

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

ИНСТИТУТ ЦИФРОВОЙ ЭКОНОМИКИ И ИННОВАЦИЙ

УТВЕРЖДАЮ

Директор института цифровой
экономики и инноваций,

профессор

В. А. Семидоцкий

29 мая 2023 г.



Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(Адаптированная рабочая программа для лиц с ограниченными возможностями
здоровья и инвалидов, обучающихся по адаптированным основным
профессиональным образовательным программам высшего образования)

Направление подготовки
38.03.01 Экономика

Направленность
Цифровая экономика

Уровень высшего образования
бакалавриат

Форма обучения
очная

Краснодар
2023

Рабочая программа дисциплины «Информационная безопасность» разработана на основе федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 38.03.01 Экономика, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 12 августа 2020 г. № 954.

Авторы:

доктор экон. наук, профессор



В. А. Семидоцкий

Рабочая программа обсуждена и рекомендована к утверждению решением кафедры цифровой экономики от 17.04.2023 г., протокол № 9.

доктор экон. наук, профессор



В. А. Семидоцкий

Рабочая программа одобрена на заседании методической комиссии института цифровой экономики и инноваций от 11.05.2023, протокол № 9.

Председатель
методической комиссии
доктор экон. наук, профессор



В. А. Семидоцкий

Руководитель
основной профессиональной
образовательной программы
доктор экон. наук, профессор



В. А. Семидоцкий

1 Цель и задачи освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачи

- формирование умения обеспечить защиту информации и объектов информатизации;
- формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли;
- формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов;
- формирование навыков обеспечения защиты объектов интеллектуальной собственности, результатов исследований и разработок как коммерческой тайны предприятия.

2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

В результате освоения дисциплины формируются следующие компетенции:

ПК-5. Способность выявлять потребности и формировать задачи управления ИТ-инфраструктурой организации, проводить анализ результатов и осуществлять контроль за реализацией поставленных задач

3 Место дисциплины в структуре ОПОП ВО.

«Информационная безопасность» является дисциплиной части, формируемой участниками образовательных отношений ОПОП подготовки обучающихся по направлению подготовки 38.03.01 Экономика, направленность Цифровая экономика.

4 Объем дисциплины (108 часа, 3 зачетные единицы)

Виды учебной работы	Объем, часов
	Очная форма обучения
Контактная работа	49
в том числе:	
– аудиторная по видам учебных занятий	48
– лекции	32
– практические	16
– внеаудиторная	1
– зачет	1
Самостоятельная работа	59
Итого по дисциплине	108

5 Содержание дисциплины

По итогам изучаемой дисциплины обучающиеся сдают зачет
Дисциплина изучается на 3 курсе, в 5 семестре по учебному плану очной формы обучения.

Содержание и структура дисциплины по очной форме обучения

№ п/п	Тема. Основные вопросы	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)		
				Лекции	Практические занятия	Самостоятельная работа
1	Введение в информационную безопасность Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности	ПК-5	5	4	2	9
2	Правовое обеспечение информационной безопасности Основные нормативно-правовые	ПК-5	5	4	2	9

	акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны					
3	Анализ способов нарушений информационной безопасности. Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем	ПК-5	5	6	2	9
4	Технические средства и методы защиты информации Инженерная защита объектов. Защита информации от утечки по техническим каналам.	ПК-5	5	6	4	10
5	Программно-аппаратные средства и методы обеспечения информационной безопасности Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи. Использование средств стеганографии для защиты файлов. Изучение настроек средств антивирусной защиты информации.	ПК-5	5	6	4	10
6	Криптографические методы защиты информации Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Создание защищенного канала связи средствами виртуальной частной сети.	ПК-5	5	6	4	10
Итого				32	16	59

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

6.1 Методические указания (собственные разработки)

