МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
федеральное государственное бюджетное образовательное учреждение высшего образования
КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
им.В.П.АСТАФЬЕВА
(КГПУ им.В.П.Астафьева)

Институт/факультет Институт математики, физики и информатики
(полное наименование института/факультета/филиала)

Выпускающая кафедра Базовая кафедра информатики и информационных технологий в образовании
(полное наименование кафедры)

Куприенко Виктор Григорьевич

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема **Формирование навыков информационной безопасности обучающихся старших классов через игровую деятельность**

Направление подготовки 44.03.01 Педагогическое образование
(код и наименование направления)

Профиль Информатика
(наименование профиля для бакалавриата)

ДОПУСКАЮ К ЗАЩИТЕ
Заведующий кафедрой
д.п.н., профессор Пак Н.И.
(ученая степень, ученое звание, фамилия, инициалы)

(дата, подпись)

Руководитель К.ф-м.н., доцент кафедры ИИТвО Романов Д.В
(ученая степень, ученое звание, фамилия, инициалы)

Дата защиты

Обучающийся Куприенко В.Г
(фамилия, инициалы)

(дата, подпись)

Оценка
(прописью)

Красноярск 2017

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Разработка и реализация безопасности информационных технологий и методов обучения, обозначено одним из основных мероприятий в Федеральной программе развития образования, обеспечивающих развитие системы образования в интересах формирования гармонично развитой, социально активной, творческой личности и в качестве одного из факторов экономического и социального прогресса общества [27].

Распространение информационных образовательных технологий в результате реализации вышеназванной программы позволит обеспечить вхождение страны в международное информационное и коммуникационное пространство.

Скачкообразное насыщение компьютерами, случившееся в начале 2000-ых годов в России, породило целый ряд насущных проблем, связанных с внедрением информационных технологий в процесс обучения. В последние 10 лет одной из основных задач системы образования стало выстраивание информационной образовательной среды. Сейчас, когда уже можно говорить, о существующей информационной среде в образовательных учреждениях, один из самых важных вопросов, стоящих сейчас перед школами с точки зрения информационных технологий – это вопрос их информационной безопасности, или говоря иначе – создание безопасной информационной среды образовательных учреждений [6].

Информация и информационная деятельность призваны играть ключевую роль в информационном обществе. Переход к данному обществу чаще всего идентифицируют по смене доминирующих технологий. Однако сами технологии не всегда оказывают непосредственное воздействие на социальную сферу, включая образование. Более важными оказываются изменения, инициируемые ими в обществе и влияющие на сферу образования.

В современном мире риски и угрозы во всем своем многообразии оказывают неоднозначное и многоплановое воздействие на безопасность общества и личности. Разумеется, наиболее безопасным с точки зрения

социальной динамики состоянием является стабильность. Однако общество обладает динамическим характером и траектория его развития лежит через периоды неопределенности. Сложность проблем, связанных с обеспечением безопасности, в том-то и заключается, что риски и угрозы неотделимы от жизненно необходимых позитивных социальных изменений, и культура безопасности требует осмысленной минимизации рисков и угроз в ходе реализации таких изменений, а вовсе не отказа от них. Это говорит о необходимости изучения учащимися современных рисков и угроз в школьном курсе информационной безопасности.

Современная подача предмета информатики в школе, относительно тематики информационной безопасности акцентирована на программно-технических средствах защиты. При этом часто опускаются, или затрагиваются вскользь, организационные вопросы, связанные с информационной безопасности. Эта область, как и обеспечение информационной безопасности на всех уровнях, от индивидуального до государственного требуют большего внимания, что находит отражения в последних учебных программах.

Таким образом, актуализация качественно новых угроз безопасности учащихся, затрагивающих сущность информационной связи общества и человека, а также отсутствие педагогических условий обеспечения учебного процесса свидетельствует об актуальности данной работы.

Цель работы – разработать и обосновать применение ряда игр для формирования навыков информационной безопасности учащихся старших классов.

Для выполнения поставленной цели необходимо решить следующие задачи:

1. Дать понятие информационной безопасности в общем и применительно к школьному процессу обучения.

2. Охарактеризовать место информационной безопасности в школьном курсе преподавания информатике.

3. Охарактеризовать дидактические мини-игры в школьном курсе информационной безопасности.

4. Проанализировать существующую систему обучения ИБ в школе.

5. Дать практические советы по применению игр в школьном курсе информационной безопасности.

Предмет исследования – формирование навыков информационной безопасности у школьников.

Объект исследования – процесс преподавания в школьном курсе информационной безопасности.

Гипотеза исследования: состоит в том, что в школе можно развить навыки информационной безопасности школьника с помощью разнообразных видов игровой деятельности в информационной сфере.

Работа состоит из введения, двух глав, заключения и списка использованных источников.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАРШЕКЛАСНИКА В УЧЕБНОМ ПРОЦЕССЕ

1.1 Об основных подходах к понятию «информационная безопасность»

Введение термина «информационная безопасность» вызвано двумя факторами: постоянно ускоряющимся развитием компьютерных технологий и переходом на компьютеризацию производства. Исходя из этого следует разделять информационную безопасность на несколько уровней:

- персональную – направленную на конфиденциальность индивидуальных данных;

- корпоративную – состоящую на службе организаций и предприятий различной формы собственности или масштаба;

- социальную – как защиту общества и государственных интересов.

Наряду с этим, информационная безопасность достигается не только техническими средствами. Обезопасить данные призвано специально разрабатываемое программное обеспечение, математические средства – шифрование сетевых потоков в частности.

На индивидуальном уровне, рассматривать информационную безопасность принято с двух позиций. Это защита формирующейся личности, когда информационное воздействие определяет становление конкретной персоны (ребенка, подростка). Второй аспект – безопасность уже сформировавшейся личности. Если рассматривать личностный фактор не только на персональном уровне, а и во взаимодействии с окружающим человека социумом, то следует затронуть и тему межгосударственной (международной) информационная безопасность.

Предварительным этапом информационной безопасности на личностном уровне выступает разработка оптимальных моделей оценки рисков, как на индивидуальном уровне, так и в разрезе интересов общества. Персональный подход, предусматривает создание на базе оценок рисков методических рекомендаций, с последующим их внедрением в образовательный процесс как школы, так и ВУЗов.

Современные стандарты средней школы включают тему информационная безопасность в курс предмета «Информатика», который, по мнению многих, давно уже пора разделить на информационные технологии и программирование. Основной акцент подачи информационной безопасности в школе сосредоточен больше на защите данных, нежели противодействии информационным атакам. Таким образом, среднее образование оперирует с защитой от вредоносных программных продуктов, а также базовыми принципами обеспечения конфиденциальности пользователя Интернет.

Как результат, трактовка понятия «информационная безопасность» даже если и приводится в учебниках для средней школы, то ограничена достаточно узкими смысловыми рамками и размыта без какой-либо конкретики. Например, учебное издание А.Г. Гейн и А.И. Сенокосова «Информатика и информационных и коммуникационных технологий» (2012) гласит: «под информационной безопасностью понимают защищенность 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». Определение, как видно, достаточно громоздкое. Более удачное определение приводит учебное пособие «Информатика и ИКТ» для 11 класса, издания 2009 года, под редакцией проф. Н.В. Макаровой. Термин также подан достаточно обобщенно, но намного проще для восприятия школьником: «информационная безопасность - это совокупность мер по защите информационной среды общества и человека».

Сходство обеих терминологий – подача информационной безопасности, как защита данных, концентрируя внимание ученика на информационной системе или среде, в первом и втором случаях соответственно.

Расширение определения термина информационная безопасность необходимо для придания ему той важности, которые информационные технологии играют в современном мире. И делать это необходимо, несмотря на шаблонность фразы, со школьной скамьи. На наш взгляд, более корректно предоставлять сегодня для школы определение информационной безопасности, как доступности, достоверности информации, это важно прежде всего для формирования адекватной картины мира учащихся, независимо от года образования.

Альтернативный вариант предусматривает включение в учебные пособия нескольких разноплановых определений информационной безопасности:

1. Информационная безопасность индивидуума ставит целью невозможность нанесения вреда персоне, общественная позиция и деятельность которой тесно привязана к новостному потоку. Иными словами человеку, поле деятельности которого предполагает регулярный обмен информацией на индивидуальном и социальном уровнях.

2. Информационная безопасность детей определяется защищенностью ребенка от неверной, негативной информации, а также от любого контента, способного нанести ему травму физического, психического или нравственного характера.

3. Информационная безопасность гражданина обеспечивается созданием возможности гражданам защищать и свободно реализовывать свои информационные права, не причиняя вреда другим гражданам. Это предусматривает как гарантию конфиденциальности персональных сведений, так и защиту от злоупотреблений информационными правами, приводящих к нанесению вреда социуму, отдельной персоне или нежелательному вмешательству в ее личный мир.

4. Информационная безопасность человека - это сведение к минимуму рисков причинения вреда от информации.

5. Информационная безопасность личности представляет комплекс условий, позволяющих индивидууму реализовать собственные информационные права, не совершая правонарушений или причинения вреда другим гражданам, общественным группам, а также государству.

Основные компоненты, определяющие уровень защищенности информации это: технические средства, идеологическая база и психологическая устойчивость. Рассмотрим каждый аспект информационной безопасности по-отдельности. Первый пункт - информационно-техническая защищенность, которая призвана обеспечить сохранность деловых, аналитических и прочих, корпоративных или общедоступных данных от воздействий, совершенных случайно или с умыслом. Информационно-идеологическая защита акцентирована на безопасность индивидуума в плане

соблюдения его прав в следующих аспектах, связанных с информацией: потребление, создание и последующее распространение сведений, остающихся в правовом поле, доступ к ресурсам, инфраструктуре. Одновременно с этим, индивидуальные действия не должны нарушать нормы морали, этики или оказывать деструктивное воздействие на прочих граждан, иметь выраженные антиобщественные установки. Информационно-психологическая безопасность направлена на защиту личности, а также социальных групп от негативного воздействия информационного поля на внутренний мир, сознание человека.

Завершая вступительную часть, направленную на объемность определения термина «информационная безопасность», выразим его следующим образом. ИБ личности – это комплекс мер и условий, обеспечивающих индивидуальные права на свободный доступ к информации, ее создание и размещение, а также наличие гарантий персональной конфиденциальности и отсутствие угроз, причиняемых человеку от воздействия информационных потоков.

Затрагивая тематику информационной безопасности общества, ограничимся наиболее распространенными определениями этого термина.

Первый вариант определяет социальную информационную безопасность как защищенность нравственно-этических норм, принятых обществом, его духовных и культурных ценностей. Альтернативное видение информационной безопасности акцентировано на защите, наряду с духовными ценностями, экономической составляющей, а также предупреждение использования информации как средства внешних или внутренних угроз социуму или государству.

Информационная безопасность социальной группы обеспечивает защищенность их информационного поля, позволяющего координировать совместные действия и мероприятия, не причиняющие вред другим общественным группам, а также выражать солидарность, определять общие нравственные и культурные ценности.

Информационная безопасность общественных объединений акцентируется на защите конфиденциальных сведений каждого члена структуры и ее деятельности в целом, а также обеспечивает возможность распространения информации, соответственно правовым нормам и принятым морально-этическим нормативам.

Перейдем к определению информационной безопасности на уровне государственных интересов. Во-первых, это защита конституционного строя, суверенности, а также территориальной целостности страны от попыток посредством информационных воздействий разрушить одну из перечисленных категорий. Во-вторых, информационная безопасность государства предусматривает предотвращение вмешательства в функционирование управляющих структур страны с целью нарушить ее экономическую, финансовую или внутриполитическую стабильность.

Духовная среда также выступает объектом, где применимы категории информационной безопасности. Обеспечение информационной безопасности в этой сфере направлено на защиту тех норм и устоев, включая гарантированные конституцией, которые связаны с формированием личности в духовном плане, становлении внутреннего мира индивидуума, а также имеющегося культурного наследия и исторически сложившихся норм нравственно этического воспитания. Относительно такой многонациональной страны как Россия, сложность в обеспечении информационной безопасности духовной сферы состоит в различии культурных наследий. Поэтому защита одних культурных традиций не должна наносить вреда ценностям других народностей, а наоборот, способствовать сплочению различных национальностей вокруг общего государственного ядра, косвенно укрепляя экономику страны, ее обороноспособность и безопасность.

Основополагающими критериями обеспечения информационной безопасности выступают:

- превентивность принимаемого комплекса мер, способность выявить и закрыть потенциальные угрозы от информации до того, как они нанесут вред;

- оперативное информирование объектов информационной безопасности, как внутренних, так международных.

