

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Юридический факультет имени А.А. Хмырова



УТВЕРЖДАЮ:

Проректор по учебной работе,
качеству образования – первый
проректор

Хагуров А.Т.

05

2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.17 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Специальность 40.04.05 Судебная и прокурорская деятельность

Специализация Судебная деятельность

Форма обучения очная, заочная

Квалификация юрист

Краснодар 2025

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по специальности 40.05.04 «Судебная и прокурорская деятельность», утвержденную приказом Министерства науки и высшего образования Российской Федерации от «31» августа 2020 г. №1138.

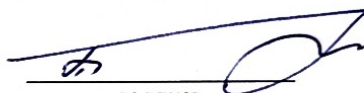
Программу составил:

Г.А. Маркосян, доцент кафедры криминалистики
и правовой информатики, к.э.н.


подпись

Рабочая программа дисциплины «Информационная безопасность» утверждена на заседании кафедры криминалистики и правовой информатики протокол № 10 от «28» апреля 2025 г.

А.В. Руденко, заведующий кафедрой криминалистики
и правовой информатики, д-р юрид. наук, профессор


подпись

Утверждена на заседании учебно-методической комиссии
юридического факультета имени А.А. Хмырова
протокол № 9 от «22» мая 2025 г.

Председатель УМК факультета Прохорова М.Л.


подпись

Рецензенты:

Р.Г. Мартыненко, руководитель отдела криминалистики следственного управления Следственного комитета Российской Федерации по Краснодарскому краю, полковник юстиции, кандидат юридических наук.

Н.Н. Щелочков, заместитель председателя Первомайского районного суда г.Краснодара, кандидат юридических наук.

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Целью освоения учебной дисциплины «Информационная безопасность» является формирование у обучающихся профессиональных компетенций в процессе изучения различных аспектов защиты информации для последующего применения знаний и навыков в профессиональной деятельности юриста.

1.2 Задачи дисциплины

- систематизация, формализация и расширение знаний по основным положениям теории информации, информационной безопасности и стандартами шифрования;
- изучение математических основ защиты информации; а так же методов, средств и инструментов шифрования, применяемых в сфере информационных технологий и бизнеса;
- дать студенту достаточно прочные представления о информационной безопасности, включая аппаратную часть и математическое обеспечение;
- привитие навыков работы с методами шифрования и криптоанализа;
- формирование современной культуры программирования.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к части Блока 1 «Дисциплины» учебного плана, формируемой участниками образовательных отношений. До изучения данной дисциплины обучающиеся должны иметь представления о государственно-правовых явлениях и процессах из курса информационных технологий, информатика.

Дисциплина «Информационная безопасность» является базовой для успешного прохождения и освоения практик, формирующих профессиональные навыки обучающихся, прохождения государственной итоговой аттестации, а также для последующего успешного обучения в аспирантуре.

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора*	Результаты обучения по дисциплине
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия.	
ИУК-4.1. Устанавливает взаимодействие и организует обмен информацией в соответствии с потребностями совместной деятельности, используя современные коммуникационные технологии.	ИУК-4.1.3-1. Знает взаимодействие и организует обмен информацией в соответствии с потребностями совместной деятельности, используя современные коммуникационные технологии в интересах обеспечения национальной безопасности.
	ИПК-1.1.У-1. Умеет определять круг взаимодействий и организовывать обмен информацией в соответствии с потребностями совместной деятельности, используя современные коммуникационные технологии. в интересах обеспечения национальной

	безопасности в части различных правоотношений.
ИУК-4.2. Составляет в соответствии с нормами русского языка различные виды деловой документации.	ИУК-4.2.3-1. Знает правила создания в соответствии с нормами русского языка различные виды деловой документации в интересах обеспечения безопасности.
	ИУК-4.2.У-1. Умеет составлять в соответствии с нормами русского языка различные виды деловой документации в интересах обеспечения безопасности.
ИУК-4.3. Составляет типовую деловую документацию для образовательных и рабочих задач на иностранном языке.	ИУК-4.3.3-1. Знает правила создания типовой деловой документации для образовательных и рабочих задач на иностранном языке в интересах обеспечения безопасности.
	ИУК-4.3.У-1. Умеет составлять типовую деловую документацию для образовательных и рабочих задач на иностранном языке.в интересах обеспечения безопасности.
ИУК-4.4. Организует обсуждение итогов исследовательских и проектных работ на различных публичных мероприятиях на русском языке, подбирая наиболее подходящий формат.	ИУК-4.4.3-1. Знает содержание нормативных правовых актов, применяемых к общественным отношениям в интересах обеспечения национальной безопасности.
	ИУК-4.4.У-1. Умеет определять круг нормативных правовых актов, применяемых к общественным отношениям, возникающим при осуществлении профессиональной публично-правовой деятельности в интересах обеспечения национальной безопасности в части различных правоотношений

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет: для ОФО 3 зачетных единицы (108 часов) их распределение по видам работ представлено в таблице

Виды работ	Всего часов	Форма обучения
		очная
	ОФО	1 семестр (часы)
Контактная работа, в том числе:	54,3	54,3
Аудиторные занятия (всего):	52	52
занятия лекционного типа	34	34
лабораторные занятия	-	-

занятия семинарского типа (практические занятия)	18	18
Иная контактная работа:	2,3	2,3
Контроль самостоятельной работы (КСР)	2	2
Промежуточная аттестация (ИКР)	0,	0,3
Самостоятельная работа, в том числе:	18	18
Контрольная работа	4	4
Реферат/эссе (подготовка)	4	4
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, дискуссиям)	4	4
Подготовка к текущему контролю	6	6
Контроль:	35,7	35,7
Общая трудоемкость	час.	108
	в том числе контактная работа	54,3
	зач. ед	3

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по темам дисциплины.

Темы дисциплины, изучаемые в 1 семестре 1 курса (очная форма обучения)

№	Наименование тем	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	СЗ	ЛР	СРС
1.	Основные составляющие информационной безопасности	15	7	4	-	4
2.	Криптографические способы защиты информации	15	7	4	-	4
3.	Антивирусная защита	15	7	4	-	4
4.	Сетевая безопасность	18	6	6	-	6
	ИТОГО по темам дисциплины	70	34	18	-	18
	Контроль	35,7				
	Контроль самостоятельной работы (КСР)	2	-	-	-	-
	Промежуточная аттестация (ИКР)	0,3	-	-	-	-
	Общая трудоемкость по дисциплине	108	-	-	-	-

Примечание: Л – лекции, СЗ – занятия семинарского типа (практические занятия), ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание тем дисциплины

2.3.1 Занятия лекционного типа (очная форма обучения)

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля ¹
1	2	3	4
1.	Основные составляющие информационной безопасности	1. Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. 2. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. 3. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности	Р, Д, КРЗ
2.	Криптографические способы защиты информации	1. Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом.	Р, С, РП, КРЗ
3.	Антивирусная защита	1. Общие понятия антивирусной защиты. Уязвимости. 2. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. 3. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы	Р, С, РП, КРЗ
4.	Сетевая безопасность	1. Защита информации в локальных сетях. 2. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. 3. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. 4. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети.	Р, РП, С

Примечание: Р – написание реферата, РП – написание реферата с презентацией, С – сообщение, Д – дискуссия, КРЗ – контрольное решение задач.

¹ Конкретная форма текущего контроля избирается преподавателем.

