ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра Судебной экспертизы

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ В ЮРИСПРУДЕНЦИИ

Учебное пособие для студентов
специальности 030900 Юриспруденция

Бишкек 2016

УДК [004.021:34](075.8)
ББК

Рецензенты:
А.К. Курманбаева, канд. физ.-мат. наук,
А.А. Калыбаева, канд. юрид. наук

Рекомендовано к изданию кафедрой судебной экспертизы
и Ученым советом юридического факультета КРСУ

Коваль И.Г.
МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ В ЮРИСПРУДЕНЦИИ: учебное пособие. – Бишкек: Изд-во КРСУ, 2016. – 94 с.

Учебное пособие посвящено изучению разделов математики, методы которых с применением информационных технологий широко применяются в юриспруденции.

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Цель учебного пособия *«Математическое моделирование в юриспруденции»* в системе подготовки юриста – освоение необходимого математического аппарата, с использованием информационных технологий. Это необходимо для анализа моделирования и решения прикладных юридических задач, в том числе с использованием ЭВМ.

Задачи изучения математических методов как фундаментальной дисциплины состоят в развитии логического и алгоритмического мышления, в выработке умения моделировать реальные правовые процессы.

ВВЕДЕНИЕ

Математика, наука в большей степени прикладная. Однако на современном этапе основной своей задачей она ставит изучение явлений окружающего мира. Одним из способов реализации данной задачи является математическое моделирование, включающее в себя не только построение самой модели, но и изучение объектов данной модели. Математическое моделирование является связующим звеном между математикой и другими науками, в частности, юриспруденции. На современном этапе развития юридической науки увеличивается объем нормативно-правовой, криминологической, уголовно-статистической и иной информации. В этой связи, особую актуальность приобретает анализ математических средств и методов исследования разнообразных правовых явлений и процессов.

Информатика, как фундаментальная наука, занимается разработкой методологии создания информационного обеспечения процессов управления любыми объектами, в том числе и правовыми, на базе компьютерных информационных систем.

Математика и информатика все в большей степени становятся необходимыми атрибутами юридической науки. Это объясняется рядом весомых причин. Рассмотрим некоторые из них:

1. Органическое единство природы и общества. Общество состоит из значительного числа экономических, социальных, правовых и иных систем. Функционирование и развитие этих систем (включая и объекты государственно-правовой реальности) представляют собой естественно-исторический и управленческо-информационный процесс, который должен изучаться с математической точностью.

2. Правовые системы, явления и процессы (прежде всего, механизмы правотворчества, правового регулирования, законности, борьбы с преступностью), *наряду с качественными свойствами* (структурностью, целостностью, устойчивостью), *обладают и количественной мерой* (количеством норм, связей, интенсивностью потоков информации, степенью развития, целенаправленности и т.д.).

3. Оптимизация функционирования правовых систем, юридических органов и процессов. Эти проблемы не могут быть решены без привлечения разнообразных математических методов, так как сущность оптимизации в этом случае состоит в разработке формализованных способов достижения целей функционирования систем с наименьшими затратами материальных средств и времени в решении информационных, логических и математических задач.

4. Понятийный аппарат математики. С его помощью представляется возможным отразить в абстрактном виде структуру отдельных правовых систем, их цели, функции, происходящие в них процессы сбора, обработки и использования информации. К числу этих понятий относятся: высказывание, суждение, множество, подмножество, функция, распознавание образов, «дерево целей», операция, критерий оптимальности, модель и т.д.

5. Количественные параметры. В юридической науке, особенно в таких ее областях, как государственное управление, правовое регулирование предпринимательской деятельности, криминология, криминалистика и правовая информатика, приходится часто иметь дело с количественными параметрами. Последние касаются объема информации, поступающей в государственные органы, количественных оценок правового регулирования, ка-

чества и объема промышленной продукции, состояния и уровня преступности, криминалистических показателей и т.п.

Об аргументах в пользу широкого применения математических средств и методов и о тесной взаимосвязи количественного анализа с качественным в юридических науках забывают. Многие юристы ссылаются на сложность, социальный характер нормативно-правовых и иных, связанных с ними, систем, явлений и процессов. Они указывают на то, что в процессе своей повседневной деятельности имеют дело с фактами не только объективного, но и субъективного порядка, трансформация которых в математическую форму не всегда может осуществляться в рамках положений и аксиом высшей и прикладной математики, а также отмечают невозможность математизации всех явлений правовой реальности.

Общеизвестно, что объекты, изучаемые юридическими науками, действительно социальные, многомерные по своей природе и чрезвычайно сложные. Однако вопрос заключается в другом. Информатизация всех сторон жизни нашего общества, усложнение хозяйственных и социальных связей в условиях рыночных отношений вызывают естественное усложнение систем в сфере юридической деятельности. Это требует всестороннего, в том числе – количественного, математического анализа отдельных правовых и связанных с ними систем, явлений и процессов в области государственного управления, правового регулирования предпринимательства, информационного обеспечения в области права, криминологии, информационного права, криминалистики и т.д. Социальный характер информационных правовых систем, явлений и процессов не может служить препятствием для разумного применения математических методов в юридических науках.

В настоящее время уже можно говорить о содержании «математической юриспруденции», в которую включаются разнообразные понятия и методы математики, некоторые понятия дифференциального и интегрального исчисления, теория множеств, теория вероятностей и математическая статистика, теория информации, теория игр, моделирование причин преступности, сетевые методы управления в сфере правопорядка и т.д. Иначе говоря, под математикой в области юридических наук можно понимать науку

о количественных и пространственных моделях, а также о теоретических информационных моделях в правовой действительности.

Построение математических моделей наряду со специальными знаниями требует знакомства с методологией математики, языка и базовыми понятиями. После построения модели производится её анализ, включающий обработку входной информации, численное решение задачи, анализ результатов вычисления. Современный юрист должен знать суть этих методов, разбираться в проблемах применимости математических методов и их точности.

ГЛАВА 1.
ОБЩИЕ ПОНЯТИЯ, ПРЕДМЕТ И МЕТОДЫ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ 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 следующие 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 их изучения может и должна использоваться *математическая логика*. Применение средств и методов математической логики в правотворческом процессе позволяет:

- улучшить редакцию правовых норм, устранить нечеткие формулировки, упростить громоздкие структуры;
- исследовать нормативно-правовой акт на непротиворечивость;
- символически представить юридические знания для их дальнейшей автоматизированной обработки и компьютеризированного поиска, промоделировать логическую структуру правовой нормы;
- совершенствовать уровень логической завершенности правовых актов и норм права, совершенствовать их логическую структуру;
- уточнить логический смысл и содержание правовых норм путем их толкования;

- проводить логическую экспертизу нормативных правовых актов.

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.

Идея применения математических методов для решения задач криминалистики и судебной экспертизы была высказана на рубеже XIX–XX веков рядом выдающихся криминалистов (Альфонс Бертильон 23.04.1853–13.02.1914, Е.Ф. Буринский 6.02.1849–18.03.1912, Фрэнсис Гальтон 16.02.1822–17.01.1911).

Достаточно активно математические методы стали внедряться для решения задач судебной экспертизы в середине 50-х годов. Впервые в истории криминалистики были выполнены обширные работы по подсчету частоты встречаемости различных криминалистических признаков. Несколько позже *аппарат теории вероятности, комбинаторики, теории множеств и математической статистики* был применен при разработке новых методов судебно-портретной экспертизы (З.И. Кирсанов), аналитического исследования свинца и бумаги (В.М. Колосова), дактилоскопической экспертизы (А.Я. Палиашвили). Среди всех видов судебных экспертиз наибольшее практическое значение математические методы имеют для почерковедческой и дактилоскопической экспертизы.

Методы математической статистики и теории вероятностей могут быть применены для:

- оценки идентификационного значения качественных и количественных признаков, характеризующих объекты судебно-экспертного решения, а также комплекса признаков;
- исследования взаимозависимости признаков;
- оценки надежности идентификации.

Основанием применения вероятностно-статистических методов для оценки идентификационных признаков является массовый характер последних, случайность их появления в силу действия закона больших чисел.

Методы *математической статистики* широко применяются для анализа социологической статистической информации – официально документированных сведений, дающих количественную характеристику социальным массовым событиям и явлениям. К таким явлениям в правовой сфере относятся: преступность, административные правонарушения, массив уголовных и гражданских дел и т.д. Для применения статистических методов в правовых исследованиях существенное значение имеет тот факт, что многим объектам юридической практики присущи статистические закономерности. Так, правовое сознание общества складывается из огромного числа правосознаний отдельных личностей. На этой основе образуется статистическое согласие. Другим характерным примером является массив правонарушений. Статистическими особенностями обладает и сам механизм действия правовой нормы: она рассчитана на многократное применение и действие по отношению к различным индивидам в различных социальных ситуациях.

Методы *теории вероятности* и *комбинаторики* играют большую роль в области *криптографии*. Веками создавались самые различные системы тайнописи, которыми владели только «посвященные», умевшие и зашифровать текст, и расшифровать его. Конечно, для «непосвященных» разгадать шифр всегда было очень важно. Поэтому веками разрабатывались как способы расшифровки чужих шифров, так и способы создания своих шифров, которые не поддавались бы расшифровке. Проблема расшифровки связана не только с секретами, которые следует скрыть от посторонних. Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом или битовой последовательностью, обычно называемой шифрующим ключом.

Преступность представляет собой сложную динамическую систему. Поскольку она как система характеризуется множеством

факторов (уровнем, динамикой, структурой, а также связями с другими процессами, явлениями, факторами), то для достижения высокой степени познания такой системы необходимы глубокие и многогранные исследования, путь к которым открывает *математическое моделирование*, в том числе, с помощью компьютерной техники. Для обеспечения комплексности исследований, повышения достоверности их результатов и наглядного отображения информации, целесообразно алгоритмизировать на математической основе:

- модели пространственно-временного распределения преступности;
- модели динамики преступности;
- факторные модели преступности;
- структурно-динамические модели преступности.

Воспроизведение этих моделей с помощью компьютера позволяет быстро вносить коррективы, обусловленные изменением криминальной ситуации, анализировать модели в их взаимосвязи. Следовательно, дает более широкие возможности делать обоснованные криминологические прогнозы, разрабатывать наилучшие формы и методы борьбы с преступностью, наиболее эффективно использовать имеющиеся средства предупреждения и раскрытия преступлений.

Перспективное направление в сфере моделирования социально-правовых процессов – имитационное моделирование, которое часто называют «машинным экспериментом». Идея этого *математико-кибернетического* метода моделирования состоит в имитации (искусственном воспроизведении) исследуемого явления или процесса на основе имеющейся ретроспективной информации о нем.

Таким образом, из приведенных примеров видно, что математические методы с применением информационных технологий широко применяются в юриспруденции. Изучению именно этих разделов математики, как уже было отмечено выше, и посвящено учебное пособие.

ГЛАВА 2.
ОСНОВЫ МАТЕМАТИЧЕСКОЙ ЛОГИКИ

2.1. Логика как наука

Логика – это наука, изучающая формы и законы мышления, закономерности мыслительного процесса. Слово «логика» произошло от греческого *logos,* что означает *слово, понятие, рассуждение, разум*.

Этапы становления логики как науки

Логика Античности (VI век до н.э.) зародилась в лоне философии как инструмент ораторского искусства и научного знания. Основатели: Демокрит, Аристотель. Демокрит (460–370 гг. до н.э.) начал борьбу против софистики («софизм» – хитрость). Аристотель (384–322 гг. до н.э.) в ходе борьбы с софистикой заложил основы науки о мышлении, которую назвал «аналитикой». Впервые термин «логика» для обозначения самостоятельной науки стал употребляться стоиками[1] (Зенон, Хризипп).

Логика Средневековья (V–XI вв.). Теоретический поиск в логике вёлся по проблеме истолкования природы общих понятий. Реалисты считали, что общие понятия существуют реально, независимо от единичных вещей. Номиналисты же, напротив, считали, что реально существуют только единичные предметы, а общие понятия – лишь имена, названия для них. Представители этих направлений: Петр Испанский, англ. Думс Скотт, Вильям Оккам, нем. Альберт Саксонский.

Логика Возрождения (XV–XVII вв.). Идёт бурное развитие науки. Развивается методология научного познания. Возрастает роль логики в научном познании. Англичанин Френсис Бэкон (1561–1626) разработал основы индуктивной логики. Французский философ Рене Декарт (1569–1650) сформировал четыре правила научного исследования. Таким образом, возрождается роль логики в познании мира.

[1] Стоик – человек, стойко и мужественно переносящий жизненные испытания.

Логика Нового Времени (XVII–XIX вв.). В логике произошла научная революция. На смену традиционной логике пришла математическая, или символическая. В основе последней лежат идеи немецкого учёного Г. Лейбница (1636–1716) о возможности представить доказательство как математическое вычисление. Г. Гегель (1770–1831) разработал проблемы диалектической логики. Русские учёные М.В. Ломоносов (1711–1765), А.Н. Радищев (1749–1802) разработали классификацию умозаключений по сходству.

Логика Современности (XIX–XX вв.). Символическая логика, широко применяется в математике, физике, биологии, кибернетике, экономике, лингвистике. Большая заслуга в этом англичанина Дж. Буля (1815–1904), немецкого учёного Г. Фреге (1848–1925), английского философа Б. Рассела (1872–1970), русского учёного Порецкого (1846–1907 гг.). В трудах философов и учёных Германии К. Маркса (1818–1883) и Ф. Энгельса (1820–1895) развивается диалектическая логика. В России разработку отдельных проблем диалектической логики, её соотношения с логикой формальной продолжали Г. Плеханов (1856–1918) и В.И. Ульянов (Ленин) (1870–1924).

Логические знания чрезвычайно важны для повышения эффективности мыслительной деятельности человека и предотвращения логических ошибок. В формальной логике семиотической категорией является суждение (высказывание) – повествовательное предложение. Предложение высказывает мысль по своему логическому значению истинную или ложную. Законы и правила формальной логики необходимо знать для построения правильных рассуждений. Согласно основному принципу логики, правильность рассуждения (вывода) определяется только его логической формой (структурой) и не зависит от конкретного содержания входящих в него утверждений. Например, рассуждения «Все люди смертны. Сократ – человек. Следовательно, Сократ смертен» и «Все металлы электропроводны. Медь – металл. Следовательно, медь электропроводна» имеют одинаковую логическую структуру, называемую *силлогизмом***.** Отличительная особенность правильного вывода состоит в том, что из истинных исходных утверждений всегда получаются истинные заключения.

Это позволяет из одних истин получать другие с помощью только рассуждения, разума, без обращения к опыту.

Логика состоит из большого числа логических систем, описывающих отдельные типы содержательных рассуждений. Эти системы принято делить на *классическую логику,* включающую классические логику высказываний и логику предикатов, и *неклассическую логику,* в которую входят *модальная* логика, *многозначная* логика, *деонтическая* логика, логика *времени*, *паранепротиворечивая* логика, *парафальсифицирующая* логика и др. Все эти частные системы, пользующиеся одними и теми же методами исследования при описании отдельных логических процессов, соединяясь вместе образуют логику как единую науку. Для любой логики характерно отвлечение от конкретного содержания высказываний или умозаключений и оперирование только их формальным содержанием, использование единого языка символов и формул.

Как самостоятельная наука логика оформилась в трудах греческого философа Аристотеля (384–322 гг. до н.э.). Он систематизировал известные до него сведения, и эта система стала впоследствии называться традиционной или Аристотелевой логикой. Аппарат логики Аристотеля оказался настолько мощным, что, например, на его основе средневековый философ и богослов Фома Аквинский (1225–1274) осуществил обоснование всей христианской теологии. Широкое применение силлогистика нашла также в судебной практике, когда материалы предварительного следствия брались за истинные посылки. Применяя к этим посылкам процедуры порождения новых утверждений по правилам теории Аристотеля, судьи делали вывод о виновности или невиновности подсудимого. Традиционная логика просуществовала без серьезных изменений более двадцати столетий.

В XIX – начале XX веке в логике произошла научная революция и на смену традиционной логике пришла современная логика, называемая также математической или символической. Развитие математики выявило недостаточность Аристотелевой логики и поставило задачу об её дальнейшем построении на математической основе. Впервые в истории идеи о таком построении логики были

высказаны немецким математиком Готфридом Лейбницем (1646–1716) в конце XVII века. Он считал, что основные понятия логики должны быть обозначены символами, которые соединяются по определенным правилам, и это позволяет всякие рассуждения заменить вычислением. Джордж Буль (1815–1864) в своей работе «Исследование законов мысли» (1854) истолковывал умозаключения как результат решения логических равенств, в результате чего логическая теория приняла вид обычной алгебры и получила название алгебры высказываний. Буль рассматривал свою алгебру как инструмент изучения законов человеческого мышления.

Введение символических обозначений в логику имело для этой науки такое же решающее значение, как и введение буквенных обозначений для математики. Именно благодаря введению символов в логику была получена основа для создания новой науки – математической логики. Предметом математической логики служат рассуждения, при изучении которых она пользуется математическими методами.

При этом, на первых порах развитие математической логики позволило представить логические теории в новой удобной форме и применить вычислительный аппарат к решению задач, малодоступных человеческому мышлению, что, конечно, расширило область логических исследований. Однако, главное назначение математической логики определилось в конце XIX века, когда стала ясна необходимость обоснования понятий и идей самой математики. Эти задачи имели логическую природу и, естественно, привели к дальнейшему развитию математической логики.

В этом отношении показательны работы немецкого математика Готлоба Фрёге (1848–1925) и итальянского математика Джузеппе Пеано (1858–1932), которые применили математическую логику для обоснования арифметики и теории множеств.

В развитие логики значительный вклад внесли Бертран Рассел (1872 – 1970), А. Уайтхед (1861–1947), Д. Гильбер (1862–1943), К. Гедель (1906–1978), А. Тарский (1901–1983) и др.

В первой половине XX века стали складываться *многозначная логика,* предполагающая, что утверждение может быть не только истинным или ложным, но иметь и другие значения истинности;

деонтическая логика, изучающая логические связи нормативных высказываний; *модальная логика,* рассматривающая понятия необходимости, возможности, случайности и т.п.; *эпистемическая логика,* изучающая такие понятия, как опровержимо, неразрешимо, доказуемо, убежден и т.п., *паранепротиворечивая логика; парафальсифицирующая логика* и др. Все эти новые разделы логики были связаны с естественными и гуманитарными науками. Перемены, происшедшие с логикой в XX веке, приблизили ее к непосредственному человеческому мышлению, к практической деятельности человека.

Знание логики является неотъемлемой частью юридического образования. Оно позволяет правильно строить судебно-следственные версии, составлять четкие планы расследования преступлений, не допускать ошибок при составлении официальных документов, протоколов, обвинительных заключений, решений и постановлений.

Знаменитые юристы всегда использовали знание логики. В суде они, например, не ограничивались простым несогласием с доводами обвинения, если видели в них логическую ошибку. Они объясняли, какая ошибка допущена, говорили, что эта ошибка специально рассматривается в логике и имеет особое название. Такой довод оказывал воздействие на всех присутствующих, даже если присутствующие никогда не изучали логики.