Вышеуказанные аспекты только подтверждают необходимость аналитического подхода, моделирования в обеспечении и изучении ИБ как целого, так и на уровне ее подсистем.

Существующая практика противодействия информационным атакам уже успела показать целесообразность защитных технологий моделирования ситуаций, разрабатываемых на базе формирования своеобразного «заместителя» потенциальной угрозы. Естественно, подобная модель отличается от реальной ситуации более общим подходом, отсутствием конкретики. Не изобретая информационно-безопасные велосипеды, выделим основные аспекты концептуальной модели информационной безопасности, согласно тезисам В. И. Ярочкина:

- объекты опасности;
- угрозы непосредственно;
- источники атаки;
- цели злоумышленников;
- способы неправомерного доступа к конфиденциальной среде;
- источники информации, а также направления, методы и средства ее защиты.

1.2 Анализ современной ситуации в области информатизации образования

Анализ учебно-методических комплексов (УМК) по информатике и ИКТ для основной школы на предмет изучения информационной безопасности позволяет сделать вывод о том, что на уровне основного общего образования в рамках предмета «Информатика» акцент в соответствии с

требованиями ФГОС делается на формировании навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

УМК «Информатика» 7 - 9 класс (ФГОС), автор Угринович Н. Д.

Тема «Информационное общество и информационная безопасность». Всего 3 часа: 1 час в 7 кл. и 2 часа в 9 кл. Содержание темы: Информационное общество. Информационная культура. Перспективы развития информационных и коммуникационных технологий. Правовая охрана программ и данных. Защита информации. Правовая охрана информации. Лицензионные, условно бесплатные и свободно распространяемые программы.

УМК «Информатика» 7 - 9 класс (ФГОС), авторы Семакин И.Г. и др.

Аспекты информационной безопасности рассматриваются в 7 и 9 классах в рамках тем «Компьютер: устройство и программное обеспечение» (содержание темы: правила техники безопасности и эргономики при работе за компьютером, использование антивирусных программ) и «Информационные технологии и общество» (содержание темы: проблемы безопасности информации, этические и правовые нормы в информационной сфере).

УМК «Информатика» 5-9 класс (ФГОС), автор Босова Л.Л.

Предметные результаты «Формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права» формируются в 5 классе при изучении темы «Передача информации», в 7 классе при изучении тем «Всемирная паутина» и «Программное обеспечение компьютера», в 9 классе при изучении темы «Информационные ресурсы и сервисы Интернета».

УМК «Информатика» 7-9 класс, (ФГОС), авторы Горячев А.В.

Некоторые аспекты информационной безопасности рассматриваются в 7 классе при изучении темы «Общение в сети Интернет». Содержание темы:

Как вести себя и чего опасаться в сети Интернет. Ваша личная территория в сети Интернет. Личное и публичное общение в Интернете. Как правильно спорить в Интернете.

УМК «Информатика» 7-9 класс, (ФГОС), авторы Гейн А.Г, Юнерман Н.А. и др.

В 9 классе в рамках темы «Правовые вопросы Интернета. Безопасность и этика Интернета. Защита информации» рассматриваются вопросы информационной безопасности в сети Интернет.

Таким образом, все авторские коллективы уделяют внимание вопросам информационной безопасности, в основном аспектам безопасного поведения в Интернете и защите от компьютерных вирусов. В целом такие уроки запланированы авторами в начале 7 класса и в конце 9 класса. При этом, с учетом потери уроков в праздничные дни и подготовкой к ОГЭ в конце 9 класса, учителя информатики часто предлагают данные темы на самостоятельное изучение обучающимся. А в 5, 6, 8 классах эта тема в явном виде вообще отсутствует. Однако именно в подростковом возрасте дети становятся участниками сетевых сообществ, ведут активную деятельность в Интернете. Конечно же, на этом этапе необходимо рассказать им о защите персональных данных, о признаках компьютерной зависимости и синдрома информационной усталости, о мошенничестве, связанном с использованием мобильных устройств. Также дать рекомендации родителям. Поэтому совершенно необходимо дополнительное проведение занятий информационной безопасности. Это могут быть классные часы или внеурочные занятия, проектная деятельность.

Подростковая возрастная категория – наиболее уязвимый этап при формировании личности. Сегодня, ситуация обостряется высокой технической оснащенностью и неконтролируемым информационным потоком. В подростковом возрасте, ребенок переживает дополнительную психологическую нагрузку, источником которой формирования собственного «Я». Подкрепляется это скептическим отношениям к замечаниям,

нравоучениям, а также недоверием рекомендациям от взрослых: родителей, учителей. Имеющаяся техническая подготовленность подростка, с другой стороны, делает ему доступной сеть Интернет, где поток неконтролируемой информации оказывает непредвиденное воздействие на психику, способен изменить мировоззрение ребенка [15]. К примеру, секты, вербовка детей из неблагополучных семей в криминал и подпольные группы [52].

Опишем упрощенную модель информационной среды образовательного учреждения с точки зрения обеспечения ее безопасности. Наша модель будет основываться на теории рисков. В качестве определения риска выберем следующее:

Риск — это неопределённое событие или условие, которое в случае возникновения, приводит к обязательным неблагоприятным последствиям.

Из приведенного выше определения следует наличие у риска следующих обязательных характеристик.

Неопределённость. Эта характеристика означает, что риск существует только тогда, когда различные варианты развития событий могут осуществиться, а могут и нет.

Ущерб. Эта характеристика означает, что риск существует только тогда, когда исход может привести к ущербу или иному, но обязательно негативному последствию.

Значимость. Эта характеристика означает, что риск существует, когда предполагаемое событие имеет практическое значение и затрагивает интересы хотя бы одного субъекта.

Рассмотрим эти характеристики на примерах. В качестве первого примера выберем риск взлома сайта образовательного учреждения, который будет распространять вирус с материалами, размещенных на сайте. У данного события присутствует характеристика – неопределенность. Сайт может быть заражен вирусом, а может быть и нет. В случае заражения образовательному учреждению будет нанесен и финансовый ущерб, который будет выражен в оплате работ по возвращению сайта в работоспособное состояние и

репутационный ущерб, если потребуется значительное время на восстановление сайта. А это означает, что и вторая характеристика у данного риска присутствует. Субъектом, чьи интересы затрагивает предполагаемое событие (третья характеристика), в данном случае, является непосредственно образовательное учреждение. В качестве второго примера выберем следующее событие: окончание лицензии на антивирусное программное обеспечение (например, антивирус Касперского). После остановки работы антивирусного ПО, организация(субъект) понесет ущерб от заражения компьютеров вирусом. Но данный пример не является риском, поскольку не работает характеристика неопределенности. Лицензия действует четко обозначенный срок (обычно 1 или 2 года) и соответственно рассмотренное событие обязательно произойдет.

Второе ключевое понятие для модели безопасности информационно-образовательной среды – это понятие угрозы. Под угрозой будем понимать потенциально возможное событие, которое может привести к нанесению ущерба.

Риск – определяет степень опасности воздействия угрозы (или набора угроз) на систему (объект, ресурс или процесс).

Для каждой информационно-образовательной среды существуют риски, реализация которых приведет информационную среду в неработоспособное состояние или в состояние, в котором эффективность работы среды будет существенно снижена. Для каждого риска есть некоторый набор угроз.

Часть из этих угроз являются актуальными. Актуальными угрозами считается те угрозы, которые имеют высокую степень опасности воздействия на систему.

Под безопасной информационно-образовательной средой мы будем понимать такую информационную среду, для которой определен набор актуальных угроз наступления рисков и для каждой из угроз выбран способ защиты, позволяющий наиболее эффективно предотвратить угрозу или минимизировать возможные потери.

Таким образом, для получения конкретной модели безопасной информационно-образовательной среды необходимо описать возможные группы рисков данной среды, определить набор актуальных угроз, которые могут привести к реализации рисков и определить комплекс защитных мероприятий, позволяющих нейтрализовать угрозы или минимизировать их последствия. Необходимо отметить, что в комплекс мероприятий должны входить и технические, и педагогические и организационные действия.

В группу педагогических рисков, включаются те риски, которые могут повлиять на учебный процесс. Здесь надо отметить риски, в результате реализации которых будет невозможно использовать компьютерное оборудования при ведении уроков. Стоит напомнить, что согласно новым ФГОС использование подобного оборудования является обязательным. Большие группы педагогических рисков связаны с влиянием на оценивание результатов учащихся и с непосредственным отрицательным влиянием на учащихся, что делает необходимым включение дополнительных тем и (или разделов) в учебный процесс и проведением дополнительных воспитательных мероприятий для детей, родителей и педагогического коллектива.

К группе психолого-медицинских рисков, прежде всего, относятся те риски, которые могут повлиять на здоровье, как учащихся, так и сотрудников ОУ.

В группу управленческих рисков, включим те риски, которые приведут к необходимости временной или постоянной перестройки организационной структуры образовательного учреждения. Ярким примером подобного риска может служить риск временной неработоспособности локальной сети учреждения при использовании школой электронного журнала.

В группу финансовых рисков, включим все те риски, которые связаны с понёсшим учреждением финансового ущерба. Это в первую очередь порча оборудования и программного обеспечения.

В группу политических рисков включим риски, отрицательно влияющие на имидж учреждения, что может сказаться на наборе желающих учиться в

данной школе, и может привести либо к ухудшению контингента учащихся, либо даже к его уменьшению, что при нынешних принципах финансирования может серьезно сказаться на бюджете. Часть политических рисков связана с необходимостью выполнением ОУ федеральных и региональных законодательных актов, и иных нормативных документов, связанных с информатизацией, а также требований надзорных органов. К сожалению, зачастую образовательное учреждение оказывается в «вилке» между двумя нормативными документами. Так, до недавнего времени, в Санкт-Петербурге проверка районных баз «льготное питание учащихся» в социальном регистре населения проводилась по регламенту, утвержденному правительством города. Однако этот регламент не соответствовал 152-ФЗ «О защите персональных данных».

Необходимо отметить, что иногда грани отделяющие одну группу рисков от другой достаточно условны. Так, например, есть часть рисков, которые можно отнести и к педагогическим рискам, и к психолого-медицинским.

Еще один важнейшим фактором является то, что существуют угрозы, которые могут привести к реализации сразу нескольких рисков. Сгоревшее оборудование приведет как к отмене занятия (педагогический риск), так и к прямым финансовым потерям (финансовый риск).

Конечно, конкретные наборы рисков могут отличаться в зависимости от региона, особенностей учреждения, его уровня информатизации, но значительная часть рисков, а также общие подходы к созданию безопасной информационной среды ОУ будут одинаковы

Для анализа возможных педагогических рисков информационной образовательной среды подробнее рассмотрим данный вид рисков и угрозы, которые влияют на его возникновение. Разделим педагогические риски на три группы, в соответствии с объектом (субъектом) влияния. Первая группа педагогических рисков влияет непосредственно ведение уроков, вторая на оценивание образовательных результатов и третья группа влияет на субъекты

образовательного процесса (учащихся и педагогов). Подобное деление не является единственно возможным, но позволит сгруппировать схожие риски, что упростит анализ вероятности их реализации.

Первая группа педагогических рисков информационной образовательной среды — это риски, влияющие на ведение учебного процесса. Эти риски могут привести к следующему:

− отмене конкретного учебного занятия (урока);

− отмене ряда занятий по предмету или группе предметов в определенный временной интервал от одного урока в трех-четырех классах, до отмены всех уроков в ОУ в течение дня (нескольких дней);

− ухудшение качества проведения учебного занятия (или нескольких занятий);

− проведение занятий в формате несоответствующему требованиям законодательства (например, ФГОС).

Вторая группа включает в себя риски, влияющие на оценивание результатов учащихся:

− искажение результатов учащихся после преднамеренного воздействия учащихся или иных лиц (примером реализации подобного риска, может являться ситуация получения правильных ответов учащимися при тестировании через Интернет с помощью мобильных устройств);

− искажение результатов учащихся после непреднамеренного воздействия учащихся или иных лиц;

− искажение оценивания результатов после преднамеренного воздействия учащихся или иных лиц (примером является изменение результата учащегося в системе без ведома учителя);

- искажение оценивания результатов из-за неправильной работы педагогических программных средств (ППС) (примером может служить ситуация, когда в базе тестов в качестве верного указан не тот номер ответа);

− искажение оценивания результатов по вине сбоя (отказа) аппаратно-программного обеспечения или после воздействия вредоносного программного обеспечения (компьютерные вирусы и т.п.);

− полная или частичная утеря результатов учащихся по вине сбоя (отказа) аппаратно-программного обеспечения или после воздействия вредоносного программного обеспечения (компьютерные вирусы и т.п.);

− полная или частичная утеря результатов после преднамеренного воздействия учащихся или иных лиц.

