МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ,
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

ГОУ ВПО Кыргызско-Российский Славянский университет им. Б.Н. Ельцина

МОДУЛЬ: ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Математическое моделирование информационных технологий в юриспруденции

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Судебной экспертизы**

Учебный план b40030134_21_1ю.plx
Направление 40.03.01 - РФ, 530500 - КР Юриспруденция

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 36
самостоятельная работа 35,8

Виды контроля в семестрах:
зачеты с оценкой 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
Недель	15			
Вид занятий	УП	РП	УП	РП
Практические	36	36	36	36
Контактная работа в период теоретического обучения	0,2	0,2	0,2	0,2
В том числе инт.	8	8	8	8
Итого ауд.	36	36	36	36
Контактная работа	36,2	36,2	36,2	36,2
Сам. работа	35,8	35,8	35,8	35,8
Итого	72	72	72	72

Программу составил(и):
Старший преподаватель, Коваль Ирина Геннадьевна _____

Рецензент(ы):
д.ю.н., профессор, Тугельбаева Б.Г. _____

Рабочая программа дисциплины
Математическое моделирование информационных технологий в юриспруденции

разработана в соответствии с ФГОС 3++:
Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 40.03.01 Юриспруденция (уровень бакалавриата) (приказ Минобрнауки России от 13.08.2020г. №1011)

составлена на основании учебного плана:
Направление 40.03.01 - РФ, 530500 - КР Юриспруденция
утвержденного учёным советом вуза от 29.06.2021 протокол № 10.

Рабочая программа одобрена на заседании кафедры
Судебной экспертизы

Протокол от 02.09.2021 г. № 1
Срок действия программы: 2021-2025 уч.г.
Зав. кафедрой к.ю.н., Тыныбеков Н.Т.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
_7_ ___09_____ 2022 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры
Судебной экспертизы

Протокол от _6_ ____09_____ 2022 г. № _1
Зав. кафедрой к.ю.н., Тыныбеков Н.Т

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
__ _____ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
Судебной экспертизы

Протокол от __ _____ 2023 г. № __
Зав. кафедрой к.ю.н., Тыныбеков Н.Т

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
__ _____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры
Судебной экспертизы

Протокол от __ _____ 2024 г. № __
Зав. кафедрой к.ю.н., Тыныбеков Н.Т.

Визирование РПД для исполнения в очередном учебном году

Председатель УМС
__ _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Судебной экспертизы

Протокол от __ _____ 2025 г. № __
Зав. кафедрой к.ю.н., Тыныбеков Н.Т

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цель дисциплины «Математическое моделирование информационных технологий в юриспруденции» в системе подготовки юриста – освоение математических знаний, необходимых для решения прикладных юридических задач и способствующих развитию умений рассуждать, быть логичным, убедительным, моделировать реальные правовые процессы, прогнозировать результат на основе статистических данных. Для достижения данной цели обозначаются и решаются следующие задачи: применение современные информационные технологий для проведения статистического анализа информации; осуществление перевода информации с языка, характерного для предметной области на математический язык; подборка задач для реализации поставленной учебной цели; использование основных методы статистической обработки экспериментальных данных; разработка математических моделей, связанных с исследованием прикладных задач; самостоятельно изучать математическую литературу, анализировать полученные результаты, выступать с научными сообщениями.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.О.11
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Для освоения дисциплины необходимы знания, умения и компетенции, полученные обучающимися в средней общеобразовательной школе, и при изучении профессиональных дисциплин 1курса.
2.1.2	Курс «Математическое моделирование информационных технологий в юриспруденции» предполагает наличие базовых знаний из курса математики средней школы и дисциплин «Информационные технологии в юридической деятельности» и «Современные информационные технологии».
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Нет в программе бакалавриата

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Сущность информации, основные свойства информации и закономерности развития современного информационного общества; основные закономерности создания и функционирования информационных процессов в правовой сфере; основы государственной политики в области информатики; методы и средства поиска, систематизации и обработки правовой информации; место и роль математики в современном мире, мировой культуре и истории и юриспруденции.
3.1.2	Сущность информации, основные свойства информации и закономерности развития современного информационного общества; основные закономерности создания и функционирования информационных процессов в правовой сфере; основы государственной политики в области информатики; методы и средства поиска, систематизации и обработки правовой информации; основные математические понятия и методы решения базовых математических задач, рассматриваемых в рамках дисциплины; математические методы анализа и обработки правовой информации.
3.2	**Уметь:**
3.2.1	Распознавать опасности и угрозы, возникающие в процессе работы с секретной информацией; применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов и проведения статистического анализа информации; применять современные информационные технологии для проведения статистического анализа информации; осуществлять перевод информации с языка, характерного для предметной области на математический язык; подбирать задачи для реализации поставленной учебной цели; использовать основные методы статистической обработки экспериментальных данных.
3.2.2	Распознавать опасности и угрозы, возникающие в процессе работы с секретной информацией; применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов и проведения статистического анализа информации; разрабатывать математические модели, связанные с исследованием прикладных задач в правовой сфере; самостоятельно изучать математическую литературу, анализировать полученные результаты, выступать с научными сообщениями.
3.3	**Владеть:**
3.3.1	Навыками сбора и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности; навыками обработки конфиденциальной информации, в том числе содержащей государственную тайну, в соответствии со всеми требованиями по защите информации; математической символикой для выражения количественных и качественных отношений между элементами математических моделей.

3.3.2	Навыками сбора и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности; навыками обработки конфиденциальной информации, в том числе содержащей государственную тайну, в соответствии со всеми требованиями по защите информации; методами сбора и обработки данных; навыками обработки математической информации имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности; навыками анализа и оценки полученных результатов.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Пр. подг.	Примечание
	Раздел 1. Разбор практических ситуаций (Мат. логика, комбинаторика)							
1.1	Логика, наука о формах и законах человеческого мышления.Становление формальной логики. /КрТО/	7	0,05		Л1.1 Л1.2Л2.1			
1.2	Алгебра высказываний /Пр/	7	2		Л1.1 Л1.2Л2.1	2		Презентация "Основы матлогики_1"
1.3	Матлогика в юриспруденции. Законы логики /Пр/	7	2		Л1.1 Л1.2Л2.1			
1.4	Законы логики: инверсия, конъюнкция, дизъюнкция /Ср/	7	1,8		Л1.1 Л1.2Л2.1			
1.5	Правила построения таблиц истинности. Применение таблиц истинности для решения задач, возникающих в правой сфере /Пр/	7	2		Л1.1 Л1.2Л2.1			
1.6	Посторение таблиц истинности /Ср/	7	2		Л1.1 Л1.2Л2.1			
1.7	Преобразование логических операций /Пр/	7	2		Л1.1 Л1.2Л2.1	2		Презентация "Основы матлогики_2"
1.8	Законы логических преобразований /Ср/	7	2		Л1.1 Л1.2Л2.1			
1.9	Законы логических преобразований (тавтология) /Ср/	7	2		Л1.1 Л1.2Л2.1			
1.10	Основы комбинаторики /КрТО/	7	0,1		Л1.1Л2.1			
1.11	Комбинаторика,раздел математики,занимающийся подсчетом всех возможных комбинаций, составленных по некоторму правилу /Пр/	7	2		Л1.1 Л1.2Л2.1	2		Презентация "Основы комбинаторики и теории вероятности"
1.12	Основные комбинаторные конфигурации /Пр/	7	2		Л1.1 Л1.2Л2.1			
1.13	Сочетания, размещения, перестановки /Ср/	7	2		Л1.1 Л1.2Л2.1			
1.14	Комбинаторные методы для решения задач, возникающих в правой сфере /Пр/	7	2		Л1.1 Л1.2Л2.1			
1.15	Размещения /Ср/	7	2		Л1.1 Л1.2Л2.1			
1.16	Сочетания /Ср/	7	2		Л1.1 Л1.2Л2.1			
1.17	Перестановки /Ср/	7	2		Л1.1 Л1.2Л2.1			

	Раздел 2. Разбор практических ситуаций (Теория вероятности, множеств, криптография)							
2.1	Терия вероятности отражает закономерности, присущие случайным событиям массового характера /Пр/	7	2		Л1.2 Л1.1Л2.1			
2.2	Классическая формула вероятности /Пр/	7	2		Л1.1 Л1.2Л2.1			
2.3	Случайные события /Ср/	7	2		Л1.1 Л1.2Л2.1			
2.4	Типы событий. Совместные, несовместные, зависимые и независимые события /Ср/	7	2		Л1.1 Л1.2Л2.1			
2.5	Классическая формула вероятности /Ср/	7	2		Л1.1 Л1.2Л2.1			
2.6	Условная вероятность /Пр/	7	2		Л1.1 Л1.2Л2.1			
2.7	Условная вероятность /Ср/	7	2		Л1.1 Л1.2Л2.1			
2.8	Формула полной вероятности /Пр/	7	2		Л1.1 Л1.2Л2.1			
2.9	Формула Байеса. Формула Бернулли /Пр/	7	2		Л1.1 Л1.2Л2.1			
2.10	Формула полной вероятности. /Ср/	7	2		Л1.1 Л1.2Л2.1			
2.11	Формула Байеса. Формула Бернулли /Ср/	7	2		Л1.1 Л1.2Л2.1			
2.12	Теория множеств. Основные понятия множества /Пр/	7	2		Л1.1 Л1.2Л2.1			
2.13	Типы множеств.Операции над множествами /Пр/	7	2		Л1.1 Л1.2Л2.1			
2.14	Графическое отображение множеств /Ср/	7	2		Л1.1 Л1.2Л2.1			
2.15	Криптология /КрТО/	7	0,05		Л1.1Л2.1			
2.16	Криптография, наука о сохранении секретов. Симметричное и ассиметричное шифрование /Пр/	7	2		Л1.1 Л1.2Л2.1	2		Презентация "Математические основы криптографии. Криптология"
2.17	Математические методы шифрования. Шифр Цезаря, матричное шифрование /Пр/	7	2		Л1.1 Л1.2Л2.1			
2.18	Шифры сложной замены. Шифры Виженера, Гронсфельда, арифметика остатков /Пр/	7	2		Л1.1 Л1.2Л2.1			
2.19	Шифры сложной замены /Ср/	7	2		Л1.1 Л1.2Л2.1			
2.20	Ассиметричное шифрование. Алгоритм RSA /Пр/	7	2		Л1.1 Л1.2Л2.1 Э1			
2.21	Алгоритм RSA /Ср/	7	2		Л1.1 Л1.2Л2.1			
2.22	Хеширование. Электронно-цифровая подпись /Ср/	7	2		Л1.1 Л1.2Л2.1			
2.23	/ЗачётСОц/	7			Л1.1 Л1.2Л2.1			

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Вопросы для проверки уровня обученности ЗНАТЬ:
1. Предмет математики. Аксиоматический метод
2. История развития математики
3. Роль математики в современном мире
4. Математические методы в юриспруденции
5. Понятие множества
6. Классификация множеств. Подмножества
7. Операции над множествами
8. Дополнение множеств. Мощность множеств
9. Предмет и история развития математической логики
10. Понятие высказывания. Простые и сложные высказывания
11. Логические операции
12. Моделирование логической структуры правовой нормы
13. Логические формулы
14. Равносильность логических формул
15. Тавтологии
16. Доказательства логических заключений
17. Логические задачи
18. Предмет теории вероятностей
19. События и испытания
20. Классическое определение вероятности
21. Элементы комбинаторики
22. Вычисление вероятности с помощью классического определения
23. Геометрическое и статистическое определения вероятности
24. Алгебра событий
25. Вероятность суммы случайных событий
26. Вероятность произведения событий
27. Формула полной вероятности. Формула Байеса
28. Формула Бернулли
29. Понятие случайной величины. Закон распределения дискретной случайной величины
30. Числовые характеристики дискретных случайных величин
31. Функция распределения
32. Непрерывные случайные величины. Плотность распределения вероятностей
33. Закон равномерного распределения вероятностей
34. Нормальный закон распределения
35. Классификация множеств
36. Подмножества
37. Операции над множествами
38. Диаграммы Эйлера
39. Дополнение множеств
40. Мощность множеств
41. Криптография
42. Шифры в криптографии
43. Шифрование в криптографии
44. Открытый (исходный) текст
45. Криптосистема
46. Шифрованный (закрытый) текст
47. Криптографические ключи
48. Криптоанализ
49. Криптографическая стойкость
50. Криптология

Задания для проверки уровня обученности УМЕТЬ и ВЛАДЕТЬ:
По заданному материалу:
1. Выделять простые высказывания из сложных высказываний
2. Использовать логические связи в сложных высказываниях
3. Применять законы логики для нахождения истинности логических выражений
4. Уметь строить таблицы истинности
5. По таблицам истинности делать правильные выводы
6. Применять законы логики для преобразования и упрощения логических выражений
7. Уметь пользоваться правилами комбинаторики
8. Распознавать комбинаторные объекты
9. Уметь применять формулы сочетания, размещения и перестановки
10. Пользоваться формулой классической вероятности
11. Различать события по типам
12. Теорема сложения вероятностей

