСО/МЭК 15408 "Общие критерии".
6. Руководящие документы уполномоченных органов (регуляторов) Российской Федерации.

Тема 1.3. Политика государства в области информационной безопасности.
(Очно-заочная: Внеаудиторная контактная работа - 1ч.; Лабораторные занятия - 2ч.; Самостоятельная работа - 9ч.; Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.)
1. Стратегия национальной безопасности.
2. Доктрина информационной безопасности.
3. Законодательство в области защиты информации.
4. Государственная тайна.
5. Коммерческая тайна.
6. Персональные данные.

Раздел 2. Модель угроз информационной безопасности.
(Очная: Лабораторные занятия - 4ч.; Лекционные занятия - 4ч.; Самостоятельная работа - 14ч.; Очно-заочная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 17ч.)

Тема 2.1. Модель угроз информационной безопасности.
(Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.; Очно-заочная: Лабораторные занятия - 1ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 8ч.)
1. Назначение и структура модели угроз ИБ.
2. Принцип оценки актуальности угроз.
3. Оценка возможности реализации угроз, степени ущерба и ее актуальности.

Тема 2.2. Методы контроля и разграничения доступа.
(Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.; Очно-заочная: Лабораторные занятия - 1ч.; Самостоятельная работа - 9ч.)
1. Основные понятия контроля доступа субъектов.
2. Аутентификация субъектов доступа.
3. Модели разграничения доступа.

Раздел 3. Меры обеспечения защиты информации.
(Очная: Внеаудиторная контактная работа - 1ч.; Лабораторные занятия - 8ч.; Лекционные занятия - 10ч.; Самостоятельная работа - 36ч.; Очно-заочная: Лабораторные занятия - 6ч.; Лекционные занятия - 4ч.; Самостоятельная работа - 43ч.)

Тема 3.1. Меры обеспечения защиты информации.
(Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.; Очно-заочная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 8ч.)
1. Организация защиты информации.
2. Организационные защиты информации.
3. Программно-технические средства защиты информации.

Тема 3.2. Криптографические методы защиты информации.
(Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.; Очно-заочная: Лабораторные занятия - 1ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 8ч.)

1. Криптографические методы защиты данных.
2. Шифры.
3. Компьютерные вирусы.

Тема 3.3. Техническая защита информации.
(Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.; Очно-заочная: Лабораторные занятия - 1ч.; Самостоятельная работа - 9ч.)

1. Основные понятия технической защиты инфориации.
2. Технические каналы утечки информации.
3. Принципы осуществления технической разведки.
4. Принципы защиты от технической разведки.

Тема 3.4. Программно-технические меры защиты информации.
(Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.; Очно-заочная: Лабораторные занятия - 1ч.; Самостоятельная работа - 9ч.)

1. Сервисы безопасности.
2. Антивирусная защита.
3. Межсетевое экранирование.
4. Системы предотвращения утечки информации.
5. Протоколирование и аудит.

Тема 3.5. Системы обнаружения и предотвращения компьютерных атак.
(Очная: Внеаудиторная контактная работа - 1ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 8ч.; Очно-заочная: Лабораторные занятия - 1ч.; Самостоятельная работа - 9ч.)

1. Назначения систем обнаружения и предотвращения компьютерных атак.
2. Понятие компьютерной атаки.
3. Требования к системам обнаружения и предотвращения компьютерных атак.
4. Классификация систем обнаружения и предотвращения компьютерных атак.
5. Критерии выбора систем обнаружения и предотвращения компьютерных атак.

6. Оценочные материалы текущего контроля

Раздел 1. Основы информационной безопасности

Форма контроля/оценочное средство: Компетентностно-ориентированное задание
Вопросы/Задания:

.

Раздел 2. Модель угроз информационной безопасности.

Форма контроля/оценочное средство: Компетентностно-ориентированное задание
Вопросы/Задания:

.

Раздел 3. Меры обеспечения защиты информации.