Знание правил и законов логики не является конечной целью ее изучения. Конечная цель изучения логики – умение применять ее правила и законы в процессе мышления. Истина и логика взаимосвязаны, поэтому значение логики невозможно переоценить. Логика помогает доказывать истинные сужения и опровергать ложные, она учит мыслить четко, лаконично, правильно.

Далее мы рассмотрим наиболее важный для будущих юристов раздел логики – *логику высказываний.*

2.2. Использование логики высказываний в юриспруденции

Логика высказываний – раздел логики, в котором вопрос об истинности или ложности высказываний рассматривается и ре-

шается на основе изучения способа построения высказываний из элементарных выражений (далее не разлагаемых и не анализируемых) с помощью логических связок. Логику высказываний, задаваемую системой постулатов (аксиом и правил вывода), называют также исчислением высказываний.

Основным понятием этого раздела логики, естественно, является *высказывание*.

Высказыванием называется всякое утверждение (повествовательное предложение), про которое всегда определенно и объективно можно сказать, является ли оно истинным или ложным. Например, предложения «Дважды два – четыре», «Студенты гуманитарных специальностей изучают информатику и математику», «3 больше 5», «Число 10 является нечетным», «На улице идет дождь», «Уголовное дело отправлено на доследование» являются высказываниями. Побудительные предложения («Кругом», «Налево», «Подойдите, пожалуйста, ко мне»), вопросительные («Вы не подскажете, как пройти в библиотеку?»), восклицательные («Да здравствует свобода!») высказываниями не являются.

Повествовательное предложение, содержащее переменную, также не является высказыванием. Например, утверждение «*x* – положительное число» не будет высказыванием, так как нельзя определить ложно оно или истинно. Если же мы подставим вместо переменной *x* какое-либо число, то получим высказывание: «*5* – положительное число» (истинное высказывание), «*0* – положительное число» (ложное высказывание).

Обратимся к вышеприведенным высказываниям. В рассмотренных примерах высказываний два первых являются истинными во всех возможных ситуациях. Такие высказывания называются *абсолютно истинными*. Третье и четвертое являются *абсолютно ложными*. Абсолютно истинные и абсолютно ложные высказывания называются *логическими константами*. Пятое и шестое высказывания будут истинны или ложны в зависимости от конкретной ситуации. В одних случаях они будут истинными, в других – ложными. Поэтому точнее говорить, что данное высказывание истинно или ложно в определенной фиксированной си-

туации. Ситуация может быть определена в самом высказывании («Вечером второго июня 2013 года в городе Бишкек осадков не наблюдалось»), а может описываться дополнительно.

Высказывания обычно обозначаются заглавными латинскими буквами: *A, B, C* и т.д.

Например, *A* – «Неман впадает в Балтийское море», *B* – «2 больше 6», *C* – «На улице идет снег». Подобные обозначения вводятся для упрощения анализа высказывания. В этом случае вместо сложных рассуждений мы получим выражения, традиционно встречающиеся в математике. Будем полагать значение истинного высказывания равным *1*, а ложного – равным *0*. Тогда, *A = 1*, так как «Неман впадает в Балтийское море» – абсолютно истинное высказывание; *B = 0* как абсолютно ложное; *C* может быть равно *1*, а может *0,* в зависимости от рассмотренной ситуации. В математической логике для обозначения истинности и ложности высказываний используют буквы *И* (истина) и *Л* (ложь), или *t* (true) и *f* (false).

С помощью союзов *«и», «или», «если…… то»*, частицы «*не*» из нескольких высказываний (повествовательных предложений) можно составить различные новые высказывания. При этом исходные высказывания, которые нельзя разбить на еще более мелкие, называются *простыми*, а сконструированные при помощи логических связок – *сложными*.

В определенной ситуации истинность или ложность простых высказываний очевидна. Для определения истинности сложных высказываний необходимо не только знать, истинны или ложны простые высказывания, из которых построены сложные, но и проанализировать их структуру. Разрешение вопроса об истинности или ложности сложных высказываний, рассматриваемого на основе изучения способа их построения из элементарных, является основной задачей логики высказываний.

Логика высказываний – раздел логики, изучающий связи между высказываниями, которые определяются тем, как одни высказывания строятся из других. Эту часть логики еще называют алгеброй высказывания или исчислением высказываний.

Например: Рассмотрим два высказывания: «Сегодня будет хорошая погода», «Мы пойдем на прогулку». Из этих простых высказываний можно сконструировать сложные:

- «Сегодня будет хорошая погода, и мы пойдем на прогулку».
- «Мы не пойдем на прогулку».
- «Если сегодня будет хорошая погода, то мы пойдем на прогулку».
- «Мы пойдем на прогулку сегодня тогда и только тогда, когда будет хорошая погода».
- «Сегодня будет хорошая погода или мы пойдем на прогулку».
- «Если мы пойдем на прогулку, то сегодня будет хорошая погода».

В последней фразе нарушается нормальная причинно-следственная связь, однако, это сложное высказывание, с точки зрения логики высказываний, ничем не хуже остальных. В ней допускаются любые грамматически правильно составленные высказывания, а их смысловая характеристика не изучается. Важно только то, что получившееся предложение может быть формально либо истинным, либо ложным. Например: Значение истинности (т.е. истинность или ложность) высказывания *«норма жилой площади устанавливается в размере 18 кв. м на одного человека»* определяется принятым ЖК (жилищный кодекс РФ). Различают простые и составные высказывания. Высказывание *«наследники умершей – ее муж и сын»* – составное, в то время как высказывания *«наследник умершей – ее муж»* и «*наследник умершей – ее сын»* – простые. Связывание простых высказываний в составные осуществляется логическими операциями, называемыми связками. Сложное высказывание получается путем объединения простых высказываний *логическими связками НЕ, И, ИЛИ*. Значение истинности сложных высказываний зависит от истинности входящих в них простых высказываний и объединяющих их связок.

Например, даны простые высказывания: *Наследник умершей – ее муж*; *наследник умершей – ее сын*. Составим из них сложное высказывание:

*«Наследники умершей – ее муж **И** сын».*

Например, даны простые высказывания:

На улице идет дождь. На улице светит солнце. На улице пасмурная погода. Составим из них сложные высказывания: *На улице идет дождь* ***И*** *на улице светит солнце. На улице светит солнце* ***ИЛИ*** *на улице пасмурная погода.* ***НЕВЕРНО****, что на улице идет дождь.*

В математической логике не рассматривается конкретное содержание высказывания, важно только, истинно оно или ложно. Поэтому высказывание можно представить некоторой переменной величиной, значением которой может быть только *0* или *1*. Если высказывание истинно, то его значение равно *1*, если ложно – *0*. Простые высказывания назвали *логическими переменными* и для простоты записи их обозначают латинскими буквами: *A, B, C.*

Луна является спутником Земли: *A = 1. Москва – столица Германии: B = 0.* Сложные высказывания называются *логическими функциями*. Значения логической функции также может принимать значения только *0* или *1*. В алгебре высказываний, как и в обычной алгебре, вводится ряд операций. Логические связки *И, ИЛИ* и *НЕ* заменяются логическими операциями: *конъюнкцией, дизъюнкцией и инверсией, импликацией и эквивалентностью.* Это – основные логические операции, при помощи которых можно записать любую логическую функцию.

2.3. Базовые логические операции

Логическая операция ИНВЕРСИЯ (ОТРИЦАНИЕ)

Соответствует частице *НЕ, NOT.* Обозначается черточкой над именем переменной или знаком ¬ перед переменной. *Инверсия логической переменной истинна, если сама переменная ложна, и, наоборот, инверсия ложна, если переменная истинна.* Логическое отрицание (инверсия) делает истинное высказывание ложным и, наоборот, ложное высказывание истинным. Например: Пусть *A = «Два умножить на два равно четырем»* – истинное высказывание, тогда высказывание *B = «Два умножить на два не равно четырем»,* образованное с помощью операции логического отрицания, – ложное высказывание.

Таблица 1 – Таблица истинности инверсии

A	$\bar{A}$
0	1
1	0

Логическая операция КОНЪЮНКЦИЯ (ЛОГИЧЕСКОЕ УМНОЖЕНИЕ)

Соответствует союзу *И, AND,* обозначается знаком *&* или *Λ*, или *******. Конъюнкция двух логических переменных истинна тогда и только тогда, когда оба высказывания истинны.* Это определение можно обобщить для любого количества логических переменных, объединенных конъюнкцией. *A & B & C = 1, только если A = 1, B = 1, C = 1*. Например: Высказывание *«Юрист должен знать информатику и математику»* является конъюнкцией высказываний: A – *«юрист должен знать информатику»* и B – *«юрист должен знать математику».*

Таблица 2 – Таблица истинности конъюнкции

A	**B**	**A & B**
0	**0**	**0**
0	**1**	**0**
1	**0**	**0**
1	**1**	**1**

Логическая операция ДИЗЪЮНКЦИЯ (ЛОГИЧЕСКОЕ СЛОЖЕНИЕ)

Соответствует союзу *ИЛИ, OR,* обозначается знаком *(v)* или *(+)* или (|). *Дизъюнкция двух логических переменных ложна тогда и только тогда, когда оба высказывания ложны.* Это определение можно обобщить для любого количества логических переменных, объединенных дизъюнкцией. *A v B v C = 0,* только если *A = 0, B = 0, C = 0.*

Например, в высказывании *«Договор может быть заключен в устной или письменной форме»* допускается возможность заключения договора не только в какой-то одной форме, но и в обоих. А в высказывании *«5 марта я поеду на шахматный*

турнир в Москву или во Владивосток» исключено посещение обоих турниров одновременно.

Таблица 3 – Таблица истинности дизъюнкции

A	B	A v B
0	0	0
0	1	1
1	0	1
1	1	1

Логическая операция разделительная дизъюнкция (НЕРАВНОЗНАЧНОСТЬ)

Разделительной дизъюнкцией (сумма по модулю 2) высказываний A и B называется высказывание, истинное тогда и только тогда, когда одно высказывание истинное, а другое – ложное. Неравнозначность высказываний A и B обозначается A E.

Таблица 4 – Таблица истинности неравнозначности

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Например: Рассмотрим два высказывания: *A = «Кошка охотится за мышами»* и *B = «Кошка спит на диване».* Очевидно, что новое высказывание *A B* истинно только в двух случаях: *когда кошка охотиться за мышами либо когда кошка мирно спит.* Это высказывание будет *ложно, если кошка не делает ни того, ни другого, т.е. когда оба события не происходят*. Но это высказывание *будет ложным и тогда, когда предполагается, что оба высказывания произойдут одновременно.* В силу того, что этого произойти не может, высказывание и является ложным. В логике связкам *«либо»* и *«или»* придается разное значение, однако в русском языке связку *«или»* иногда употребляют вместо связки *«либо».* В этих случаях однозначность определения используемой логической операции связана с анализом содержания высказывания.

Например, анализ высказывания *«Алмаз находится в аудитории 508 либо в аудитории 503»* заменить на *«Алмаз находится в аудитории 508 или в аудитории 503»,* то анализ последнего высказывания однозначно укажет на логическую операцию «разделительная дизъюнкция», т.к. человек не может находиться в двух разных местах одновременно.

Логическая операция ИМПЛИКАЦИЯ (ЛОГИЧЕСКОЕ СЛЕДОВАНИЕ)

Импликация двух высказываний *A* и *B* соответствует союзу *«ЕСЛИ…ТО».* Она обозначается символом →. Запись *A → B* читается как *«из A следует B». Импликация двух высказываний истинна всегда, кроме случая (A = 1, B = 0), если первое высказывание истинно, а второе ложно.*

Таблица 5 – таблица истинности импликации двух суждений *A* и *B***.**

Таблица 5 – Таблица истинности импликации

A	B	A → B
0	0	1
0	1	1
1	0	0
1	1	1

Операция импликации A → *B* хорошо описывается союзом *«если ..., то ...»* в случаях описания *причинно-следственной связи* между A и *B*.

Например, высказывание *«Если долго мучиться, то что-нибудь получится»* – выражение логического следования *B* из *A*.

Например, высказывание *«Если все люди смертны и Сократ – человек, то Сократ смертен».* В этих высказываниях существует связь между содержанием высказываний *A* и *B,* объединенных союзом.

Примечание. В логике высказываний рассматриваются только значения истинности высказываний, а не их содержание. Тем самым логические операции не выражают связь между содержанием высказываний. Логические операции, образующие из простых высказываний сложные, определяют только соотношения между значениями истинности этих высказываний.

Логическая операция ЭКВИВАЛЕНТНОСТЬ (ЛОГИЧЕСКОЕ РАВЕНСТВО, ФУНКЦИЯ ТОЖДЕСТВА)

Она обозначается символами ≡ или <=> («тогда и только тогда»). Запись $A \equiv B$ читается как *«A эквивалентно B». Эквивалентность двух высказываний истинна только в тех случаях, когда оба высказывания ложны или оба истинны.* Таблица 6 – таблица истинности эквивалентности двух суждений *A* и *B*.

Таблица 6 – Таблица истинности эквивалентности

A	B	A ≡ B
0	0	1
0	1	0
1	0	0
1	1	1

Эта операция обозначается символом ↔ либо ~. Сложное высказывание A«B читается: *«A эквивалентно B»*, либо *«A равносильно B»*, либо *«A тогда и только тогда, когда B»*, либо *«B, если и только если A»*. Эквивалентность примерно соответствует употреблению выражения *«тогда и только тогда, когда»*, хотя, как и в случае с импликацией, такое соответствие далеко не полное.

Например:

1. «Два треугольника равны *тогда и только тогда, когда* три стороны одного треугольника равны соответствующим сторонам другого треугольника».
2. «Деяние кража *равносильно* тайному хищению чужого имущества».
3. «Распространение заведомо ложных сведений является клеветой, *если и только если* эти сведения задевают честь и достоинство другого лица или подрывают его репутацию».

2.4. Логические выражения и таблицы истинности

Сложные высказывания можно записывать в виде формул. Для этого простые логические высказывания нужно обозначить как логические переменные буквами и связать их с помощью знаков логических операций. Такие формулы называются *логическими выражениями.* Например:

$$\overline{(A \vee B \,\&\, C)} \quad (A \vee B)\,\&\,(\overline{A} \vee \overline{B})$$

Чтобы определить значение логического выражения, необходимо подставить значения логических переменных в выражение и выполнить логические операции. Операции в логическом выражении выполняются слева направо с учетом скобок в следующем порядке:

- Инверсия;
- Конъюнкция;
- Дизъюнкция; неравнозначность;
- Импликация и эквивалентность.

Для изменения указанного порядка выполнения логических операций используются круглые скобки. Для каждого составного высказывания (логического выражения) можно построить *таблицу истинности*, которая определяет истинность или ложность логического выражения при всех возможных комбинациях исходных значений простых высказываний (логических переменных). При построении таблиц истинности целесообразно руководствоваться определенной последовательностью действий:

1. Записать выражение и определить порядок выполнения операций.
2. Определить количество строк в таблице истинности. Оно равно количеству возможных комбинаций значений логических переменных, входящих в логическое выражение (определяется по формуле $Q = 2^n$, где n – количество входных переменных).
3. Определить количество столбцов в таблице истинности *(= количество логических переменных + количество логических операций*).
4. Построить таблицу истинности, обозначить столбцы (имена переменных и обозначения логических операций в порядке их выполнения) и внести в таблицу возможные наборы значений исходных логических переменных.

5. Заполнить таблицу истинности, выполняя базовые логические операции в необходимой последовательности и в соответствии с их таблицами истинности.

Теперь мы можем определить значение логической функции для любого набора значений логических переменных.

Например, построим таблицу истинности для логической функции:

$$F(A,B,C) = \overline{A}\,\&\,(B \vee C)$$

1. Количество входных переменных в заданном выражении равно трем *(A, B, C)*. Значит, количество входных наборов, а значит и строк $Q = 2^3 = 8$.

2. Количество столбцов равно *6* (3 переменные + 3 операции). Столбцы таблицы истинности соответствуют значениям исходных выражений *A, B, C*, промежуточных результатов и *(B V C)*, а также искомого окончательного значения сложного арифметического выражения.

Таблица 7 – Таблица истинности логического выражения

A	B	C	$\overline{A}$	$B \vee C$	$\overline{A}\,\&\,(B \vee C)$
0	**0**	**0**	**1**	**0**	**0**
0	**0**	**1**	**1**	**1**	**1**
0	**1**	**0**	**1**	**1**	**1**
0	**1**	**1**	**1**	**1**	**1**
1	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**0**	**1**	**0**
1	**1**	**0**	**0**	**1**	**0**
1	**1**	**1**	**0**	**1**	**0**

Исследовать свойства логических выражений позволяют таблицы истинности (таблица 7), которые представляют собой перечисление всех возможных комбинаций значений переменных с указанием значения функции для каждой комбинации. Таблицы истинности позволяют решать прикладные задачи:

Пример 1. Разбирается дело *Львова, Перова и Бакаева.* Кто-то из них нашел и утаил клад. На следствии каждый из них сделал по два заявления.

Бакаев: «Я *не* делал этого. Перов сделал это».

Львов: «Перов *не* виновен. Бакаев сделал это».

Перов: «Я *не* делал этого. Львов *не* делал этого».

Суд установил, что один из них дважды *солгал,* другой *дважды сказал правду,* третий *один раз солгал, один раз сказал правду.*

Вопрос: Кто утаил клад?

Решение:

Введём обозначения: *Б* – клад утаил *Бакаев, П* – клад утаил *Перов, Л* – клад утаил Львов. Рассмотрим *три возможных варианта:* виноват *Бакаев (= 1),* виноват *Перов (= 1),* виноват *Львов (= 1).* Полученные при таких вариантах значения высказываний трёх обвиняемых представлены в таблице 8.

Таблица 8 – Таблица истинности для решения задачи

Возможные варианты			**Высказывания Бакаева**		**Высказывания Львова**		**Высказывания Перова**		**Соответствие условию задачи**
Б	**Л**	**П**	**¬Б**	**П**	**¬П**	**Б**	**¬П**	**¬Л**	
1	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**–**
0	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**1**	**+**
0	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**–**

1. В первом варианте *один солгал дважды, а двое сказали правду дважды,* что не соответствует условию задачи.

2. В третьем варианте *все один раз сказали правду и один раз солгали*, что также не соответствует условию задачи.

3. Во втором варианте *один дважды солгал, другой дважды сказал правду,* а третий *один раз сказал правду (Львов не делал этого),* а один раз солгал *(Перов: Я не делал этого),* что соответствует условию задачи.

Следовательно, клад утаил *Перов* (таблица 8).

Пример 2. Трое подозреваемых в преступлении *Ильин, Панин* и *Саматов* дали следующие показания:

1. Ильин сказал: «Если виновен *Саматов*, то и *Панин* тоже виновен».

2. Панин сказал: «Виновен либо *Ильин*, либо *Саматов*, но не оба».

3. Саматов сказал: «Я не виновен, а виновен *Панин*».

