На правах рукописи

Танова Элеонора Владимировна

ФОРМИРОВАНИЕ КОМПЕТЕНТНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ У ШКОЛЬНИКОВ В ПРОЦЕССЕ ОБУЧЕНИЯ ИНФОРМАТИКЕ

13.00.02 – теория и методика обучения и воспитания
(информатика, уровень общего образования)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата педагогических наук

Екатеринбург – 2005

Работа выполнена на кафедре информатики и методики преподавания информатики ГОУ ВПО «Челябинский государственный педагогический университет»

Научный руководитель: доктор педагогических наук, профессор Матрос Дмитрий Шаевич

Официальные оппоненты: доктор технических наук, профессор Красноперов Геннадий Васильевич

кандидат педагогических наук, доцент Данилина Ирина Исааковна

Ведущая организация: Омский государственный педагогический университет

Защита состоится _____ в _____ час. на заседании диссертационного совета К 212.283.07 при Уральском государственном педагогическом университете по адресу: 620017, г. Екатеринбург, ул. К. Либкнехта, 9а, ауд. 1.

С диссертацией можно ознакомиться в научной библиотеке Уральского государственного педагогического университета.

Автореферат разослан _____

Ученый секретарь
диссертационного совета Зуев П.В.

ОБЩАЯ ХАРАКТЕРИСТИКА ИССЛЕДОВАНИЯ

Актуальность исследования. В настоящее время перед системой образования встает новая проблема – подготовить подрастающее поколение к жизни и профессиональной деятельности в новой, высокоразвитой информационной среде, эффективному использованию ее возможностей и защите электронных информационных ресурсов от негативных воздействий сторонних пользователей.

В Концепции модернизации российского образования на период до 2010 года подчеркивается, что общеобразовательная школа должна формировать целостную систему универсальных знаний, умений, навыков осуществления самостоятельной деятельности и личной ответственности обучающихся, то есть ключевые компетенции.

Среди ключевых компетенций, классификации которых посвящены научные труды И.А. Зимней, Е.Я. Когана, В. Хутмахера, А.В. Хуторского, одной из главных компетенций (компетентностей) называется информационная, сформированность которой служит непременным условием успешности любого вида деятельности человека в информационном обществе.

Одной из важнейших составляющих информационной компетентности является способность человека защищать информацию от посторонних воздействий в процессе осуществления повседневной информационной деятельности. Тем не менее, как показывают исследования И.Е. Васильевой, Т.А. Гудковой, Е.В. Ивановой, О.А. Кизик, Ш. Хьюгс и др., в качестве значимых компонентов информационной компетентности рассматриваются только умения находить и обрабатывать информацию, а необходимость осуществлять ее защиту ограничивается знанием и использованием правовых и этических норм.

В фундаментальных работах в области компетентностного подхода отечественных и зарубежных исследователей Д.А. Иванова, Е.Я. Когана, Т. Орджи, Дж. Шапиро проблеме формирования информационной компетентности уделяется большое внимание. Однако, несмотря на значительные теоретические результаты, полученные исследователями, методическая проблема формирования компетентности в области защиты информации не нашла своего решения. Анализ работ А.Г. Гейна, В.А. Каймина, А.Г. Кушниренко, Н.В. Макаровой, И.Г. Семакина свидетельствует о том, что школьные учебники по информатике не содержат учебного материала по защите информации, а, сле-

довательно, отсутствуют разработанные методики обучения защите информации в общеобразовательной школе.

Среди диссертационных исследований в области теории и методики обучения информатике рассматривались вопросы формирования информационной компетентности и элементы правовой защиты информации. Однако формирование компетентности в области защиты информации в общеобразовательной школе до настоящего времени не являлось предметом диссертационных исследований, несмотря на то, что компетентность в области защиты информации является весьма значимой для человека, живущего в информационном обществе.

Анализ научной, методической и учебной литературы, а также результатов диссертационных исследований позволил выявить следующие **противоречия**:

- между возрастающими требованиями общества к уровню компетентности молодого поколения в области защиты информации и современным состоянием процесса обучения информатике в общеобразовательной школе, не обеспечивающим формирование данной компетентности у учащихся;
- между высокой значимостью умения субъектов общества защищать информацию от несанкционированного доступа и фрагментарным представлением данного раздела в учебных программах по информатике и теоретически обоснованных методик обучения защите информации.

Важность разрешения указанных противоречий обуславливает актуальность данного диссертационного исследования и определяет его **проблему**: каким образом необходимо формировать компетентность учащихся в области защиты информации при обучении информатике на всех этапах школьного образования?

Объект исследования: процесс обучения информатике в общеобразовательной школе.

Предмет исследования: формирование компетентности учащихся в области защиты информации в процессе обучения информатике на всех этапах школьного образования.

Цель исследования: Разработка и теоретическое обоснование методики формирования компетентности учащихся в области защиты информации.

В соответствии с целью и предметом исследования была сформулирована **гипотеза исследования**:

Эффективное формирование компетентности учащихся в области защиты информации при обучении информатике в общеобразовательной школе будет достигнуто, если:

- в содержание раздела «информация и информационные процессы» включить вопросы защиты информации, разработать и использовать соответствующую методику обучения;

- методика изучения криптографической защиты информации будет основана на последовательном изучении основных классов криптоалгоритмов и их математических основ, а также применении учебных задач-ситуаций, сформулированных с учетом реальных проблем, возникающих при осуществлении защиты информации.

