МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное образовательное учреждение высшего образования

«КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.П. Астафьева»

(КГПУ им. В.П. Астафьева)

Институт/факультет Математики, физики и информатики

Выпускающая(ие) кафедра(ы) Кафедра информатики и информационных технологий в образовании

Борзова Любовь Сергеевна

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: "Элективный курс "Современные антивирусные программы" как средство формирования представлений об обеспечении безопасности компьютера у школьников 10-11 классов"

Направление подготовки 44.03.05 Педагогическое образование

Профиль Математика и информатика

ДОПУСКАЮ К ЗАЩИТЕ

Зав. кафедрой д.пед.н., профессор Н.И. Пак

17.06.19.

(дата, подпись)

Руководитель:

к.пед.н, доцент М.А. Сокольская

17.06.19.

Дата защиты: 27 июня 2019 года

Обучающийся: Борзова Л.С.

17.06.19

(дата, подпись)

Оценка удовлетворительно

Красноярск 2019

Содержание

Введение

Актуальность исследования. В современном мире информация играет важнейшую роль, являясь важным ресурсом для многих сфер человеческой деятельности. Для работы с информацией человечество использует и развивает компьютерные технологии. С момента появления компьютерные системы являлись крайне сложными, предполагали необходимость высокой квалификации и находились в научных лабораториях. Специалисты формулировали цели и задачи, после чего переводили их на доступный компьютерам язык. Спустя годы мир осуществил значительный скачок в сфере информационных технологий, вследствие появления микросхем, развития математики, физики.

Компьютеры и мобильные устройства в настоящее время используются во всех областях деятельности общества. Компьютеры научились работать автономно, а также стали переносными, минимизированными. В настоящее время реализуется переход от постиндустриального общества к информационному, поэтому информация становится одним из наиболее важных ресурсов. С появлением компьютеров в нашей жизни и развитием сети Интернет стало возможным находить и использовать большой объем информации. Количество информации, которую люди доверяют сетевым ресурсам, с каждым днем растет, поэтому рано или поздно каждый задается вопросом: «Как обеспечить надежную сохранность данных?»

Сегодня невозможно встретить пользователя персонального компьютера, который не слышал бы о компьютерных вирусах. В Интернете такие вредоносные программы существуют в огромном количестве. Компьютерные вирусы приносят большой урон пользователям компьютерной техники. Чтобы эффективно бороться с вирусами, необходимо иметь представление о вирусах и разбираться в методах борьбы с ними.

95% школьников имеют компьютер в домашнем пользовании, а, следовательно, должны уметь обеспечить безопасность своей работы. Чтобы эффективно бороться с вирусами, современному пользователю необходимо иметь представление о вирусах и разбираться в методах противодействия вирусам. В школьном курсе, изучению такой важной темы как «Компьютерные вирусы. Антивирусные программы» уделяется очень мало внимания, это говорит о том, что рассмотрение вопросов информационной безопасности в школе является оправданным и в данный момент очень актуальным. Современный пользователь способен грамотно применять средства антивирусной защиты лишь тогда, когда он имеет соответствующую теоретическую подготовку, а также практический опыт работы с ними.

Объект исследования – процесс обучения информатике в школе

Предмет исследования – формирование представлений об обеспечении безопасности компьютера у старшеклассников посредством элективного курса «Современные антивирусные программы»

Цель исследования - разработка элективного курса "Современные антивирусные программы", способствующего формированию представлений старшеклассников об обеспечении безопасности персонального компьютера.

Задачи исследования.

1. Анализ литературы по теме исследования с целью определения сущности понятия информационная безопасность.
2. Выявление особенностей формирования представлений об информационной безопасности в школе.
3. Разработка целей и содержания элективного курса «Современные антивирусные программы»
4. Разработка примеров занятий по программе элективного курса.

Методы исследования: теоретический анализ литературы по данной проблеме, анализ документации (рабочих программ и учебно-методических

комплексов по учебным дисциплинам, ведомостей успеваемости и учета рейтинговых баллов, математическая обработка статистических данных.

Структура выпускной квалификационной работы включает в себя: введение, две главы, заключение, список использованных источников.

Глава 1. Теоретические основы формирования информационной безопасности обучающихся

1.1 Информационная безопасность

Информационная безопасность и защита информации – новая, бурно развивающаяся область знаний. Здесь пока нет устоявшихся авторитетов, жестко сконструированных теоретических конструкций, схем и надстроек, нет и общепризнанных понятий, категорий и принципов, все очень быстро и достаточно просто меняется под влияние научно-технического прогресса. Современный этап развития общества характеризуется возрастающей ежедневно ролью информационного взаимодействия между элементами информационных инфраструктур и субъектов, осуществляющих сбор, формирование, распространение и использование информации. Информация сегодня превратилась в глобальный неистощимый ресурс управления, развития, образования, промышленного производства, процессам, обеспечивающим устойчивость и выживаемость любых систем.

Само понятие «безопасность информации» описывает ситуацию, исключающую доступ для просмотра, модернизации и уничтожения, данных субъектами без наличия соответствующих прав. Этот термин включает обеспечение защиты от утечки и кражи информации с помощью инновационных устройств современных технологий. Система безопасности потенциальных и реальных угроз непостоянна, так как те могут появляться, исчезать, уменьшаться либо увеличиваться. В процессе обеспечения безопасности информации все участники отношений, будь то государство, человек, организация или какой-либо регион, представляют собой многоуровневые сложные системы, для которых сложно определить уровень необходимой безопасности [1, с. 240].

Развитие информационных и телекоммуникационных технологий стало причиной революции в сфере документационного обеспечения управления. Последние несколько лет спрос на системы электронного

документооборота (СЭД) увеличивался и, по прогнозам экспертов, эта тенденция продолжится. Внедрение электронного документооборота в организациях, позволило создать более гибкую систему в обработке и хранении информации и, конечно же, ускорило многие делопроизводственные процессы. Это объясняет увеличение спроса на системы электронного документооборота. В то же время, применение СЭД повлекло за собой новые риски и уже оправданные опасения по поводу информационной безопасности организации [6, с. 44].

Под информационной безопасностью государства следует понимать состояние сохранности информационных ресурсов. Причем как в лице государства, так и общества и личности [2].

Помимо того информационная безопасность определяется как процесс гарантии конфиденциальности, целостности и доступности информации. Что касается конфиденциальности, то она обеспечивается доступом к информации только активизированным пользователям. Целостность позволяет решить вопросы надежности и полноты информации и способов ее обработки. Доступность – это вероятность гарантии доступа к информации и относящейся с ней средствами активизированных пользователей по мере необходимости [1].

Безопасность информации связана с недостатком либо снижением недопустимого риска. Он может относиться к неразрешенным воздействиям на информационные ресурсы школы. Такое влияние может быть непреднамеренным. А также вероятна утечка информации по техническим каналам [15].

Под безопасностью информации следует понимать состояние защищённости информации, обеспечивающее сохранность информации, для обработки которой она употребляется, и информационную безопасность автоматизированной информационной системы, в которой она выполнена[16].

Информационная безопасность – защищенность информации от случайных влияний природного или искусственного характера, которые могут причинить огромный ущерб субъектам информационных отношений. Удерживающая инфраструктура – системы электро-, тепло-, водо-, газоснабжения, системы кондиционирования и т. д., а также обслуживающий персонал. Недопустимый ущерб – ущерб, который нельзя игнорировать [30].

Редко выделяют необходимые категории критерии безопасности: подотчётность – обеспечение распознания субъекта доступа и регистрации его действий; достоверность – соотношение определенному результату; подлинность – иначе истинность; неотказуемость – умение удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отторгнуты [12].

Итак, можно выделить следующие стороны рассматриваемого вопроса: научная, нормативно правовая база, а также полномочия органов в сфере информационных технологий [9].

В научных исследованиях Г. Грачева, Х. Домозетова, И. Мельника и др., посвященных информационной безопасности, показано, что воздействие информации на человека может иметь различную направленность, в том числе с помощью информации можно воздействовать, управлять и манипулировать сознанием и психикой личности [17].

В.Ю. Статьев и В.А. Тиньков определяют информационную безопасность как защиту информации с помощью программных методов с целью недопущения причинения вреда владельцам этой информации или поддерживающей его инфраструктуре [13].

Г.Г. Феоктистовым информационная безопасность определяется как получение максимальной информации о намерениях и потенциальных действиях своих оппонентов и минимальная утечка информации в своих планах. А.Д. Урсул считает, что информационная безопасность – это состояние защищенности основных сфер жизнедеятельности по отношению к опасным информационным воздействиям [29].

Говоря об «информационной безопасности» с педагогической стороны, необходимо разобраться с понятием «безопасности» [18]. Это понятие представляет собой сложное явление, его изучением занимаются специалисты, работающие в различных отраслях знаний. Изучив основные подходы в научной литературе к данному понятию, представляется, что оно означает полное отсутствие угрозы. [4].

В педагогической литературе понятия информационной безопасности не содержится, но изучив основные подходы в научной литературе к определению информационной безопасности В.Ю. Статьева, В.А. Тинькова, можно дать определение данного термина и в педагогическом аспекте [28].

Итак, «безопасность» – это состояние защищенности от угроз, а иначе полное ее отсутствие. Информация же представляет собой какие-либо сведения. Таким образом, информационная безопасность – это состояние защищенности от угроз интересов личности, заключающаяся в умении выявлять и вовремя пресекать угрозы информационного влияния.

Угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения информационной безопасности [5]. Возникновение угрозы связано, как правило, с уязвимостью, благодаря которой, к сожалению, и происходит реализация угроз.

Важно сказать об угрозе раскрытия информационных ресурсов. Она заключается в том, что какие-либо данные становятся известными тем, кто не должен знать соответствующей информации. Это может произойти как в открытых ресурсах, так и ограниченного доступа [26].

Самыми распространенными ситуациями, влекущими угрозу безопасности, являются ошибки самих пользователей, а также системных администраторов и операторов связи, которые занимаются обслуживанием информационных систем.

Важно поговорить о так называемых интернет-угрозах, так как школьник получает информацию, не только из учебников, от учителей и родителей, но и из средств массовой информации. Статистика показывает,

что информация из электронных ресурсов преобладает. В СМИ можно наблюдать жестокие сцены насилия, порнографии, можно услышать нецензурную лексику на многих телеканалах. Такие негативные факторы, очевидно, отрицательно влияют на психику и сознание ребенка.

Газета «НИ» описывает инцидент, который произошел в Ульяновской области. При проверке работниками прокуратуры кабинетов информатики было обнаружено, что во многих учебных заведениях на компьютерах нет сетевых фильтров, и школьники прямо на уроках, подключившись к интернету, смотрели порно-сайты. Сетевые фильтры, специально закупленные для компьютеров, не были установлены, и ученики имели доступ к нежелательным Интернет-ресурсам. Учителя даже не подозревали, чем их ученики на уроках информатики занимаются. Сотрудники областной прокуратуры разрушили наивные представления преподавателей, проведя проверку в местных школах [23].

Виртуальное общение в сети Интернет затормаживает развитие умственных способностей, так как школьник лишается возможности самостоятельного поиска какой-либо информации, а также может привести к замкнутости и зажатости ребенка. В медицинском плане у ребенка ухудшается зрение. Из-за большого круга общения подростку не удается полноценно вести коммуникативный диалог: возникают «контакты», но не прибавляется друзей. Это приводит к замкнутости и десоциализации.

Школьник может стать жертвой различного вида мошенничества:

– фишинг (несанкционированный доступ к паролям и логинам);

– фарминг (пользователя перенаправляют на ложный IP-адрес);

– смс-мошенничество (предложения отправить сообщение на короткий номер, согласие на рассылку приводит к уменьшению средств на телефонном счету без уведомления хозяина);

– кардинг (взламывают серверы интернет магазинов, расчетные и платежные системы, персональные компьютеры и с непосредственно, или с

помощью «трояны» и т.п. происходит похищение реквизитов платежных карт) и т.д. [8].

В социальных сетях много вредоносных ссылок и непроверенных приложений, поэтому школьник может стать жертвой кибербуллинга (подростковый виртуальный террор).