Третья группа педагогических рисков связана с непосредственным отрицательным влиянием элементов информационной среды на учащихся. В число таких рисков входят:

− доступ учащихся к информации, строго запрещенной законодательством (например, информация экстремистского содержания, детская порнография, пропаганда наркотических средств и т.п.);

− доступ учащихся к информации, не запрещенной законодательством, но которая может нанести им вред (примером такой информации может служить информация, разрешенная для учащихся старше 16 лет и нежелательная для остальных групп учащихся);

− общение через сеть Интернет с людьми, желающими оказать вредные воздействия на учащихся или призывающие их к противоправным действиям;
− травля учащегося с использованием средств информационной среды иными учащимися ОУ или посторонними (кибербуллинг) [52].

Для каждого из педагогических рисков информационной среды приведем примеры угроз, которые могут привести к его возникновению.

Рассмотрим риск отмены конкретного учебного занятия. Под отменой конкретного учебного занятия, мы будем понимать, отмену конкретного урока в конкретном классе (например, математики во 2-а классе) или вынужденную замену данного урока на другой (например, замена математики уроком ИЗО).

К реализации данного риска могут привести следующие угрозы:

1. Неработоспособность компьютерного или демонстрационного оборудования, необходимого для проведения конкретного урока. Это могут быть компьютер (ноутбук), стоящий в классе, мультимедийный проектор, интерактивная доска, а также школьный сервер, на котором находится необходимая для урока информация.

2. Неработоспособность локальной сети, которая приводит к невозможности использовать необходимую для урока информацию, расположенную на школьном сервере или в сети Интернет.

3. Отсутствие выхода из школьной локальной сети в Интернет, которое приводит к невозможности использовать необходимую для урока информацию.

4. Неработоспособность необходимого для проведения занятия программного обеспечения.

Стоит отметить, когда мы говорим о рисках, нас меньше интересуют причины возникновения тех или иных угроз. В данном случае для нас имеет не столь существенное значения причина, по которой, например, во время конкретного урока отсутствует Интернет (это могут быть внутренние школьные проблемы с оборудованием, технические проблемы провайдера, или даже неоплата услуг провайдера) гораздо больше нас волнует последствие данного события. Хотя при высчитывании коэффициента реализуемости угрозы нас будет интересовать вероятность ее реализации.

Риск отмены ряда занятий по предмету или группе предметов в определенный временной интервал. Под отменой ряда занятий по предмету или группе предметов в определенный временной интервал мы будем понимать и отмену одного урока в трех-четырех классах, которые должны были идти параллельно, и отмену всех уроков по некоторым предметам в ОУ в течение дня (нескольких дней).

Конечно, при существующем уровне информатизации образования пока еще сложно представить такую сильную зависимость преподавания от информационных технологий. Но даже сейчас может сложиться ситуация, при

которой при отсутствии работоспособного компьютерного оборудования невозможно будет в течение некоторого времени (от 1 дня до недели) осуществлять преподавание информатики в старших классах или предмета технологии в 8 классе, где раздел – черчение, часто преподается с помощью компьютерных графических средств.

К реализации рассматриваемого риска могут привести следующие угрозы:

1. Неработоспособность серверного оборудования, которое приводит к невозможности проводить занятия.

2. Неработоспособность локальной сети, которая приводит к невозможности использовать необходимую для урока информацию, расположенную на школьном сервере или в сети Интернет.

3. Неработоспособность необходимого для проведения занятия программного обеспечения.

Приведенные выше примеры не полностью исчерпывают ситуации, которые могут реально возникнуть. Надо отметить, что использование в образовательном процессе виртуальных лабораторий по физике и химии, лабораторий по робототехнике иных новых технических средств обучения все сильнее увеличивает зависимость учебного процесса от информационных технологий, а соответственно увеличивают вероятность возникновения рисков.

1.3 Игровая деятельность в школьном курсе информационной безопасности

Игровая деятельность - один из тех видов деятельности, которой используется взрослыми в целях воспитания школьников, обучая их различным действиям с предметами, способам и средствам общения. В игре ребёнок развивается как личность, у него формируется те стороны психики, от

которых в последствии будут зависеть успешность его учебной и трудовой деятельности, его отношения с людьми [12].

Много игр с готовым содержанием и правилами создается в настоящее время педагогами. Игры с правилами предназначены для формирования и развития определенных качеств личности ребенка. В школьной педагогике принято делить игры с готовым содержанием и правилами на дидактические, подвижные [17].

Для всех игр с готовым содержанием и правилами характерны следующие особенности: наличие игрового замысла или игровой задачи, которые реализуются (решаются) через игровые действия. Игровой замысел (или задача) и игровые действия составляют содержание игры; действия, и отношения играющих регулируются правилами; наличие правил, и готовое содержание позволяют детям самостоятельно организовывать и проводить игру [16].

Среди дидактических игр различают игры в собственном смысле слова и игры-занятия, игры–упражнения. Для дидактической игры характерно наличие игрового замысла или игровой задачи. Существенным элементом дидактической игры являются правила. Выполнение правил обеспечивает реализацию игрового содержания. Наличие правил помогает осуществить игровые действия и решить игровую задачу. Следовательно, ребенок в мине-игре учится непреднамеренно [19].

В дидактической игре формируется умение подчиниться правилам, т.к. от точности соблюдения правил зависит успех игры. В результате мини-игры оказывают влияние на формирование произвольного поведения, организованности [23].

По характеру используемого материала дидактические игры условно делятся на игры с предметами, настольно-печатные игры и словесные игры [21].

Настольно–печатные игры направлены на уточнение представлений об окружающем, стимулирование знаний, развитие мыслительных процессов и

операций (анализ, синтез, обобщение, классификацию и др.)

Настольно печатные игры разделены на несколько видов: парные картинки, лото, домино, разрезные картинки и складные кубики.

Словесные игры. В эту группу входит большое количество народных игр типа «Краски», «Молчок», «Черное и белое» и др. Игры развивают внимание, сообразительность, быстроту реакции [21].

Структура дидактической игры, ее задачи, игровые правила, и игровые действия объективно содержат в себе возможность развития многих качеств социальной активности [24].

Дидактическую игру условно разделяют на несколько стадий. Для каждой характерны определенные проявления детской активности. Знание этих стадий нужно воспитателю для правильной оценки эффективности игры. Первая стадия характеризуется появлением у ребенка желания играть, активно действовать. Возможны различные приемы с целью вызвать интерес к игре: беседа, загадки, считалочки, напоминание о понравившейся игре. На второй стадии ребенок учится выполнять игровую задачу, правила и действия игры. В этот период закладываются основы таких важных качеств, как честность, целеустремленность, настойчивость, способность преодолевать горечь неудачи, умение радоваться не только своему успеху, но и успеху товарищей. На третьей стадии ребенок, уже знакомый с правилами игры, проявляет творчество, занят поиском самостоятельных действий. Он должен выполнить действия, содержащиеся в игре: угадать, найти, спрятать, изобразить, подобрать. Чтобы успешно справиться с ними, необходимо проявить смекалку, находчивость, способность ориентироваться в обстановке. Ребенок, усвоивший мини-игру, должен стать и ее организатором, и ее активным участником. Каждому этапу игры соответствуют и определенные педагогические задачи. На первой стадии педагог заинтересовывает детей мини-игрой, создает радостное ожидание новой интересной игры, вызывает желание играть. На второй стадии воспитатель выступает не только как наблюдатель, но и как равноправный партнер, умеющий вовремя прийти на

помощь, справедливо оценить поведение детей в игре. На третьей стадии роль дефектолога заключается в оценке детского творчества при решении игровых задач [22].

Следовательно, дидактическая игра – доступный, полезный, эффектный метод воспитания самостоятельности мышления у детей. Она не требует специального материала, определенных условий, а требует лишь знания воспитателя самой игры. При этом необходимо учитывать, что предлагаемые игры будут способствовать развитию самостоятельности мышления лишь в том случае, если они будут проводиться в определенной системе с использованием необходимой методики [23].

Дидактическими мини-играми называют вид учебных занятий, которые организуют в виде учебных игр, реализующих ряд принципов игрового, активного обучения и отличающихся наличием правил, фиксированной структуры игровой деятельности и системы оценивания, один из методов активного обучения [19].

Дидактическая игра – это такая коллективная, целенаправленная учебная деятельность, когда каждый участник и команда в целом объединены решением главной задачи и ориентируют свое поведение на выигрыш. Дидактическая игра – это активная учебная деятельность по имитационному моделированию изучаемых систем, явлений, процессов [16].

Дидактическая игра является ценным средством воспитания умственной активности детей, она активизирует психические процессы, вызывает у учащихся живой интерес к процессу познания. В ней учащиеся охотно преодолевают значительные трудности, тренируют свои силы, развивают способности и умения. Игра помогает сделать любой учебный материал увлекательным, вызывает у учеников глубокое удовлетворение, создает радостное рабочее настроение, облегчает процесс усвоения знаний [12].

Игры в своем развитии эволюционируют от предметных к ролевым и от ролевых к дидактическим. Интерес детей в дидактической игре перемещается от игрового действия к умственной задаче.

Дидактические игры конструируются по-разному. В некоторых из них есть все элементы ролевой игры: сюжет, роль, действие, игровое правило, в других - только отдельные элементы: действие или правило, или то и другое. Поэтому по структуре дидактические игры делятся на сюжетно-ролевые и игры-упражнения. В дидактической игре ее замысел, правило, действие и включенная в них умственная задача представляют собой единую систему формирующих воздействий [17].

В настоящее время в области компьютерного моделирования получил широкое распространение так называемый объектно-ориентированный подход. Для успешного обучения информатике в процессе игры нужно применять не только модели изучаемого материала, но и предметы, окружающие учащегося.

Психологи определили [12], что усвоение учеником знаний начинается с материального действия с предметами или их моделями, рисунками, схемами. При этом образы предметов, их свойства, признаки и действия, которые дети осуществляют с предметами или их моделями, переносятся в план представлений. Практические действия дети описывают словесно. Это процесс отражает взаимодействие ученика с познаваемым материалом. Значит, осуществляется связь между материальной и внешнеречевой формами действия и активизируется учебная деятельность ребенка. Учебная задача - ключевой компонент учебной деятельности.

При постановке учебно-дидактической задачи необходимо выполнение следующих требований:

1. Дидактическая задача должна ориентировать учащегося на поиск нового способа действия, мотивировать его познавательную деятельность.

2. В процессе ее решения школьники должны осознать нужду и рациональность нового знания. Перед проведением дидактической игры нужно доступно изложить сюжет, распределить роли, поставить перед учащимися познавательную задачу, подготовить нужное оборудование. Если

дидактическая задача скрыта сюжетом, ролью, игровым действием, то в ходе беседы с детьми учителю нужно обратить на нее внимание [21].

В мине-игре надлежит продумывать не только характер деятельности учащихся, но и организационную сторону, характер управления игрой. С этой целью применяют средства обратной связи со школьником. В большинстве игр нужно вносить элементы соревнования, что также повышает активность учащихся в процессе обучения. Нужно отнестись с большим тактом к ученикам, которые допустили ошибки. Ошибки школьников нужно разбирать не в ходе игры, а в конце, чтобы не нарушать впечатление от мини-игры.

ГЛАВА 2. ПРИМЕНЕНИЕ ИГРОВОЙ ДЕЯТЕЛЬНОСТИ ДЛЯ ФОРМИРОВАНИЯ НАВЫКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАРШЕКЛАССНИКОВ

2.1 Современные подходы к решению проблемы информационной безопасности школьника

Целевая направленность педагогического процесса задается федеральным государственным образовательным стандартом (ФГОС), находя свое отражение в разрабатываемых учебных планах, мероприятиях и программах.

Целевая подоплека среднего образования, соответственно требованиям ФГОС, предусматривает формирование у учащихся навыков обработки информации, выработку умений использовать ее, и средства коммуникации для решения комплекса задач, носящих когнитивный или организационный характер, с соблюдением норм, установленных концепцией ИБ. Достижение подобных целей невозможно без программы социализации учеников, их воспитания с учетом духовно-нравственного развития. Подобный аспект органично переплетается с нормативами относительно метапредметных результатов освоения базового курса общеобразовательной программы для средней школы. Они включают в себя навыки самостоятельной деятельности в информационном поле, а именно: умение ориентироваться среди источников поступления сведений, интерпретировать получаемый контент, критически оценивать актуальность и достоверность поступающих данных.