В качестве показателей эффективности разработанной методики были приняты критерии компетентности М. Холстеда и Т. Орджи, конкретизированные нами в действиях ученика при осуществлении защиты информации.

В соответствии с поставленной целью и выдвинутой гипотезой исследования были сформулированы следующие **задачи:**

1. Провести анализ научной, научно-методической и учебной литературы, посвященной компетентностному подходу к образованию, информационной безопасности и криптографии, на основе которого определить состояние проблемы и обосновать ее значимость.
2. Обосновать выбор учебного материала по криптографии для конструирования курса «Защита информации».
3. Предложить и теоретически обосновать методику обучения учащихся вопросам защиты информации, реализация которой основана на изучении алгоритмов криптографической защиты данных и использовании принципов компетентностного подхода.
4. Разработать критерии для оценивания уровня сформированности компетентности учащихся в области защиты информации.
5. Провести педагогический эксперимент с целью проверки эффективности разработанной методики.

Теоретико-методологической основой диссертационного исследования стали теории и идеи:

- о компетентностном подходе к образованию (А.А. Вербицкий, Д.А. Иванов, Е.Я. Коган, В.В. Нестеров, Дж. Равен, И.Д. Фрумин, В. Хутмахер, А.В. Хуторской, Дж. Шапиро, С.Е. Шишов и др.);
- о понятии «информационная компетенция» и «информационная компетентность» (И.Е. Васильева, Т.А. Гудкова, Е.В. Иванова, О.А. Кизик, Н.Х. Насырова, А.В. Хуторской, Ш. Хьюгс, Дж. Шапиро и др.);
- по проблемам методологии педагогики (Ю.К. Бабанский, Л.Я. Зорина, М.В. Кларин, В.В. Краевский, И.Я Лернер, К.А. Славская и др.);
- о защите информации и информационной безопасности (А.И. Алексенцев, С.Г. Баричев, П. Гаррет, У. Диффи, В. Жельников, Н. Коблиц, Д.А. Ловцов, А. Менезес, В. А. Онегов, М.Э. Хеллман, В.В. Ященко и др.);
- по математическим основам информационной безопасности (М. Айгнер, Дж. Андерсон, Е. Андреева, Н.Я. Виленкин, Ф. Р. Гантемахер, Н. Коблиц, В.Н. Нефедов, Ф.А. Новиков, В.М. Фомичев и др.);
- по проблемам обучения информатике в общеобразовательной школе (С.А. Бешенков, А.Г. Гейн, А.П. Ершов, В.А. Каймин, А.А. Кузнецов, А.Г. Кушниренко, Н.В. Макарова, И.Г. Семакин, Н.Д. Угринович);
- нормативные документы: стандарты начального общего образования по технологии, основного общего и среднего (полного) общего образования по информатике и ИКТ, примерные программы по информатике для базового и профильного уровней, стандарты по специальностям «Криптография», «Информационная безопасность телекоммуникационных систем» и «Информатика и вычислительная техника».

Для реализации целей и задач исследования использовались **теоретические методы:** теоретический анализ и синтез при исследовании и обобщении психолого-педагогической литературы; анализ материалов конференций по использованию компетентностного подхода в обучении; анализ учебно-методической, научной и научно-популярной литературы; анализ государственного образовательного стандарта по информатике и ИКТ начального общего, основного общего и среднего (полного) общего образования; сравнительный анализ существующих стандартов, программ, учебников и учебных пособий по информатике для специальности «Информационная безопасность телекоммуникационных систем», «Информатика и вычислительная техника», «Криптография»; и **эмпирические методы:** педагогический эксперимент, на-

блюдение, тестирование, статистические методы обработки данных и проверки выдвигаемой гипотезы.

Поставленные цели и задачи определили ход исследования, которое проводилось в три этапа в период 2001 – 2005 гг.

На первом этапе (2001 – 2003гг.) проводилось изучение проблемы формирования информационной компетентности учащихся. Был проведен анализ психолого-педагогической, научной, научно-методической, учебной и методической литературы, сформулирована гипотеза исследования, составлен план опытно-экспериментальной работы. В 2003 году был проведен констатирующий эксперимент для выяснения уровня сформированности компетентности учащихся в области защиты информации.

На втором этапе (2003 – 2005гг.) был проведен отбор содержания образования для конструирования курса «Защита информации», разработана и теоретически обоснована методика обучения учащихся защите информации на всех этапах школьного образования, а также создана необходимая программная поддержка. С целью апробации разработанной методики был организован и проведен формирующий эксперимент.

На третьем этапе (2005г.) была выполнена корректировка разработанной методики обучения вопросам защиты информации, а также проведен контрольно-оценочный педагогический эксперимент с целью проверки справедливости гипотезы, выполнена обработка результатов.