Также для школьников необходимо проводить беседы про вредоносные программы, такие как «банер», «блокер», «майнер», «троян» и т.д. Школьники должны знать про вредоносные программы, такие как программы-вирусы «троянский конь», черви и т.п. Эти программы созданы для сбора и уничтожения личной информации и распространяются без ведома хозяина компьютера на компьютеры знакомых, родственников, всех, кто находится в базе электронной почты, по всей интернет-сети. Сначала компьютер начинает медленнее работать, потом неожиданно перезагружаться, потом пропадают файлы.

Как показывает наша жизнь, увлечение Интернетом приводит к побегу в виртуальную реальность и, как следствие, к зависимости и привыканию. Более сложной формой расстройства считается депрессия, которая может возникнуть при ограничении доступа в Интернет.

Несложно заметить, что дети с каждым днем становятся все более зависимы от электронных гаджетов (ПК, мобильные телефоны, планшеты), при этом избегая живого общения. При этом дети, ввиду малого жизненного опыта не могут оценить угрозы, которые содержатся в сети. И проблема также в том, что многие родители либо не задумываются об этом, либо не имеют должного уровня знаний, которые бы помогли предпринять действия по защите от нежелательной информации своего ребенка.

Меры и способы обеспечения информационной безопасности

На сегодняшний день контроль за движением и хранением информации стал обязанностью каждого пользователя компьютера. Когда компьютеры впервые появились, они были доступны только небольшому числу людей, обученных их использовать. Обычно эти технические средства

помещались в специальных помещениях, удаленных территориально от помещений, где работали служащие. Сейчас все изменилось. Компьютерные терминалы в настольные компьютеры используются везде.

Трудно обобщать, но теперь компьютерным преступником может быть:

- конечный пользователь, не технический служащий и не хакер;
- тот, кто не находится на руководящей должности;
- тот, кто не был судим;
- умный, талантливый сотрудник;
- тот, кто любит много работать;
- тот, кто абсолютно не разбирается в компьютерах;
- тот, на кого бы вы подумали в последнюю очередь;
- именно тот, кого вы взяли бы на работу.

Компьютерным преступником может быть любой. Обычный компьютерный преступник – это служащий, которому разрешен доступ к системе. При совершении какого-либо взлома используются следующие технологии.

Мошенничества:

1. Ввод ложной информации.
2. Манипуляция информацией.
3. Манипуляции файлов с информацией.
4. Обход внутренних мер защиты.

Злоупотребления:

1. Кража программ, информации и оборудования.
2. Разработка компьютерных программ для неслужебного использования.
3. Неправильное использование работ на компьютерах.
4. Ввод неавторизованной информации.

Всегда нужно вести контроль компьютера и доступа информации в нем.

Меры защиты.

Во-первых, это так называемая идентификация пользователей. Лучше использовать одного пользователя системы для безопасности проникновения угрозы и требовать, чтобы остальные пользователи выполняли входы в компьютер, используя средство для идентификации в начале работы.

Что касается аутентификации пользователей, нужно использовать личные пароли, которые не являются комбинациями данных пользователя. Пароли – это защита информации от несанкционированного доступа.

Роль школьного педагога должна быть приоритетной, так как ребенок большую часть времени проводит в учебном заведении. Высока роль также самого учебного заведения, и его обязанностью является установление сетевых фильтров, которые ограничивают доступ к запрещенным сайтам.

Таким образом, необходимо выделить следующие меры по защите школьников от небезопасной информации: прежде всего, нужно установить антивирусное программное обеспечение, которое блокирует всплывающие окна и противодействует установке вирусов и нежелательных программ, а также включить функцию родительского контроля.

1.2 Место и роль формирования информационной безопасности в курсе информатики основной школы

Становление информационного общества ведет к развитию информационного образа жизни человека, формированию новых информационных структур общества (сети, виртуальные сообщества и др.), возникновению новых проблем информационной экологии личности и общества (компьютерная преступность, угрозы нарушения информационной безопасности, интернет-зависимость и т. д.). Сама информация часто носит противоречивый, агрессивный и негативный характер и влияет на социальные ориентиры общественной жизни, искажая нравственные нормы.

Важным становится понимание личностью сущности понятия «информационная безопасность», которое, по сути, является интегративным для всего школьного курса информатики.

Информационная безопасность становиться стратегически важной задачей как для государства, так и для общества в целом. Информационный образ жизни человека с каждым днем затрагивает все больше сфер его жизнедеятельности и сталкивает с новыми проблемами информационной экологии личности и общества (кибер - преступность, угрозы нарушения информационной безопасности - конфиденциальности личной информации, Интернет-зависимость и т. д.). Попытки управления массовым общественным сознанием через сеть Интернет влияют на социальные ориентиры общественной жизни, искажая нравственные нормы. Мы это видим на примере проявления таких проблем как создание суицидальных групп, сайтов вербовки в религиозные секты, терроризм, разработки психологических методик вовлечения в такие группы.

Данные проблемы, по причине своей важности и актуальности, поднимаются на государственном уровне, так, например, министр образования Васильева О.Ю. на парламентских слушаниях в Совете Федерации предлагает ввести в школьную программу межпредметный школьный курс «основы кибербезопасности», аргументируя это тем, что навык информационной безопасности должен прививаться с малых лет. Образовательный процесс в школах и даже в дошкольных учреждениях должен быть перестроен с учётом требований времени. Важно заниматься профилактикой интернет-зависимости, воспитанием у детей навыков и культуры безопасного пользования Интернетом.

При этом существует проблема недостаточной разработанности методических аспектов формирования данного понятия в рамках содержательной линии социальной информатики, сложности обучения которой обусловлены недостаточным ее отражением в учебниках и учебно-методических пособиях; необходимостью при обучении информатике опоры

на межпредметные связи с гуманитарными науками — философией, культурологией, правом, этикой и др.; использованием неустоявшегося категориально-понятийного аппарата; недостаточным количеством часов для обучения этой линии [1].

Сегодня общественностью обсуждается Концепция по информационной безопасности детей [2], поскольку обеспечение информационной безопасности детей в современном обществе требует скоординированных действий всех заинтересованных лиц: от государственных органов власти, образовательных учреждений, общественных организаций до семьи

Над концепцией работают ведущие отечественные ученые: психологи, культурологи, лингвисты, социологи, медики, журналисты и представители других гуманитарных специальностей. Их задача — заложить правовую базу под изменение российского законодательства с целью сделать его более надежным инструментом по защите детей от вредоносного воздействия информационной среды. Концепция определяет само понятие «информационная безопасность детей», разъясняет спорные и неясные моменты Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию». Так, например, получило определение понятие «безопасная информационная продукция»; обозначены критерии информации, провоцирующей агрессивное поведение детей и подростков; вырабатываются алгоритмы и критерии для отнесения детской электронной продукции к разным возрастным группам.

Система образования сегодня выдвигает одной из ключевых задач, согласно ФГОС, формирование у обучающихся информационной компетентности, на что приоритетно направлено содержание дисциплины «Информатика и ИКТ».

Информационная безопасность важна и с точки зрения формирования универсальных учебных действий (УУД), поскольку ИКТ сегодня являются основой современной учебной деятельности. Понятие «информационная

безопасность» является одним из ключевых понятий линии социальной информатики как научного направления, изучающего комплекс проблем, связанных с протеканием информационных процессов в обществе, влиянием использования ИКТ на общество и личность.

Мы полагаем, что наряду с самим понятием «информационная безопасность» необходимо ввести систему дополнительных вспомогательных дидактических единиц, которая представлена с помощью уровневых понятий.

Данная система является развивающейся, кроме того, в рамках нашего исследования мы разрабатываем адекватные ей методы, формы и средства обучения информатике.

Целью обучения информационной безопасности школьников является приобретенные ими после окончания школы компетенции в области информационной безопасности, которые позволят им с успехом социализироваться в современном информационном обществе. Для этого, соответственно, нужно, чтобы у выпускников было сформировано целостное представление о предметной области обеспечения информационной безопасности. Следовательно, необходимо сформировать у выпускников целостное представление об информационной безопасности и её составляющие (информационная безопасность детей, личности, государства, общества и международная информационная безопасность). Всё это должно происходить в условиях информатизации общества, в момент, когда развитие информационных и коммуникационных технологий делает средства массовой информации главным институтом социализации, который начинает выполнять функции многих традиционных социальных институтов (школы, групп сверстников, семьи и государства).

Заметим: 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» применительно к защите от вредоносного программного обеспечения и защите персональных данных.

Важным становится понимание личностью сущности понятия «информационная безопасность», на что приоритетно должен быть направлен школьный курс информатики. Таким образом, в методике обучения информатики сложилась ситуация, когда необходимо совершенствовать школьный курс информатики и соответственно разрабатывать методику формирования понятия информационной безопасности как интегративного понятия. При этом существует проблема недостаточной разработки методических аспектов формирования данного понятия в рамках содержательной линии социальной информатики, сложности обучения которой, обусловлены необходимостью опоры на межпредметные связи с гуманитарными науками, использованием неустоявшегося категориально-понятийного аппарата, недостаточным количеством часов для обучения.

Охарактеризуем в целом компоненты методики формирования понятия «информационная безопасность»:

Целевой компонент.

Учебные цели:

- формирование представлений учащихся о роли и месте информационной безопасности в современном мире;

- раскрытие понятия информационной безопасности;

- формирование представлений о видах компьютерных угроз, преступлений и факторах, им способствующих;

- систематизация представлений о компьютерных вирусах и вредоносных программах;

- выработка умений и навыков защиты личной информации.

Развивающие цели:

- формирование правовой и этической культуры учащихся как части информационной культуры;

- формирование мировоззрения личности через представления о значимости информационной безопасности в информационной картине мира учащегося;

- развитие опыта оценивать информацию с этических, нравственных позиций.

Воспитательные цели:

- воспитание бережного отношения к конфиденциальности информации, своей и чужой;

- воспитание этического, нравственного неприятия компьютерного вандализма и вирусотворчества;

- воспитание культуры общения в Интернете

; - воспитание ответственности за действия в информационной среде.

Содержательный компонент.

Мы, наряду с понятием «информационная безопасность», считаем необходимым ввести дополнительные вспомогательные дидактические единицы.

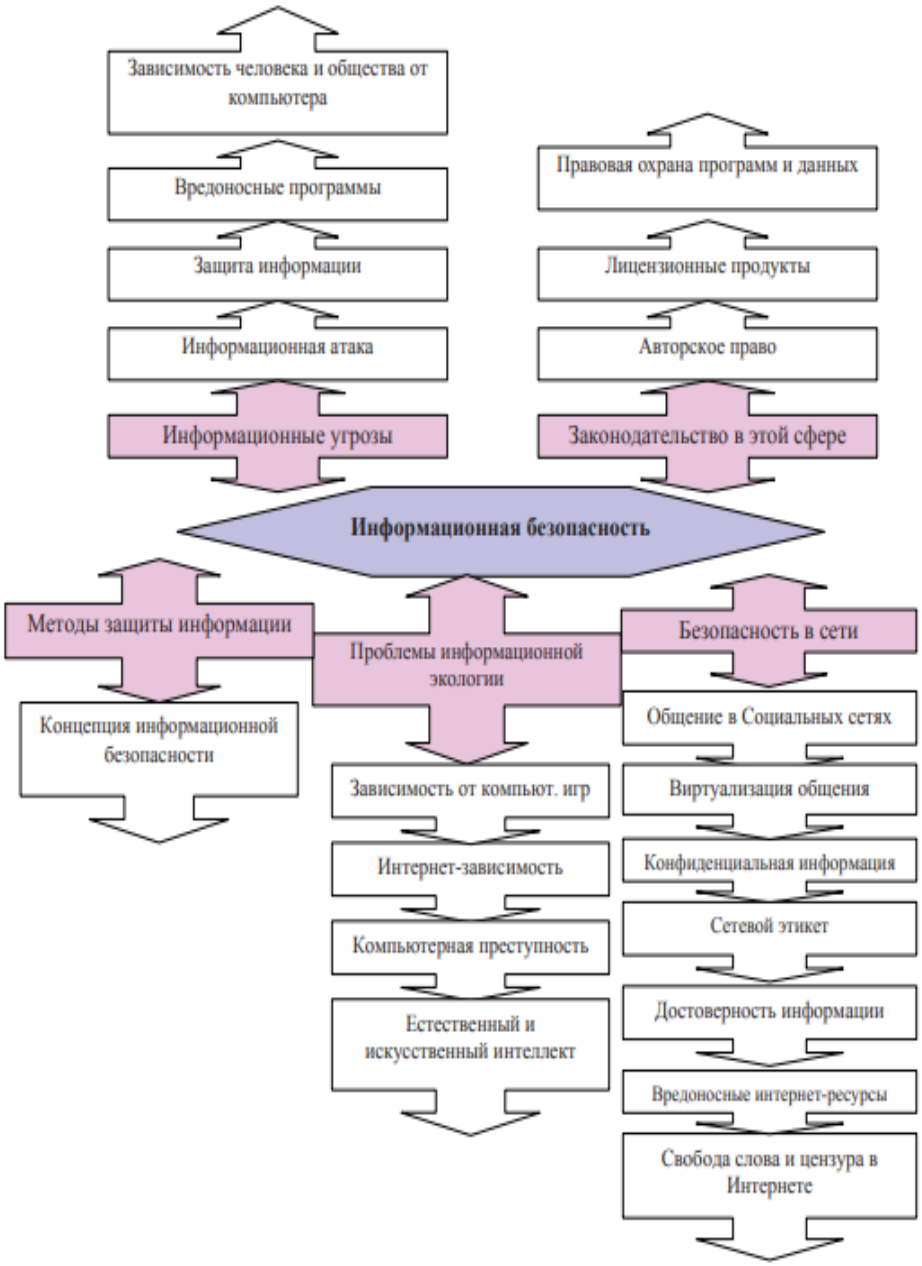

Рис 1. Структура уровневых вспомогательных понятий к понятию «информационная безопасность»

Процессуальный компонент.