13. Теорема умножения вероятностей
14. Применять формулу Байеса
15. Применять формулу Бернулли
16. Классифицировать множества
17. Работать с диаграммами Эйлера
18. Уметь производить операции над множествами
19. Распознавать способы шифрования
20. Шифровать закрытыми ключами
21. Шифровать открытыми ключами

5.2. Темы курсовых работ (проектов)

Не предусмотрены дисциплиной(модулем)

5.3. Фонд оценочных средств

1.ПРАКТИЧЕСКОЕ ЗАДАНИЕ. Перечень заданий в ПРИЛОЖЕНИИ 32.КОМПЛЕКТ ЗАДАНИЙ ПО ВАРИАНТАМ К КОНТРОЛЬНЫМ РАБОТАМ
Контрольная работа проводится по вариантам. Вариант содержит 3 задания, одно посвящено нахождению истинности логического выражения, вторая построению таблицы истинности на логическое выражение, третья нахождению истинности алгебраического выражения.
Вариант№1
I. Постройте таблицу истинности логической формулы:
NOT (a OR b) AND (NOT a OR b)
II. 4 человека подозревается в угоне машины: Никонов, Маралбаев, Лапенко и Рузиметов. Один из них был организатором. 3 следователя вели допросы. После допросов следователи сделали выводы:
1 следователь: организатор Никонов, а Маралбаев помощник.
2 следователь: помощник Лапенко, а Рузиметов – стоял на страже.
3 следователь: Рузиметов - водитель, а Никонов - помощник.
Оказалось, что каждый из следователей был прав только в одном из своих выводов.
Вопрос: При помощи таблицы истинности выясните, кто был организатором, помощником, водителем и кто стоял на страже: Никонов, Маралбаев, Лапенко, Рузиметов?
Вариант№2
I. На складе совершено хищение. Подозрение пало на трех человек: Алымкулова, Багазиева, и Сергеева, они были доставлены для допроса. Установлено следующее:
1. Никто, кроме Алымкулова, Багазиева, и Сергеева, не был замешан в деле.
2. Алымкулов никогда не ходит на дело без, по крайней мере, одного соучастника.
3. Сергеев не виновен.
Вопрос: Виновен ли Байгазиев? Узнайте это, применяя метод преобразования логических операций.
II. В коробке для срочных документов лежат 12 дел с убийствами и 9 дел с кражами (все разные). Судья Павлов выбирает или 1 дело с убийством, или 1 дело с кражей, после него из оставшихся дел судья Назирова выбирает дело с убийством и дело с кражей.
Вопрос:
1. Сколько возможно таких выборов?
2. При каком выборе Павлова у Назировой больше возможностей выбора?
Вариант№3
I. Вероятность выпуска бракованного изделия на станке равна 0,2. Определить вероятность того, что в партии из десяти выпущенных на данном станке деталей ровно k будут без брака.
Вопрос: Какова вероятность для k = 0, 1, 10.
II. Постройте таблицу истинности логической формулы: (NOT a OR b)OR NOT c
Вариант№4
I. Постройте таблицу истинности логической формулы:
(a AND b) OR (NOT a AND NOT b)
II. В некотором поселке банда собирается грабить магазин. Сотрудник УГРО прибывает на место, и спрашивает одного из местных жителей: «Есть ли в поселке магазин?». В ответ на его вопрос он заявляет: «Магазин есть в том и только в том случае, если я бандит». Примечание. Одни из участников разговора всегда говорит только правду, если он не бандит
Вопрос:
1. Можно ли определить, кто такой этот местный - бандит или нет?
2. Можно ли определить, есть ли магазин в поселке?
Вариант№5
I. В деле об убийстве имеются двое подозреваемых - Ишанкулов и Петренко. Допросили четырех свидетелей, которые последовательно дали такие показания:
A- Ишанкулов не виноват, Петренко не виноват;
B- Из двух первых показаний, по меньшей мере, одно истинно;
C - Показания третьего ложны;
D - Четвертый свидетель оказался прав.
Вопрос: При помощи таблицы истинности выясните, кто виновен?
II. Во время встречи 16 человек пожали друг другу руки.
Вопрос: Сколько всего сделано рукопожатий?
Вариант№6
I. Постройте таблицу истинности логической формулы:

NOT(a OR NOT b AND NOT c)
II. Программа экзамена содержит 25 вопросов, из которых студент знает 20. Преподаватель последовательно задает 3 вопроса. Вопрос: Какова вероятность того, что студент может ответить на вопросы A,B,C
Вариант№7
I . Стрелок производит два выстрела по мишени. Вероятность попадания при каждом выстреле 0,8. Составить полную группу событий и найти их вероятности.
II. Постройте таблицу истинности логической формулы: c AND(NOT a OR NOT b)
Вариант№8
I. Дело о хищении телефона Алихановой.
Подозреваемые: Ишанов, Палванов и Сатинбаева.
На вопрос: Кто из троих взял телефон Алихановой, был получен следующий ответ:
Неверно, что если телефон Алихановой брал Палванов, то и Сатинбаева брала телефон Алихановой, и если телефон взял Ишанов, то Палванов не брал.
Вопрос: Кто взял телефон Алихановой?
II. Постройте таблицу истинности логической формулы:
NOT b OR (a OR NOT b AND NOT c)

РАСЧЕТНО-ПРАКТИЧЕКСКИЕ РАБОТЫ
Кейс-задача. Проблемное задание, в котором студенту предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы.
ТЕМЫ РПР
- Зашифровать матричным способом слово ХИРОМАНТ
- Зашифровать матричным способом слово ЛЕКТОРИЙ
- Зашифровать матричным способом слово РАССТРЕЛ
- Зашифровать матричным способом слово СЕНСАЦИЯ
- Зашифровать матричным способом слово ПАМЯТНИК
- Зашифровать матричным способом слово СОВЕТНИК
- Алгоритм RSA. Выбрать два простых числа: p = 7, q = 17, e = 5. Вывести открытый и закрытый ключи и зашифровать слово МЕЛ
- Алгоритм RSA. Выбрать два простых числа: p =5, q = 17, e=7. Вывести открытый и закрытый ключи и зашифровать слово РОМ
- Алгоритм RSA. Два простых числа: p = 17 и q = 31, e=7.
- Вывести открытый и закрытый ключи и зашифровать слово КИС
- Алгоритм RSA. Два простых числа: p = 11 и q = 13, e=7.
- Вывести открытый и закрытый ключи и зашифровать слово ЛЮК
- Алгоритм RSA. Выбрать два простых числа: p = 5, q = 23, e =7.
- Вывести открытый и закрытый ключи и зашифровать слово МОЛ
- Алгоритм RSA. Выбрать два простых числа: p = 7, q = 17, e = 5.
-Вывести открытый и закрытый ключи и зашифровать слово КОТ

ТЕСТ. Тестовые вопросы и демонстрационные варианты тестов для фронтального опроса в ПРИЛОЖЕНИИ 2

5.4. Перечень видов оценочных средств

Тест
Выполнение практических работ
Расчетно - практические работы
Зачет

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Уткин В.Б., Балдин К.В., Рукосуев А.В.	Математика и информатика: Учебное пособие	М.: Издательско-торговая корпорация "Дашков и К" 2012
Л1.2	В.А. Копылов, Ю.Н. Миронова и др.	Инф и математика для юристов: Уч пособие	М 2003

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Андрианика Х.А., С.Я Казанцева	Информатика и математика для юристов: уч пособие для студентов вузов	М.: Юнити; Закон и право 2001

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Электронная библиотека	http://www.newlibrary.ru/genre/nauka/matematika/

6.3. Перечень информационных и образовательных технологий

6.3.1 Компетентностно-ориентированные образовательные технологии

6.3.1.1	Традиционные образовательные технологии: практические работы репродуктивного типа,
6.3.1.2	ориентированные, прежде всего на сообщение знаний и способов действий, передаваемых студентам в готовом виде и предназначенных для воспроизводящего усвоения и разбора конкретных ситуаций информационных технологий.
6.3.1.3	Инновационные образовательные технологии – занятия в интерактивной форме, которые формируют системное мышления и способность генерировать идеи при решении различных творческих задач. К ним относятся электронные тексты лекций с презентациями, кейс - задачи по информационным технологиям; использование интерактивной доски.
6.3.1.4	Информационные образовательные технологии – самостоятельное использование студентом компьютерной техники и Интернет-ресурсов для выполнения практических заданий и самостоятельной работы.

6.3.2 Перечень информационных справочных систем и программного обеспечения

6.3.2.1	Доступ к сети «Интернет» при самостоятельной работе.
6.3.2.2	Программное обеспечение: ОС Windows, Microsoft Office (MS Word, MS Excel, MS Power Point, MS ACCESS).
6.3.2.3	Интерактивная доска на базе Whiteboard DualPenS.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Лекционные и практические занятия проводятся в учебных аудиториях, оснащенных мультимедийным оборудованием (проектором, экраном, ПК). Для практических занятий – ауд.304, 305 (корпус 7), количество посадочных мест 11.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Технологическая карта дисциплины: ПРИЛОЖЕНИЕ5

МОДУЛЬНЫЙ КОНТРОЛЬ ПО ДИСЦИПЛИНЕ ВКЛЮЧАЕТ:

1. Текущий контроль: усвоение учебного материала на аудиторных занятиях (лекциях, практических занятиях, в том числе учитывается посещение и активность) и выполнение обязательных заданий для самостоятельной работы

2. Рубежный контроль: проверка полноты знаний и умений по материалу модуля в целом. Выполнение модульных контрольных заданий проводится в письменном виде или в электронном является обязательной компонентой модульного контроля.

3. Промежуточный контроль - завершенная задокументированная часть учебной дисциплины (7 семестр - зачет) – совокупность тесно связанных между собой зачетных модулей.

ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОМЕЖУТОЧНОМУ КОНТРОЛЮ

При явке на экзамены и зачёты студенты обязаны иметь при себе зачётные книжки, которые они предъявляют экзаменатору в начале экзамена или зачета. Преподавателю предоставляется право поставить зачёт без опроса по билету тем студентам, которые набрали более 60 баллов за текущий и рубежный контроли. На промежуточном контроле студент должен, верно, ответить на теоретические вопросы билета и определить основные принципы информационных технологий. Студенты могут использовать технические средства, справочно-нормативную литературу, учебные программы.

Оценка промежуточного контроля:

- min 20 баллов - Вопросы для проверки уровня обученности ЗНАТЬ (в случае, если при ответах на заданные вопросы студент правильно формулирует основные понятия)
- 20-25 баллов – Задания для проверки уровня обученности УМЕТЬ и ВЛАДЕТЬ (в случае, если студент правильно формулирует сущность заданной в билете проблемы и дает рекомендации по ее решению)
- 25-30 баллов - Задания для проверки уровня обученности УМЕТЬ и ВЛАДЕТЬ (в случае полного выполнения контрольного задания)

ОСНОВНЫЕ ТРЕБОВАНИЯ К ТЕКУЩЕМУ КОНТРОЛЮ.

Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:

1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня.

2. При подготовке к следующей лекции, нужно просмотреть текст предыдущего материала, подумать о том, какая может быть тема следующей лекции.

3. В течение недели выбрать время для работы с рекомендуемой литературой.