7 Фонд оценочных средств для проведения промежуточной аттестации

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП ВО

Номер семестра*	Этапы формирования и проверки уровня сформированности компетенций по дисциплинам, практикам в процессе освоения ОПОП ВО
ПК-5. Способность выявлять потребности и формировать задачи управления ИТ-инфраструктурой организации, проводить анализ результатов и осуществлять контроль за реализацией поставленных задач	
1	Цифровизация социально-экономических процессов
2	Основы программирования
3	Программирование
4	Базы данных
4	Системный анализ
4	Учебная практика: Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)
5	<i>Информационная безопасность</i>
6	Цифровая логистика
7	Облачные технологии
7	Цифровые технологии на финансовых рынках
8	Цифровые рынки
6	Производственная практика: Практика по получению профессиональных умений и опыта профессиональной деятельности
8	Производственная практика: Преддипломная практика
8	Подготовка к процедуре защиты и защита выпускной квалификационной работы

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

Планируемые результаты освоения компетенции	Уровень освоения				Оценочное средство
	неудовлетво р ительно (минимал ьный не достигнут)	удовлетворительн о(минимальный пороговый)	хорошо (средний)	отлично (высокий)	
ПК-5. Способность выявлять потребности и формировать задачи управления ИТ-инфраструктурой организации, проводить анализ результатов и осуществлять контроль за реализацией поставле нных задач					
ПК-5.1. Организует процесс выявления потребностей в ИТ-инфраструктуре и формирует задачи управления ИТ-инфраструктуро й на основе выявленных потребностей и согласование этих задач с заинтересованны ми лицами ПК-5.2. Осуществляет инициирование и планирование выполнения задач управления ИТ-инфраструктуро й и согласование с заинтересованны ми лицами этих планов	Уровень знаний ниже минималь ных требовани й, имели место грубые ошибки При решении стандартн ых задач не продемонс трирован ы основные умения , имели место грубые ошибки, не продемонс трирован ы базовые навыки	Минимально допустимый уровень знаний , допущено много негрубых ошибок. Продемонстри рованы основные умения , решены типовые задачи. Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Уровень знаний в объеме, соответству ющем программе подготовки, допущено несколько негрубых ошибок. Продемонст рированы все основные умения , решены все основные задачи с негрубыми ошибками, продемонстри рованы базовые навыки при решении стандартнх задач	Уровень знаний в объеме, соответст вующем программ е подготов ки, без ошибок. Продемо нстриров аны все основные умения , решены все основные задачи с отдельны м и несущест венными недочета ми, Продемо нстриров аны навыки при решении нестанда ртных задач	Устный опрос, решение задач, реферат, тест

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций в процессе освоения ОПОП ВО

Тесты (примеры)

1. Кто является основным ответственным за определение уровня классификации информации?
 - а) Руководитель среднего звена
 - б) Высшее руководство
 - в) Владелец
 - г) Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
 - а) Сотрудники
 - б) Хакеры
 - в) Атакующие
 - г) Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
 - а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
 - б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
 - в) Улучшить контроль за безопасностью этой информации
 - г) Снизить уровень классификации этой информации

4. Кто в конечном счете несет ответственность за гарантию того, что данные классифицированы и защищены?
 - а) Владельцы данных
 - б) Пользователи
 - в) Администраторы
 - г) Руководство

5. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
 - а) Поддержка высшего руководства
 - б) Эффективные защитные меры и методы их внедрения
 - в) Актуальные и адекватные политики и процедуры безопасности
 - г) Проведение тренингов по безопасности для всех сотрудников

6. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

- а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
- б) Когда риски не могут быть приняты во внимание по политическим соображениям
- в) Когда необходимые защитные меры слишком сложны
- г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

7. Что такое политики безопасности?

- а) Пошаговые инструкции по выполнению задач безопасности б) Общие руководящие требования по достижению определенного уровня безопасности
- в) Широкие, высокоуровневые заявления руководства
- г) Детализированные документы по обработке инцидентов безопасности

8. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

- а) Анализ рисков
- б) Анализ затрат / выгод в) Результаты ALE
- г) Выявление уязвимостей и угроз, являющихся причиной риска

9. Тактическое планирование – это:

- а) Среднесрочное планирование б) Долгосрочное планирование в) Ежедневное планирование
- г) Планирование на 6 месяцев

10. Что является определением воздействия (exposure) на безопасность?