Определяя специфику процессуального компонента (методы, средства и формы обучения), мы не можем опираться на распространенные методы обучения (объяснительно-иллюстративный, задачный и т.д.), так как тема информационной безопасности является дискутируемой, связанной с разноплановыми оценками объектов, явлений и процессов современной информационной среды. Поэтому мы определяем доминирование проектного, исследовательского и диалогического методов обучения, метода

построения проблемных ситуаций. Эти методы превалируют, потому что вопросы информационной безопасности носят этический, правовой, философский, культурологический характер.

Выделим специфику формирования понятия информационной безопасности на пропедевтическом этапе обучения информатике в школе.

В пропедевтическом курсе информатики важным является формирование представлений об информации как источнике возможных угроз личности, семье, ближайшему окружению на основе которых вырабатываются умения младшего школьника действовать в определенных типовых ситуациях информационных угроз, в ходе моделирования таких ситуаций в учебной деятельности.

Актуальность изучения понятия «Информационная безопасность» выражается в том, что большинство современных детей рано начинают использовать компьютер — использовать не как предмет изучения, а как удобное средство решения тех или иных повседневных задач или развлечение. Необходимо научить ребенка правильному взаимодействию с компьютером подобно тому, как мы учим его в школе правильно держать ручку или правилам обеспечения собственной безопасности.

Изучение информатики и информационных технологий в пропедевтическом курсе направлено на достижение следующих целей:

- развитие умений ориентироваться в информационных потоках окружающего мира;

- овладение практическими способами работы с информацией: поиск, анализ, преобразование, передача, хранение информации, ее использование в учебной деятельности и повседневной жизни;

- формирование начальной ИКТ-компетентности и элементов информационной культуры;

- развитие умений, позволяющих обмениваться информацией, осуществлять коммуникации с помощью имеющихся технических средств (телефон, магнитофон, компьютер, телевизор и др.);

-развитие умения различать и предугадывать опасности информационной среды.

Выделим основные проблемы, угрожающие младшим школьникам и относящиеся к теме «Информационная безопасность»:

- Зависимость от компьютерных игр;
- Зависимость от общения в социальных сетях;
- Материалы порнографического содержания в сети;
- Сцены насилия и жестокости над людьми в сети;
- Сцены насилия и жестокости над животными в сети;
- Агрессивное поведение (троллинг) в социальных сетях;
- Информация о способах приготовления и применения наркотических средств;
- Информация о способах суицида;
- Суицидальные группы;
- Информация о способах приготовления и применения взрывчатых веществ;
- Стремление к выставлению в социальных сетях опасного селфи;
- Информация, способствующая развитию неприязни по расовому, религиозному, национальному признаку и нагнетанию межнациональной розни;
- Нарушение конфиденциальности личной и чужой информации в сетях;
- Материалы, пропагандирующие различные запрещенные в РФ общества, объединения — фашиствующие, агрессивные неформальные молодежные объединения, религиозные секты и организации.

Наше исследование показывает, что проблема формирования понятия информационной безопасности является одной из ключевых при обучении линии социальной информатики и курса информатики в целом. Это понятие сегодня можно рассматривать как одно из интегративных понятий всего

курса, потому что изучение практически любой содержательной линии в курсе информатики обязательно включает обсуждение какого-либо понятия, раскрывающего понятие информационной безопасности. Например, изучение линии информационных технологий, программного обеспечения — приводит нас к изучению понятия авторского права, вопросов лицензионного программного обеспечения; изучение линии информации и информационных процессов приводит нас к изучению понятий — ответственность за информацию, информационная деятельность человека и т.д.

Также, мы считаем, что целесообразным будет учителю информатики провести беседы с родителями о возможных информационных угрозах для повышения контроля и воспитательных возможностей со стороны родителей.

1.3 Обзор и анализ методов, приемов, форм и средств для успешного формирования информационной безопасности на уроках информатики

В последние годы значительно возросло число атак и угроз несанкционированного доступа к личным данным пользователей информационной сети, что приводит к моральному, а порой и к материальному ущербу. Грамотное использование различных мер по их предотвращению и способов устранения одна из основных проблем информационной безопасности современного общества. В связи, с чем актуальным является вопрос обучения использования мер, средств и методов защиты данных, начиная со школы.

Цели обучения информационной безопасности школьников старших классов отражены в федеральных государственных образовательных стандартах (ФГОС), учебных планах, программах, согласно которым у выпускника должно сформироваться целостное представление о способах защиты персональных данных, рабочего места и о мерах предотвращения угроз информационной безопасности. Однако, анализ различных методических подходов (В. Г. Герасименко, Д. П. Зегжда, А. А. Малюк, М. П.

Сычев, С. П. Расторгуев, С. Пейпертом и др.) к освещению данной проблемы в школьном курсе информатики свидетельствует о том, что лишь незначительное внимание уделяется теоретическим аспектам информационной безопасности в рамках раздела «Социальная информатика» в старших классах, в то время, как практическая реализация защиты информации отсутствует.

В тех малочисленных случаях, когда в учебниках по предмету «Информатика и ИКТ» упоминается понятие «информационная безопасность», оно, как правило, применяется только в узком его смысле. Например, в учебнике А.Г. Гейн и А.И. Сенокосова «Информатика и ИКТ» [4] под информационной безопасностью понимается: «состояние защищенности информации и поддерживающей инфраструктуры информационной системы от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб субъектам информационных отношений, имеющих место в рамках данной информационной системы». А в учебнике «Информатика и ИКТ» для 11 класса под редакцией профессора Н.В. Макаровой (2009) [8] «информационная безопасность – это совокупность мер по защите информационной среды общества и человека».

В обоих приведённых примерах делается акцент на защите информации: в первом случае – в рамках информационной системы, а во втором – в информационной среде. Следует отметить, что в Доктрине об информационной безопасности главным определение этого понятия является «сбалансированность интересов личности, общества и государства».

Исходя из анализа, следует определять понятие информационной безопасности, исходя из широкого смысла, то есть, говоря о формировании системных знаний в столь значимой в современном информационном обществе области, как обеспечение информационной безопасности.

Рассматривая ФГОС по Информатике и ИКТ среднего (общего) и хотелось бы отметить, что целью обучения Информационной безопасности в

ходе освоения основной общеобразовательной программы заключается в формировании у старшеклассников умения использовать средства коммуникационных и информационных технологий в решении заданных задач с соблюдением всех необходимых норм информационной безопасности. Построенная на основе изложенных выше подходов к ключевым компонентам формируемой методики обучения ИБ модель обучения ИБ старшеклассников представлена в таблице 1.

Таблица 1. Модель обучения информационной безопасности старшеклассников

<table>
<tr><td>Предметная область</td><td colspan="5">Области обеспечения ИБ</td></tr>
<tr><td></td><td>ИБ детей</td><td>ИБ личности</td><td>ИБ общества</td><td>ИБ государства</td><td>международная ИБ</td></tr>
<tr><td>Цель обучения</td><td colspan="5">Социализация, профориентация и профильное обучение школьников в области ИБ</td></tr>
<tr><td rowspan="2">Содержание бучения</td><td colspan="3">Базовый уровень</td><td colspan="2">Профильный уровень</td></tr>
<tr><td colspan="2">ФГОС Среднего (полного) общего образования, примерные программы, учебно-методические материалы</td><td>Стандарты направлений профессиональной подготовки, не входящие в направление «Информационная безопасность» ГОСТ ВПО РФ, в содержании обучения которых значительное место занимают проблемы обеспечения ИБ</td><td>ФГОС Среднего (полного) общего образования, примерные программы, учебно-методические материалы</td><td>Стандарты направления «Информационная безопасность» ГОСТ ВПО РФ</td></tr>
<tr><td rowspan="4">Методы обучения</td><td colspan="3">Базовый уровень</td><td colspan="2">Профильный уровень</td></tr>
<tr><td colspan="5">моделирование</td></tr>
<tr><td>Модели обучения ИБ</td><td>Практические модели (Построение на основе концептуальной модели ИБ типовых поведенческих сценариев обеспечения ИБ детей и личности)</td><td colspan="2">Экспериментальные модели (Исследование особенностей компонентов концептуальной модели обеспечения ИБ применительно к характерным общественным структурам с учетом возможности вхождения старшеклассников в различные социальные группы, общественные объединения, организации и др.)</td><td>Познавательные модели (Формирование представлений об обеспечении ИБ государства и международной ИБ на основе соответствующих компонентов концептуальной модели обеспечения ИБ)</td></tr>
<tr><td>Области обеспечения ИБ</td><td>ИБ детей</td><td>ИБ личности</td><td>ИБ общества</td><td>ИБ государства</td><td>международная ИБ</td></tr>
<tr><td rowspan="3">Формы обучения</td><td colspan="3">Базовый уровень</td><td colspan="2">Профильный уровень</td></tr>
<tr><td colspan="3">Уроки «Информатика и ИКТ», элективные курсы (темы, связанные с ИБ)</td><td colspan="2">Уроки «Информатика и ИКТ», элективный курс «Основы информационной безопасности»</td></tr>
<tr><td colspan="3">Внеурочная деятельность (экскурсии, проект, позволяющие оценить риски ИБ в социальных группах и др.)</td><td colspan="2">Внеурочная деятельность (экскурсии с посещением специализированных выставок, лабораторий и др., проект, по разработке моделей ИБ для изучаемой области обеспечения ИБ, дистанционная форма</td></tr>
<tr><td rowspan="3">Средства обучения</td><td colspan="3">Базовый уровень</td><td colspan="2">Профильный уровень</td></tr>
<tr><td colspan="3">Учебные тексты, интернет-источники, демонстрационные примеры, готовые модели, программные средства</td><td colspan="2">Учебные тексты, интернет-источники, демонстрационные примеры, готовые модели, программные средства. Специализированные программно-аппаратные средства. Средства компьютерных телекоммуникаций, имитационные и моделирующие педагогические программные средства, инструментальные программные средства.</td></tr>
<tr><td colspan="5">Доступные для демонстрации и изучения средства обеспечения комплексной информационной безопасности образовательного учреждения</td></tr>
</table>

Цели обучения школьников ИБ в педагогическом процессе находят свое отражение в федеральных государственных образовательных стандартах (ФГОС), учебных планах, программах.

В ФГОС среднего (полного) общего образования цель обучения ИБ в ходе освоения основной образовательной программы среднего (полного) общего образования заключается в формировании у старшеклассников умения использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением норм ИБ.

Цель обучения ИБ заложена и в требованиях к предметным результатам освоения базового курса информатики, которые предполагают понимание основ правовых аспектов использования компьютерных программ и работы в Интернете.

В ходе усвоения углубленного курса информатики, целью обучения ИБ является формирование у старшеклассников знаний принципов обеспечения информационной безопасности, способов и средств обеспечения надёжного функционирования средств информационных и коммуникационных технологий (далее ИКТ).