База исследования: Базой исследования служили МОУ СОШ №№147, 18 г. Челябинска, МОУ СОШ №№8, 12 г. Бакала, МОУ СОШ №№10, 13, 14 г. Сатки, МОУ СОШ №21 поселка Рудничный, ГОУ СПО «Саткинский горно-керамический колледж». Исследованием было охвачено 176 учащихся 5 – 11 классов средней школы, а также 99 студентов колледжа.

Научная новизна исследования:

В отличие от диссертационного исследования Е.Г. Изаровой, где рассматриваются элементы организационной защиты информации как один из факторов формирования информационной культуры учащихся, а также исследований В.А. Онегова и Е.В. Суховой, посвященных изучению основ криптографии в начальной школе, в настоящем исследовании разработана и научно обоснована методика формирования компетентности учащихся в области защиты информации на всех этапах школьного образования (начальное общее, основное общее, среднее (полное) общее образование), основанная на

изучении методов криптографической защиты данных и направленная на применение полученных учащимися знаний и умений в конкретных жизненных ситуациях при осуществлении повседневной информационной деятельности.

Теоретическая значимость исследования:

1. Конкретизированы критерии компетентности учащихся, разработанные М. Холстедом и Т. Орджи, в действиях ученика в условиях изучения защиты информации:

- уметь соблюдать установленные правила при работе с информацией; уметь работать с информационными ресурсами; определять уязвимые стороны информации; применять различные методы для защиты собственной информации; применять простейшие криптографические алгоритмы для защиты информации;
- анализировать поставленную проблему в области защиты информации; уметь организовывать собственную деятельность по защите информации; уметь применять алгоритмы криптографии для защиты информации; уметь выбирать способ защиты информации в зависимости от конкретных предъявляемых требований в реальных жизненных ситуациях.

2. Сформулированы требования к знаниям и умениям учащихся в области защиты информации.

3. Разработаны критерии оценивания уровня сформированности компетентности учащихся в области защиты информации (на основе конкретизированных критериев компетентности М. Холстеда и Т. Орджи).

Практическая значимость исследования:

Практическая значимость исследования состоит в том, что теоретические результаты доведены до уровня конкретных методических рекомендаций:

1. Разработана и теоретически обоснована методика обучения учащихся алгоритмам криптографической защиты данных, направленная на формирование компетентности учащихся в области защиты информации на всех этапах школьного образования и включающая в себя использование обучающих компьютерных программ и учебных проблемных задач-ситуаций.

2. Разработаны и внедрены в учебный процесс средней школы педагогические программные средства «Тридевятое королевство» для начального

образования и «CryDe» для основного и среднего образования, а также программная реализация некоторых алгоритмов криптографии.

3. Разработаны методические рекомендации для учителей информатики, представленные в виде способов преодоления предполагаемых затруднений, которые могут возникнуть у школьников в процессе изучения курса «Защита информации».

На защиту выносятся следующие положения:

1. Становление информационного общества требует от человека высокого уровня компетентности в области защиты информации. В связи с этим, наряду с изучением организационных (правовых) и аппаратных основ защиты информации, необходимым условием формирования у учащихся компетентности в области защиты информации является изучение методов и алгоритмов криптографии на всех этапах школьного образования.

2. Изучение содержания курса «Защита информации» должно обеспечить формирование у учащихся понимания важности проблем информационной безопасности на каждом этапе развития общества и повышение уровня их компетентности в данной области.

3. Методика обучения учащихся защите информации должна основываться на изучении методов криптографии, применении учебных проблемных задач-ситуаций и использовании соответствующей разработанной программной поддержки при изучении алгоритмов криптографии, что позволит сформировать у учащихся умения защищать информацию в процессе дальнейшего осуществления повседневной информационной деятельности.

4. Оценка эффективности предлагаемой методики основывается на достигнутом учащимися уровне компетентности в области защиты информации.

Достоверность и обоснованность результатов исследования обеспечивалась использованием научно-обоснованных методов с опорой на основополагающие теоретические положения, последовательным проведением педагогического эксперимента, использованием математических методов обработки результатов и педагогических критериев в их качественной интерпретации.

Апробация и внедрение результатов исследования осуществлялась в форме докладов и сообщений автора на Всероссийской конференции «Информатизация общего и педагогического образования – главное условие их модернизации» (2004г.); на научно-методических семинарах при кафедре ин-

форматики и методики преподавания информатики Челябинского государственного педагогического университета (2003 - 2005гг.); на конференциях по итогам научно-исследовательской работы преподавателей и аспирантов ЧГПУ (2004 – 2005гг.); на семинарах учителей математики и информатики школ города Челябинска и Челябинской области (2004 – 2005гг.), а также посредством публикаций в журнале «Информатика и образование», в Вестнике института развития образования и воспитания подрастающего поколения при ЧГПУ, серия 3 «Новые информационные технологии», в вестнике ЮУрГУ по результатам научно-исследовательских работ, получивших гранты областной администрации, тезисах Всероссийской конференции «Информатизация общего и педагогического образования – главное условие их модернизации».

Структура диссертации. Диссертация состоит из введения, трех глав, заключения, библиографического списка, пяти приложений. Общий объем текста диссертации составляет 173 страницы. В текст входит 31 рисунок, 16 таблиц. Библиографический список включает 148 наименований, из них 16 на английском языке.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность проблемы и выбор темы исследования, степень ее теоретической разработанности, определяется цель, объект, предмет и задачи исследования, формулируется гипотеза, раскрывается научная новизна, теоретическая и практическая значимость работы, формулируются положения, выносимые на защиту.