2.3.2 Занятия семинарского типа (практические занятия). Очная форма обучения

№	Наименование раздела (темы)	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1.	Основные составляющие информационной безопасности	1. Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. 2. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. 3. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности	ответ на семинаре, реферат, контрольное решение задач,
2.	Криптографические способы защиты информации	1. Введение в основы современных шифров с симметричным ключом. Модульная арифметика. 2. Сравнения и матрицы. Традиционные шифры с симметричным ключом.	ответ на семинаре, реферат, реферат с презентацией, сообщение
3.	Антивирусная защита	1. Общие понятия антивирусной защиты. Уязвимости. 2. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. 3. Методы защиты от вредоносных программ. Основы работы антивирусных программ: 4. Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы	Реферат, реферат с презентацией, сообщение, дискуссия, контрольное решение задач, ответ на семинаре
4.	Сетевая безопасность	1. Защита информации в локальных сетях. 2. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. 3. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. 4. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. 5. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети.	Реферат, реферат с презентацией, сообщение, контрольное решение задач, ответ на семинаре

Примечание: Р – написание реферата, РП – написание реферата с презентацией, С – сообщение, Д – дискуссия.

При изучении дисциплины могут применяться электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

2.3.3 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

2.4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Виды СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка учебного (теоретического) материала	Методические указания для обучающихся по освоению дисциплин кафедры криминалистики и правовой информатики, в том числе, по организации самостоятельной работы студентов, утвержденные кафедрой, протокол № 10 от 28 апреля 2025г.
2	Подготовка сообщений, презентаций	Методические указания для обучающихся по освоению дисциплин кафедры криминалистики и правовой информатики, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой, протокол № 10 от 28 апреля 2025г.
3	Выполнение реферата	Методические указания для обучающихся по освоению дисциплин кафедры криминалистики и правовой информатики, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой, протокол № 10 от 28 апреля 2025г.
4	Подготовка к текущему контролю	Методические указания для обучающихся по освоению дисциплин кафедры криминалистики и правовой информатики, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой, протокол № 10 от 28 апреля 2025г.
5	Регламентированная дискуссия	Методические указания для обучающихся по освоению дисциплин кафедры криминалистики и правовой информатики, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой, протокол № 10 от 28 апреля 2025г.
6.	Тестирование	Методические указания для обучающихся по освоению дисциплин кафедры криминалистики и правовой информатики, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой, протокол № 10 от 28 апреля 2025г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

3. Образовательные технологии, применяемые при освоении дисциплины

При изучении дисциплины «Информационная безопасность» применяются такие образовательные технологии, используемые при реализации различных видов учебной работы, как дискуссия, проблемная лекция.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Оперативно-розыскная деятельность».

Оценочные средства включают контрольные материалы для проведения **текущего контроля** в форме рефератов, сообщений, коллоквиумов, вопросов для устного (письменного) опроса по теме и **промежуточной аттестации** в форме вопросов к зачету.

Структура оценочных средств для текущей и промежуточной аттестации ОФО

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия.	ИУК-4.1. Устанавливает взаимодействие и организует обмен информацией в соответствии с потребностями совместной деятельности, используя современные коммуникационные технологии. ИУК-4.2. Составляет в соответствии с нормами русского языка различные виды деловой документации. УИК-4.3. Составляет типовую деловую документацию для образовательных и рабочих задач на иностранном языке. ИУК-4.4. Организует обсуждение итогов исследовательских и проектных работ на различных публичных мероприятиях на русском языке, подбирая наиболее подходящий формат.	Вопросы для устного (письменного) опроса по теме, коллоквиум, подготовка реферата, сообщения	Вопрос на зачете: 1-60.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Тема 1. Основные составляющие информационной безопасности

1. Составление плана и основных положений политики безопасности для учреждения

Темы сообщений, рефератов, презентаций

1. Шифрование перестановкой
2. Шифрование подстановкой

Тема 2. Криптографические способы защиты информации

1. Написание, ввод, отладка и тестирование программ шифрования подстановкой и перестановкой
2. Написание, ввод, отладка и тестирование программ шифрования RSA, аналитически и гаммированием

Темы сообщений, рефератов, презентаций

1. Виды шифрования

Тема 3. Антивирусная защита

1. Диагностика работы антивируса и создание тестового вируса"

Темы сообщений, рефератов, презентаций

1. Типы и виды вирусов.
2. Типы и виды Антивирусные программ.

Тема 4. Сетевая безопасность

1. Создание цифровой подписи
2. Парольный доступ и парольная аутентификация

Темы сообщений, рефератов, презентаций

1. Виды ЭЦП

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен)

Перечень вопросов для экзамена

1. Основные понятия информационной безопасности. Классификация угроз.
2. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Алгоритм шифрования данных IDEA.
3. Особенности правового регулирования информационных отношений в сети Интернет.
4. Целостность и конфиденциальность. Классификация средств защиты информации.
5. Стандарт шифрования данных RSA.
6. Информационные правонарушения (правонарушения в информационной сфере) и ответственность за их совершение.
7. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.
8. Основы работы антивирусных программ: Сигнатурный анализ. Приведите примеры использования.
9. Правовое регулирование информационных отношений в информационном обществе.
10. Базовые понятия теории информации.
11. Эвристический анализ при работе антивирусных программ.
12. Правовые основы документирования информации.
13. Измерение дискретной информации. Энтропия Шеннона.

14. Основные приемы криптоанализа при симметричных ключах. Виды атак. Принцип Керкгоффса.
15. Право на информацию.
16. Методы и средства организационно-правовой защиты информации.
17. Формулы аддитивных шифров. Криптоанализ.
18. Правовые основы информационной безопасности.
19. Методы и средства инженерно-технической защиты.
20. Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты сети.
21. Правовые основы документирования информации.
22. Формулы мультипликативных шифров. Аффинные шифры. Криптоанализ аффинного шифра.
23. Принципы организации централизованного управления антивирусной защитой. Компоненты системы удаленного управления.
24. Правовое регулирование распространения информации среди неопределенного круга лиц.
25. Модель сетевой безопасности. Классификация сетевых атак.
26. Брандмауэры. Определение типов брандмауэров.
27. Правовая охрана информации в режиме интеллектуальной собственности.
28. Сервисы и механизмы безопасности.
29. Конфигурация межсетевого экрана. Построение набора правил межсетевого экрана для различных типов архитектуры.
30. Особенности правового регулирования информационных отношений в сети Интернет.
31. Модель сетевого взаимодействия, модель безопасности информационной системы.
32. Одноразовый блокнот и роторные шифры. Устройство и принцип работы шифровальной машины «Энигма».
33. Информационные правонарушения (правонарушения в информационной сфере) и ответственность за их совершение.
34. Простые криптосистемы. Шифрование методом замены (подстановки): Одноалфавитная подстановка.
35. Основные приемы криптоанализа при асимметричных ключах.
36. Задачи органов Государственной системы защиты информации.
37. Простые криптосистемы. Шифрование методом замены (подстановки): Многоалфавитная одноконтурная обыкновенная.
38. Базовые методы и алгоритмы стеганографии.
39. Персональные данные, их классификация.
40. Простые криптосистемы. Шифрование методом замены (подстановки): Многоалфавитная многоконтурная подстановка.
41. Правовое регулирование информационных отношений в информационном обществе.
42. Система защиты сведений, составляющих государственную тайну.
43. Простые криптосистемы. Шифрование методом замены (подстановки): Моноалфавитная многоконтурная подстановка.
44. Право на информацию.
45. Законодательство об электронной цифровой подписи.
46. Арифметика целых чисел. НОД и алгоритм Евклида Бинарные операции.
47. Правовые основы информационной безопасности.
48. Защита прав и законных интересов субъектов информационной сферы.
49. Расширенный алгоритм Евклида . Линейные диофантовы уравнения.