5. Для подготовки к лабораторным занятиям и выполнению самостоятельной работы необходимо сначала прочитать основные понятия и подходы по теме задания. Рекомендуется использовать методические указания по курсу, глоссарий (ПРИЛОЖЕНИЕ 6), конспекты и тезисы теоритического материала к практическим занятиям (ПРИЛОЖЕНИЕ 1) . При выполнении задания нужно сначала понять, что требуется в нем, какой теоретический материал нужно использовать, наметить план решения задачи, а затем приступить к расчетам и сделать качественный вывод. Рекомендуется использовать:

-Методические указания

-Электронные курсы

6. При подготовке к промежуточному и рубежному контролям нужно изучить теорию: определения всех понятий и

подходы к оцениванию до состояния понимания материала и самостоятельно выполнить несколько типовых заданий из каждой темы. При решении задач всегда необходимо уметь качественно интерпретировать итог решения.
7. Практические занятия призваны закрепить знания студентов по отдельным разделам курса «Математическое моделирование информационных технологий в юриспруденции» привить им первые навыки математического моделирования. Для практических занятий обязательным является изучение математических методов, используемых для решения задач, возникающих в правовой сфере. Практические занятия проводятся в специально оборудованных аудиториях (ауд.№304, 305) с применением необходимых средств обучения: персональных компьютеров
При выполнении практических работ студент должен:
-Отработать различные практические приемы, в том числе профессиональные, работа с оборудованием.
-Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
-Использовать информационно-коммуникационные технологии в профессиональной деятельности.
8. Отработки пропущенных занятий.
Контроль над усвоением студентами материала учебной программы дисциплины осуществляется систематически преподавателем кафедры и отражается в журнале преподавателя в баллах. Студент, получивший неудовлетворительную оценку по текущему материалу, обязан подготовить данный раздел и ответить по нему преподавателю на индивидуальном собеседовании. При фронтальном обучении неудовлетворительная оценка должна быть отработана в течение месяца со дня ее получения, при цикловом обучении - до конца цикла.
Отработка лабораторных занятий.
- Каждое занятие, пропущенное студентом без уважительной причины, отрабатывается в обязательном порядке. Отработки проводятся по расписанию кафедры, согласованному с деканатом.
- При фронтальном обучении пропущенные занятия должны быть отработаны в течение 10 дней со дня пропуска, при цикловом обучении - до конца цикла. Пропущенные студентом без уважительной причины практические занятия отрабатываются не более одного занятия в день. Пропущенные занятия по уважительной причине (по болезни, пропуски с разрешения деканата) отрабатываются по тематическому материалу без учета часов.
- Студент, не отработавший пропуск в установленные сроки, допускается к очередным занятиям только при наличии разрешения декана или его заместителя в письменной форме. Не разрешается устранение от очередного практического занятия студентов, слабо подготовленных к данным занятиям.
- Для студентов, пропустивших практические и лабораторные занятия из-за длительной болезни, отработка должна проводиться после разрешения деканата по индивидуальному графику, согласованному с кафедрой.
- В исключительных случаях (участие в межвузовских конференциях, соревнованиях, олимпиадах, дежурство и др.) декан и его заместитель по согласованию с кафедрой могут освобождать студентов от отработок некоторых пропущенных занятий.

РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ

ПРАКТИЧЕСКАЯ РАБОТА
Методические указания по выполнению практических работ в методических указаниях к практическим занятиям по курсу «Математическое моделирование информационных технологий в юриспруденции» для студентов специальности «Юриспруденция»

КОНТРОЛЬНАЯ РАБОТА
Методические указания по выполнению контрольных работ в методическом руководстве для практических занятий по курсу «Математическое моделирование информационных технологий в юриспруденции» для студентов специальности «Юриспруденция».

РПР (РАСЧЕТНО – ПРАКТИЧЕКСКАЯ РАБОТА)
Расчетно-практическая работа (РПР) – это самостоятельное исследование студента. Выполняя РПР, студент совершенствует знания и умения, полученные в процессе изучения дисциплины «Математическое моделирование информационных технологий в юриспруденции», а именно: определять цель, выделять задачи, формулировать проблемы и находить способы их решения. Работая над РПР студент, получает умения и навыки, которые будут полезными в будущем – при выполнении более сложных задач (дипломная работа, диссертация, научное исследование).
Выполнение расчетно–практической работы является одной из форм самостоятельной работы по дисциплине «ММИТвЮ».
Целью написания РПР является:
-систематизация, закрепление и расширение теоретических знаний и практических умений студента;
-приобретение опыта работы с литературой и другими источниками информации, умение обобщать и анализировать научную информацию, вырабатывать собственное отношение к проблеме;
-выработка умения применять информационные и компьютерные технологии для решения прикладных правовых задач;
-развитие навыков овладения специализированным программным обеспечением;
-проведение глубокого анализа результатов собственных исследований и формирование содержательных выводов относительно качества полученных результатов.
ЭТАПЫ ВЫПОЛНЕНИЯ РАСЧЕТНО–ПРАКТИЧЕСКОЙРАБОТЫ
Расчетно–практическая работа выполняется в соответствии с кредитно-модульной структурой дисциплины поэтапно:
-выбор темы РПР,
-определение актуальности и цели работы,
-подбор источников информации согласно избранной теме,
-систематизацию и структурирование данных,

-выбор метода обработки информации,
-обоснование и описание избранного метода,
-обработку информации,
-получение результатов,
-интерпретацию результатов,
-формулирование выводов,
-оформление отчета,
-подготовка к публичной защите выполненной работы.
Отчет о выполнении РПР оформляется в электронном виде. К отчету прилагаются электронные файлы с результатами обработки информации (текстовые файлы).
РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ РАСЧЕТНО-ПРАКТИЧЕКСКОЙ РАБОТЫ
Тема РПР согласовывается с преподавателем.
Цель РПР состоит в том, чтобы проанализировать определенную проблему. В ней сконцентрирована главная идея работы, ее конечный познавательный и теоретический результат. Цель должна носить практически-прикладной характер.

РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ТЕСТОВОЙ РАБОТЫ
1.Большая часть тестовых заданий адресована не только собственно к простому воспроизведению знаний, но к умению рассуждать, анализировать, создавать новые для себя знания в процессе выполнения теста;
2.При подготовке к контрольной работе, выполняя задания, следует определить, какие разделы изучены лучше, а какие – хуже, с тем, чтобы сосредоточить внимание на имеющихся «пробелах»;
3.Начинать выполнение теста с просмотра заданий, различая для себя легкие и трудные; приступать к выполнению работы, начиная с тех заданий, правильные ответы на которые не вызывают сомнений и в любом случае пользоваться черновиком;
4.Не останавливаться подолгу на отдельных трудных, а выполнять «пунктирно» посильные задания. Когда нерешенное задание оставляется «на потом», подсознательная работа над ним продолжается и может оказаться результативной;
5.Следует помнить, что для получения отличной и хорошей оценки необязательно правильное выполнение абсолютно всех 100% заданий.
6.Приступая к каждой части экзаменационной работы, всегда внимательно читать инструкцию; стремиться понять, как должен выглядеть ответ на задание и где его надо записать, т.к. от этого зависит правильное выполнение работы в целом;
7.При подготовке лучше заострить внимание на наиболее важных и узловых проблемах обществознания, т.к. именно им посвящено большее число заданий. Второстепенные факты и проблемы значительно реже включаются в содержание теста.
8.Для подготовки к тестированию целесообразно один из учебников взять за основу, дополняя его содержание при необходимости материалом из других источников.

ПРИЛОЖЕНИЕ1

ТЕЗИСЫ ЛЕКЦИЙ

Лекция 1. Логика в юриспруденции

Область юриспруденции представляет широкое поле для применения формализованных, абстрактно-научных приемов мышления, приемов математического аппарата, позволяющих найти однозначные, точные решения.

В настоящее время можно выделить основные направления применения математических методов с целью моделирования социально-правовых явлений и процессов в праве.

Одним из направлений использования математических методов в юридической деятельности и государственном управлении является правотворчество. Все правовые нормы имеют форму логических суждений, т.е. таких предложений, в которых что-либо утверждается, либо отрицается об объектах и отношениях действительности. Поэтому для изучения правовых норм, может и должна использоваться **математическая логика**, методы которой в правотворческом процессе позволяют:

1. Улучшить редакцию правовых норм, устранить нечеткие формулировки, упростить громоздкие структуры;
2. Исследовать нормативно-правовой акт на непротиворечивость;
3. Символически представить юридические знания для их дальнейшей автоматизированной обработки и компьютеризированного поиска, промоделировать логическую структуру правовой нормы;
4. Совершенствовать уровень логической завершенности правовых актов и норм права, совершенствовать их логическую структуру;
5. Уточнить логический смысл и содержание правовых норм путем их толкования;
6. Проводить логическую экспертизу нормативных правовых актов.

Лекция 2. Матлогика в юриспруденции Основной задачей **математической логики,** являются вопросы применения математических методов для решения логических задач и построения логических схем.

Слово **«Логика»** означает систематический метод рассуждений, или анализ методов рассуждений. **Логика** не интересуется истинностью или ложностью отдельных **посылок** и **заключений,** она только **выясняет**, вытекает ли истинность заключения данного рассуждения из истинности его **посылок.** Другими словами можно сказать, что **логика** это наука о законах доказательных рассуждений **(высказываний**).

Логика высказываний - раздел логики, в котором вопрос об истинности или ложности **высказываний** рассматривается и решается на основе изучения способа построения высказываний с помощью **логических связок.**

Математическая модель — математическое представление реальности, один из вариантов модели, как системы, исследование которой позволяет получать информацию о некоторой другой системе.

Логическое моделирование дает возможность ясно, четко и наглядно представить логическую структуру правовой нормы. Это особенно важно, если учесть, что словесная форма правовых норм может нередко скрывать или затемнять присущие им логические связи. В законодательной практике можно найти такие правовые нормы, которые нарушают требования логики, страдают логическими дефектами. Поэтому анализ норм права имеет важное практическое значение.

Лекция 3. Комбинаторика

Комбинаторика — раздел математики, посвященный решению задач выбора и расположения элементов некоторого, обычно конечного, **множества** в соответствии с заданными правилами. Каждое такое правило определяет способ построения некоторой конструкции из элементов исходного **множества,** называемой **комбинаторной конфигурацией**.

В комбинаторных задачах необходимо подсчитать, сколькими способами можно сделать тот или иной выбор, выполнить то или иное требование, выполнить какое-либо условие.

Лекция 4. Комбинаторные методы

В наше время комбинаторика получила новый толчок для развития в связи с появлением быстродействующих ЭВМ и широким использованием методов дискретной математики. **Комбинаторные методы** используются для решения транспортных задач, задач по составлению расписаний, в задачах линейного программирования, **юридической статистики,** теории информации, **для разработки кодирования и декодирования шифров (криптография)**.

Первые комбинаторные задачи были связаны с азартными играми: картами, костями, «орлянкой». Наиболее любопытные игроки интересовались, **например,** тем, сколькими способами можно выбросить данное количество очков, бросая две или три кости или сколькими способами можно получить двух тузов при раздаче карт.

Лекция 5. Теория вероятности

Теория вероятностей – математическая наука, изучающая закономерности случайных явлений.

Теория вероятностей не может ответить на вопрос, произойдет или нет какое-то конкретное, уникальное случайное явление (событие). Однако если случайные события могут наблюдаться **многократно** при осуществлении одних и тех же условий (такие случайные события называются массовыми однородными случайными событиями), то, оказывается, существуют определенные закономерности, которым они подчиняются. Установлением таких закономерностей и занимается **теория вероятностей.**

Лекция 6. Предмет изучения теории вероятностей

Предметом изучения теории вероятностей являются закономерности массовых однородных случайных событий. Знание этих закономерностей позволяет прогнозировать характеристики процессов и явлений **(в юриспруденции: расчет превентивных мер для снижения количества правонарушений)**, в которых присутствуют случайные события. **Например,** хотя нельзя определить попадет или нет снаряд в конкретном выстреле в определенных условиях, можно предсказать, сколько снарядов попадет в цель, если произведено достаточно много выстрелов, или дать рекомендации, сколько выстрелов необходимо сделать для поражения цели с заданной надежностью.

Теория вероятностей также позволяет по данным вероятностям одних случайных событий находить вероятности других событий, связанных каким-либо образом с первыми. Одна из **задач** теории вероятностей состоит в выяснении закономерностей, возникающих при взаимодействии большого числа случайных факторов.

Лекция 7. Теория множеств

Понятие **множество** является первичным и неопределяемым. Множество можно представить себе как совокупность элементов, обладающих некоторым общим свойством. Объекты любой природы (числа, люди, вещи и т. д.), составляющие множество, называют его элементами. Например, студент Иванов является элементом множества студентов IV курса, март – элементом множества месяцев в году и т.д. Для того чтобы некоторую совокупность элементов можно было назвать множеством, необходимо, чтобы выполнялись следующие условия:

- должно существовать правило, позволяющее определить, принадлежит ли указанный элемент данной совокупности;
- должно существовать правило, позволяющее отличать элементы друг от друга (это означает, что множество не может содержать двух одинаковых элементов).

Тот факт, что элемент ***a*** принадлежит множеству ***A*** записывается так: в противном случае пишем Для однозначного описания некоторого множества мы будем пользоваться следующими способами: – перечислением всех его элементов. Например, множество ***A,*** состоящее из объектов: ***a, b, c, d*** записывают так: ***A = {a, b, c, d}.*** Данный способ применим только для конечных множеств, число элементов которых невелико; – указанием общего свойства элементов, принадлежащих множеству. В этом случае в фигурных скобках записывают обозначение произвольного элемента множества, ставят вертикальную черту, а затем свойство, характеризующее в точности все элементы множества. Например, множество *K* натуральных чисел, меньших 5 можно записать: *K*= **{1, 2, 3, 4}** или ***K*={*x* | *x N* и *x* < 5}.** Множества могут быть конечными или бесконечными.