В первой главе «Умение защищать информацию как составляющее информационной компетентности учащихся» дается анализ состояния проблемы исследования в отечественной и зарубежной научно-методической литературе; определяется основной подход к решению проблемы; приводится содержательная характеристика основных понятий, дидактические основы конструирования содержания курса «Защита информации»; определяются критерии компетентности учащихся в области защиты информации.

Проведенный анализ проблемы компетентностного подхода к образованию позволил выявить, что различные авторы по-разному подходят к трактовке понятий «ключевая компетенция» и «ключевая компетентность». Некоторые авторы (Д.А. Иванов, К.Г. Митрофанов, Е.Я. Коган) вообще не разделяют этих понятий, принимая их в качестве синонимов. Все авторы, работы

которых посвящены рассмотрению ключевых компетентностей (ключевых компетенций), выделяют информационную компетентность в качестве одной из наиболее важных и значительных.

Обоснован выбор определения информационной компетентности, предложенный исследователями американской ассоциации ACRL (Association of College and Research Libraries) Ш. Хьюгс и Дж. Шапиро. Этими авторами рассматривается умение человека производить, распространять собственную информацию, организовывать доступ к информационным ресурсам и соблюдать все нормы информационной безопасности в качестве составляющих информационной компетентности. Данный подход обобщает остальные подходы и классификации (Е.Я. Когана, О.В. Чураковой, Дж. Равена, М. Холстеда, Д.И. Иванова и др.) и охватывает все возможные ситуации, которые могут возникнуть при работе с информацией, в частности и ее защиту, что послужило основанием для выбора этого подхода в качестве основного для нашего исследования.

Выявлено, что одной из составляющих информационной компетентности многие авторы называют умение организовывать доступ к информации, ее хранение, передачу, придерживаясь при этом законодательных актов и морально-этических норм. Однако сегодня явно недостаточно просто знать правовые и этические нормы и придерживаться их при работе с информационными ресурсами. Одним из важных моментов становится умение защищать собственную информацию от несанкционированного доступа.

Обобщая проанализированные подходы к определению понятия «защита информации» будем придерживаться следующего: *защита информации* – есть комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный доступ к засекреченной информации и ее носителям.

Среди всех методов защиты информации выделены криптографические средства обеспечения безопасности данных – математические алгоритмы, программно реализованные на персональных компьютерах. Данный способ обеспечения безопасности данных является достаточно простым в использовании и позволяет обеспечить сохранность любой информации. Криптография является одним из разделов информатики. Информатика, в свою очередь,

является учебным предметом, представленным в школьной программе. Поэтому именно криптографические способы защиты информации можно рассматривать на школьных уроках.

Проведенный анализ государственного образовательного стандарта по информатике и ИКТ, а также анализ школьных учебников по информатике, показал, что вопросам защиты информации практически не уделяется внимания в школьной программе. Материал данного раздела ограничивается рассмотрением правовых аспектов защиты данных и методов защиты данных от физического разрушения. Анализ учебных курсов и учебной литературы по информатике свидетельствует о том, что на сегодняшний день нет разработанных курсов и методик обучения защите информации на этапе школьного образования, хотя важность этого вопроса подчеркивается многими авторами.

В соответствии с этим обоснована необходимость начинать изучение вопросов, связанных с защитой информации, одновременно с изучением информационных процессов, что позволит формировать у школьника компетентность в данной области.

Как показали В.А. Болотов, Е.Я. Коган и В.В. Сериков, формирование компетентности должно начинаться с формирования знаний, умений и навыков, постепенно переходя к формированию умения применять их на практике для решения поставленных жизненных задач.

В основу конструирования содержания курса «Защита информации», главной целью которого является формирование компетентности учащихся в области защиты данных, положены принципы и критерии отбора основ содержания образования, сформулированные И.Я. Лернером и В.В. Краевским (принципы научности и практической значимости, принцип соответствия содержания социальному заказу общества, принцип доступности) и общедидактические принципы.

В основу методики обучения учащихся защите информации были положены принципы построения образовательных программ в условиях компетентностного подхода, предложенные В.А. Болотовым и В.В. Сериковым:

1. Описание признаков и ожидаемого (планируемого) уровня компетентности в некоторой области.

2. Определение необходимого и достаточного набора учебных задач-ситуаций, последовательность которых выстроена в соответствии с возрастанием полноты, проблемности, конкретности, новизны, жизненности, практич-

ности, межпредметности, креативности, ценностно-смысловой рефлексии и самооценки.

3. Технология процесса, в том числе последовательность предъявления ученикам задач-ситуаций различных типов и уровней.

4. Алгоритмы и эвристические системы, организующие деятельность учеников по преодолению затруднительных ситуаций.

5. Технология сопровождения, консультирования и поддержки учащихся в процессе прохождения программы.

Как показали исследования Е.Я. Когана, компетентность должна формироваться на основе знаний, умений и навыков учащихся. В связи с этим нами были определены требования к знаниям и умениям учащихся в области защиты информации.