Для примера, подтверждающего использование подобного подхода в школьных учебниках по предмету «Информатика и ИКТ» рассмотрим содержание параграфа 35 «Этика интернета. Безопасность в Интернете» учебника для 9 класса А.Г. Гейн «Информатика и информационные технологии» [4]. Оно почти полностью повторяет содержание параграфа 44 с таким же названием «Этика интернета. Безопасность в Интернете» в учебнике по предмету «Информатика и ИКТ» для 11 класса А.Г. Гейн [3]. Та же ситуация складывается и с параграфом 36 «Защита информации» учебника для 9 класса. Параграф 36 повторяется с незначительными изменениями в учебнике для 11 класса, только порядковый номер стал 46.

Для подтверждения своих слов, хотелось бы рассмотреть содержание раздела «Защита информации» в учебнике Н.Д. Угриновича для 8 класса

«Информатика и ИКТ» [16]. Информация в параграфе дублируется с незначительными изменениями в разделе «Защита от несанкционированного доступа к информации» в учебниках этого же автора, только за 10 класс [11].

В вопросах изучения информационной безопасности в средней и старшей школах необходимо использовать спиральный принцип обучения для обеспечения соответствия уровня сложности материала возрастным особенностям учеников. Необходимо углубленное содержание раскрываемых понятий. Школьники при таком подходе получат увеличенный интерес к вопросам информационной безопасности, смогут расширить свой кругозор, улучшат мотивацию к восприятию нового материала.

Так же анализ учебных материалов различных авторов для 8-11 классов привёл к выводу, что некоторые авторы учебников, приводя конкретные примеры, не дают определения основным понятия по информационной безопасности, ограничиваясь примерами и отсылая обучающегося к Интернет – источникам, которые зачастую даже не рассчитаны на аудиторию этого возраста.

Например, в учебнике Л.Ф. Соловьевой для 8 класса «Информатика и ИКТ» [17] приводятся следующие рекомендации по работе с основными понятиями в области информационной безопасности: «Основные понятия и термины, используемые в сфере информационной безопасности при работе в интернете можно найти, например, в справочной системе обозревателя Internet Explorer». И далее: «в Интернете нет недостатка в сведениях, касающихся информационной безопасности при работе в сети. На сайте http://www.securitylab.ru, например, можно найти подробный обзор существующих угроз и дополнительных средств обеспечения информационной безопасности». Или, например, «Пользуясь справочной службой операционной системы Windows, можно найти необходимые для обеспечения информационной безопасности сведения». Это не позволяет сформировать системные знания учащихся о данной предметной области.

Модель содержания обучения учащихся средней и старшей школ предполагает преемственность знаний по информационной безопасности с предыдущими ступенями обучения, систематизацию понятий в этой области знания.

Примером систематизации понятий отдельных тем по информационной безопасности может быть материал учебника И.Г. Семакина для 10–11 классов «Информатика и ИКТ (базовый уровень)» [10] (параграф 12 второй главы «Информационные процессы и системы»). Авторами систематизированы основные понятия в области защиты цифровой информации и представлены в виде иерархической схемы под названием Система основных понятий (рис. 2).

<table>
<tr><td colspan="4">Защита цифровой информации</td></tr>
<tr><td colspan="4">Цифровая информация —
информация, хранение, передача и обработка которой осуществляются средствами ИКТ</td></tr>
<tr><td colspan="4">Защищаемая информация —
информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.</td></tr>
<tr><td colspan="2">Угроза утечки</td><td colspan="2">Угроза разрушения</td></tr>
<tr><td colspan="2">Преднамеренная кража, копирование, прослушивание и пр.</td><td>Несанкционированное разрушение</td><td>Непреднамеренное разрушение</td></tr>
<tr><td>Проникновение в память компьютера, в базы данных информационных систем</td><td>Перехват в каналах передачи данных, искажение, подлог данных</td><td>Вредоносные программные коды-вирусы; деятельность хакеров, атаки</td><td>Ошибки пользователя, сбои оборудования, ошибки и сбои в работе ПО, форс-мажорные обстоятельства</td></tr>
<tr><td colspan="4">Меры защиты информации</td></tr>
<tr><td colspan="2">Физическая защита каналов; криптографические шифры; цифровая подпись и сертификаты</td><td>Антивирусные программы; брандмауэры; межсетевые экраны</td><td>Резервное копирование; использование ББП; контроль и профилактика оборудования; разграничение доступа</td></tr>
</table>

Рис. 2 Система основных понятий

Так же анализ содержания учебников по предмету «Информатика и ИКТ» показал взаимосвязь технологических научных понятий в области информационной безопасности и более широкого круга понятий, которые

относятся к информационной культуре: информационная этика, этика интернета, компьютерная этика, сетевой этикет, этика сетевого общения, нормы поведения при использовании информации. Наверняка это связано с тем, что информационная безопасность связана со всеми сферами жизни школьников.

Например, в учебнике А.Г. Гейна для восьмого класса «Информатика и информационные технологии» [5] устанавливается важная связь понятия «информационная культура» и аспектов информационной безопасности: «Информационная культура каждого человека подразумевает готовность человека к жизни и деятельности в высокоразвитой информационной среде, умение эффективно использовать ее возможности и защищаться от ее негативных воздействий». В характеристике составляющих элементов информационной культуры указаны, в том числе, имеющие непосредственное отношение к области информационной безопасности поступающей информации и этичное поведение при использовании информации», что также указывает на соподчиненность понятия «информационной этики» понятию «информационная культура».

Н.Д. Угринович в своём учебник «Информатика и ИКТ» для 9 класса [16] считает, что «информационная культура состоит не только в овладении определенным комплексом знаний и умений в области информационных и коммуникационных технологий, но и предполагает знание и соблюдение юридических и этических норм и правил».

Подобным образом, авторы создают предпосылки для конкретизации и систематизации, на первый взгляд, достаточно абстрактных культурологических понятий, которые непосредственно связанны с областью информационной безопасности. С другой стороны, необходимо при обучении информационной безопасности избегать излишней конкретики и обеспечивать учеников правдивой информации на момент её приобретения. Например, утверждение Н.Д. Угриновича в своём учебнике «Информатика и ИКТ» для 8 класса [15] о том, что «наиболее надёжную защиту от вирусов

обеспечивают российские антивирусные системы DrWeb и Антивирус Касперского» кажутся слишком категоричными и не совсем отражают действительность.

Анализируя преемственность содержания обучения в вопросах информационной безопасности было установлено, что имеет место быть достаточно большой дисбаланс в равномерности распределения материала для каждого класса, последовательность выдачи материала происходит без учета важных внутрипредметных связей.

В настоящее время необходимость введения курса «Информатика» до 7 класса оставляется на усмотрение школы. Таким образом, формирование компьютерной грамотности у школьников младшего возраста, а также их навыков безопасного пользования сетью практически целиком и полностью возлагается на родителей, на факультативные дисциплины и дополнительные занятия в школе. Рассмотрим, какое внимание уделяется вопросам личной информационной безопасности у школьников среднего и старшего звена в популярных учебниках по информатике различных авторов.

Так, в соответствии с пояснительной запиской к линии учебников «Информатика» для 7-9 классов общеобразовательных учреждений И. Г. Семакина, Л. А. Залоговой, С. В. Русакова, Л. В. Шестаковой [3], на формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права направлен единственный параграф «Информационная безопасность», в котором одновременно рассматриваются понятие об информационных преступлениях, правовая защита информации (законодательство), программнотехнические способы защиты, компьютерные вирусы, антивирусные средства, опасности при работе в Интернете и средства защиты.

В предметной линии учебников «Информатика» для 7-9 классов Н. Д. Угриновича [4] рассматриваемой проблеме уделяется 4 часа в 9 классе в рамках темы «Информационное общество и информационная безопасность»,

где освещаются вопросы правовой охраны программ и данных, защиты информации, правовой охраны информации, лицензионных, условно бесплатных и свободно распространяемых программах, т. е. основной акцент в данной теме приходится на изучение авторского права и защиты интеллектуальной собственности.

В учебниках по информатике для 5-9 классов Л. Л. Босовой и А. Ю. Босовой [5], на формирование навыков в области информационной безопасности в соответствии с пояснительной запиской приходятся темы, которые лишь косвенно способствуют повышению уровня безопасного поведения при работе с компьютером, в частности в Интернете: в 5 классе – тема «Передача информации», в 6 классе – «Всемирная паутина», «Программное обеспечение компьютера», в 9 классе – «Информационные ресурсы и сервисы Интернета».

Метапредметные результаты освоения основной образовательной программы [6] в старшей школе (10-11 классы) в соответствии с ФГОС основного среднего (полного) образования должны, в числе прочего, отражать «использование средств ИКТ с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности». Так же, согласно требованиям к результатам освоения ООП полного общего образования по учебному предмету «Математика и информатика», необходимо: «... сформировать понимание основ правовых аспектов использования компьютерных программ и работы в Интернете», «сформировать представление о влиянии информационных технологий на жизнь человека в обществе… », «принятие этических аспектов информационных технологий; осознание ответственности людей, вовлеченных в создание и использование информационных систем, распространение информации».

В соответствии с пояснительной запиской к завершенной предметной линии «Информатика» для 10-11 классов Н. Д. Угриновича [7], вопросы по информационной безопасности включены в тему «Социальная информатика»

(2 часа в 11 классе), наряду с вопросами «Информационное общество», «Информационная культура», «Правовые основы информационной среды», «Лицензирование программного обеспечения», «Социальные сервисы и сети».

В методических рекомендациях по информатике И. Г. Семакина [8] в разделе социальной информатики на более глубоком уровне, чем в основной школе, раскрываются проблемы информатизации общества, информационного права, информационной безопасности. При этом, в соответствии с этими рекомендациями, вопросам информационной безопасности уделяется 2 часа.

Авторы Н. В. Макарова, Ю. Ф. Титова, Ю. Н. Нилова в своем учебнике по информатике [9] для формирования рассмотренных выше метапредметных результатов освоения программы предлагают две темы: «Этика сетевого общения» и «Информационная безопасность сетевой технологии работы».

Выполнив полный анализ содержания учебников на предмет содержания в них требований стандартов и примерных образовательных программ в области обучения вопросам информационной безопасности учащихся основной и старшей школы, хотелось бы отметить, что авторы включают в содержание учебника практически все понятия стандарта. Но многие из этих авторов не вводят понятие «информационная безопасность», несмотря на то, что оно указано в требованиях ФГОС как для основной, так и для старшей школы. При этом авторы учебников по информатике предпочитают использовать концентрический принцип в преподавании разделов, относящихся к данной проблематике, часто повторяя содержание по данному разделу в неизменном виде, как в основной школе, так и в старшей.

Таким образом, в настоящее время содержание учебников по информатике базового уровня недостаточно формирует компетентную базу личной информационной безопасности школьника в современной

информационной среде, что может негативно сказаться на психологическом и нравственном здоровье учащихся. Во всех приведенных авторских линиях не рассматриваются вопросы, связанные с навыками фильтрации нежелательного контента из огромной массы информации в Интернете, противодействия деструктивным программам, фишингу, психологическим преследованиям в сети, а также профилактикой интернет-зависимости у детей

Для решения данной проблемы необходимо реализовать следующие методические рекомендации:

- для базового курса информатики в старших классах выделить 5 уроков на изучение информационной безопасности, где уделить особое внимание практической реализации защиты информации (например, изучение процесса кодирования слов с использованием ключевого слова);
- для углубленного курса – следует рассмотреть вопросы связанные не только с механизмом защиты данных, но и предотвращения их возникновения (например, организация процесса сканирования наличия уязвимостей в информационной сети);
- внедрение элективного курса «Информационная безопасность», задача которого сформировать у учащихся представления о сущности информационной безопасности, развить навыки защиты информации на персональном компьютере и в глобальной сети;
- организация и проведения недели «Безопасного интернета» учениками под руководством учителя информатики и классных руководителей.

В рамках недели «Безопасного интернета» ученики средних и старших классов разрабатывают и проводят для 1-4 классов: урок на тему «Путешествие в страну Интернет» и конкурс буклетов и презентаций на тему «Как я должен вести себя в интернете». Для 5-7 классов организуют круглый стол «Как защитить себя от атак в глобальной сети», проводят урок на тему: «Интернет-безопасность», а для 8-10 классов – деловая игра – дебаты «Я и

Интернет». Кроме того, можно провести общешкольное родительское собрание «Интернет. Территория безопасности», где выпускники на основе полученных знаний делаться опытом о правилах работы в сети интернет и формируют у слушателей в ходе дискуссии навыки работы по защите от вирусов, организации защиты своих персональных данных и др.