Лекция 8. Криптография

Как только люди научились писать, у них сразу же появилось желание сделать написанное понятным не всем, а только узкому кругу. Даже в самых древних памятниках письменности учёные находят признаки намеренного искажения текстов: изменение знаков, нарушение порядка записи и т. д. Изменение текста с целью сделать его понятным только избранным, дало начало науке **криптографии** (перевод с греческого **«тайное письмо»**). Процесс преобразования текста, написанного общедоступным языком, в текст, понятный только адресату, называют **шифрованием,** а сам способ такого преобразования называют **шифром.** Но если есть желающие скрыть смысл текста, то найдутся и желающие его прочитать. Методы чтения зашифрованных текстов изучает наука **криптоанализ**. Методы **криптографии** и **криптоанализа** тесно связаны с математикой, во все времена многие известные математики участвовали в расшифровке важных сообщений. Часто именно математики добивались заметных успехов, ведь они в своей работе постоянно имеют дело с разнообразными и сложными задачами, а каждый шифр — это серьезная логическая задача. Постепенно роль математических методов в криптографии стала возрастать, и за последнее столетие они существенно изменили эту древнюю науку.

Не только азартные игры давали пищу для **комбинаторных размышлений** математиков. Еще с давних пор дипломаты, стремясь к тайне переписки, изобретали все более и более сложные шифры, а секретные службы других государств пытались эти шифры разгадать. Одним из простейших шифров была **«тарабарская грамота»,** в которой буквы заменялись другими по определенным правилам. Однако такие шифры легко разгадывались по характерным сочетаниям букв. Поэтому стали применять шифры, основанные на **комбинаторных принципах,**

Лекция 9. Криптографические методы

например, на различных перестановках букв, заменах букв с использованием ключевых слов и т. д.

В науке шифрования существуют понятия:

Криптография - это раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования.

Криптоанализом называют науку о раскрытии шифров. Поскольку проверка шифров на **стойкость** является обязательным элементом их разработки, криптоанализ также является частью процесса разработки шифра.

Криптология - это наука, предметом которой являются **математические основания,** как криптографии, так и криптоанализа одновременно.

Крипто аналитической атакой называют использование специальных методов для раскрытия ключа шифра и/или получения открытого текста. Предполагается, что атакующей стороне уже известен алгоритм шифрования, и ей требуется только найти конкретный ключ.

Криптограф ищет методы, обеспечивающие секретность и/или подлинность информации путём шифрования исходного текста.

Криптоаналитик пытается выполнить обратную задачу, раскрывая шифр или подделывая сообщение так, чтобы выдать их за подлинные данные.

ПРИЛОЖЕНИЕ2

1.ТЕСТ

Для проверки и последующего анализа полученных знаний студентам предлагается пройти тестовые задания, сгруппированные в билет из **30 вопросов**. Выбор заданий осуществляется тестирующей системой случайным образом. Тестовые задания интерактивны. По структуре формирования **тесты единственного выбора**

Задание №1		
Сложное суждение: **«Посеешь ветер – пожнёшь бурю»**, – является:		
Выберите один из 4 вариантов ответа:		
1)		импликация
2)		инверсия
3)		конъюнкция
4)		ддизъюнкция

Задание №2		
Форма мышления: умозаключение		
Выберите один из 4 вариантов ответа:		
1)		форма мышления, в которой отражаются существенные признаки массы неоднородных объектов и субъектов
2)		форма мышления, в которой отражаются существенные признаки отдельного объекта или класса однородных объектов
3)		форма мышления, посредством которой из одного или нескольких истинных суждений, называемых посылками, мы по определенным правилам вывода получаем новое суждение (заключение)
4)		форма мышления, в которой что-либо утверждается или отрицается об объектах, их свойствах и отношениях

Задание №3		
Высказывание: **«25 марта я поеду на тренинг казуального интеллекта в Минск либо в Прагу»**, это		
Выберите один из 4 вариантов ответа:		
1)		строгая дизъюнкция
2)		дизъюнкция
3)		эквивалентность
4)		импликация

Задание №4		
Сколько столбцов и строк будет в таблице истинности для логического выражения: **NOT (a AND b AND c)**		
Выберите один из 4 вариантов ответа:		
1)		столбцов: 6 строк:8
2)		столбцов: 5 строк:8
3)		столбцов: 7 строк:8
4)		столбцов: 6 строк:7

Задание №5		
Высказывание: **«Договор может быть заключен в устной или письменной форме»**, это		
Выберите один из 4 вариантов ответа:		
1)		дизъюнкция
2)		строгая дизъюнкция
3)		инверсия
4)		импликация

Задание №6
Отдел уголовного розыска, состоящий из начальника Акматова, заместителя Верещагина и трех сотрудников Сухого, Досматова, Евкурова проводит совещание. Условились, что будут готовить отчет в таком порядке: 1. Когда начальник Акматов готовит отчет, то Верещагин заместитель делает то же. 2. Сотрудники Досматов и Евкуров, оба или один из них, готовит отчет

3. Из двух членов отдела – заместитель Верещагин и сотрудник Сухой – готовит отчет один и только один.
4. Сотрудники Сухой и Досматов или оба готовят, или оба не готовят.
5. Если сотрудник Евкуров готовит отчет, то начальник Акматов и сотрудник Досматов делают то же.
Вопрос: Кто из сотрудников отдела в этот раз готовит отчет?

Выберите один из 4 вариантов ответа:

1)		Сухой и Досматов готовят отчет, остальные нет
2)		Евкуров, Досматов и Верещагин готовят отчет, остальные нет
3)		Сухой готовит отчет, остальные нет
4)		Сухой и Акматов готовят отчет, остальные нет

Задание №7

Из группы студентов, в которую входят **A**, **B**, **C** и **K**, преподаватель выбирает **двоих** для участия в конкурсе. Чем будут отличаться пары ?

Выберите один из 4 вариантов ответа:

1)		только составом
2)		только порядком
3)		составом и порядком
4)		порядком и составом

Задание №8

Комбинаторная конфигурация, это

Выберите один из 4 вариантов ответа:

1)		расположение бесконечного множества элементов, удовлетворяющее ряду специальных свойств
2)		расположение конечного множества элементов, удовлетворяющее ряду специальных свойств
3)		расположение конечного подмножества элементов, удовлетворяющее ряду специальных свойств
4)		расположение конечного множества элементов, удовлетворяющее ряду математических конфигураций

Задание №9

Среди размещений из **12** букв **a, b, c,** ... по **5** сколько таких, которые не содержат буквы **a?**

Выберите один из 4 вариантов ответа:

1)		83160
2)		94320
3)		93420
4)		81360

Задание №10

Во сколько раз **145!** больше **144!**.....?

Выберите один из 4 вариантов ответа:

1)		в 145 раз
2)		в 145-144! раз
3)		в 145:144! раз
4)		в 144!

Задание №11

Из цифр **«1»**, **«2»** и **«3»** составили такие комбинации : **12; 13; 21; 31; 32; 23**. Как называются такие комбинации ?

Выберите один из 4 вариантов ответа:

1)		размещения
2)		сочетания
3)		перестановки
4)		расстановки

Задание №12

Указать верное свойство. **Вероятность случайного события:**

Выберите один из 4 вариантов ответа:

1)		больше нуля и меньше единицы

2)		равна нулю
3)		равна единице
4)		равна 0,5

Задание №13		
Формула **Бернулли** определяет, что		
Выберите один из 4 вариантов ответа:		
1)		выполнение эксперимента происходит ровно с двумя исходами
2)		выполнение эксперимента происходит ровно с тремя исходами
3)		выполнение эксперимента происходит ровно без исходов
4)		выполнение эксперимента происходит ровно с четырьмя исходами

Задание №14		
Указать правильное утверждение:		
Выберите один из 4 вариантов ответа:		
1)		вероятность суммы событий равна сумме вероятностей этих событий
2)		вероятность суммы независимых событий равна сумме вероятностей этих событий
3)		вероятность суммы несовместных событий равна сумме вероятностей этих событий
4)		вероятность суммы несовместных событий равна произведению вероятностей этих событий

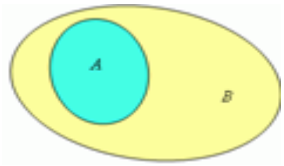
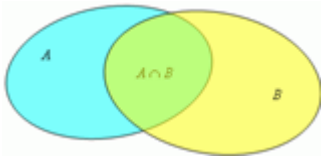
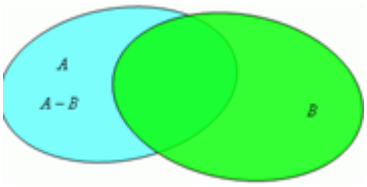
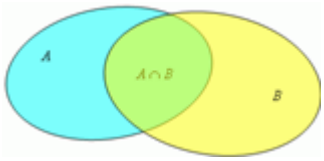
Задание №15		
Указать верное определение. **Произведением двух событий называется**:		
Выберите один из 4 вариантов ответа:		
1)		новое событие, состоящее в том, что происходят оба события одновременно
2)		новое событие, состоящее в том, что происходит или первое, или второе, или оба вместе
3)		новое событие, состоящее в том, что происходит одно но не происходит другое
4)		новое событие, состоящее в том, что происходит одно или не происходит другое

Задание №16		
Классическая формула вероятности		
Выберите один из 4 вариантов ответа:		
1)		численная мера объективной возможности её появления
2)		когда событие **A** тождественно событию **B**
3)		если событие **C** происходит тогда и только тогда, когда происходит событие **A** , и не происходит событие **B**
4)		совместное наступление событий в результате испытания

Задание №17		
В ящике **10** патронов от автомата и **5** пистолета. Вынимаются наудачу две патрона. Какова вероятность, что патроны будут одинаковые?		
Выберите один из 4 вариантов ответа:		
1)		0,524
2)		0,523
3)		0,15
4)		15

Задание №18		
Программа экзамена содержит **25** вопросов, из которых студент знает **20.** Преподаватель последовательно задает **3** вопроса. Найти вероятность того, что студент может ответить на вопросы **A,B,C**		
Выберите один из 4 вариантов ответа:		
1)		0,496
2)		0,489
3)		0,236
4)		0,497

Задание №19		
В группе студентов **10** мальчиков и **5** девочек. На конференцию выбираются наудачу два студента. Какова вероятность, что студенты будут однополыми?		
Выберите один из 4 вариантов ответа:		
1)		0,524
2)		0,523
3)		0,625
4)		0,365

Задание №20		
Подмножества это		
Выберите один из 4 вариантов ответа:		
1)		
2)		
3)		
4)		

Задание №21		
Разность множеств A и B		
Выберите один из 4 вариантов ответа:		
1)		есть множество элементов, которые принадлежат множеству A , но не принадлежат множеству B.
2)		есть множество элементов, которые не принадлежат множеству A , и не принадлежат множеству B.
3)		есть множество элементов, которые принадлежат множеству A , или не принадлежат множеству B.
4)		есть множество элементов, которые принадлежат множеству A , и принадлежат множеству B.

Задание №22		
Дискретные множества		
Выберите один из 4 вариантов ответа:		
1)		нет отдельных элементов. Распознаются путём измерения
2)		состоят из конечного числа элементов, когда можно пересчитать все элементы множества
3)		распознаются путём улучшения совокупности объектов
4)		имеют отдельные элементы. Путём счёта распознаются

Задание №23		
Круги Эйлера применяются для		
Выберите один из 4 вариантов ответа:		
1)		для выполнения действий с множествами или демонстрации их отношений
2)		для красоты
3)		для математических процедур
4)		для наглядного преставления логических элементов

Задание №24		
Элементы множества		
Выберите один из 4 вариантов ответа:		
1)		то, из чего это множество
2)		то, из чего состоят элементы
3)		подгруппы множество
4)		совокупности множеств

Задание №25		
Задайте перечислением множество **B = {x: x2 − 2x + 1 = 0}**. Это стандартная запись для задания множества, читается она так: множество элементов **x** таких, что $\mathbf{x^2 - 2x + 1 = 0}$		
Выберите один из 4 вариантов ответа:		
1)		B = {1}
2)		B = {2}.
3)		B = {0,1}.
4)		B = {1,1}.