Учащиеся должны **знать/понимать:**

1. Уязвимые стороны информации, возможные угрозы и необходимость ее защиты.

2. Основные способы защиты информации и их характеристику.

3. Математические правила, лежащие в основе криптографической защиты информации.

4. Принципы построения и работы основных криптоалгоритмов.

5. Основные методы атак на защищенную информацию.

Учащиеся должны **уметь:**

1. Давать характеристику различным способам защиты информации.

2. Работать с системами защиты информации.

3. Выбирать алгоритм защиты информации для решения поставленной задачи.

Требования к уровню компетентности учащихся были сформулированы на основе критериев компетентности, разработанных М. Холстедом и Т. Орджи:

1) учащийся должен показать, что он в состоянии убедиться, что правильно понял предлагаемую ему проблему и сделать два предложения по ее решению;

2) учащийся должен показать, что он в состоянии увидеть проблему или проблемную ситуацию, описать ее основные характеристики и предложить два способа ее решения.

Выбор данных критериев компетентности был сделан на основе научных исследований Е.Я. Когана, Д.И. Иванова, К.Г. Митрофанова, А.А. Вербицкого, И.Д. Фрумина, которые применяют уровни компетентности М. Холстеда и Т. Орджи в качестве базовых и на их основе формулируют критерии и уровни компетентности учащихся в различных областях.

Данные критерии компетентности были конкретизированы нами в действиях ученика в условиях изучения защиты информации.

Чтобы показать, что компетентность учащегося отвечает первому критерию, учащийся должен выполнять следующие действия:

1) уметь соблюдать установленные правила при работе с информацией;
2) уметь работать с информационными ресурсами;
3) определять уязвимые стороны информации;
4) применять различные методы для защиты собственной информации;
5) применять простейшие криптографические алгоритмы для защиты информации.

Компетентность учащегося будет отвечать второму критерию в том случае, если учащийся:

1) анализирует поставленную проблему в области защиты информации;
2) умеет организовывать собственную деятельность по защите информации;
3) умеет применять алгоритмы криптографии для защиты информации;
4) умеет выбирать способ защиты информации в зависимости от конкретных предъявляемых требований в реальных жизненных ситуациях.

Во второй главе «Методика изучения курса «Защита информации» и его использование в учебном процессе для формирования компетентности учащихся в области защиты данных» рассматривается структура и содержание курса «Защита информации» для всех этапов школьного образования и методика обучения учащихся защите информации.

Разработка методики обучения учащихся вопросам защиты информации проводилась на основе теоретических подходов, определенных в первой главе исследования. В соответствии с этим для каждого этапа школьного образования были разработаны:

1. Последовательность и методика предъявления учебного материала учащимся в соответствии с возрастанием его сложности, проблемности и практического применения (программа курса, граф, отражающий связи между

изучаемыми темами, понятийный аппарат для каждой темы, краткое содержание учебного материала, модель деятельности учителя и ученика при изучении курса на каждом этапе).

2. Требования к уровню компетентности учащихся в области защиты информации после изучения курса «Защита информации».

3. Набор учебных проблемных задач-ситуаций для каждой темы.

4. Анализ возможных трудностей и проблемных моментов, которые могут возникнуть у учителя или учащихся в процессе изучения данного материала и способы их преодоления.

Программа курса «Защита информации» приведена в таблице 1.

Таблица 1

Программа курса «Защита информации» для всех этапов школьного образования

Класс	Тема	Количество часов
1 – 4 класс	Основы криптографии – 18 часов	
	Уязвимость информации и способы ее защиты	3
	Графические шифры	3
	Шифры замены	4
	Шифры перестановки	4
	Шифры с ключом	4
5 – 9 класс	Основы симметричной криптографии – 34 часа	
	Уязвимость информации и способы ее защиты	7
	Введение в криптографию	4
	Математические основы симметричной криптографии	7
	Симметричные шифры (шифры замены, шифры перестановки, блочные шифры)	16
10 – 11 класс	Основы несимметричной криптографии – 34 часа	
	Математические основы симметричной криптографии	8
	Симметричная криптография и ее проблемы	14
	Математические основы несимметричной криптографии	6
	Алгоритмы несимметричной криптографии	6

На рисунке 1 в качестве примера приведен граф, отражающий связь между темами курса «Защита информации» для основного образования.