50. Правовые основы документирования информации.
51. Защита прав и законных интересов субъектов информационной сферы.
52. Модульная арифметика. Операции по модулю. Система вычетов. Сравнения. Инверсии.
53. Правовая защита конфиденциальной информации.
54. Нормативно-методические документы по обеспечению безопасности информации.
55. Шифрование методом перестановки: Простая перестановка.
56. Правовое регулирование распространения информации среди неопределенного круга лиц.
57. Организация подготовки кадров и повышения квалификации в области обеспечения информационной безопасности.
58. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования.
59. Правовая охрана информации в режиме интеллектуальной собственности.
60. Организация работы подразделений (служб) обеспечения информационной безопасности.

Критерии оценивания результатов обучения

Критерии оценки экзамена

Оценка «отлично» выставляется студенту, если студентом дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по теме, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений.

Оценка «хорошо» выставляется студенту, если студентом дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной гистологической терминологии. Могут быть допущены 2–3 неточности или незначительные ошибки, исправленные обучающимся с помощью преподавателя.

Оценка «удовлетворительно» выставляется при недостаточно полном и недостаточно развернутом ответе. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Обучающийся не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано.

Оценка «неудовлетворительно» выставляется при несоответствии ответа заданному вопросу, использовании при ответе ненадлежащих нормативных и иных источников, когда ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа обучающегося.

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;

- 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;
- при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

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.

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.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1. Нормативные правовые акты и акты толкования

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с попр.) // <https://www.pravo.gov.ru>
2. О полиции: Федеральный закон РФ от 07 февраля 2011 г. № 3-ФЗ. (с изм. и доп.) // <https://www.pravo.gov.ru>

5.2. Учебная литература

1. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=598988> (дата обращения: 27.05.2024). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.
2. Аудит информационной безопасности органов исполнительной власти : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, М. В. Рудановский. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 100 с. : ил., схем., табл. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=93259> (дата обращения: 27.05.2024). – Библиогр.: с. 83-84. – ISBN 978-5-9765-1277-1. – Текст : электронный.

5.3. Периодическая литература

1. Юридический вестник Кубанского государственного университета // <http://law.kubsu.ru/q-q-64/>.

5.4. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

Перечень договоров ЭБС		
Учебный год	Наименование документа с указанием реквизитов	Срок действия документа
2025	ЭБС «Лань» http://e.lanbook.com/ ООО «ЭБС ЛАНЬ» Контракт № 1212/2024/2 от 25 декабря 2024 г. ЭБС «Университетская библиотека онлайн» https://biblioclub.ru ООО «Директ-Медиа» Контракт № 1212/2024/1 от 25 декабря 2024 г. ОП «Юрайт» https://urait.ru/ ООО «Электронное издательство Юрайт» Лиц.договор № 1212/2024/3 от 25 декабря 2024 г. ЭБС «BOOK.ru» https://book.ru ООО «КноРус медиа» Договор № 580-ЕП/223-ФЗ/2024 от 25 декабря 2024 г. ЭБС «ZNANIUM» https://znanium.ru ООО «ЗНАНИУМ» Контракт № 1212/2024 от 25 декабря 2024 г.	С 01.01.25 по 31.12.25 С 01.01.25 по 31.12.25 С 20.01.25 по 19.01.26 С 01.01.25 по 31.12.25 С 01.01.25 по 31.12.25
2024	ЭБС «Лань» http://e.lanbook.com/ ООО «ЭБС ЛАНЬ» Контракт № 0712/2023 от 19 декабря 2023 г. ЭБС «Университетская библиотека онлайн» https://biblioclub.ru ООО «Директ-Медиа» Контракт № 0712/2023/3 от 19 декабря 2023 г. ОП «Юрайт» https://urait.ru/ ООО «Электронное издательство Юрайт» Лиц.договор № 0712/2023/1 от 19 декабря 2023 г. ЭБС «BOOK.ru» https://book.ru ООО «КноРус медиа» Договор № 450-ЕП/223-ФЗ/2023 от 29 ноября 2023 г. ЭБС «ZNANIUM» https://znanium.ru ООО «ЗНАНИУМ» Контракт № 0712/2023/2 от 19 декабря 2023 г.	С 01.01.24 по 31.12.24 С 01.01.24 по 31.12.24 С 20.01.24 по 19.01.25 С 01.01.24 по 31.12.24 С 01.01.24 по 31.12.24

Профессиональные базы данных:

1. Научная электронная библиотека (НЭБ) <http://www.elibrary.ru/>
2. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) <https://rusneb.ru/>
3. Президентская библиотека им. Б.Н. Ельцина <https://www.prilib.ru/>
4. «Лекториум ТВ» <http://www.lektorium.tv/>

Информационные справочные системы:

1. Консультант Плюс – справочная правовая система (доступ по локальной сети с компьютеров библиотеки).
2. ГАРАНТ – Справочная Правовая Система (ГАРАНТ).

Ресурсы свободного доступа:

1. КиберЛенинка <http://cyberleninka.ru/>;
2. Министерство науки и высшего образования Российской Федерации <https://www.minobrnauki.gov.ru/>;
3. Федеральный портал «Российское образование» <http://www.edu.ru/>;
4. Проект Государственного института русского языка имени А.С. Пушкина «Образование на русском» <https://pushkininstitute.ru/>;
5. Справочно-информационный портал «Русский язык» <http://gramota.ru/>;
6. Служба тематических толковых словарей <http://www.glossary.ru/>;
7. Словари и энциклопедии <http://dic.academic.ru/>;
8. Образовательный портал «Учеба» <http://www.ucheba.com/>
9. Законопроект «Об образовании в Российской Федерации». Вопросы и ответы

http://xn--273--84d1f.xn--plai/voprosy_i_otvety.

10. Сайт Комиссии Таможенного союза Республики Беларусь, Республики Казахстан и Российской Федерации. - Режим доступа: <http://www.tsouz.ru>
11. Официальный сайт Президента РФ. www.kremlin.ru
12. Официальный сайт Совета Федерации Федерального Собрания Российской Федерации Режим доступа: www.council.gov.ru
13. Сайт Государственной Думы Федерального Собрания РФ. - Режим доступа: <http://www.duma.gov.ru>
14. Сайт Президента РФ. Режим доступа: <http://www.president.kremlin.ru>
15. Сайт Правительства РФ. Режим доступа: www.government.ru.
16. Сайт Конституционного Суда РФ. Режим доступа: <http://ksrf.ru>
17. Сайт Верховного Суда РФ. Режим доступа: <http://www.supcourt.ru>
18. Сайт Генеральной Прокуратуры РФ. Режим доступа: <http://genproc.gov.ru>
19. Сайт Совета Безопасности РФ. - Режим доступа: <http://www.scrf.gov.ru/index.shtml>
20. Сайт Министерства юстиции РФ. Режим доступа: <http://www.mibjust.ru>
21. Сайт Министерства иностранных дел РФ. Режим доступа: www.mid.ru
22. Официальный сайт юридического факультета Кубанского государственного университета. Режим доступа: www.law.kubsu.ru
23. Интернет-ресурс Судебные и нормативные акты РФ (СудАкт) Режим доступа: <https://sudact.ru>

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения <http://moodle.kubsu.ru>
2. База учебных планов, учебно-методических комплексов, публикаций и конференций <http://mschool.kubsu.ru/>
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий <http://mschool.kubsu.ru;>
4. Электронный архив документов КубГУ <http://docspace.kubsu.ru/>
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала «ШКОЛЬНЫЕ ГОДЫ» <http://icdau.kubsu.ru/>.

6. Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины «Информационная безопасность» необходимо руководствоваться действующим федеральным и иным законодательством и разработанными на его основе подзаконными нормативными актами.

Изучение курса осуществляется в тесном взаимодействии с другими юридическими и общественными дисциплинами. Форма и способы изучения материала определяются с учетом специфики изучаемой темы. Однако во всех случаях необходимо обеспечить сочетание изучения теоретического материала, научного толкования того или иного понятия, даваемого в учебниках и лекциях, с самостоятельной работой студентов, выполнением практических заданий, подготовкой сообщений и рефератов.