В рамках ВКР невозможно разработать полный курс, охватывающий все аспекты информационной безопасности, поэтому в целях формирования умений и навыков защиты информации мы предлагаем в старших классах в рамках элективного курса «Современные антивирусные программы» изучить ряд тем формирующих теоретические знания о современных компьютерных вирусах и практические умения и навыки работы с антивирусными программами.

Выводы по главе 1

1. Школьники, испытывающие дефицит общения в реальной жизни, неосознанно переносят опыт общения в сети Интернет на общение в повседневной жизни. Имея минимум жизненного опыта, дети не видят угроз, которые присутствуют в глобальной интернет-сети.

2. Информационная безопасность в образовательном учреждении – это состояние защищенности от угроз интересов личности, заключающееся в умении выявлять и вовремя пресекать угрозы информационного влияния в условиях школьной среды.

3. В работе показано, что в настоящее время содержание учебников по информатике базового уровня недостаточно формирует компетентную базу личной информационной безопасности школьника в современной информационной среде. Помимо разработки норм поведения и рекомендаций необходимо проводить дополнительные занятия со школьниками, развивающие практические компетенции безопасного применения ИКТ на уроках информатики.

4. Компьютерные вирусы приносят большой урон пользователям компьютерной техники. Чтобы эффективно бороться с вирусами, необходимо иметь представление о вирусах и разбираться в методах борьбы с ними. В рамках элективного курса «Современные антивирусные программы», позволяет сформировать целостное представление о компьютерных вирусах, методах и средствах борьбы с ними у современных школьников.

Глава 2. Элективный курс «Современные антивирусные программы»

2.1 Цели и задачи элективного курса.

Традиционная подготовка учащихся, сложившаяся в современной системе образования, к сожалению, в данный момент малоэффективна, так как не обеспечивает современной подготовки в области антивирусной защиты.

Из анализа, современной учебной литературы и фактического состояния проблемы, можно сделать вывод о необходимости разработки такой системы занятий, которая отражает типичные ситуации, возникающие в практической деятельности учащихся и связанные с компьютерными вирусами.

В целях формирования умений и навыков защиты информации мы предлагаем в старших классах в рамках элективного курса «Современные антивирусные программы» включить ряд тем формирующих теоретические знания о современных компьютерных вирусах и практические умения и навыки работы с антивирусными программами.

Модуль «Компьютерные вирусы и антивирусная защита» включает следующие основные вопросы:

- Понятие «компьютерный вирус». Виды компьютерных вирусов. Особенностями каждого вида вируса. Признаки заражения вирусами. Способы заражения. Примеры компьютерных вирусов.
- Методы защиты: программные, аппаратные, организационные методы защиты.
- Защита от вирусов: общие средства защиты информации (резервное копирование информации; разграничение доступа); профилактические меры, уменьшающие вероятность заражения; специализированные программы для защиты от вирусов; методы поиска вирусов, применяемые антивирусными

программами: сканирование, эвристический анализ, обнаружение изменений, резидентные мониторы; ошибочные действия пользователей.

- Предотвращение заражения компьютерными вирусами: предотвращение поступления вирусов; предотвращение вирусной атаки, если вирус все-таки поступил на ПК; предотвращение разрушительных последствий, если атака все-таки произошла.

Данный модуль позволяет сформировать целостное представление о компьютерных вирусах: как появлялись, рассмотреть процесс эволюции вирусов, какие способы распространения и обхода антивирусов, какие методы борьбы с ними существовали раньше и современные методы, какие компьютерные угрозы существуют в данный момент вместе с вирусами и т.д.

По данному модулю учащиеся выполняют проект, готовят доклады, выступают со своими инновационными предложениями по защите информации от компьютерных вирусов. В процессе работы учащиеся овладевают как общеучебными умениями и навыками (универсальные для многих школьных предметов способы получения и применения знаний), так и предметными (специфические для информатики). Школьники учатся самостоятельно пополнять свои знания, ориентироваться в современной ситуации по изучаемой теме, приобретают опыт коллективной, групповой и индивидуальной работы.

Особо следует выделить практическую составляющую данного модуля. Для полноценного усвоения курса и совершенствования практических умений и навыков, каждый раздел должен подкрепляться практической работой. Практическая работа повышает интерес к изучению вопросов, связанных с информационной безопасности. Учащиеся получают возможность непосредственной работы с компьютерными вирусами, последствиями заражения, программами антивирусной защиты, их видами и

назначением, а также практические навыки тестирования различных объектов на заражение компьютерными вирусами.

В процессе изучения раздела учащиеся получают навыки:

◦ самостоятельного мышления, умения находить и решать проблемы защиты информации;

◦ привлечения знаний из разных областей современных наук;

◦ прогнозирования результатов и возможных последствий применения различных средств защиты;

◦ установления причинно-следственных связей;

◦ ответственного отношения к процессу работы с информацией и осознанного осуществления антивирусной защиты и т.д.

Цели обучения.

Образовательные:

- обобщить знания по теме «Компьютерные вирусы и антивирусные программы»;
- формировать навыки работы с антивирусной программой;
- научить выполнять проверку на наличие вирусов с помощью программы Антивирус Касперского;
- развивать информационную культуру и компьютерную грамотность;
- изучить современные антивирусные программы.

Развивающие:

- развитие способности ориентироваться в современных антивирусных программах;
- способствовать формированию умений обучающихся выделять критерии для анализа,
- развивать умения поиска и анализа информации по выделенным критериям на заданную тему;
- развитие способности к рефлексии, контролю и самоконтролю.

Воспитательные:

- способствовать созданию благоприятного психологического климата в группе,
- формирование умения работать в команде, коммуникативных навыков.

2.2. Содержание элективного курса «Современные антивирусные программы»

Рассмотрим содержательную часть курса, разработанную на основе целей. В основе содержания лежит теоретическая подготовка, а также практический опыт.

Тематическое планирование

Таблица 2. Тематический план элективного курса

№ п/п	Тема занятия	Содержание	Часы
1	Техника безопасности при работе ПК. Понятие информационной безопасности	ТБ и ПБ в кабинете информатики. Понятие «информационная безопасность»	1
2	Угрозы информационной безопасности.	Виды угроз подвергающих информацию в опасность (взлом, копирование, проникновение вирусов).	1
3	Виды компьютерных вирусов	Виды компьютерных вирусов.	1
4	Антивирусные программы	Виды антивирусных программ.	1
5	Практическая работа №1«Установка и обзор антивирусной программы в ПК»	Установка и обзор антивирусной программы Касперского.	1
6	Практическая работа №2 «Работа антивирусных программ по поиску угрозы на ПК»	Поиск угроз на ПК, способы поиска.	1
7	Уровни защиты информации.	Уровни защита информации, методы организации защиты.	1
8	Практическая работа №3 «Поиск вирусов	Показать на примере поиск вирусов.	1

	на флеш носителе»		
9	Правовая защита информации.	Понятие правовая защита, законы и подзаконные акты.	1
10	Виды компьютерных правонарушений.	Виды правонарушений при работе (использовании) на ПК.	1
11	Защита авторских прав на тиражирование информации.	Понятие «авторское право». Ознакомление с видами защиты дисков.	1
12	Практическая работа №4 «Степень защиты лицензионных дисков»	Показать на примере невозможность копирования дисков.	1
13	Виды программного обеспечения (лицензионное, условно бесплатное, бесплатное).	Виды программного обеспечения (на примере лицензионных обучающих дисков)	1
14	Обеспечение информационной безопасности средствами ОС Windows XP	Средства информационной безопасности ОС.	1
15	Практическая работа №5 «Создаем защиту файлов»	Защита файлов хранящихся на ПК или носителях.	1
16	Параметры безопасности ПК	Знакомство с параметрами безопасности.	1
17	Практическая работа №6 «настройка параметров безопасности»	Настройка параметров безопасности на ПК.	1
18	Паролирование ПК	Виды паролей, критерии устойчивости паролей, установка и смена паролей.	1
19	Практическая работа №7 «Ставим пароль на ПК в ПЗУ»	Показать на примере ввода пароля на ПЗУ. Повторение «Что такое ПЗУ»	1
20	Средства восстановления системы	Понятие восстановления системы.	1
21	Практическая работа №8 «Восстановление системы с ранее созданных образов»	Восстановление системы на основе ранее созданных образов.	1
22	Служебные программы Windows 7-10: очистка диска, дефрагментация диска, аварийное восстановление пароля.	Служебные программы Windows 7-10.	1

23	Отличие защиты Windows 7-10 и Seven	Отличия защиты на ОС на примере Microsoft	1
24	Современные защиты данных	Современные защиты данных	1
25	Новые технологии защиты данных	Новые технологиями защиты данных	1
26	Создание учетной записи	Создание учетной записи	1
27	Изменение типа учетной записи	Изменение типа учетной записи	1
28	Создание пароля в своей учетной записи	Понятие создание пароля в учетной записи	1
29	Практическая работа №9 «Что делать, если забыли пароль?»	Практическая работа, как восстанавливается пароль на ПК	1
30	Администрирование ПК	Понятие «Администрирование ПК»	1
31	Принципы и приемы защиты информации во время транспортировки по электронным сетям	Принципами и приемами защиты информации.	1
32	Сетевая безопасность	«Что такое сетевое окружение» Понятие сетевой безопасности.	1
33	Практическая работа №10 «Пути проникновения вирусов и вредоносных программ в ПК»	Показать на примере пути проникновения вирусных программ в ПК	1
34	Зачет «Защита компьютера в своем доме»	Проверка ЗУН по теме «Защита информации»	1
		Итого	34

Рассмотрим подробнее содержание некоторых тем элективного курса.

Тема «Виды компьютерных вирусов»

Компьютерный вирус - это специально написанная небольшая по размерам программа, которая может записывать свои копии в компьютерные программы, расположенные в исполнимых файлах, системных областях дисков, драйверах, документах и т.д., причём эти копии сохраняют возможность к "размножению". Процесс внедрения вирусом своей копии в

другую программу называется заражением, а программа или иной объект, содержащий вирус - заражённым.

Если вы подозреваете, что компьютер заражен вирусом, или уверены в этом, то ниже перечислены некоторые основные признаки заражения компьютера:

- Компьютер работает медленнее, чем обычно.
- Компьютер перестает отвечать или периодически блокируется.
- В работе компьютера происходит сбой, затем он перезагружается каждые несколько минут.
- Компьютер самопроизвольно перезагружается. Кроме того, компьютер работает не так, как обычно.
- Приложения, установленные на компьютере, работают неправильно.
- Не удается получить доступ к дискам.
- Не удается правильно распечатать документы.
- Появляются необычные сообщения об ошибках.
- Меню и диалоговые окна отображаются в искаженном виде.
- Недавно открытое вложение имеет двойное расширение (JPG, VBS, GIF или EXE).
- Антивирусная программа почему-то оказалась отключена. Кроме того, ее не удается запустить снова.
- Антивирусную программу невозможно установить или запустить.
- На рабочем столе появляются новые значки, которые туда никто не помещал, или значки, не связанные с последними установленными программами.
- Динамики неожиданно воспроизводят странные звуки или музыку.
- С компьютера самопроизвольно удаляются приложения.

При заражении компьютера вирусом (или при подозрении на это) важно соблюдать определенные правила.

Прежде всего, не надо торопиться и предпринимать опрометчивых действий, непродуманные действия могут привести не только к потере части данных, которые можно было бы восстановить, но и к повторному заражению компьютера.

Тем не менее, одно действие должно быть выполнено немедленно. Если Вы не абсолютно уверены в том, что обнаружили вирус до того, как он успел активизироваться на Вашем компьютере, то надо выключить компьютер, чтобы вирус не продолжал своих разрушительных действий.

Все действия по обнаружению вида заражения и лечению компьютера следует выполнять только при правильной загрузке.

Лечение от вируса обычно несложно, но иногда (при существенных разрушениях, причинённых вирусом) оно очень затруднительно. Если Вы не обладаете достаточными знаниями и опытом для лечения компьютера, попросите помочь Вам более опытных коллег.