Второй важный аспект в подходе к изучению информационной безопасности – это привязка базового курса информатики к правовым нормам отечественного законодательства так же особенностей использования лицензионного программного обеспечения и безопасной работы в сети Интернет. Дополнительно внимание должно уделяться формированию у

учащихся старших классов базовых принципов информационной безопасности, понимания как обеспечить надежное функционированию комплекса информационных и коммуникационных технологий. Именно развитие средств информационных и коммуникационных технологий, наряду с множеством положительных моментов, содержит количество потенциальных угроз относительно безопасности и конфиденциальности информации на всех уровнях: индивидуальном, корпоративном, общественном и государственном. Как результат, возникает необходимость совершенствования средств обеспечения информационной безопасности, что в свою очередь требует большего притока профильных специалистов. А последняя проблема напрямую связана с качеством и эффективности среднего и впоследствии высшего образования. При этом, навыки информационной безопасности задаются будущему специалисту непосредственно в школе.

Вычислительная составляющая также важный элемент построения процесса обучения информационной безопасности. Как видно, обучение информационной безопасности требует определенной универсализации образовательного процесса. Создаваемая под эти цели Программа (далее так и именуемая в тексте) формирования общих умений и навыков, должна охватывать следующие сферы:

- непосредственно основы информационной безопасности;

- применение комплекса ИКТ на уровне стандартного пользователя без вреда для информационной безопасности;

- владения навыками безопасной работы в сети Интернет.

Результатом успешного освоения Программы должно выступать умение применять средства ИКТ под разрешения различного рода задач: когнитивные, организационные и коммуникативные, оставаясь при этом в правовом поле и соблюдая принятые морально-этические нормы [1].

Продвинутый уровень предмета «Информатика» должен в дополнение к базовым навыкам, выработать комплекс умений, включающих понимание базы информационной этики и права, принципов обеспечения

информационной безопасности, методик, направленных на надёжное функционирование комплекса информационных и коммуникационных технологий.

Возвращаясь к аналитическому аспекту информационной безопасности, отметим еще раз важность обучения старшеклассников моделированию потенциальных угроз и на основе этого выработки способов их предотвращения. Подобный аспект важен независимо от характера курса: общего или продвинутого. В этом смысле полезной оказывается практическая модель [24], которая разрабатывается для различных поведенческих сценариев по обеспечению информационной безопасности, как у ребенка, так и взрослого человека. Подобный подход требует создания и экспериментальных моделей, направленных на изучение различных составляющих основной концептуально моделируемой структуры. Например, можно рассматривать моделирование таких ситуаций, как вхождение учащихся в социальные группы, объединения по интересам, прочие общественные организации. Обучение государственной информационной безопасности, включая также международный аспект информационной защиты, должно дать ученику базовые предоставления соответствующей концептуальной модели.

Сейчас мы подошли к тому моменту, когда требуется рассмотреть непосредственно формы обучения информационной безопасности.

Внеурочная часть программы обучения – обязательный элемент образовательной системы информационной безопасности. Ее задача расширение кругозора, углубление уже полученных базовых навыков на практическом уровне и акцентом на область персональных интересов, возможностей или склонностей. Чтобы охватить максимально широкую аудиторию, рекомендуется использовать дистанционную форму обучения.

Современная подача предмета информатики в школе, относительно тематики информационной безопасности акцентирована на программно-технических средствах защиты. При этом часто опускаются, или затрагиваются вскользь, организационные вопросы, связанные с

информационной безопасностью. Эта область, как и обеспечение информационной безопасности на всех уровнях, от индивидуального до государственного, требуют большего внимания, что находит отражение в последних учебных программах.

Тем не менее, современные учебники все еще недостаточно хороши для обучения информационной безопасности в полном объеме. В частности, целесообразным кажется создание обучающих информационной безопасности веб ресурсов для школьников, выкладка в сеть лабораторных работ, а также заданий на создание типовых моделей или творческих схем реализации безопасного использования информации.

Переходя к конкретному рассмотрению вопросов обучения информационной безопасности в общеобразовательных учреждениях, возьмем за пример программу по предмету Информатика. Относительно программы «Формирование ИКТ компетентности обучающихся» можно сказать следующее: прохождение курса обучает нормативам информационной культуры, морально-этическим и правовым аспектам, прививает культуру уважительного отношения к информационным правам каждой личности, а также уважению персональной конфиденциальности.

Сфера навыков потенциального выпускника, прошедшего предмет «Информатика», дополняется умением шифровать тексты, декодировать их при наличии известных таблиц и алгоритмов. Также, аудитория учащихся в рамках этого предмета должна получить навыки организации личного информационного пространства, с использованием технических средств: накопители на жестких дисках, флэш карты памяти и прочие, включая веб сервисы хранения данных. Аналогично предыдущему предмету, курс «Информатики» также предполагает ознакомление учеников с нормами информационной этики, правовыми аспектами использования программного обеспечения и ресурсов сети Интернет.

Важным результатом процесса обучения предмету «Информатика» выступает умение выпускника аналитически оценивать информацию. В

частности, пройдя курс, учащийся должен уметь оценивать степень достоверности информации, определять насколько она подкреплена доказательной базой или аргументирована, изучить подлинность контента, используя разнообразные критерии: надежность источника; наличие аналогичных сообщений на других, вызывающих доверие, ресурсах; оценить сообщение во временном разрезе.

Основы шифрования данных излагаются в разделе «Информация и способы её представления». Тут изучаются как непосредственно алгоритмы шифрования информации, проводится знакомство с кодовыми таблицами, так и уделяется внимание представлению текстов в компьютерах. Изучается двоичная система исчисления и методика преобразования информации между подобным и стандартным – десятичным форматом. Непосредственная безопасность данных относительно программных средств воздействия реализуется курсом «Использование программных систем и сервисов», также внимание учеников концентрируется на компьютерных вирусах, троянских разработках, прочем зловредном ПО, а также задаются основы антивирусной профилактики.

Пользуясь в обыденной речи словами «риск», «рисковать», мы, прекрасно понимая их значение, редко пытаемся строго его сформулировать. Первое, что необходимо здесь подчеркнуть, — это то, что, говоря о риске, мы вторгаемся в сферу возможного, а не действительного бытия. Риск — это то, что связано с возможностью как благоприятного, так и неблагоприятного, даже трагического исхода.

Во-вторых, риск всегда сопряжен с утратой или снижением уровня определенности. Рискуя, человек ввергает себя в состояние повышенной неопределенности, расширяет для себя диапазон как позитивных, так и негативных возможностей. Действие в условиях повышенной неопределенности поэтому часто бывает более продуктивным, однако и сопряжено с большими потенциальными потерями, чем аналогичное действие в обычных условиях.

В-третьих, риск всегда предполагает действие. Будучи источником риска, то или иное действие несет в себе в качестве потенциального основного или побочного результата какие-либо негативные последствия. Таким образом, риск — это характеристика потенциальной стороны действия.

Следовательно, риск можно определить, как потенциальную характеристику действия, проявляющуюся в возможности негативных последствий его результатов. Поскольку риск неотделим от действия, предпринимаемого человеком в обществе и преследующего социальные цели, это явление социальное, точнее, социально-поведенческое. В.И. Зубков, утверждал, что «риск представляет собой социальное поведение субъекта, осуществляемое в условиях неопределенности его исходов». В таком случае риск с необходимостью составляет предмет изучения социологии. С социологией безопасности тесно граничит и переплетается в своей предметной области социология рисков — направление, продуктивно разрабатываемое в рамках современной зарубежной социологической науки.

Неопределенность — основа любого риска, поскольку сама ситуация риска может рассматриваться как некая разновидность нс «определенности, преодоление которой и вызывает действия со стороны субъекта риска. Таким образом, определенные действия в целях снятия рисковой ситуации позволяют снять ситуацию неопределенности.

Вероятность как характеристика риска проявляется в степени отклонения результата риска и его непредсказуемости. Отклонения могут носить как положительный характер, так и отрицательный, и в этом заключается содержание риска.

Противоречивость риска определяется тем, что, с одной стороны, деятельность, связанная с риском, может привести к общественно значимым результатам, но, с другой стороны, очень часто риск и деятельность, связанная с ним, оказываются несовместимы с нормами и стандартами, принятыми в обществе относительно тех или иных методов решения проблем. В итоге риск и сама рисковая деятельность приобретают аномичный (отклоняющийся)

характер, и результат деятельности, положительный для субъекта риска, не расценивается как таковой общественностью, поскольку разрушает сложившиеся нормы и представления о механизмах социальной адаптации, достижении социального успеха и т. д.

Отношение к риску — это весьма специфическая категория социально-психологического характера, отражающая социокультурную и историческую специфику общества, так как в каждом социуме складывается свое отношение к риску. Так, для общества традиционного типа любое поведение, отклоняющееся от общепринятых норм, воспринимается негативно, и, соответственно, действия, связанные с риском, оцениваются крайне отрицательно. Да их и не может быть много в таком обществе, которое регулируется общественными нормами, сложившимися устоями и принципами. Для риска в таком обществе почва крайне неблагоприятная, поскольку в нем видят явную угрозу сложившимся устоям и правилам, нормам и традициям.

Альтернативность риска определяется возможностью выбора того или иного варианта решения проблемы, действия, от которого зависит и характер последствий риск- деятельности. Альтернативность риска находится в прямой зависимости от типа обществ» и характера его развития. Общество, в котором социальные нор мы перестали выполнять эффективно свою регулирующую функцию, предоставляет индивиду обширный выбор тех или иных жизненных стратегий, жизненных стилей, реализации стремлений и планов, что приводит к расширению и увеличению зоны риска. По сути, эта зона риска и становится тем пространством, в котором осуществляют свою деятельность индивиды в эпоху великих трансформаций.

Рассмотрим еще понятие угрозы. Следует проводить различие между риском и угрозой. Если риск — это возможностная характеристика действия с точки зрения его негативных потенциальных последствий, то под угрозой понимается наличие некоего внешнего объективно- субъективного фактора, который независимо от воли и поведения реципиента может вызвать

негативные и опасные последствия. Таким образом, риск создаем своими действиями мы сами, тогда как угроза существует вне нас и независимо от нас. Угроза — это реальная возможность обусловленных внешними факторами деструктивных изменений в отношении значимых и ценных для общества и личности объектов, субъектов, состояний. Так, военная угроза представляет собой «объективное состояние военно-политических отношений, для которого характерна высокая вероятность возникновения войны и нанесения государству и обществу ущерба военным путем, средствами вооруженного насилия». Как и риск, угроза составляет фактор негативного воздействия на процессы обеспечения безопасности.

С поддержанием безопасности как стабильного, не допускающего неконтролируемых изменений, состояния связано еще одно понятие того же ряда — понятие вызова. В отличие от риска и угрозы вызов — это то, чему невозможно противостоять и сопротивляться. В то время как риск исходит от нашего собственного действия, а угроза таится в намерениях и действиях другого, вызов порождается объективной логикой текущих процессов и изменений, и суть его в том, что он требует ответных социальных изменений. Дестабилизирующий характер вызова определяется изменчивостью самого общества как динамической системы связей и отношений, неравномерностью и сложностью его динамики, взаимной увязанностью всех его элементов. Назревшие в одном сегменте системы перемены в силу ее целостности с необходимостью побуждают меняться соответствующим образом и другие ее части. Через вызовы и следование им, то есть ответы на них, и происходит развитие социальной системы как единый процесс. В таком смысле — в контексте общего развития и усложнения общества — использует понятие вызова, в частности, знаменитый британский социальный мыслитель А. Тойнби. Он пишет: «Вызов побуждает к росту. Ответом на вызов общество решает вставшую перед ним задачу, чем переводит себя в более высокое и более совершенное с точки зрения усложнения структуры состояние». Таким образом, вызов есть состояние некоторой напряженности, возникающее

внутри общества как системы и требующее разрешения. Его можно определить, как противоречие между наличным состоянием общества как социокультурной и идентификационной целостности, включающей определенные ценности, нормы, идеалы, стереотипы, и возникшей потребностью в глубоких социальных изменениях, проявляющееся в повышении уровня неопределенности и нестабильности, угрожающем безопасности системы.