Методические указания по занятиям лекционного типа

В ходе занятия лекционного типа студентам рекомендуется конспектировать ее основные положения, не стоит пытаться дословно записать всю лекцию, поскольку скорость лекции не рассчитана на аутентичное воспроизведение выступления лектора в конспекте. Тем не менее, она является достаточной для того, чтобы студент смог не только усвоить, но и зафиксировать на бумаге сущность затронутых лектором проблем, выводы, а

также узловые моменты, на которые обращается особое внимание в ходе лекции. Основным средством работы на лекционном занятии является конспектирование. Конспектирование – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста. Результат конспектирования – запись, позволяющая студенту немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу, его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других. Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей концепции лекции (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т.е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Определения, которые дает лектор, стоит по возможности записать дословно и выделить другим цветом или же подчеркнуть. В случае изложения лектором хода научной дискуссии желательно кратко законспектировать существо вопроса, основные позиции и фамилии ученых, их отстаивающих. Если в обоснование своих выводов лектор приводит ссылки на справочники, статистические данные, нормативные акты и другие официально опубликованные сведения, имеет смысл лишь кратко отразить их существо и указать источник, в котором можно полностью почерпнуть излагаемую информацию.

Во время лекции студенту рекомендуется иметь на столах помимо конспектов также программу курса, которая будет способствовать развитию мнемонической памяти, возникновению ассоциаций между выступлением лектора и программными вопросами.

В случае возникновения у студента по ходу лекции вопросов, их следует записать и задать в конце лекции в специально отведенное для этого время.

По окончании лекции (в тот же или на следующий день, пока еще в памяти сохранилась информация) студентам рекомендуется доработать свои конспекты, привести их в порядок, дополнить сведениями с учетом дополнительно изученного нормативного, справочного и научного материала. Крайне желательно на полях конспекта отмечать не только изученные точки зрения ученых по рассматриваемой проблеме, но и выражать согласие или несогласие самого студента с законспектированными положениями.

Лекционное занятие предназначено для изложения особенно важных, проблемных, актуальных в современной науке вопросов. Лекция, также как и семинарское, практическое занятие, требует от студентов определенной подготовки. Студент обязательно должен знать тему предстоящего лекционного занятия и обеспечить себе необходимый уровень активного участия: подобрать и ознакомиться, а при необходимости иметь с собой рекомендуемый преподавателем нормативный материал, повторить ранее пройденные темы по вопросам, которые будут затрагиваться в предстоящей лекции, вспомнить материал иных дисциплин.

Применение отдельных образовательных технологий требует специальной подготовки не только от преподавателя, но и участвующих в занятиях студентов. Так, при проведении лекции-дискуссии, которая предполагает разделение присутствующих студентов на группы, студент должен быть способен высказать свою позицию относительно выдвинутых преподавателем точек зрения.

Методические указания для подготовки к занятиям семинарского типа (практическим занятиям)

Занятия семинарского типа (практические занятия) представляют собой одну из важных форм самостоятельной работы студентов над нормативными актами, научной и учебной литературой непосредственно в учебной аудитории под руководством преподавателя.

В зависимости от изучаемой темы и ее специфики преподаватель выбирает или сочетает следующие формы проведения занятий семинарского типа (практических занятий): обсуждение теоретических вопросов, подготовка рефератов, научные дискуссии, собеседования и т.п. Проверка усвоения отдельных (ключевых) тем может осуществляться посредством проведения коллоквиума.

Подготовка к занятию семинарского типа (практическому занятию) заключается в подробном изучении конспекта лекции, нормативных актов, учебной и научной литературы, основные положения которых студенту рекомендуется конспектировать.

Активное участие в работе на занятиях семинарского типа (практических занятий) предполагает выступления на них, дополнение ответов однокурсников, коллективное обсуждение спорных вопросов и проблем, что способствует формированию у студентов навыков формулирования, аргументации и отстаивания выработанного решения, умения его защитить в дискуссии и представить дополнительные аргументы в его пользу. Активная работа на занятии способствует также формированию у студентов навыков публичного выступления, умения ясно, последовательно, логично и аргументированно излагать свои мысли.

При выступлении на занятиях семинарского типа (практических занятиях) студентам разрешается пользоваться конспектами для цитирования нормативных актов или позиций ученых. По окончании ответа другие студенты могут дополнить выступление товарища, отметить его спорные или недостаточно аргументированные стороны, проанализировать позиции ученых, о которых не сказал предыдущий выступающий.

В конце занятия после подведения его итогов преподавателем студентам рекомендуется внести изменения в свои конспекты, отметить информацию, прозвучавшую в выступлениях других студентов, дополнения, сделанные преподавателем и не отраженные в конспекте.

Занятия семинарского типа (практические занятия) требуют предварительной теоретической подготовки по соответствующей теме: изучения учебной и дополнительной литературы, ознакомления с нормативным материалом. Рекомендуется при этом вначале изучить вопросы темы по учебной литературе. Если по теме прочитана лекция, то непременно надо использовать материал лекции, так как учебники часто устаревают уже в момент выхода в свет.

Применение отдельных образовательных технологий требуют предварительного ознакомления студентов с содержанием применяемых на занятиях приемов. Так, при занятиях семинарского типа студент должен представлять как его общую структуру, так и особенности отдельных методических приемов: дискуссии, контрольные работы, использование правовых документов и др.

Примерные этапы занятия семинарского типа и методические приемы их осуществления:

- постановка целей занятия: обучающей, развивающей, воспитывающей;
- планируемые результаты обучения: что должны студенты знать и уметь;
- проверка знаний: устный опрос, фронтальный опрос, программированный опрос, блиц-опрос, письменный опрос, комментирование ответов, оценка знаний, обобщение по опросу;
- изучение нового материала по теме;

– закрепление материала предназначено для того, чтобы студенты запомнили материал и научились использовать полученные знания (активное мышление).

Формы закрепления:

– групповая работа (коллективная мыслительная деятельность).

Домашнее задание:

– работа над текстом учебника.

В рамках занятия семинарского типа студент должен быть готов к изучению предлагаемых правовых документов и их анализу.

В качестве одного из оценочных средств в рамках занятий может использоваться *контрольная работа*.

Для проведения *контрольной работы* в рамках занятий семинарского типа студент должен быть готов ответить на проблемные вопросы, проявить свои аналитические способности. При ответах на вопросы контрольной работы в обязательном порядке необходимо:

- правильно уяснить суть поставленного вопроса;
- сформировать собственную позицию;
- подкрепить свой ответ ссылками на нормативные, научные, иные источники;
- по заданию преподавателя изложить свой ответ в письменной форме.

Методические указания подготовки к контрольному решению задач

Контрольное решение задач является одной из форм текущего контроля успеваемости студентов. В соответствии с учебным планом овладение курсом включает выполнение студентами двух работ. Успешное выполнение задач свидетельствует об овладении студентами соответствующим теоретическим материалом на уровне его применения для решения профессионально-ориентированных задач. Задания работы ориентированы на выявление у студентов уровня сформированности способности исследовать их и интерпретировать полученные результаты.

При оформлении решения сюжетных задач, содержанием выделяются три этапа решения:

- построение математической модели, включающее описание вводимых обозначений, процесса построения модели;
- исследование математической модели, предполагающее решение задачи, адекватной построенной модели;
- интерпретация результата решения, включающая его представление посредством терминологии и обозначений, принятых в соответствующей сфере познания, установление их соответствия смыслу задачи, ограничениям на величины.

Завершается оформление решения каждой задачи записью ответа.

Методические указания подготовки к коллоквиуму

Коллоквиум может проводиться в устной и письменной форме.

