МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК
Кафедра алгебры и математической логики

РЕКОМЕНДОВАНО К ЗАЩИТЕ В ГЭК
Заведующий кафедрой
к.э.н., доцент
_____С.В. Вершинина
_25.06._____20__ г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
магистерская диссертация

ИНТЕГРАЦИЯ МАТЕМАТИКИ И ИНФОРМАТИКИ ПРИ ИЗУЧЕНИИ ЭЛЕМЕНТОВ КРИПТОГРАФИИ В КЛАССАХ С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ МАТЕМАТИКИ

44.04.01 Педагогическое образование
Магистерская программа «Современное математическое образование»

Выполнила работу
студентка 2 курса
очной формы обучения — Ширшова Полина Александровна

Научный руководитель
к.п.н., доцент — Шармин Дмитрий Валентинович

Рецензент
к.ф.-м.н., доцент кафедры программной и системной инженерии ТюмГУ — Трефилина Елена Рудольфовна

Тюмень
2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Требования федерального государственного образовательного стандарта среднего (полного) образования к результатам подготовки старшеклассников актуализируют дидактическую задачу развития информационной культуры и информационно-коммуникативной компетентности у выпускников школ, что означает владение знаниями и навыками, необходимыми для защиты информации.

И. Г. Хангельдиева рассматривала информационную культуру, как «качественную характеристику жизнедеятельности человека в области получения, передачи, хранения и использования информации». Увеличение количества информации, интенсивности развития информационных технологий показывает необходимость формирования у школьников информационной культуры. [Хангельдиева, с..2]

В современном обществе информация играет важную роль в различных сферах жизни человека. Возможность несанкционированного использования информации возникает из-за уязвимости, связанной с незаконными действиями лиц, осуществляющих доступ к программному обеспечению и информационным ресурсам компьютерных сетей.

Обучение приемам защиты информации в основном происходит на специализированных курсах или при получении высшего образования. В школьном образовании рассматривается данная проблема в узком смысле, поднимаются такие темы как определение информационной безопасности, защита компьютера от вирусов, поведение в сети Интернет.

Таким образом, возникает противоречие между необходимостью развития информационной культуры школьников в области информационной безопасности и недостаточном использовании для этого процесса обучения в школе.

Для решения выявленного противоречия ставится проблема в выборе средств обучения, способствующих формированию у учащихся умений в области информационной безопасности.

Объект исследования: процесс использования межпредметных связей в процессе обучения в школе.

Предмет исследования: интеграция математики и информатики при изучении элементов криптографии.

Цель исследования: разработать модель интеграции математики и информатики при изучении элементов криптографии в классах с углубленным изучении математики и апробировать ее элементы.

В соответствии с поставленной целью были выделены следующие задачи:

1. Подобрать и проанализировать литературу по теме исследования.

2. Выявить межпредметные связи математики и информатики.

3. Провести анализ содержания школьных учебников информатики, с целью выявления изучаемых элементов криптографии.

4. Разработать модель интеграции математики и информатики при изучении элементов криптографии в классах с углубленным изучении математики.

5. Апробировать элементы модели и сделать выводы.

Гипотеза исследования: если в процессе обучения информатике использовать

- интегрированные уроки с математикой,

- элементы криптографии,

то это позволит повысить уровень осведомленности в области информационной безопасности.

Методы исследования:

- теоретические (анализ литературы, анализ педагогического опыта и др.);

- практические (разработка заданий, обработка результатов эксперимента и др.).

Методологическая база исследований теории межпредметных связей Глинская Е.А., Гурьев И.И, Зверев И.Д., Левченко И.В., Лошкарева Н.А., Максимова В.Н., Федорова В.Н. и другие.

Этапы исследований:

Первый этап (с 1.10.2019 по 31.01.2020). Осуществлялся выбор темы исследования, подбор и анализ литературы, актуализация исследования.

Второй этап (с 1.02.2020 по 31.12.2020). Построение модели, подбор задания, подбор содержания интегрированных уроков, частичная апробация.

Третий этап (с 1.01.2021 по 25.06.2021). Завершающий этап исследования, на котором проходила обработка полученных экспериментальных данных, оформление результатов исследования.

База исследований муниципальное автономное общеобразовательное учреждение средняя общеобразовательная школа № 48.

Научная новизна исследования заключается в разработанной модели интегрированных уроков по криптографии.

Теоретическая значимость исследования состоит в анализе существующих практик обучения школьников элементам криптографии и применения межпредметных связей математики и информатики.

Практическая значимость исследования заключается в том, что разработанные планы внедрения изучения элементов криптографии в курс информатики для классов с углубленным изучением математики, могут быть использованы учителями математики и информатики в процессе профессиональной деятельности.

ГЛАВА 1. МЕЖПРЕДМЕТНЫЕ СВЯЗИ МАТЕМАТИКИ И ИНФОРМАТИКИ

1.1. ПРИМЕНЕНИЕ ИНТЕГРАЦИИ В СИСТЕМЕ ШКОЛЬНОГО ОБРАЗОВАНИЯ

Существующая предметная система обучения отображает традиционно сложившееся разделение наук на естественные, технические и гуманитарные. Обособленность предметов мешает формированию целостной картины мира, препятствует внутреннему восприятию.

Одной из проблем современного образования является конкурирующий характер школьных учебных предметов, каждый предмет представляет собой набор сведений в определенной области и не стремится к системному описанию действительности. При изучении отдельных предметов, у обучающихся формируется разрозненное представление о мире, они не могут связывать новый материал по одному предмету с уже пройденному по другим. Также практикующие учителя отмечают сокращение учебного материала непрофильных предметов в старших классах вследствие чего наблюдается тенденция к уменьшению целостности обучения и отодвиганию непрофильных предметов на второй план. Как инструмент решения выделенных проблем можно рассматривать внедрение межпредметности в учебный процесс.

Реализация межпредметности в образовательном процессе происходит через интеграцию, которая является необходимым условием, описанным в федеральных стандартах.

Интерес к проблеме интеграции просматривается в трудах Зверова И.Д, Максимовой В.Н., Крупецкой Н.К. и других, но первое научное осмысление интеграционных технологий в образовании было получено В.Т. Фоменко в первой половине 90-х. Ученые отмечают, что интеграция позволяет расширить границы научных знаний, перейти от замкнутого изучения предметов к их взаимодействию, а затем и к целостности.[Факторович, с. 20]

Б.М. Кедров утверждает, что «под интеграцией наук следует понимать такую форму взаимодействия, которая предполагает наличие у разных областей знания общих научно-исследовательских задач и целей». [Кедров, с. 2]

Выделяют два общих понятия интеграции: интеграция, как цель обучения, изучает создание целостного представления мира; интеграция, как средство обучения, исследует нахождение общих взаимосвязей предметов. Интеграционные процессы, происходящие в современном обществе, предъявляют новые требования к школьному образованию. Предметное обучение создает слишком узкие рамки для изучения наук.

Планируя преподавание своего предмета, учитель должен спрогнозировать интеграцию теоретического и практического материала в систему образования на данной ступени обучения. Последнее требует от него ознакомления с программами всех школьных предметов, а это просто физически невозможно. Кроме того, реализация интеграции должна строиться на комплексном подходе, что часто не осуществляется в школах, а интегрированное обучение проводится зачастую только эпизодически.

Базовый учебный план четко регламентирует предметное обучение, а Федеральные государственные образовательные стандарты устанавливают требования не только предметные, но также метапредметные и личностные, что серьезно ограничивает самостоятельное интегрирование предметов учителем. С другой стороны, межпредметные связи позволяют вывести решение задач на новый уровень, а также помогают заложить фундамент к решению сложных проблем реальной жизни.

Продуктивность применение интеграции при обучении школьников может быть достигнута при соблюдении условий, возникающих на различных направлениях интеграции. Всего выделяют три уровня интеграции содержания учебных предметов: внутрипредметную, межпредметную и системную.

1. Внутрипредметная интеграция подразумевает системой поход при создании дисциплин, позволяющий объединять понятия, правила и законы из

одной области знаний в блоки, таким образом, чтобы ученики могли получить полную информацию о предмете.

2. Межпредметная интеграция проявляется в использовании знаний умений и навыков одной дисциплины при изучении другой. На рисунке 1 можно увидеть классификацию межпредметной интеграции.

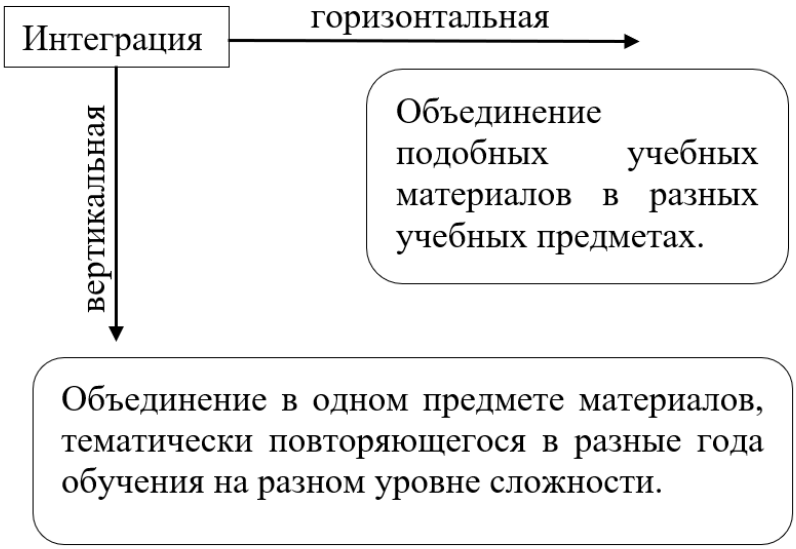

Рис. 1. Виды интеграции

Особенностями межпредметной интеграции являются: использование эпизодически материала другого урока; сохранение самостоятельности каждого предмета; сохраняется изначальная программа.

3. Системная интеграция характеризуется как объединение знаний, получаемых детьми как в школе, так и вне учебного процесса.

Интеграция является методологической категорией в современных педагогических исследованиях. Она используется для создания таких связей, которые обеспечивают целостность образовательного процесса (образовательных систем, системы образования в целом). Одновременно интеграция служит способом познания и изменения педагогической действительности.

Сущность интегративного подхода в обучении школьников состоит, главным образом, во всестороннем гармоничном развитии, которое

соответствует внутренним потребностям личности и направленно на свободу самореализации.

