

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Балашовский институт (филиал)

Кафедра математики, информатики, физики

**МЕТОДИКА ИЗУЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В  
КУРСЕ ИНФОРМАТИКИ ОСНОВНОГО И СРЕДНЕГО ОБЩЕГО  
ОБРАЗОВАНИЯ**

**АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ**

студентки 5 курса 151 группы  
направления подготовки 44.03.05 «Педагогическое образование с двумя  
профилями подготовки»,  
профили «Математика и информатика»,  
факультета математики и естественных наук  
Аксеновой Анастасии Александровны

Научный руководитель  
доцент кафедры математики,  
информатики, физики \_\_\_\_\_ М. Ю. Грибанова-Подкина  
(подпись, дата)

Зав. кафедрой математики, информатики, физики  
кандидат педагогических наук,  
доцент \_\_\_\_\_ Е.В. Сухорукова  
(подпись, дата)

**Балашов 2021**

## ВВЕДЕНИЕ

**Актуальность исследования.** В школьном курсе информатики изучению информационной безопасности уделяется достаточно много времени. Знакомство с данным понятием начинается в 7 классе, далее понятие расширяется и углубляется. Важно вооружить обучающихся знаниями информационной безопасности, ведь проблема обеспечения информационной безопасности в Интернете все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

В современных условиях информационные технологии стали неотъемлемой частью нашей жизни. Между тем существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для детей угрозу.

**Цель работы** – разработать методическое сопровождение по теме «Информационная безопасность».

Для достижения цели поставлены следующие **задачи**:

1. Рассмотреть теоретические основы обучения информационной безопасности школьником в школьном курсе информатики 7-11 классов.
2. Проанализировать УМК по изучению информационной безопасности 7-11 классах.
3. Осуществить разработку методического сопровождения изучения информационной безопасности в школьном курсе информатики.

**Объект исследования** – изучение информационной безопасности в основной и старшей школе.

**Предмет исследования** – методическое сопровождение темы «Информационная безопасность» в курсе информатики основной и старшей школы.

**Практическая значимость исследования** заключается в том, что материалы бакалаврской работы могут быть использованы на уроках информатики при изучении темы «Информационная безопасность», во внеурочной деятельности при подготовке учеников к олимпиадам и конкурсам по информатике.

Методами теоретического и практического исследования работы послужили: анализ, сравнение, обобщение.

Бакалаврская работа состоит из введения, трёх глав, заключения, списка использованных источников и 2 приложений.

## **ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ**

**В первой главе** «Теоретические основы содержания обучения информационной безопасности в школьном курсе информатики» представлены теоретические основы обучения информационной безопасности, а также рассмотрен правовой уровень обеспечения информационной безопасности.

Информационная безопасность – это набор методов и действий, ориентированных на защиту от несанкционированной деятельности против данных. Информация – это сведения, передаваемые устно и письменно с помощью знаков, технических механизмов, жестов, программ. Информация и ее принципы все еще изучаются экспертами для повышения эффективности хранения и использования данных.

Информационной безопасностью является система методов, которая помогает в защите технологий, обеспечивающих кибербезопасность внутри государства или компании.

В систему основных составляющих информационных данных входят:

Доступность – это состояние информации, позволяющее субъектам, имеющим право доступа, беспрепятственно её реализовывать. Исключением

являются данные, скрытые от всеобщего обозрения, разглашение которых может нанести серьезный ущерб субъектам и информации.

Целостность – один из элементов информации, гарантирующий ее стабильность при намеренном (ненамеренном) преобразовании или уничтожении определенных данных. Она бывает статической (стабильность основных объектов от первоначального состояния) и динамической (точная реализация последовательных действий). Если будет нарушено единство информации, это может привести к серьезным негативным последствиям. Эта характеристика является основной и актуальной в информационном пространстве.

Конфиденциальность – основное свойство, разрешающее доступ к информации исключительно юридически правомочным субъектам: клиентам, платформам (программам), процессам. Конфиденциальность – это самый исследованный, проработанный аспект ИБ.

Составляющие информационной безопасности не могут функционировать без соблюдения основных принципов, к которым относятся: простота использования, контроль за операциями, разграничение доступа.

Процесс защиты информации является многогранным, сложным, требует много сил со стороны правительства, компаний, граждан. Сохранением безопасности в информационной сфере необходимо заниматься постоянно, на законодательном уровне. Специалисты обязаны следить за процессом, являющимся ключевым в моментах сохранности, надежности и конфиденциальности данных. Должны реализовываться меры предосторожности, защиты от утечки и утраты информации всевозможными способами, так как, попадая в чужие руки, она может быть использована против личности или государства.