Вопрос: Построить таблицу истинности каждого высказывания и по ней определить:

1. Кто виновен, если все говорят правду?
2. Кто виновен, если все лгут?
3. Кто лжет, если все виновны?
4. Кто лжет, если все невиновны?
5. Кто виновен, если виновные лгут, а невиновные говорят правду?

Решение:

Введем простые высказывания:

A = {виновен *Ильин*};

B = {виновен *Панин*};

C = {виновен *Саматов*}.

Тогда показания *Ильина* будут иметь вид: $C \rightarrow B$ (*импликация*), показания *Панина*: $A \oplus C$ (*разделительная дизъюнкция*), показания *Саматова*: $\neg C \,\&\, B$.

Составляем таблицу истинности каждого высказывания.

Таблица 9 – Таблица истинности высказываний подозреваемых

A	**B**	**C**	**¬C**	**Показания Ильина C → B**	**Показания Панина A ⊕ C**	**Показания Саматова ¬C & B**
0	**0**	**0**	**1**	**1**	**0**	**0**
0	**0**	**1**	**0**	**0**	**1**	**0**
0	**1**	**0**	**1**	**1**	**0**	**1**
0	**1**	**1**	**0**	**1**	**1**	**0**
1	**0**	**0**	**1**	**1**	**1**	**0**
1	**0**	**1**	**0**	**0**	**0**	**0**
1	**1**	**0**	**1**	**1**	**1**	**1**
1	**1**	**1**	**0**	**1**	**0**	**0**

По оставленной таблице (таблица 9) отвечаем на вопросы задачи.

1. *Если все говорят правду,* то в показаниях (последние три столбца) должны быть три единицы. Такому условию соответствует *предпоследняя строка*, из которой по значениям в первых трех столбцах *(1, 1, 0)* делаем вывод, что *Ильин* и *Панин* виновны, а *Саматов* нет.

2. *Если все лгут,* то в показаниях должны быть три нуля. Такому условию соответствует *шестая строка,* из которой по значениям в первых трех столбцах делаем вывод, что *Ильин* и *Саматов* виновны, а *Панин* нет.

3. Условию того, *что все виновны,* соответствует *последняя строка*, у которой в первых трех столбцах все единицы. По значениям показаний (последние три столбца) видно, что *Ильин* говорит правду, а *Панин* и *Саматов* лгут.

4. Условию того, что *все невиновны*, соответствует *первая строка*, у которой в первых трех столбцах все нули. По значениям показаний видно, что *Ильин* говорит правду, а *Панин* и *Саматов* лгут.

5. *Если виновные лгут, а невиновные говорят правду*, то в каждой паре значений столбцов виновности (первые три) и показаний (последние три) для каждого подозреваемого должны стоять разные значения. Этому условию соответствует *третья строка,* у которой значения первых трех столбцов *(0, 1, 0),* а последних трех *(1, 0, 1)*. Это означает, что *Ильин* невиновен и говорит правду, *Панин* виновен и лжет, а *Саматов* невиновен и говорит правду.

Пример 3. Петров, Иванов и Сидоров сдавали экзамен по ТГП.

1. Если Петров *не* сдал экзамен на «отлично», то и Иванов *не* сдал на «отлично».
2. Сидоров и еще один из друзей сдали экзамен на «отлично».

Вопрос: Следует ли отсюда, что *не верно,* что Петров сдал экзамен *не* на «отлично», а Иванов – на «отлично»?

Решение:

Обозначим высказывание: Петров не сдал экзамен на «отлично» – *П*, Иванов не сдал экзамен на «отлично» – *И, (П → И)*, Сидоров – не сдал экзамен на «отлично» – *С*.

Составим таблицу истинности исходя из условия задачи: $\neg С \wedge П \rightarrow И$.

Таблица 10 – Таблица истинности высказываний студентов

П	**И**	**С**	**¬ С**	**П →И**	$\neg С \wedge П \rightarrow И$.
1	**1**	**1**	**0**	**1**	**0**
1	**1**	**0**	**1**	**1**	**1**
1	**0**	**1**	**0**	**0**	**0**
1	**0**	**0**	**1**	**0**	**0**
0	**1**	**1**	**0**	**1**	**0**
0	**1**	**0**	**1**	**1**	**1**
0	**0**	**1**	**0**	**1**	**0**
0	**0**	**0**	**1**	**1**	**1**

Анализируя данные, полученные в таблице (таблица 10), можно сделать вывод: значение истина, мы видим *в шестой и в восьмой* строках. Но восьмая строка не соответствует условию, что вместе с Сидоровым получил «отлично» еще один студент. Для Иванова высказывание, что он получил «отлично», равно 1, является ложью в шестой строке.

Поэтому, *да следует,* что *не верно*, что Петров сдал экзамен *не* на «отлично», а Иванов на «отлично».

Пример 4. При решении логических задач, постоянно возникающих в деятельности юриста, необходимо формализовать имеющиеся утверждения, определить базовую связь между ними и упростить полученное выражение путем равносильных преобразований. Для этого используется *алгоритм решения логических задач:*

1. Внимательно изучить условие.
2. Выделить простые высказывания и обозначить их латинскими буквами.
3. Записать условие задачи на языке алгебры логики.
4. Составить конечную формулу. Для этого объединить логическим умножением формулы каждого утверждения, приравнять произведения к единице.
5. Упростить формулу.

6. Проанализировать полученный результат или составить таблицу истинности, найти по таблице значения переменных, для которых значения функции равно 1.
7. Записать ответ.

Из-за отсутствия документов наряд милиции задержал трех студентов разных вузов: *Рината, Сергея* и *Павла*. На допросе каждый них показал следующее:

Ринат: Я учусь в КРСУ, а *Сергей* – в КНУ;

Сергей: Я учусь в КРСУ, а *Ринат* – в КГУСТА;

*Павел***:** Я учусь в КРСУ, а *Ринат* **–** в КНУ.

В ответах каждого из них *одно утверждение истинно,* а другое – *нет.* Поэтому в милиции легко определили, кто и где учится. Как это было установлено?

Решение:

Обозначим через *РС* студента, чье имя начинается с буквы *Р,* а *С* – первая буква названия института, в котором он учится. К примеру, утверждение «Ринат учится в КРСУ (Славянский) запишется как *РС***,** Сергей учится в КРСУ (Славянский) – *СС,* Павел учится в КРСУ (Славянский) – *ПС.*

Так как в показаниях студентов одно утверждение верно, а другое – нет, то, по условию задачи, можно составить следующие истинные дизъюнкции:

РС V СН = 1

СС V РА = 1

ПС V РН = 1

Тогда будет истинной и конъюнкция этих высказываний:

$$(РС \vee СН) \,\&\, (СС \vee РА) \,\&\, (ПС \vee РН) = 1$$

Используем *законы идемпотентности (равносильности)* **(**Приложение 1).

$$A \vee A = A \quad A \,\&\, A = A$$

Конъюнкция одинаковых «сомножителей» равносильна одному из них. Дизъюнкция одинаковых «слагаемых» равносильна одному.

Для первых двух скобок:

(РС V СН) & (СС V РА) = (РС & СС) V (РС & РА) V (СН & СС) V (СН & РА) = 0 V 0 V 0 V (СН & РА) = СН & РА

Так как все студенты из разных вузов, и каждый студент не может одновременно учиться в двух вузах, получается такая формула.

А теперь полученный результат, используем с третьей скобкой

(СН & РА) & (ПС V РН) = (СН & ПС) V (СН & РН) V (РА & ПС) V (РА & РН) = (СН &ПС) V 0 V (РА & ПС) V 0 = (СН & ПС) V (РА & ПС) = (СН & РА) & ПС= СН & РА & ПС

Так по конъюнкции *СН & РА & ПС = 1,* Сергей учится в Национальном, Ринат – в Архитектурном, Павел – в Славянском.

Задания для самостоятельного решения

1. Постройте таблицу истинности логических выражений (таблица 11):

Таблица 11 – Логические выражения

Задание 1	Задание 2
NOT (a OR b) AND (NOT a OR b)	NOT(a OR NOT c)
NOT (a AND NOT b)	(NOT a AND b) AND d
NOT (a AND b OR c)	NOT (a OR b) OR c
NOT (a AND b AND c)	(NOT a OR NOT b)
C AND (NOT a OR b)	NOT (a AND b) OR (a AND b)
(a AND b) OR (NOT a AND NOT b)	(NOT a AND NOT b)
NOT (a AND NOT b)	(a OR NOT b) OR NOT c
NOT(a OR NOT b)	NOT (a OR b) OR d
NOT (a AND b) OR c	(a OR NOT b) OR c
NOT (NOT a OR NOT b)	NOT (a AND b) AND d

2. Проверьте правильность рассуждений.

2.1. Проверить правильность суждений средствами *логики суждений*: «Если человек осужден судом, то он лишается избирательных прав. Если человек признан невменяемым, то он также лишается избирательных прав. Следовательно, если человек обладает избирательным правом, то он здоров и не был осужден судом».

2.2. Проверить правильность суждений средствами *логики суждений*: «*Иванов* утверждает, что не встречал этой ночью *Сидорова*. Если *Иванов* не встречал *Сидорова* этой ночью *Сидорова***,** то либо *Сидоров* был убийцей, либо *Иванов* лжет. Если *Сидоров* не был убийцей, то *Иванов* не встречал его этой ночью, а убийство было совершено после полуночи. Если убийство было совершено после полуночи, то либо *Сидоров* был убийцей, либо *Иванов* лжет. Следовательно, убийцей был *Сидоров*».

2.3. Проверить правильность суждений средствами *логики суждений*: «Если бы он не пошел в кино, то он не получил бы двойки. Если бы он подготовил домашнее задание, то не пошел бы в кино. Он получил двойку. Значит, он не подготовил домашнее задание».

2.4. Проверить правильность рассуждения «Для того, чтобы сдать экзамен, мне необходимо достать учебник или конспект лекций. Я достану конспект лекций только в том случае, если мой приятель не уедет. Мой приятель уедет, только если я сдам экзамен. Следовательно, я сдам экзамен»

2.5. Выяснить, кто из четверых виновен на основе информации: «*Петров* виновен, только если виновен *Иванов*. Неверно, что виновность *Сидорова* влечет виновность *Родионова* и что *Иванов* виновен, а *Сидоров* нет».

2.6. *Петров, Иванов* и *Сидоров* сдавали экзамен по математике. Если *Петров* не сдал экзамен на «отлично», то и *Иванов* не сдал на «отлично». *Сидоров* и еще один из друзей сдали экзамен на «отлично». Следует ли отсюда, что не верно, что *Петров* сдал экзамен не на «отлично», а *Иванов* – на «отлично»?

2.7. На складе совершено хищение. Подозрение пало на трех человек: *a, b* и *c,* они были доставлены для допроса. Установлено следующее:

- Никто, кроме *a, b, c,* не был замешан в деле;
- *a* никогда не ходит на дело без, по крайне мере, одного соучастника;
- *c* не виновен.

Виновен ли *b*?

2.8. Разбирается дело *Иванова, Петрова* и *Сидорова*. Один из них совершил преступление. В процессе расследования каждый из них сделал два заявления.

Иванов: Я не делал этого. *Петров* не делал этого.

Петров: Сидоров сделал это. *Иванов* не делал этого.

Сидоров: Я не делал это. *Иванов* сделал это.

Далее было установлено, что один из них дважды солгал, другой дважды сказал правду, а третий раз солгал, раз сказал правду.

Кто совершил преступление? Каков будет ответ при условии, что каждый из них один раз сказал правду, а один раз солгал?

2.9. В деле об убийстве имеются двое подозреваемых – *Иванов* и *Петров.* Допросили четырех свидетелей, которые дали такие показания: «*Иванов* не виноват», «*Петров* не виноват», «Из двух первых показаний, по меньшей мере, одно истинно», «Показания третьего ложны». Четвертый свидетель оказался прав. Кто виновен?

2.10. По подозрению в совершенном преступлении задержали *Иванова*, *Петрова* и *Сидорова*. Один из них был уважаемым в городе стариком, другой малоизвестным чиновником, третий – известным мошенником. В процессе следствия старик говорил правду, мошенник лгал, а третий задержанный в одном случае говорил правду, а в другом – ложь. Вот, что они утверждали:

Иванов: Я совершил это. *Петров* не виноват.

Петров: Иванов не виноват. Преступление совершил *Сидоров.*

Сидоров: Я не виноват. Виноват *Иванов***.**

Требуется определить фамилии старика, мошенника и чиновника, и кто из них виноват, если известно, что преступник только один.

Вопросы для самоподготовки

1. Логика как наука. Что изучает логика.
2. Что является предметом математической логики.
3. Основные формы мышления.
4. Высказывания, простые и сложные. Алгебра высказываний.
5. Алгебра логики. Базовые логические операции.

6. Логические выражения и таблицы истинности.
7. Логические связки.
8. Логические законы.
9. Правила преобразования логических операций.
10. Тавтология, силлогизм, контрапозиция.

Темы рефератов

1. «Жизнь» и деятельность Николы Бурбаки.
2. Аксиоматический метод со времен античности до работ Д. Гильберта.
3. Великая теорема Ферма от П. Ферма до А. Уайлса.
4. Игра в кости и другие азартные игры в развитии теории вероятности.
5. Интегрированные и дифференциальные методы древних.
6. Интуиция и логика в математике.
7. История нуля.
8. История числа π.
9. Математика Древнего Вавилона.
10. Математика Древнего Египта.

Список литературы

1. *Агарева О.Ю.* Математическая логика и теория алгоритмов: учеб. пособ. / О.Ю. Агарева, Ю.В. Селиванов. М: МАТИ, 2011. 80 с.
2. *Арбузов П.В., Герасименко В.Н., Гуде С.В., Медянцев Д.В.* Высшая математика для юристов: учеб. пособ. / Кафедра информационного обеспечения ОВД РЮИ МВД России. Феникс, 2007. 443 с.
3. *Ломиворотов М.М.* Логика для юристов: учеб. пособ. в схемах и упражнениях. Волгоград: ВолгГТУ, 2006. 32 с.
4. Математические методы в юриспруденции. http://posobiemii.narod.ru/HTML.html
5. *Моисеев С.И.* Математика для юриста: учеб. пособ. Воронеж: Московская академия экономики и права, Воронежский филиал, 2006. 80 с.

6. *Шевелев Ю.П.* Дискретная математика. Теория множеств. Булева алгебра (Автоматизированная технология обучения «Символ»): учеб. пособ. Томск: Томский гос. ун-т систем управления и радиоэлектроники, 2003. 118 с.

ГЛАВА 3.
ТЕОРИЯ МНОЖЕСТВ

3.1. Понятие множества

Под множеством понимается любое собрание определенных и различных между собой объектов, мыслимое как единое целое. Часто приходится говорить о нескольких вещах, объединенных некоторым общим признаком. Можно сказать, что множество – это совокупность, система, класс, ансамбль, собрание, коллекция и т.д. Однако все это не математические определения. Так, можно говорить о множестве предметов, находящихся на столе, множестве студентов, присутствующих в данный момент в аудитории, множестве звезд, наблюдаемых на небе, множестве всех точек, равноудаленных от данной, множестве всех клеток человеческого организма и т.д. Человеческому мышлению свойственно трактовать то или иное собрание предметов, родственных по какому-либо признаку, как самостоятельный объект. Совокупность кофейника, молочника, сахарницы, шести чашек и блюдец мы называем сервизом. Буквы *А, Б, В, Г, Д* и т.д. объединяем в алфавит. Не случайно каждую из этих совокупностей мы называем существительным в единственном числе: сервиз, алфавит – идея объединения проглядывает даже в такой мелочи.

Основное и самое существенное в понятии множества – это акт *объединения различных объектов в одно целое.*

Основатель теории множеств – немецкий математик и философ Георг Кантор (1845–1918) писал: «Под многообразием или множеством я понимаю вообще всякое многое, которое можно мыслить как единое, т.е. всякую совокупность определенных элементов, которая может быть связана в одно целое с помощью некоторого закона». Перефразируя Кантора можно сказать, что множество – любая совокупность определенных и различимых между собой объектов, рассматриваемых как единое целое. Природа таких объектов может быть совершенно любой. Это могут быть числа, функции, книги, молекулы, высказывания, сами множества. Соединенные Штаты Америки – множество из *50* элементов – штатов, в каждом из которых, в свою очередь, есть множество округов. Объекты множества могут даже и не существовать реально. Трактовка слова «множество» в обыденном языке отличается от математического определения, так как подразумевает некоторое изобилие. В математике этот термин такого свойства совсем не имеет. Множество может состоять из двух элементов (например, множество естественных спутников Марса – Фобос и Деймос), может состоять из одного элемента (множество естественных спутников Земли – Луна), может вообще не иметь элементов.

Существенными в понятии множества являются следующие признаки:

- Объекты, входящие во множество, определенные. Это означает, что для каждого объекта можно однозначно сказать, принадлежит ли он данному множеству или нет.
- Объекты, входящие во множество, различимы между собой. Следовательно, во множестве не может быть двух или более одинаковых объектов.
- Все объекты, входящие во множество, мыслятся как единое целое. Этим подчеркивается, что все объекты рассматриваются в совокупности, а от свойств отдельных объектов абстрагируются.

Слова «совокупность определенных элементов, которая может быть связана в одно целое с помощью некоторого закона» позволяют сказать, что множество определяется либо своими элементами, либо законом (характеристическим признаком), согласно которому происходит объединение различных объектов в одно целое. Поэтому можно сказать, что основным понятием теории множеств будет являться отношение принадлежности отдельных объектов к совокупности.

Множества обычно обозначают прописными курсивными буквами латинского алфавита: *A, B, C* и т.д. Для наиболее важных числовых множеств приняты постоянные обозначения. Множество натуральных чисел стандартно обозначается буквой *N,* множество целых чисел – *C,* множество действительных чисел – буквой *R.* Эти множества широко используются в школьном курсе математики.

Объекты, составляющие данное множество, называют его элементами и обозначают строчными курсивными буквами латинского алфавита: *a, x, y.* Для того, чтобы указать, что *x* – элемент множества *A,* записывают $x \in A$ (читается: «*x* принадлежит *A*»). Например, если *A* – множество дней недели, а *x* – понедельник, то $x \in A$. Чтобы указать, что x не является элементом множества *A*, записывают $x \notin A$ («*x* не принадлежит *A*»). В нашем примере, если x – ноябрь, то $x \notin A$.

Из канторовского понятия множества следует, что задать множество можно двумя способами. *Первый способ* – явный или перечислительный – состоит в простом перечислении всех элементов, в совокупности составляющих данное множество. Элементы множества заключаются в фигурные скобки { }, которые показывают, что элементы объединены в одно целое, в совокупность.. Если *A* – множество дней недели, то записывают *A* = {понедельник, вторник, среда, четверг, пятница, суббота, воскресенье}, множество арифметических действий В задают так: *B* = {сложение, вычитание, умножение, деление}, множество корней квадратного уравнения: $x^2 - 5x + 6 = 0$, $X : X = \{2, 3\}$.