Согласно теории интеграции образования Данилюка А.Я. интеграция не должна рассматриваться как соединение разных предметов в один. Целью интеграции является создание такой образовательной системы, в которой один феномен будет изучаться со всех сторон, за счет изучения его в различных научных сферах. [Факторович, с. 26]

Интегрированная образовательная деятельность основывается на объединении нескольких видов деятельности, таких как физическая, интеллектуальная, социальная и так далее, а также разных средств развития обучающихся. Сабуровой Д.А. была предложена следующая структура интеграции, рассмотренная на рисунке 2. [Сабурова, с.4]

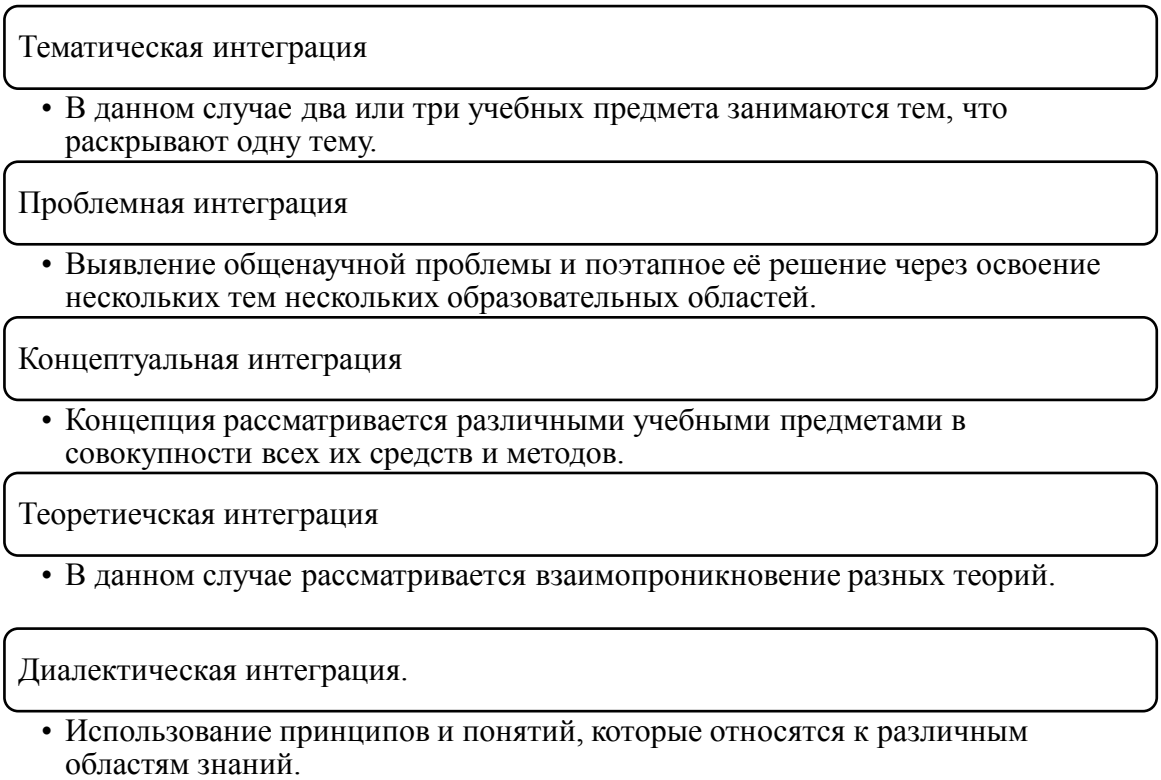

Рис. 2. Структура интеграции

Внедрение интегрированных методов обучения:

- позволяет реализовать один из важнейших принципов обучения - принцип системности;

- позволяет создавать благоприятные условия для развития логичности, гибкости, критичности мышления;

- способствует формированию системного мировоззрения, согласованности личности учащихся;

- уменьшает многопредметность, расширяет и углубляет межпредметные связи, для получения большего объема знаний;

- является средством мотивации учения школьников, стимулирует познавательную деятельность, способствует развитию творческих способностей.

Но также интегрированное образование имеет и ряд недостатков, таких как требование высокого уровня педагогических навыков учителя; увеличение плотности урока, отсутствие детализации, в некоторых случаях, требуется больше времени на подготовку к уроку. Интеграция предметов на постоянной основе невозможно по причинам низкой осведомленности учителей-предметников в содержании учебных программ других дисциплин, отсутствии опыта в реализации межпредметных связей, недостаточность методических рекомендаций. Для подбора содержания интегрированных предметов необходимо соблюдение некоторых условий:

1) материал предметов должен совпадать или быть близким по содержанию;

2) должны использоваться одинаковые или близкие методы обучения;

3) интегрируемые предметы должны строиться на общих закономерностях, концепциях;

4) уровень материала должен соответствовать уровню знаний обучающихся.

Содержание интегрированных предметов должно опираться на некоторые принципы, выделенные Дегтяревым В.А., такие как принцип научности: исследуемая информация должна влиять на принципиально важные общие закономерности мира; принцип соответствия: материал должен объяснять взаимосвязь между предметами, систематизировать изучение теории; принцип перспективности: знакомство с будущими сферами деятельности, возможностями применения полученных знаний. [Дегтярев, с. 6]

Интеграция может осуществляться на любом этапе педагогического процесса (Таблица 1).

Таблица 1

Реализация интеграции на различных этапах обучения

Этапы	Формы интеграции
интеграция на уровне педагогических целей	ориентация на такие интегральные свойства и характеристики личности, как активность, самостоятельность, креативность
интеграция на уровне содержания	интегрированные программы, интегрированные учебные курсы
интеграция на уровне сфер активности школьников	интегрированные уроки, экскурсии, конференции, проекты
интеграция на уровне педагогических технологий	разнообразие форм интеграции и методов педагогического воздействия

В современном образовательном процессе выделяют три основных уровня реализации интеграции:

Первый уровень: интеграция естественнонаучных и гуманитарных направлений. Поиска во взаимодействии предметов пути к целостному виденью мира.

Второй уровень: интеграция предметов путем формирования целостности содержания и форм учебной деятельности.

Третий уровень: интеграция за счет использования и усиления межпредметных связей цикла предметов.

Ученые выделяют две основные формы интеграции, используемых в школе: интегрированный урок и интегрированный курс.

1. Интегрированный урок – это урок, объединяющий обучение несклонным предметам при изучении одного понятия, закона, теоремы, имеющий особую структуру и методику преподавания. Выделяют следующие примеры интегрированных уроков: урок-лекция, урок-экскурсия, урок-исследование, урок-проект и урок-наблюдение.

2. Интегрированный курс – это курс, объединяющий обучение нескольким предметом в отдельную дисциплину. Модели реализации интегрированных курсов предоставлены на рисунке 3.

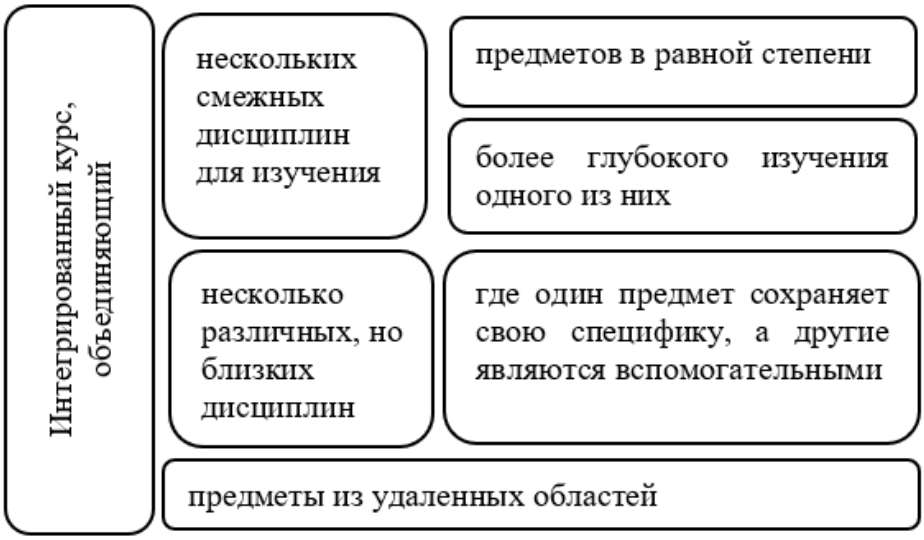

Рис. 3. Модели реализации интегрированных курсов

Таким образом внедрение межпредметных связей помогает школьникам сформировать полную картину природных явлений и взаимосвязей между ними, что делает знания более значимыми и применимыми на практике.

1.2. МЕЖПРЕДМЕТНЫЕ СВЯЗИ МАТЕМАТИКИ И ИНФОРМАТИКИ

Межпредметные связи – взаимодействие учебных программ таким образом, что содержание каждой дисциплины основано на остальных, создавая единую систему образования. Данная система образования помогает ученикам использовать знания других дисциплин при изучении нового материала. С помощью различных межпредметных связей не только решаются задачи обучения и развития учащихся, а также помощи в дальнейшем выборе профессиональной сферы. Поэтому межпредметные связи являются важным требованием непрерывного обучения.

Федорец Г.В., Максимова В.Н., Кукушин В.С и другие рассматривают разные классификации межпредметных связей, проанализировав и систематизировав их была составлена общая классификация, представленную на рисунке 4. В первую очередь все виды межпредметных связей можно объединить в четыре типа:

1) содержательные объясняется взаимосвязью элементов между блоками учебного материала, характеризует единство научных фактов, понятий и законов (классификация по видам знаний);

2) операционные делаться по формируемым навыкам, умениям (классификация по видам умений);

3) методические раскрывают используемые методы учебно-познавательной деятельности, средства и условия обучения (классификация по способу усвоения, по значимости, по способу взаимодействия);

4) организационные определятся формами и способами организации учебного процесса (классификация по форме реализации, по постоянству реализации, по направлению действия).

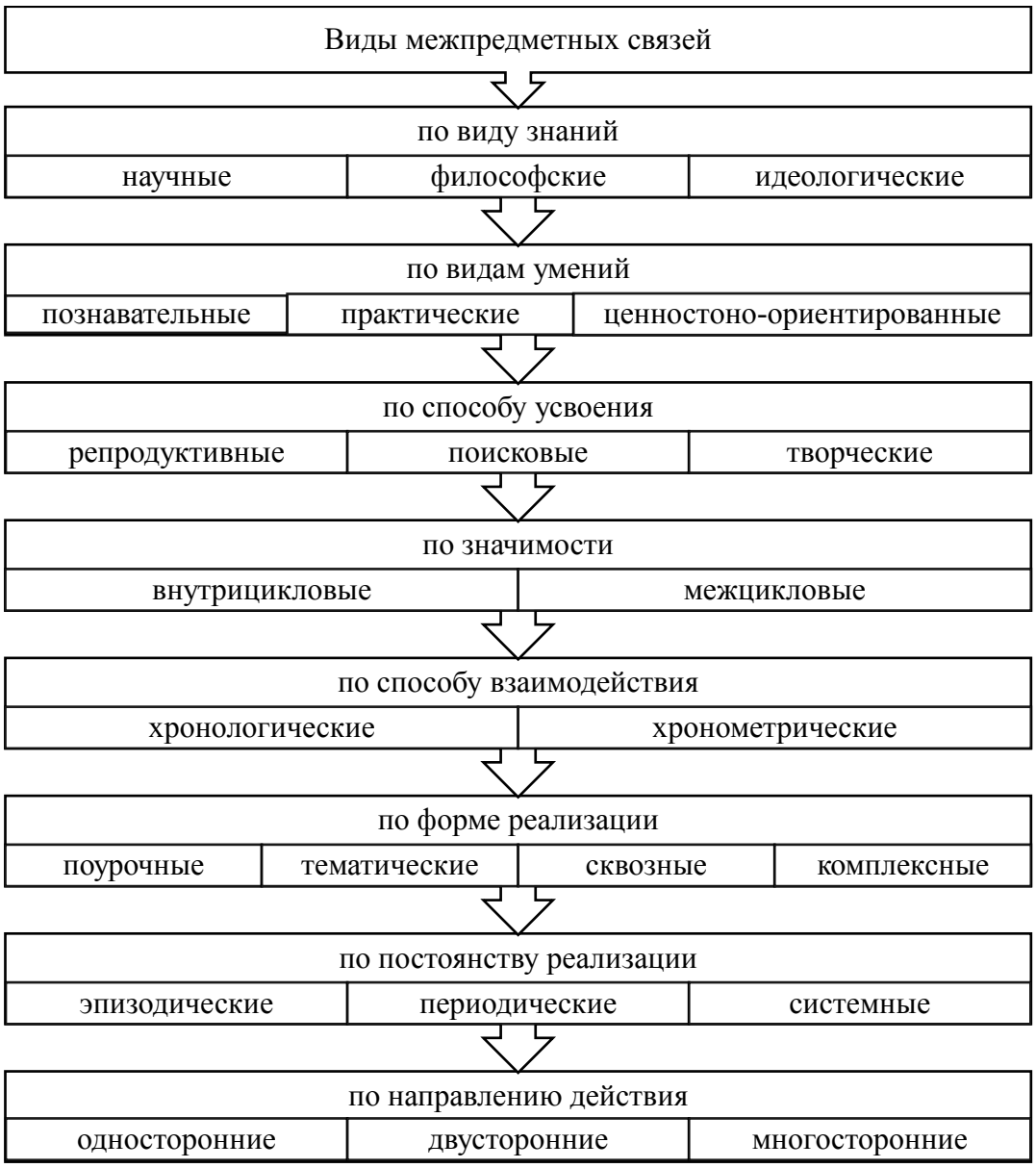

Рис. 4. Классификация межпредметных связей

- По виду знаний: научные межпредметные связи делятся на фактические, понятийные и теоретические, каждый из них направлен на установление и укрепление связи фактов, понятий и теория, соответственно, одинаковых в разных учебных предметах.