Несмотря на то, что в образовательных стандартах, как для основной, так и для старшей школы явным образом указано понятие «информационная безопасность», в школьных учебниках информатики авторы, как правило,

определяют и концентрируют внимание обучающихся на термине «защита информации», который в школьном стандарте в явном виде не приводится. Этот термин упоминается только в примерной программе для основной школы применительно к средствам защиты личной информации и примерной учебной программе по предмету «Информатика и ИКТ» применительно к защите от вредоносного программного обеспечения и защите персональных данных.

В обеспечении информационной безопасности успех может принести только комплексный подход. Для защиты интересов субъектов информационных отношений необходимо объединить меры следующих уровней: законодательные; административные (приказы и другие меры руководства организаций, связанных с охраняемыми информационными системами); процессуальные (меры безопасности, ориентированные на людей); программно-технические.

Законодательные меры в сфере информационной безопасности направлены на формирование в стране законодательной базы, которая ужесточает и регулирует поведение субъектов и объектов информационных отношений, а также определяет ответственность за нарушение установленных норм.

Основными документами по информационной безопасности в Российской Федерации являются Конституция Российской Федерации и понятие национальной безопасности.

**Во второй главе** «Анализ УМК по изучению информационной безопасности в 5-9 классах», рассмотрены учебники следующих авторов: Семакина И.Г. [и др.], Полякова К.Ю. [и др.], Босовой Л.Л. [и др.], Горячева А.В. [и др.].

Исследование показало, что изучение информационной безопасности в основном начинается в 7 классе, далее к этой теме возвращаются в курсе старшей школы.

Подробнее рассмотрим раскрытие темы в разных учебно-методических комплектах. Так в учебнике Семакина И.Г в 7 классе информационная безопасность представлена разделом: «Компьютер: устройство и программное обеспечение». На изучение данного раздела отводится 6 часов. Он включает в себя следующие темы: «Правила техники безопасности и эргономики при работе за компьютером», «Использование антивирусных программ».

Следующим учебно-методическим комплектом был рассмотрен под авторством Полякова К.Ю, в котором в курсе 7 класса вопросам информационной безопасности уделена в главе «Компьютер» тема «Защита от вирусов». В параграфе рассмотрены понятия компьютерного вируса, вредоносных программ, а также описан ряд признаков при заражении компьютера вирусом. Кроме того описаны типы вредоносных программ и антивирусных программ.

А в 7 классе в учебнике информатики Босовой Л.Л., Горячева А.В. данные вопросы раскрываются в разделе «Информация и информационные процессы» при изучении тем «Всемирная паутина как информационное хранилище» и в разделе «Компьютер как универсальное устройство для работы с информацией» в темах: «Программное обеспечение компьютера. Системное программное обеспечение», «Системы программирования и прикладное программное обеспечение».

В УМК Семакина присутствует отдельный практикум, который является отличным подспорьем при изучении материала.

В практикуме для 10 класса представлена работа 2.3. Шифрование данных:

Задание 1. Шифр Цезаря. Этот шифр реализует следующее преобразование текста: каждая буква исходного текста заменяет следующей после нее буквой в алфавите, который считается написанным по кругу.

Используя шифр Цезаря, зашифровать следующие фразы:

- а) Делу время – потехе час;

- b) С Новым годом;
- c) Первое сентября.

Задание 2. Используя шифр Цезаря, декодировать следующие фразы:

- a) Лмбттоьк шбт;
- b) Вёмпё тпмочё рфтуьой.

Задание 3. Шифр Виженера. Этот шифр Цезаря с переменной величиной сдвига. Величину сдвига задают ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв исходного текста: 3 1 9 1 3 1 9 1 и т. д. Используя в качестве ключевого слово ЗИМА, закодировать слова: АЛГОРИТМИЗАЦИЯ, КОМПЬЮТЕР, ИНТЕРНЕТ.

Задание 4. Слово ЖПЮЩЕБ получено с помощью шифра Виженера с ключевым словом БАНК. Восстановить исходное слово.

Задание 5. С помощью табличного процессора Excel автоматизировать процесс кодирования слов с использованием ключевого слова bank (предполагает, что слова будут состоять только из строчных латинских букв и их длина не будет превышать 10 символов). Для решения задачи использовать текстовые функции СИМВОЛ и КОДСИМВОЛ. Каждая буква должна храниться в отдельной ячейке. Величина сдвига должна определяться автоматически (код буквы ключевого слова минус код буквы «а» плюс единица). Попробовать с помощью вашей таблицы зашифровать слова: algebra, geometry, english.

В рамках исследования была изучена программа курса «Информатика», которая разработана на основе образовательного стандарта второго поколения и предназначена для учащихся второго этапа системы общего образования с учетом ее концептуальных и методических особенностей.