Устная форма. Ответы оцениваются одновременно в традиционной шкале ("неудовлетворительно" — "отлично"). Билеты содержат как теоретические вопросы, так и задачи практического характера. На коллоквиум выносятся часть материала экзамена. Оценка за коллоквиум учитывается при выставлении финальной оценки за экзамен. Коллоквиум ставит следующие задачи: - проверка и контроль полученных знаний по изучаемой теме; - расширение проблематики в рамках дополнительных вопросов по данной теме; - углубление знаний при помощи использования дополнительных материалов при подготовке к занятию; - студенты должны продемонстрировать умения работы с различными видами исторических источников; - формирование умений коллективного

обсуждения (поддерживать диалог в микрогруппах, находить компромиссное решение, аргументировать свою точку зрения, умение слушать оппонента, готовность принять позицию другого учащегося;)

Этапы проведения коллоквиума 1. Подготовительный этап: - Формулирование темы и проблемных вопросов для обсуждения (преподаватель должен заранее продумать проблемные вопросы, в соответствии с уровнем учащихся в группе и создать карточки, вопросы в которых будут дифференцироваться по уровню сложности); - Предоставление списка дополнительной литературы; - Постановка целей и задач занятия; - Разработка структуры занятия; - Консультация по ходу проведения занятия; 2. Начало занятия: - Подготовка аудитории: поскольку каждая микрогруппа состоит из 5-7 студентов, то парты нужно соединить по две, образовав квадрат, и расставить такие квадраты по всему помещению. - Комплектация микрогрупп. - Раздача вопросов по заданной теме для совместного обсуждения в микрогруппах. 3. Подготовка учащихся по поставленным вопросам. 4. Этап ответов на поставленные вопросы: - В порядке установленном преподавателем, представители от микрогрупп зачитывают выработанные, в ходе коллективного обсуждения, ответы; - студенты из других микрогрупп задают вопросы отвечающему, комментируют и дополняют предложенный ответ; - Преподаватель регулирует обсуждения, задавая наводящие вопросы, корректируя неправильные ответы (важно, чтобы преподаватель не вмешивался напрямую в ход обсуждения, не навязывал собственную точку зрения); - После обсуждения каждого вопроса необходимо подвести общие выводы и логично перейти к обсуждению следующего вопроса (важно вопросы распределить таким образом, чтобы ответы микрогрупп чередовались); - После обсуждения всех предложенных вопросов преподаватель подводит общие выводы; 5. Итог: - Преподаватель должен соотнести цели и задачи данного занятия и итоговые результаты, которых удалось добиться; - Заключительный этап суммирует все достигнутое с тем, чтобы дать новый импульс для дальнейшего изучения и решения обсуждавшихся вопросов (в рамках одного занятия невозможно решить все поставленные проблемы, одна из задач подобного вида занятий, спровоцировать интерес к обсуждаемым проблемам); - Преподаватель должен охарактеризовать работу каждой микрогруппы, выделить наиболее грамотные и корректные ответы учащихся.

Методические указания для подготовки и проведения дискуссии

Дискуссия – от лат. «discussion» (рассмотрение, исследование).

Дискуссия представляет собой метод активного обучения и позволяет оценить способность студентов осуществлять поиск решения той или иной научной проблемы на основе ее публичного обсуждения, сопоставления различных точек зрения, обмена информацией в малых группах. Дискуссия, кроме того, позволяет выявить знания студента по соответствующей теме, умение формулировать вопросы и оценочные суждения по теме, осуществлять конструктивную критику существующих подходов к решению научной проблемы; владение культурой ведения научного спора и т. д.

Дискуссия проводится на занятии семинарского типа среди присутствующих студентов.

Сценарий проведения дискуссии

1. Определение темы дискуссии.
2. Участники круглого стола: ведущий (преподаватель соответствующей дисциплины) и диспутанты (студенты). Возможно приглашение эксперта из числа других преподавателей кафедры.
3. Непосредственное проведение дискуссии.
4. Подведения итогов дискуссии ведущим.
5. Оформление тезисов по итогам проведения круглого стола.

Этапы подготовки и проведения дискуссии.

Первый этап: Выбор темы. Осуществляется с ориентацией на направления научной работы кафедры и преподавателей. Преподаватель предлагает тему дискуссии с обоснованием необходимости ее обсуждения и разработки. Тема дискуссии должна отвечать критериям актуальности, дискуссионности. Она должна представлять научный и практический интерес. Участникам дискуссии дается 7-10 дней для подготовки к дискуссии по заявленной теме.

Второй этап. Определение участников.

Обязательным участником дискуссии является *ведущий*. Ведущий изучает интересы и возможности аудитории, определяет границы проблемного поля, в пределах которого может разворачиваться обсуждение; формулирует название дискуссии, определяет будущий регламент работы и определяет задачи, которые должны быть решены ее участниками; регламентирует работу участников, осуществляет управление их когнитивной, коммуникативной и эмоциональной активностью; стимулирует развитие элементов коммуникативной компетентности участников дискуссии; контролирует степень напряженности отношений оппонентов и соблюдение ими правил ведения дискуссии; занимается профилактикой конфликтных ситуаций, возникающих по ходу дискуссии, при необходимости использует директивные приемы воздействия; мысленно фиксирует основные положения, высказанные участниками, отмечает поворотные моменты, выводящие обсуждение на новый уровень; резюмирует и подводит итоги обсуждения.

Вместе с тем позиция ведущего остается нейтральной. Он не имеет права высказывать свою точку зрения по обсуждаемой проблеме, выражать пристрастное отношение к кому-либо из участников, принимать чью-либо сторону, оказывая давление на присутствующих.

Непосредственными участниками дискуссии (*оппонентами*) являются студенты соответствующей группы. Студенты при подготовке к теме выступления должны проанализировать существующие в науке мнения по проблеме, изучить нормативный материал, практические проблемы, связанные с рассматриваемой темой, сформулировать собственные выводы и подходы к решению проблемы.

В качестве участника дискуссии возможно приглашение *эксперта*, который оценивает продуктивность всей дискуссии, высказывает мнение о вкладе того или иного участника дискуссии в нахождение общего решения, дает характеристику того, как шло общение участников дискуссии.

Третий этап. Ход дискуссии.

Введение в дискуссию. Дискуссию начинает ведущий. Он информирует участников о проблеме, оглашает основные правила ведения дискуссии, напоминает тему дискуссии, предоставляет слово выступающим.

Групповое обсуждение. Этап представляет собой полемику участников. Ведущий предоставляет участникам право высказаться по поставленной проблеме. После окончания выступления (2-3 мин) другим участникам представляется возможность задать выступающему вопросы. После того, как вопросы будут исчерпаны, право выступить представляется оппоненту. По окончании выступления оппоненту также могут быть заданы вопросы. Процесс повторяется до тех пор, пока не выступят все участники дискуссии.

Правила обсуждения: выступления должны проходить организованно, каждый участник может выступать только с разрешения председательствующего (ведущего), недопустима перепалка между участниками; каждое высказывание должно быть подкреплено фактами; в обсуждении следует предоставить каждому участнику возможность высказаться; в ходе обсуждения недопустимо «переходить на личности», навешивать ярлыки, допускать уничижительные высказывания и т. п.

Четвертый этап. Подведение итогов. В завершении круглого стола ведущий подводит итоги. Делает общие выводы о направлениях решения обсужденных в ходе дискуссии вопросов. Дает оценку выступлению каждого из студентов.

По итогам дискуссии студенты готовят тезисы. Тезисы участников оформляются в виде «Материалов дискуссии». Тезисы для включения в «Материалы дискуссии» должен быть выполнен 14 шрифтом, 1,5 интервалом, Все поля – 2 см, объем – 2-3 страницы.