Согласно определению, во множестве не бывает одинаковых элементов. Поэтому запись {*2, 2, 3*} считается некорректной. Ее необходимо заменить на следующую {*2, 3*}. Порядок следования элементов во множестве роли не играет. Поскольку {*2, 3, 4*} и {*4, 3, 2*} состоят из одних и тех же элементов, они задают одно и то же множество.

В тех случаях, когда множество содержит много элементов, такой способ оказывается неудобным. Кроме того, при таком задании множества остается замаскированным сам принцип его образования.

Второй способ задания состоит в том, что мы указываем условие, по которому выбираем эти и только эти элементы во множество, признак, характеризующий все элементы множества. Такой способ называется описательным. В этом случае для задания множества X с элементами x применяется следующая запись: $X = \{x \mid признак\}$. Например, $X = \{x \mid x^2 - 5x + 6 = 0\}$, A = {*a* | *a* – день недели}, *B* = {*b* | *b* – арифметическое действие}. Описательный способ задания множества напрямую связан с алгеброй высказываний, так как записываемый признак и есть высказывание, касающееся элементов рассматриваемого множества.

Задание множества описательным способом иногда приводит к некоторым осложнениям. Может получиться, что два различных способа задания задают одно и тоже множество. Большие трудности при задании множеств возникают из-за недостаточной точности описания характеризующего признака вследствие неоднозначности человеческой речи. Например, задавая множество всех деревьев на земном шаре, нужно сказать, идет ли речь о деревьях, которые существовали, и будут существовать на Земле или о деревьях, существующих с некоторой определенной даты. Кроме того, существует ряд промежуточных форм между деревьями и кустарниками и нужно четко определить, какие из них относятся к рассматриваемому множеству.

Даже множество планет Солнечной системы определено не вполне однозначно. Наряду с большими планетами существуют также около *1600* малых (астероидов), поперечник которых доходит всего до *1 км*. По мере улучшения методов наблюдений, открываются все более и более мелкие. И возникает вопрос, где заканчиваются планеты, а начинаются метеориты.

Существуют случаи, когда задание множества обладает внутренними противоречиями. Например, парадокс брадобрея. Генерал призвал брадобрея и приказал брить всех солдат, за исключением тех, кто бреется самостоятельно. Брадобрей без забот проработал один день. Утром следующего дня у него возникла проблема: он не смог выполнить приказ генерала. Ощупав утром своё лицо, он взялся за бритву, и вдруг он понял, что не имеет права побриться, ведь ему приказано брить только тех, кто не

бреется сам. С другой стороны, если он не будет бриться сам, то он обязан побрить себя. Подскажите, как ему выполнить приказ? Брадобрей – не солдат. Но есть и другая версия парадокса. Прилагательное русского языка назовем рефлексивным, если оно обладает тем свойством, которое определяет. Например, прилагательное «русский» – рефлексивное, а прилагательное «английский» – нерефлексивное. Прилагательное «трехсложный» – рефлексивное (состоит из трех слогов). А прилагательное «четырехсложный» – нерефлексивное (состоит из пяти слогов). Интересно: а прилагательное «трудновыговариваемое» рефлексивно или нет? Следовательно, все прилагательные можно разделить на два множества: рефлексивные и нерефлексивные прилагательные. Но рассмотрим само прилагательное «нерефлексивный». Оно рефлексивное или нет? Изучение вопроса, при каких случаях это может произойти, привело к глубоким исследованиям в области логики, полностью изменившим эту науку. Неразумно рассматривать множество идей, множество капель воды в стакане и т.п. Так как само понятие множества не является достаточно четким, нельзя рассматривать также и множество всех множеств (это приводит к противоречию).

Численность множества – число элементов в данном множестве. Обозначается так: n. Записывается так: $n(M) = 4$.

Множества бывают:

1. Конечные множества – состоят из конечного числа элементов, когда можно пересчитать все элементы множества.
2. Бесконечные множества – когда невозможно пересчитать все элементы множества.
3. Пустые множества – множества, не содержащие элементов и обозначающиеся Ø. Записывают так: $n(A) = 0$; $A = Ø$. Пустое множество является подмножеством любого множества.

Виды множеств:

1. Дискретные множества (прерывные) – имеют отдельные элементы. Распознаются путём счёта.
2. Непрерывные множества – нет отдельных элементов. Распознаются путём измерения.

3. Конечные множества – состоят из конечного числа элементов, когда можно пересчитать все элементы множества.
4. Бесконечные множества – когда невозможно пересчитать все элементы множества.
5. Упорядоченные множества. Элемент из множества предшествует или следует за другим. Например, множество натуральных чисел, расположенных в виде натурального ряда.
6. Непорядочные множества. Любое непорядочное множество можно упорядочить.

Способы задания множеств:

1. Перечислением элементов (подходит для конечных множеств). Указать характеристическое свойство множества, т.е. то свойство, которым обладают все элементы данного множества.
2. С помощью изображения: на луче, в виде графика.
3. С помощью кругов Эйлера. В основном используется при выполнении действий с множествами или демонстрации их отношений.

Подмножества. Если любой элемент множества В принадлежит множеству А, то множество В называется подмножеством множества А. ⊂ – Знак включения. Запись $B \subset A$ означает, что множество B является подмножеством множества A.

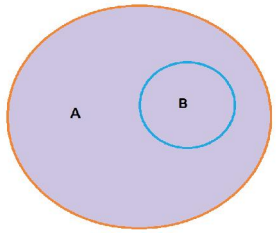


Рисунок 1 – Подмножество B

Виды подмножеств:

Собственное подмножество. Множество B называется собственным подмножеством (рисунок 1) множества A, если выполняются условия: $B \neq Ø$, $B \neq A$.

Не собственные подмножества. Множество B называется не собственным подмножеством множества A, если выполняются условия: $B \neq \varnothing$, $B = A$. Пустое множество является подмножеством любого множества. Любое множество является подмножеством самого себя.

Равенство множеств. Множества равны (рисунок 2), если они состоят из одних и тех же элементов. Два множества являются равными, если каждый из них является подмножеством другого. В этом случае пишут: $A = B$.

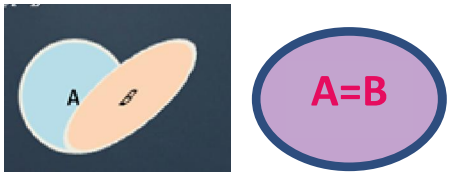


Рисунок 2 – Равенство множеств

3.2. Операции над множествами

Объединением двух множеств A и B называется множество (рисунок 3), элементами которого являются элементы, входящие в хотя бы в одно из данных множеств.

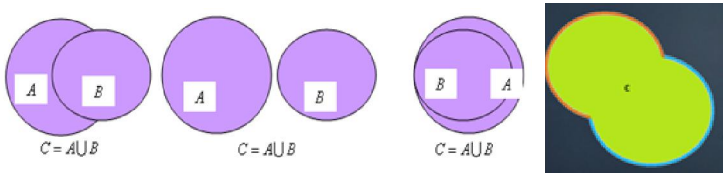


Рисунок 3 – Объединение множеств

Пересечением двух множеств A и B называется множество (рисунок 4), элементами которого являются элементы, входящие в каждое из этих множеств

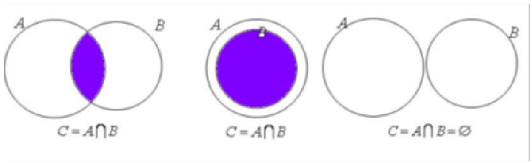
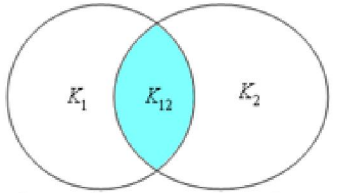


Рисунок 4 – Пересечение множеств

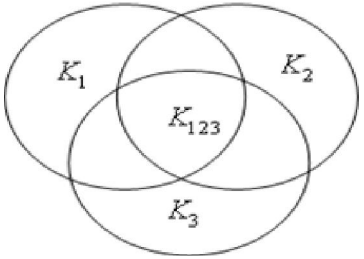
Формула сложения. Если два множества состоят из конечного числа элементов, то, как видно на рисунке 5, число элементов, входящих в их объединение, выражается формулой.



$$n(K_1 \cup K_2) = n(K_1) + n(K_2) - n(K_1 \cap K_2)$$

Рисунок 5 – Сложение двух множеств

Если же свойств три, то можно по аналогии определить множества (Рисунок 6).



$$K_{12} = K_1 \cap K_2,\ K_{23} = K_2 \cap K_3,\ K_{31} = K_3 \cap K_1$$

$$n(K_1 \cup K_2 \cup K_3) = n(K_1) + n(K_2) + n(K_3) - n(K_{12}) - n(K_{23}) - n(K_{31}) + n(K_{123})$$

Рисунок 6 – Сложение трех множеств

Разность множеств. Разностью множеств A и B (рисунок 7) называется множество всех объектов, являющихся элементами множества A и не принадлежащих множеству B. «\» – знак разности, соответствует предлогу «без». Разность множеств A и B записывается так: $A \setminus B$.

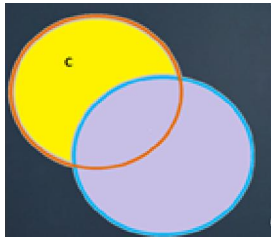


Рисунок 7 – Разность множеств

Дополнение множеств. Множество элементов множества B, не принадлежащих множеству A, называется дополнением множества A до множества B (рисунок 8). Часто множества являются подмножествами некоторого основного, или универсального множества U. Дополнение обозначается $\bar{A}$.

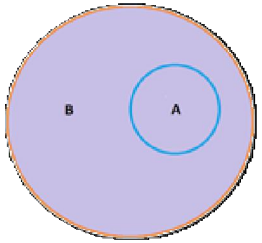
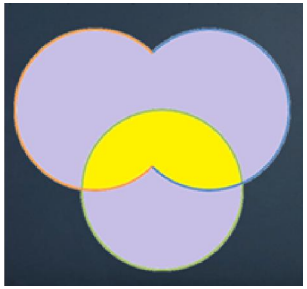
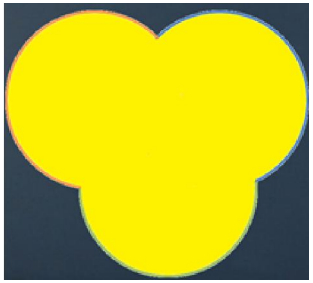


Рисунок 8 – Дополнения множеств

Пересечение и объединение множеств обладают следующими свойствами: *коммутативность, ассоциативность, дистрибутивность* (рисунки 9, 10, 11)**.**

Ассоциативность (рисунок 9)

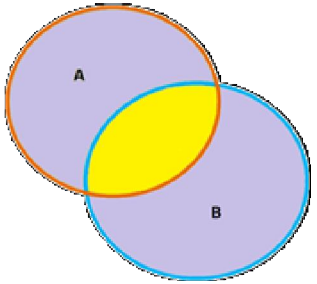


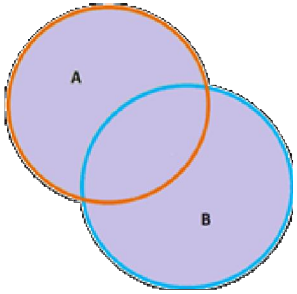


$(A \cap B) \cap C = A \cap (B \cap C)$ $(A \cup B) \cup C = A \cup (B \cup C)$

Рисунок 9 – Ассоциативность

Коммутативность (рисунок 10)

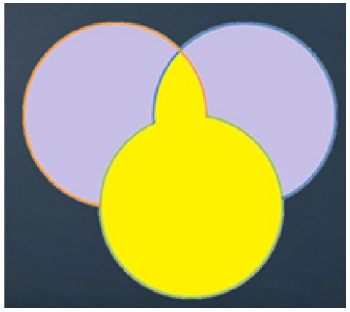


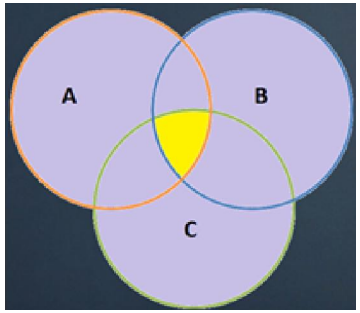


$A \cap B = B \cap A$ $A \cup B = B \cup A$

Рисунок 10 – коммутативность

Дистрибутивность (рисунок 11)





$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ $(A \cup B) \cup C = A \cup (B \cup C)$

Рисунок 11 – Дистрибутивность

Отношения множеств. В теории множеств рассматриваются следующие отношения между множествами:

1. Тождественность. Если каждый элемент множества *A* является также и элементом множества *B*, и каждый элемент множества *B* есть также элемент множества *A*, то эти множества тождественны. Обозначается так: *A = B.*

2. Эквивалентность. Соответствие между элементами множеств *A* и *B*, при котором каждому элементу множества *A* соответствует единственный элемент множества *B*, и, наоборот, различным элементам одного множества соответствуют различные элементы другого множества, называется взаимно однозначными. Если существует, по крайней мере, одно взаимно однозначное соответствие между элементами множеств *A* и *B*, то такие множества называются эквивалентными.

Свойства эквивалентности: Отношение эквивалентности обладает следующими свойствами:

1. Симметричность (взаимность). Если множество *A* эквивалентно множеству *B*, то множество *B* эквивалентно множеству *A*. *A~B, B~A.*

2. Транзитивность (переходность). Если множество *A* эквивалентно множеству *B,* а множество *B* эквивалентно множеству *C*, то множества *A* и *C* эквивалентны. *A~B, B~C, A~ C.*

3. Рефлексивность (возвратность). Всякое множество эквивалентно самому себе. *A~A.*

Использование отношения эквивалентности позволяет разбить всевозможные множества на классы эквивалентных между собой множеств.

Приведем несколько примеров решения задач с применением тории множеств:

Пример 1. Если *A = {1, 2, 3, 4, 5}*, а *B = {2, 4, 6, 7}*, *то* $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$. Если *A* – множество отличников группы, а *B* – множество ударников, то $A \cup B$ составляет множество и отличников, и ударников. Если *A* – множество отличников группы, а *B* – все множество студентов группы, то элементами $A \cup B$ являются все студенты группы.

Пример 2. Если *A* – множество успевающих студентов группы, *B* – множество юношей, а *C* – множество неуспевающих девушек, то $A \cup B \cup C$ – множество всех студентов группы.

Из определения операции объединения следует, что она обладает многими теми же свойствами, что и операция сложения чисел:

$A \cup B = B \cup A$ – коммутативность (переместительность);

$(A \cup B) \cup C = A \cup (B \cup C)$ – ассоциативность (сочетательность).

Пример 3. В *Ю1-14* группе – *29* студентов. Каждый из них изучает или английский, или немецкий язык. *5* студентов изучают и английский, и немецкий одновременно. Сколько студентов занимается в английской группе, если в немецкой – *12* студентов?

Обозначим через *A* множество студентов, изучающих английский язык, а через *B* – немецкий язык. Количество студентов в немецкой группе – $N(B) = 12$. Множество студентов, изучающих одновременно и английский, и немецкий – $A \cap B$. $N(A \cap B) = 5$. Всего студентов $N(A \cup B) = 29$. Значит количество студентов в английской группе по формуле включений и исключений ($N(A \cup B) = N(A) + N(B) - N(A \cap B)$) можно найти так:

$N(A) = N(A \cup B) - N(B) + N(A \cap B) = 29 - 12 + 5 = 22.$

Пример 4. Льюис Керрол. В одной из повестей Льюиса Керрола – автора «Алисы в стране чудес», «Алисы в зазеркалье»

и др. – есть такая задача: «В ожесточенном бою 70 из 100 пиратов потеряли один глаз, 75 – одно ухо, 80 – одну руку и 85 одну ногу. Каково минимальное количество потерявших одновременно глаз, ухо, руку и ногу?».

Обозначим через A – множество пиратов, потерявших один глаз, через B – одно ухо, через C – одну руку, через D – одну ногу. Тогда множество потерявших и глаз, и ухо, и руку, и ногу одновременно – $A \cap B \cap C \cap D$. Универсальное множество I можно представить в виде: $I = \overline{(A \cap B \cap C \cap D)} \cup (A \cap B \cap C \cap D)$. По закону Моргана = $\overline{A \cap B \cap C \cap D} = \overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{D}$.

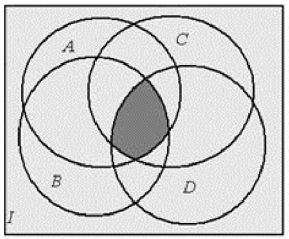


Рисунок 12 – Множества I, A ∩ B ∩ C ∩ D

На рисунке 12 множество A ∩ B ∩ C ∩ D выделено на диаграмме темно-серым цветом, множество $\overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{D}$ – светло-серым.

Так как множества $\overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{D}$ и $A \cap B \cap C \cap D$ не пересекаются, то $N(I) = N(\overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{D}) + N(A \cap B \cap C \cap D)$. Множества $\overline{A}\ \overline{B}\ \overline{C}\ \overline{D}$ могут попарно пересекаться. Значит $N(\overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{D}) <= N(\overline{A}) + N(\overline{B}) + N(\overline{C}) + N(\overline{D})$. $N(\overline{A}) = N(I) - N(A) = 100 - 70 = 30$, $N(\overline{B}) = N(I) - N(B) = 100 - 75 = 25$, $N(\overline{C}) = N(I) - N(C) = 100 - 80 = 20$, $N(\overline{D}) = N(I) - N(D) = 100 - 85 = 15$. Таким образом, $N(I) <= N(\overline{A}) + N(\overline{B}) + N(\overline{C}) + N(\overline{D}) + N(A \cap B \cap C \cap D)$, а $N(A \cap B \cap C \cap D) >= N(I) - N(\overline{A}) - N(\overline{B}) - N(\overline{C}) - N(\overline{D}) = 100 - 30 - 25 - 20 - 15 = 10$.

Итак, $N(A \cap B \cap C \cap D) >= 10$, т.е. не менее 10 пиратов одновременно лишились и глаза, и уха, и руки, и ноги.

Задания для самостоятельной работы

В группе *K* человек. Из них *16* играют в баскетбол, *17* – в хоккей, *18* – в футбол. Увлекаются двумя видами спорта: баскетболом и хоккеем – четверо, баскетболом и футболом – трое, футболом и хоккеем – пятеро. Трое не увлекаются ни баскетболом, ни хоккеем, ни футболом. Сколько студентов увлекается одновременно тремя видами спорта? Сколько студентов увлекается лишь одним из этих видов спорта

2. В юридической фирме *K1 (*количество) юристов являются специалистами по гражданскому праву, *K2* – по уголовному, *K3* – по административному. Кроме того, *K4* сотрудника являются специалистами по гражданскому и уголовному, *K5* – по уголовному и административному, *K6* – по гражданскому и административному, а *K7* сотрудников являются специалистами во всех трех правах. Сколько сотрудников работает в фирме?