Форма контроля/оценочное средство: Компетентностно-ориентированное задание
Вопросы/Задания:

.

7. Оценочные материалы промежуточной аттестации

Очная форма обучения, Седьмой семестр, Зачет
Контролируемые ИДК: ПК-П6.1
Вопросы/Задания:

1. Вопросы к зачету.

1. Международные стандарты информационной безопасности.
2. Концепция информационной безопасности страны.
3. Место информационной безопасности в социально-экономических системах.
4. Основные нормативные руководящие документы, касающиеся государственной тайны.
5. Виды возможных нарушений информационной системы.
6. Актуальность проблемы информационной безопасности.
7. Модели безопасности и их применение.
8. Классификация методов ИБ от несанкционированного доступа (НСД).
9. Классификация средств ИБ от НСД.
10. Механизмы ИБ от НСД.
11. Государственные требования к системам ИБ.
12. Концепция ИБ от НСД.
13. Требования к криптографическим средствам систем ЗИ (СЗИ).
14. Показатели защищенности средств вычислительной техники (СВТ) от НСД.
15. Классификация компьютерных систем и требования ИБ к ним.
16. Использование защищенных компьютерных систем (КС).
17. Методы контроля доступа к ресурсам КС.
18. Способы фиксации факта доступа.
19. Структура и функции подсистемы контроля доступа программ и пользователей.
20. Средства активного аудита компьютерных систем.
21. Идентификация и аутентификация субъектов и объектов КС.
22. Основные подходы к защите данных от НСД.
23. Модели управления доступом.
24. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.
25. Защита алгоритма шифрования и программно-аппаратные средства шифрования.
26. Построение аппаратных компонент криптозащиты данных.
27. Взаимодействие прикладных программ и программы злоумышленника.
28. Классификация разрушающих программных средств и их воздействий.
29. Компьютерные вирусы (КВ) как класс разрушающих программных воздействий.
30. Сущность, проявление, классификация КВ.
31. Необходимые и достаточные условия недопущения разрушающих программных воздействий.
32. Организационные средства защиты от КВ.
33. Роль морально-этических факторов в устранении угрозы разрушающих программных воздействий.
34. Проблема обеспечение целостности информации.
35. Способы обеспечения целостности информации.
36. Электронная цифровая подпись.
37. Криптографические хэш-функции. Схемы вычисления хэш-функции.