Задание №26		
При оценке эффективности шифра обычно руководствуются правилом		
Выберите один из 4 вариантов ответа:		
1)		Керкхоффа
2)		Лейбница
3)		Маккейна
4)		Бернулли

Задание №27		
Стойкость шифра		
Выберите один из 4 вариантов ответа:		
1)		способность криптографического алгоритма противостоять криптоанализу
2)		способность криптографического алгоритма противостоять крипто перерасчету
3)		способность криптографического алгоритма противостоять анализу
4)		способность блок схемы- алгоритма противостоять криптоанализу

Задание №28		
Симметричное шифрование используется для		
Выберите один из 4 вариантов ответа:		
1)		обеспечения конфиденциальности данных
2)		взлома шифра
3)		обеспечения стойкости шифра
4)		обеспечения идентификации данных

Задание №29		
Шифр Гронсфельда		
Выберите один из 4 вариантов ответа:		
1)		многоалфавитный шифр
2)		одно алфавитный шифр
3)		алфавитный шифр
4)		алгоритм алфавита

Задание №30		
Криптография		
Выберите один из 4 вариантов ответа:		
1)		наука о сохранении секретов
2)		наука о сохранении денег
3)		наука о сохранении папок

4)		наука о сохранении файлов

Задание №31		
Зашифровать матричным способом слово **ПАМЯТНИК**		
Выберите один из 4 вариантов ответа:		
1)		ИБКФГЙЁЕ
2)		КИБФГЙЁЕ
3)		БКФГЙЁЕИ
4)		ЁИБКФГЙЕ

Задание №32		
Зашифровать слово **ЛЮК (p = 11 и q = 13, e=7),** используя алгоритм **RSA**		
Выберите один из 4 вариантов ответа:		
1)		117_98_12
2)		116_99_12
3)		125_98_11
4)		111_98_10

2.БИЛЕТЫ К ЗАЧЕТУ С ОЦЕНКОЙ

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Предмет математики. Аксиоматический метод
2. Функция распределения

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №2
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Математические методы в юриспруденции
2. Понятие высказывания. Простые и сложные высказывания

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №3
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Равносильность логических формул
2. Классическое определение вероятности

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №4
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Доказательства логических заключений
2. Классификация множеств

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №5
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Вычисление вероятности с помощью классического определения
2. Операции над множествами

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №6
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Алгебра событий
2. Криптосистема

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №7
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Формула полной вероятности. Формула Байеса
2. Криптографические ключи

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №8
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. События и испытания
2. Формула Бернулли

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №9
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Элементы комбинаторики
2. Диаграммы Эйлера

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №10
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Геометрическое и статистическое определения вероятности
2. Шифрованный (закрытый) текст

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №11
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Шифрование в криптографии
2. Доказательства логических заключений

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №12
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Моделирование логической структуры правовой нормы
2. Предмет теории вероятностей

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №13
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Числовые характеристики дискретных случайных величин
2. Вероятность произведения событий

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ

ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №14
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Понятие высказывания. Простые и сложные высказывания
2. Числовые характеристики дискретных случайных величин

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №15
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Операции над множествами
2. Шифры в криптографии

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №16
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Роль математики в современном мире
2. Алгебра событий

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №17
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Тавтологии
2. Числовые характеристики дискретных случайных величин

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №18
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Математические методы в юриспруденции
2. Мощность множеств

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №19
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. Закон равномерного распределения вероятностей
2. Логические операции

МОУ ВПО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №20
ДИСЦИПЛИНА «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

1. События и испытания
2. Алгоритм RSA

ПРИЛОЖЕНИЕ3

ПРАКТИЧЕСКИЕ РАБОТЫ

№ Названия разделов и тем	Цель и содержание практической работы	Задание и результаты практической работы
Практическая работа№1		
Формы мышления: понятия, суждения, умозаключения. Простые, составные высказывания. Логические связки между высказываниями.	Становление формальной логики. Высказывания.	Составлять сложные высказывания из простых, используя логические связки
Практическая работа№2 (СРС)		
Базовые логические операции, функции, переменные.	Законы логики: инверсия, конъюнкция, дизъюнкция	Переводить высказывания в аппарат алгебры логики
Практическая работа№3		
Таблицы истинности для простых и сложных высказываний. Логические связки	Правила построения таблиц истинности	Построение таблиц истинности
Практическая работа№4(СРС)		
Импликация, эквивалентность. Правила преобразования логических выражений	Законы логических преобразований	Применение таблиц истинности для решения задач, возникающих в правовой сфере
Практическая работа№5(СРС)		
Упрощение логических выражений с применением аппарата математической логики	Правила преобразования логических выражений	Упрощать логические выражения, применяя правила как математики, так и логики
Практическая работа№6		
Комбинаторные задачи: выбор из группы предметов. Комбинаторные задачи: расположение предметов в определенном порядке	Основные комбинаторные объекты	Правила сложения, умножения
Практическая работа№7 (СРС)		
Комбинаторные задачи: нахождение числа возможных комбинаций.	Сочетания, перестановки (с повторениями и без повторений)	Применять правила сочетания, перестановки. размещения
Практическая работа№8		
Комбинаторные правила	Размещения (с повторениями и без повторений)	Применять правила размещения
Практическая работа№9		
Элементарная теория вероятностей	Основные понятия теории вероятности	Основные понятия теории вероятности
Практическая работа№10 и(СРС)		
Вероятностное пространство. Условная вероятность и независимость событий.	Случайные события. Типы событий. Условная вероятность	Формулы условной вероятности
Практическая работа№11и (СРС)		
Построение вероятностных моделей с помощью функций распределения	Классическая формула вероятности. Формула Байеса, формула Бернулли	Использование формулы классической вероятности
Практическая работа№12		
Понятие множества. Отношения между множествами, операции над множествами	Основные понятия множества	Отношения между множествами
Практическая работа№13(СРС)		
Конечные множества	Типы множеств. Операции над множествами	Формулы для операций над множествами
Практическая работа№14		

Бесконечные множества. Круги Эйлера	Графическое отображение множеств	Построение кругов Эйлера
Практическая работа№15		
Математическая модель шифрования, матричный способ	Математика в шифровании	Элементарные математические способы шифрования
Практическая работа№16(СРС)		
Криптографические системы закрытых ключей. Шифры Винежера, Гронсфельда	Шифры сложной замены	Применение прикладных программ для шифрования
Практическая работа№17(СРС)		
Криптографическая система открытого ключа. Алгоритм RSA	Шифры открытых ключей	Алгоритм RSA
Практическая работа№18(СРС)		
Цифровая подпись	Применение шифрования открытыми ключами	Создание цифровой подписи

ПРИЛОЖЕНИЕ4

ШКАЛА ОЦЕНИВАНИЯ ПРАКТИЧЕСКИХ ЗАДАНИЙ (текущий контроль)

Оцениваются в процентах от выполненных и защищенных практических работ согласно инструкциям по их выполнению.
85-100 % – выполнены, подготовлены отчеты и защищены все практические работы;
75-84 % – выполнены и подготовлены отчеты по всем практическим работам, защищена одна лабораторная работа;
60-74 % – выполнены и подготовлены отчеты по всем практическим работам;
0-59 %– выполнено менее 50% лабораторных работ, нет отчетов.

ШКАЛА ОЦЕНИВАНИЯ РПР (рубежный контроль)

Оцениваются в процентах от выполненных и защищенных **РПР** работ согласно инструкциям по их выполнению.
85-100 % - выполнены все этапы решения задачи; работа выполнена полностью и получен верный ответ или иное требуемое представление результата работы;
75-84 % - работа выполнена полностью, но при выполнении обнаружилось недостаточное владение навыками работы с математическими методами в юриспруденции в рамках поставленной задачи; правильно выполнена большая часть работы (свыше 85 %), допущено не более трех ошибок; работа выполнена полностью, но использованы наименее оптимальные подходы к решению поставленной задачи.
60-74 % - работа выполнена не полностью, допущено более трех ошибок, но обучаемый владеет основными навыками работы с математическими методами в юриспруденции, требуемыми для решения поставленной задачи.
0-59 %– - допущены существенные ошибки, показавшие, что обучаемый не владеет обязательными знаниями, умениями и навыками работы с математическими методами в юриспруденции или значительная часть работы выполнена не самостоятельно.
0% - работа показала полное отсутствие у обучаемого обязательных знаний и навыков практической работы с математическими методами в юриспруденции по проверяемой теме.

ШКАЛА ОЦЕНИВАНИЯ ТЕСТА (рубежный контроль)

1. В одном тестовом задании 20 закрытых вопросов.
2. К заданиям даются готовые ответы на выбор, один правильный и остальные неправильные.
3. Обучающемуся необходимо помнить: в каждом задании с выбором одного правильного ответа правильный ответ должен быть.
4. За каждый правильно ответ – 5 баллов
5. Общая оценка определяется как сумма набранных баллов.
6. Отметка (в %).

ШКАЛА ОЦЕНИВАНИЯ УСТНОГО ОПРОСА (промежуточный контроль – «ЗНАТЬ» и «УМЕТЬ»)

При оценке устных ответов на проверку уровня обученности ЗНАТЬ учитываются следующие критерии:
1. Знание основных процессов изучаемой предметной области, глубина и полнота раскрытия вопроса.
2. Владение терминологическим аппаратом и использование его при ответе.
3. Умение объяснить сущность явлений, событий, процессов, делать выводы и обобщения, давать аргументированные ответы.
4. Владение монологической речью, логичность и последовательность ответа, умение отвечать на поставленные вопросы, выражать свое мнение по обсуждаемой проблеме.

Отметкой **(16-20 баллов)** оценивается ответ, который показывает прочные знания основных принципов математических методов в правовой сфере, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа.

Отметкой **(10-15 баллов)** оценивается ответ, обнаруживающий прочные знания основных принципов современных математических методов, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна – две неточности в ответе.

Отметкой **(5-10 баллов)** оценивается ответ, свидетельствующий в основном о знании принципов математических методов, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа.

Отметкой **(1-4 баллов)** оценивается ответ, обнаруживающий незнание основных принципов математических методов, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа.

ШКАЛА ОЦЕНИВАНИЯ АНАЛИТИЧЕСКИХ И ПРАКТИЧЕСКИХ ЗАДАНИЙ
(промежуточный контроль – «УМЕТЬ и ВЛАДЕТЬ»)

При оценке ответов на проверку уровня обученности **УМЕТЬ** и **ВЛАДЕТЬ** учитываются следующие критерии:

Отметкой **(8-10 баллов)** оценивается ответ, при котором студент ставит постановку проблемы собственными словами; оценивает альтернативные решения проблемы; свободно применяет математические методами в юриспруденции. Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены.

Отметкой **(4-7 баллов)** оценивается ответ, при котором студент ставит постановку проблемы собственными словами, но не оценивает альтернативные решения проблемы; применяет математические методами в юриспруденции, но не ищет альтернативных решений. Демонстрирует значительное понимание проблемы. Большинство требований, предъявляемых к заданию выполнены.

Отметкой **(1-3 балла)** оценивается ответ, при котором студент не ставит постановку проблемы собственными словами и не оценивает альтернативные решения проблемы; применяет математические методами в юриспруденции слабо; не знает основных принципов математических методов. Демонстрирует частичное или небольшое понимание проблемы. Многие требования, предъявляемые к заданию, не выполнены.

Отметкой **(0 баллов)** оценивается ответ, при котором студент демонстрирует непонимание проблемы или нет ответа, и даже не было попытки решить задачу.

ПРИЛОЖЕНИЕ5

Технологическая карта дисциплины

«Математическое моделирование информационных технологий в юриспруденции»

Курс 4, семестр 7, Количество 2Е - 2, Отчетность - зачет

Название модулей дисциплины согласно РПД	**Контроль**	**Форма контроля**	**зачетный минимум**	**зачетный максимум**	**график контроля**
Модуль 1					
Модуль 1. Разбор практических ситуаций (Мат. логика, комбинаторика, теория вероятности)	Текущий контроль	Подготовка к выполнению практических работ. Защита практических работ. Активность, посещаемость	**5**	**10**	**9**
	Рубежный контроль	Письменная контрольная работа (Матлогика, комбинаторика, теория вероятности)	**15**	**25**	
Модуль 2					
Модуль 2. Разбор практических ситуаций (Теория множеств, криптография)	Текущий контроль	Подготовка к выполнению практических работ. Защита практических работ. Активность, посещаемость	**5**	**10**	**17**
	Рубежный контроль	Расчетно - практическая работа (Теория множеств, криптография)	**15**	**25**	
ВСЕГО за семестр			**40**	**70**	
Промежуточный контроль (Зачет)			**20**	**30**	
Семестровый рейтинг по дисциплине			**60**	**100**	

ПРИЛОЖЕНИЕ6

СЛОВАРЬ ТЕРМИНОВ МАТЕМАТИЧЕКСКОГО МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ

Глоссарий

Алгебра логики

Абдукция (от лат. abducere – приведение) – форма умозаключения, в котором из исходных суждений (описывающих свойства каких-то явлений) выбирается новое суждение (гипотеза), которое наилучшим образом объясняет или оценивает эти явления.

Абсурд (от лат. absurdum – нелепый) – бессмыслица, нелепость, привести к абсурду (reduction ad absurdum) – значит доказать противоречивость какого-либо положения или его ложность, и таким образом его опровергнуть.

Автонимия (от греч. autos-сам, опота — имя) – использование языковых выражений для обозначения их самих (знак означает сам себя).

Аксиома (от греч. axioma – значимое, бесспорное, общепринятое положение) – истинное суждение, которое при дедуктивном построении какой-либо теории принимается без доказательств в качестве исходного положения и, которое входит в основу доказательства, всех других положений данной теории.

Алгоритм (от лат. algoritmi – предписание, правило, рецепт) – точное и легко понимаемое описание (предписание, правило) последовательного (шаг за шагом) единообразного решения той или иной задачи (принятие того или иного решения в научной и практической деятельности.

Антецедент (лат. antecedens – предшествующий, предыдущий) – первый член импликации, которому предписано слово «если». «Если идёт дождь, то асфальт мокрый».