Важнейшим этапом курса является *самостоятельная работа* по дисциплине, включающая в себя проработку учебного (теоретического) материала, выполнение индивидуальных заданий (подготовка сообщений), выполнение рефератов, подготовку к текущему контролю.

Самостоятельная работа осуществляется на протяжении всего времени изучения дисциплины, по итогам которой студенты предоставляют сообщения, рефераты, презентации, конспекты, показывают свои знания на занятиях семинарского типа при устном ответе.

Методические рекомендации по подготовке рефератов, сообщений

Первичные навыки научно-исследовательской работы должны приобретаться студентами при написании рефератов по специальной тематике.

Цель: научить студентов связывать теорию с практикой, пользоваться литературой, статистическими данными, привить умение популярно излагать сложные вопросы.

Рефераты составляются в соответствии с указанными темами. Выполнение рефератов предусмотрено на листах формата А 4. Они сдаются на проверку преподавателю в соответствии с указанным графиком.

Требования к работе. Реферативная работа должна выявить углубленные знания студентов по той или иной теме дисциплины. В работе должно проявиться умение работать с литературой. Студент обязан изучить и использовать в своей работе не менее 2–3 книг и 1–2 периодических источника литературы.

Оформление реферата:

1. Реферат должен иметь следующую структуру: а) план; б) изложение основного содержания темы; в) список использованной литературы.
2. Общий объём – 5–7 с. основного текста.
3. Перед написанием должен быть составлен план работы, который обычно включает 2–3 вопроса. План не следует излишне детализировать, в нём перечисляются основные, центральные вопросы темы.
4. В процессе написания работы студент имеет право обратиться за консультацией к преподавателю кафедры.
5. В основной части работы большое внимание следует уделить глубокому теоретическому освещению основных вопросов темы, правильно увязать теоретические положения с практикой, конкретным фактическим и цифровым материалом.
6. В реферате обязательно отражается использованная литература, которая является завершающей частью работы.
7. Особое внимание следует уделить оформлению. На титульном листе необходимо указать название вуза, название кафедры, тему, группу, свою фамилию и инициалы, фамилию научного руководителя. На следующем листе приводится план работы.
8. При защите реферата выставляется дифференцированная оценка.
9. Реферат, не соответствующий требованиям, предъявляемым к данному виду работы, возвращается на доработку.

Качество реферата оценивается по тому, насколько полно раскрыто содержание темы, использованы первоисточники, логичное и последовательное изложение. Оценивается и правильность подбора основной и дополнительной литературы (ссылки по правилам: фамилии и инициалы авторов, название книги, место издания, издательство, год издания, страница).

Реферат должен отражать точку зрения автора на данную проблему.

Подготовка сообщения представляет собой разработку и представление небольшого по объему устного сообщения для озвучивания на занятии семинарского типа. Сообщаемая информация носит характер уточнения или обобщения, несет новизну, отражает современный взгляд по определенным проблемам.

Сообщение отличается от докладов и рефератов не только объемом информации, но и ее характером – сообщения дополняют изучаемый вопрос фактическими или статистическими материалами. Возможно письменное оформление задания, оно может включать элементы наглядности (иллюстрации, демонстрацию).

Регламент времени на озвучивание сообщения – до 5 мин.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7. Материально-техническое обеспечение по дисциплине

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Аудитория для проведения лекционных занятий	Ауд. 106 Интерактивный проектор, магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия, портреты ученых юристов, учебно-наглядные пособия, ноутбук	Антиплагиат-ВУЗ. Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ» версии 3.3. (интернет-версия). – Договор №19/АЭФ/44/ФЗ/2023 КонсультантПлюс - Справочная Правовая Система (КонсультантПлюс). Артикул правообладателя КонсультантПлюс – Договор №ГК/479/ЕП/223/ФЗ/2023 ГАРАНТ - Справочная Правовая Система (ГАРАНТ). «Компания АПИ «ГАРАНТ»» Артикул правообладателя ГАРАНТ – Договор №4920/НК/14 Р7-Офис - Desktopные редакторы текстовых документов, таблиц и презентаций. Лицензии на офисное программное обеспечение для рабочих мест с целью обеспечения образовательного процесса Р7-Офис. Профессиональный (Десктоп + Сервер

		оптимальный) – Договор №30-АЭФ/44-ФЗ/2022
Аудитория для семинарских занятий	Ауд. 107 Интерактивный проектор, магнитно-маркерная доска, учебная мебель, учебно-наглядные пособия, портреты ученых юристов, ноутбук	Антиплагиат-ВУЗ. Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ» версии 3.3. (интернет-версия). – Договор №19/АЭФ/44/ФЗ/2023 КонсультантПлюс - Справочная Правовая Система (КонсультантПлюс). Артикул правообладателя КонсультантПлюс – Договор №ГК/479/ЕП/223/ФЗ/2023 ГАРАНТ - Справочная Правовая Система (ГАРАНТ). «Компания АПИ «ГАРАНТ»» Артикул правообладателя ГАРАНТ – Договор №4920/НК/14 Р7-Офис - Desktopные редакторы текстовых документов, таблиц и презентаций. Лицензии на офисное программное обеспечение для рабочих мест с целью обеспечения образовательного процесса Р7-Офис. Профессиональный (Десктоп + Сервер оптимальный) – Договор №30-АЭФ/44-ФЗ/2022

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Аудитория для самостоятельной работы и курсового проектирования	Ауд. 105 Магнитно-маркерная доска, учебная мебель, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС КубГУ	Антиплагиат-ВУЗ. Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ» версии 3.3. (интернет-версия). – Договор №19/АЭФ/44/ФЗ/2023 КонсультантПлюс - Справочная Правовая Система (КонсультантПлюс). Артикул правообладателя КонсультантПлюс – Договор №ГК/479/ЕП/223/ФЗ/2023 ГАРАНТ - Справочная Правовая Система (ГАРАНТ). «Компания АПИ «ГАРАНТ»» Артикул правообладателя ГАРАНТ – Договор №4920/НК/14 Р7-Офис - Desktopные редакторы текстовых документов, таблиц и презентаций. Лицензии на офисное программное обеспечение для рабочих мест с целью обеспечения образовательного процесса Р7-Офис. Профессиональный (Десктоп + Сервер оптимальный) – Договор №30-АЭФ/44-ФЗ/2022

Приложение 1

Экзамен "Информационная безопасность" 1 курс 40.05.01 ПОНБ

Время на выполнение заданий теста **(20 вопросов) - 20 минут.**

Каждый вопрос теста содержит три варианта ответов, один из которых правильный.

За каждый правильный ответ теста обучающийся получает 1 балл, за неправильный - 0 баллов.

Критерии перевода набранных баллов в оценку:

0-9 баллов - "неудовлетворительно"

10-13 баллов - "удовлетворительно"

14-17 баллов - "хорошо"

18-20 баллов - "отлично"

Вариант 1

1.Специальной категорией персональных данных являются сведения о (об):
(Баллов: 1)

- ☐ фамилии и имени гражданина
- ☐ идентификационном номере налогоплательщика
- ☐ политических взглядах гражданина

2.Защита информации, в соответствии с положениями № 149-ФЗ "Об информации, информационных технологиях и о защите информации", представляет собой комплекс:
(Баллов: 1)

- ☐ организационно-технических мер
- ☐ правовых, организационных, технических мер