38. Методы криптографии и задачи, решаемые криптографическими средствами в КС.
39. Алгоритмы криптографических преобразований, их характеристики.
40. Методы и средства ограничения доступа к компонентам компьютеров.
41. Построение средств ЗИ для персонального компьютера (ПК).
42. Перечень и характеристики сертифицированных программно-аппаратных средств систем ЗИ от НСД для ПК.
43. Особенности ЗИ в вычислительных сетях.
44. Механизмы реализации атак на вычислительные сети.
45. Определение перечня защищаемых ресурсов и их критичности.
46. Определение категорий персонала, на которые распространяется политика безопасности.
47. Определение угроз ИБ.
48. Формирование требований к построению системы ЗИ.
49. Определение уязвимости КС и выбор средств ЗИ.
50. Антивирусные программные комплексы.
51. Настройка и применение антивирусных программ.
52. Исследование результатов воздействия КВ на программы в ОС.
53. Исследование результатов работы антивирусных программ.
54. Алгоритмы электронной цифровой подписи.
55. Основные положения национальной стратегии развития искусственного интеллекта на период до 2030 года.
56. Цель доктрины информационной безопасности РФ (от5.12.2016 №646).
57. Каковы стратегические цели и основные направления обеспечения информационной безопасности (ИБ).
58. Дайте определения угрозам и обеспечению ИБ.
59. Дайте определение силам и средствам обеспечения ИБ.
60. Раскройте содержание терминов система обеспечения ИБ и ее информационной инфраструктуры.
61. Каковы стратегические цели и задачи обеспечения ИБ РФ.
62. Основные негативные факторы, влияющие на состояние международной ИБ.
63. Основные направления обеспечения ИБ в экономической сфере.
64. Основные направления обеспечения ИБ в области науки, технологий и образовании.
65. Принципы работы государственных органов по обеспечению ИБ.
66. Задачи государственных органов в рамках деятельности по обеспечению ИБ.
67. Где и как осуществляется процесс реализации доктрины ИБ РФ.
68. Раскройте основные понятия и определения использующиеся в Доктрине ИБ?
69. Каковы стратегические цели и задачи обеспечения ИБ РФ.
70. Содержание национальной стратегии развития ИИ в РФ.
71. Поясните суть терминов: искусственный интеллект (ИИ), технология ИИ, перспективные методы и смежные области использования ИИ.
72. Содержание национальной стратегии развития ИИ в РФ.
73. Установите соотношение опасности внутренних и внешних угроз информационной безопасности (ИБ), перечислить их и укажите самые распространенные каналы утечки конфиденциальной информации.
74. Перечислите средства ИБ, используемые в РФ, предложите свои пути защиты от утечек информации.
75. Сущность правовой защиты информации (ЗИ) и ее связь со стратегией и доктриной национальной безопасности РФ.
76. Основные положения Конституции и законы РФ, предписывающие права, обязанности и действия граждан России в области ИБ.
77. Опишите сведения, отнесенные к государственной тайне, имеющие конфиденциальный характер, а также наказания при их разглашении.
78. Основные положения, термины и определения дисциплины ИБ.
79. Техническая защита конфиденциальной и секретной информации, ее место и роль в развитии современной экономики.

80. Как и для чего используется перечень сведения конфиденциального характера для экономического объекта.
81.Основные требования и рекомендации по ЗИ от утечки информации.
82. Перечислите и обоснуйте основные мероприятия для ЗИ от утечек по техническим каналам.
83. Сформулируйте условия безопасного размещения защищаемого помещения.
84. Опишите организационные мероприятия по ЗИ от утечек за счет побочных электромагнитных излучений и наводок (ПЭМИН).
85. Перечислите организационные мероприятия, направленные на исключение несанкционированного доступа в защищаемое помещения.
86. Федеральные органы исполнительной власти РФ, осуществляющие лицензирование.
87. Опишите сущность лицензирования деятельности по технической защите конфиденциальной информации (ТЗКИ).
88. Положение о лицензировании деятельности по технической защите конфиденциальной информации (ТЗКИ). Лицензионные требования и условия осуществления деятельности по ТЗКИ.
89. Перечислите документы, направляемые для получения лицензии на осуществление деятельности по ТЗКИ.
90. Опишите содержание документов, направляемых для получения лицензии.

Очно-заочная форма обучения, Седьмой семестр, Зачет
Контролируемые ИДК: ПК-П6.1
Вопросы/Задания:

1. Вопросы к зачету.

1. Международные стандарты информационной безопасности.
2. Концепция информационной безопасности страны.
3. Место информационной безопасности в социально-экономических системах.
4. Основные нормативные руководящие документы, касающиеся государственной тайны.
5. Виды возможных нарушений информационной системы.
6. Актуальность проблемы информационной безопасности.
7. Модели безопасности и их применение.
8. Классификация методов ИБ от несанкционированного доступа (НСД).
9. Классификация средств ИБ от НСД.
10. Механизмы ИБ от НСД.
11. Государственные требования к системам ИБ.
12. Концепция ИБ от НСД.
13. Требования к криптографическим средствам систем ЗИ (СЗИ).
14. Показатели защищенности средств вычислительной техники (СВТ) от НСД.
15. Классификация компьютерных систем и требования ИБ к ним.
16. Использование защищенных компьютерных систем (КС).
17. Методы контроля доступа к ресурсам КС.
18. Способы фиксации факта доступа.
19. Структура и функции подсистемы контроля доступа программ и пользователей.
20. Средства активного аудита компьютерных систем.
21. Идентификация и аутентификация субъектов и объектов КС.
22. Основные подходы к защите данных от НСД.
23. Модели управления доступом.
24. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.
25. Защита алгоритма шифрования и программно-аппаратные средства