- а) Нечто, приводящее к ущербу от угрозы
- б) Любая потенциальная опасность для информации или систем в) Любая недостаток или отсутствие информационной безопасности
- г) Потенциальные потери от угрозы

11. Эффективная программа безопасности требует сбалансированного применения:

- а) Технических и нетехнических методов б) Контрмер и защитных механизмов
- в) Физической безопасности и технических средств защиты г) Процедур безопасности и шифрования

12. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

- а) Внедрение управления механизмами безопасности
- б) Классификацию данных после внедрения механизмов безопасности
- в) Уровень доверия, обеспечиваемый механизмом безопасности
- г) Соотношение затрат / выгод

13. Что из перечисленного не является целью проведения анализа рисков?

- а) Делегирование полномочий
- б) Количественная оценка воздействия потенциальных угроз
- в) Выявление рисков
- г) Определение баланса между воздействием риска и стоимостью необходимых контрмер

14. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

- а) Поддержка
- б) Выполнение анализа рисков
- в) Определение цели и границ
- г) Делегирование полномочий

15. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

- а) Чтобы убедиться, что проводится справедливая оценка
- б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
- в) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
- г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

16. Что является наилучшим описанием количественного анализа рисков?

- а) Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
- б) Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
- в) Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков

г) Метод, основанный на суждениях и интуиции

17. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

а) Стандарты

б) Должный процесс (Due process) в) Должная забота (Due care)

г) Снижение обязательств

18. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

а) Список стандартов, процедур и политик для разработки программы безопасности

б) Текущая версия ISO 17799

в) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях

г) Открытый стандарт, определяющий цели контроля

19. Из каких четырех доменов состоит CobiT?

а) Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

б) Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

в) Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка

г) Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

20. Защита информации от утечки это деятельность по предотвращению:

а) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

б) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; в)

воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

г) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

д) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

21. Естественные угрозы безопасности информации вызваны: а) деятельностью человека; б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения; в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека; г) корыстными устремлениями злоумышленников; д) ошибками при действиях персонала.

22. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

- а) детектор; б) доктор; в) сканер; г) ревизор; д) сторож.

23. Активный перехват информации это перехват, который: а) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

б) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

в) неправомерно использует технологические отходы информационного процесса;

г) осуществляется путем использования оптической техники; д) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

Темы рефератов (примеры)

1. Основные понятия и определения информационной безопасности.

2. Виды и источники угроз безопасности информации

3. Классификация угроз информационной безопасности.

4. Методы и средства защиты информации.

5. Правовые меры обеспечения информационной безопасности.

6. Законодательные и нормативные акты Российской Федерации в области защиты информации.

7. Классификация систем защиты АС согласно документам Федеральной службы по техническому и экспортному контролю России (ранее Гостехкомиссии России).

8 Критерии оценки безопасности компьютерных систем.
«Оранжевая книга».

9. Защита программного обеспечения, основанная на идентификации аппаратного и программного обеспечения.

10. Электронные ключи.

11. Организационно-административные методы защиты информационных систем.

12. Формирование политики безопасности организации

13. Основные принципы формирования пользовательских паролей

14. Идентификация пользователей (назначение и способы реализации).

15. Аутентификация пользователей (назначение и способы реализации).

16. Авторизации пользователей (назначение и способы реализации).

17. Криптографические методы защиты информации.

18. Симметричные криптосистемы.

19. Поточные шифры.

20. Свойства синхронных и асинхронных поточных шифров.

21. Шифры подстановки и перестановки.

22. Блочные шифры.

23. Шифр Файстея.

24. Основные особенности стандарта шифрования РЕБ.

25. Стандарт шифрования ГОСТ 28147-89.

26. Асимметричные криптосистемы

27. Алгоритм шифрования ВЗА.

28. Сравнительная характеристика симметричных и асимметричных алгоритмов шифрования.

29. Реализация алгоритмов шифрования.

30. Электронная цифровая подпись.

31. Виды атак на электронную цифровую подпись.

32. Основные типы криптоаналитических атак.

33. Защита информации в компьютерных сетях.

34. Объекты защиты информации в сети

35. Уровни сетевых атак согласно эталонной модели взаимодействия открытых систем

36. Классификация межсетевых экранов.

37. Схемы подключения межсетевых экранов.