Алогизм (от греч. a –не + logos – разум) – нелогичность хода мысли, рассуждения, нарушающий определённые законченные правила логики и, поэтому всегда содержащий в себе логическую ошибку.

Антиномия (от лат. anti-против, nomos – закон, противоречие в законе) – противоположность между двумя суждениями, взаимно-исключающими друг друга, но в то же время каждое может быть признано правильным.

В

Верификация (от лат. verus – истинный + facio – делаю) – принцип проверки, установления осмысленности, т.е. возможность данного высказывания (утверждения) оказаться истинным или ложным.

Выборка – конечный набор прецедентов (объектов, случаев, событий), некоторым способом выбранных из множества всех возможных прецедентов, называемого генеральной совокупностью.

Д

Демонстрация (от лат. demonstration – показывание) – логическая форма рассуждения, в процессе которого из аргументов выводится истинность или ложность тезиса.

Дизъюнкция(от лат. disjunction – разобщение, разделение, различие) – логическая операция, выражающаяся в соединении двух или более высказываний с помощью логического союза «или» в новое, сложное высказывание.

Дилемма(от греч. dia – дважды + lemma - предсказание или двойственное предположение) – условно-разделительное умозаключение, в котором разделительное суждение в форме альтернативы утверждает или основания, или следствия условных суждений.

Дефиниция (от лат. defeno – определение) – краткое логическое определение, устанавливающее существенные отличительные признаки предмета или значение понятий – его содержание и границы.

Дефиниедум – (Dfd**)**– определяемое понятие в формуле классического определения (Dfd=dfn); понятие, содержание которого требуется раскрыть.

Дефиниенс– (dfn) – понятие или набор понятий с известным значением,
выражающим существенные признаки определяемого понятия.

Дихотомия(от греч. dicha и to me – разделяю на две части) – деление объёма
понятия на исчерпывающие объём делимого понятия.

З

Закон мышления – это внутренняя, существенная устойчивая, необходимая, повторяющаяся связь между элементами мысли и самими мыслями.

Знак– объект, используемый интерпретатором в процессе познания или общения в качестве представления какого-либо другого объекта.

Значение – содержание, связываемое с тем или иным языковым выражением.

Знаки-индексы – связаны с представляемыми ими объектами как следствия с причинами.

Знаки-образы – знаки, которые сами по себе несут информацию о представляемых ими объектах (карта местности, картина, чертеж), поскольку находится с обозначаемыми объектами в отношении подобия.

Знаки – символы – не имеют сходства с обозначаемыми предметами, а связаны только посредством мысли.

И

Импликация (от лат. implicite – тесно связывать) – логическая операция, связывающая два высказывания в сложное высказывание с помощью логической связки «если..., то…»

К

Квантор – это общее название для логических операций, ограничивающих область истинности какого-либо предиката.

Классификация (от лат. casus-разряд, facio – делаю) – распределение предметов на классы согласно наиболее существующим предметам данного рода.

Консеквент– второй член импликации, который является отрицанием антецедента, то есть это вывод, следствие (высказывание, идущее после слова «то» в конструкции «если.., то…»)

Контрадикторность (от лат. contradictories – противоречие) – отношения между противоречивыми суждениями, которые одновременно не могут быть истинными, ни ложными; из 2-х контрадикторных суждений одно-истинно, другое-ложно.

Контрарность (от лат. contrarius – противоположный) – отношения между противными или противоположными суждениями, которые одновременно не могут быть истинными, но могут быть ложными.

Конъюнкция (от лат. conjungo – соединение) – логическая операция, соединяющая два или более высказываний с помощью союза «и».

Л

Логика (от греч. logos — слово, понятие, рассуждение, разум) - нормативная наука о формах и приемах интеллектуальной познавательной деятельности, осуществляемой с помощью языка.

М

Модальность суждения (от лат. modus – мера, образ, способ) – явно или неявно выраженная в суждении дополнительная информация о логическом или фактическом статусе суждения, о регулятивных, оценочных, временных и других его характеристик.

Модус (от лат. modus – мера, образ, способ) – свойство предмета, присущее ему только в некоторых состояниях и зависящее от окружения предмета и тех связей, в которых он находится.

Модус поненс– правило вывода в исчислении высказываний. Правило вывода позволяет от утверждения условного высказывания и утверждения его основания (антецедент) перейти к утверждению следствия (консеквента) этого высказывания.

Модус толленс – рассуждение от противного, переход от утверждения условного высказывания и отрицание его следствия (консеквента) к отрицанию основания (антецедента) данного высказывания.

О

Обобщение – мысленное объединение отдельных предметов в некотором пространстве.

Обоснованность – такое качество правильного мышления, которое свидетельствует, что все мысли опираются на другие мысли, истинность которых доказана.

Обращение – непосредственное дедуктивное умозаключение, в котором происходит перемена мест субъекта и предиката при сохранении качества суждения и распределённости терминов в суждениях.

Объединение – логическая операция, позволяющая из исходных классов образовывать новый класс (множество), в который войдут все элементы из исходных классов.

Объём понятия – совокупность (множество) предметов, которые обобщаются мысленно в понятии.

Ограничение (понятий) – логическая операция перехода от родового понятия к видовому путём прибавления к содержанию родового понятия видообразующего признака.

Омонимы (от греч. homos – одинаковый, onoma – имя) – слова, совпадающие по звучанию и написано, но выражающие различные понятия.

Определение (понятий) – логическая операция, которая раскрывает содержание понятия либо устанавливает значение термина.

Определённость – качество правильного мышления воспроизводить в структуре мысли качественную определённость самих предметов и явлений, их относительную устойчивость.

Опровержение (от лат. refutation) – это логическая операция, в процессе которой обосновывается ложность какой-либо мысли с помощью других, истинных и связанных и конкретной практикой, доказательство ложности или несостоятельность какого-либо тезиса.

Основание – часть условного суждения, в которой отображается условие, от которого зависит истинность следствия.

Ответ – новое суждение, уточняющее или дополняющее в соответствии с поставленными вопросом исходное задание.

Органон (от греч. organon - инструмент, метод): 1. Общее название логических категорий Аристотеля и вообще научной системы. 2. Сочинение, в котором изложена сущность какой-либо науки.

П

Парадигма (от греч. paradeigma — пример, образец) – образец, модель решения исследовательских задач, определяющая то или иное видение мира. Смена парадигмы рассматривается как научная революция.

Парадокс (от греч. paradoxos) – неразрешимые противоречия между двумя одинаково обоснованными утверждениями.

Паронимы (от греч. para и ónyma — имя, название, слово) – близкие по звучанию однокоренные слова, имеющие разное значение или совпадающие в нём лишь частично.

Полемика – спор с целью доказать истинность своего тезиса и опровергнуть тезис оппонента.

Полисиллогизм – сложный категорический силлогизм, который стоит из двух и более простых силлогизмов, определённым образом связанных между собой, так что заключение каждого последующего силлогизма становится посылкой другого силлогизма.

Понятие (представление) - мысль, в которой на основании некоторого выделяются из универсума и обобщаются в классы предметы, обладающие данным признаком.

Последовательность- результат последовательного выбора элементов заданного множества.

Постулат(от лат.- требование) –1) положение (суждение, утверждение), принимаемое в рамках какой-либо научной теории за истинное и в силу очевидности и поэтому играющее в данной теории роль аксиомы; 2) свойство, утверждение, принимаемое без доказательства.

Посылка – исходное высказывание, из которого выводится заключение.

Большая посылка - содержит предикат заключения.

Меньшая посылка- содержит субъект заключения.

Правильность мысли- 1)есть необходимое, но недостаточное условие для установления ее истинности. Чтобы быть истинной, мысль должна соответствовать действительности, верно, отражать ее. 2) Соответствие мысли некоторым правилам ее построения.

Прагматика (от др. греч. pragma - дело, действие) - раздел семиотики, изучающий отношения между знаковыми системами и теми, кто воспринимает, интерпретирует и использует их.

Превращение - непосредственное умозаключение, в котором субъект заключения совпадает с субъектом посылки, а предикат заключения является термином, противоречащим предикату посылки.

Предикат - термин в простом атрибутивном высказывании, играющий роль логического сказуемого. То, что говорится о субъекте.

Предмет - субъект, то на что направлено наше внимание, интеллект, разум.

Представление - наглядный образ предмета, воспроизведенный по памяти в воображении.

Признаки предмета - внешние и внутренние свойства предмета.

Проблема (от греч. problemos - преграда, трудность, задача) - вопрос или целостный комплекс вопросов, возникших в ходе познания. Противоречивая ситуация, в которой имеются противоположные позиции при объяснении одних и тех же объектов, явлений и отношений между ними.

Пропозициональность (proposishion - (логизированность) истинность или ложность высказываний.

Противопоставление - логическая операция, действие, в результате которого меняется качество исходного суждения (связка меняется на противную), меняется местами субъект и предикат его, и при этом субъект (или предикат) выводного суждения должен противоречить предикату (или субъекту) исходного.

Р

Равнообъемность- отношение между двумя непустыми понятиями, объемы которых совпадают (они взаимно включаются друг в друга).

Распределенность- характеристика терминов в простых категорических суждениях (термина - субъекта и термина-предиката) с точки зрения их объема: термин распределен если он берется в полном объеме, и не распределен - если он рассматривается в части объема предметов, которые в нем мыслятся.

Релевантность (от лат. - поднимать, облегчать) - связь между высказываниями, выражающая изменение вероятности одного из них при учете второго.

- позитивная – связь между двумя высказываниями, при которой вероятность первого повышается при учете второго.
- негативная–связь между двумя высказываниями, при которой вероятность первого понижается при учете второго.

С

Семантика (от греч. – правила приписывания значений) - наука, исследующая отношения знаков с представляемыми ими объектом (правила придания смысла и значения правильно построенным выражениям языка).

Семиозис (от. греч.- знаковая ситуация) состоит из трех частей: знак, его значение и интерпретатор.

Семиотика (от греч. - знак, признак) – наука о знаках. Общая теория знаковых систем, к числу которых относятся как естественные языки, так и специальные языки конкретных наук, искусственные языки и т.д.

Силлогизм (от греч. - рассуждение) – лог. умозаключение, состоящее из двух суждений (посылок), из которых следует третье суждение заключение, вывод

Синонимы (от греч. -одноимённый) - слова указывающие на одно и то же понятие и имеющие одинаковое лексическое значение, различаются своей экспрессивной окрашенностью, закрепленным за определенным стилем.

Синтаксис(от др. греч. - построение, порядок, составление) - правила комбинирования знаков. Раздел формальной логики, изучающий правильность построения выражений, безотносительно к тому ,есть ли у этих выражений логические значения и если есть, то какие именно.

Символическая логика - 1) современный этап развития формальной логики, направление в математической логике, изучающее формальные системы.2)Логика, изучаемая посредством построения формализованных языков (главн. – символы).

Слово - одна из основных структурных единиц языка. Обозначение, имя объекта, его свойство, его поведение.

Совместимость- вид отношения между понятиями и суждениями. Два понятия называются совместимыми, если их объемы совпадают полностью или частично, то есть имеют хотя бы один общий элемент. Совместимыми называют такие суждения, которые могут быть вместе истинными, то есть истинность одного не исключает истинности другого.

Соподчинение - отношение между двумя непустыми понятиями, при котором они не имеют общих элементов объема и не исчерпывают в сумме универсум.

Сорит(от греч. - куча) - 1) цепь силлогизмов, в которых заключение является одной из посылок следующего за ним, а одна из посылок при этом не выражается в явной форме. 2) Полисиллогизм, в котором пропущено по крайней мере один промежуточное заключение.

Софизм (от греч. — уловка, ухищрение, выдумка, головоломка) - ложное умозаключение, которое, тем не менее, при поверхностном рассмотрении кажется правильным. Основан на преднамеренном, сознательном нарушении правил логики (содержит скрытую лог. ошибку).

Сравнение - акт мышления, посредством которого классифицируется ,упорядочивается и оценивается содержание бытия и познания.

Субконтрарность (частичная противоположность) – совместимость по истинности, но несовместимость по ложности.

Суждение - отношение между понятиями, которое носит утвердительный или отрицательный характер.

Т

Тавтология (от греч. - то же самое) - бессодержательное, неинформативное суждение, в котором по предмету мысли приписывается свойство, заранее заложенное в его обозначении.

Таксон (от лат. - ощупывать, определять посредством ощупывания цену, оценивать) - член таксономического деления, один из видов, подвидов и т.д. делимого понятия.

Тезис(от греч. - положение, утверждение) - положение, утверждение, выставляемое и потом доказываемое в каком-либо рассуждении.

Теория (от греч. — рассмотрение, исследование) - система связанных между собой понятий и высказываний, относящихся к некоторой предметной области. Логическая теория - система понятий и высказываний, касающихся логической формы каких-либо языковых контекстов.

Термин (от лат. - предел, граница) - выражение со строго фиксированным значением, входящее в состав предложения, но само предложением не являющимся.