шифрования.
26. Построение аппаратных компонент криптозащиты данных.
27. Взаимодействие прикладных программ и программы злоумышленника.
28. Классификация разрушающих программных средств и их воздействий.
29. Компьютерные вирусы (КВ) как класс разрушающих программных воздействий.
30. Сущность, проявление, классификация КВ.
31. Необходимые и достаточные условия недопущения разрушающих программных воздействий.
32. Организационные средства защиты от КВ.
33. Роль морально-этических факторов в устранении угрозы разрушающих программных воздействий.
34. Проблема обеспечение целостности информации.
35. Способы обеспечения целостности информации.
36. Электронная цифровая подпись.
37. Криптографические хэш-функции. Схемы вычисления хэш-функции.
38. Методы криптографии и задачи, решаемые криптографическими средствами в КС.
39. Алгоритмы криптографических преобразований, их характеристики.
40. Методы и средства ограничения доступа к компонентам компьютеров.
41. Построение средств ЗИ для персонального компьютера (ПК).
42. Перечень и характеристики сертифицированных программно-аппаратных средств систем ЗИ от НСД для ПК.
43. Особенности ЗИ в вычислительных сетях.
44. Механизмы реализации атак на вычислительные сети.
45. Определение перечня защищаемых ресурсов и их критичности.
46. Определение категорий персонала, на которые распространяется политика безопасности.
47. Определение угроз ИБ.
48. Формирование требований к построению системы ЗИ.
49. Определение уязвимости КС и выбор средств ЗИ.
50. Антивирусные программные комплексы.
51. Настройка и применение антивирусных программ.
52. Исследование результатов воздействия КВ на программы в ОС.
53. Исследование результатов работы антивирусных программ.
54. Алгоритмы электронной цифровой подписи.
55. Основные положения национальной стратегии развития искусственного интеллекта на период до 2030 года.
56. Цель доктрины информационной безопасности РФ (от5.12.2016 №646).
57. Каковы стратегические цели и основные направления обеспечения информационной безопасности (ИБ).
58. Дайте определения угрозам и обеспечению ИБ.
59. Дайте определение силам и средствам обеспечения ИБ.
60. Раскройте содержание терминов система обеспечения ИБ и ее информационной инфраструктуры.
61. Каковы стратегические цели и задачи обеспечения ИБ РФ.
62. Основные негативные факторы, влияющие на состояние международной ИБ.
63. Основные направления обеспечения ИБ в экономической сфере.
64. Основные направления обеспечения ИБ в области науки, технологий и образовании.
65. Принципы работы государственных органов по обеспечению ИБ.
66. Задачи государственных органов в рамках деятельности по обеспечению ИБ.
67. Где и как осуществляется процесс реализации доктрины ИБ РФ.
68. Раскройте основные понятия и определения использующиеся в Доктрине ИБ?
69. Каковы стратегические цели и задачи обеспечения ИБ РФ.
70. Содержание национальной стратегии развития ИИ в РФ.
71. Поясните суть терминов: искусственный интеллект (ИИ), технология ИИ, перспективные