- По видам умений: формируют умении мыслительной, творческой, учебной и развивающей деятельности, способствуют выработке практических умений, вырабатывают умения необходимые для формирования личности ученика.

- По способу усвоения: выделенные межпредметные связи направлены на закрепление, усвоение и систематизацию знаний, полученных школьниками на разных учебных дисциплинах.

- По значимости: внутрицикловые это связи между предметами, находящимися в смежных областях знаний, межцикловые – все остальные.

- По способу взаимодействия: хронологические межпредметные связи делятся на преемственный, синхронные и перспективные, зависят от временного фактора, т.е. какие знаний уже были получены школьниками, какая тема изучается сейчас и что пригодится при изучении новых тем; хронометрические показывают продолжительность взаимодействия элементов, такие как локальные, среднедействующие, длительнодействующие.

- По форме и постоянству реализации: межпредметные связи осуществляются в рамках одного предмета, нескольких смежных предметов, предметов, относящихся к разным областям знаний.

- По направлению действия: каждый из видов межпредметной связи может делиться на прямые, т.е. когда межпредметные связи применяются только для изучения темы основного предмета, и обратные, когда изучается тема в одном предмете является основой изучения других предметов.

Межпредметная интеграция несет в себе больше возможностей для потенциального развития интеллектуальных, творческих способностей учащихся через создание проблемных ситуаций и решения межпредметных задач. Повышение качества образования, формирование у студентов обобщенных знаний на межпредметной основе, развитие умений переносить знания из одной области в другую, а также применять полученные знания на практике. Подобные задачи могут быть решены путем реализации межпредметных связей между математикой и информатикой и внедрения их в учебный процесс. При этом важно:

- проводить отбор содержания обучения, способствующего постановке межпредметных проблем и задач;

- применять на учебных занятиях знания из смежных дисциплин;

- формировать у студентов обобщенные знания на межпредметной основе;

- широко использовать наглядные формы представления учебного материала (графики, схемы, диаграммы).

Выделяют следующие функции межпредметных связей (Рисунок 5).

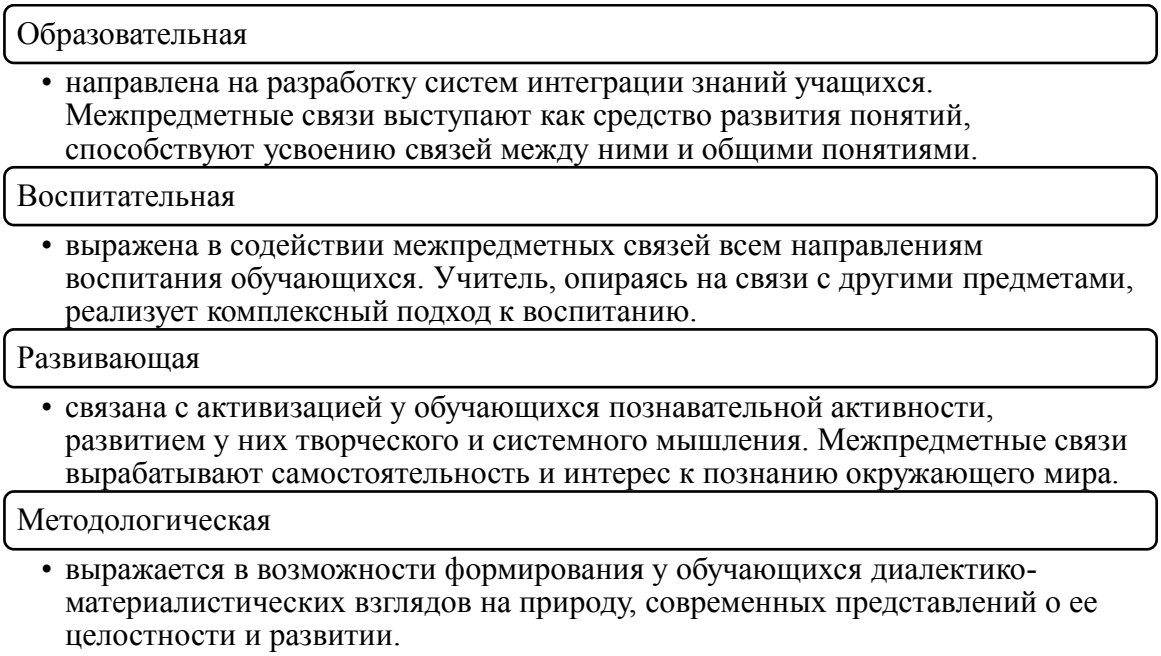

Рис. 5. Функции межпредметных связей

При реализации межпредметных связей важно понимать в каких условиях будет строиться дальнейшее обучений. В стандартах и учебных программах, регламентирующих современное школьное образование отсутствуют специальные разделы, связанные с межпредметными связями. Следовательно, профессионализм учителя становится основополагающим критерием при применении интегрированного образования. Лернер И.Я. выдвигал следующие условия реализации межпредметных связей:

1) должно обеспечиваться системное определение знаний учебного предмета на уровне учителя, программы, системы

2) подбор межпредметного материала; определение и применение практичных способов усвоения межпредметных знаний;

3) использование различных методов обнаружение связи или организация ее самостоятельного определения;

4) взаимодействие различных учебных предметов, способствующее развитию умений и способностей учащихся в познавательной деятельности, усвоении общенаучный и практической деятельности. [Лернер, с. 27.]

При использовании межпредметных связей в обучении необходимо понимать, что существуют определенные требования к учителям, организующих интеграцию своих предметов:

- изучение учителями содержания программ и учебников смежных предметов;

- согласованность учебно-воспитательных методов преподавания учителей смежных предметов;

- общая методическая работа учителей;

- посещение уроков учителей смежных предметов;

- коллективное планирование реализации межпредметных связей;

- системное их использование.

Для выполнения цели выпускной квалификационной работы были исследованы межпредметные связи математики и информатики. Рассмотрим примеры того, как понятия математики можно использовать в других предметах благодаря межпредметным связям (Рисунок 6).

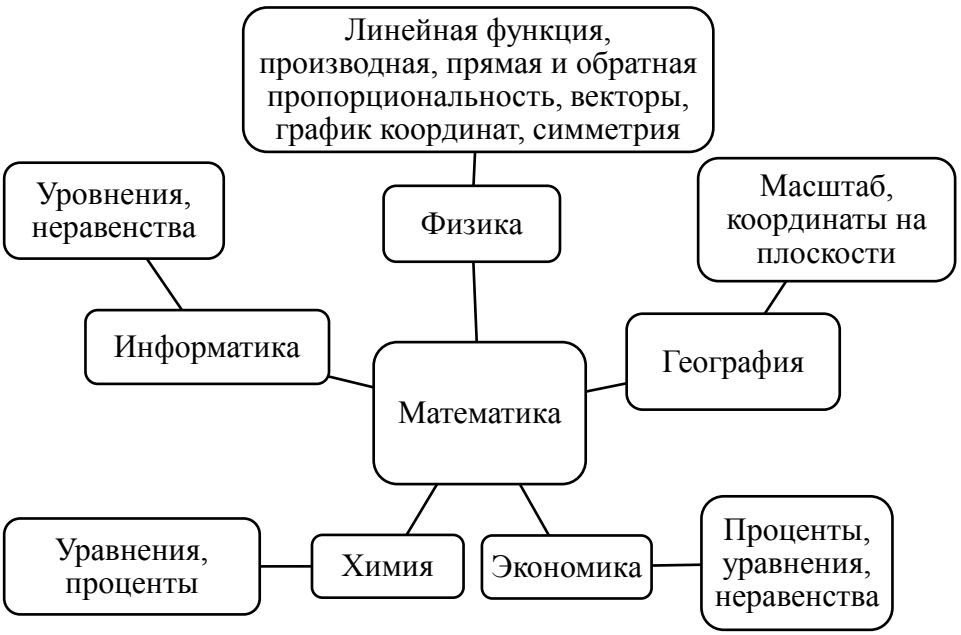

Рис. 6. Межпредметные связи математики

На основе знаний по математике развиваются вычислительные и измерительные навыки. Преемственность отношений дисциплин естественнонаучного цикла исследует практическое применение математических навыков и способностей. Это способствует развитию у учащихся целостного научного мировоззрения.

Межпредметные связи информатики с другими предметами реализуется при изучении информатики со стороны информации, информационных процессов, моделирования, алгоритмизации и программирования. Формируемые в процессе изучения информатики основы могут быть использованы практически во всех учебных предметах. Учащиеся на уроках информатики учатся работать с информацией: поиск, сбор, анализ, представление и передача. Данные знания помогают сформировать у школьников исследовательские и аналитические умения. Использование информационных технологий при обучении помогает не только сэкономить время и сделать информацию более доступной, но ещё способствует повышению мотивации обучающихся при изучении школьных предметов.

Совместное изучение курсов математики и информатики позволяет взаимно дополнять знания и структурировать их. Структуру организации межпредметных связей математики и информатики разработанную Козловым О.А. можно увидеть на рисунке 7. [Козлов, с. 57]

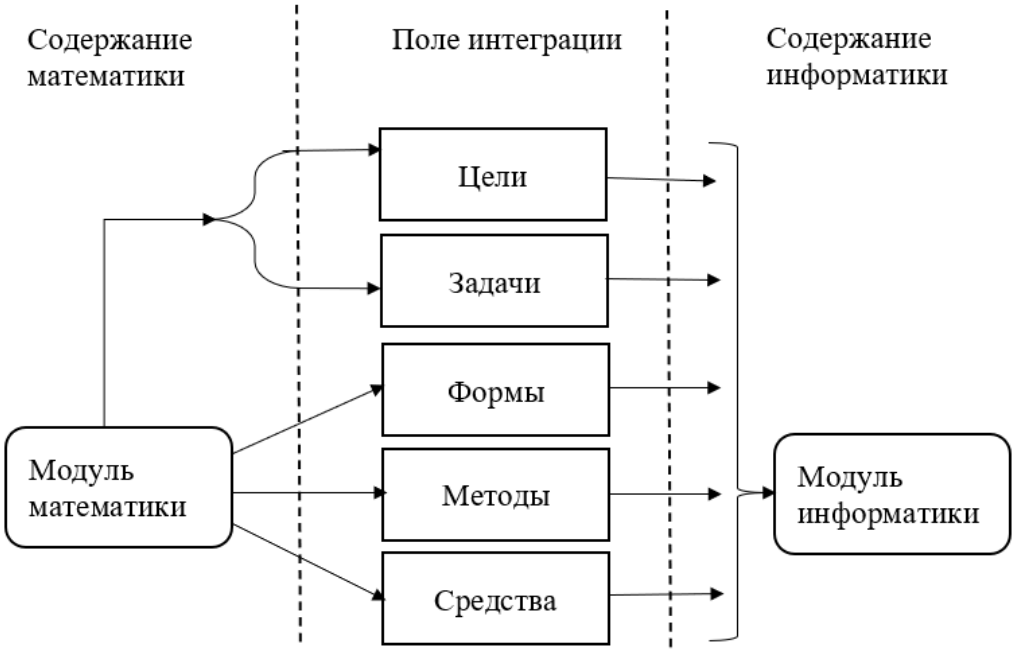

Рис. 7. Структура организации межпредметных связей

Цели и содержание образования определяются структурными компонентами научных знаний и умений необходимых будущим выпускникам. Поэтому проектирование технологии должно опираться на модель, которая задается федеральным государственным стандартом.

Межпредметность математики и информатики позволяет им находиться в центре межпредметных связей, составляя с остальными предметами единую образовательную систему. Эта система позволяет организовать последовательное обучение всему материалу без дублирования получаемой информации.

При рассмотрении курса информатики можно заметить, что некоторые темы основываются на чисто математических знания, такие как основы математической логики, системы счисления, элементы теории вероятности и математической статистики, теория графов, теория алгоритмов, основы математического моделирования и другие. Однако данные темы не входят в курс математики, а изучаются на уроках информатики. Виды межпредметных связей математики и информатики предоставлены в таблице 2.