Тема «Работа антивирусных программ по поиску угрозы на ПК»

Обзор антивирусной программы «Касперский»

Одним из распространенных заблуждений пользователей на сегодняшний день является то, что защита бесплатных антивирусных продуктов совершенно идентична помощи платных аналогичных программ. Это не совсем так. Для установки на домашний компьютер может и хватить простого бесплатного антивируса, но при условии, что регулярно будет проводиться обновление базы. Но если заражение все же произойдет, то потребуется помощь квалифицированных специалистов, в то время, как качественный платный антивирус справится в большинстве случаев с возникшей проблемой самостоятельно. Поэтому часто бывает целесообразно, чтобы не платить каждый раз, обеспечить для своего компьютера надежную защиту на платной основе.

Одним из таких качественных антивирусных продуктов на платной основе является Антивирус Касперского.

Лаборатория Касперского занимается выпуском антивирусных продуктов уже на протяжении 15 лет, что свидетельствует о качестве и востребованности их продукции. Стоит отметить, что центральный офис компании расположен в Москве, но услугами антивирусного продукта пользуется сегодня население более 200 стран всего мира.

Развитие компании достаточно быстрое и динамичное. На рынок представлены различные программные модификации, которые могут использоваться и для домашних условий, и для корпоративных сетей даже крупных предприятий. Теперь не одно приложение работниками компании выпущено и для защиты мобильных устройств.

Прежде, чем говорить о плюсах и минусах программы стоит иметь представление о самом программном продукте. Разработчики заботятся о конкурентоспособности своей продукции, поэтому своевременно дорабатывают и обновляют программы. Все современные версии антивируса обладают необходимыми возможностями для обеспечения полной защиты, компьютера на котором они установлены:

- Защиты от всех видов интернет-угроз.
- Полноценная защита от всех видов вирусов и атак, которая включает эвристический анализ, поведенческую блокировку, проверку по всем базам.
- Проверка трафика, почтовых сообщений и скачиваемых файлов в режиме реального времени.
- Защита от спама и фишинга.
- Родительский контроль.
- Защита от утечек всей конфиденциальной информации.
- Автоматическое обновление баз.
- Постоянный сетевой контроль. [10]

Как уже отмечалось, на рынок производитель поставляет несколько модификаций своей программы, каждая из которых предназначена для выполнения определенных целей и задач:

1. Для корпоративной сети стоит приобрести Kaspersky Endpoint Security.
2. Для всех видов мобильных устройств Kaspersky Mobile Security.
3. Для персональных компьютеров, установленных дома и не подключенных в локальную сеть, можно выбрать из Антивирус Касперского и Kaspersky Internet Security.

Рис. 3 Kaspersky Endpoint Security

Каждый из продуктов отличается качественной и до мелочей продуманной и реализованной защитой, причем стоимость использования его привлекательная и не будет большой тратой для владельца компьютера. Позволить себе такую защиту сегодня может практически каждый владелец персонального компьютера.

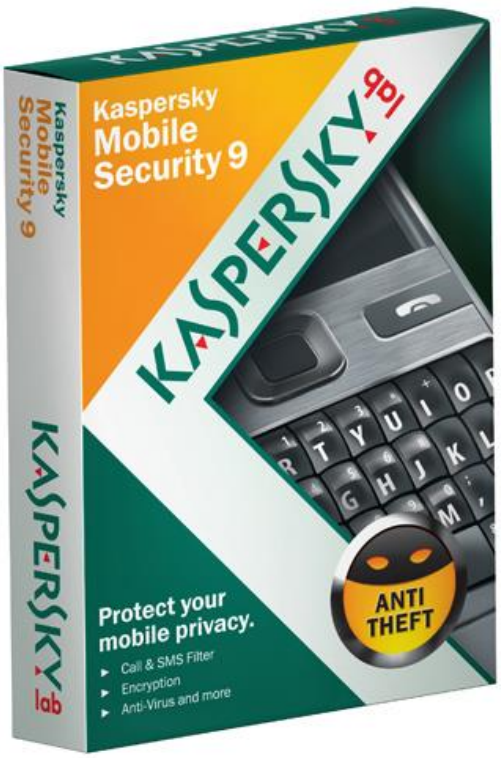

Рис. 4 Kaspersky Mobile Security

Вся информация по каждому продукту есть на официальном сайте разработчика, а также там располагаются и условия использования с указанием стоимости.

Естественно, на все функции и модули для обеспечения полноценной защиты можно рассчитывать только при приобретении ключа. Бесплатная версия программы не сможет обеспечить тот уровень защиты, о котором рассказывается.

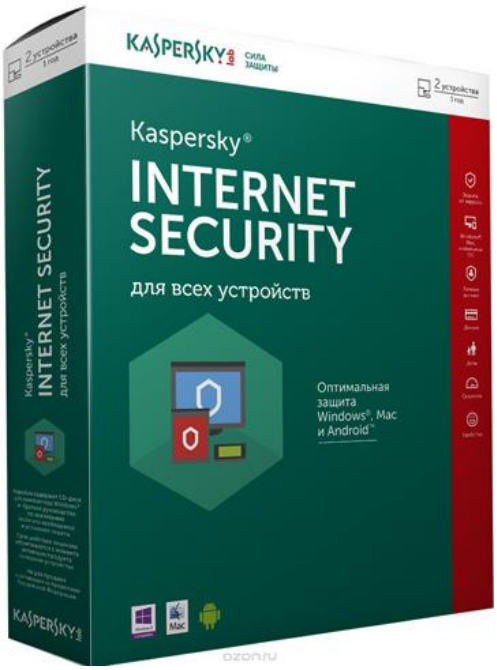

Рис. 5 Kaspersky Internet Security

Зная особенности программного продукта можно выделить и основные плюсы, и минусы.

Преимущества антивируса Касперского.

Если ознакомиться с отзывами и обзорами по работе антивируса, то в среднем сложится положительное впечатление, ведь программа имеет массу плюсов. Основные из них, следует выделить:

- Быстрая и качественная защита устройства от любого вида вирусов и атак.
- Стильный и удобный интерфейс программного продукта.
- Своевременное обновление баз.
- Надежность.
- Продуманность каждого модуля и функции.
- Гибкая система настроек, которая позволяет настроить все функции в режим удобный в конкретном случае.
- Недостатки программного продукта

- Несмотря на большой список преимуществ и возможностей, антивирус Касперского имеет список недостатков, правда, они не такие существенные, как плюсы.
- Необходимость регулярно платить за лицензионный ключ.
- Большая нагрузка на систему, которая приводит к медленной работе маломощных компьютеров.
- Занимает много места и оперативной памяти при работе.
- При выполнении проверки требуется закрытие других программ, что иногда бывает просто невозможно.
- Воспринимает некоторые нормальные файлы, как вредоносные.
- Определенные функции программы могут быть слишком навязчивыми и надоедать пользователю.

Каждый вправе решать, как он обеспечит защиту своей технике и данным, но стоит всерьез задуматься, что Антивирус Касперского – это прекрасное решение для защиты устройства, несмотря на то, что потребует постоянных незначительных вложений для покупки лицензионного ключа.

В параграфе рассмотрены содержательные детали только нескольких тем. Примеры занятий приведены далее.

2.3. Примеры занятий по программе элективного курса.

Приведем примеры нескольких занятий из программы элективного курса.

Тема практического занятия: Вирусы и антивирусные программы.

Цели урока:

1. Познакомить учащихся с путями распространения и методами борьбы с компьютерными вирусами;
2. Создать «Обзорный путеводитель по антивирусным программам»;

3.Продолжить осваивать антивирусное программное обеспечение через выполнение практических работ;

В ходе урока учащиеся должны узнать: понятие вируса, пути его распространения, методы борьбы с вирусом и типы антивирусных программ.

В ходе урока учащиеся должны уметь: определять, есть ли признаки заражения вирусом, проводить проверку на вирус при помощи антивирусной программы, анализировать и самостоятельно делать вывод, вести опорный конспект урока.

План урока.

1. Орг.момент.
2. Актуализация темы урока.
3. Объяснение нового материала в форме беседы.
4. Практическая работа «Обзор антивирусной программы Касперского».
7. Рефлексия деятельности.
8. Подведение итогов урока, выставление оценок.
9. Домашнее задание.

Ход урока.

1. Орг.момент.

2. Актуализация темы урока. (просмотр заранее снятого силами старшеклассников и учителя информатики ролика о вирусе гриппа). Цель просмотра: подвести учащихся к теме урока через их личный жизненный опыт.

3. Объяснение нового материала (в форме беседы с учащимися), обсудить с ними все вопросы, с опорой на жизненный опыт каждого. Одновременно учащиеся заполняют опорные конспекты в рабочих тетрадях.

4. Подведение итогов

5. Практическая работа «Обзор антивирусной программы Касперского»

Цель работы: научиться использовать антивирусные программы для проверки компьютера на наличие вирусов и его излечения.

1. Убедитесь в том, что Антивирус Касперского в данный момент загружен и работает, об этом символизирует иконка на системной панели в правом нижнем углу экрана. В зависимости от задачи, выполняемой антивирусом, картинка на ней может меняться. В дальнейшем в ходе лабораторных работ во время выполнения разных задач всегда обращайте внимание на вид этой иконки.

Дополнительно она служит для быстрого доступа к основным функциям антивируса: двойной щелчок левой клавишей мыши на ней вызывает главное окно интерфейса, а контекстное меню, открываемое щелчком правой клавиши мыши позволяет сразу перейти на нужное окно интерфейса.

Откройте контекстное меню иконки Антивируса Касперского и ознакомьтесь с представленным здесь списком ссылок:

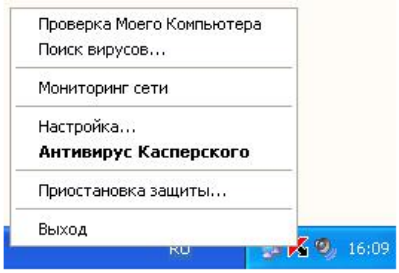

Рис.5 Меню иконки Антивируса

2. С помощью двойного щелчка на иконке откройте главное окно интерфейса Антивируса Касперского

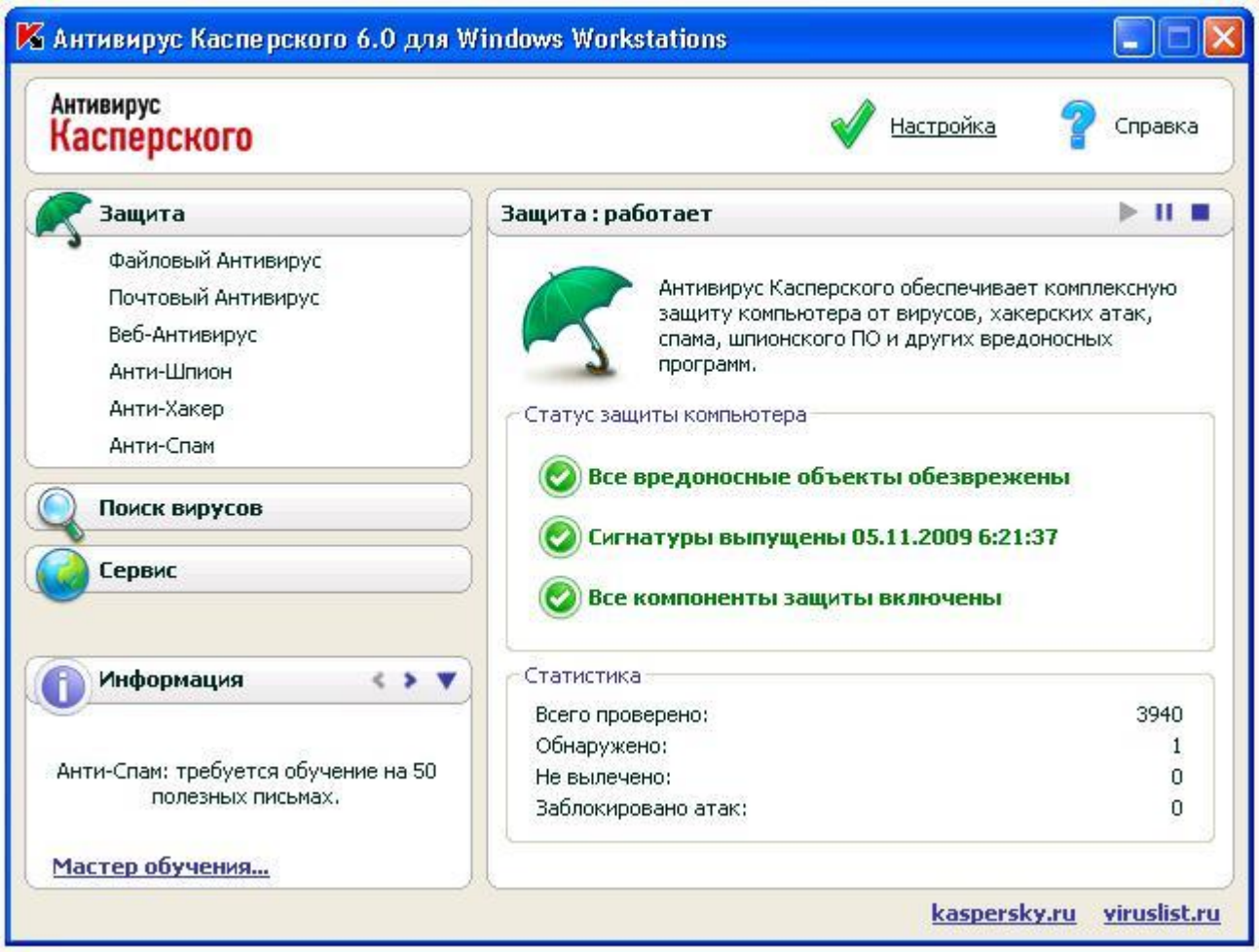

Рис.6 Главное окно интерфейса

3. В верхней правой части окна размещено две ссылки: Настройка и Справка. Первая используется для настройки антивируса, вторая - для вывода справочной системы.