Значит, риски и угрозы во всем своем многообразии оказывают неоднозначное и многоплановое воздействие на безопасность общества и личности. Разумеется, наиболее безопасным с точки зрения социальной динамики состоянием является стабильность. Однако общество обладает динамическим характером, и траектория его развития лежит через периоды неопределенности. Сложность проблем, связанных с обеспечением безопасности, в том-то и заключается, что риски и вызовы неотделимы от жизненно необходимых позитивных социальных изменений, и культура безопасности требует осмысленной минимизации рисков и угроз в ходе реализации таких изменений, а вовсе не отказа от них. Социология безопасности исследует именно возможности и средства подобной минимизации дестабилизирующих эффектов развития.

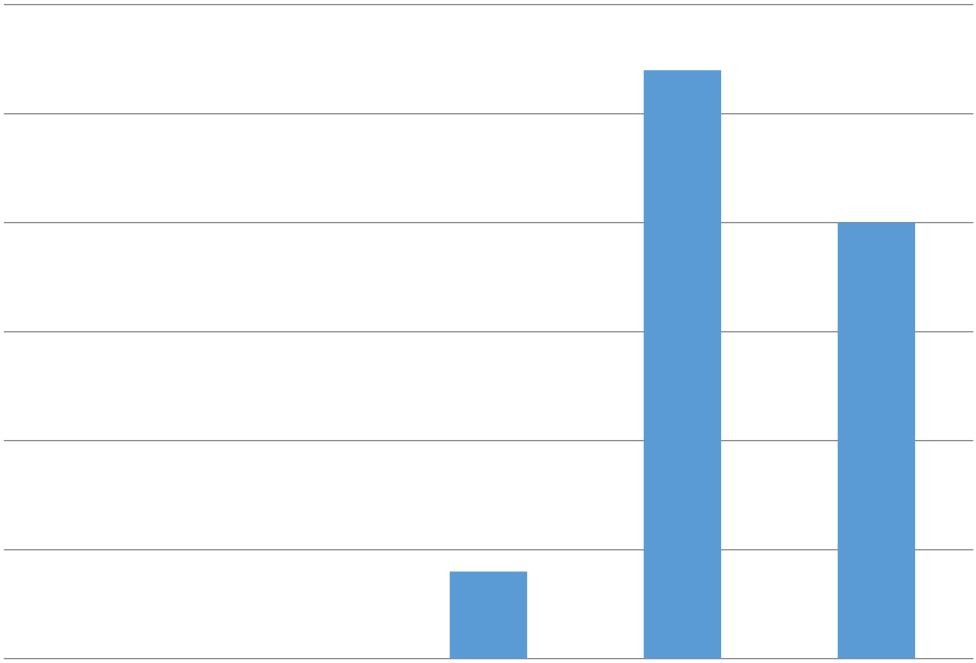
Для проверки уровня навыков информационной безопасности было проведено анкетирование учеников 11-х классов. Приложение 1. В анкетировании приняли участие 51 ученик, которые состояли из учеников 11А класса – 29 человек, обучающихся по информационно-технологическому профилю, а также учеников 11Б класса – 22 человек, обучающихся по социально-гуманитарному профилю. Анкета состояла из 15 вопросов, которые касались основных аспектов информационной безопасности, включал тестовые вопросы и задания с дополнением.

Один из вопросов анкеты: «Уделяется ли внимание вопросам защиты информации и информационной безопасности на уроках информатики?».

Ответы представлены на диаграмме 1, где можно видеть, что большинство учащихся ответили – нет, либо скорее нет, чем да.

Диаграмма 1.

Ответы на вопрос о информационной безопасности на уроках информатики

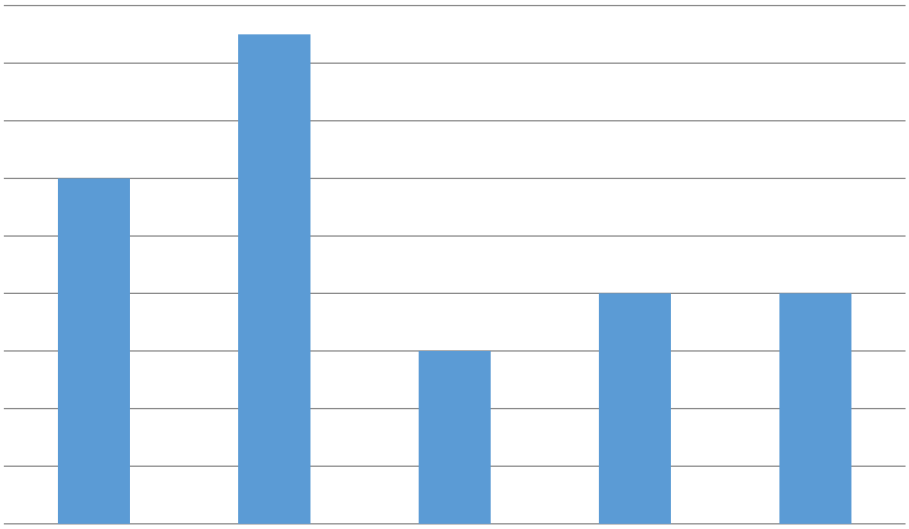


На вопрос «Хотели бы Вы пройти курс по основам информационной безопасности?» были получены результаты, представленные на диаграмме 2.

Главной задачей игровой деятельности и самой методической системы будет стоять формирование понимания учащимися процессов информации, изучение методов защиты и развитие умения учащегося самостоятельно распознать угрозу, исходящую от информационного воздействия и суметь её нейтрализовать.

Диаграмма 1.

Ответы на вопрос о прохождении курса



При рассмотрении вопросов информационной безопасности можно сделать вывод, что в данной области, учащиеся отвечают на вопросы на интуитивном уровне: нет однозначных ответов на вопрос о том, что такое информационная безопасность, также более 74% учеников ответили, что понятие «защита информации» и «информационная безопасность» имеют одинаковое значение. На вопрос – пользуются ли они антивирусными программами для защиты от компьютерных вирусов – 56% обучающихся ответили, что никогда не пользовались такими программами и утилитами. Около 90% опрошенных учащихся даже не задумывались о возможных информационных угрозах, с которыми они могут столкнуться в жизни.

Из всех опрошенных детей 10% сказали, что их аккаунты в социальных сетях уже взламывались, даже не один раз.

Можно сделать вывод, что необходимо развивать навыки информационной безопасности старших школьников.

2.2 Практические советы применения игровой деятельности для формирования навыков информационной безопасности старшеклассников

Информатика как учебный предмет в школе является достаточно нетрадиционной дисциплиной [1]. Прежде всего, это говорит о том, что, во-первых, информатика - это фундаментальная дисциплина, содействующая становлению и развитию информационного мировоззрения и компьютерного стиля мышления школьников, и, во - вторых, это дисциплина, гарантирующая приобретение учащимися совокупности знаний, умений и навыков, связанных с владением программным обеспечением, вычислительной техникой и компьютерным оборудованием. Одним из обязательных инструментов при обучении информатике является компьютер, который влияет на многие аспекты построения методологических систем обучения и основы выстраивания взаимоотношений между учеником и учителем [3]. При этих обстоятельствах насущной и актуальной является задача развить у школьника заинтересованность к самостоятельному приобретению знаний и умений, сформировать навыки применения уже существующих знаний в нетривиальных ситуациях. В этой связи, перед школой ставится задача по формированию предприимчивой личности, которая обладает углубленными знаниями, достаточными для возможности результативного потенциального обучения, что является актуальным вопросом, как для педагогики России, так и для педагогики ряда других стран [4].

В игровой и учебной практике находится ряд качественных различий, и это логично, так как игра и учеба – две разные деятельности. Объективно подмечено, что резко навязывая ребенку подход к любой деятельности методами взрослого человека, школа отводит недостаточно, а порой и слишком мало места игре. Она преуменьшает организационную позицию игры. Переключение учащихся от игровой деятельности к более важным и серьезным занятиям происходит стремительно, вследствие этого между регламентированными школьными уроками и непринужденной игрой выходит ничем не заполненный разрыв. Здесь имеют место переходные формы. В качестве таковых и выступают дидактические игры «Игра должна быть организована так, чтобы в ней предчувствовался будущий урок» [8].

Выдающийся, советский педагог - новатор В.А. Сухомлинский писал: «Присмотримся внимательно, какое место занимает игра в жизни ребенка… Для него игра – это самое серьезное дело. В игре раскрывается перед детьми мир, раскрываются творческие способности личности. Без них нет и не может быть полноценного умственного развития» [8].

Использование дидактических игр на уроках информатики является источником активизации познавательной и учебной деятельности учащихся, и, стало быть, приводят к возрастанию эффективности обучения информатике, если такие игры предназначены быть средством получения знаний, умений и навыков по информатике, отражают базисное60 содержание обучения, а также содействуют развитию мыслительной деятельности школьников.

За время возникновения и развития информатики как учебного предмета было исследовано большое количество методических разработок преподавания в средней школе. В их числе научные работы А. Г. Гейна [5], А. В. Горячева [6], Н. Д. Угриновича [7] и др.

Анализ этих исследований указывает на то, что в области методики преподавания информатики до сих пор существует ряд нерешенных проблем. В частности, учащиеся, воспринимают курс информатики, либо отдельные его разделы с видимыми затруднениями.

Однако, несмотря на то, что данной проблеме посвящены многие разработки и исследования педагогов и психологов, можно выделить ряд нерешенных проблем, основной из которых является проблема недостаточного исследования влияния дидактических мини-игр школьного курса информатики на формирование и развитие познавательной активности школьников.

Очевидно, существует противоречие между потребностью формирования познавательной активности, которая несомненно положительно влияет на эффективность изучения информатики, с одной стороны, и, напротив, «сыростью» методических подходов к развитию и

использованию дидактических мини-игр по информатике как средства развития познавательной деятельности учащихся.

Необходимость развития познавательной активности учащихся на базе применения на уроках информатики учебно-игровой деятельности составляет проблему исследования.

Важно отметить, что назначение дидактических игр на уроках информатики не сводится лишь к заполнению свободного времени. При подборе дидактической игры следует учесть, какие именно психические свойства и качества, необходимые детям, они развивают, какие воспитательные и образовательные задачи решают, так же применять игры необходимо осмысленно, последовательно и в определенной системе.

Моделирование поведенческих сценариев в применение к заданной ситуации остается базовой методикой обучения старшеклассников основам информационной безопасности. Подобный подход реализуется как при базовом получении знаний, так и в обучении профильных специалистов. Основу методики составляет концептуальная база ИБ, из которой опытных педагог может выкраивать практические модели под типовые поведенческие сценарии для обеспечения информационной безопасности ученика: ребенка или подростка.

Затрагивая тему ИБ на уровне общества, целесообразным становится применение экспериментальных моделей, для аналитического осмысления участия старшеклассника в разнообразных социальных проектах, объединениях по интересам, различных неформальных организаций и прочее. Моделирование под обеспечение информационной безопасности на международном уровне или применительно к государству, осуществляется на базе соответствующих элементов концептуальной базы ИБ.

Информационная безопасность в Интернете может обсуждаться во время уроков информатики, социологии, ОБЖ, гражданского права и др. В образовательном учреждении рекомендуется проводить неделю, день, уроки Интернет-безопасности, внеклассные мероприятия.

Мероприятия можно приурочить к профессиональным праздникам:

Международный день защиты информации - 30 ноября. Праздник начал существовать в 1998 году (с праздника есть даже сайт) т.к. в 1988 г. была зафиксирована первая массовая эпидемия червя, получившего название по имени своего «творца» - Морриса. Праздник существует и признан международным благодаря американской Ассоциация компьютерного оборудования. Цель этого Дня — напомнить всем о необходимости защиты компьютерной информации, а также обратить внимание производителей и пользователей аппаратных и программных средств на проблемы безопасности.

Международный день безопасного Интернета - второй вторник февраля (введен в 2004 году). Сайт международного дня безопасности Интернета www.saferinternetday.org

Во время мероприятий по медиабезопасности следует ознакомить обучающихся:

- с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;

- с информацией о необходимости критического отношения к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, признаках отличия достоверных сведений от недостоверных, способах нейтрализации вредной и опасной для детей информации, распознавания признаков злоупотребления доверчивостью;

- с правилами общения в социальных сетях (сетевой этикет).

В рекомендациях «Безопасный Интернет» [14], а также потенциально готовыми темами мин-игр, предлагается следующая тематика проведения школьных мероприятий по медиабезопасности:

- Противозаконная, неэтичная и вредоносная информация в Интернете: как ее избежать.