методы и смежные области использования ИИ.
72. Содержание национальной стратегии развития ИИ в РФ.
73. Установите соотношение опасности внутренних и внешних угроз информационной безопасности (ИБ), перечислить их и укажите самые распространенные каналы утечки конфиденциальной информации.
74. Перечислите средства ИБ, используемые в РФ, предложите свои пути защиты от утечек информации.
75. Сущность правовой защиты информации (ЗИ) и ее связь со стратегией и доктриной национальной безопасности РФ.
76. Основные положения Конституции и законы РФ, предписывающие права, обязанности и действия граждан России в области ИБ.
77. Опишите сведения, отнесенные к государственной тайне, имеющие конфиденциальный характер, а также наказания при их разглашении.
78. Основные положения, термины и определения дисциплины ИБ.
79. Техническая защита конфиденциальной и секретной информации, ее место и роль в развитии современной экономики.
80. Как и для чего используется перечень сведения конфиденциального характера для экономического объекта.
81.Основные требования и рекомендации по ЗИ от утечки информации.
82. Перечислите и обоснуйте основные мероприятия для ЗИ от утечек по техническим каналам.
83. Сформулируйте условия безопасного размещения защищаемого помещения.
84. Опишите организационные мероприятия по ЗИ от утечек за счет побочных электромагнитных излучений и наводок (ПЭМИН).
85. Перечислите организационные мероприятия, направленные на исключение несанкционированного доступа в защищаемое помещения.
86. Федеральные органы исполнительной власти РФ, осуществляющие лицензирование.
87. Опишите сущность лицензирования деятельности по технической защите конфиденциальной информации (ТЗКИ).
88. Положение о лицензировании деятельности по технической защите конфиденциальной информации (ТЗКИ). Лицензионные требования и условия осуществления деятельности по ТЗКИ.
89. Перечислите документы, направляемые для получения лицензии на осуществление деятельности по ТЗКИ.
90. Опишите содержание документов, направляемых для получения лицензии.

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Информационная безопасность: учебное пособие / Лойко В. И., Лаптев В. Н., Аршинов Г. А., Лаптев С. Н.. - Краснодар: КубГАУ, 2020. - 332 с. - 978-5-907346-50-5. - Текст: электронный. // RuSpLAN: [сайт]. - URL: https://e.lanbook.com/img/cover/book/254168.jpg (дата обращения: 21.02.2024). - Режим доступа: по подписке

Дополнительная литература

1. Вестник РГГУ. Серия "Информатика. Информационная безопасность. Математика", 2020, № 4: научный журнал / Москва: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Российский государственный гуманитарный университет", 2020. - 71 с. - Текст: электронный. // Общество с ограниченной ответственностью «ЗНАНИУМ»: [сайт]. - URL: https://znanium.com/cover/1478/1478379.jpg (дата обращения: 20.02.2024). - Режим доступа: по подписке

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. https://elibrary.ru/ - Научная электронная библиотека «eLIBRARY.RU»

Ресурсы «Интернет»

1. http://www.iprbookshop.ru/ - IPRbook

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Не используется.

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Университет располагает на праве собственности или ином законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации программы бакалавриата, специлитета, магистратуры по Блоку 1 "Дисциплины (модули)" и Блоку 3 "Государственная итоговая аттестация" в соответствии с учебным планом.
Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне его. Условия для функционирования электронной информационно-образовательной среды могут быть созданы с использованием ресурсов иных организаций.

Лекционный зал

221гл
Облучатель-рециркулятор воздуха 600 - 1 шт.

401мх
киноэкран ScreeerMedia 180*180 - 0 шт.
Сплит-система настенная QuattroClima Effecto Standard QV/QN-ES24WA - 0 шт.

Компьютерный класс

223гл
Интерактивная панель Samsung - 1 шт.
Компьютер персональный Aquarius i5/4Gb/500Gb/21,5" - 1 шт.
Компьютер персональный i3/2GB/500Gb/21,5" - 1 шт.
Сплит-система LS-H12KPA2/LU-H12KPA2 - 1 шт.

226гл
Интерактивная панель Samsung - 1 шт.

Персональный компьютер HP 6300 Pro SFF/Core i3-3220/4GB/500GB/NoODD/Win7Pro - 1 шт.

Сплит-система LS-H12KPA2/LU-H12KPA2 - 1 шт.