Программа не содержит обязательных для изучения на базовом уровне элементов содержания, которые можно отнести к углубленному уровню изучения информатики на уровне общего базового образования.

Информатика имеет очень большое и растущее число междисциплинарных связей, как на уровне концептуального аппарата, так и на уровне инструментария. Многие положения, разработанные информатикой, рассматриваются как основа создания и использования информационно — коммуникационных технологий (ИКТ) – одного из самых значительных технологических достижений современной цивилизации.

**В третьей главе** «Методическая разработка сопровождения уроков по теме "Информационная безопасность"» были разработаны с помощью веб-технологий Google дополнительные методические средства. В исследовании представлены пример тестирования, упражнений и веб-сайт на тему информационной безопасности, которые могут быть использованы на уроках и для самостоятельного изучения.

По теме исследования был создан веб-сайт «Информационная безопасность», который может стать сопровождением при изучении данной темы в 9 классе. Сайт имеет теоретические, дополнительные материалы, а также пример тестирования по теме изучения.

В теоретической вкладке даны определения информационной безопасности, рассмотрены виды информационных угроз, к которым относятся хищение или копирование информации, уничтожение информации, искажение информации (искажение, нарушение целостности), введение ложной информации, отрицание подлинности представляемой информации, нарушение доступности.

Также освещена проблема информационной безопасности и приведены примеры компьютерных преступлений: несанкционированный доступ к информации, ввод в программное обеспечение "логических бомб", разработка и распространение компьютерных вирусов, хищение компьютерной информации, подделка компьютерной информации.

На сайте раскрывается понятие политики безопасности как комплекса мер и активных действий по управлению и совершенствованию систем и технологий безопасности, включая информационную безопасность. Далее

приведены основные способы и методы защиты информации, к которым относятся: разработка специальных инструкций по выполнению всех технологических процедур, организационные меры, средства аппаратной защиты, программные средства защиты, межсетевые экраны, идентификация пользователей.

Дополнительные материалы содержат историю информационной безопасности, информацию об опасности социальных сетей. А также для закрепления материалы предлагаются вопросы и задания.

Кроме теории, сайт предлагает проверить свои знания с помощью тестирования, которое может использоваться в качестве первичной проверки усвоенных знаний.

В рамках исследования было создано несколько упражнений на тему «Информационная безопасность» с помощью сервиса для создания мультимедийных интерактивных упражнений learningapps.

Для проверки знаний по теме можно использовать различные средства диагностики, например кроссворд. Был разработан кроссворда на тему информационной безопасности, состоящий из 8 вопросов. Данное задание проверяет знание основных определений и теоретических сведений по теме.

Ресурс позволяет использовать для контроля усвоения темы и оценивания информационной и компьютерной грамотности обучающихся всевозможные задания. В этих целях можно использовать различные викторины. Была разработана викторина под названием «Информационная безопасность».

Созданные методические разработки будут очень полезны и при самостоятельном изучении темы, и при сопровождении изучения темы на уроке информатики.

В приложениях представлены конспекты уроков на темы: «Правовая охрана программ и данных. Защита информации» для обучающихся 9 класса, «Общение в интернете. Поиск информации» для обучающихся 8 класса.

В конспектах представлена организация работы на уроке, подробно изложены задания и упражнения. Разработки отвечают личностно-ориентированным принципам. Уделено внимание здоровьесберегающим технологиям, предусмотрены физкультминутки. В рамках урока обучающиеся развивают коммуникативные навыки, делают самоанализ при подведении итогов урока и др.

## **ЗАКЛЮЧЕНИЕ**

Тема «Информационная безопасность» достаточно типичная, её изучение начинается в 7 классе. Важно вооружить обучающихся знаниями информационной безопасности, ведь проблема обеспечения информационной безопасности в Интернете все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

**Цель работы** – разработать методическое сопровождение по теме «Информационная безопасность».

Целью работы была разработка методических рекомендаций для обучения информационной безопасности учащихся, использующих Интернет и ПК на уроках информатики. Она достигнута благодаря тому, что проанализировано большое количество различных источников.

В результате исследования была проанализирована литература по теме исследования, было расширено представление об информационной безопасности, основных составляющих информационных данных, способах защиты информации.

Рассмотрены теоретические основы обучения информационной безопасности школьником в школьном курсе информатики 7-11 классов. Было выяснено, что понятие информационной безопасности впервые встречается в курсе 7 класса, далее понятие углубляется и расширяется.

Приведены методические разработки по основам информационной безопасности в школьном курсе информатики – упражнения, тестирование, сайт «Информационная безопасность»

Материалы бакалаврской работы можно использовать на уроках информатики при изучении темы «Информационная безопасность, во внеурочной деятельности при подготовке учеников к олимпиадам и конкурсам по информатике.