Таблица 2

Виды межпредметных связей математики и информатики

Фактические	Понятийные	Теоретические
• системы счисления • законы алгебры логики • свойства функция	• множества • алгоритмы • модели • системы счисления	• теория графов • теория алгоритмов • теория вероятности

Для понимания возможностей интеграции математики и информатики был проанализирован отечественный опыт внедрения интегрированного обучения. Носковым М.В. и Поповой В.В. был разработан примерный вариант применения межпредметных связей при изучении курсов математики и информатики (Таблица 3). [Носков, с.3]

Таблица 3

Межпредметные связи в курсах математики и информатики

Темы, изучаемые в курсе математики	Темы, изучаемые в курсе информатики
Векторы	Векторная графика в Paint
Элементарные функции. Графики функций. Производная функций	Построение графиков функций с помощью Paint. Построение графиков и нахождение производных функций в Mathcad. Построение графиков в Excel.
Системы линейных алгебраических уравнений	Вычисление в Mathcad
Перевод чисел из одной системы счисления в другую	Кодирование числовой информации
Вычисление площадей фигур и объемов тел	Моделирование геометрических операций в Paint. Математическое вычисление в Excel и Mathcad
Исследование функций. Точки разрыва. Наибольшее и наименьшее значения функции в области	Алгоритмизация и программирование
Численные методы	Численное решение уравнений в Excel и Mathcad

Разработка межпредметных связей математики и информатики может проводиться с использованием следующих методов: решение задач межпредметного характера; решение математических задач на уроках информатики; использование информационных технологий для решения задач на уроках математики.

Актуальным является создание задач интеграционного характера, решение которых обеспечило бы формирование не только определенных умений, но и навыков использования современных компьютерных технологий. Для этого необходимо добиться оптимального сочетания объемов учебного материала, относящегося к сфере математики и информатики.

При отборе содержания обучения необходимо, ориентируюсь на цели обучения, руководствоваться принципами фундаментальности, профессиональной направленности, междисциплинарной интеграции и др. Необходимо тщательно согласовывать терминологию и обозначения в трактовке общих для курсов математики и информатики понятий, исключать противоречия и дублирование.

Важными моментами для преподавателя являются также структура и объем учебного материала. Программа должна отражать, фиксировать и реализовывать межпредметные связи с учетом профессиональной направленности преподавания общеобразовательных и общетехнических предметов.

Клочкова Н.Н. разработала примерные методические рекомендации для учителя математики при реализации межпредметных связей, на примере информатики, а также несколько примеров уроков по ним. Данные рекомендации предоставленные в таблице 4. [Клочкова, с. 3.]

Таблица 4

Методические рекомендации реализации межпредметных связей

Основные содержательные линии курса математики	Темы курсов, позволяющие реализовывать межпредметные связи	
	математика	Информатика
Числа и вычисления	1. Действия над рациональными числами	1. Ввод математического текста, работа с редактором формул в Word 2. Работа с электронными таблицами Excel, математические расчеты 3. Использование Matlab в качестве суперколькулятора
Уравнения и неравенства	1. Элементарные функции и их свойства 2. Построение графиков функций 3. Производная функций	1. Численное решение уравнений в Excel и Matlab 2. Решение нелинейных уравнений в Matlab 3. Решение неравенств в Excel и Matlab 4. Решение систем уравнений и неравенств в Excel и Matlab
Функция и их свойства	1. Элементарные функции и их свойства 2. Постоянные графики функций 3. Производная функции 4. Интеграл	1. Построение простейших графиков функций в Excel 2. Табулирование функций в Word и Excel 3. Интервальная переменная. Способы задания функции в Matlab 4. Построение графиков в Matlab 5. Вычисление интегралов и производных в Matlab

Продолжение таблицы 4

Геометрические фигуры и тела	1. Свойства геометрических фигур (треугольник, окружность, многоугольник) 2. Свойства геометрических тел (призма, пирамида, круглые тела)	1. Построение геометрических фигур в Космос и Word 2. Создание геометрических композиций в Компас 3. Геометрическое моделирование в Excel 4. Геометрические операции в Matlab. Программирование в Matlab
Геометрические величины	1. Вычисление площадей, длин отрезков, углов, объемов	1. Моделирование геометрических операций в Компас 2. Математическое вычисление в Excel и Matlab
Векторный анализ	1. Прямоугольная система координат на плоскости и в пространстве 2. Действия над векторами	1. Векторная графика в Компас 2. Исследование математических моделей и программирование в Matlab

Использование данных рекомендаций позволяет не только легко понять, как можно применять межпредметные связи, но и позволяет сэкономить время при проектировании уроков. Построение модели служит основой для создания любой технологии.

1.3. ОСНОВЫ КРИПТОГРАФИИ

Информационная безопасность детей – первостепенная задача Государства, но, невзирая на заинтересованность государства в вопросах предоставления достаточного уровня знаний в области криптографии, как базового средства обеспечения информационной безопасности, в современном школьном курсе информатики они рассматривается лишь частично.

Проанализировав содержание школьных учебников и авторских программ по информатике, можно сделать вывод: среди учебников углубленного курса информатики только один содержит в себе изучение элементов криптографии. Учебник Поляков К.Ю имеет в содержании следующие разделы, включающие изучение элементов криптографии в рамках темы: «Информационная безопасность»:

- шифрование: даются определения шифрования, криптографии и криптоанализа, ключа; рассказывается о симметричных шифрах, криптостойкости, шифрах перестановки;

- хэширование и пароли;

- современные алгоритмы шифрования: блочный шифр AES, алгоритм RSA, определение цифровой подписи;

- стеганография.

Изучение криптографии может быть включено в школьное обучение в виде внеурочной деятельности: факультативных занятий или кружков. В данной выпускной квалификационной работе мы рассматриваем возможность изучение криптографии как средства обеспечения межпредметных связей математики и информатики. И если с информатикой все понятно на фундаментальном уровне: криптография является средством обеспечения безопасности информации, а информация, в свою очередь является базовой составляющей информатики. Остается рассмотреть связь криптографии с математикой.

Криптография – это наука, использующая математические методы для обеспечения конфиденциальности, невозможности получения информации

посторонними), целостности (невозможности незаконного изменения информации), аутентификации (проверки подлинности владельца информации) и шифрования. Шифрование – обратимое изменение информации для предотвращения получения ее незарегистрированным пользователем. Необходимость защиты информации предъявляет следующие требования к шифрам:

- стойкость шифра характеризуется способностью шифра противостоять атакам на него; шифр можно назвать стойким, если его дешифровка требует достаточно большой вычислительной мощи или полный перебор ключей является более действенным;

- простота использования описывается удобством алгоритмов зашифрования и расшифрования;

- обеспечение секретности ключа гораздо важнее, чем сохранение секретности алгоритма шифрования.

На рисунке 8 составлена классификация криптографических шифров.

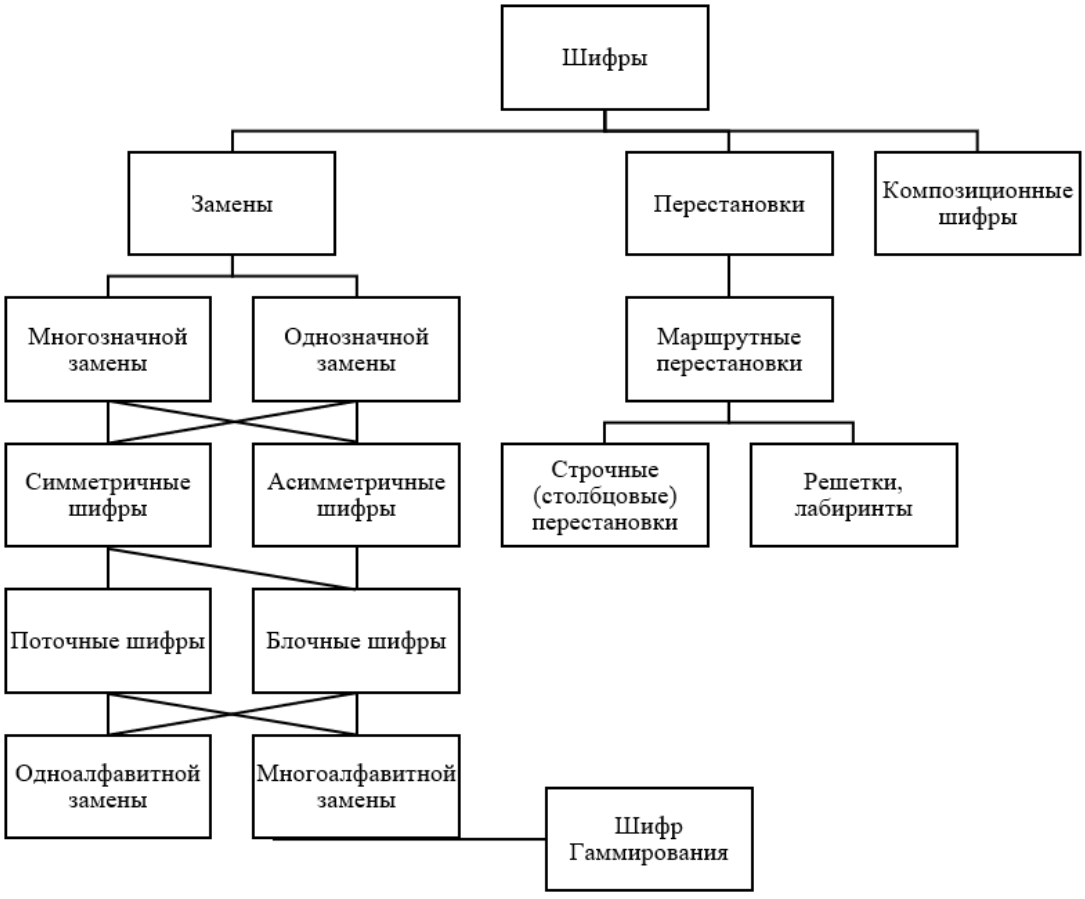

Рис. 8. Классификация криптографических шифров

Существенное влияние на усиление роли математики в криптографии оказали появившиеся в середине 20 века работы математика Клода Шеннона. В своих работах она описывал опыт работы с шифрами и доказал, что можно создать стойкий алгоритм используя только простые шифры замены и подстановки в комплексе. [Жданов, с. 33.]

Криптографические методы защиты информации и их математическое обоснование – это фундаментальные исследования, которые связывают вместе области математики, информатики и физики. Методы из различных разделов математики, а именно арифметики, алгебры, теории вероятности, математические модели и другие, используются для создания и исследования различных шифров.

Шифрование в первую очередь опирается на алфавит, но как понять какой будет использоваться в конкретном случае. Универсальным языком, применяемым при использовании компьютерных технологий, является двоичный код, состоящий из двух элементов – «0» и «1». Простейшим переводом на двоичный код является побуквенная кодировка, n-ным количеством символов, вычисляемым по формуле:

$$2^n = p, \quad (1)$$

где p – размер исходного алфавита,

n – количество символов, выделяемых на каждую букву.

В русском языке 33 буквы, следовательно по формуле ближайшее число $n = 5$ символов двоичного кода. Тогда получится нужно привести исходный алфавит к 32 буквам, обычно исключают букву «Ё» и принимают «Ъ» и «Ь» за одну букву, добавляют пробел «_». Подставив к каждой букве исходного алфавита ее двоичное значение получим (Рисунок 9).

$$\_ \rightarrow 00000, А \rightarrow 00001, Б \rightarrow 00010, В \rightarrow 00011, Г \rightarrow 00100,$$

$$Д \rightarrow 00101, Е \rightarrow 00110, \dots, Ю \rightarrow 11101, Я \rightarrow 11111$$

Рис. 9. Пример перевод русского алфавита в двоичный код

Рассмотрим несколько формальных формальные моделей простых шифров. Простыми называют шифры замены и подстановки. Наиболее известными примерами шифров замены являются шифр Цезаря, азбука Морзе, «пляшущие человечки» А. Конан Дойля. Из названия ясно, что шифр замены реализует изменение букв или частей исходного текста в шифрованный. Достаточно просто дать математическое описание данному действию. Предположим, есть два алфавита X и Y, имеющие равное количество символов равное n; $g: X \to Y$ - взаимно однозначное отображение X в Y. В этом случает шифр замены работает следующим образом: исходный текст $x_1 x_2 \dots x_n$ преобразуется в шифрованный текст $g(x_1)g(x_2) \dots g(x_n)$.