Промежуточная аттестация

Вопросы к зачету:

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Экономическая информация как товар и объект безопасности.
6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
7. Персональные данные и их защита.
8. Информационные угрозы, их виды и причины возникновения.
9. Информационные угрозы для государства.
10. Информационные угрозы для компании.
11. Информационные угрозы для личности (физического лица).
12. Действия и события, нарушающие информационную безопасность.
13. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
14. Способы воздействия информационных угроз на объекты.
15. Внешние и внутренние субъекты информационных угроз.
16. Компьютерные преступления и их классификация.
17. Исторические аспекты компьютерных преступлений и современность.
18. Субъекты и причины совершения компьютерных преступлений.
19. Вредоносные программы, их виды.
20. История компьютерных вирусов и современность.
21. Государственное регулирование информационной безопасности.
22. Деятельность международных организаций в сфере информационной безопасности.
23. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.
24. Доктрина информационной безопасности России.
25. Уголовно-правовой контроль над компьютерной преступностью в России.
26. Федеральные законы по ИБ в РФ.
27. Политика безопасности и ее принципы.
28. Фрагментарный и системный подход к защите информации.
29. Методы и средства защиты информации.
30. Организационное обеспечение ИБ.
31. Организация конфиденциального делопроизводства.

32. Комплекс организационно-технических мероприятий по обеспечению защиты информации.
33. Инженерно-техническое обеспечение компьютерной безопасности.
34. Организационно-правовой статус службы безопасности.
35. Защита информации в Интернете. 3
6. Электронная почта и ее защита.
37. Защита от компьютерных вирусов.
38. «Больные» мобильники и их «лечение».
39. Популярные антивирусные программы и их классификация.
40. Организация системы защиты информации экономических объектов.
41. Криптографические методы защиты информации.
42. Этапы построения системы защиты информации.
43. Оценка эффективности инвестиций в информационную безопасность.
44. План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.
45. Управление информационной безопасностью на государственном уровне.
46. Аудит ИБ автоматизированных банковских систем.
47. Электронная коммерция и ее защита.
48. Менеджмент и аудит информационной безопасности на уровне предприятия.
49. Информационная безопасность предпринимательской деятельности.
50. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Критериями оценки реферата являются: новизна текста, обоснованность выбора источников литературы, степень раскрытия сущности вопроса, соблюдения требований к оформлению.

Оценка «отлично» $\frac{3}{4}$ выполнены все требования к написанию реферата: обозначена проблема и обоснована её актуальность; сделан анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция; сформулированы выводы, тема раскрыта полностью, выдержан объём; соблюдены требования к внешнему оформлению.

Оценка «хорошо» $\frac{3}{4}$ основные требования к реферату выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении.

Оценка «удовлетворительно» $\frac{3}{4}$ имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата; отсутствуют выводы.

Оценка «неудовлетворительно» $\frac{3}{4}$ тема реферата не раскрыта, обнаруживается существенное непонимание проблемы или реферат не представлен вовсе.

Критерии оценки тестовых заданий

Оценка «отлично» выставляется при условии правильного ответа студента не менее чем на 85 % тестовых заданий.

Оценка «хорошо» выставляется при условии правильного ответа студента не менее чем на 70 % тестовых заданий.

Оценка «удовлетворительно» выставляется при условии правильного ответа студента не менее чем на 51 %.

Оценка «неудовлетворительно» выставляется при условии правильного ответа студента менее чем на 50 % тестовых заданий.

Критерии оценки на зачете

Оценка «отлично» выставляется обучающемуся, который обладает всесторонними, систематизированными и глубокими знаниями материала учебной программы, умеет свободно выполнять задания, предусмотренные учебной программой, усвоил основную и ознакомился с дополнительной литературой, рекомендованной учебной программой. Как правило, оценка «отлично» выставляется обучающемуся усвоившему взаимосвязь основных положений и понятий дисциплины в их значении для приобретаемой специальности, проявившему творческие способности в понимании, изложении и использовании учебного материала, правильно обосновывающему принятые решения, владеющему разносторонними навыками и приемами выполнения практических работ.