3. Среди математиков каждый *седьмой* – философ, а среди философов каждый *девятый* – математик. Кого больше: философов или математиков? Рассмотрите людей, являющихся математиками и философами одновременно.

4. Даны *1985 множеств*, каждое из которых состоит из *45* элементов, причём объединение любых двух множеств содержит ровно *89* элементов. Сколько элементов содержит объединение всех этих *1985* множеств?

5. 30 студентов одной группы решили побывать друг у друга в гостях. Известно, что студент за вечер может сделать несколько посещений, и что в тот вечер, когда к нему кто-нибудь должен прийти, он сам никуда не уходит. Покажите, что для того, чтобы все побывали в гостях у всех, а) четырёх вечеров недостаточно; б) пяти вечеров также недостаточно; в) десяти вечеров достаточно; г) и даже семи вечеров тоже достаточно.

6. Из *45* курсантов академии МВД *25* – юноши. *30* курсантов учатся на «*4*» и «*5*». *28* – занимаются спортом, из них *18* юношей и *17* ударников. *15* юношей учатся на «*4*» и «*5*» и занимаются спортом. Сколько юношей при этом могут быть ударниками?

7. В двух группах учатся *50* студентов. Для прибытия в институт *12* из них пользуются автобусом, *18* добираются пешком,

7 и идут, и едут в автобусе. Используя теорию множеств, найдите: Сколько человек или добираются пешком или пользуются автобусом? Сколько человек пользуется только автобусом? Сколько человек пользуется другим транспортом?

8. На первом курсе академии МВД в одной группе учатся *40* курсантов. Из них по теории государства и права имеют тройки *19* человек, по информатике и математике – *17* человек и по физкультуре – *22* человека. Только по одному предмету имеют тройки: по теории государства и права – *4* человека, по информатике и математике – *4* человека и по физкультуре – *11* человек. *7* человек имеют тройки и по информатике и математике, и по физкультуре, из них *5* имеют тройки и по теории государства и права. Сколько человек учится без троек? Сколько человек имеют тройки по двум из трех дисциплин?

9. Первая рота первого курса состоит из *70* курсантов. Из них *27* занимаются в драмкружке, *32* поют в хоре, *22* увлекаются спортом. В драмкружке – *10* курсантов из хора, в хоре – *6* спортсменов, в драмкружке – *8* спортсменов; *3* спортсмена посещают и драмкружок и хор. Найти: Сколько курсантов не поют в хоре, не увлекаются спортом и не занимаются в драмкружке? Сколько человек, занимающихся в драмкружке и в хоре, не занимаются спортом? Сколько спортсменов драмкружка не поют в хоре? Сколько поющих спортсменов, не посещающих драмкружок? Сколько спортсменов посещают хор или драмкружок? Сколько увлекаются только спортом?

Вопросы для самоподготовки

1. Понятие множества.
2. Численность множества.
3. Виды множеств.
4. Способы задания множеств.
5. Подмножества.
6. Равенство множеств.
7. Объединение множеств.
8. Пересечение множеств.
9. Формула сложения.

10. Разность множеств.
11. Дополнение множеств.
12. Свойства множеств: ассоциативность, коммутативность, дистрибутивность.
13. Отношения множеств: тождественность, эквивалентность.
14. Свойства эквивалентности.

Темы рефератов

1. Математика народа Майя.
2. Философия и математика Кантора.
3. Математические методы в юриспруденции.
4. Математическое обоснование решений.
5. Основы математического моделирования.
6. Имитационное моделирование (ситуационное моделирование).
7. Классификация математических моделей.
8. Математическое образование в юриспруденции.
9. Создание математического, специального языка юридической науки.
10. Математические методы, используемые в юридических науках.

Список литературы

1. *Арбузов П.В., Герасименко В.Н., Гуде С.В., Медянцев Д.В.* Высшая математика для юристов: учеб. пособ. / Кафедра информационного обеспечения ОВД РЮИ МВД России. Феникс, 2007. 443 с.
2. *Блувштейн Ю.Д.* Изучение причин преступности методом распознавания образов: учеб. пособ. М.: Правовая кибернетика, 1973. 120 с.
3. *Блувштейн Ю.Д.* Криминология и математика: учеб. пособ. М., 1974. 154 с.
4. *Верещагин Н.К., Шень А.* Начала теории множеств: лекции по математической логике и теории алгоритмов. Часть 1. 4-е изд., доп. М.: МЦНМО, 2012. 112 с.

5. *Вицин С.Е.* Моделирование в криминологии: учеб. пособ. М., 1973. 105 с.
6. *Ли Д.А.* Преступность как социальное явление: учеб. пособ. М., 1997. 230 с.
7. *Лавров И.А., Максимова Л.Л.* Задачи по теории множеств, математической логике и теории алгоритмов: учеб. пособ. 5-е изд., испр. М.: ФИЗ-МАТЛИТ, 2004. 256 с.
8. *Шевелев Ю.П.* Дискретная математика. Теория множеств. Булева алгебра (Автоматизированная технология обучения «Символ»): учеб. пособ. Томск: Томский гос. ун-т систем управления и радиоэлектроники, 2003. 118 с.

ГЛАВА 4.
НАЧАЛО КОМБИНАТОРИКИ И ТЕОРИЯ ВЕРОЯТНОСТЕЙ

4.1. Элементы комбинаторики

Во всех вышеперечисленных испытаниях мы рассматривали появление одного объекта из некоторого конечного множества. При этом, число исходов испытания находилось достаточно просто. Однако, чаще всего, при вычислении вероятности какого-либо события необходимо уметь находить число комбинаций выбора нескольких объектов.

Область математики, в которой изучаются вопросы о том, сколько различных комбинаций, подчиненных тем или иным условиям, можно составить из заданных объектов, называется *комбинаторикой*. В комбинаторных задачах необходимо подсчитать, сколькими способами можно сделать тот или иной выбор, выполнить то или иное требование, выполнить какое-либо условие.

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. Основы теоретических положений комбинаторики были разработаны французскими учеными Блезом Паскалем и Пьером Ферма в XVII веке.

Дальнейшее развитие комбинаторика получила в работах Я. Бернулли, Г. Лейбница и Л. Эйлера.

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

Большинство комбинаторных задач может быть решено с помощью двух основных правил: правила суммы и правила произведения.

Правило умножения: 4 мужчины и *4* женщины заводятся в *8* расположенных подряд допросные камеры, причем мужчины заводятся в камеры с четными номерами, а женщины – с нечетными номерами. Сколькими способами это можно сделать?

Решение: Первого мужчину могут завести в любую из четырех четных камер, второго – в любую из оставшихся трех камер, третьего – в любую из оставшихся двух. Последнему мужчине предоставляется всего одна возможность. Согласно правилу умножения, мужчины могут занять четыре камеры *4 * 3 * 2 * 1 = 24* способами. Столько же возможностей имеют и женщины. Таким образом, согласно правилу умножения, мужчины и женщины могут занять комнаты – *24 * 24 = 576 способами.*

Правило сложения: Преступник может проникнуть в квартиру либо через входную дверь, либо через окно. Число способов проникновения через дверь – *4,* через окно – *3*. Сколько всего существует способов проникновения в квартиру?

Решение. Так как способы проникновения в квартиру через окно и через дверь различны, то мы можем воспользоваться правилом суммы. Тогда количество способов проникновения либо через окно, либо через дверь, т.е. количество различных способов проникновения в квартиру, будет равно *4 + 3 = 7*.

4.2. Теория вероятности

При изучении химии, биологии, математики, физики в средней школе в основном рассматривались такие явления и процессы, в которых можно было точно предсказать результат по заданным начальным условиям. Так, например, при нормальном атмосферном давлении *760 мм рт. ст.* температура кипения химически чистой воды равна *100 °С* ; дальность полета тела, брошенного с начальной скоростью v под углом а к горизонту, составляла $\frac{v^2}{g}\sin 2\alpha$. Однако, в реальной жизни, в обществе существует много явлений, в которых невозможно заранее предсказать результат при известных начальных условиях. Так, например, неизвестно заранее, попадет или нет снаряд в цель, выпущенный из орудия с известной начальной скоростью, если цель располагается достаточно далеко. Неизвестно, пойдет или не пойдет дождь завтра, если сегодня мы точно знаем состояние погоды. Неизвестно, состоится или нет дорожно-транспортное происшествие на определенном участке дороги. Неизвестно, сколько завтра произойдет преступлений в городе или в каком-то его районе, хотя все криминологические данные на сегодня известны. Неизвестно, сколько раз попадет в «десятку» спортсмен на соревнованиях из произведенных ста выстрелов.

На все эти вопросы невозможно дать точного ответа, поскольку процессы, описанные в них, лишены полной определенности. В этих явлениях необходимо учитывать не только основные факторы, но и множество второстепенных, приводящих к случайным возмущениям и искажениям результата. Мы знаем дальность полета тела, брошенного под углом к горизонту, однако при моделировании полета снаряда необходимо учитывать не только действие силы тяжести, но и силу сопротивления воздуха, воздействие на снаряд ветра, небольшие отклонения начальной скорости снаряда от заданной и т.д. Безопасность дорожного движения зависит не только от точного выполнения предписанных правил всеми его участниками, но и от огромного числа причин: погоды, состояния дорожного покрытия, освещенности, взаимного расположения автомобилей на дороге, психологического состояния водителей и пешеходов, технического состояния транспортных средств, опыта водителей и многих других. Такие явления называются *случайными*.

Элемент неопределенности, свойственный случайным явлениям и обусловленный второстепенными факторами, требует специальных методов их изучения. Разработкой таких методов, изучением специфических закономерностей, наблюдаемых в случайных явлениях, и занимается теория вероятностей.

Теория вероятностей – математическая наука, изучающая закономерности случайных явлений.

Теория вероятностей не может, да и не ставит задачу ответить на вопрос, произойдет или нет какое-то конкретное, уникальное случайное явление. 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.

Итак, *предметом изучения теории вероятностей* являются закономерности массовых однородных случайных событий. Знание этих закономерностей позволяет прогнозировать характеристики процессов и явлений, в которых присутствуют случайные события. Например, хотя нельзя определить, попадет или нет снаряд в конкретном выстреле в определенных условиях, можно предсказать, сколько снарядов попадут 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.

Первые работы, в которых зарождались основные понятия теории вероятностей, принадле¬жали Л. Пачоли («Сумма знаний

по арифметике, геометрии, отношениям и пропорциональности», 1487), Дж. Кардано (рукопись «Книга об игре в кости», датированная 1526 годом, но изданная лишь в 1563 году), Н. Тарталья («Общий трактат о мере и числе», 1556), Галилео Галилею (работа «О выходе очков при игре в кости», изданная в 1718 году), Х. Гюйгенсу (трактат «О расчетах в азартных играх», 1656). Становление теории вероятностей как математической науки относится к середине XVII века и связано с попытками создания *теории азартных игр*. Основателями науки о вероятностях считаются Б. Паскаль и П. Ферма, в переписке которых решена задача о разделе ставок двух и более игроков при неоконченной игре, состоящей из нескольких партий. На развитие теории вероятностей значительное влияние оказали исследования Дж. Граунта и В. Петти по демографии или, как говорили в то время, по политической арифметике. К концу XVII века накопились обширные сведения о случайных событиях, описание решений многих задач теории вероятностей. Однако классическое понятие вероятности было введено лишь в XVIII веке в трактате Я. Бернулли «Искусство предположений» (1713), хотя и в далеко несовершенной форме. В трактате Бернулли присутствуют классическая и статистическая концепции вероятности.

Дальнейшее развитие теории вероятностей связано с потребностями развития естествознания и общественной практики (теория ошибок наблюдений, задачи теории стрельбы, проблемы статистики народонаселения). Значительную роль в развитии методов теории вероятностей сыграли А. Муавр, П. Лаплас, К. Гаусс, С. Пуассон, и др. (XVII–XIX века), русские математики П.Л. Чебышев, А.М. Ляпунов и А.А. Марков (XIX – начало XX века). В данный период теория вероятностей становится стройной математической наукой. Значительный вклад в современное развитие этой науки был сделан такими математиками, как С.Н. Бернштейн, В.И. Романовский, АН. Колмогоров, А.Я. Хинчин, Ю.В. Линник, Б.В. Гнеденко, Н.В. Смирнов, Ю.В. Прохоров, Стьюдент (псевдоним В. Госсета), Р. Фишер, Э. Пирсон, Е. Нейман, А. Вальд и др.

В настоящее время математический аппарат теории вероятностей широко используется при изучении массовых явлений

в науке, технике, обществе, праве. Методы теории вероятностей играют важную роль при обработке статистических данных. Вот несколько примеров решения задач с применением законов комбинаторики и теории вероятности:

Пример 1. Во взводе 25 курсантов. Сколько существует способов назначения командира взвода и его заместителя?

Решение. Сначала выберем командира взвода. Число способов выбора равно 25, так как каждый курсант может быть назначен на эту должность. После этого остается 24 курсанта, каждый из которых, может быть назначен заместителем командира взвода. Т.е. число способов назначения заместителя командира – 24. По правилу произведения количество способов назначения пары курсантов на указанные должности *24 * 25 = 600*.

Пример 2. Из отделения в 5 курсантов необходимо назначить двоих для патрулирования территории института. Сколькими различными способами можно сделать такой выбор?

Решение. В задаче мы не можем применить правило произведения, найдя сначала число способов выбора 1-го курсанта – 5, а потом – второго – 4 и перемножив их, получив 20 различных нарядов. Причиной этого является то, что порядок выбора курсантов в наряд не имеет значения. Важен лишь состав наряда. Поэтому будем решать задачу следующим образом. Обозначим курсантов *a, b, c, d, e*. Из пяти курсантов составим всевозможные пары для несения службы в патруле:

ab, ac, ad, ae,
bc, bd, be,
cd, ce,
de.

Так как, к примеру, пара *ab* и *ba* идентичны, то всего получается 10 различных вариантов наряда.

Пример 3. Сколько различных нарядов, состоящих из 7 курсантов, можно составить из взвода численностью 20 курсантов?

Количество различных нарядов равно числу сочетаний из 20 по 7 – C_{20}^{7}. По формуле сочетаний получим

$$C_{20}^{7}=\frac{(20-7+1)\ldots\cdot 18\cdot 19\cdot 20}{7!}=\frac{14\cdot 15\cdot 16\cdot 17\cdot 18\cdot 19\cdot 20}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7}=\frac{16\cdot 17\cdot 18\cdot 19\cdot 20}{4\cdot 6}=77520$$

Итак, количество различных нарядов равно 77520.

Пример 4. Сколько существует различных цифровых номеров автомашин, цифры которых не повторяются?

Решение. Если цифры номера машины не повторяются, то количество комбинаций номеров равно числу размещений из *10* (общее количество цифр) по *3* (количество цифр в номере автомашины), т.е. равно

$$A_{10}^{3} = (10-3+1) \ldots \cdot 10 = 8 \cdot 9 \cdot 10 = 720$$

Пример 5. Сколько существует вариантов проведения собрания учебной группы, если количество выступающих на собрании – 4?

Решение. Так как на собрании должны выступить всего четверо ораторов, то число способов расположения их, в списке выступающих и, соответственно, число способов проведения собрания *равно числу перестановок из 4 элементов*

$$P_4 \cdot P_4 = 4! = 24$$

Пример 6. В случайном эксперименте игральный кубик бросают один раз. Найдите вероятность того, что выпадет четное число.

1, 2, 3, 4, 5, 6.

$$P(A) = \frac{3}{6} = 0,5$$

Пример 7. Следователь Интерпола опрашивает свидетелей по совершенному преступлению. По делу проходят: 4 свидетеля из Финляндии, 7 свидетелей из Дании, 9 свидетелей из Швеции и 5 – из Норвегии. Порядок, в котором допрашиваются свидетели, следователь определяет жребием. Найдите вероятность того, что свидетель, которого допросят последним, окажется из Швеции.

Решение.

$$P(A) = \frac{N(A)}{N}$$

Всего свидетелей: *N = 4 + 7 + 9 + 5 = 25, N = 25. A = {последний из Швеции}, N(A) = 9.*

$$P(A) = \frac{9}{25} = 0,36$$

Пример 8. В коробке *20* патронов: *8* – от пистолета Макарова, *7* – от ТТ (пистолет Токарева), остальные – от Баярда (Bayard). Порядок, в котором берутся патроны, определяется жребием. Найдите вероятность того, что первый патрон окажется от Баярда.

Решение: A = {первым будет патрон от Баярда}

N = 20

N(A) = 20 – 8 – 7 = 5

$$P(A) = \frac{N(A)}{N} = \frac{5}{20} = 0,25$$

Пример 9. В оружейном шкафу хранятся 6 пистолетов Макарова и 4 пистолета ТТ. Вероятность поражения мишени из пистолета Макарова – 0,7; из пистолета ТТ – 0,8. Какова вероятность поражения стрелком мишени из наугад взятого пистолета?

Решение.

A – вероятность поражения мишени наугад;

A_1 – вероятность попадания наугад первого пистолета;

A_2 – вероятность попадания наугад второго пистолета.

Вероятности попадания по условию равны *P(A1) = 0,6; P(A2) = 0,4.*

Условные вероятности наступления события поражения мишени:

P(A/B1) = 0,7; *P(A/B2) = 0,8.*

Вероятность поражения мишени наугад:

*P(A) = P(A1) * P(A/B1) + P(A2) * P(A/B2) = 0,6 * 0,7 + 0,4 * 0,8 = 0,42 + 0,32 = 0,74*

Пример 10. В первой коробке находятся *10* патронов, *4* из которых являются холостыми, во второй коробке – *15* патронов, из которых *3* холостых. Найти вероятность того, что взятый наудачу патрон будет холостым. Найти вероятность того, что патрон был взят из первой коробки, если он оказался холостым.

Решение. Событие *A* – то, что взятый наудачу патрон будет холостым – может наступить при условии появления двух гипотез:

- патрон берется из первой коробки (обозначим эту гипотезу через B_1);
- патрон берется из второй коробки (B_2).

Вероятность этих гипотез одинакова $P(B_1) = P(B_2) = \frac{1}{2}$.

Условная вероятность того, что из *первой* коробки будет извлечен холостой патрон, $P_{B_1}(A) = \frac{4}{10} = \frac{2}{5}$. Условная вероятность того, что холостой патрон будет извлечен из *второй* коробки $P_{B_2}(A) = \frac{3}{15} = \frac{1}{5}$.

Вероятность события *A* рассчитывается по *формуле полной вероятности*:

$$P(A) = P(B_1) * P_{B_1}(A) + (B_2) * P_{B_2}(A) = \frac{1}{2} \cdot \frac{2}{5} + \frac{1}{2} \cdot \frac{1}{5} = \frac{3}{10}.$$

Пример 11. Вероятность того, что телевизор имеет скрытые дефекты, равна *0,2*. На склад поступило *20* телевизоров. Какое событие вероятнее: что в этой партии имеется *два* телевизора со скрытыми дефектами или *три*?