Нажмите ссылку Справка Открывшееся окно содержит руководство пользователя Антивирусом

Касперского. При возникновении каких-либо проблем, в первую очередь всегда нужно обращаться к нему. Ознакомьтесь с содержанием справочной системы в левой панели окна и закрыв его вернитесь к главному окну антивируса

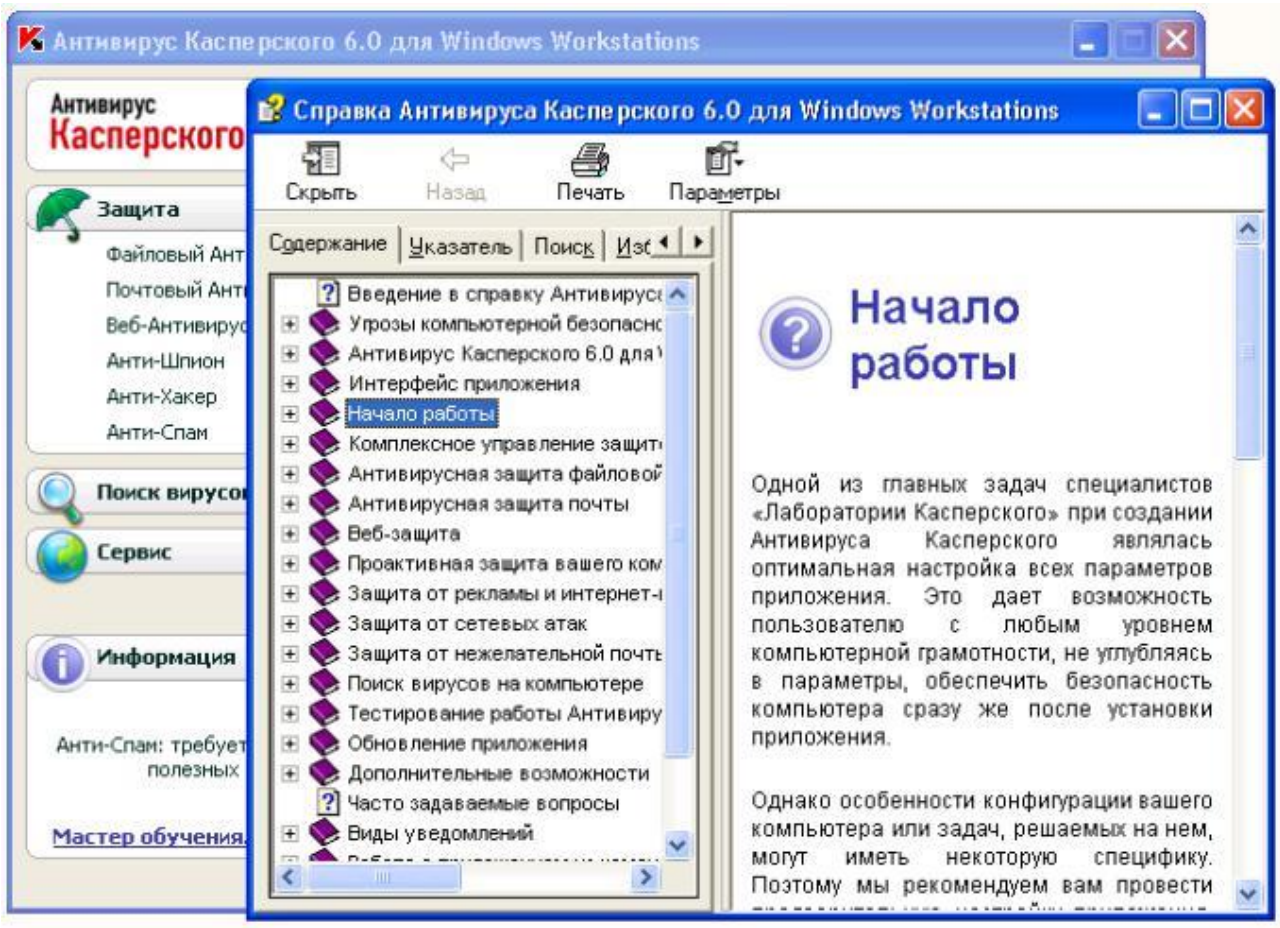

Рис.7 Справка Антивируса Касперского

4. В главном окне нажмите ссылку Настройка, расположенную слева от Справка.

Открывшееся окно Настройка предназначено для настройки параметров работы антивируса.

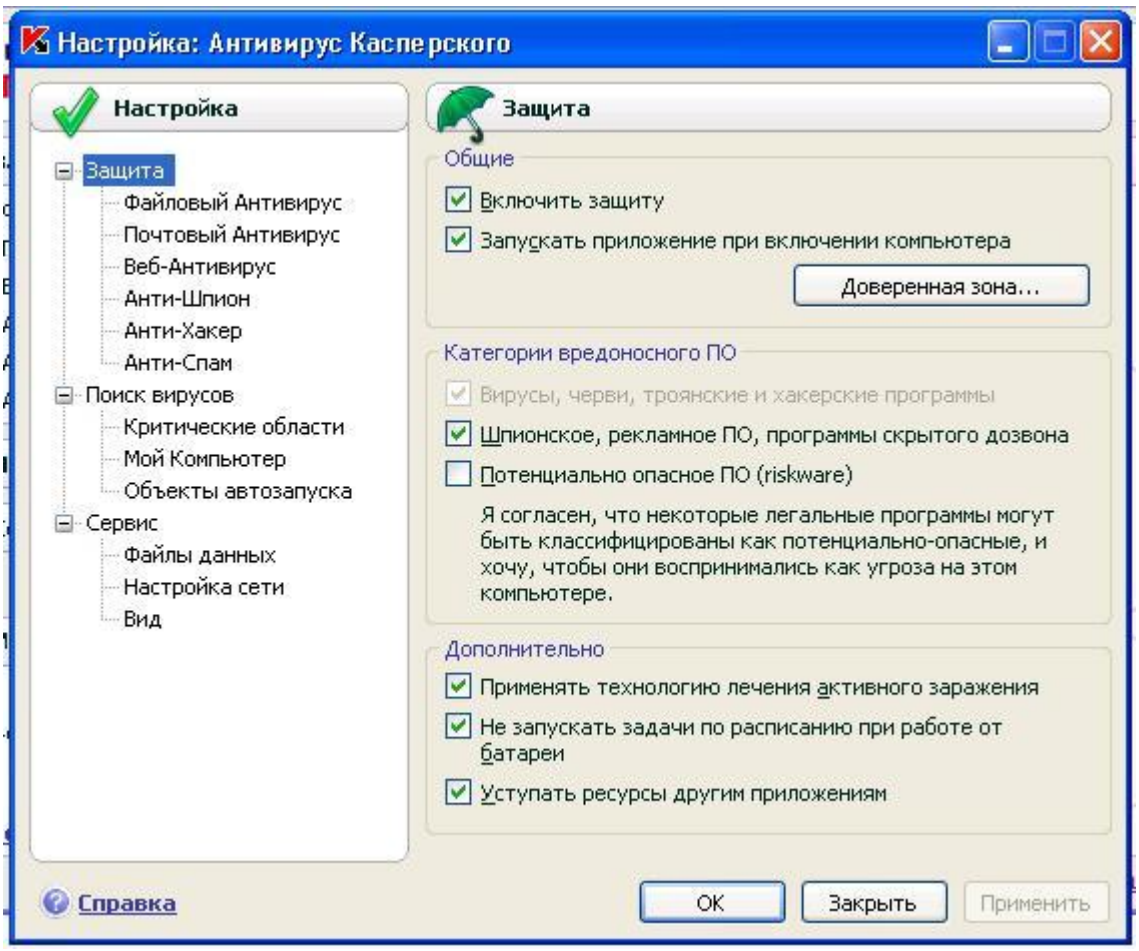

Рис.8 Меню настройки Антивируса Касперского

5.Изучите настройки антивируса. Какие по вашему мнению для эффективной работы антивируса лучше произвести настройки?

По интересующим вопросам обратитесь к разделу Справка. Сохраните ваши настройки

6.Зайдите в раздел поиска вирусов нажав на кнопку в контекстном меню

Произведите выбор объектов для проверки нажав на кнопку «Добавить» и «Удалить».

Произведите поиск вирусов нажав на кнопку «Поиск вирусов».

7. При окончании поиска изучите файл отчета поиска.

Задание № 2

1.Чтобы проверить насколько эффективно работает антивирус создайте текстовый файл.

2.В текстовый файл вставьте строку с кодом вируса.

*X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H**

Сохраните файл.

Если вы произвели правильные настройки антивируса, то он мгновенно должен отреагировать на созданный вами файл.

Задание № 3

1. Откройте ваш текстовый процессор.

2.Произведите настройки вашего текстового процессора от макровирусов установив высокую степень защиты. Для этого зайдите в Параметры -> Безопасность.

Задание № 4

Подготовьте доклад и презентацию на тему: «Общие сведения и особенности работы антивирусной программы *[Название антивирусной программы]*». Название антивирусной программы выбрать согласно своему варианту из вариантов заданий к работе.

Объем доклада 4-5страницы. Слайдов в презентации не менее пяти, по времени 7-10 минут.

Варианты заданий:

Вариант	**Название антивирусной программы**
1	AVG
2	Dr.Web
3	Avira
4	Panda AntiVirus
5	McAfee VirusScan
6	Eset Nod32
7	Microsoft Security Essentials
8	Norton AntiVirus

9	Антивирус Касперского
10	Avast!

7. Рефлексия деятельности.

Учащиеся прочитывают памятку о профилактике заражения вирусами своего ПК

8. Подведение итогов урока, выставление оценок.

9. Домашнее задание: п.1.7 стр.59-62, дополнить опорный конспект, задача 1.21 стр.62.

Тема практического занятия: Компьютерные вирусы и антивирусные программы

Тип урока: урок обобщения материала.

Структура урока:

- *Вводная часть.*
- *Выступления учащихся.*
- *Обсуждения выступлений.*
- *Рефлексия урока.*
- *Подведение итогов урока, выставление отметок.*

Методы, формы: проектная деятельность обучающихся

Оборудование: компьютеры, мультимедиа, учебные плакаты наглядные пособия

Проблема: Как можно избежать нежелательного воздействие разных видов вирусов на компьютер?

Цели:

- Обобщить основные знания по теме «компьютерные вирусы и антивирусные программы»;
- Углубить знания обучающихся о типах компьютерных вирусов

- Развивать проектные, коммуникативные умения, творческое отношение к порученному делу.