- ☐ правовых, криптографических, криминалистических, специальных мер
3. Среди видов угроз информации, изменение состава и содержания её сведений, образуют:
(Баллов: 1)
- ☐ уничтожение
- ☐ модификацию
- ☐ блокирование
4. Одним из видов технических мер обеспечения информационной безопасности, является:
(Баллов: 1)
- ☐ сертификация средств обеспечения информационной безопасности
- ☐ использование антивирусного программного обеспечения
- ☐ оформление юридической документации
5. Среди видов угроз информации, полное разрушение её целостности как программными, так и физическими средствами, образуют:
(Баллов: 1)
- ☐ модификацию
- ☐ уничтожение
- ☐ ознакомление
6. Основным принципом симметричного шифрования выступает:
(Баллов: 1)
- ☐ расшифровывание информации возможно как с помощью ключа, имеющего определенное соотношение к ключу, которым производилось её зашифровывание, так и с помощью того же ключа, которым производилось её зашифровывание
- ☐ расшифровывание информации возможно только с помощью того же ключа, которым производилось её зашифровывание
- ☐ расшифровывание информации возможно только с помощью ключа, имеющего определенное соотношение к ключу, которым производилось её зашифровывание
7. Целью защиты информации выступает:
(Баллов: 1)
- ☐ обратимость данных

- ☐ доступность данных
- ☐ компилируемость данных

8.Время, необходимое для взлома шифра, или количество всех возможных ключей шифра, определяют [...] алгоритма шифрования

(Баллов: 1)

- ☐ конфиденциальность информации
- ☐ криптостойкость
- ☐ кодификационные параметры

9.Санкционированным является доступ к информации, который:

(Баллов: 1)

- ☐ соответствует правилам организации (учреждения) по разграничению доступа пользователей
- ☐ соответствует внутреннему убеждению пользователя о правомерности доступа к информации
- ☐ соответствует только техническим параметрам подключения к защищаемой компьютерной сети

10.Одной из организационных мер защиты информации, выступает:

(Баллов: 1)

- ☐ использование программ антивирусной защиты
- ☐ установление пропускного режима на территорию и в помещения организации
- ☐ использование программных средств зашифровывания информации

11.Российская Федерация защищает правовыми средствами:

(Баллов: 1)

- ☐ информацию, нарушающую тайну личной жизни, личную и семейную тайну
- ☐ информацию, распространяемую зарегистрированными средствами массовой информации
- ☐ информацию, унижающую честь и достоинство граждан

12.Эвристический анализ, осуществляемый антивирусной программой, предполагает:

(Баллов: 1)

- ☐ поиск вредоносных программ по описанию их размера, расширения, имени файла

- ☐ поиск вредоносных программ, добавленных в базы данных антивирусной программы
- ☐ поиск вредоносных программ, отсутствующих в базах данных антивирусной программы

13.Необходимость введения логина и пароля, подтверждающих факт формирования определенным лицом, определяет сущность [...] электронной подписи

(Баллов: 1)

- ☐ простой
- ☐ неквалифицированной
- ☐ квалифицированной

14.Правовая защита информации включает в себя:

(Баллов: 1)

- ☐ использование различных технических средств для обеспечения защиты информации
- ☐ регламентацию производственной деятельности работодателя с работником в сфере защиты информации
- ☐ совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в сфере защиты информации

15.Деятельность, направленная на предотвращение утечки информации, несанкционированных действий с информацией:

(Баллов: 1)

- ☐ защита информации
- ☐ конфиденциальность информации
- ☐ предоставление информации

16.Подход к представлению информации как универсальному свойству материи, составляют сущность:

(Баллов: 1)

- ☐ функционализма
- ☐ атрибутизма
- ☐ антропоцентризма

17.Открытым называется такой ключ шифрования, в котором:

(Баллов: 1)

- ☐ ключи пользователей одного алгоритма шифрования перераспределяются между ними каждую минуту
- ☐ ключи пользователей могут быть расшифрованы с помощью метода перебора ключей за одни сутки
- ☐ ключи пользователей размещены в открытых для доступа хранилищах

18.DDoS-атака на сервер или компьютерную сеть, преследует цель:

(Баллов: 1)

- ☐ перехват передаваемых по сети данных пользователем
- ☐ невозможность получения доступа к ресурсам сети пользователем
- ☐ установка звукозаписывающих или видеозаписывающих устройств на компьютер пользователя

19.Метод симметричного шифрования, заключающийся в том, что символы шифруемого текста последовательно складываются с символами некоторой специально подготовленной последовательности:

(Баллов: 1)

- ☐ аналитическое преобразование
- ☐ гаммирование
- ☐ перестановка

20.Атака методом грубой силы (brute-force attack), в криптографии представляет собой:

(Баллов: 1)

- ☐ осуществление исчерпывающего перебора ключей для раскрытия шифра
- ☐ применение физической силы и попыток к специалисту-криптографу, для получения от него информации об используемом алгоритме шифрования
- ☐ использование специализированной компьютерной программы для несанкционированного уничтожения зашифрованной информации и ее источника

Вариант 2

1.Одним из видов технических мер обеспечения информационной безопасности, является:

(Баллов: 1)

- ☐ сертификация средств обеспечения информационной безопасности

- ☐ использование антивирусного программного обеспечения
- ☐ оформление юридической документации

2. Среди видов угроз информации, полное разрушение её целостности как программными, так и физическими средствами, образуют:

(Баллов: 1)

- ☐ модификацию
- ☐ уничтожение
- ☐ ознакомление

3. Основным принципом симметричного шифрования выступает:

(Баллов: 1)

- ☐ расшифровывание информации возможно как с помощью ключа, имеющего определенное соотношение к ключу, которым производилось ее зашифровывание, так и с помощью того же ключа, которым производилось ее зашифровывание
- ☐ расшифровывание информации возможно только с помощью того же ключа, которым производилось ее зашифровывание
- ☐ расшифровывание информации возможно только с помощью ключа, имеющего определенное соотношение к ключу, которым производилось ее зашифровывание

4. Целью защиты информации выступает:

(Баллов: 1)

- ☐ обратимость данных
- ☐ доступность данных
- ☐ компилируемость данных

5. Время, необходимое для взлома шифра, или количество всех возможных ключей шифра, определяют [...] алгоритма шифрования

(Баллов: 1)

- ☐ конфиденциальность информации
- ☐ криптостойкость
- ☐ кодификационные параметры

6. Санкционированным является доступ к информации, который:

(Баллов: 1)

- ☐ соответствует правилам организации (учреждения) по разграничению доступа пользователей

- ☐ соответствует внутреннему убеждению пользователя о правомерности доступа к информации
- ☐ соответствует только техническим параметрам подключения к защищаемой компьютерной сети

7.Одной из организационных мер защиты информации, выступает:
(Баллов: 1)

- ☐ использование программ антивирусной защиты
- ☐ установление пропускного режима на территорию и в помещения организации
- ☐ использование программных средств зашифровывания информации

8.Российская Федерация защищает правовыми средствами:
(Баллов: 1)

- ☐ информацию, нарушающую тайну личной жизни, личную и семейную тайну
- ☐ информацию, распространяемую зарегистрированными средствами массовой информации
- ☐ информацию, унижающую честь и достоинство граждан

9.Эвристический анализ, осуществляемый антивирусной программой, предполагает:
(Баллов: 1)

- ☐ поиск вредоносных программ по описанию их размера, расширения, имени файла
- ☐ поиск вредоносных программ, добавленных в базы данных антивирусной программы
- ☐ поиск вредоносных программ, отсутствующих в базах данных антивирусной программы

10.Необходимость введения логина и пароля, подтверждающих факт формирования определенным лицом, определяет сущность [...] электронной подписи
(Баллов: 1)

- ☐ простой
- ☐ неквалифицированной
- ☐ квалифицированной

11.Правовая защита информации включает в себя:
(Баллов: 1)

- ☐ использование различных технических средств для обеспечения защиты информации
- ☐ регламентацию производственной деятельности работодателя с работником в сфере защиты информации
- ☐ совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в сфере защиты информации

12. Деятельность, направленная на предотвращение утечки информации, несанкционированных действий с информацией:

(Баллов: 1)

- ☐ защита информации
- ☐ конфиденциальность информации
- ☐ предоставление информации