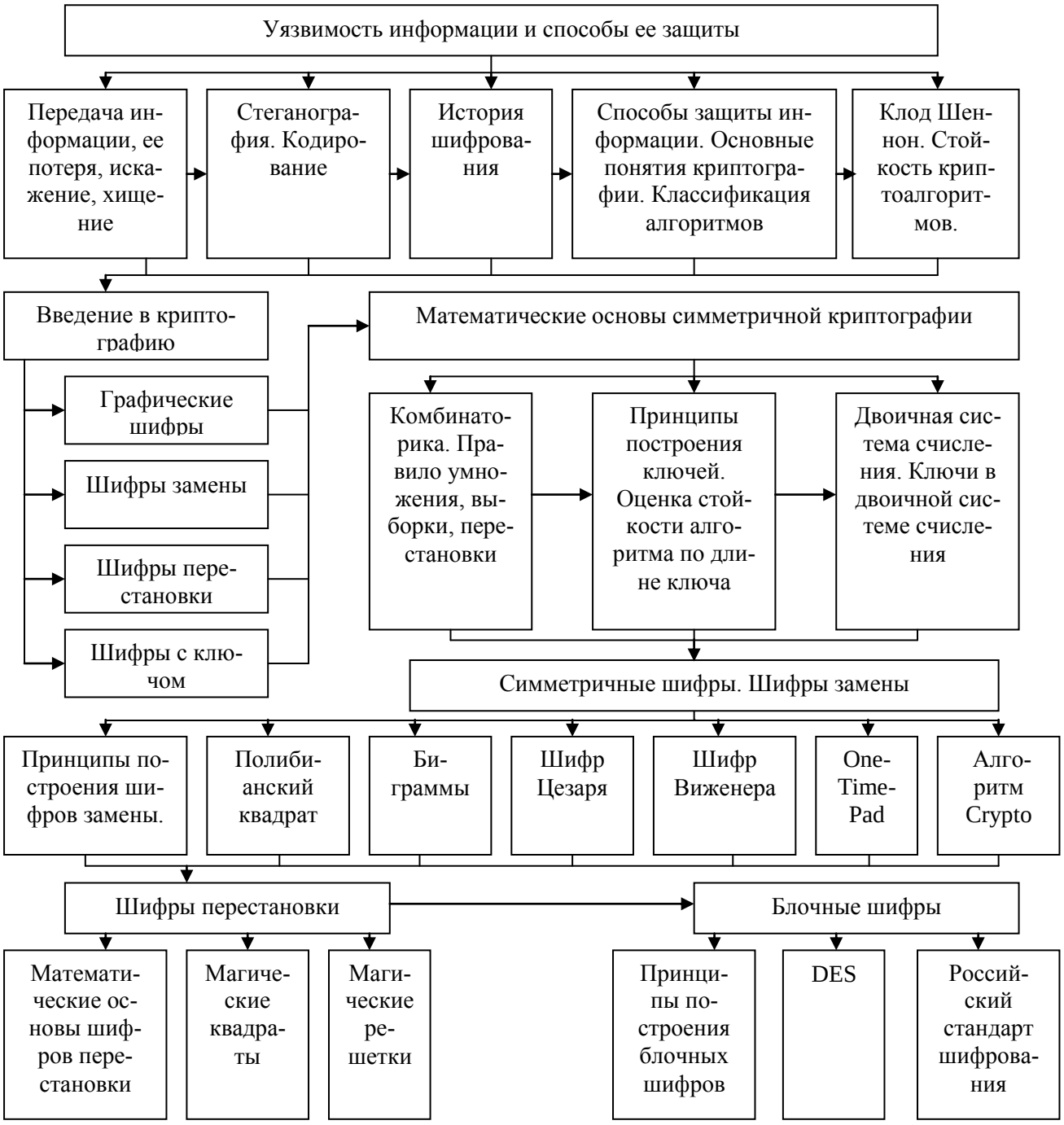


Рис. 1. Взаимосвязь изучения тем курса «Защита информации» для основного образования

Для каждого этапа были сформулированы требования к уровню компетентности учащихся после изучения курса «Защита информации».

Начальное образование

1. Уметь находить решение проблемы защиты информации с опорой на личный опыт.

2. Уметь определять уязвимые стороны информации.

3. Уметь применять простейшие алгоритмы криптографии для защиты информации в повседневной жизни.

4. Уметь выбирать алгоритм шифрования для защиты информации конкретного вида.

Основное образование

1. Соблюдать установленные правила при работе с информацией.

2. Уметь работать с информационными ресурсами.

3. Уметь организовывать безопасность собственного информационного пространства, указывая на возможность криптографической защиты данных.

4. Объяснять необходимость использования криптографической защиты данных в заданной ситуации.

5. Уметь выбирать алгоритм шифрования, в зависимости от требований к его стойкости, быстроте и простоте реализации и использовать его для защиты информации.

Среднее (полное) образование

1. Анализировать поставленную проблему, связанную с защитой информации.

2. Уметь применять алгоритмы симметричной и несимметричной криптографии для защиты информации.

3. Уметь выбирать алгоритм шифрования в зависимости от предъявляемых к нему требований и применять его для решения конкретной проблемы защиты информации.

4. Организовывать деятельность по защите информации, применяя комбинированные криптографические алгоритмы.

Для формирования компетентности учащихся в области защиты информации на каждом этапе школьного образования должны применяться учебные проблемные задачи – ситуации. Приведем несколько подобных заданий в качестве примера для среднего (полного) образования.

1. В силу рода своей профессиональной деятельности Вам приходится обмениваться с филиалами Вашей компании финансовыми документами различной степени важности через Интернет. Какими способами возможно обеспечить безопасность передаваемых по сети документов и данных?

2. Все банковские операции являются засекреченными. При снятии денег со счета через банкомат информация о произведенной операции передает-

ся в центральное отделение банка. Какой вариант защиты этой информации вы могли бы предложить в подобной ситуации?

3. Вам предложено разработать систему секретной связи для обмена документацией по открытому каналу связи, например, по почте. Что Вы предложите заказчику и как обоснуете именно такой выбор параметров?