Задачи:

- Включить обучающихся в процесс обобщения знаний на основе подготовки мини- проектов;
- Организовать презентацию проектов учащихся;
- Продолжить формирование логического мышления, умения находить информацию и работать с ней
- Формировать у обучающихся внимание, наблюдательность, интерес к изучению информатики и понимание необходимости знаний для правильного применения их в окружающем мире
- Организовать дискуссию по обсуждению представленных проектов;
- Стимулировать желание самостоятельно работать с дополнительными образовательными ресурсами в школе во внеурочное время и дома.

1.Подготовка к уроку:

Урок планируется как самостоятельная проектная деятельность учащихся. Перед проведением урока учитель предлагает тематику проектов:

«Что такое вирус?»

«Графическое представление вирусов»

«Борьба с вирусами»

В соответствии с выбранной тематикой ученики разделяются на группы: «Вирусы», «Программисты», «Антивирусы», которые рассматривают понятие «вирус», проявления различных типов вирусов на компьютере, а также практические советы, сводящие к минимуму возможность заразить свой компьютер.

Для выполнения задачи, обучающиеся сами, планируют вид деятельности: изготовление схемы-сообщения, презентации, выпуск газеты или брошюры с советами.

В дальнейшем обучающиеся самостоятельно распределяют обязанности, осуществляют поиск и сбор информации, ее анализ и представление, обсуждение плана эксперимента, подготовки необходимого оборудования для его выполнения.

2. Вводная часть.

Учитель: «Сегодня мы обсуждаем тему: «Компьютерные вирусы и антивирусные программы.» Для этого мы разделились на группы «Вирусы», которые дадут понятие «Вирус» и расскажут о их типах, группа «Программисты» расскажут и представят презентацию о графическом изображении разных типов вирусов, и группа «Антивирусы» о борьбе с вирусами и раздадут памятки, которые сведут к минимуму возможность заразить свой компьютер. Чтобы группам приступить к выступлениям, давайте ответим на несколько вопросов:

В каком году произошла первая «эпидемия» компьютерного вируса и как он назывался?

Сколько вирусов известно на настоящий момент?».

Выступления учащихся.

Выступление группы «Вирусы».

Компьютерный вирус – это программа, способная создавать свои копии, внедрять их в различные объекты или ресурсы компьютерных систем, сетей и производить определенные действия без ведома пользователя.. о среде обитания они делятся на сетевые, файловые, загрузочные и файлово-загрузочные вирусы.

Сетевые вирусы распространяются по различным компьютерным сетям.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot – сектор) или в сектор, содержащий программу загрузки системного диска

(Master Boot Record – MBR). Некоторые вирусы записывают свое тело в свободные сектора диска, помечая их в FAT – таблице как “плохие” (Bad cluster).

Файловые вирусы инфицируют исполняемые файла компьютера, имеющие расширения com и exe. К этому же классу относятся и макровирусы, написанные помощью макрокоманд. Они заражают неисполняемые файлы (например, в текстовом редакторе MS Word или в электронных таблицах MS Excel).

Загрузочно – файловые вирусы способны заражать и загрузочные секторы и файлы.

3.Выступление группы «Программисты» (демонстрируют презентацию)

Каждый тип вируса выглядит по-разному и сейчас мы вам наглядно это продемонстрируем в нашей презентации.

4.Группа «Антивирусы» (раздают памятки каждому обучающемуся о том, как не заразить свой компьютер)

Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

- копирование информации — создание копий файлов и системных областей дисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений

программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

5.*Рефлексия деятельности*

6.*Подведение итогов, выставление отметок.*

Выводы по главе 2.

В рамках решения задач 3 и 4 исследования: разработка целей и содержания элективного курса «Современные антивирусные программы», разработка примеров занятий по программе элективного курса:

- сформулированы цели обучения, направленные на формирование представлений школьников о возможностях современных антивирусных программ и защите персонального компьютера;
- разработана программа элективного курса «Современные антивирусные программы», включающая не только работу с антивирусными программами, но и базовые сведения о компьютерной безопасности в целом;
- разработаны примеры занятий по программе, включающие практические задания и теоретические сведения по конкретным темам.

Заключение

Школьники, испытывающие дефицит общения в реальной жизни, неосознанно переносят опыт общения в сети Интернет на общение в повседневной жизни. Имея минимум жизненного опыта, дети не видят угроз, которые присутствуют в глобальной интернет-сети.

Информационная безопасность в образовательном учреждении – это состояние защищенности от угроз интересов личности, заключающееся в умении выявлять и вовремя пресекать угрозы информационного влияния в условиях школьной среды.

Проанализировав содержание учебников, используемых чаще всего в учебном процессе можно отметить, что изучению такой важной темы как «Компьютерные вирусы. Антивирусные программы» уделяется очень мало внимания. 95% школьников имеют компьютер в домашнем пользовании, а, следовательно, должны уметь обеспечить безопасность своей работы. Чтобы эффективно бороться с вирусами, современному пользователю необходимо иметь представление о вирусах и разбираться в методах противодействия вирусам.

Целью работы была разработка элективного курса «Современные антивирусные программы", способствующего формированию представлений старшеклассников об обеспечении безопасности персонального компьютера. В целях формирования умений и навыков защиты информации в старших классах в рамках элективного курса «Современные антивирусные программы» включили ряд тем включающих теоретические знания о современных компьютерных вирусах и задания на развитие практических умений и навыков работы с антивирусными программами. Для полноценного усвоения курса и совершенствования практических умений и навыков, каждый раздел подкрепляется практической работой. Практическая работа повышает интерес к изучению вопросов, связанных с информационной безопасности. Учащиеся получают возможность непосредственной работы с компьютерными вирусами, последствиями заражения, программами

антивирусной защиты, их видами и назначением, а также практические навыки тестирования различных объектов на заражение компьютерными вирусами. Таким образом цель работы достигнута, задачи решены.

Список использованных источников

1. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – ДМК Пресс, 2013. – С. 238– 241.
2. Бочкин, А. И. Методика преподавания информатики: учеб. пособие. – Москва: Высшая школа, 2003. – 431 с.
3. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации / В. Л. Бройдо. – Санкт Петербург: Питер, 2002. – 464 с.
4. Васильков, А.В. Информационные системы и их безопасность: Учебное пособие / А.В. Васильков, А.А. Васильков, И.А. Васильков. – М.: Форум, 2013. – С. 129–132.
5. Гаврилов, Э. П. Коммерческая тайна и результаты интеллектуальной деятельности / Э. П. Гаврилов // Патенты и лицензии. – 2002. – № 4. – С.19-23.
6. Гершунский, Б. С. Философия образования / Б. С. Гершунский. – Москва, 1998.
7. Городов, О. А. Информация как объект гражданского права / О. А. Городов // Правоведение. – 2001. – № 5. – С.80-82.
8. Гражданское право / под ред. Е. А. Суханова. – Москва: Волтерс Клувер, 2004 – 734 с.
9. Даниленко, А.Ю. Безопасность систем электронного документооборота: Технология защиты электронных документов / А.Ю. Даниленко. – М.: Ленанд, 2015. – С. 167–170.
10. Днепров, Э. Д. Три источника и три составные части нынешнего школьного кризиса / Э. Д. Днепров. – Москва, 1999.
11. Дозорцев, В. А. Интеллектуальные права. Понятие. Система. Задачи кодификации / В. А. Дозорцев – Москва: НОРМА, 2003. – 400 с.
12. Дозорцев, В. А. Понятие исключительного права / В. А. Дозорцев // Юридический мир. 2000. – № 3. – С.4-11; – № 6. – С.25-35.

13. Ерохин, В.В. Безопасность информационных систем: Учебное пособие / В.В. Ерохин. – М.: Флинта, 2015. – С. 95–96.

14. Закон РФ от 10 июля 1992 г. № 3266-1 «Об образовании» (с изменениями от 24 декабря 1993 г., 13 января 1996 г., 16 ноября 1997 г., 20 июля, 7 августа, 27 декабря 2000 г., 30 декабря 2001 г., 13 февраля, 21 марта, 25 июня, 25 июля, 24 декабря 2002 г., 10 января, 7 июля, 8, 23 декабря 2003 г., 5 марта, 30 июня, 20 июля 2004 г.)

15. Зверева, Е. А. Информация как объект неимущественных гражданских прав / Е. А. Зверева // Право и экономика. 2003. – № 9. – С.28-33.

16. Информатика / под ред. С. В. Симоновича. – Санкт Петербург: Питер, 2001. – 400 с.

17. Каймин, В. А. Информатика / В. А Каймин. – Москва: ИНФРА-М. 2002 – 328 с.

18. Каймин, В. А. Информатика и дистанционное образование / В.А. Каймин. – Москва: НОРМА-ИНФРА-М. 2002 – 432 с.

19. Кирмайер, М. С. Информационные технологии / М.С. Кирмайер. – Санкт Петербург: Питер, 2003. – 443 с.

20. Концепция информатизации сферы образования Российской Федерации // Проблемы информатизации высшей школы. – Москва, 1998.

21. Концепция создания и развития системы дистанционного образования в РФ. – Москва, 1998.

22. Копылов, В. А. Информационное право Российской Федерации / В. А. Копылов. – Москва: Инфра-М. 2006 – 400 с.

23. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере / Н.Н. Куняев. – Логос, 2015. – С. 228–230.

24. Лапчик, М. П. Методика преподавания информатики: учеб. пособие для студ. пед. вузов. / М. П. Лапчик, И. Р. Семакин, Е. К. Хеннер;

под общей редакцией М. П. Лапчика. – Москва: Издательский центр Академия. 2001. – 624 с.

25. Моисеев, А. М. Проблемы и пути совершенствования внутришкольного управления. Пособие для руководителей образовательных учреждений. Тамбов: ТОИПКРО. 2002. – 331 с.

26. Основы безопасности жизнедеятельности. Комплексная учебная программа для 5-11 классов общеобразовательных учреждений под общей редакцией А. Т. Смирнова, Б. О. Хренников. – Москва: Просвещение, 2010.

27. Основы информационной безопасности: учеб. пособие для студ. высших учебных заведений / С. П. Расторгуев. – Москва: Издательский центр «Академия». 2007. – 192 с.

28. Педагогика / под ред. А. А. Радугина. Москва: Центр. 2001. – 272 с.

29. Психология профессионального здоровья: учебное пособие / под ред. проф. Г. С. Никифорова. – Санкт Петербург: Речь. 2006. – 466-480 с.

30. Пятибратов, А. П. Вычислительные системы, сети и телекоммуникации / А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. – Москва: Финансы и статистика. 2002 – 512 с.

31. Роберт, И. Современные информационные технологии в образовании: дидактические проблемы; перспективы использования / И. Роберт. – Москва: Школа-Пресс. 2001 – 292 с.

32. Рогаткин, Д. В. Службы примирения в системе школьного самоуправления / Д. В. Рогаткин // Вестник восстановительной юстиции. – 2002. – № 4. – С. 12-33.

33. Селевко, Г. К. Современные образовательные технологии / Г. К. Селевко. – Москва: Народное образование. 2002 – 255 с.

34. Социальные опасности и защита от них: учебник для студ. учреждений высш. проф. образования / (В. М. Губанов, Л. А. Михайлов, В.П. Соломин и др.); под ред. Л. А. Михайлова. – Москва: Издательский центр «Академия». 2012. – 304 с. – (Сер. Бакалавриат)

35. Суглобов, А.Е. Экономическая безопасность предприятия: Учебное пособие / А.Е. Суглобов, С.А. Хмелев, Е.А. Орлова. – М.: ЮНИТИ, 2015. – С. 44–46.

36. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС Гарант

37. Цветков, В. Я. Технологии и системы информационной безопасности. Аналитический обзор / В. Я. Цветков. – Москва: ВНТИЦ Минпромнауки России. 2001.

38. Чашников, Л. А. Современные модели информационно-аналитического обеспечения школьного управления / Л. А. Чашников // Вопросы психологии. 1993. – № 9. – С.36-41.

39. Чупрасова, В. И. Современные технологии в образовании / В. И. Чупрасова. – Владивосток: Издательский дом «ДВР». 2004 – 154 с.

40. Шамсиев А. Общие требования к информационно-коммуникационным технологиям, используемым в условиях личностно-ориентированного обучения математике для развития познавательного интереса / А. Шамсиев, Ш. Р. Юсупова // Молодой ученый. 2015. – №5. – С. 14-18.