Оценка «хорошо» выставляется обучающемуся, обнаружившему полное знание материала учебной программы, успешно выполняющему предусмотренные учебной программой задания, усвоившему материал основной литературы, рекомендованной учебной программой. Как правило, оценка «хорошо» выставляется обучающемуся, показавшему систематизированный характер знаний по дисциплине, способному к самостоятельному пополнению знаний

в ходе дальнейшей учебной и профессиональной деятельности, правильно применяющему теоретические положения при решении практических вопросов и задач, владеющему необходимыми навыками и приемами выполнения практических работ.

Оценка «удовлетворительно» выставляется обучающемуся, который показал знание основного материала учебной программы в объеме, достаточном и необходимым для дальнейшей учебы и предстоящей работы по специальности, справился с выполнением заданий, предусмотренных учебной программой, знаком с основной литературой, рекомендованной учебной программой. Как правило, оценка «удовлетворительно»

выставляется обучающемуся, допустившему погрешности в ответах на экзамене или выполнении экзаменационных заданий, но обладающему необходимыми знаниями под руководством преподавателя для устранения этих погрешностей, нарушающему последовательность в изложении учебного материала и испытывающему затруднения при выполнении практических работ. Оценка «неудовлетворительно» выставляется обучающемуся, не знающему основной части материала учебной программы, допускающему принципиальные ошибки в выполнении предусмотренных учебной программой заданий, неуверенно с большими затруднениями выполняющему практические работы. Как правило, оценка «неудовлетворительно» выставляется обучающемуся, который не может продолжить обучение или приступить к деятельности по специальности по окончании университета без дополнительных занятий по соответствующей дисциплине.

Оценка «зачтено» соответствует параметрам любой из положительных оценок («отлично», «хорошо», «удовлетворительно»), а «незачтено» – параметрам оценки «неудовлетворительно»).

8 Перечень основной и дополнительной учебной литературы

Основная учебная литература

1. Информационная безопасность [Электронный ресурс]: Учеб. пособие / Т.Л. Партыка, И.И. Попов. – Издательство ФОРУМ, 2021. - 432 с. – Режим доступа: <https://znanium.com/read?id=364624>
2. Информационная безопасность и защита информации [Электронный ресурс]: Учебное пособие / Е.К. Баранова, А.В. Бабаш – РИОР, 2022. - 336 с. – Режим доступа: <https://znanium.com/read?id=393765>
3. Информационная безопасность [Электронный ресурс]: Учебное пособие / С.В. Озерский, И.В. Попов, М.В. Рычаго, Н.И.

Улендеева - Самарский юридический институт ФСИН России, 2019. - 84 с. –
Режим доступа: <https://znanium.com/read?id=358668>

Дополнительная учебная литература

1. Информационная безопасность. История специальных методов криптографической деятельности [Электронный ресурс]: учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин —РИОР, 2022. — 236 с. - Режим доступа: <https://znanium.com/read?id=388319>

2. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. — Издательский дом ФОРУМ, 2021. — 416 с.— Режим доступа: <https://znanium.com/read?id=364622>

3. Защита информации и информационная безопасность [Электронный ресурс]: учебное пособие / Ю.Н. Сычев — НИЦ Инфра- М, 2022. — 201 с. — Режим доступа: <https://znanium.com/read?id=388766>

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень ЭБС

№	Наименование	Тематика	Ссылка
1	Znaniy.com*	Универсальная	https://znanium.com/
	IPRbook*	Универсальная	http://www.iprbookshop.ru/
	Образовательный портал КубГАУ*	Универсальная	https://edu.kubsau.ru/

Перечень Интернет сайтов:

- ГАРАНТ - Законодательство (кодексы, законы, указы, постановления) РФ, аналитика, комментарии, практика [Электронный ресурс]. – Режим доступа: <http://www.garant.ru> , свободный. – Загл. с экрана;
- «Консультант Плюс» - законодательство РФ: кодексы, законы, указы, постановления Правительства Российской Федерации, нормативные акты [Электронный ресурс]. – Режим доступа: <http://www.consultant.ru> , свободный. – Загл. с экрана;
- eLIBRARY.RU - научная электронная библиотека [Электронный ресурс]. – Режим доступа: <http://elibrary.ru>, свободный. – Загл. с экрана.