Для каждого этапа школьного образования разработана модель деятельности учителя, которая описывает последовательность применяемых методов обучения, рекомендации по организации форм работы учащихся, последовательность предъявления учебного материала и рекомендации по использованию разработанных педагогических программных средств.

Третья глава «Педагогический эксперимент и его результаты» посвящена описанию и анализу организованного и проведенного констатирующего и формирующего эксперимента, а также определению статистической достоверности полученных результатов. Целью констатирующего эксперимента было определение уровня компетентности учащихся в области защиты информации.

В констатирующем эксперименте принимало участие 312 учащихся школ г. Челябинска и челябинской области, а также учащихся колледжа г. Сатка, обучающихся по программе общеобразовательной школы. Констатирующий эксперимент проводился в 2003 – 2004 учебных годах.

При проведении констатирующего эксперимента учащимся предлагалось найти способ решения проблемы, связанной с умением защищать информацию. Сформулированный и предложенный учащимся набор проблемных задач-ситуаций охватывает все стороны защиты информации, что позволяет адекватно судить об уровне информационной компетентности учащихся в области защиты данных.

Исходя из предложенного содержания курса «Защита информации», уточненных уровней компетентности и обоснованных критериев компетентности учащихся в области защиты информации были сформулированы критерии оценивания уровня сформированности компетентности учащихся в области защиты информации, которые представлены в таблице 3.

Формирующий эксперимент проводился в 2004 – 2005 учебном году. Целью данного этапа было внедрение разработанного содержания курса и методики его преподавания в учебный процесс средней школы и колледжа и опре-

деление влияния изучения данного курса на изменение уровня информационной компетентности учащихся.

В формирующем эксперименте принимало участие 275 учащихся из 7 школ г. Челябинска и челябинской области и ГОУ СПО «Саткинского горно-керамического колледжа». Кроме этого, в формирующем эксперименте приняли участие 10 человек среди учителей, которые проводили занятия по разработанной нами методике.

Таблица 3

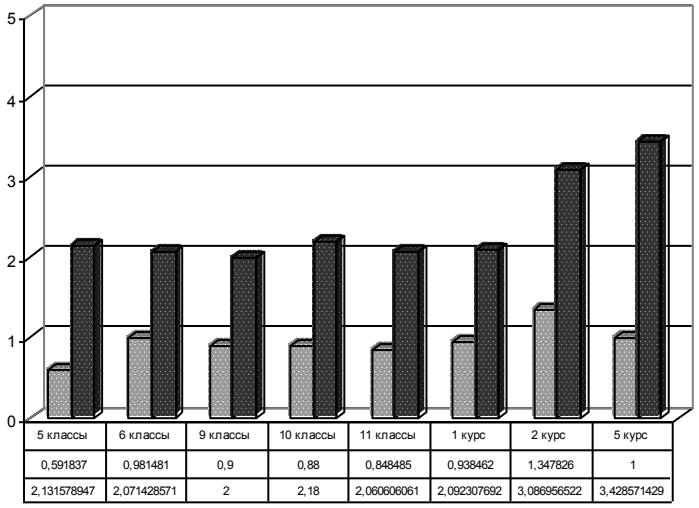
Шкала оценивания уровня компетентности учащихся в области защиты информации.

Баллы	Действия ученика
0	Полное непонимание проблемы, отсутствие решения.
1	Предлагается способ решения с опорой на личный опыт или знания, полученные в регулярном курсе информатики.
2	Предлагается не менее двух способов решения проблемы, указывается возможность использования алгоритмов криптографии.
3	Предлагается не менее двух способов решения с использованием алгоритмов криптографии, дается обоснование необходимости использования именно криптографическую защиту.
4	Дается характеристика проблемы, указываются возможные причины ее возникновения, предлагается не менее двух решений с использованием алгоритмов криптографии.
5	Дается характеристика проблемы, указываются возможные причины ее возникновения, предлагается не менее двух решений комбинированным способом с объяснением преимуществ такого решения.

После окончания изучения курса с целью выяснения изменений в уровне компетентности учащимся вновь был предложен ряд проблемных заданий для решения. Оценивание уровня компетентности проводилось в соответствии с разработанными критериями.

Анализ результатов эксперимента показывает, что только у 9,93% учащихся, что составляет 27 человек, уровень компетентности не изменился. В эту группу входят в основном те учащиеся, чей уровень компетентности изначально был 2 или 3 балла, то есть выше, чем у остальных испытуемых.

Результаты формирующего эксперимента показали, что после изучения курса уровень компетентности учащихся в области защиты информации повысился. Сравнение уровня компетентности до и после изучения курса представлено на рисунке 2.



5 классы	6 классы	9 классы	10 классы	11 классы	1 курс	2 курс	5 курс
0,591837	0,981481	0,9	0,88	0,848485	0,938462	1,347826	1
2,131578947	2,071428571	2	2,18	2,060606061	2,092307692	3,086956522	3,428571429

Рис. 2. Итоги формирующего эксперимента.

Для подтверждения достоверности полученных данных были использованы два метода статистической обработки экспериментальных данных: критерий знаков (G – критерий) и парный t-критерий Стьюдента.