Интересующее событие А – наличие скрытого дефекта. Всего телевизоров $n = 20$, вероятность скрытого дефекта $p = 0,2$. Соответственно, вероятность получить телевизор без скрытого дефекта равна $q = 1 - 0,2 = 0,8$.

Получаем стартовые условия для *схемы Бернулли*:

$n = 20; p = 0,2; q = 0,8$.

Найдем вероятность получить *два* «дефектных» телевизора ($k = 2$) и *три* ($k = 3$):

$$P_{20}(2) = C_{20}^2 p^2 q^{18} = \frac{20!}{2!18!} \cdot 0,2^2 \cdot 0,8^{18} \approx 0,137$$

$$P_{20}(3) = C_{20}^3 p^3 q^{17} = \frac{20!}{3!17!} \cdot 0,2^3 \cdot 0,8^{17} \approx 0,41$$

Очевидно, $P_{20}(3) > P_{20}(2)$, т.е. вероятность получить три телевизора со скрытыми дефектами больше вероятности получить только два таких телевизора.

Задания для самостоятельной работы

1. Имеется *K* задержанных. Для проведения расследования необходимо устроить парные очные встречи каждого с каждым. Сколько таких встреч нужно организовать?

2. В бригаде ОМОН число сотрудников *K*. Для выполнения задания их них нужно отобрать группу из *H* человек. Сколько таких групп можно создать?

3. Программа экзамена содержит *25* вопросов, из которых студент знает *N*. Преподаватель последовательно задает три вопроса. Найти вероятность того, что студент ответит на три вопроса *A, B, C*.

4. Студент подготовил к экзамену по ТГП *20* билетов из *25*. В каком случае шансы взять известный билет больше – когда студент пришел на экзамен первым или вторым? Предположим, что *5* мужчин из *100* и *25* женщин из *10 000* являются дальтониками. Наугад выбранное лицо страдает дальтонизмом. Какова вероятность, что это мужчина?

5. В первой папке содержится *10* дел, из них *8* по убийствам; во второй – *20* дел, из них *4* – по убийствам. Из каждой папки наудачу извлекли по одному делу, а затем из этих двух дел наудачу взяли одно дело. Найти вероятность того, что взято дело с убийством.

6. В пирамиде *пять* винтовок, *три* из которых снабжены оптическим прицелом. Вероятность того, что стрелок поразил мишень при выстреле из винтовки с оптическим прицелом, равна *0,95;* для винтовки без оптического прицела эта вероятность равна *0,7*. Найти вероятность того, что мишень будет поражена, если стрелок произведет один выстрел из наудачу взятой винтовки.

7. Стрелок производит два выстрела по мишени. Вероятность попадания при каждом выстреле *0,8*. Составить полную группу событий и найти их вероятности.

8. В оружейном шкафу хранятся *6* пистолетов Макарова и *4* пистолета ТТ. Вероятность поражения мишени из пистолета Макарова – *0,7*; из пистолета ТТ – *0,8*. Какова вероятность поражения стрелком мишени из наугад взятого пистолета?

9. Из *12* студентов необходимо отобрать по одному человеку для участия в конференциях по *ТГП, ИГП, МП, АФП*. Каждый студент участвует только в одной конференции. Сколькими способами можно это сделать?

10. Сколько существует *семизначных* телефонных номеров, в которых все цифры различны и первая цифра отличается от нуля?

Вопросы для самоподготовки

1. Элементы комбинаторики.
2. Правило умножения.
3. Правило сложения.
4. Сочетания, размещения, перестановки.
5. Случайные события. Операции над событиями.
6. Классическая формула вероятностей.
7. Теорема сложения вероятностей.
8. Теорема умножения вероятностей. Условная вероятность.
9. Формула полной вероятности. Формула Байеса.
10. Формула Бернулли.

Темы рефератов

1. Математическое творчество.
2. Основные определения теории игр. Правила игры, игроки, их стратегии и выигрыши.
3. Основные положения теории принятия решений.
4. Открытие логарифмов и проблемы совершенствования вычислительных средств в XVII–XIX веках.
5. Открытие неевклидовой геометрии и ее значение для развития математики и математического естествознания.
6. Петербургская школа П.Л. Чебышева и предельные теоремы теории вероятностей.
7. Применение системного подхода в социально-правовой сфере.
8. Рождение аналитической геометрии и ее роль в развитии математики в XVII веке.
9. Рождение математического анализа в трудах И. Ньютона и Г. Лейбница.
10. Теория игр в контексте математического обоснования принятия решений.
11. Управление – основа функционирования различных систем.
12. Христианство и математические науки.

Список литературы

1. *Арбузов П.В., Герасименко В.Н., Гуде С.В., Медянцев Д.В.* Высшая математика для юристов: учеб. пособ. Феникс: Кафедра информационного обеспечения ОВД РЮИ МВД России, 2007. 443 с.
2. *Гмурман В.Е.* Теория вероятностей и математическая статистика: учеб. пособ. для студ. вузов. 11-е изд., стер. М.: Высшая школа, 2005. 479 с.
3. Математика для юридических специальностей: учеб. пособ. для студ. вузов / Под ред. С.Я. Казанцева. М.: Академия, 2011. 217 с.
4. Математические методы в юриспруденции. http://posobiemii.narod.ru/HTML.html.
5. *Моисеев С.И.* Математика для юриста: учеб. пособ. Воронеж: Московская академия экономики и права, Воронежский филиал, 2006. 80 с.
6. *Романов В.Ф.* Основы дискретной математики. Методические указания к практическим занятиям. Владимир: Владимирский гос. ун-т, 2008. 40 с.

ГЛАВА 5.
МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

5.1. Криптография

Криптография – наука о защите информации от прочтения ее посторонними. *Криптология* – это раздел математики, изучающий математические основы криптографических методов. Защита информации достигается шифрованием, т.е. преобразованием, которые делают защищенные входные данные трудно раскрываемыми по входным данным без знания специальной ключевой информации – ключа. Под ключом понимается легко изменяе-

мая часть криптосистемы, хранящаяся в тайне и определяющая, какое шифрующее преобразование из возможных выполняется в данном случае.

Криптосистема – семейство выбираемых с помощью ключа обратимых преобразований, которые преобразуют защищаемый открытый текст в шифрограмму и обратно. По характеру использования ключа известные криптосистемы можно разделить на два типа: *симметричные* (одноключевые, с секретным ключом) и *несимметричные* (с открытым ключом).

Методы криптографии и криптоанализа до недавнего времени были не очень тесно связаны с математикой, но во все времена многие известные математики участвовали в расшифровке важных сообщений. Часто именно они добивались заметных успехов, ведь математики 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,* например, на различных перестановках букв, заменах букв с использованием ключевых слов и т.д.

5.1.1. Основные понятия криптографии

- *Криптография* – наука о методах шифрования информации с целью её защиты от незаконных пользователей.
- *Шифр* – метод преобразования информации с целью её защиты.

- *Шифрование* – процесс преобразования защищаемой информации в шифрованное сообщение с помощью определённых правил, содержащихся в шифре.
- *Открытый (исходный) текст* – данные (не обязательно текстовые), передаваемые без использования криптографии.
- *Шифрованный (закрытый) текст* – данные, полученные после применения криптосистемы с указанным ключом.
- *Криптосистема* – семейство обратимых преобразований открытого текста в шифрованный.
- *Ключ* – параметр шифра, определяющий выбор конкретного преобразования данного текста. В современных шифрах алгоритм шифрования известен и *криптографическая стойкость* шифра целиком определяется секретностью ключа (Принцип Керхгоффа).
- *Криптоанализ* – наука, изучающая математические методы нарушения конфиденциальности и целостности информации.
- *Криптология* – это наука, предметом которой являются *математические основания,* как криптографии, так и криптоанализа одновременно.
- *Криптоаналитической 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.

С древнейших времен основная задача шифрования была связана с сохранением тайны переписки. Сообщение, попадавшее в руки постороннему человеку, должно было быть непонятно ему, а посвященный человек мог без труда расшифровать послание. Приемов тайнописи великое множество. Невозможно описать все известные шифры. Наиболее простейшими из криптографи-

ческих шифров являются шифры замены или подстановки (симметричное шифрование), когда одни символы сообщения заменяются другими символами, согласно некоторому правилу.

К шифрам замены относится и один из первых известных кодов в истории человечества *код Цезаря,* применявшийся в древнем Риме. Суть этого кода состояла в том, что буква алфавита заменялась другой с помощью сдвига по алфавиту на одно и то же число позиций.

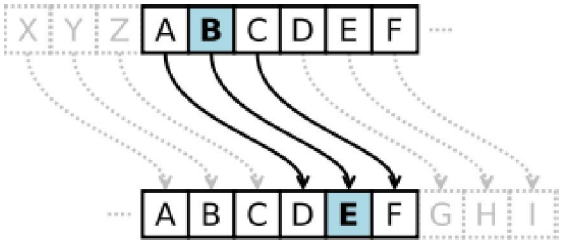


Рисунок 13 – Шифр Цезаря

Шифр Цезаря – один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. *Шифр Цезаря* можно классифицировать как *шифр подстановки,* при более узкой классификации — *шифр простой замены*. Ключом в *шифре Цезаря* является величина сдвига на *3*. Например, в шифре со сдвигом *вправо* на *3,* буква *А* была бы заменена на *Г, Б* станет *Д,* и так далее. Шифр назван в честь римского императора *Гая Юлия Цезаря,* использовавшего его для секретной переписки (рисунок 13).

Например, зашифруем слово *ТАЙНОПИСЬ,* используя сдвиг на одну букву вперед по алфавиту. Получим слово *УБКОПРЙТЭ*. Если будем для того же исходного слова применять сдвиг на две позиции назад, то получим *РЮЗЛМНЖПЪ*. Расшифровка таких записей очень проста, даже при незнании сдвига. Для этого применяется метод полосок. На нескольких горизонтальных полосках записывается алфавит. Затем эти полоски прикладываются друг к другу так, чтобы по горизонтали получалось зашифрованное слово (непонятный набор символов). Остается в одной из

строк найти осмысленное слово, которое и было зашифровано. Тогда определяется и сдвиг, и значение всех символов (таблица 12). Фрагмент расшифровки с помощью полосок содержится в таблице. Обратите внимание на строки *2, 4* и *5*. В них содержатся слово до шифровки и его шифры, уже знакомые нам.

Таблица 12 – Шифр со сдвигом

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	П	Э	З	К	Л	М	Ё	О	Щ
2	**Р**	**Ю**	**Ж**	**Л**	**М**	**Н**	**Ж**	**П**	**Ъ**
3	С	Я	И	М	Н	О	З	Р	Ы
4	**Т**	**А**	**Й**	**Н**	**О**	**П**	**И**	**С**	**Ь**
5	**У**	**Б**	**К**	**О**	**П**	**Р**	**Й**	**Т**	**Э**
6	Ф	В	Л	П	Р	С	К	У	Ю
7	Х	Г	М	Р	С	Т	Л	Ф	Я

5.1.2. Математическое описание шифра замены

Математическая модель шифрования и дешифрования *шифра Цезаря* можно выразить следующими формулами:

$y = x + k \quad x = y - k$

где x – символ открытого текста, y – символ шифрованного текста, а k – ключ.

$A = \{a_1, a_2, a_3, \ldots, a_{33}\}$ – множество букв алфавита и знаков препинания,

$B = \{b_1, b_2, b_3, \ldots, b_{35}\}$ – множество знаков шифра.

Пусть также $f: A \rightarrow B$ – взаимно-однозначное отображение A в B. Это значит, что каждой букве a_k алфавита A сопоставляется однозначно определенная буква b_k алфавита B, которую мы обозначаем символом $f(a_k)$, причем разным буквам сопоставляются разные буквы. Тогда шифр замены действует так: открытый текст $a_1 a_2 \ldots a_k$ преобразуется в шифрованный текст $f(x_1)\, f(x_2) \ldots f(x_k)$. Для русского языка можно обойтись *35* знаками; *1* буква *(е, ё,* и *ь, ъ* не различаются), пробел, точка, запятая, тире. Если число знаков, используемых при шифровании, тоже равно *35,* то каждый

такой шифр задается взаимнооднозначным отображением одного множества из *35* элементов на другое такое же множество. Число таких отображений равно *1 * 2 * 3 * 4 ....* 35*. Это настолько громадное число, что его трудно себе представить, оно примерно равно 10^{40}.

5.2. Симметричные и асимметричные криптосистемы

Алгоритмы с использованием ключа делятся на два класса: *симметричные* (или алгоритмы секретным ключом) и *асимметричные* (или алгоритмы с открытым ключом). В первом случае в шифраторе отправителя и дешифраторе получателя используется один и тот же ключ. Шифратор образует шифр – текст, который является функцией открытого текста, конкретный вид функции шифрования определяется секретным ключом. Дешифратор получателя сообщения выполняет обратные преобразования аналогичным образом. Секретный ключ хранится в тайне и передается отправителем сообщения получателя по каналу, исключающему перехват ключа *криптоаналитиком* противника. Обычно предполагается *правило Кирхгофа: стойкость шифра определяется только секретностью ключа,* т.е. криптоаналитику известны все детали процесса шифрования и дешифрования, кроме секретного ключа. Открытый текст обычно имеет произвольную длину, если его размер велик, и он не может быть обработан вычислительным устройством шифратора целиком, то он разбивается на блоки фиксированной длины, и каждый блок шифруется в отдельности, не зависимо от его положения во входной последовательности. Разница в том, что симметричные алгоритмы используют один и тот же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки). В то время как асимметричные алгоритмы используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу шифровки.

Симметричные алгоритмы подразделяют на *потоковые шифры* и *блочные шифры.* Потоковые позволяют шифровать информацию побитово, в то время как блочные работают с некоторым набором бит данных (обычно размер блока составляет 64 бита)

и шифруют этот набор как единое целое. Начальное представление о них можно получить в статье об алгоритмах.

Ассиметричные шифры (также именуемые алгоритмами с открытым ключом, или криптографией с открытым ключом) допускают, чтобы открытый ключ был доступен всем (скажем, опубликован в газете). Это позволяет любому зашифровать сообщение. Однако расшифровать это сообщение сможет только нужный человек (тот, кто владеет ключом дешифровки). Ключ для шифрования называют *открытым ключом*, а ключ для дешифрования *закрытым ключом* или *секретным ключом*.

5.3. Криптосистема RSA-шифрование с открытым ключом, асимметричное шифрование

RSA – криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись (аутентификация – установление подлинности). *Криптосистема RSA* разработана в 1977 году и названа в честь ее разработчиков RONALD RIVEST, ADI SHAMIR и LEONARD ADLEMAN.

Алгоритмы асимметричного шифрования используют два ключа, которые образуют неразрывную пару. Создатель ключей оставляет один ключ себе: этот ключ называют *закрытым* (личным). Второй ключ публикуется. Его называют *открытым* (публичным). В случае асимметричного шифрования каждый субъект обмена данными должен обладать парой из закрытого и открытого ключей. Безопасность обеспечивается сложностью алгоритма, что исключает возможность получения второго компонента пары ключей, зная первый компонент.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая *PGP, TLS/SSL, IPSek/IKE* и других.

Рассмотрим *алгоритм* криптосистемы *RSA* (рисунок 14):

Поскольку алгоритм является несимметричным, то ключи должны быть взаимосвязаны.

1. Выбираются *два* (лучше больших) *простых* (приложение 2) числа, например: *p(3)* и *q(11),* p и q не должны быть слишком близки друг к другу, иначе можно будет их найти, используя метод факторизации Ферма[1].

Простое число – это такое число, которое делится без остатка только на себя и на единицу. Использование простых чисел повышает *криптостойкость* алгоритма.

Вычисляется модуль $n = p * q$

$n = 3 * 11 = 33$.

2. Вычисляется значение *функции Эйлера* от числа *n,* $\varphi(n)=\lambda$ по формуле $= (p – 1) * (q – 1) = \lambda = (3 – 1) * (11 – 1) = 20$.

3. Назначается (выбирается) *e,* такое, чтобы *e* и λ были взаимно простыми (например, $e = 7$).

4. Вычисляется *число d (целое число),* удовлетворяющее условию: $(d * e) \bmod d\lambda = 1$, которое преобразовывается, используя алгоритм *Евклида*[2]:

$d * e = 1 + \lambda$, $d * 7 = 1 + 20$; $d = (20 + 1) / 7 = 3$.

5. $\{e, n\}$ – *открытый ключ* $e = 7$; $n = 33$.

$\{d, n\}$ – *секретный ключ* $d = 3$; $n = 33$.

Число *d* хранится в строжайшем секрете – это и есть секретный ключ, который позволит читать все послания, зашифрованные с помощью пары чисел *(e, n).*

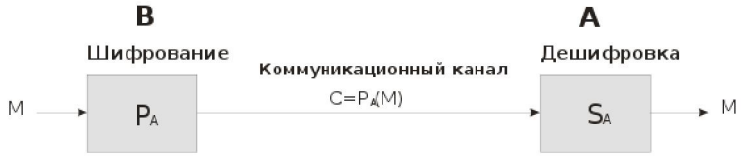


Рисунок 14 – Схема асимметричного шифрования

[1] Метод основан на поиске таких целых чисел X и Y, которые удовлетворяют соотношению, $\mathbf{x^2 – y^2 = n}$, что ведёт к разложению $\mathbf{n=(x–y)*(x+y)}$

[2] Эффективный алгоритм для нахождения наибольшего общего делителя двух целых чисел. Алгоритм назван в честь греческого математика Евклида, который впервые описал его в VII и X книгах «Начал».

5.4. Электронная цифровая подпись, хеширование

Ассиметричная криптография позволяет любому пользователю зашифровать своё сообщение открытым ключом получателя. Но остаётся угроза подмены сообщения третьим лицом (злоумышленником). Для защиты от этого была предложена в 1976 году *У. Диффи* и *М. Хелманом* идея цифровой подписи, вычисляемой на основе закрытого ключа отправителя и проверяемой открытым ключом отправителя. Таким образом, только отправитель может поставить свою подпись, и в то же время любой желающий может удостовериться, что это именно его подпись.

Электронная цифровая подпись (ЭЦП) – это присоединяемое к сообщению его криптографическое преобразование *(хеш-образ),* которое позволяет при получении проверить авторство и подлинность сообщения. *ЭЦП* содержит зашифрованные сведения о передаваемом сообщении и его авторе. При этом электронная цифровая подпись надёжнее решает не только традиционные задачи авторства и подлинности документа, которые ранее обеспечивались рукописной подписью под бумажным документом, но и следующие важные задачи электронного документооборота:

– целостность документа;

– невозможность подделки подписи;

– предотвращение отказа от подписи;

– юридическая значимость документа.

Хеширование – это преобразование по детерминированному алгоритму[1] входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются – *хеш-функциями* или функциями свёртки, а их результаты называют *хешем*.

Одним из свойств *хеш-функций* является то, что это очень затруднительное восстановление исходного значения из хеша. *Хеш-функция – однонаправленная* функция, т.е. вычислить значения по аргументу – элементарно, а вот аргумент по значению – практически невозможно.

[1] Алгоритмический процесс, который выдаёт уникальный и предопределённый результат для заданных входных данных.