Лаборатория

306зр

Доска интерактивная (доска, проектор, крепления, 87 дюймов) - 0 шт.

Компьютер LENOVO - 0 шт.

Микроскоп Микромед-1 вар 2-20 - 0 шт.

Микроскоп стереоскопический Модель СМ-1 (бинокуляр) - 0 шт.

Микроскоп стереоскопический (бинокуляр) МСП-1 вариант - 2 - 0 шт.

Сплит-система LS-H24KPA2/LU-H24KPA2 - 0 шт.

9. Методические указания по освоению дисциплины (модуля)

Учебная работа по направлению подготовки осуществляется в форме контактной работы с преподавателем, самостоятельной работы обучающегося, текущей и промежуточной аттестаций, иных формах, предлагаемых университетом. Учебный материал дисциплины структурирован и его изучение производится в тематической последовательности. Содержание методических указаний должно соответствовать требованиям Федерального государственного образовательного стандарта и учебных программ по дисциплине. Самостоятельная работа студентов может быть выполнена с помощью материалов, размещенных на портале поддержки Moodl.

Методические указания по формам работы

Лекционные занятия

Передача значительного объема систематизированной информации в устной форме достаточно большой аудитории. Дает возможность экономно и систематично излагать учебный материал. Обучающиеся изучают лекционный материал, размещенный на портале поддержки обучения Moodl.

Лабораторные занятия

Практическое освоение студентами научно-теоретических положений изучаемого предмета, овладение ими техникой экспериментирования в соответствующей отрасли науки. Лабораторные занятия проводятся с использованием методических указаний, размещенных на образовательном портале университета.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

Для инвалидов и лиц с ОВЗ может изменяться объём дисциплины (модуля) в часах, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося (при этом не увеличивается количество зачётных единиц, выделенных на освоение дисциплины).

Фонды оценочных средств адаптируются к ограничениям здоровья и восприятия информации обучающимися.

Основные формы представления оценочных средств – в печатной форме или в форме электронного документа.

Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением зрения:

– устная проверка: дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.;

– с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, дистанционные формы, если позволяет острота зрения - графические работы и др.;
– при возможности письменная проверка с использованием рельефно-точечной системы Брайля, увеличенного шрифта, использование специальных технических средств (тифлотехнических средств): контрольные, графические работы, тестирование, домашние задания, эссе, отчеты и др.
Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением слуха:
– письменная проверка: контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.;
– с использованием компьютера: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы и др.;
– при возможности устная проверка с использованием специальных технических средств (аудиосредств, средств коммуникации, звукоусиливающей аппаратуры и др.): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.
Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением опорно-двигательного аппарата:
– письменная проверка с использованием специальных технических средств (альтернативных средств ввода, управления компьютером и др.): контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.;
– устная проверка, с использованием специальных технических средств (средств коммуникаций): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.;
– с использованием компьютера и специального ПО (альтернативных средств ввода и управления компьютером и др.): работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы предпочтительнее обучающимся, ограниченным в передвижении и др.
Адаптация процедуры проведения промежуточной аттестации для инвалидов и лиц с ОВЗ.
В ходе проведения промежуточной аттестации предусмотрено:
– предъявление обучающимся печатных и (или) электронных материалов в формах, адаптированных к ограничениям их здоровья;
– возможность пользоваться индивидуальными устройствами и средствами, позволяющими адаптировать материалы, осуществлять приём и передачу информации с учетом их индивидуальных особенностей;
– увеличение продолжительности проведения аттестации;
– возможность присутствия ассистента и оказания им необходимой помощи (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с преподавателем).
Формы промежуточной аттестации для инвалидов и лиц с ОВЗ должны учитывать индивидуальные и психофизические особенности обучающегося/обучающихся по АОПОП ВО (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями зрения:
– предоставление образовательного контента в текстовом электронном формате, позволяющем переводить плоскопечатную информацию в аудиальную или тактильную форму;
– возможность использовать индивидуальные устройства и средства, позволяющие адаптировать материалы, осуществлять приём и передачу информации с учетом индивидуальных особенностей и состояния здоровья студента;
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;
– использование чёткого и увеличенного по размеру шрифта и графических объектов в мультимедийных презентациях;
– использование инструментов «лупа», «прожектор» при работе с интерактивной доской;
– озвучивание визуальной информации, представленной обучающимся в ходе занятий;