10 Методические указания для обучающихся по освоению дисциплины

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

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине позволяют:

- обеспечить взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет»;
- фиксировать ход образовательного процесса, результатов промежуточной аттестации по дисциплине и результатов освоения образовательной программы;
- организовать процесс образования путем визуализации изучаемой информации посредством использования презентационных технологий.

Перечень программного обеспечения

№	Наименование	Краткое описание
1	Microsoft Windows	Операционная система
2	Microsoft Office (включает Word, Excel, PowerPoint)	Пакет офисных приложений

Перечень профессиональных баз данных и информационных справочных систем

№	Наименование	Тематика
1	Научная электронная библиотека eLibrary	Универсальная
2	Гарант	Правовая
3	КонсультантПлюс	Правовая

Доступ к сети Интернет

Доступ к сети Интернет, доступ в электронную информационно-образовательную среду университета.

12 Материально-техническое обеспечение для обучения по дисциплине для лиц с ОВЗ и инвалидов

Входная группа в главный учебный корпус и корпус зооинженерного факультета оборудованы пандусом, кнопкой вызова, тактильными табличками, опорными поручнями, предупреждающими знаками, доступным расширенным входом, в корпусе есть специально оборудованная санитарная комната. Для перемещения инвалидов и ЛОВЗ в помещении имеется передвижной гусеничный ступенькоход. Корпус оснащен противопожарной звуковой и визуальной сигнализацией.

Планируемые помещения для проведения всех видов учебной деятельности

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики,	Наименование помещений для проведения всех видов учебной деятельности, предусмотренных учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня	Адрес (местоположение) помещений для проведения всех видов учебной деятельности,
--------------	---	---	---

	иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	предусмотренных учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	Информационная безопасность	<p>Помещение №221 ГУК, площадь – 101 м²; посадочных мест – 95; учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы, в том числе для обучающихся с инвалидностью и ОВЗ.</p> <p>специализированная мебель (учебная доска, учебная мебель), в том числе для обучающихся с инвалидностью и ОВЗ;</p> <p>технические средства обучения, наборы демонстрационного оборудования и учебно-наглядных пособий (ноутбук, проектор, экран), в том числе для обучающихся с инвалидностью и ОВЗ;</p> <p>программное обеспечение.</p>	350044, Краснодарский край, г. Краснодар, ул. им. Калинина, 13
2	Информационная безопасность	<p>Помещение №114 ЗОО, площадь — 43м²; посадочных мест – 25; учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы, в том числе для обучающихся с инвалидностью и ОВЗ.</p> <p>специализированная мебель (учебная доска, учебная мебель), в том числе для обучающихся с инвалидностью и ОВЗ</p>	350044, Краснодарский край, г. Краснодар, ул. им. Калинина, 13

13 Особенности организации обучения лиц с ОВЗ и инвалидов

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

Категории студентов с ОВЗ и инвалидностью	Форма контроля и оценки результатов обучения
<i>С нарушением зрения</i>	<p>– устная проверка: дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.;</p> <p>– 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.;</p> <p>при возможности письменная проверка с использованием рельефно- точечной системы Брайля, увеличенного шрифта, использование специальных технических средств (тифлотехнических средств): контрольные, графические работы, тестирование, домашние</p>

	задания, эссе, отчеты и др.
<i>С нарушением слуха</i>	<ul style="list-style-type: none"> – 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.
<i>С нарушением опорно-двигательного аппарата</i>	<ul style="list-style-type: none"> – 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 АООП ВО (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).

Специальные условия, обеспечиваемые в процессе преподавания дисциплины

Студенты с нарушениями зрения

- предоставление образовательного контента в текстовом электронном формате, позволяющем переводить плоскостную 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.

Студенты 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, апелляция к ограничениям по времени, контактные виды работ, групповые задания др.);
- обеспечение беспрепятственного доступа в помещения, а также пребывания в 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.).

Студенты с нарушениями слуха (глухие, слабослышащие, позднооглохшие)

- предоставление образовательного контента в текстовом электронном формате, позволяющем переводить аудиальную форму лекции в плоскостную информацию;
- наличие возможности использовать индивидуальные звукоусиливающие устройства и сурдотехнические средства, позволяющие осуществлять приём и передачу информации; осуществлять взаимобратный 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; чёткость 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 части; 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).

Студенты 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.