Вычисление ЭЦП

Алгоритм цифровой подписи начинается с предварительного *хеширования* сообщения – вычисляется значение некоторой контрольной функции от всего сообщения. Для вычисления хеш-образа *H* сообщения *T* в данной работе предлагается использовать упрощённую хеш-функцию квадратичной свёртки:

$$H_i = (H_{i-1} + M_i)^2 \ mod \ n$$

где $H_0 = 0$, n из открытого ключа автора сообщения, M_i – коды символов сообщения, открытого или предварительно зашифрованного. После обработки последнего символа получаем хеш-образ всего сообщения *H*.

В алгоритмах цифровой подписи назначение открытого и закрытого ключей меняются – сообщение подписывается закрытым ключом отправителя, после чего любой может проверить подлинность с помощью открытого ключа отправителя. Вычисление электронной цифровой подписи *S* проводится по хеш-образу *H (d, n)* пересылаемого сообщения *T* с помощью закрытого ключа автора сообщения по формуле $S = H^d \ mod \ n$.

Формирование сообщения, подписанного *ЭЦП*, для передачи осуществляется присоединением *ЭЦП S* к сообщению *M:SM.*

5.5. Симметричное шифрование

Приведем некоторые примеры шифрования, используя математические методы.

1. Шифр Цезаря.

Послание Цезаря: *VENI VIDI VICI* (в переводе на русский язык означает «Пришел, Увидел, Победил»), направленное его другу Аминтию после победы над понтийским царем Фарнаком, сыном Митридата, выглядело бы в зашифрованном виде так: *YHQL YLGL YLFL*. Свое название этот шифр получил по имени римского императора *Гая Юлия Цезаря,* который использовал этот шифр при переписке с Цицероном (около 50 г. до н.э.). Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). При шифровании исходного текста каждая буква менялась на другую букву того же алфавита

по следующему правилу. Заменяющая буква определялась путем смещения по алфавиту от исходной буквы на *K* букв. При достижении конца алфавита выполнялся циклический переход к его началу. Цезарь использовал шифр замены при смещении *K = 3*. Такой шифр замены можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифр текста. Совокупность возможных подстановок для *K = 3* показана в таблице 13.

Таблица 13 – Совокупность возможных подстановок

A	**D**	**J**	**M**	**S**	**V**
B	**E**	**K**	**N**	**T**	**W**
C	**F**	**L**	**O**	**U**	**X**
D	**G**	**M**	**P**	**V**	**Y**
E	**H**	**N**	**Q**	**W**	**Z**
F	**I**	**O**	**R**	**X**	**A**
G	**J**	**P**	**S**	**Y**	**B**
H	**K**	**Q**	**T**	**Z**	**C**
I	**L**	**R**	**U**		

2. Кодирование двоичным кодом.

Алфавит: *А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я* делится на три равных строки, что обозначается тремя символами, где единица указывает из какой строки нужно брать букву. Затем нужно указать номер буквы от края: ноль – три символа, единица – один. Но самым первым знаком идёт символ, определяющий сторону, с которой нужно отсчитывать: Ноль – право, единица – лево. Например: слово *«Галилео»* шифруется следующим образом:

110001 – *Г*
11001 – *А*
101011 – *Л*
010011 – *И*
101011 – *Л*
110000 – *Е*
1010011 – *О*

3. Математическая модель шифрования.

Слово *«Криптография»* зашифровано словом *«Пхнфчузхещнд»,* используя ключ $K = n + 5$, где n – номер буквы в алфавите.

Таблица 14 – Математическая модель шифрования

Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Номер 1	12	18	10	17	20	16	4	18	1	22	10	33
Номер 1 +5	17	23	15	22	25	21	9	23	6	27	15	5
Шифр	П	Х	Н	Ф	Ч	У	З	Х	Е	Щ	Н	Д

4. Матричный способ кодирования.

Для кодирования текста на русском языке занумеруем все буквы по месту их расположения в алфавите – от *1* до *33*, добавив *34-ю* пробел.

Таблица 15 – Матричный способ кодирования

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	#
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34

Возьмем какое-нибудь простое предложение, например, *«шёл снег»,* и каждую букву заменим соответствующей цифрой. Получим последовательность: *26, 7, 13, 34, 19, 15, 6, 4.*

Построим из этой последовательности две таблички *2*х*2:*

$$\begin{pmatrix} 26 & 7 \\ 13 & 34 \end{pmatrix}, \begin{pmatrix} 19 & 15 \\ 6 & 4 \end{pmatrix}$$

Такие таблички из четырех чисел называются матрицей. Зашифруем эту последовательность с помощью еще одной матрицы $A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ – *кодирующей* – по следующему правилу:

$$\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} * \begin{pmatrix} 26 & 7 \\ 13 & 34 \end{pmatrix} = \begin{pmatrix} 2*26+3*13 & 2*7+3*34 \\ 1*26+2*13 & 1*7+2*34 \end{pmatrix} = \begin{pmatrix} 91 & 116 \\ 52 & 75 \end{pmatrix},$$

$$\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} * \begin{pmatrix} 19 & 15 \\ 6 & 4 \end{pmatrix} = \begin{pmatrix} 2*19+3*6 & 2*15+3*4 \\ 1*19+2*6 & 1*15+2*4 \end{pmatrix} = \begin{pmatrix} 56 & 42 \\ 31 & 23 \end{pmatrix}.$$

Такой способ шифрования и называют *матричным.* Ваш адресат получит текст: *91, 116, 52, 75, 56, 42, 31, 23.*

А как же он его расшифрует? Оказывается, и это нетрудно: он должен взять *декодирующую матрицу* $B = \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$ *(B – матрица обратная к A).*

Например: $\{A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} B = \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix}\}$ и проделать с полученным текстом то же самое, что делали мы с исходным текстом.

$$\begin{pmatrix} -2 & -3 \\ 1 & 2 \end{pmatrix} * \begin{pmatrix} 91 & 116 \\ 52 & 75 \end{pmatrix} = \begin{pmatrix} 2*91+(-3)*52 & 2*116+(-3)*75 \\ (-1)*91+2*52 & (-1)*116+2*75 \end{pmatrix} = \begin{pmatrix} 26 & 7 \\ 13 & 34 \end{pmatrix},$$

$$\begin{pmatrix} -2 & -3 \\ 1 & 2 \end{pmatrix} * \begin{pmatrix} 56 & 42 \\ 31 & 23 \end{pmatrix} = \begin{pmatrix} 2*56+(-3)*31 & 2*42+(-3)*23 \\ (-1)*56+2*31 & (-1)*42+2*23 \end{pmatrix} = \begin{pmatrix} 19 & 56 \\ 6 & 4 \end{pmatrix}.$$

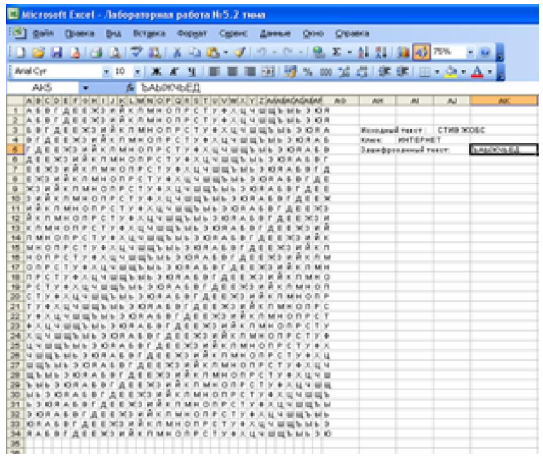
После замены матриц на последовательность *26, 7, 13, 34, 19, 15, 6, 4,* а затем – чисел на буквы дешифровальщик получит исходный текст *«шёл снег».*

Ясно, что никто посторонний, не знающий ни кодирующей, ни декодирующей матрицы, получить этот текст не сможет.

Однако матричный способ шифрования не смог бы существовать, если бы в качестве кодирующей можно было брать только матрицу $\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$.

На самом деле таких матриц бесконечно много, придумывать их очень легко. И вообще вы можете менять свою систему *«тайнописи»* каждый день. Для этого нужно знать очень немного – уметь любые две матрицы «перемножать», т.е. по определенному правилу составлять из них третью.

$\begin{pmatrix} x & y \\ z & t \end{pmatrix} * \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} xp+yr & xq+ys \\ zp+tr & zq+ts \end{pmatrix}$ – *правило умножения матриц.*



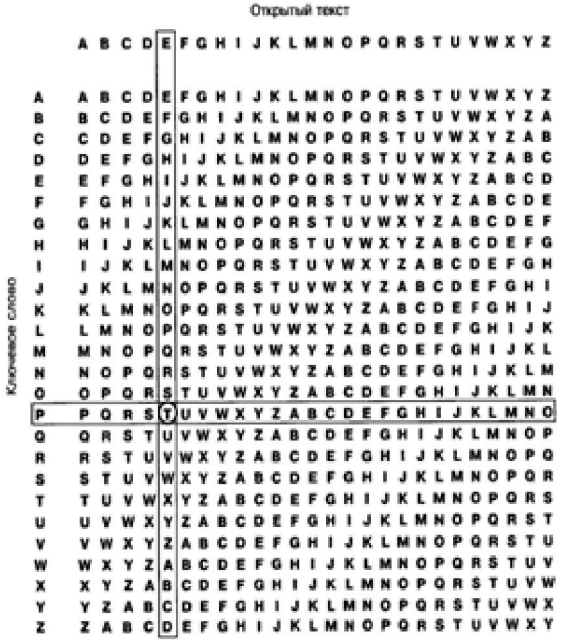


Рисунок 14 – Квадраты Виженера

4. Шифры сложной замены

Шифр Виженера (рисунок 14) состоит из последовательности нескольких шифров *Цезаря* с различными значениями сдвига. Для зашифрования может использоваться таблица алфавитов, называемая *квадрат Виженера.* Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается *26* различных шифров *Цезаря*. На разных этапах кодировки *шифр Виженера* использует различные алфавиты из этой таблицы. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Предположим, что исходный текст имеет вид:

ATTACKATDAWN

Посылающий сообщение записывает ключевое слово *«LEMON»* циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

LEMONLEMONLE

Первый символ исходного текста *A* зашифрован последовательностью *L*, которая является первым символом ключа. Первый символ *L* шифрованного текста находится на пересечении строки *L* и столбца *A* в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; т.е. второй символ шифрованного текста *X* получается на пересечении строки *E* и столбца *T.* Остальная часть исходного текста шифруется подобным способом.

Исходный текст: *ATTACKATDAWN*

Ключ: *LEMONLEMONLE.* Зашифрованный текст: *LYFOPVEFRNHR.*

5.6. Ассиметричное шифрование

1. Описание *алгоритма RSA.* Зашифруем и расшифруем сообщение *«CAB»* по алгоритму *RSA.*

Представим шифруемое сообщение как последовательность чисел в диапазоне от *0* до *33*. Буква *A = 1, B = 2, C = 3.*

Функция Mod – остаток от деления целого числа.

1) Взять открытый ключ *(e, n)* стороны *A*;

2) Взять открытый текст *M*;

3) Передать шифрованное сообщение: $P_a(M) = M^e \bmod n$

C1 = (3^7) mod 33 = 2 187 mod 33 = *9*;

C2 = (1^7) mod 33 = 1 mod 33 = *1*;

C3 = (2^7) mod 33 = 128 mod 33 = *29*.

Зашифрованное сообщение: *9_1_ 29.*

1) Принять зашифрованное сообщение *C*;

2) Применить свой секретный ключ *(d, n)* для расшифровки сообщения:

$S_a(C) = C^d \bmod n$

M1 = (9^3) mod 33 = 729 mod 33 = 3 *(C);*

M2 = (1^3) mod 33 = 1 mod 33 = 1 *(A);*

M3 = (29^3) mod 33 = 24 389 mod 33 = 2 *(B);*

Расшифрованное сообщение: *«CAB».*

2. Вычисление ЭЦП. Возьмём {*5;91*} **–** в качестве открытого ключа и {*29;91*} **–** в качестве закрытого.

Поставим электронную цифровую подпись на сообщение ***«МАША»*** (таблица 14) с помощью закрытого ключа отправителя *(d, n) = (29,91).* Для этого вычислим хеш-образ сообщения.

Таблица 14 – Расчет ЭЦП на сообщение МАША

i	Символы исходного сообщения $\mathbf{M_i}$	Коды символов $\mathbf{M_i}$	Вычисление хеш-образа **H**
$H_0 = 0$			
1	**М**	**14**	$\mathbf{H_1 = (H_0 + M_1)^2 \bmod n = (0 + 14)^2 \bmod 91 = 14}$
2	**А**	**1**	$\mathbf{H_2 = (H_1 + M_2)^2 \bmod n = (14 + 1)^2 \bmod 91 = 43}$
3	**Ш**	**26**	$\mathbf{H_3 = (H_2 + M_3)^2 \bmod n = (43 + 26)^2 \bmod 91 = 29}$
4	**А**	**1**	$\mathbf{H_4 = (H_3 + M_4)^2 \bmod n = (29 + 1)^2 \bmod 91 = 81}$
Хеш-образ			$\mathbf{H' = 81}$
Цифровая подпись			$\mathbf{S = H^d \bmod n = 81^{29} \bmod 91 = 9}$

Хеш-образом H′ отправляемого сообщения *«МАША»* является число *81*. Вычисление *«ЭЦП S»* по *хеш-образу* с помощью закрытого ключа отправителя производится по формуле $H' = S^e \bmod n$.

$$S = H^d \bmod n$$

Электронной цифровой подписью сообщения является число *9*. Сформируем сообщение для передачи, добавив к нему *ЭЦП.* Получим *«9МАША».*

Проверка подлинности ЭЦП

Процедура проверки подлинности *ЭЦП* и самого сообщения заключается в следующем:

1. Отделяется *ЭЦП* от основного сообщения.
2. Выделяется из *ЭЦП* хеш-образ полученного сообщения *открытым ключом* отправителя по формуле: $H' = S^e \bmod n$.
3. Вычисляется хеш-образ *H″* полученного сообщения на стороне получателя по формуле: $H_i = (H_{i-1} + M_i)^2 \bmod n$.
4. Сравнивается *H′ и H′.′*

ЭЦП признаётся подлинной, если значения хеш-образов совпадают.

$$H' = H''$$

Например, предположим, что при передаче нашего сообщения ***«9МАША»*** оно было изменено на ***«9МИША».*** Проверим подлинность полученного сообщения (таблица 15).

Таблица 15 – Расчет ЭЦП на сообщение МИША

Хэш-образ из ЭЦП			$\mathbf{H' = S^e \bmod n = 9^5 \bmod 91 = 81}$
i	Символы принятого сообщения $\mathbf{M_i}$	Коды символов $\mathbf{M_i}$	Вычисление хеш-образа на стороне получателя **H″**
$H_0 = 0$			
1	**М**	**14**	$\mathbf{H_1 = (H_0 + M_1)^2 \bmod n = (0 + 14)^2 \bmod 91 = 14}$
2	**И**	**10**	$\mathbf{H_2 = (H_1 + M_2)^2 \bmod n = (14+10)^2 \bmod 91 = 30}$
3	**Ш**	**26**	$\mathbf{H_3 = (H_2 + M_3)^2 \bmod n = (30 + 26)^2 \bmod 91 = 42}$
4	**А**	**1**	$\mathbf{H_4 = (H_3 + M_4)^2 \bmod n = (42 + 1)^2 \bmod 91 = 29}$
Вычисленный хеш-образ H″ = 29			

В таблице показано, что *ЭЦП* принятого сообщения равна *9*, хеш-образ сообщения согласно *ЭЦП H′ = 81*, вычисленный хеш-образ полученного сообщения на стороне получателя открытым ключом отправителя *H″ = 29*. Из неравенства *H′ ≠ H″* делаем вывод, что при передаче сообщения произошло его случайное или умышленное изменение.

При сравнении таблиц 14 и 15 видно, что даже при изменении одной буквы в исходном сообщении его хеш-образ существенно изменяется. Такие изменения легко выявляются при проверке подлинности электронной цифровой подписи.

Задания для самостоятельной работы

1. Постройте зашифрованный алфавит *s(a) = d, s(b) = e, s(c) = f, s(d) = g, s(e) = h, ...* Зашифруйте, используя шрифт Цезаря, фразу: *«Один из древнейших шифров».*

2. Постройте в табличном процессоре *MS EXCEL* квадрат *Вижинера* русского алфавита. Придумайте ключевое слово. Зашифруйте фразу *«Задание будет выполнено».*

3. Зашифруйте текст из трёх слов, обменяйтесь зашифрованными сообщениями и расшифруйте.

4. Неизвестный русский последователь Цезаря, не ищущий легких путей, использует для шифрования преобразование: $C_i = (M_i * k + n) \bmod 32$, где k и n – натуральные числа, M_i и C_i – коды i-ых символов исходного текста и шифротекста соответственно. Шифруются только прописные русские буквы, остальные символы остаются без изменений. Таким способом был получен шифротекст:

ЦПЙЫМ. ГЯЯЫККНТ РУТНЖУГШНЙГКЫТ

Расшифрованное выражение, с учетом пробелов и знаков препинания, и будет ответом к этой задаче.

5. На каждой из трех осей установлено по одной вращающейся шестеренке и неподвижной стрелке. Шестеренки соединены последовательно. На первой шестеренке *33* зубца, на второй *– 10,* на третьей *– 7*. На каждом зубце первой шестеренки по часовой стрелке написано по одной букве русского языка в алфавитном порядке:

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р
С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

На зубцах второй и третьей шестеренки в порядке возрастания по часовой стрелке написаны цифры от *0* до *9* и от *0* до *6* соответственно. Когда стрелка первой оси указывает на букву, стрелки двух других осей указывают на цифры. Буквы сообщения шифруются последовательно. Зашифровывание производится вращением первой шестеренки против часовой стрелки до первого попадания шифруемой буквы под стрелку. В этот момент последовательно выписываются цифры, на которые указывают вторая и третья стрелки. В начале шифрования стрелка 1-го колеса указывала на букву *А*, а стрелки 2-го и 3-го колес — на цифру *0*. Зашифруйте слово *«ОЛИМПИАДА».*

6. Текст:

ЦЗЩИОНФЛЦЩРИОПЖЩЭЩХЖНФЛТЪЙ
ЗНЛУФ_АЩЛЗПИАЗНЭПЬОИВЛОПАЛ
АПАЛТЪЙЗЛЖФЛЦЗВХФОЛХПИОЩОН
ЛЬИЦЩУДЁЩЭПЖЪВЛЗПЁУЪХЖНШЛИ
ЪЮЭЩУЩЭЛЭЛЩОАЗНОЩЮЛОФАИОФ

получен из исходного текста шифром простой замены. А текст:

ЯАЧЕЕТВТВРАКНОО_ЛТКЛЛОРСТА
РИФШЫ_ПС_ЫЗХО_ЫКЫК_ОВОТЕНЕ
ЛСЯДЫП_ЧРВПСАК_ЕЗ_СГРМАОТН
*СВ_ЕПР_Н_КТСЫОРААЙТОООТИК_*
ТРИ_НО_ТЧЧЬЫШВЮ_ФАИ_МЕИСЯ

получен из исходного текста простым перестановочным шифром. Найти исходное сообщение.