- Достоверность информации в Интернете, проблемы и способы проверки информации на достоверность и полноту.

- Этика сетевого общения.

- Личная информация: нужна ли она в Интернете, как защитить личную информацию в блогах, социальных сетях и пр.

- Социальные сети: как общаться в сети и не попасть в сети мошенников и злоумышленников.

- Что такое хакерство? Почему хакеров считают преступниками.

- Интернет-зависимость: угрозы, реальность, проблемы, решения.

- Web -серфинг: как не потерять себя и свое время в Интернете.

- Как распознать кибермошенничество и не стать жертвой.

- Нигерийские письма: предложения в письмах и как не попасться на удочку мошенников.

- Что такое киберхулиганство: как не стать жертвой и киберхулиганом.

- Как защитить свою почту от спама и не стать спамером.

- Компьютерные вирусы и методы борьбы с ними.

- Законодательство России о киберпреступлениях.

- Безопасность в коммерческих Интернет-сервисах: Интернет-магазины, услуги различных фирм и др.,

- Компьютерные игры, как не стать игроманом.

- Азартные игры в Интернете - поле чудес для....?

- Мобильные угрозы в современном мире.

- Как правильно вести себя с киберхулиганами и защититься от нежелательного общения.

Одним из эффективных способов изучения любого учебного материала и в частности вопросов по информационной безопасности является метод высокотехнологичных учебных проектов. Учителю любой дисциплины важно инициировать большие и малые телекоммуникационные учебные проекты.

В методических рекомендации по проведению уроков «Безопасность в Интернете» в начальной и средней школе [11] учебный телекоммуникационный проект рассматривается как совместная учебно-познавательная, творческая или игровая деятельность учащихся-партнеров,

организованная на основе компьютерной телекоммуникации, имеющая общую цель, согласованные способы деятельности, направленная на достижение общего результата деятельности.

Так, например, можно участвовать в сетевых проектах для школьников, организованных дистанционно или организовать собственный учебный проект.

Школьной проектной деятельностью учитель решает сразу несколько проблем [11]: во-первых, учащиеся приобретают навык практического применения полученных теоретических знаний по использованию компьютеров, компьютерных технологий и Интернета и связанные с этим вопросы безопасности; во-вторых, и это самое главное, школьник начинает видеть в компьютере и Интернете не только игрушку и поток непотребных ресурсов, но инструмент создания нового, интересного и нужного не только ему, но и окружающим его в школе и дома людям, пространства. И в этом пространстве ребёнок подобен творцу: каким он его создаст, таким его мир и будет.

Лучше всего инициировать глобальный (на один или несколько классов) проект, связанный с усиленной необходимостью коммуникации. То есть каждый школьник выполняет часть работы по общему учебному телекоммуникационному проекту. Чем глобальнее и трудозатратнее проект, тем лучше. Для этого проект должен быть:

а) интересен самим детям и, желательно, и предложен же ими, чтобы они позднее не могли отказаться от того, что сами же и предложили;

б) очень высокотехнологичным, чтобы для его реализации школьнику было необходимо полностью проявить свою компьютерную «продвинутость», да ещё и подучиться разным сложным технологиям, общаясь со своими виртуальными друзьями.

в) долгосрочным и предусматривающим дальнейшее коммуникативное дополнение. После размещения его в сети у детей, гордящихся проделанной работой, должен быть стимул общаться в Интернете

на тему своего проекта и постоянно дополнять и дорабатывать его. Для этого необходимо устраивать публичные показы проектов школьников на классных часах, на предметных уроках, в рамках программы которых сделаны эти проекты.

В качестве примера можно привести сетевую игру, организованную в МКОУ ГО Заречный «СОШ№4». 40 детей из 7 городов России в течение месяца рассказывали в сети друг другу о своем городе и градообразующем мероприятии в форме сетевых презентаций, видеороликов и сетевых газет, а затем с помощью созданных сетевых интерактивных заданий проверяли друг у друга приобретенные за это время знания. Времени детям хватало только на то, чтобы в сети создавать и творить собственные сетевые ресурсы, смотреть и анализировать работы других участников игры. Прогуливаться по различным сомнительным сайтам возможности не было. Сейчас ребята знают, чем можно заниматься в сети.

Если ребенок с социально-значимым результатом побывал в сети, узнал, что в сети можно оформлять фото и видео материалы, создавать презентации, инструменты для проверки знаний, организовать личное сетевое пространство, проводить информационные исследования, то вряд ли у него появится в дальнейшем желание вновь перейти к праздному лицезрению сетевых ресурсов.

Конкретным примером реализации проектной деятельности может стать WEB-квест. Для примера можно рассмотреть WEB-квест «Безопасный Интернет [50].

Веб-квест - это игра, реализованная на сетевом ресурсе с заданиями над которыми работают учащиеся, выполняя ту или иную возложенную на них миссию - выбрав одну из ролей, предложенных учителем.

Особенностью образовательных веб-квестов является то, что часть или вся информация для самостоятельной или групповой работы учащихся с ним находится на различных веб-сайтах, ссылки на которые может предложить педагог, предварительно выбрав самые интересные и информативные по

изучаемому вопросу. Кроме того, результатом работы с веб-квестом является публикация работ учащихся в виде веб-страниц и веб-сайтов (локально или в Интернет).

Итак, выделим, на что необходимо обратить особенное внимание при рассмотрении вопроса об Интернет безопасности детей основной школы:

1. Относись к информации осторожно. То, что веб-сайт эффектно выглядит, еще ни о чем не говорит. В чем меня хотят убедить его создатели? Чего этому сайту не достает? Узнай об авторах сайта: зайди в раздел «О нас» или нажми на похожие ссылки на странице. Узнай, кто разместил информацию. Если источник надежный, например, университет, то, вполне возможно, что информации на сайте можно доверять.

2. Часто в Сети можно столкнуться с подделками под известные сайты социальных сетей или почтовых сервисов, так называемым «фишингом». После неосторожного ввода имени пользователя и пароля на страницах не настоящих, поддельных сайтов, злоумышленники используют пароли в своих целях на реальных сайтах. Например, для рассылки спама от имени владельца почтового ящика или злоумышленного обращения в социальных сетях от имени владельца аккаунта. Каждый сайт в Интернете имеет свой уникальный адрес. Необходимо проверять именно адрес страницы, не доверяя внешнему оформлению, которое может быть скопировано с оригинального.

3. Любое практическое применение информации полученной внутри веб пространство должно базироваться на правиле трех источников. Это минимальный набор однотипных ссылок, подтверждающих достоверность материала. Суть методики состоит в поиске аналогичной информации и сравнении ее содержимого на примере минимума в три различных источника. Дополнительным критерием проверки могут служить временные рамки опубликованного материала по всем найденным источникам. Необходимо помнить – Интернет, территория с минимальной цензурой, что наряду с положительной чертой несет и негативный аспект. Поэтому достоверности

используемой информации стоит уделять повышенное внимание, особенно если ее предполагается применять по работе.

Полная свобода стиля общения в сети Интернет не лишена определенных норм этикета и вежливости. Несмотря на долю открытой грубости, присутствующую на веб пространстве, рекомендуется не терять выдержки и проявлять терпимость к чужим мнениям, отличным от вашей точки зрения. Анонимность в сети - не повод пренебрегать нормами человеческого общения. Помочь преодолеть эмоциональную реакцию на неприятное сообщение может пауза. Лучше выждать несколько минут, чтобы ответное послание руководствовалось здравым смыслом, а не эмоциональным фоном. Основные правила общения в сети описаны в приложении «Сетевой этикет».

Жизнь современного человека развивается настолько стремительно, что порой бывает очень тяжело за ней угнаться, поток информации, который сопровождает человека, с каждым годом растет и в данном случае очень сложно переоценить роль Интернета как информационного ресурса. Но, невзирая на бесспорно глобальное значение Интернета в жизни людей, у общества стали возникать трудности с его использованием.

Активными пользователями сети сегодня являются как взрослые люди, так и несовершеннолетние, порой даже кажется, что современный ребенок уже родился со знаниями использования современных гаджетов. Мы наблюдаем, что процесс социализации, развития ребенка как личности происходит непосредственно в информационном пространстве, сопровождаясь естественным образом, большим потоком информации. Но современные дети используют компьютер не только в домашних условиях, но и для учебы. В учреждениях образования очень активно применяются информационно-коммуникационные технологии [1]. Ребенок в образовательном процессе, может оказаться незащищенным от всех потоков информации, в связи с этим стоит обратить особое внимание на безопасность школьников [2]. Целесообразно ввести специальный курс, позволяющий расширить знания

школьников в области информационной безопасности, проблем, возникающих при использовании Интернета, методов и форм защиты от этих угроз [3].

Согласно российскому законодательству информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию [7].

Дети, в силу своего возраста, еще не имеют сформированную должным образом психику. Они восприимчивы и склонны всю информацию по телевизору и в Интернете принимать «на веру». Ребенку очень тяжело увидеть и распознать в рекламных роликах по телевизору или в ярких картинках в Интернете манипулятивные техники. Дети из-за небольшого жизненного опыта не умеют анализировать степень достоверности информации, а так же подлинность ее источников. Дети должны знать о тех опасностях, которые могут быть при использовании Интернета и уметь себя защитить.

Факторов риска, которым подвержен пользователь Сети большое количество. Во-первых, стоит обратить внимание непосредственно нам сам контенет. Контенет – это нелегальная информация, не предназначенная для детей, это могут быть как текстовые документы, так и видеоролики, картинки и аудиозаписи [5]. Интернет сегодня пестрит суицид-сайтами, на которых можно узнать о том, какими методами можно расстаться с жизнью. Широко распространяются сайты-форумы потенциальных самоубийц, сайты порнографической направленности, наркосайты, где можно узнать подробно о рецептах изготовления в домашних условиях злосчастного зелья. В последнее время все больше активизируются сайты, разжигающие национальную рознь, расовое неприятие, религиозную рознь, национализм, терроризм, экстремизм и т.д.

Любимым занятием большинства школьников в свободное время являются компьютерные игры, тем временем, уже давно доказано, что у

ребенка может возникнуть психологическая зависимость. Родителям стоит контролировать своего ребенка в Сети и выделять определенное время для игр. Рынок игр сейчас очень широк, игр большое количество, все они разные, но есть игры, причем их большое количество, в которых присутствует жестокость, насилие, агрессия – все это может повлиять на неустойчивую психику ребенка.

Следующий бич современного общества – социальные сети, дети также являются приверженцами виртуального общения. В первую очередь не стоит забывать о том, что виртуальное общение никогда не сможет заменить реального, а дети, которые являются сторонниками именно виртуального общения, в дальнейшем могут потерять коммуникативные способности и тогда, им будет тяжело общаться в реальной жизни и ребенок просто может замкнуться в себе. Родителям также стоит обращать внимание на то, с кем общается ребенок в Сети, потому что не исключены контакты с педофилами, мошенниками и т.д. Возможно, родителям даже стоит завести личный акаунт в сети и стать виртуальным другом своего ребенка.

Родителям нужно знать, что дети и подростки погружаются в виртуальность тогда, когда в реальном мире у них нет полноценных занятий. Рекомендуем внимательно отнестись к этой проблеме. Найти в своем расписании свободное время и посвятить его своему ребенку, играя, читая с ним. Просто посмотреть на все (в том числе и на компьютеры, ТВ, мобильник, плеер и прочие розеточные изобретения) глазами детей и подростков. И тогда виртуальный мир станет помощником вашей семье, для чего он, собственно, и предназначен [4].

Интернет является очень удобным средством общения, получения необходимой информации, но родителям и педагогам следует помнить, что детям интересно все и они с легкостью, «кликая» мышкой, попадают на различные сайты, никоем образом не предназначенные для школьников. Родителям стоит использовать средства блокировки нежелательного контента, таким образом, обеспечивая информационную безопасность своих детей.

Отдельной категорией угроз стоит выделить спам, компьютерные вирусы и другие вредоносные программы. Попадание вируса в компьютер может привести к колоссальным потерям информации, ее искажение, нарушение конфиденциальности данных. А в случае, если такой вирус проникнет в домашнюю сеть или сеть образовательного учреждения, то он может открыть доступ к закрытой информацией и открыть злоумышленникам полный доступ к конфиденциальной информации. Спам также может содержать в себе вредоносные файлы и повредить работу компьютера.

Таким образом, мы убеждаемся в том, что угроз информационной безопасности существует много и школьников нужно предупреждать о них, а реализовать это можно совместными усилиями родителей и педагогов.