Умозаключение - 1) умственное действие, связывающее в ряд «посылок» и «следствий» мысли различного содержания. 2) форма мышления, посредством которой из одного или нескольких суждений выводится новое суждение. 3) способ получения нового знания, на основе уже имеющихся.

Универсум (от лат. - совокупность, общность) - предметная область, о которой идет речь в данном языковом контексте.

Ф

Формализация (от лат. - вид, образ) - отображение результатов мышления в точных понятиях и утверждениях. Формализация уточняет содержание путем выявления его формы и может осуществляться с разной степенью полноты.

Формальная логика - наука, изучающая формы мысли - понятия, суждения, умозаключения, доказательства - со стороны их логической структуры, то есть отвлекаясь от конкретного содержания мыслей.

Э

Эристика (от греч. – искусство спорить) – искусство спора, диспута, полемики, разрабатывалась софистами.

Эквивалентность (от лат. - равносильный, равнозначащий) - отношение между двумя высказываниями, при котором они логически следуют друг за другом.

Экстенсионал знака (от лат.- протяжение, пространство, распространение) - класс предметов, обозначаемых этим признаком.
Энтимема(от греч. - в уме) - сокращенный силлогизм, в котором пропущена одна из посылок или заключение.
Эпистемология - (от греч. - знание и слово, учение) - теория познания, изучение закономерностей и возможностей познания, отношение знания.
Я
Язык логики - специально создаваемый современной логикой для своих целей язык, способный следовать за логической формой рассуждения и воспроизводить ее даже в ущерб краткости и легкости общения (формализованный язык).
Язык - система знаков, предназначенная для фиксирования, хранения, передачи и переработки информации.

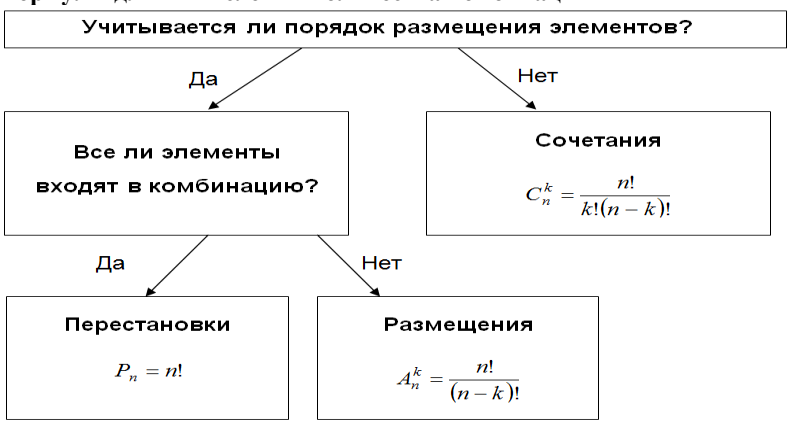
Комбинаторика
К
Комбинаторика—раздел математики, изучающий дискретные объекты, множества (сочетания, перестановки, размещения и перечисления элементов). Комбинаторика связана со многими другими областями математики — алгеброй, геометрией, теорией вероятностей, и имеет широкий спектр применения в различных областях знаний (например, в генетике, информатике, статистической физике).Термин «комбинаторика» был введён в математический обиход Лейбницем, который в 1666 году опубликовал свой труд «Рассуждения о комбинаторном искусстве».
П
Перестановкой из n элементов (например, чисел 1,2,…,n) называется всякий упорядоченный набор из этих элементов.
Число всех перестановок порядка n равно факториалу: $P_n=n!$
Правило умножения заключается в том, что для того, чтобы найти число всех возможных исходов независимого проведения двух испытаний A и B, следует перемножить число всех исходов испытания A и число всех исходов испытания B.
Р
Размещением называется расположение «предметов» на некоторых «местах» при условии, что каждое место занято в точности одним предметом и все предметы различны.
В отличие от сочетаний размещения учитывают порядок следования предметов. Так, например, наборы < 2,1,3 > и < 3,2,1 > являются различными, хотя состоят из одних и тех же элементов {1,2,3} (то есть, совпадают как сочетания).

$$A_n^k = n^{\underline{k}} = (n)_k = n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!} = \binom{n}{k}k!.$$

Термин «Размещение» употребил впервые Якоб Бернулли в книге «Искусство предположений».
С
Сочетаниями из n элементов по k называются соединения, которые можно образовать из n элементов, собирая в каждое соединение k элементов; при этом соединения отличаются друг от друга только самими элементами (различие порядка их расположения во внимание не принимается).
Например, из 3 элементов (a,b,c) по 2 можно образовать следующие сочетания: ab, ac, bc.
Число сочетаний из n элементов по k обозначают C_n^k. Оно равно

$$\binom{n}{k} = C_n^k = \frac{n!}{k!\,(n-k)!}.$$

Ф
Факториал числа n (обозначается n!, произносится эн факториал) — произведение всех натуральных чисел от 1 до n включительно.
По определению полагают 0! = 1. Факториал определён только для целых неотрицательных чисел.
1! = 1,
2! = 2•1 = 2,
3! = 3 •2 •1 = 6,
4! = 4 •3 •2 •1 = 24,
Формулы для вычисления количества комбинаций



Теория вероятности
А
Аксиоматическое определение вероятности — отношение подмножества, благоприятствующего событию к общему множеству.
Асимметрия — отношение центрального момента третьего порядка к кубу среднеквадратического отклонения.
Б
Бесповторная выборка — выборка, при которой отобранный объект после проведения обследований не возвращается в генеральную совокупность.

В

Вероятность — отношение числа благоприятных исходов к общему числу исходов.

Внутригрупповая дисперсия — средняя арифметическая групповых дисперсий, взвешенная по объемам групп.

Выборка — совокупность случайно отобранных из изучаемой совокупности объектов.

Г

Геометрическое определение вероятности — отношение длины отрезка к длине отрезка L.

Гистограмма — ступенчатая фигура, состоящая из прямоугольников, основаниями которых служат интервалы длиною h, а высоты n.

Групповая дисперсия — дисперсия значений признака, принадлежащих группе, относительно групповой средней.

Групповая средняя — среднее арифметическое значений признака, принадлежащих группе.

Д

Двумерная случайная величина — величина, имеющая два аргумента.

Дискретная случайная величина — величина, принимающая отдельные значения с определенными вероятностями.

Дисперсия — математическое ожидание квадрата отклонения случайной величины от ее математического ожидания.

Доверительный интервал — интервал, который покрывает неизвестный параметр θ с заданной надежностью y.

Достоверное событие — событие, которое обязательно произойдет, если будет осуществлена определенная совокупность условий.

З

Закон распределения случайной величины — соответствие между возможными значениями случайной величины и их вероятностями.

И

Интервальная оценка — оценка, которая определяется концами интервала.

К

Конкурирующая гипотеза — гипотеза противоречащая основной.

Корреляционная зависимость — зависимость, при которой при изменении одной из величин изменяется среднее значение другой.

Корреляционный момент — характеристика связи между двумя случайными величинами.

Коэффициент вариации — выраженное в процентах отношение выборочного среднего квадратического отклонения к выборочной средней.

Коэффициент корреляции — отношение ковариации к произведению средних квадратических отклонений двух случайных величин.

Критическая область — совокупность значений критерия, при которых нулевую гипотезу отвергают.

М

Математическое ожидание — число, относительно которого стабилизируется среднее арифметическое возможных значений случайной величины при достаточно большом количестве испытаний.

Межгрупповая дисперсия — дисперсия групповых средних относительно общей средней.

Мода — варианта ряда, которая имеет наибольшую частоту.

Моменты случайных величин — характеристики случайных величин, определяющие математическое ожидание k-й степени отклонения случайной величины.

Н

Непрерывная случайная величина — величина, принимающая значения, сколь угодно мало отличающиеся друг от друга.

Несмещенная оценка — оценка θ^*, математическое ожидание которой равно оцениваемому параметру θ.

Нулевая гипотеза — основная выдвинутая гипотеза.

О

Общая дисперсия — дисперсия значений признака всей совокупности относительно общей средней.

П

Плотность распределения вероятностей — вероятность того, что непрерывная случайная величина примет значение на указанном интервале.

Повторная выборка — выборка, при которой отобранный объект возвращается после проведения обследования обратно в генеральную совокупность.

Полигон частот — ломаная линия, отрезки которой соединяют точки (x_1, n_1).

Производящая функция — функция, определяющая вероятность наступления события при различных вероятностях появления в каждом испытании.

Р

Размах варьирования R — разность между наибольшей и наименьшей вариантой.

Регрессия — представление одной случайной величины как функции другой.

С

Случайная величина — величина, которая в результате испытания примет одно и только одно значение, до опыта неизвестно какое.

Состоятельная оценка — оценка, которая при $n \to \infty$ стремится по вероятности к оцениваемому параметру.

Статистическая гипотеза — гипотеза о виде неизвестного распределения, или параметрах неизвестного распределения.

Статистический критерий — случайная величина, служащая для проверки нулевой гипотезы.

Статистическое распределение выборки — перечень вариант и соответствующих им частот или относительных частот.

Стохастическая зависимость — зависимость, при которой изменение одной из величин влечет изменение другой.

Т

Теорема Лапласа — определение вероятности наступления события в k измерениях из n (при больших k и n).

Теория вероятностей — наука, изучающая общие закономерности случайных явлений массового характера.

Точечная оценка — оценка, которая определяется одним числом.

У

Условная вероятность — вероятность наступления интересующего нас события, связанная с дополнительными условиями.

Ф

Формула Байеса - определение апостериорной (после опытной) вероятности на основе априорной (доопытной) на основе проведения эксперимента.
Формула Бернулли — определение вероятности наступления события в измерениях из n.
Функция распределения — функция, определяющая вероятность того, что *X* примет значение меньше *x*.
Х
Характеристики положения — характеристики, определяющие наиболее возможные значения случайной величины.
Характеристики рассеивания — характеристики, определяющие разброс возможных значений случайной величины.
Ц
Центральная предельная теорема — теорема, доказывающая, что суммирование большого числа случайных величин с различными законами распределения приводит в итоге к нормальному распределению.
Э
Эксцесс распределения — величина, определяемая отношением центрального момента четвертого порядка к четвертой степени среднего квадратического отклонения за вычетом тройки.
Эффективная оценка — такая оценка, которая при заданном объеме выборки *n* имеет наименьшую возможную дисперсию.

Теория множеств
А
Аксиома объемности. **Если все элементы множества А принадлежат множеству В, а все элементы множества В принадлежат также множеству А, то А=В.**
Аксиома пары. **Для произвольных переменных a и b существует множество, единственными элементами которого являются {a,b}.**
Аксиома степени. Для любого множества X существует множество всех его подмножеств P(X).
Аксиома бесконечности. Существует, по крайней мере, одно бесконечное множество – натуральный ряд чисел.
Аксиома выбора. Для всякого семейства непустых множеств существует функция, которая каждому множеству семейства сопоставляет один из элементов этого множества. Функция называется функцией выбора для заданного семейства.
Б
Бесконечным множеством называется, если оно содержит бесконечное число элементов. $B=\{b_1,b_2,b_3, ...\}$.
Д
Декартовым произведением множеств А и В называется множество пар, первая компонента каждой из которых принадлежит множеству А, а вторая — множеству В. Декартово произведение множеств А и В обозначают А х В. Таким образом, $A\times B=\{(x,y)|x\in A\wedge y\in B\}$.
Дополнением множества А до универсального множества называется множество, каждый элемент которого принадлежит универсальному и не принадлежит А.

$$A'_U = \{x | x \notin A \wedge x \in U\}$$

К
Конечным множеством называются, если число его элементов конечно, т.е. если существует натуральное число n, являющееся числом элементов множества. $A=\{a_1, a_2, a_3, ..., a_n\}$.
Круги Эйлера - Операции над множествами и отношения между ними можно изобразить с помощью кругов Эйлера. Это специальные чертежи, на которых обычные множества изображаются кругами, универсальное множество - прямоугольником
М
Множество — основное понятие теории множеств. Этим термином объединяются все уникальные отдельные (дискретные) элементы, выбранные согласно некоторому критерию. Количество элементов множества в общем случае далеко не всегда выражается конечным числом.
О
Объединением множеств А и В называется операция, результатом которой является множество, состоящее из тех и только тех элементов, которые принадлежат множеству А или множеству В (т.е. хотя бы одному из этих множеств). $A\cup B=\{x|x\in A\vee x\in B\}$
П
Пересечением множеств А и В называется операция, результатом которой является множество, состоящее из тех и только тех элементов, которые принадлежат и А и В одновременно. $A\cap B=\{x|x\in A\wedge x\in B\}$
Подмножество. Множество А называется подмножеством множества Х, если в А нет таких элементов, которые не принадлежали бы Х
Пустое множество (обозначается символом ∅) — множество, в составе которого нет ни одного элемента
Р
Разностью множеств А и В называется операция, результатом которой является множество, состоящее из тех и только тех элементов, которые принадлежат А и не принадлежат В одновременно. $A\setminus B=\{x\in A\wedge x\notin B\}$
С
Счетное множество — это такое множество А, все элементы которого могут быть занумерованы в последовательность (м.б. бесконечную) $a_1, a_2, a_3, ..., a_n, ...$ так, чтобы при этом каждый элемент получил ишь один номер n и каждое натуральное число n было бы в качестве номера дано одному и лишь одному элементу нашего множества.
Т
Теория множеств — раздел дискретной математики, в котором рассматриваются множества, их свойства, операции над ними.