Критерий знаков использовался для установления общего направления изменения уровня компетентности учащихся. Для проверки гипотезы о том, что изучение курса «Защита информации» влияет на повышение уровня информационной компетентности учащихся, был использован парный t-критерий Стьюдента для каждой группы учащихся, принимавшей участие в эксперименте.

Результаты статистической обработки экспериментальных данных показали, что выдвинутая гипотеза принимается в каждой группе для уровня значимости 0,01.

Проведенный эксперимент свидетельствует о целесообразности изучения курса «Защита информации» в средней школе и колледже и выявил эффективность использования разработанной методики обучения данному курсу.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

1. В теоретическом плане наиболее исследован вопрос о компетентностном подходе к образованию. Установлено, что данный подход базируется на выделении ряда ключевых компетенций (компетентностей), среди которых одной из главнейших ученые называют информационную компетентность. Показано, что одним из важных признаков информационно компетентного

человека является способность осуществлять защиту информации при осуществлении повседневной информационной деятельности. Обосновано, что одной из главнейших частей компетентности в области защиты информации являются умения применять в повседневной практической деятельности алгоритмы криптографической защиты данных.

2. Изучение и анализ государственных образовательных стандартов по информатике и ИКТ для всех этапов школьного образования, стандартов для специальностей, связанных с информационной безопасностью и криптографией, а также учебной и учебно-методической литературы по информатике позволили выявить ряд недостатков, основными из которых являются: ограничение рассмотрения защиты информации аппаратными и правовыми аспектами, а также фрагментарное представление учебного материала по криптографической защите данных.

3. Основная роль в содержании разработанного курса «Защита информации» должна отводиться алгоритмам криптографии и их математическим основам. На каждом этапе школьного образования необходимо расширять круг изучаемых криптоалгоритмов (на этапе начального образования - графические и простейшие симметричные шифры; на этапе основного образования – алгоритмы симметричной криптографии, блочные шифры; на этапе полного (среднего) образования – симметричная криптография и ее недостатки, несимметричные криптоалгоритмы); обучать школьников принципам работы с криптосистемами, реализующими определенные методы шифрования; знакомить с современными методами защиты информации.

4. Разработанная методика формирования компетентности в области защиты информации у школьников основана на систематичном изучении криптографических способов защиты информации, использовании учебных проблемных задач-ситуаций, решение которых позволяет учащимся получить некоторый опыт в области защиты информации, и применении педагогических программных средств (обучающих программ и программной реализации некоторых криптоалгоритмов).

5. Разработанные критерии оценивания уровня компетентности школьников (0 – 5) основаны на конкретизированных в действиях ученика для изучения защиты информации критериях компетентности М. Холстеда и Т. Орджи.

6. Проведенная экспертиза уровня компетентности в области защиты информации среди учащихся основного общего и среднего (полного) общего образования гг. Челябинска, Сатки и Бакала, а также среди учащихся колледжа в 2003 – 2004 гг. показала, что одному из важных составляющих информационной компетентности не уделяется должного внимания в образовательном процессе. Организованный и проведенный педагогический эксперимент показал эффективность применения разработанной методики. Анализ полученных в ходе эксперимента данных дал возможность сделать вывод о том, что изучение вопросов, связанных с защитой данных и обеспечением информационной безопасности положительно влияет на изменение уровня компетентности учащихся в области защиты информации.

Дальнейшее исследование по проблеме может быть осуществлено в следующих направлениях: разработка новых форм и методов изучения различных способов защиты информации, расширение и углубление содержания курса для учащихся школ с информационным или математическим профилем, а также для студентов колледжей со специальностью «информационная безопасность».

Основное содержание диссертации изложено в **публикациях** автора:

1. Матрос Д.Ш., Танова Э.В. Изучение элементов криптографии в школе / Информатика и образование. – 2003. – №6. – С. 19 – 27 (авторских 50%).

2. Танова Э.В., Дмитриева О.А., Яковлева О.А. Система защиты информации в локальной сети / Вестник института развития образования и воспитания подрастающего поколения при ЧГПУ. Серия 3. Новые информационные технологии. – 2002. – № 12. – С.126 – 133 (авторских 70%).

3. Танова Э.В. Система защиты информации на основе одноключевых шифров / Вестник ЮУрГУ. – 2002. – С. 8 – 9.

4. Танова Э.В. Факультативный курс «Основы криптографии» для учащихся средней школы. / Тезисы выступлений участников конференции «Информатизация общего и педагогического образования – главное условие их модернизации». – 2004. – С. 54.

5. Матросов В.Л., Жданов С.А., Воронина О.В., Танова Э.В. и др. Использование современных информационных и коммуникационных технологий в образовательном процессе: Учебно-методический комплект для системы педагогического образования / Под общ. ред. А.М. Семибратова. – М.: АПК и ПРО, 2004. – 200 с. (авторских 6%).

Подписано в печать _____ Формат бумаги 60Х84 1/16. Бумага для множит. ап.
Печать на ризографе. Уч.-изд. лист. 1,44. Тир. 100 экз. Заказ _____
ГОУ ВПО «Челябинский государственный педагогический университет»
Отдел множительной техники
454080, г. Челябинск, пр. Ленина, 69