13. Подход к представлению информации как универсальному свойству материи, составляют сущность:

(Баллов: 1)

- ☐ функционализма
- ☐ атрибутизма
- ☐ антропоцентризма

14. Открытым называется такой ключ шифрования, в котором:

(Баллов: 1)

- ☐ ключи пользователей одного алгоритма шифрования перераспределяются между ними каждую минуту
- ☐ ключи пользователей могут быть расшифрованы с помощью метода перебора ключей за одни сутки
- ☐ ключи пользователей размещены в открытых для доступа хранилищах

15. DDoS-атака на сервер или компьютерную сеть, преследует цель:

(Баллов: 1)

- ☐ перехват передаваемых по сети данных пользователем
- ☐ невозможность получения доступа к ресурсам сети пользователем
- ☐ установка звукозаписывающих или видеозаписывающих устройств на компьютер пользователя

16. Метод симметричного шифрования, заключающийся в том, что символы шифруемого текста последовательно складываются с символами некоторой специально подготовленной последовательности:

(Баллов: 1)

- ☐ аналитическое преобразование
- ☐ гаммирование
- ☐ перестановка

17. Атака методом грубой силы (brute-force attack), в криптографии представляет собой:

(Баллов: 1)

- ☐ осуществление исчерпывающего перебора ключей для раскрытия шифра
- ☐ применение физической силы и попыток к специалисту-криптографу, для получения от него информации об используемом алгоритме шифрования
- ☐ использование специализированной компьютерной программы для несанкционированного уничтожения зашифрованной информации и ее источника

18. Специальной категорией персональных данных являются сведения о (об):

(Баллов: 1)

- ☐ фамилии и имени гражданина
- ☐ идентификационном номере налогоплательщика
- ☐ политических взглядах гражданина

19. Защита информации, в соответствии с положениями № 149-ФЗ "Об информации, информационных технологиях и о защите информации", представляет собой комплекс:

(Баллов: 1)

- ☐ организационно-технических мер
- ☐ правовых, организационных, технических мер
- ☐ правовых, криптографических, криминалистических, специальных мер

20. Среди видов угроз информации, изменение состава и содержания её сведений, образуют:

(Баллов: 1)

- ☐ уничтожение
- ☐ модификацию
- ☐ блокирование

Вариант 3

1.Целью защиты информации выступает:

(Баллов: 1)

- ☐ обратимость данных
- ☐ доступность данных
- ☐ компилируемость данных

2.Время, необходимое для взлома шифра, или количество всех возможных ключей шифра, определяют [...] алгоритма шифрования

(Баллов: 1)

- ☐ конфиденциальность информации
- ☐ криптостойкость
- ☐ кодификационные параметры

3.Санкционированным является доступ к информации, который:

(Баллов: 1)

- ☐ соответствует правилам организации (учреждения) по разграничению доступа пользователей
- ☐ соответствует внутреннему убеждению пользователя о правомерности доступа к информации
- ☐ соответствует только техническим параметрам подключения к защищаемой компьютерной сети

4.Одной из организационных мер защиты информации, выступает:

(Баллов: 1)

- ☐ использование программ антивирусной защиты
- ☐ установление пропускного режима на территорию и в помещения организации
- ☐ использование программных средств зашифровывания информации

5.Российская Федерация защищает правовыми средствами:

(Баллов: 1)

- ☐ информацию, нарушающую тайну личной жизни, личную и семейную тайну
- ☐ информацию, распространяемую зарегистрированными средствами массовой информации
- ☐ информацию, унижающую честь и достоинство граждан

6.Эвристический анализ, осуществляемый антивирусной программой, предполагает:

(Баллов: 1)

- ☐ поиск вредоносных программ по описанию их размера, расширения, имени файла
- ☐ поиск вредоносных программ, добавленных в базы данных антивирусной программы
- ☐ поиск вредоносных программ, отсутствующих в базах данных антивирусной программы

7.Необходимость введения логина и пароля, подтверждающих факт формирования определенным лицом, определяет сущность [...] электронной подписи

(Баллов: 1)

- ☐ простой
- ☐ неквалифицированной
- ☐ квалифицированной

8.Правовая защита информации включает в себя:

(Баллов: 1)

- ☐ использование различных технических средств для обеспечения защиты информации
- ☐ регламентацию производственной деятельности работодателя с работником в сфере защиты информации
- ☐ совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в сфере защиты информации

9.Деятельность, направленная на предотвращение утечки информации, несанкционированных действий с информацией:

(Баллов: 1)

- ☐ защита информации
- ☐ конфиденциальность информации
- ☐ предоставление информации

10.Подход к представлению информации как универсальному свойству материи, составляют сущность:

(Баллов: 1)

- ☐ функционализма
- ☐ атрибутизма
- ☐ антропоцентризма

11.Открытым называется такой ключ шифрования, в котором:

(Баллов: 1)

- ☐ ключи пользователей одного алгоритма шифрования перераспределяются между ними каждую минуту
- ☐ ключи пользователей могут быть расшифрованы с помощью метода перебора ключей за одни сутки
- ☐ ключи пользователей размещены в открытых для доступа хранилищах

12.DDoS-атака на сервер или компьютерную сеть, преследует цель:

(Баллов: 1)

- ☐ перехват передаваемых по сети данных пользователем
- ☐ невозможность получения доступа к ресурсам сети пользователем
- ☐ установка звукозаписывающих или видеозаписывающих устройств на компьютер пользователя

13.Метод симметричного шифрования, заключающийся в том, что символы шифруемого текста последовательно складываются с символами некоторой специально подготовленной последовательности:

(Баллов: 1)

- ☐ аналитическое преобразование
- ☐ гаммирование
- ☐ перестановка

24.Атака методом грубой силы (brute-force attack), в криптографии представляет собой:

(Баллов: 1)

- ☐ осуществление исчерпывающего перебора ключей для раскрытия шифра
- ☐ применение физической силы и пыток к специалисту-криптографу, для получения от него информации об используемом алгоритме шифрования
- ☐ использование специализированной компьютерной программы для несанкционированного уничтожения зашифрованной информации и ее источника

15.Специальной категорией персональных данных являются сведения о (об):

(Баллов: 1)

- ☐ фамилии и имени гражданина
- ☐ идентификационном номере налогоплательщика
- ☐ политических взглядах гражданина

16.Защита информации, в соответствии с положениями № 149-ФЗ "Об информации, информационных технологиях и о защите информации", представляет собой комплекс:

(Баллов: 1)

- ☐ организационно-технических мер
- ☐ правовых, организационных, технических мер
- ☐ правовых, криптографических, криминалистических, специальных мер

17. Среди видов угроз информации, изменение состава и содержания её сведений, образуют:

(Баллов: 1)

- ☐ уничтожение
- ☐ модификацию
- ☐ блокирование

18. Одним из видов технических мер обеспечения информационной безопасности, является:

(Баллов: 1)

- ☐ сертификация средств обеспечения информационной безопасности
- ☐ использование антивирусного программного обеспечения
- ☐ оформление юридической документации

19. Среди видов угроз информации, полное разрушение её целостности как программными, так и физическими средствами, образуют:

(Баллов: 1)

- ☐ модификацию
- ☐ уничтожение
- ☐ ознакомление

20. Основным принципом симметричного шифрования выступает:

(Баллов: 1)

- ☐ расшифровывание информации возможно как с помощью ключа, имеющего определенное соотношение к ключу, которым производилось её зашифровывание, так и с помощью того же ключа, которым производилось её зашифровывание
- ☐ расшифровывание информации возможно только с помощью того же ключа, которым производилось её зашифровывание
- ☐ расшифровывание информации возможно только с помощью ключа, имеющего определенное соотношение к ключу, которым производилось её зашифровывание