Криптография
А
Асимметричная криптосистема. Криптосистема, содержащая преобразования (алгоритмы), наборы параметров (ключи) которых различны и таковы, что, по крайней мере, для одного из алгоритмов вычислительно невозможно определить ключи, даже зная ключи всех остальных алгоритмов криптосистемы.
Асимметричный шифр. Шифр, являющийся, асимметричной криптографической системой. В асимметричных шифрах для выполнения процедур за - и расшифрования используются различные ключи. Обычно ключ зашифрования делается

общедоступным (несекретным), в результате чего зашифровать сообщение для получателя может кто угодно, а расшифровать полученное сообщение - только законный получатель, обладающий секретным ключом расшифрования. Синонимы: шифр с открытым ключом.

Атака. Попытка злоумышленника вызвать отклонения от нормального протекания информационного процесса.

Аутентичность данных и систем. Свойство данных быть подлинными и свойство систем быть способными обеспечивать подлинность данных. Подлинность данных означает, что они были созданы законными участниками информационного процесса и не подвергались случайным или преднамеренным искажениям. Способность системы обеспечивать подлинность данных означает, что система способна обнаружить все случаи искажения данных с вероятностью ошибки, не превышающей заданной величины.

Аутентификация. Процедура проверки подлинности данных и субъектов информационного взаимодействия.

Б

Блок, блок криптоалгоритма/шифра. Порция данных фиксированного для заданного криптоалгоритма размера, преобразуемая им за цикл его работы.

В

Взлом, вскрытие криптосистемы. Создание процедуры, позволяющей вызывать отклонения информационного процесса, защищенного использованием криптосистемы, от условий его нормального (штатного) протекания.

Вычислительная неосуществимость, вычислительная невозможность. Невозможность выполнить определенное преобразование данных с использованием имеющихся на сегодняшний день или предполагаемых к появлению в не очень отделенном будущем вычислительных средств за разумное время.

Вычислительно необратимая функция. Функция, легко вычислимая в прямом направлении, в то время как определение значения ее аргумента при известном значении самой функции вычислительно неосуществимо. Вычисление обратного значения для хорошо спроектированной вычислительно необратимой функции невозможно более эффективным способом, чем полным перебором по множеству возможных значений ее аргумента. Синоним: односторонняя функция.

Г

Гамма. Псевдослучайная последовательность элементов данных, вырабатываемая по заданному алгоритму и используемая для зашифрования открытых данных и расшифрования зашифрованных путем комбинирования с ними с использованием обратимой бинарной операции.

Гаммирование. Процесс наложения по определенному закону гаммы шифра на открытые данные для их зашифрования.

Д

Дешифрование Получение открытых данных по зашифрованным в условиях, когда алгоритм расшифрования не является полностью (вместе со всеми секретными параметрами) известным и расшифрование не может быть выполнено обычным путем.

Дешифрование шифротекстов является одной из задач крипто аналитика.

З

Зашифрование. Процесс преобразования открытых данных в зашифрованные при помощи шифра.

Злоумышленник. Субъект, оказывающий на информационный процесс воздействия с целью вызвать его отклонение от условий нормального протекания. Злоумышленник идентифицируется набором возможностей по доступу к информационной системе, работу которой он намеревается отклонить от нормы. Считается, что в его распоряжении всегда есть все необходимые для выполнения его задачи технические средства, созданные на данный момент.

И

Имитозащита. Защита систем передачи и хранения информации от навязывания ложных данных.

Имитовставка. Отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и секретного ключа и добавленный к данным для обеспечения имитозащиты.

Информационный процесс, информационное взаимодействие. Процесс взаимодействия двух и более субъектов, целью и основным содержанием которого является изменение имеющейся у них информации хотя бы у одного из них.

К

Ключ, криптографический ключ. Конкретное секретное значение набора параметров криптографического алгоритма, обеспечивающее выбор одного преобразования из совокупности возможных для данного алгоритма преобразований.

Код аутентификации. Имитовставка, код фиксированной длины, вырабатываемый из данных с использованием секретного ключа и добавляемый к данным с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных. Код обнаружения манипуляций (manipulation detection code).Код фиксированной длины, вырабатываемый из данных с использованием вычислительно необратимой функции с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных.

Криптоанализ

Отрасль знаний, целью которой поиск и исследование методов взлома криптографических_алгоритмов, а также сама процедура взлома.

Криптоаналитик. Человек, осуществляющий криптоанализ.

Криптограф. Специалист в области криптографии.

Криптографическая защита. Защита информационных процессов от целенаправленных попыток отклонить их от нормальных условий протекания, базирующаяся на криптографических преобразованиях данных.

Криптографический алгоритм. Алгоритм преобразования данных, являющийся секретным полностью или частично, или использующий при работе набор секретных параметров. К криптографическим также обычно относят алгоритмы, не являющиеся таковыми в смысле данного выше определения, но работающие с ними в единой технологической цепочке преобразования данных, когда использование одного из них не имеет смысла без использования другого. Примером являются алгоритмы проверки цифровой подписи и зашифрования в асимметричных криптосистемах подписи и шифрования соответственно - они не являются секретными и не используют в работе секретных параметров, но, тем не менее, также считаются криптографическими, так как применяются в единой технологической цепочке вместе с соответствующими алгоритмами формирования цифровой подписи или расшифрования.

Криптографическое преобразование. Преобразование данных по криптографическому алгоритму, то есть такое преобразование, часть деталей которого держится в секрете и которое не может быть осуществлено без знания этих деталей.

Криптография. Отрасль знаний, целью которой является изучение и создание криптографических преобразований и алгоритмов. В настоящее время четко различаются две отрасли криптографии: классическая или традиционная криптография и «современная» криптография.
Криптология Наука, изучающая криптографические преобразования, включает в себя два направления - криптографию и криптоанализ.
Криптосистема, криптографическая система. Набор криптографических преобразований или алгоритмов, предназначенных для работы в единой технологической цепочке для решения определенной задачи защиты информационного процесса.
Криптостойкая гамма. По известному фрагменту, которой нельзя определить другие ее фрагменты и восстановить со всеми деталями алгоритм, использованный для ее выработки.
Криптостойкость, криптографическая стойкость. Устойчивость криптографического алгоритма к его криптоанализу.
О
Односторонняя хэш-функция. Хэш-функция, являющаяся вычислительно необратимой функцией.
Открытый Ключ. Несекретный набор параметров асимметричной криптографической системы, необходимый и достаточный для выполнения отдельных криптографических преобразований.
Открытый текст. Массив незашифрованных данных.
П
Перемешивание. Свойство шифрующего преобразования усложнять взаимосвязи между элементами данных, что затрудняет восстановление функциональных и статистических связей между открытым текстом, ключом и шифротекстом.
Принцип Кирхгофа. Принцип построения криптографических алгоритмов, согласно которому в секрете держится только определенный набор их параметров (ключ), а все остальное может быть открытым без снижения стойкости алгоритма ниже допустимой величины. Был впервые сформулирован в работах голландского криптографа Кирхгофа (возможные варианты транскрипции - Кирхкопф, Керхкофф и т.п.) в списке требований, предъявляемых к практическим шифрам и единственный из всего списка «дожил» до наших дней ассоциированным с именем автора.
Протокол криптографический. Набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах.
Р
Развертывание ключа. Процедура выработки последовательности раундовых ключей из ключа шифрования. Обычно суммарный объем раундовых ключей значительно превышает размер ключа шифрования.
Рандомизация. Преобразование исходных данных перед или во время зашифрования с использованием псевдослучайной последовательности данных, имеющее целью скрыть наличие в них регулярностей различного типа, например - наличие идентичных блоков.
Рассеивание. Распространение влияния одного знака открытого текста на много знаков шифртекста, а также распространение влияния одного элемента ключа на много знаков шифртекста.
Расшифрование. Процесс преобразования зашифрованных данных в открытые при помощи шифра
Раунд. Один шаг шифрования в шифре Файстеля и близких ему по архитектуре шифрах, в ходе которого одна или несколько частей шифруемого блока данных подвергается модификации.
Раундовый ключ. Секретный элемент, получаемый из ключа криптоалгоритма, и используемый шифром Файстеля и аналогичными крипто алгоритмами на одном раунде шифрования.
С
Секретность. Свойство данных быть известными и доступными только тому кругу субъектов, которому для которого они предназначены, и свойство криптосистемы обеспечивать секретность защищаемых данных.
Секретный ключ. Набор секретных параметров одного из алгоритмов асимметричной криптосистемы.
Симметричная криптосистема. Криптографическая система, содержащая преобразования (алгоритмы), выполняемые на одном наборе параметров (ключе) или на различных наборах параметров (ключах) но таким образом, что параметры каждого из преобразований могут быть получены из параметров других преобразований системы.
Симметричный шифр. Шифр, являющийся, симметричной криптографической системой, то есть использующий для за - и расшифрования один и тот же ключ или такие различные ключи, что по одному из них легко может быть получен другой.
Современная криптография Раздел криптографии, изучающий и разрабатывающий асимметричные криптографические системы
Синонимы: двух ключевая криптография, криптография с открытым ключом.
Субъект. Активный компонент, участник процесса информационного взаимодействия, может быть пользователем (человеком), устройством или компьютерным процессом.
Т
Традиционная криптография Раздел криптографии, изучающий и разрабатывающий симметричные криптографические системы .Синонимы: одно ключевая криптография, криптография с секретным ключом.
Ф
Функция шифрования. Функция, используемая в шифре Файстеля и близких по архитектуре шифрах для выработки кода из постоянной части шифруемого блока и раундового ключа, который используется для модификации преобразуемой части шифруемого блока в одном раунде шифрования.
Х
Хэширование. Преобразования массива данных произвольного размера в блок данных фиксированного размера, служащий заменителем исходного массива в некоторых контекстах.
Хэш, Хэш-блок, хэш-значение. Блок данных фиксированного размера, полученный в результате хэширования массива данных, т.е. в результате работы хэш-функции (хэш-алгоритма) с заданным массивом данных на входе.
Хэш-функция. Функция, осуществляющая хэширование массива данных.
Ш
Шифр. Совокупность алгоритмов криптографических преобразований, отображающих множество возможных открытых данных на множество возможных зашифрованных данных, и обратных им преобразований.
Шифр абсолютно стойкий. Шифр, в котором знание шифртекста не позволяет улучшить оценку соответствующего открытого текста, для абсолютно стойкого шифра дешифрование не имеет практического смысла, так как по вероятности

успеха ничем не лучше простого угадывания открытого текста в отсутствии каких-либо дополнительных данных. Синонимы: не вскрываемый, совершенный шифр.

Шифр аддитивный. Шифр гаммирования, в котором для наложения гаммы на данные используется бинарная операция аддитивного типа.

Шифр блочный. Шифр, в котором данные шифруются порциями одинакового размера, называемыми блоками, и результат зашифрования очередного блока зависит только от значения этого блока и от значения ключа шифрования, и не зависит от расположения блока в шифруемом массиве и от других блоков массива.

Шифр гаммирования. Потоковый шифр, в котором для зашифрования данных используется гаммирование.

Шифр замены. Шифр, в котором отдельные символы исходного текста или их группы заменяются на другие символы или группы символов, сохраняя при этом свое положение в тексте относительно других заменяемых групп.

Шифр несовершенный. Шифр, не являющийся абсолютно стойким.

Шифр перестановки. Шифр, в котором процедура зашифрования заключается в перестановках элементов открытого текста или их групп, сами элементы при этом остаются неизменными.

Шифр потоковый или поточный. Шифр, в котором результат зашифрования очередной порции данных зависит от самой этой порции и от всех предыдущих данных шифруемого массива, в важном частном случае он зависит от самой порции данных и от ее позиции в массиве и не зависит от значения предшествующих и последующих порций данных. Иногда данное условие дополняют требованием, что за один шаг шифруется элементарная структурная единица данных - бит, символ текста или байт.

Шифр составной Шифр, составленный из нескольких более простых шифров, которые используются в определенной последовательности при зашифровании и расшифровании данных, обычно составные шифры строятся из большого числа элементарных шифров, каждый из которых заключается в элементарном преобразовании данных.

Шифр Файстеля. Шифр, построенный в соответствии с архитектурой сеть Файстеля.

Шифрование. Процесс зашифрования или расшифрования.

Шифртекст Массив зашифрованных данных, то есть данных, подвергнутых процедуре зашифрования.