Шифр перестановки реализует изменение перестановкой букв в исходном тексте. Известным примером шифра перестановки является Сцитало. Как правило исходный текст разбивается на отрезки равной длины, которые шифруются независимо друг от друга. Пусть имеется исходный текст X, разделенный на отрезки длиной n, Q - взаимно однозначное отображение множества $\{1, 2, \dots, n\}$ на себя. В таком случае шифр перестановки работает следующим образом: отрезок исходного текста $x_1 x_2 \dots x_n$ преобразуется в отрезок шифрованного.

Криптоанализ – наука о дешифровке зашифрованной информации. Современный криптоанализ основывается на следующих разделах математики: теория вероятности, математическая статистика, алгебра, теория числе, теория алгоритмов и другие. Криптоанализ развивается в четырех направлениях:

1. Статистический криптоанализ. Исследование вероятности взлома на основе изучения статистического анализа исходного и зашифрованного текстов.

2. Алгоритмический криптоанализ. Поиск математически слабых элементов криптографических систем.

3. Дифференциальный криптоанализ. Анализ зависимости изменения шифрованного текста при изменении исходного.

4. Линейный криптоанализ. Основан на поиске линейного приближения между исходным и шифрованным сообщениями.

Рассмотрим пример криптоанализа. Дешифрование шифров замены строится на следующих закономерностях:

- в осмысленных текстах естественных языков разные буквы встречаются с разной частотой;

- в любом естественном языке есть возможность «отгадать» сообщение даже если есть пропущенные буквы.

В таблице 5 приведена относительная частота появления букв в русском алфавите, состоящем из 32 букв, содержащих пробел.

Таблица 5

Относительная частота букв в русском алфавите

Буква	Относительная частота	Буква	Относительная частота
А	0,062	Р	0,040
Б	0,014	С	0,045
В	0,038	Т	0,053
Г	0,013	У	0,021
Д	0,025	Ф	0,002
Е, Ё	0,072	Х	0,009
Ж	0,007	Ц	0,004
З	0,016	Ч	0,012
И	0,062	Ш	0,006
Й	0,010	Щ	0,003
К	0,026	Ь, Ъ	0,014
Л	0,032	Ы	0,016
М	0,026	Э	0,003
Н	0,053	Ю	0,006
О	0,090	Я	0,016
П	0,029	пробел	0,175

Данные таблицы используются при криптоанализе шифров простой замены. В данном случае дешифровка происходит следующим образом: определяется частота букв зашифрованного текста и наиболее частые буквы

заменяются частыми буквами исходного алфавита и так далее по убыванию, пока не будет понятно содержание сообщения.

В криптографических шифрах с открытым ключом, таких как протокол Диффи-Хеллмана, алгоритмы RSA и DSA, ГОСТ 34.10-2018 и другие, для генерации секретных ключей, зачастую, применяется математический аппарат на основе диофантовых уравнений. Он заключается в поиске целочисленного решения линейного диофантового уравнения (2).

$$ax - by = c, \quad (2)$$

где $a, b, c \in Z$.

Рассмотрим его применение на примере. Протокол Диффи-Хеллмана предоставляет двум или более сторонам возможность получить общий секретный ключ по незащищенным каналам связи. Алгоритм действия протокола работает по следующему принципу:

1. Представим, что существуют два пользователя A и B, которым нужно создать общий секретный ключ. Пользователь A передает по открытому каналу связи B случайные величины g и p.

2. Оба пользователя генерируют большие случайные величины a и b, соответственно, данные числа являются закрытыми ключами.

3. Пользователи A и B вычисляют остаток од деления по формулам:

$$A = g^a mod\ p, \quad (3)$$

$$B = g^b mod\ p, \quad (4)$$

где p – случайное простое число,

g – простое число, являющееся первообразным корнем по модулю p,

A и B – открытые ключи,

a и b – закрытые ключи.

4. Полученные открытые ключи передаются другому пользователю. Но основе полученного открытого ключа и имеющегося закрытого ключа A и B вычисляют значения:

$$B^a mod\ p = g^{ab} mod\ p, \quad (5)$$

$$A^b mod\ p = g^{ab} mod\ p. \quad (6)$$

5. Можно заметить, что получившиеся в итоге ключи идентичны. Следовательно полученный секретный ключ имеет вид (7).

$$K = g^{ab} mod\ p. \quad (7)$$

В России существуют свои стандарты, регламентирующие использование криптографических технологий, применяемых для защиты информации в разных сферах жизнедеятельности. ГОСТ 34.10-2018 описывает алгоритмы формирования и проверки электронной цифровой подписи. Цифровая подпись позволяет определить авторство электронного документа. Данный алгоритм использует хеш-функцию, регулируемую стандартом ГОСТ 34.11-2012. Хэш-функция осуществляет перевод массива входных данных произвольной длины в выходную битовую функцию нужной длины. Рассмотрим простейшую хэш-функцию (8), в которой каждое число кодируется согласно таблице ASCII.

$$hash(s) = s_1 + s_2 + s_3 + \cdots + s_{n-1}, \quad (8)$$

где n – длина массива,

s – строка, в которой $s[i]$ – закодированное число исходного массива.

Мы рассмотрели случаи применения математических технологий в криптографии и можно сделать вывод, что все составляющие элементы криптографии имеют математическую основу или могут быть изучены с помощью математики.

ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ

Использование интеграции в образовании изучается уже многие годы и насчитывает множество исследований в области методики применения интеграции. Применение интеграции в школьном курсе позволяет организовывать системный подход к обучению, что положительно влияет не только на мыслительные процессы учеников, но и повышает мотивацию изучения одних предметов за счет интереса к другим.

При исследовании данной темы не было найдено материалов, описывающих применение криптографии как средства реализации межпредметных связей математики и информатики. Криптография напрямую связана с каждой из этих дисциплин. С одной стороны информатика является базой для изучения криптографии со стороны обеспечения информационной безопасности, с другой стороны математические средства являются основой для реализации и исследования большинства криптографических шифров.

Криптография является хорошей возможность применения интеграции математики и информатики. Следовательно, необходимо разработать модель интеграции математики на уроках информатики при изучении элементов криптографии. Модель должна содержать методы и средства обучения каждого из интегрированных предметов, а подбираемый материал соответствовать выбранной возрастной группе.

ГЛАВА 2. МЕТОДИЧЕСКИЕ ОСНОВЫ ИНТЕГРАЦИИ МАТЕМАТИКИ И ИНФОРМАТИКИ ПО ИЗУЧЕНИИ ЭЛЕМЕНТОВ КРИПТОГРАФИИ

2.1. МОДЕЛЬ ИНТЕГРАЦИИ МАТЕМАТИКИ И ИНФОРМАТИКИ ПРИ ИЗУЧЕНИИ ЭЛЕМЕНТОВ КРИПТОГРАФИИ

При исследовании в рамках выпускной квалификационной работы была разработана модель интеграции математики на уроках информатики при изучении элементов криптографии (Рисунок 10).

Рис. 10. Модель интеграция математики и информатики при изучении элементов криптографии

Для применения данной модели на уроках информатики надо понимать куда она будет внедряться. В соответствии с примерными программами обучения сложно будет вписать изучение нового материала в базовый курс информатики. Программа углубленного курса информатики для 10-11 классов в общем включает изучение следующих тем: информация и информационные процессы, устройство компьютера, моделирование, алгоритмы и программирование, базы данных, остальные темы в разных учебных программах варьируются. К изучению криптографии лучше всего подходить имея базу знаний в области программирования и моделирования, следовательно данный раздел лучше включать в конец программы 10 или середину 11 классов. В соответствии с примерными программами обучения сложно будет вписать изучение нового материала в базовый курс информатики

В поле криптографии заложены знания математики:

- Уравнения и функции: при решении задач криптографии необходимы умения преобразовывать и решать уравнения, использовать различные математические функции.

- Степени и корни: при генерации большинства ключей используются большие случайные числа, запись которых осуществляется в виде степеней, важно уметь преобразовывать степени уменьшения затрачиваемой вычислительной мощности.

- Элементы математической статистики: при криптоанализе важно уметь анализировать шифры с помощью методов статистики.

- Комбинаторика и вероятность: многие блочные криптосистемы используют вероятностные модели для генерации случайных ключей.

- Математическая логика: при шифровании текста, кодированного двоичным кодом, применяются действия из математической логики.

В поле криптографии заложены знания информатики:

- Информация является основным элементом криптографии, вокруг которого строятся алгоритмы защиты.

- Программное обеспечение: знание программного обеспечения позволяет более эффективно осуществлять защиту информации.

- Информационная безопасность: криптография является средством обеспечения информационной безопасности.

- Элементы теории алгоритмов: каждый криптографический шифр представляет собой определенный алгоритм, направленный на изменение информации.

- Программирование: современный криптографические системы являются компьютерным кодом, написанным на определённом языке программирования.

В федеральном государственном стандарте среднего общего образования обозначены знания, умения и навыки, которыми должны владеть ученики 10-11 классов. В таблице 6 представлены те из них, которые могут применяться при изучении элементов криптографии.

Таблица 6

Знания, умении и навыки математики и информатики по ФГОС СОО

Математика	Информатика
- иметь представление о необходимости доказательств; - уметь моделировать реальные системы, исследовать построенные модели; - знать основные понятия математического анализа; - уметь составлять вероятностные модели, применять формулы комбинаторики, исследовать случайные величины; - понимать аппарат: знать основные теоремы, формулы и уметь их применять; уметь доказывать теоремы и находить нестандартные решения.	- знать основные алгоритмы обработки числовой и текстовой информации, алгоритмов поиска и сортировки информации; - владеть языком программирования; - уметь строить математические объекты информатики, в том числе логические формулы; - знать устройство компьютерных сетей, нормы информационной этики и прав, принципы обеспечения информационной безопасности; - владеть опытом построения и использования компьютерно-математических моделей.

Опираясь на выявленные знания, умения и навыки математики и информатики, выделены необходимые для криптографии:

- знать: свойства информации, подлежащей сокрытию; виды шифров и их классификацию; методы криптографии и криптоанализа;

- уметь применять математические методы описания и исследования простейших криптографических систем;

- владеть навыками анализа простейших шифров; математического моделирования шифров.

Реализация межпредметных связей математики и информатики при изучении элементов криптографии осуществляется следующими средствами:

- математика: применение знаний математических понятий и их свойств, умений решать математические задачи в поставленных условиях; умений создавать математические модели алгоритмов шифрования; применять математические формулы при решении задач криптографии;

- информатика: примените программного обеспечения для компьютеризации шифрования; навыков поиска в сети Интернет для изучения информации необходимой для работы шифров; технических средств для облегчения работы.

При изучении элементов криптографии используются следующие методы обучения: объяснительно-иллюзорные, методы проблемного обучения, методы исследовательской деятельности, практические методы взятые из курсов математики и информатики.

2.2. РАЗРАБОТКА СОДЕРЖАНИЯ ИНТЕГРАЦИИ

Реализацию модели интеграции математики и информатики при изучении элементов криптографии на уроках информатики в классах с углубленным изучение математики лучше всего проводить после изучения основных блоков информатики, таких как программирование и моделирование.

Было разработано тематическое планирование по криптографии, где отмечены все темы, предлагаемые для изучения учащимся 10-11 классов (Таблица 7).

Таблица 7

Тематическое планирование внедрения элементов криптографии

Тема	Содержание
Введение	Основные понятия и определения. Виды защищаемой информации. Значение криптографии.
Древние шифры	Кодирование и сокрытие информации. Понятие о стеганографии. Простейшие шифры перестановки и замены.
Классификация шифров	Шифры замены, перестановки и гаммирования. Композиции шифров. Криптоанализ.
Компьютерные шифры	Первые компьютерные шифры. Поточные шифры. Криптография с открытым ключом.
Отечественное шифрование	История развития отечественной криптографии. Шифры Второй мировой войны.
Современная криптография	Современная криптография. Российские стандарты ГОСТ. Цифровая подпись.

Тема 1. Введение.

Цель: познакомить школьников с основными понятиями криптографии, с важностью защиты информации.