7. *Алгоритм RSA*. Выбираем два простых числа: *p = 3557, q = 2579.*

8. *Алгоритм RSA*. Выбираем два простых числа: *p = 79, q = 71.*

9. Поставьте электронную цифровую подпись на сообщение *«ПРАВО»* с помощью закрытого ключа отправителя *(30, 15).* Для этого вычислите хеш-образ сообщения.

10. Поставьте электронную цифровую подпись на сообщение *«МЕТОД»* с помощью закрытого ключа отправителя *(31, 20)* Для этого вычислите хеш-образ сообщения.

Вопросы для самоподготовки

1. Криптография.
2. Шифр.
3. Шифрование.
4. Открытый (исходный) текст.
5. Криптосистема.
6. Шифрованный (закрытый) текст.
7. Ключ.
8. Криптоанализ.
9. Криптографическая стойкость.
10. Криптология.

Темы рефератов

1. Переписка Юлия Цезаря с Цицероном.
2. Шифровальные письма Индии, Египта, Месопотамии.
3. Аристотель и сциталла.
4. Полибий и его сигнализация, как метод шифрования.
5. Стремление человека разгадать загадки древней письменности.
6. Шифры «посольского приказа».
7. Виды криптограмм.
8. Симметричные системы шифрования.
9. Асимметричные системы шифрования.
10. Стеганография.

Список литературы

1. *Гатчин Ю.А., Коробейников А.Г.* Основы криптографических алгоритмов: учеб. пособ. СПб.: СПбГИТМО (ТУ), 2002. 123 с.
2. *Коробейников А.Г.* Математические основы криптографии: учеб. пособ. СПб: СПб ГИТМО (ТУ), 2002. 100 с.

3. *Масленников М.* Практическая криптография: учеб. пособ. СПб: БХВ- Петербург, 2003. 34 с.
4. *Ященко В.В.* Введение в криптографию: учеб. пособ. М: МЦНМО, 2000. 245 с.
5. *Гонина Е.Е.* Шифры, коды, тайны / Живая математика. № 1. 2008. 99 с.

ЗАКЛЮЧЕНИЕ

Математические методы, информационные технологии, специфически преломляясь в учении о государстве и праве, обогащают и усиливают его собственные методы, не заменяя их.

В то же время, при всех достоинствах математизации и информатизации юридической науки и права, нельзя преувеличивать их возможности и сводить сущность государственно-правовых проблем к чистой математике и информатике. Ведущая роль в юридических науках принадлежит качественному анализу. Использование здесь математических средств и методов ориентировано в настоящее время, по существу, на решение частных практических проблем и задач. Математические средства и методы исследования правовых систем ограничиваются только измерением однородных связей данных систем; им недоступны всеобщие связи правовой системы общества в целом в силу их универсальности. Математические методы, используемые в юридических науках, не оторваны от реальной жизни, юридической практики и теории. Напротив, они вытекают из реальных научно-практических потребностей юриспруденции.

Задачи изучения математических методов применением информационных технологий как фундаментальной дисциплины состоят в развитии логического и алгоритмического мышления, в выработке умения моделировать реальные правовые процессы.

Приложение 1

Логические законы и правила преобразования логических выражений:

1. Закон тождества

Всякое высказывание тождественно самому себе. Этот закон сформулирован древнегреческим философом Аристотелем. Закон тождества утверждает, что мысль, заключенная в некотором высказывании, остается неизменной на протяжении всего рассуждения, в котором это высказывание фигурирует.

$$A = A$$

2. Закон непротиворечия (противоречия)

Высказывание не может быть одновременно истинным и ложным. Если высказывание A – истинно, то его отрицание *не A* должно быть ложным. Следовательно, логическое произведение высказывания и его отрицания должно быть ложно:

$$\overline{A} \,\&\, A = 0$$

Закон непротиворечия говорит о том, что никакое предложение не может быть истинно одновременно со своим отрицанием. Например: ***«Это яблоко спелое»*** и ***«Это яблоко не спелое».***

3. Закон исключенного третьего

Высказывание может быть либо истинным, либо ложным, третьего не дано. Это означает, что результат логического сложения высказывания и его отрицания всегда принимает значение истина:

$$A \vee \overline{A} = 1$$

Закон исключенного третьего говорит о том, что для каждого высказывания имеются лишь две возможности: это высказывание либо истинно, либо ложно. Третьего не дано. Например: ***«Сегодня я получу 5, либо не получу».*** Истинно либо суждение, либо его отрицание.

4. Закон двойного отрицания

Если дважды отрицать некоторое высказывание, то в результате мы получим исходное высказывание:

$$\overline{\overline{A}} = A$$

Отрицать отрицание какого-нибудь высказывания – то же, что утверждать это высказывание. Например*:* ***«Неверно, что 2× 2 =не 4»; «Если неверно, что Вселенная не является бесконечной, то она бесконечна».***

5. Законы идемпотентности (равносильности)

В алгебре логики нет показателей степеней и коэффициентов.

Конъюнкция одинаковых «сомножителей» равносильна одному из них:

$$A\&A = A$$

Дизъюнкция одинаковых «слагаемых» равносильна одному:

$$A \vee A = A$$

6. Законы де Моргана (общей инверсии)

Смысл законов де Моргана (Август де Морган (1806-1871) – шотландский математик и логик) можно выразить в кратких словесных формулировках:

$\overline{A \vee B} = \overline{A}\ \&\ \overline{B}$ – отрицание логической суммы эквивалентно логическому произведению отрицаний слагаемых;

$\overline{A\ \&\ B} = \overline{A} \vee \overline{B}$ – отрицание логического произведения эквивалентно логической сумме отрицаний множителей.

7. Правило коммутативности (переместительный закон)

В обычной алгебре слагаемые и множители можно менять местами. В алгебре высказываний можно менять местами логические переменные при операциях логического умножения и логического сложения:

Логическое умножение:$A\&B=B\&A$

Логическое сложение: $A \vee B = B \vee A$

8. Правило ассоциативности (сочетательный закон)

Если в логическом выражении используются только операция логического умножения или только операция логического сложения, то можно пренебрегать скобками или произвольно их расставлять:

Логическое умножение: $(A\ \&\ B)\ \&\ C = A\ \&\ (B\ \&\ C)$

Логическое сложение: $(A \vee B) \vee C = A \vee (B \vee C)$

9. Правило дистрибутивности (распределительный закон)

В отличие от обычной алгебры, где за скобки можно выносить только общие множители, в алгебре высказываний можно выносить за скобки, как общие множители, так и общие слагаемые:

Дистрибутивность умножения относительно сложения:

$$(A\ \&\ B) \vee (A\ \&\ C) = A\ \&\ (B \vee C)$$

Дистрибутивность сложения относительно умножения:

$$(A \vee B)\ \&\ (A \vee C) = A \vee (B\ \&\ C)$$

10. Закон исключения (склеивания)

Для логического сложения

$$(A\ \&\ B) \vee (\overline{A}\ \&\ B) = B$$

Для логического умножения

$$(A \vee B)\ \&\ (\overline{A} \vee B) = B$$

11. Закон исключения констант

Для логического сложения:

$$A \vee 1 = 1 \qquad A \vee 0 = A$$

Для логического умножения:

$$A\ \&\ 1 = A \qquad A\ \&\ 0 = 0$$

12. Законы поглощения

$A\ \&\ (A \vee B) = A \quad A \vee (A\ \&\ B) = A\ \&\ B$

13. Закон силлогизма

Закон силлогизма можно прочесть так. Если из высказывания *A* следует *B*, а из высказывания *B* следует *C*, то можно заключить, что из *A* следует *C*. Этот закон позволяет при доказательствах некоторого утверждения пользоваться цепочками заключений. Например: ***«Если будет хорошая погода, мы пойдем на пляж. Если мы пойдем на пляж, то обязательно искупаемся».*** Следовательно, согласно закону силлогизма можно сделать вывод: ***«Если будет хорошая погода, мы искупаемся».***

$$½ = \left[(A \to B) \wedge (B \to C)\right] \to (A \to C)$$

14. Modus ponens (гипотетический силлогизм)

Если *A* – истинно и из *A* следует *B*, то *B* также будет истинно.

Этот закон очень часто применяется при математических доказательствах. Например, ***треугольники ABC и A1B1C1 равны. Если треугольники равны, то соответствующие их стороны***

равны друг другу. Значит, согласно modus ponens, стороны AB и A1B1, BC и B1C1, AC и A1C1 равны.

$$\left[A \wedge \left(A \to B\right)\right] \to B$$

Закон позволяет от утверждения условного высказывания и утверждения его основания перейти к утверждению следствия этого высказывания: ***Если A, то B. A, следовательно, B.***

15. Закон контрапозиции

Следование из высказывания *A* высказывания *B* равносильно тому, что из *не B* следует *не A*. Например: высказывание ***«Если погода будет хорошей, мы пойдем на пляж»*** равносильно (эквивалентно) высказыванию ***«Из того, что мы не ходили на пляж следует, что погода была плохой».*** (Такое соответствие закону контрапозиции не совсем строгое, так как мы изменили времена глаголов во втором высказывании). Законы контрапозиции говорят о перемене позиций высказываний с помощью отрицания: из условного высказывания «если есть первое, то есть второе» вытекает «если нет второго, то нет и первого», и наоборот.

Например: из высказывания ***«Если есть следствие, то есть и причина»*** следует высказывание ***«Если нет причины, нет и следствия»,*** и из второго высказывания вытекает первое.

$$\left(A \to B\right) \leftrightarrow (\overline{B} \to \overline{A})$$

$$A \to B = \overline{A} \vee B,\ A \to B = \overline{B} \to \overline{A}$$

$$A \leftrightarrow B = \left(A \cdot B\right) \vee \left(\overline{A} \cdot \overline{B}\right).$$

Приложение 2

Простые числа

2 3 5 7 11 13
17 19 23 29 31 37
41 43 47 53 59 61
67 71 73 79 83 89
97 101 103 107 109 113
127 131 137 139 149 151
157 163 167 173 179 181
191 193 197 199 211 223
227 229 233 239 241 251
257 263 269 271 277 281
283 293 307 311 313 317
331 337 347 349 353 359
367 373 379 383 389 397
401 409 419 421 431 433
439 443 449 457 461 463
467 479 487 491 499 503
509 521 523 541 547 557
563 569 571 577 587 593
599 601 607 613 617 619
631 641 643 647 653 659
661 673 677 683 691 701
709 719 727 733 739 743
751 757 761 769 773 787
797 809 811 821 823 827
829 839 853 857 859 863
877 881 883 887 907 911
919 929 937 941 947 953
967 971 977 983 991 997
1009 1013 1019 1021 1031 1033
1039 1049 1051 1061 1063 1069
1087 1091 1093 1097 1103 1109
1117 1123 1129 1151 1153 1163
1171 1181 1187 1193 1201 1213
1217 1223 1229 1231 1237 1249
1259 1277 1279 1283 1289 1291
1297 1301 1303 1307 1319 1321
1327 1361 1367 1373 1381 1399
1409 1423 1427 1429 1433 1439
1447 1451 1453 1459 1471 1481
1483 1487 1489 1493 1499 1511
1523 1531 1543 1549 1553 1559
1567 1571 1579 1583 1597 1601
1607 1609 1613 1619 1621 1627
1637 1657 1663 1667 1669 1693
1697 1699 1709 1721 1723 1733
1741 1747 1753 1759 1777 1783
1787 1789 1801 1811 1823 1831
1847 1861 1867 1871 1873 1877
1879 1889 1901 1907 1913 1931
1933 1949 1951 1973 1979 1987
1993 1997 1999 2003 2011 2017
2027 2029 2039 2053 2063 2069
2081 2083 2087 2089 2099 2111
2113 2129 2131 2137 2141 2143
2153 2161 2179 2203 2207 2213
2221 2237 2239 2243 2251 2267
2269 2273 2281 2287 2293 2297
2309 2311 2333 2339 2341 2347

2351 2357 2371 2377 2381 2383
2389 2393 2399 2411 2417 2423
2437 2441 2447 2459 2467 2473
2477 2503 2521 2531 2539 2543
2549 2551 2557 2579 2591 2593
2609 2617 2621 2633 2647 2657
2659 2663 2671 2677 2683 2687
2689 2693 2699 2707 2711 2713
2719 2729 2731 2741 2749 2753
2767 2777 2789 2791 2797 2801
2803 2819 2833 2837 2843 2851
2857 2861 2879 2887 2897 2903
2909 2917 2927 2939 2953 2957
2963 2969 2971 2999 3001 3011
3019 3023 3037 3041 3049 3061
3067 3079 3083 3089 3109 3119
3121 3137 3163 3167 3169 3181
3187 3191 3203 3209 3217 3221
3229 3251 3253 3257 3259 3271
3299 3301 3307 3313 3319 3323
3329 3331 3343 3347 3359 3361
3371 3373 3389 3391 3407 3413
3433 3449 3457 3461 3463 3467
3469 3491 3499 3511 3517 3527
3529 3533 3539 3541 3547 3557
3559 3571 3581 3583 3593 3607
3613 3617 3623 3631 3637 3643
3659 3671 3673 3677 3691 3697
3701 3709 3719 3727 3733 3739
3761 3767 3769 3779 3793 3797
3803 3821 3823 3833 3847 3851

3853 3863 3877 3881 3889 3907
3911 3917 3919 3923 3929 3931
3943 3947 3967 3989 4001 4003
4007 4013 4019 4021 4027 4049
4051 4057 4073 4079 4091 4093
4099 4111 4127 4129 4133 4139
4153 4157 4159 4177 4201 4211
4217 4219 4229 4231 4241 4243
4253 4259 4261 4271 4273 4283
4289 4297 4327 4337 4339 4349
4357 4363 4373 4391 4397 4409
4421 4423 4441 4447 4451 4457
4463 4481 4483 4493 4507 4513
4517 4519 4523 4547 4549 4561
4567 4583 4591 4597 4603 4621
4637 4639 4643 4649 4651 4657
4663 4673 4679 4691 4703 4721
4723 4729 4733 4751 4759 4783
4787 4789 4793 4799 4801 4813
4817 4831 4861 4871 4877 4889
4903 4909 4919 4931 4933 4937
4943 4951 4957 4967 4969 4973
4987 4993 4999 5003 5009 5011
5021 5023 5039 5051 5059 5077
5081 5087 5099 5101 5107 5113
5119 5147 5153 5167 5171 5179
5189 5197 5209 5227 5231 5233
5237 5261 5273 5279 5281 5297
5303 5309 5323 5333 5347 5351
5381 5387 5393 5399 5407 5413
5417 5419 5431 5437 5441 5443

5449 5471 5477 5479 5483 5501
5503 5507 5519 5521 5527 5531
5557 5563 5569 5573 5581 5591
5623 5639 5641 5647 5651 5653
5657 5659 5669 5683 5689 5693
5701 5711 5717 5737 5741 5743
5749 5779 5783 5791 5801 5807
5813 5821 5827 5839 5843 5849
5851 5857 5861 5867 5869 5879
5881 5897 5903 5923 5927 5939
5953 5981 5987 6007 6011 6029
6037 6043 6047 6053 6067 6073
6079 6089 6091 6101 6113 6121
6131 6133 6143 6151 6163 6173
6197 6199 6203 6211 6217 6221
6229 6247 6257 6263 6269 6271
6277 6287 6299 6301 6311 6317
6323 6329 6337 6343 6353 6359
6361 6367 6373 6379 6389 6397
6421 6427 6449 6451 6469 6473
6481 6491 6521 6529 6547 6551
6553 6563 6569 6571 6577 6581
6599 6607 6619 6637 6653 6659
6661 6673 6679 6689 6691 6701
6703 6709 6719 6733 6737 6761
6763 6779 6781 6791 6793 6803
6823 6827 6829 6833 6841 6857
6863 6869 6871 6883 6899 6907
6911 6917 6947 6949 6959 6961
6967 6971 6977 6983 6991 6997
7001 7013 7019 7027 7039 7043

7057 7069 7079 7103 7109 7121
7127 7129 7151 7159 7177 7187
7193 7207 7211 7213 7219 7229
7237 7243 7247 7253 7283 7297
7307 7309 7321 7331 7333 7349
7351 7369 7393 7411 7417 7433
7451 7457 7459 7477 7481 7487
7489 7499 7507 7517 7523 7529
7537 7541 7547 7549 7559 7561
7573 7577 7583 7589 7591 7603
7607 7621 7639 7643 7649 7669
7673 7681 7687 7691 7699 7703
7717 7723 7727 7741 7753 7757
7759 7789 7793 7817 7823 7829
7841 7853 7867 7873 7877 7879
7883 7901 7907 7919 7927 7933
7937 7949 7951 7963 7993 8009
8011 8017 8039 8053 8059 8069
8081 8087 8089 8093 8101 8111
8117 8123 8147 8161 8167 8171
8179 8191 8209 8219 8221 8231
8233 8237 8243 8263 8269 8273
8287 8291 8293 8297 8311 8317
8329 8353 8363 8369 8377 8387
8389 8419 8423 8429 8431 8443
8447 8461 8467 8501 8513 8521
8527 8537 8539 8543 8563 8573
8581 8597 8599 8609 8623 8627
8629 8641 8647 8663 8669 8677
8681 8689 8693 8699 8707 8713
8719 8731 8737 8741 8747 8753

8761 8779 8783 8803 8807 8819
8821 8831 8837 8839 8849 8861
8863 8867 8887 8893 8923 8929
8933 8941 8951 8963 8969 8971
8999 9001 9007 9011 9013 9029
9041 9043 9049 9059 9067 9091
9103 9109 9127 9133 9137 9151
9157 9161 9173 9181 9187 9199
9203 9209 9221 9227 9239 9241
9257 9277 9281 9283 9293 9311
9319 9323 9337 9341 9343 9349
9371 9377 9391 9397 9403 9413
9419 9421 9431 9433 9437 9439
9461 9463 9467 9473 9479 9491
9497 9511 9521 9533 9539 9547
9551 9587 9601 9613 9619 9623
9629 9631 9643 9649 9661 9677
9679 9689 9697 9719 9721 9733
9739 9743 9749 9767 9769 9781
9787 9791 9803 9811 9817 9829
9833 9839 9851 9857 9859 9871
9883 9887 9901 9907 9923 9929
9931 9941 9949 9967 9973

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ
В ЮРИСПРУДЕНЦИИ

Учебное пособие

Редактор *В.Ю. Коваленко*
Компьютерная верстка *З.Б. Турашевой*

Подписано в печать
Формат 60×84 $^{1}/_{16}$. Печать офсетная.
Объем п. л. Тираж 100 экз. Заказ 108

Издательство КРСУ
720000, г. Бишкек, ул. Киевская, 44

Отпечатано в типографии КРСУ
720048, г. Бишкек, ул. Горького, 2