– обеспечение раздаточным материалом, дублирующим информацию, выводимую на экран;
– наличие подписей и описания у всех используемых в процессе обучения рисунков и иных графических объектов, что даёт возможность перевести письменный текст в аудиальный;
– обеспечение особого речевого режима преподавания: лекции читаются громко, разборчиво, отчётливо, с паузами между смысловыми блоками информации, обеспечивается интонирование, повторение, акцентирование, профилактика рассеивания внимания;
– минимизация внешнего шума и обеспечение спокойной аудиальной обстановки;
– возможность вести запись учебной информации студентами в удобной для них форме (аудиально, аудиовизуально, на ноутбуке, в виде пометок в заранее подготовленном тексте);
– увеличение доли методов социальной стимуляции (обращение внимания, апелляция к ограничениям по времени, контактные виды работ, групповые задания и др.) на практических и лабораторных занятиях;
– минимизирование заданий, требующих активного использования зрительной памяти и зрительного внимания;
– применение поэтапной системы контроля, более частый контроль выполнения заданий для самостоятельной работы.
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями опорно-двигательного аппарата (маломобильные студенты, студенты, имеющие трудности передвижения и патологию верхних конечностей):
– возможность использовать специальное программное обеспечение и специальное оборудование и позволяющее компенсировать двигательное нарушение (коляски, ходунки, трости и др.);
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;
– применение дополнительных средств активизации процессов запоминания и повторения;
– опора на определенные и точные понятия;
– использование для иллюстрации конкретных примеров;
– применение вопросов для мониторинга понимания;
– разделение изучаемого материала на небольшие логические блоки;
– увеличение доли конкретного материала и соблюдение принципа от простого к сложному при объяснении материала;
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;
– увеличение доли методов социальной стимуляции (обращение внимания, аппеляция к ограничениям по времени, контактные виды работ, групповые задания др.);
– обеспечение беспрепятственного доступа в помещения, а также пребывания них;
– наличие возможности использовать индивидуальные устройства и средства, позволяющие обеспечить реализацию эргономических принципов и комфортное пребывание на месте в течение всего периода учёбы (подставки, специальные подушки и др.).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями слуха (глухие, слабослышащие, позднооглохшие):
– предоставление образовательного контента в текстовом электронном формате, позволяющем переводить аудиальную форму лекции в плоскопечатную информацию;
– наличие возможности использовать индивидуальные звукоусиливающие устройства и сурдотехнические средства, позволяющие осуществлять приём и передачу информации; осуществлять взаимообратный перевод текстовых и аудиофайлов (блокнот для речевого ввода), а также запись и воспроизведение зрительной информации;
– наличие системы заданий, обеспечивающих систематизацию вербального материала, его схематизацию, перевод в таблицы, схемы, опорные тексты, глоссарий;
– наличие наглядного сопровождения изучаемого материала (структурно-логические схемы, таблицы, графики, концентрирующие и обобщающие информацию, опорные конспекты, раздаточный материал);
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;