Задачи:

- изучить понятие криптографии;
- познакомиться с визами защищаемой информации;
- узнать важность криптографии.

Предлагаемые формы проведения урока: урок-лекция, урок-исследование, интегрированный урок с иностранным языком.

На данном уроке не используется интеграция с математикой, т.к. данный урок является вводным и несет цель выдать основные понятия, которые будут использоваться при дальнейшем изучении криптографии. Данный урок может быть организован в форме интегрированного урока с английским языком, знание которого очень важно при изучении программирования и криптографии.

В ходе данного урока школьники изучают основные понятия криптографии: криптология, криптография и криптоанализ; рассматривают виды информации, которую необходимо защищать: государственная тайна, юридическая тайна, врачебная тайна, тайна переписки и другое; дается понятие открытого и зашифрованного текстов, видов ключей: открытый, закрытый и секретный, для чего они нужны; поясняется разница между расшифрование и дешифрованием. Необходимо определить для учеников роль криптографии в жизни человека, важность информационной безопасности.

Тема 2. Древние шифры.

Цель: познакомить учеников с простейшими алгоритмами шифрования.

Задачи:

- вспомнить способы кодирования информации;
- рассмотреть методы стеганографии, простейшие шифры;
- научиться решать задачи по криптографии.

Форма проведения: на данном уроке интеграция математики вводится за счет применения знаний школьного курса при решении задач по криптографии.

Из поля математики в данной теме применяются методы решения задач, применения математических формул, умений преобразовывать и решать уравнения.

Из поля информатики используются средства преобразования систем счисления, программное обеспечение для изучения криптографии

Содержание интеграции:

Тема кодирования информации изучалась ранее на уроках информатики. Существует множество кодов применимых в тех или иных ситуациях, например, вся информация на компьютере хранится в двоичном коде, системы счисления изучались на уроках информатики в 8 классе. В школьных учебниках часто кодирование и шифрование представляют как тождественные определения, но это не так. Кодирование является преобразованием текста по общедоступной схеме, предназначено для практичного использования данных. Шифрование является преобразованием текста таким образом, чтобы только один человек мог вернуть ему исходный вид, предназначено для сохранения конфиденциальности сообщения. Необходимо дать понять ученикам четкое разделение данных понятий. На уроках криптографии речь будет идти именно о шифровании.

Стеганография, в отличие от криптографии, стремится полностью скрыть факт передачи сообщения. Современная стеганография применяется совместно с криптографией. Выделяют два вида стеганографии: классический и компьютерный. Примерами классических методов стеганографии являются книжный шифр и симпатические чернила. На примере симпатических чернил и их проявителей можно провести интегрированный урок с химией у среднего звена.

С появлением компьютерных технологий методов сокрытия информации стало еще больше. В целом большинство цифровых стеганографических методов основано на двух принципах. Во-первых, файлы, не требующие абсолютной точности (например, изображения, аудиоинформация и т. Д.), могут быть изменены до некоторой степени без потери функциональности. Во-вторых, отсутствие специальных инструментов или неспособность человеческого разума достоверно различать незначительные изменения в таких исходных файлах.

Простейшими шифрами называют древние шифры замены и перестановки. Шифры замены – это шифры основанное на замене каждого символа исходного текста. Простейшими шифрами являются одноалфавитные шифры Цезаря, Полибея, «Плещущие человечки», азбука Морзе и другие. Рассмотрим алгоритм работы с шифрами замены на примере шифра простой замены:

Для шифрования нам понадобится алфавит, на котором будет происходить шифрование равный длине алфавита исходного текста, примеры таблиц замены можно увидеть на рисунке 11.

А	Б	В	Г	Д	Е	Ё	Ж	З	…	Э	Ю	Я
П	Л	Е	К	З	М	Ы	Ч	Г	…	В	У	Ь

Пример замены символов на другие буквы того же алфавита.

А	Б	В	Г	Д	Е	Ё	Ж	З	…	Э	Ю	Я
33	17	8	16	2	15	14	12	73	…	37	39	18

Пример замены символов на числа

Рис. 11. Примеры таблиц замены

Каждый участник имеет одинаковую таблицу замены. Шифрование происходит путем замены каждого символа текста символом из таблицы. Для расшифрования шифра замены достаточно применить алгоритм шифрования в обратном порядке.

Шифр перестановки изменяет порядок символов в тексте, не преображая их. Каждое преобразование шифра задается с помощью таблицы, по формуле (9). В верхней строке таблицы стоят номера от 1 до n, а во втором ряду те же числа, но в произвольном порядке.

$$\begin{pmatrix} 1\ 2 \dots n \\ i_1\ i_2 \dots i_n \end{pmatrix}, \tag{9}$$

где n – длина сообщения.

Зная перестановку, можно как зашифровать текст, так и расшифровать. Самым известным примером шифра перестановки является Сцитало, палочка на которую наматывалось сообщение таким образом, что не имея палки того же диаметра его было невозможно расшифровать.

Рассмотрим примеры задач на криптографию.

Задача 1.

Было получено зашифрованное сообщение: HFPSHJB, известного алгоритма шифрования. К порядковому номеру каждой буквы было добавлено значение многочлена (10).

$$\mathrm{f}(x) = x^6 + 5x^5 + 4x^4 + x^3 + 6x^2 + 9x + 5. \tag{10}$$

Известно, что один из корней квадратного уравнения: $y = x^2 + 5x + 4$, является ключом данного шифра. Расшифруйте сообщение.

Решение:

1. Раскладываем многочлен на множители: $f(x) = (x^2 + 5x + 4)(x^4 + x + 1)$

2. Решаем квадратное уравнение: $y = x^2 + 5x + 4$. Корни данного уравнения равны -4 и -1.

3. Подставляем найденные корни в многочлен и находим значение $f(x) = 1$. Следовательно сдвиг порядковых номеров равен 1.

4. Определяем порядковые номера зашифрованного текст: 8 6 16 19 8 10 2, отнимаем от каждого порядкового номера $f(x) = 1$ и получаем: 7 5 15 18 8 9 1.

5. Преобразуем полученную последовательность цифр в тест: GEORGIA.

Задача 2.

Сообщение было записано в решетку 5x4 слева направо, затем было выписано снизу вверх сначала пятый столбик, потом третий, четвертый, первый и второй. Получилось зашифрованное сообщение: ЛИВРОТЕЕЬКТСБЕАВЫ. Расшифруйте сообщение.

Решение:

1. Составим решетку заданного размера, где отметим слева направо 17 клеток, длина сообщения (Рисунок 12).

1	2	3	4	5

Рис. 12. Решетка перестановки.

2. Разделим зашифрованное сообщение с учетом закрашенных клеток и порядка выписывания символов: ЛИВ РОТ ЕЕЬ КТСБ ЕАВЫ.

3. Записываем зашифрованное сообщение обратно в решетку в том же порядке. Можно увидеть исходное сообщение слева направо. (Рисунок 13.)

1	2	3	4	5
Б	Ы	Т	Ь	В
С	В	О	Е	И
Т	А	Р	Е	Л
К	Е			

Рис. 13. Исходное сообщение.

Исходное сообщение: БЫТЬ В СВОЕЙ ТАРЕЛКЕ.

Тема 3. Классификация шифров.

Цель: изучить методы дешифровки шифров замены.

Задачи:

- познакомиться с шифрами гаммирования;

- научиться использовать частотный криптоанализ.

Форма проведения: интеграция математики проявляется в использовании элементов статистики для дешифровки текста, создания математических моделей шифров.

Из поля математики берутся знания в области статистики, умений строить математические модели.

Из поля информатики используются средства редактирования информации.

Содержание интеграции:

Шифр гаммирования – это шифр многоалфавитной замены. Суть шифра заключается в сложении каждого элемента исходного текста с элементом ключа по модулю равному длине алфавита. Общая классификация шифров представлена на рисунке 8.

Криптоанализ занимается дешифрованием зашифрованных текстов без знания ключа. Для этого необходимо понимание работы алгоритмов

шифрования, в этих целях ученикам дается задание: построить математические модели простейших шифров.

Для получения исходного текста в шифрах применяются различные алгоритмы вскрытия шифров, опирающие на атаки на разные составляющие шифрования. Частотный криптоанализ основывается на предположении, что существует определенная частота появления отдельных символов в тексте. Предлагается следующий план частотного криптоанализ, применимый на уроке информатики:

1. Ученикам дается несколько текстов, по которым они должны определить частоту появления каждой буквы русского алфавита. Они вычисляют средние значения для каждого из текстов и сравнивают получившиеся значения с эталонным образцом из таблицы 4.

2. Ученикам выдаются зашифрованный шифром замены текст. Они должны определить частоту каждой буквы алфавита шифрования и заменить наиболее часто встречаемые буквы данного алфавита на буквы русского алфавита от большего к меньшему.

3. Изменений текст проверяется на читабельность, если текст прочитать невозможно, то буквы подстановки меняются. Обычно для ускорения работы, замену символов проводят на выборочном, достаточно длинном, слове.

Тема 4. Компьютерные шифры.

Цель: познакомить учеников с асимметричными шифрами.

Задачи:

- рассмотреть принцип работы алгоритма асимметричного шифрования;
- научиться создавать общий секретный ключ протокола Диффи-Хеллмана.

Форма проведения: реализация межпредметных связей осуществляется за счет исследования криптографических алгоритмов.

Из поля математики используются знания действий со степенями, вычисление остатка от деления, применение математических теорем и функций.

Из поля информатики применяются умения строить алгоритмы шифрования.

Содержание интеграции:

Во время первой мировой войны широкое распространение получили шифры использующие компьютерные технологии. В начала первой мировой воны Великобритания отключила подводные кабели Германии, создавая необходимость в использования международных кабелей. Тогда Германия стала шифровать свои сообщения, чтобы избежать перехвата информации.

Клод Шеннон разработал следующие требования к абсолютно стойким шифрам: длина ключа должна быть равна длине текста, ключ должен использоваться только один раз. Но осуществление данных требований очень затратно. По такому принципу работает одноразовый блокнот, в котором шифрование представляет собой сложение по модулю 26 (английский алфавит), 33 (русский алфавит) символа открытого текста и символа ключа одноразового блокнота, после шифрования блокнот с ключом уничтожался.

Существуют две криптосистемы: симметричные и асимметричные. В симметричных криптосистемах для шифрования и расшифрования использовался один ключ, все ранее рассмотренные шифры относились к данной криптосистеме. Главным недостатком симметрических шифров было распространение ключей, оно требовало наличие конфиденциальной передачи ключа, что не всегда было доступно.

В 1976 г. У. Диффи и М. Хеллман разработали общие принципы работы криптографии с открытым ключом, они заключались в следующем: при шифровании использовалось два ключа: открытый ключ, на котором будет шифроваться сообщение, являлся общедоступным; закрытый ключ, используемый для дешифровки, известен только законному получателю информации.

Был разработал протокол Диффи-Хелмана позволяющий двум или более людям получить один и тот же секретный ключ. Он работает по принципу передачи открытого ключа и преобразованию его с обоих сторон для получения одинакового результата. Работа с данным протоколом рекомендована для

отработки в парах, где каждая пара генерирует секретные ключи с общим открытым ключом для всего класса.

Преобразование ключей происходит по формуле:

$$K = A\ mod\ m, \quad (11)$$

где m – простое число,

A – случайное большое число.

Как же нам найти остаток от деления 2^{100} на 13. Проведем некоторые преобразования: $2^{100} = 2^4 * 2^{96} = 16 * (2^{12})^8$. Утверждается, что $16 * (2^{12})^8\ mod\ 13 = 16\ mod\ 13 = 3$, но как это было получено. Оказывается, что $2^{12} mod\ 13 = 1$. Для этого используют малую теорему Ферма, которая является главной основой всех ключей шифрования. Она утверждает следующее:

$$a^{p-1} mod\ p = 1, \quad (12)$$

где p – простое число,

a – целое число, такое что a не делится на p.

Первым полноценным протоколом с открытым ключом является RSA. Системы с открытым ключом работают по принципу: если известно x, то вычислить $f(x)$ легко, но если известно $y = f(x)$, то вычислить x потребует больших затрат и считается неэффективным. Процедура создания ключей RSA:

1. Выбираются два простых числа p и q и вычисляется их произведение n. Следует отметить, что p и q выбирают таким образом, чтобы n было больше любого кода открытого текста.