Обеспечение информационной безопасности в образовательном процессе - задача учителя. Педагоги должны иметь представление об угрозах, связанных с использованием компьютера в учебной деятельности и уметь предотвращать их. Преподавателю следует уделять значительное внимание учебно-воспитательной работе со школьниками, направленной на преодоление негативного воздействия информационно-коммуникационных технологий. С этой целью, следует проводить различные инструктажи, классные часы по доступу к ресурсам Интернет, проводить лекции не только для детей, но и для их родителей.

Только комплексный подход решения проблемы, как со стороны семьи, так и со стороны школы, позволит значительно уменьшить риски возникновения угроз. Обеспечение информационной безопасности школьников должно стать одним из приоритетных направлений в учебно-воспитательной деятельности современной школы

2.3 Разработка дидактических игр в школьном курсе информационной безопасности

Дидактическая мини-игра обладает такой же структурой, как и всякая учебная деятельность, т.е. она включает в себя цель, средства, процесс мини-игры и результат. Помимо воспитательной, мини-игра преследует одновременно две цели: игровую и учебную. С одной стороны – это средство моделирования окружающей действительности, а с другой – метод обучения. Творческая атмосфера, свобода от шаблона, возникающие в процессе мини-игры, способствуют раскрепощению творческих резервов человеческой психики, нейтрализуют чувство тревоги, создают ощущение спокойствия, облегчают общение [1].

Назначение дидактических мини-игр – развитие познавательных процессов у школьников (восприятие, внимание, память, наблюдательность, сообразительность и другие) и закрепление знаний, приобретаемых на уроке. Характерным для каждой дидактической игры является, с одной стороны, решение различных дидактических задач: уточнение представлений о предмете в целом и о его существенных особенностях и т. д. В этом смысле игра носит обучающий характер. С другой стороны, неотъемлемым элементом каждой игры является игровое действие. Внимание ученика направлено именно на него, а уже в процессе игры он незаметно для себя выполняет общую задачу. Поэтому дидактические игры представляются учащимся не просто забавой, а интересным, необычным делом.

Сформулируем ряд требований к дидактической мини-игре:

– мини-игра должна основываться на свободном творчестве и самодеятельности учащихся;

– мини-игра должна быть доступной, цель мини-игры – достижимой, оформление – красочным, разнообразным;

– обязательный элемент каждой мини-игры – её эмоциональность. Мини-игра должна вызывать удовольствие, весёлое настроение, удовлетворение от удачного ответа;

– в дидактических мини-играх обязательно наличие соревновательного элемента между командами или отдельными участниками игры [2].

В ходе выполнения исследования нами разработана система дидактических мини-игр для использования в процессе формирования навыков информационной безопасности старших классов для изучения современных рисков и угроз в 9-11 х классах. Вот некоторые их них: (приложение 3).

Мы полагаем, с помощью дидактических игр приблизиться к реализации своей цели в формировании навыков информационной безопасности, чтобы учащийся мог использовать знания и умения, полученные на уроках информатики, в реальной взрослой жизни [1].

Еще одним способом для изучения современных рисков и угроз является эвристическая беседа. Этот метод применяется при первом знакомстве учащихся с каким-либо явлением или понятием. При этом учитель обязательно должен опираться на опыт школьника в его повседневной жизни, постепенно выстраивая цепочку шагов к тому явлению или понятию, которое должно быть усвоено на уроке.

Эвристическая беседа направлена на формирование критического мышления, сущность которого заключается в умении учащегося выполнять проверку предложенных решений с целью определения области их возможного применения.

Мы предлагаем следующую технологию реализации эвристической беседы:

– учитель обозначает проблему, задает вопрос о том, что известно ученикам по этой проблеме;

– учащиеся записывают в тетради все, что им известно по проблеме (строго индивидуальная работа, продолжительность которой 1-2 минуты);

– учитель организует обмен информацией по проблеме в парах или группах (время обсуждения – не более трех минут);

– группы по кругу называют сведения, факты, не повторяя ранее сказанного, при этом учащиеся составляют список идей; в это время учитель записывает все высказывания учащихся на доске без комментариев (даже ошибочные мнения);

– по мере освоения новой информации происходит связывание ее в логические цепочки, исправление ошибок;

– для применения метода эвристической беседы учитель должен обладать довольно высоким уровнем мастерства, чтобы вовлечь в беседу весь класс.

Метод эвристической беседы может и должен применяться как на начальной ступени изучения информатики, так и на последующих настолько, насколько это необходимо для максимальной эффективности обучения. Различными же на разных ступенях являются цели применения данного метода. В IX классах основной целью применения метода эвристической беседы является поддержание устойчивости внимания, а в X классах на первое место выходит развитие мышления учащихся [4].

Ценность этого метода обучения обусловлена тем, что по характеру вопросов учитель может судить о глубине знаний учащихся, степени их познавательной активности, стремлении понять сущность рассматриваемых явлений, процессов, т. е. вопросы учащихся являются своеобразным средством «обратной связи». Кроме того, зачастую вопрос учащегося включает в цепочку последовательно связанные между собой другие вопросы: решение первого порождает второй, третий, и таким образом учащиеся вовлекаются в активную работу. Вопросы в этом случае становятся не только критерием глубины знаний и интереса учащихся, но и средством, поддерживающим этот интерес.

Мы полагаем, что применение игровой деятельности способствует формирования навыков информационной безопасности старших школьников, а также содействует росту интеллектуальной активности учащихся на уроке, развитию мышления, глубокому пониманию учащимися изучаемого

материала, умению применить имеющиеся знания для решения новых познавательных и практических задач.

Таким образом, мы пришли к выводу о том, что участие школьников в дидактических мини-играх способствует формированию мировоззрения, теоретических знаний и практических умений, расширения кругозора, навыков самообразования; происходит развитие мышления, активности, памяти, способности выражать свои мысли, а также развитие познавательного интереса, побуждение к применению полученных знаний, умений, проявление инициативы, самостоятельности, коллективного сотрудничества.

ЗАКЛЮЧЕНИЕ

Игровая деятельность способствует формированию навыков информационной безопасности старших школьников. Также в круг рассмотренных задач входит взаимодействия взрослых и подростка в отношении использования компьютера, способы снижения информационных рисков, исключения деструктивной составляющей пребывания в сети Интернет, а также правовые и этические аспекты использования конфиденциальных данных.

Эффективным дополнением к усилиям педагогического состава выступает осознание родителями учеников актуальности и значимости роли информации, а особенно обеспечении информационной безопасности. Это позволяет перенести процесс обучения на дом, где он проходит в непрямой форме и создает предпосылки для профилактики негативных тенденций относительно становления информационной культуры подростка.

Совершенствование теоретических предпосылок закрепляется моделированием практических поведенческих сценариев, а также переносов образовательной нагрузки вне класса. Внеурочная форма особенно эффективна в коллективном варианте, при посещение специализированных мероприятий по информационной безопасности. Она также выступает своеобразным средством диагностики потенциала ученика относительно безопасной жизнедеятельности в информационно-общественной среде.

Мы пришли к выводу, что с помощью игровой деятельности приблизиться к реализации своей цели в формировании навыков информационной безопасности старшеклассников, чтобы учащийся мог использовать знания и умения, полученные на уроках информатики, в реальной взрослой жизни.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Абдулова Т.П. Социализация подростков в информационном пространстве // Мир психологии. 2011. № 3 (67). С. 197-207.

[2] Аверченков В. И., Рытов М. Ю. Организационная защита информации: учеб. пособие для вузов. – 3-е изд., стереотип. – М.: ФЛИНТА, 2011.

[3] Аниськин В. Н. Электронные аудиовизуальные средства обучения: устройство и дидактические возможности. Санкт-Петербург: Книжный дом, 2006. 303 с.

[4] Беляев Д.А. Актуальные проблемы аспирантуры как института воспроизводства научных кадров современной России // Молодежь в науке: проблемы и перспективы: сб. материалов международной конференции молодых ученых. Воронеж: Артефакт, 2010. С. 198 - 203.

[5] Беляев Д.А. Мультикультурализм как стратегия создания дискретного «сверхобщества» в контексте постмодернистской культуры: теория и практика // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. Тамбов. 2012. № 8 - 1. С. 46 - 50.

[6] Беляев Д.А. Университет как социокультурный феномен: прошлое, настоящее, будущее // Современное образование в условиях реформирования: инновации и перспективы: Материалы I Всероссийской научно - практической конференции 17 марта 2010 г. / под общей ред. А.И. Таюрского. Красноярск: В 3 - х ч. 2010. Ч. 2. С. 21 - 24.

[7] Беляев Д.А. Феномен массовой коммуникации: исторический аспект и современные проблемы // Социогуманитарные науки в трансформирующемся обществе: человек и общество в условиях социально - экономического и социокультурного кризиса: сборник статей и тезисов докладов VIII всероссийской научной конференции. Май 2010. Липецк: Из - во ЛГТУ. 2010. С. 200 - 202.

[8] Богомолов В. А. Экономическая безопасность: учеб. пособие для студентов вузов, обучающихся по специальностям эко- номики и управления. – М.: ЮНИТИ-ДАНА, 2010. – 295 с.

[9] Босова Л. Л. Информатика и ИКТ: учебник для 5 класса – 4-е изд. М.: БИНОМ. Лаборатория знаний, 2012. 199 с.: ил.

[10] Босова Л. Л. Информатика и ИКТ: учебник для 6 класса – 4-е изд. М.: Бином. Лаборатория знаний, 2012. 215 с.

[11] Босова Л. Л. Информатика и ИКТ: учебник для 7 класса – 4-е изд. М.: БИНОМ. Лаборатория знаний, 2012. 237 с.

[12] Бочаров М.И., Симонова И.В. Методика обучения информационной безопасности в школе. // Пространство и время, № 4, 2013.

[13] Брандман Э. Информационная безопасность российского общества в современных условиях [Электронный ресурс] //

[14] Власть. 2007. № 5. С. .68-71. Режим доступа: http://www.isras.ru/files/File/Vlast/2007/05/Informacionnaya_bezopasnost.pdf

[15] Гафарова Г.Г., Смелянская В.В. Информационная безопасность личности [Электронный ресурс] // «Безопасность личности:состояние и возможности обеспечения». Материалы конференции. Пенза: Научно-издательский центр «Социосфера». 2012. Режим доступа: http://sociosphera.com/publication/conference/2012/140/informacionnaya_bezopasnost_lichnosti/.

[16] Гейн А. Г. Информатика и ИКТ. 11 класс: Учеб. для общеобразоват. учреждений: базовый и профил. уровни // Г. Гейн, А.И. Сенокосов. М.: Просвещение, 2012.

[17] Гейн А. Г., Шолохович В. Ф. Преподавание курса «Основы информатики и вычислительной техники» в средней школе: Руководство для учителя. - Екатеринбург, 1992.138 с.

[18] Гордеева М., Дмитрик Н., Лазарев Д., Наумов В., Савельев Д. Федеральный закон «Об обеспечении информационной безопасности».

Проект [Электронный ресурс] // Park Media Consulting. 2003 Режим доступа: http://www.parkmedia.ru/about.asp?obno=69

[19] Горячева А. В., Шафрин Ю. А. Практикум по информационным технологиям. М.: Лаборатория Базовых Знаний, 1999. 356 с.

[20] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895) // Российская газета. 2000. 28 сентября. № 187.

[21] Ермоленко В.А. Дидактические основы безопасности жизнедеятельности. М.: ИТИП РАО, 2010.

[22] Информатика и ИКТ. 11 класс. Базовый уровень / Под ред. проф. Н.В. Макаровой. СПб.: Питер, 2009.

[23] Карташова Л.И. Возможности различных этапов урока информатики по развитию познавательной мотивации старшеклассников // Бюллетень лаборатории математического, естественнонаучного образования и информатизации: рецензируемый сборник научных трудов. Т. II. Воронеж: Научная книга, 2012. С. 232–235.

[24] Карташова Л.И. Модель развития познавательной мотивации старшеклассников при обучении информатике // Вестник Московского городского педагогического университета. Серия «Информатика и информатизация образования». 2011. № 1 (21). С. 54–61.

[25] Ковалева Н.Н. Информационное право России: Учеб. пособие. М.: Издательско-торговая корпорация, «Дашков и К°», 2007.

[26] Киселев Г.М. Информационные технологии в педагогическом образовании: Учебник / Г.М. Киселев, Р.В. Бочкова. — 2-е изд., перераб. и доп. — М.: Издательско-торговая корпорация «Дашков и К», 2014. — 304 с.