– обеспечение практики опережающего чтения, когда студенты заранее знакомятся с материалом и выделяют незнакомые и непонятные слова и фрагменты;
– особый речевой режим работы (отказ от длинных фраз и сложных предложений, хорошая артикуляция; четкость изложения, отсутствие лишних слов; повторение фраз без изменения слов и порядка их следования; обеспечение зрительного контакта во время говорения и чуть более медленного темпа речи, использование естественных жестов и мимики);
– чёткое соблюдение алгоритма занятия и заданий для самостоятельной работы (называние темы, постановка цели, сообщение и запись плана, выделение основных понятий и методов их изучения, указание видов деятельности студентов и способов проверки усвоения материала, словарная работа);
– соблюдение требований к предъявляемым учебным текстам (разбивка текста на час¬ти; выделение опорных смысловых пунктов; использование наглядных средств);
– минимизация внешних шумов;
– предоставление возможности соотносить вербальный и графический материал; комплексное использование письменных и устных средств коммуникации при работе в группе;
– сочетание на занятиях всех видов речевой деятельности (говорения, слушания, чтения, письма, зрительного восприятия с лица говорящего).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с прочими видами нарушений (ДЦП с нарушениями речи, заболевания эндокринной, центральной нервной и сердечно-сосудистой систем, онкологические заболевания):
– наличие возможности использовать индивидуальные устройства и средства, позволяющие осуществлять приём и передачу информации;
– наличие системы заданий, обеспечивающих систематизацию вербального материала, его схематизацию, перевод в таблицы, схемы, опорные тексты, глоссарий;
– наличие наглядного сопровождения изучаемого материала;
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;
– обеспечение практики опережающего чтения, когда студенты заранее знакомятся с материалом и выделяют незнакомые и непонятные слова и фрагменты;
– предоставление возможности соотносить вербальный и графический материал; комплексное использование письменных и устных средств коммуникации при работе в группе;
– сочетание на занятиях всех видов речевой деятельности (говорения, слушания, чтения, письма, зрительного восприятия с лица говорящего);
– предоставление образовательного контента в текстовом электронном формате;
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;
– возможность вести запись учебной информации студентами в удобной для них форме (аудиально, аудиовизуально, в виде пометок в заранее подготовленном тексте);
– применение поэтапной системы контроля, более частый контроль выполнения заданий для самостоятельной работы;
– стимулирование выработки у студентов навыков самоорганизации и самоконтроля;
– наличие пауз для отдыха и смены видов деятельности по ходу занятия.

10. Методические рекомендации по освоению дисциплины (модуля)

Основными видами учебных занятий являются: лекции, лабораторные работы, самостоятельная работа обучающихся и консультации.
Лекции составляют основу теоретического обучения и должны давать систематизированные основы научных знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей профессиональной отрасли, области науки и техники, профессиональной (служебной) деятельности, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

В ходе лекционных занятий у обучающихся формируется теоретическая база профессиональных компетенций.
Лекции читаются заведующим кафедры, профессором, доцентами и старшими преподавателями, как правило, для лекционных потоков.
Лабораторные работы имеют целью практическое освоение обучающимися научно-теоретических положений изучаемой дисциплины, овладение ими техникой экспериментальных исследований и анализа полученных результатов, привитие навыков работы с вычислительной техникой. По выполнении лабораторной работы обучающиеся представляют отчет и защищают его.
Самостоятельная работа является частью учебной деятельности обучающихся по освоению основной учебной программы и организуется в целях закрепления и углубления полученных знаний, умений и навыков, поиска и приобретения новых знаний, а также выполнения учебных заданий, подготовки к предстоящим занятиям, зачету.
Контроль успеваемости и качества подготовки обучающихся по дисциплине включает текущий контроль успеваемости и промежуточную аттестацию обучающихся.
Текущий контроль успеваемости осуществляется для проверки хода и качества усвоения учебного материала, стимулирования учебной деятельности обучающихся, совершенствования методики проведения занятий и проводится в ходе всех видов занятий в форме, предусмотренной избранной преподавателем. Результаты текущего контроля успеваемости отражаются в журнале учета учебных занятий.
Промежуточная аттестация осуществляется в целях определения степени достижения учебных целей по дисциплине и проводится в 7 семестре в форме зачета.