2. Вычисляется функция Эйлера $\varphi(n) = (p-1)(q-1)/$

3. Выбирается открытый ключ e – взаимно простое число с результатов функции Эйлера.

4. Вычисляется закрытый ключ d такой, что $(d * e) mod\ \varphi(n) = 1$.

Открытый ключ публикуется в таком канале связи, в котором его можно прочитать, но нельзя изменить. Процедура шифрования и расшифрования проходит по формулам (13) и (14) соответственно.

$$C = T^e mod\ n, \quad (13)$$

$$T = C^d mod\ n, \quad (14)$$

где Т- открытый текст,

С – зашифрованный текст.

Тема 5. Отечественные шифры.

Цель: познакомить школьников с отечественными разработками в области криптографии.

Задачи:

- знакомство с отечественными шифрами;

- изучение шифров Второй мировой войны.

Форма проведения: данная тема может изучаться в форме урока-исследования. Межпредметные связи с математикой не используются. Можно организовать интегрированный урок с историей при прохождении событий Второй мировой войны.

Тема 6. Современные шифры.

Цель: дать основные сведения о современных криптографических алгоритмах.

Задачи:

- знакомство с отечественными стандартами шифрования;

- изучение работы Цифровой подписи.

Форма проведения: использование вычислительных навыков для работы с понятием цифровой подписи.

Из поля математики применяются вычислительные навыки при нахождении криптографических функция.

Из поля информатики используется умения строить алгоритмы работы шифрования.

Содержание интеграции:

На сегодняшний день криптографические методы защиты информации используют в большинстве сфер жизни: обеспечение безопасности банковских систем, пластиковых карт, банкоматов; электронных изданий; беспроводных устройство и других. Но к криптография используется не только для

шифрования данных, с целью сохранения конфиденциальности, но и для обеспечения аутентификации и целостности.

Электронно-цифровая подпись - современный метод подтверждения подлинности владельца информации, отвечает за целостность передаваемых данных. Цифровая подпись чаще всего использует асимметричное шифрование с открытым ключом, имеет цифровой идентификатор, выдаваемый аккредитованным центром сертификации. Формирование и проверка электронно-цифровой подписи регламентируется российским стандартом ГОСТ 34.10-2018.

Работа цифровой подписи обеспечивается за счет хэширования данных. Хэш-функция не использует ключи шифрования, она преобразовывает большой объем данных в двоичный код заданной длины, который трудно скопировать. Каждый хэш уникален для исходного текста, если текст изменится, то создастся новый хэш. Наиболее простым примером хэш-кода будет являться остаток от деления количества входных данных на количество выходных данных $h(k) = k \; mod \; M$.

Было разработано несколько методов защиты паролей и цифровых подписей от фальсификации. Одним из таких методов является добавление криптографической «соли», случайного набор символов к хэш-коду. Добавление случайных данных значительно затрудняет анализ полученных хэш-таблиц.

2.3. ПЕДАГОГИЧЕСКИЙ ЭКСПЕРИМЕНТ И ЕГО РЕЗУЛЬТАТЫ

Педагогический эксперимент состоял из двух частей: актуализация исследования и частичная апробация разработанной модели. Необходимо было изучить педагогических опыт использование интеграции на уроках. Были опрошены 5 учителей, трое учителя математики и двое учителя гуманитарного цикла. В результате были сделаны следующие выводы:

- Применение технологий интеграции зависит от опыта преподавателя. Молодые специалисты применяют интеграцию в редких случаях, например при проведении открытых уроков.

- Интеграция в островном осуществляется со смежными предметами: математика-информатика, математика-физика, обществознание-история, литература-история.

- Возможность применения информационных технологий для обучения детей полностью зависит от возможностей школы.

Согласно информации администрации школы, на базе которой проходило исследование, интеграция применяется практически на всех предметах как внутрипредметная, так и межпредметная. Также разработаны специальные модули интегрированного обучения, например модуль «Математическая логика». Но применение интеграции с информатикой происходит только в части применения некоторых цифровых технологий.

Основными технологиями, которые применяли при интеграции математики и информатики учителя-предметники назвали:

- использование игр и специальных программ для обучения детей математике;

- организация исследовательской детальности с созданием учениками презентаций и защита их;

- применение дистанционных методов интеграции: онлайн-тесты, онлайн-занятия.

В школе, на базе которой проходило исследование, была проведена частичная апробация разработанной модели, были проведены несколько занятия по криптографии. Эксперимент проводился в 2020-2021 учебном году в рамках внеурочной деятельности. И проанализированы их итоги. Во-первых, была проведена первичная проверка знаний учащихся. Во-вторых, была проведена оценка отношения обучавшихся к интегрированному занятию и возможности дальнейшего изучения этой темы.

Сначала необходимо было понять какие знания в области информационной безопасности и, в частности, криптографии имеются у школьников. Были заданы следующие вопросы:

1. Знаете ли вы, что такое криптография?
2. Какие алгоритмы шифрования вы изучали?
3. Какие методы защиты информации вы знаете?

Большинство учеников ответило, что раньше проходили шифрование, но точных определений дать не могли, пятеро вспомнили названия шифров, пятеро назвали определение криптографии, трое человек не ответило ни на один вопрос (Рисунок 14).

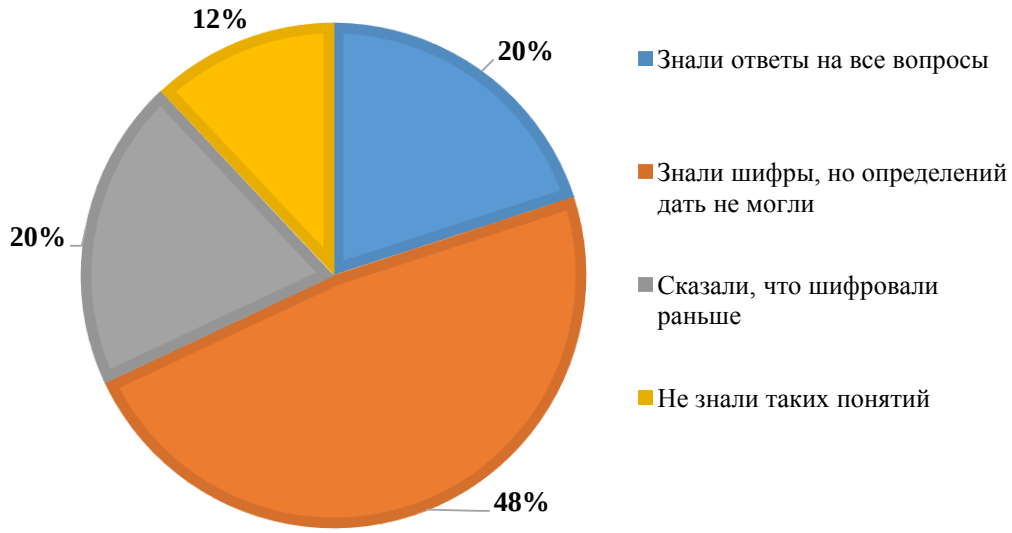

Рис. 14. Знания учащихся в области криптографии (n = 25)

Учеников просили оценить заинтересованность в дальнейшем обучении элементам криптографии по пятибалльной шкале, итоги оценки предоставлены на рисунке 15.

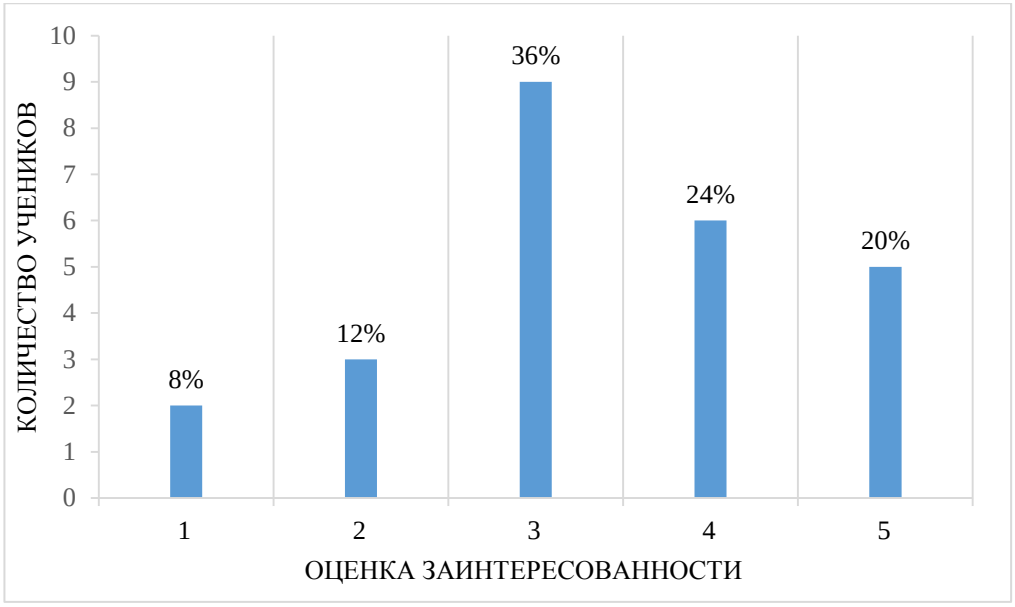

Рис. 15. Оценка заинтересованности школьников в изучении элементов криптографии (n = 25)

Проанализировав ответы учеников и их оценку заинтересованности, было замечено, что ученики, не ответившие ранее на вопросы, поставили самые низкие оценки заинтересованности. Многие отмечали, что практическое применение алгоритмов шифрования их заинтересовало, но с теорией возникали проблемы.

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

В результате исследования в рамках выпускной квалификационной работы было была разработана модель интеграции математики и информатики при изучении криптографии, которую модно применить на уроках информатики. В содержание модели используется изучение элементов криптографии методами и средствами математики и информатики. Материалы подбирались таким образом, чтобы при изучении каждой темы использовались различные математические методы решения задач криптографии. Содержание может варьироваться в зависимости от доступных часов на изучение элементов криптографии, возможности применения интеграции с другими предметами.

В рамках педагогического эксперимента была исследована тема использования технологи интеграции учителями на примере школы, на базе которой проходили исследования. Были проведены занятия по криптографии для 10-11 классов в рамках внеурочной деятельности. После апробации было проведено исследование заинтересованности школьников в дальнейшем изучении элементов криптографии на уроках информатики.

ЗАКЛЮЧЕНИЕ

Исследуя тему выпускной квалификационной работы, была изучен литература в сфере интеграции и применения межпредметных связей. Выявленные принципы интеграции и применение их в системе образования показали важность применения межпредметных связей для системного обучения и развития учеников. Изучение возможностей применения межпредметных связей математики и информатики привело нас к идее реализации данных связей через изучение элементов криптографии. Криптография соединяет в себе знания защиты информации и математическими методами осуществления этого.

Изучая школьные учебники по информатике, было выявлено, что на изучение темы информационной безопасности в них уделяется очень мало времени. Однако развитие информационной культуры школьников является основополагающей в современном мире, следовательно возникла необходимость введения дополнительного материала.

Была разработана модель интеграции математики и информатики при изучении криптографии, включающая применение их методов и средств при решении задач криптографии. По мере возможности, для каждой темы содержания модели применялись разные подходы к интеграции.

Проведение педагогического эксперимента проходило в два этапа. Во-первых, был изучен педагогический опыт применения технологий интеграции на базе школы. Во-вторых, было проведено частичное внедрение разработанной модели, на базе МАОУ СОШ № 48. Апробация происходила в рамках внеурочной деятельности, ученикам был выдан материал по криптографии и проведена оценка заинтересованности в дальнейшем изучении на уроках информатики.

Таким образом все поставленные задачи были решены, цель выпускной квалификационной работы выполнена. Результатом является модель интеграции, которая в дальнейшем может использоваться учителями для обучения школьников элементам криптографии.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) Аминов И. Б., Кадитов Т. Формирование информационной компетентности учителей математики с применением межпредметных связей информатики и математики // Вестник науки и образования, 2019, № 22(76), С. 47-49. URL: https://cyberleninka.ru/article/n/formirovanie-informatsionnoy-kompetentnosti-uchiteley-matematiki-s-primeneniem-mezhpredmetnoy-svyazi-informatiki-i-matematiki/viewer (дата обращения: 26.11.2019)

2) Андреева Е.В., Босова Л.Л., Фалина И.Н. Математические основы информатики. Элективный курс: Учебное пособие. Москва: БИНОМ. Лаборатория знаний, 2005. 328с.

3) Арзяева Н.А., Горячева К.Г. Элементы криптографии в школьном курсе математики [Электронный ресурс] / Красноярский государственный педагогический университет им. В.П. Астафьева. Электрон. текстовые дан. 2017. URL: http://arbir.ru/miscellany/U18S878E56908-Элементы-криптографии-в-школьном-курсе-математики (дата обращения: 24.02.2021)

4) Афанасьева И.А. Реализация межпредметных связей как одно из направлений повышения качества образования. Москва: Книжный мир, 2002. 457 с.

5) Борисов В.В. Интеграция образования и науки: ее смысл и способы воплощения. Проблемы развития науки в России. 2010. С. 157-169. URL: https://riep.ru/upload/iblock/ee6/ee6c47f8165ef4e6fdc2dda9085e3155.pdf (дата обращения: 12.05.2021)

6) Волошенко Л. Н. Межпредметные связи на уроках информатики // По материалам семинара, 2009.

7) Глинская Е.А., Титова С.В. Межпредметные связи в обучении. 3-е изд. Тула: Инфо, 2007. 44 с.

8) Гурьев И.И. Межпредметные связи в системе современного образования. Москва: Владос, 2002. 632 с.

9) Дегтерев В.А. Интеграция в системе непрерывной подготовки специалистов социальной сферы. // Современные проблемы науки и

образования. 2012. Раздел 3. URL: https://www.science-education.ru/pdf/2012/3/6490.pdf (дата обращения: 28.02.2020)

10) Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. Москва: ТЭИС. 1994.

11) Доронина А.В., Канушина Ю.Н. Использование математики в криптографии. // Юный ученый. 2019. № 4 (24). С. 28-31. URL: https://moluch.ru/young/archive/24/1421/ (дата обращения: 06.03.2021)

12) Дьячук П.П. Условия и принципы интеграции школьных курсов алгебры и информатики // Вестник Красноярского государственного педагогического университета им. В.П. Астафьева. 2014. № 2. С. 62-66. URL: https://cyberleninka.ru/article/n/usloviya-i-printsipy-integratsii-shkolnyh-kursov-algebry-i-informatiki/viewer (дата обращения: 08.12.2020)

13) Заикина Н.А. Межпредметные связи математики с предметами естественнонаучного цикла // Педагогические науки. 2012. № 5(5). С. 34-36. URL: https://research-journal.org/pedagogy/mezhpredmetnye-svyazi-matematiki-s-predmetami-estestvennonauchnogo-cikla/ (дата обращения: 06.03.2021)

14)Зверев И.Д., Максимов В.Н. Межпредметные связи в современной школе. 2-е изд. Москва: Педагогика. 2006. 195 с.

15) Жданов О.Н., Золотарев В.В. Методы и средства криптографической защиты информации: учебное пособие. Красноярск: СибГАУ. 2007. 217 с.

16) Касумова А.М. Интегрированное обучение на уроках математики и информатики // Вестник университета. 2014. № 21. С. 26-28. URL: https://cyberleninka.ru/article/n/integrirovannoe-obuchenie-na-urokah-matematiki-i-informatiki/viewer (дата обращения: 26.11.2019)

17) Кедров Б. М. О синтезе наук // Вопросы философии. 1973. № 3. С. 81-85.

18) Клименкова Г.Н. Основы информационной безопасности: правовой аспект в воспитании школьников // Социальная педагогика. 2013. №6. С. 33-40.

19) Клочкова Н.Н. Использование межпредметных связей на занятиях по информатике (Электронный ресурс) URL:

https://znanio.ru/media/ispolzovanie_mezhpredmetnyh_svyazej_na_zanyatiyah_po_informatike-258068 (Дата обращения: 26.03.2021)

20) Козлов О.А., Михайлов Ю.М. Управление формированием индивидуальной траектории курсантов военных вузов с использованием информационных технологий. Военная подготовка. Москва: Проспект. 2017.

21) Коробейников А.Г. Гатчин Ю.А. Математические основы криптографии. Учебное пособие. Санкт-Петербург: СПб ГУ ИТМО. 2004. 106 с.

22) Кубасов О.П. Интеграция в образовании: сущностная характеристика // Казанский педагогический журнал. 2008. № 10. С. 70-77. URL: https://cyberleninka.ru/article/n/integratsiya-v-obrazovanii-suschnostnaya-harakteristika (дата обращения: 28.02.2020)

23) Кузнецова В.Ю. Обеспечение компетентности российских школьников в вопросах криптографии: анализ целей, возможных подходов и технологий, средств их программной поддержки // Прикаспийских журнал: управление и высокие технологии. 2019. №2. С. 163-170. URL: https://www.elibrary.ru/item.asp?id=39168828 (дата обращения: 28.10.2020)

24) Кукушин В.С. Педагогические технологии: Учебное пособие для студентов педагогических специальностей. Ростов-на-Дону: МарТ. 2006. 336 с.

25) Левченко И. В., Карташова Л. И. Задачи межпредметного характера как средство развития познавательной мотивации старшеклассников на уроках информатики // Информационные технологии в науке и образовании: Сборник научных трудов. Воронеж: Научная книга. 2009. С.68–73. URL: https://cyberleninka.ru/article/n/kriterii-otbora-zadach-mezhpredmetnogo-haraktera-i-ih-reshenie-v-protsesse-obucheniya-informatike-s-tselyu-razvitiya-poznavatelnoy/viewer (дата обращения: 26.11.2019)

26) Лернер И.Я. Содержание межпредметных связей и пути их реализации // Межпредметные связи в процессе преподавания основ наук в средней школе: Тезисы докладов Всесоюзной конференции. Москва. 1972. 221 с.

27) Леченко И. В., Карташова Л. И. Использование межпредметных связей информатики для развития познавательной мотивации старшеклассников //

Вестник Российского университета дружбы народов. Серия: Информатизация образования. 2010. № 1. С. 35-40. URL: https://cyberleninka.ru/article/n/ispolzovanie-mezhpredmetnyh-svyazey-informatiki-dlya-razvitiya-poznavatelnoy-motivatsii-starsheklassnikov/viewer (дата обращения: 08.12.2020)

28) Лиферон А.П. Интеграция мирового образования - реальность третьего тысячелетия. Москва: Педагогика, 1997.

29) Лошкарева Н.А. О понятии и видах межпредметных связей // Советская педагогика. 1972. № 6(53). 165 с.

30) Максимова В.Н. Интеграция в системе образования. Санкт-Петербург: ЛОНРО. 2000. 83 с.

31) Максимова В.Н. Межпредметные связи и совершенствование процесса обучения: Книга для учителя. Москва: Просвещение. 2012. 754 с.

32) Маскаева Т.А., Баляйкина В.М., Лабутина М.В. Межпредметные связи как принцип интеграции обучения. // Современные проблемы науки и образования. 2019. № 6. URL: https://www.science-education.ru/ru/article/view?id=29320 (дата обращения: 26.03.2020)

33) Наумова Е.И. Реализация требований ФГОС при изучении курса внеурочной деятельности «Основы криптологии» // Актуальные проблемы гуманитарных и естественных наук. 2017. № 8. С. 125-126. URL: https://cyberleninka.ru/article/n/realizatsiya-trebovaniy-fgos-pri-izuchenii-kursa-vneurochnoy-deyatelnosti-osnovy-kriptologii/viewer (дата обращения: 28.10.2020)

34) Нефедов Д.Е. Об интеграции содержания школьных предметов математики и информатики // Ярославский педагогический вестник. 2015. № 2. Том 2 С. 34-38. URL: https://cyberleninka.ru/article/n/ob-integratsii-soderzhaniya-shkolnyh-predmetov-matematiki-i-informatiki/viewer (дата обращения: 19.03.2021)

35) Носков М.В., Попова В.В. Реализация межпредметных связей математики и информатики в современном учебном процессе // Вестник Красноярского государственного педагогического университета им. В.П. Астафьева. 2015. № 1. С. 65-68. URL: https://cyberleninka.ru/article/n/realizatsiya-

mezhpredmetnyh-svyazey-matematiki-i-informatiki-v-sovremennom-uchebnom-protsesse/viewer (дата обращения: 19.03.2021)

36) Поляков К.Ю., Еремин Е.А. Информатика. Углубленный уровень. Учебник для 10 класс. Москва: БИНОМ. Лаборатория знаний, 2013. 304с.

37) Поляков К. Ю., Еремин Е. А. Информатика. Углубленный уровень. Учебник для 11 класса. Москва: БИНОМ. Лаборатория знаний, 2013. 310с.

38) Потешкина Г.В. Приемы и методы повышения мотивации учащихся при изучении предмета «информатика» // Проблемы педагогики. 2016. № 12. С. 65-69. URL: https://cyberleninka.ru/article/n/priemy-i-metody-povysheniya-motivatsii-uchaschihsya-pri-izuchenii-predmeta-informatika/viewer (дата обращения: 28.02.2020)

39) Рагулина М.И. Тенденции развития математического образования в условиях перехода к информационному обществу // Вестник Эжно-Уральского государственного гуманитарно-педагогического университета. 2008. №10. С. 83-92. URL: https://cyberleninka.ru/article/n/izmenenie-paradigmy-matematicheskogo-obrazovaniya-v-usloviyah-informatizatsii/viewer (дата обращения: 08.12.2020)

40) Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии Москва: Горячая линия-Телеком, 2010. – 232с.

41) Сабурова Д.А. Интеграция информатики с другими предметами школьного курса //Информационно-коммуникационные технологии в образовании (ИКТО-Архангельск-2010): материалы Всероссийской научно-практической конференции.

42) Сухаревская Е.Ю. Технология интегрированного урока. Ростов-на-Дону: Изд-во «Учитель», 2003. 128 с.

43) Усова А.В. Решение проблемы использования межпредметных связей в условиях стандартизации образования. Горно-Алтайск: ГАГУ. 2014. С. 27-30

44) Факторович А.А. Педагогические технологии: учебное пособие для академического бакалавриата. Москва: Издательство Юрайт. 2019. 128 с.

45) Федеральный образовательный стандарт среднего общего образования [Электронный ресурс] // Федеральные образовательные стандарты М.: Институт

стратегических исследований в образовании РАО. URL: https://fgos.ru/ (Дата обращения: 10.05.2021)

46) Федорец Г.В. Межпредметные связи в процессе обучения. Ленинград: ЛГПИ им. А.И. Герцена. 1983. 88 с.

47) Федорова В.Н., Кирюшин Д.М. Межпредметные связи. Москва: Педагогика. 1972. 446с.

48) Хангельдиева И.Г. О понятии "информационная культура" // Информационная культура личности: прошлое, настоящее, будущее: Междунар. науч. конф. Краснодар: Тез. докл. 1993.

49) Хасанов А.А., Маматкаримов К.З. Межпредметные связи как дидактическое условие повышения эффективности учебного процесса // Молодой ученый. 2016. № 20 (124). С. 738-741. URL: https://moluch.ru/archive/124/33275/ (дата обращения: 20.05.2020).

50) Чухина Е.В. Интеграция образования: сущность, современные интегративно-педагогические концепции. // Педагогическая наука и практика. 2015. №1(7). С. 58-63 URL: https://cyberleninka.ru/article/n/integratsiya-obrazovaniya-suschnost-sovremennye-integrativnopedagogicheskie-kontseptsii (дата обращения: 28.02.2020)

51) Криптографическая защита информации: учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. Тамбов: Изд-во Тамб. гос. тех. ун-та. 2006. 140 с.

52) Ятайкина А.А. Об интегрированном подходе в обучении // Школьные технологии. 2001. №6. С. 10–15. URL: https://old.altspu.ru/Journal/vestnik1/ARHIW/N2_2002/nauch_konf/4_sekz/yataikina/yataikina.pdf (дата обращения: 26.11.2019)