[27] Конвенция об обеспечении международной информационной безопасности (концепция) (Электронный ресурс] // Министерство иностранных дел Российской Федерации. Официальный сайт. 22.09.2011. Режим доступа: http://qoo.by/2bNt

[28] Крошилин С. В., Медведева Е. И. Информационные технологии и системы в экономике: учеб. пособие. – М.: ИПКИР, 2008.

[29] Крошилин С. В., Медведева Е. И. Безопасность информационных ресурсов предприятия: выявление угроз и методы их устранения // Информационные ресурсы России. – М.: Российское энергетическое агентство Минэнерго РФ- 2009. – Вып. 5. – С. 32–37.

[30] Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации: учебник. – М.: Издательство: Издательский центр «Академия», 2012.

[31] Мельников В.П. Информационная безопасность и защита информации: Учеб. пос. для студ. высш. учеб. заведений / П. Мельников, С.А. Клейменов, А.М. Петраков; под. ред. С.А. Клейменова. 4-е изд., стер. М.: Издательский центр «Академия» 2009.

[32] Панфилова А.П. Инновационные педагогические технологии: Активное обучение: учеб. пособие для студ. высш. учеб. заведений / А.П. Панфилова. — М.: Издательский центр «Академия», – 2009. – 192 с.

[33] Патаракин Е.Д. Социальные сервисы Веб 2.0 в помощь учителю / Е.Д. Патаркин. – М: Интуит.ру, 2007. – 64 с. [Электронный ресурс]. – Режим доступа: http://www.iteach.ru/met

[34] Петров В.П., Петров С.В. Информационная безопасность человека и общества: Учебное пособие. М.: ЭНАС, 2007.

[35] Полат Е.С. Новые педагогические и информационные технологии в системе образования / Е.С. Полат. – М: Издательский центр «Академия». – 2002. – с. 272.

[36] Полат Е.С. Современные педагогические и информационные технологии в системе образования: учеб. пособие для студентов высш. учеб. заведений / Е.С. Полат, М.Ю. Бухаркина. – М: Издательский центр «Академия». – 2007. – 368 с.

[37] Райзберг Б.А., Лозовский Л.Ш., Стародубцева Е.Б. Современный экономический словарь. М.: ИНФРА-М, 2006.

[38] Самойлова И.С. Методические рекомендации по организации урока информационной безопасности в основной школе. // Образование, № 12, 2015.

[39] Селевко Г.К. Педагогические технологии на основе дидактического и методического усовершенствования УВП. – М.: НИИ школьных технологий, 2005. – 288 с.

[40] Стрельцов А. А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. М.: МЦНМО, 2002.

[41] Сухомлинский В.А. Избранные педагогические сочинения: В 3 - х т. Т.1 / Составители: О.С.Богданова, В.З.Смаль - М.: изд. «Педагогика», 1979.

[42] Угринович Н. Д. Информатика и информационные технологии: Учеб. Пособие М., 2000. 211 с.

[43] Федеральный закон Российской Федерации от 19.05 1995 № 82-ФЗ «Об общественных объединениях» [Электронный ресурс] // Референт. Правовая система нового поколения. Режим доступа: http://www.referent.ru/1/78600).

[44] Федеральный закон Российской Федерации от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // Российская газета. 2010. 31 дек. Федеральный выпуск №5376.

[45] Фролов С.С. Социология. Учебник для высших учебных заведений. М.: Наука, 1994.

[46] Хуторской А.В. Ключевые компетенции как компонент личностно-ориентированной парадигмы образования [Текст] / А.В. Хуторской // Народное образование. – 2003. – №2. – С. 58-64.

[47] Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. 2-е изд. М.: Академический Проект; Гаудеамус, , 2004.

[48] Ясенев В. Н. Информационные системы и технологии в экономике: учеб. пособие. – 3-е изд., перераб. и доп. – М.: ЮНИ- ТИ-ДАНА, 2012.

[49] http://www.it2b.ru/

[50] http://www.openclass.ru/node/447288

[51] http://qoo.by/2bMB

[52] https://goo.gl/Gnw3NV

ПРИЛОЖЕНИЕ 1

Анкета для учащихся 6-10 классов

Дорогой друг! Целью анкетирования является изучение твоего отношения к компьютеру, вопросам информационной безопасности.

1. **Класс, в котором ты учишься?_____**

2. **Пользуешься ли ты Интернетом в школе? (***возможны несколько вариантов ответов***)**

а) да, б) нет в) редко

3. **Установлены ли в твоей школе на компьютерах программы, ограничивающие доступ на какие - либо сайты?** а) да б) нет в) не знаю

4. Есть ли у тебя дома компьютер, подключенный к сети интернет?

а) да б) нет в) есть только для родителей

5. Сколько времени в день ты проводишь за компьютером?

а) менее часа б) 1-3 часа в) более 3 часов

6. Что такое информационная безопасность

Ответ:____

7. Взламывали ваш аккаунт в социальных сетях?

а) да, один раз

б) да, много раз

в) не помню

г) нет

8. При регистрации в социальных сетях ты пользуешься настоящим или вымышленным именем; называешь личные данные?

а) да, подлинные данные б) нет, имя и данные вымышленные в) когда как

9. Пользуются ли они антивирусными программами для защиты от компьютерных вирусов

а) да, б) нет

10. Что ты делаешь, когда приходит предложение зарегистрироваться в «друзьях» от незнакомых людей?

а) удаляю информацию б) добавляю в «друзья»

в) пытаюсь сначала что-либо узнать о них г) другое

11. Как ты реагируешь на получение спамов, рекламных роликов, различных сообщений, содержащих неприятную информацию, оскорбления, запугивания и др.; приглашений на участие в лотереях, конкурсах, азартных играх?

а) сразу удаляю б) пытаюсь найти для себя что-то интересное

в) мне это неинтересно г) меня это раздражает

12. Знаком ли ты с правилами безопасного поведения в Интернете?

а) да, знакомили в школе б) да, рассказали родители в) да, прочитал(а) на специальных сайтах в Интернете г) нет никаких правил, Интернет - это свободное пространство, в котором можно все

13. Контролируют ли родители твою деятельность в Интернете?

а) да, разрешают выходить в интернет только в их присутствии б) да, установили специальные программы в) да, проверяют журнал посещений и загрузок г) нет, они мне доверяют д) нет, не контролируют

14. Уделяется ли внимание вопросам защиты информации и информационной безопасности на уроках информатика?

а) да б) скорее да, чем нет в) не помню г) скорее нет, чем да д) нет

15. Хотели бы Вы пройти курс по основам информационной безопасности?

а) да б) скорее да, чем нет в) затрудняюсь ответить г) скорее нет, чем да д) нет

Спасибо за искренние ответы!

ПРИЛОЖЕНИЕ 2

Список 11А класса:

1. Астафьев Дмитрий
2. Бакаева Арина
3. Беликов Константин
4. Берко Полина
5. Боровков Владимир
6. Быстров Денис
7. Галацан Полина
8. Гасанов Павел
9. Гацаев Изновр
10. Горьковская Елена
11. Григорьев Иван
12. Добрылев Олег
13. Доценко Сергей
14. Исевич Александр
15. Клещева Екатерина
16. Косенко Алексей
17. Костенко Арсений
18. Лагутина Анна
19. Лукин Александр
20. Лукьянов Тимофей
21. Муслимова Альбина
22. Плешакова Дарья
23. Попова Юлия
24. Растяпина Анастасия
25. Рославцева Эвелина
26. Сазонов Дмитрий
27. Сидоров Константин

28. Чернявский Лев
29. Щепоткин Михаил

Список 11Б класса:

1. Ходырев Олег
2. Дубачева Дарья
3. Рокотянская Мария
4. Чекунов Иван
5. Хвостова Анастасия
6. Ткаченко Андрей
7. Зудилова Софья
8. Дехтярь Герман
9. Салямова Амина
10. Волков Вячеслав
11. Семенов Андрей
12. Плотников Матвей
13. Шаренков Михаил
14. Сергеев Максим
15. Соколова Софья
16. Волчанский Анатолий
17. Баклакова Полина
18. Косогов Матвей
19. Журавлева Александра
20. Поветкина Екатерина
21. Клюкач Даниил
22. Федоров Максим

ПРИЛОЖЕНИЕ 3

"Информационная безопасность"

Урок-игра по информатике для 11 класса

Цель: повторение и контроль знаний по теме «Защита информации», развитие всесторонней личности ребят, повышение их интеллектуального уровня развития, закрепление навыков работы с программой Power Point.

Задачи:

Расширить кругозор учащихся об информационной защите, о видах вирусов, о существующих законах о защите информации;

Продолжить воспитывать у учащихся чувство дружбы, формировать умение работать в коллективе.

Формировать умение работать с дополнительной литературой, использовать средства ИКТ (при подготовке к игре);

Воспитывать у учащихся сознательное отношение к законодательству.

Оформление:

компьютер для подсчёта баллов;

запись фрагмента музыки из телеигры “Счастливый случай”;

компьютеры учащихся;

мультимедийная презентация с геймами игры;

плакаты команд;

Подготовка к игре.

В игре принимают участие 2 команды, в каждой команде по 7 человек. Команды должны придумать название команды, девиз, составить вопросы соперникам. Предварительно был пройден раздел «Защита информации», состоящий из уроков по темам:

«Вредоносные программы и антивирусные программы»

«Компьютерные вирусы и защита от них»

«Сетевые вирусы и защита от них»

«Троянские программы и защита от них»

«Рекламные и шпионские программы и защита от них»

«Спам и защита от него»

«Хакерские утилиты и защита от них»

«Защита информации от несанкционированного доступа».

Также были проведены практические работы по защите информации от различных видов компьютерных вирусов, настройка межсетевого экрана, настройка антивирусной программы. Данная игра проводится как урок-обобщение.

Назначаются два помощника для подготовки и проведения игры, выбирается жюри.

Продолжительность игры: 45 минут.

Ход игры

1. Организационный момент. Постановка цели и задач урока-игры.

Учитель:

Добрый день, дорогие ребята! Сегодня мы встретились здесь, чтобы провести «Урок безопасности». Как много интересного таит в себе эта тема.

Я представляю участников игры. Поприветствуем их (команды должны объявить свое название и озвучить девиз). Пожелаем, им удачи, счастливого случая. Итак, вперед к успеху!

2. Проведение игры

I гейм. Разминка “Дальше, дальше!”

За 30 секунд команды должны ответить на 5 вопросов. Каждый правильный ответ оценивается в 1 балл. Если команда ответа не знает, она говорит: «Дальше». Команды приглашаются по очереди.

Вопросы 1 команде.

Как называются вирусы, использующие для своего распространения протоколы или команды компьютерных сетей и электронной почты? *(сетевые вирусы)*

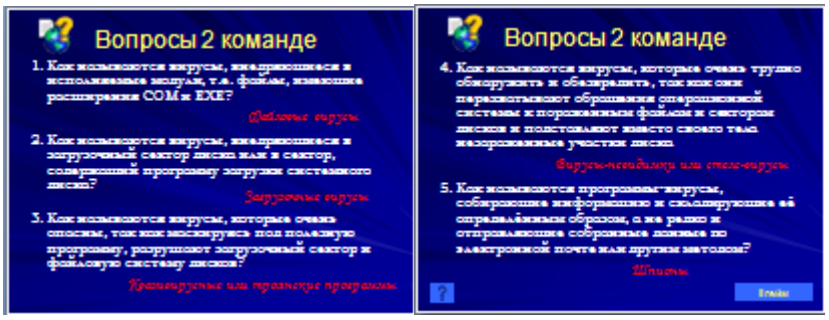
Как называются вирусы, написанные на макроязыках, заражают файлы данных? *(макровирусы)*

Как называются вирусы, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии? *(вирусы-репликаторы или черви)*

Как называются вирусы, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того вируса не имеют ни одной повторяющейся цепочки байтов? *(вирусы-мутанты)*

Как называются программы-вирусы, различными методами удаляющие и модифицирующие информацию в определённое время, либо по какому-то условию? *(логические (временные) бомбы)*

Вопросы 2 команде.



Как называются вирусы, внедряющиеся в исполняемые модули, т.е. файлы, имеющие расширения COM и EXE? *(файловые вирусы)*

Как называются вирусы, внедряющиеся в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска? *(загрузочные вирусы)*

Как называются вирусы, которые очень опасны, так как маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков? *(квазивирусные или троянские программы)*

Как называются вирусы, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска? *(вирусы-невидимки или стелс-вирусы)*

Как называются программы-вирусы, собирающие информацию и складирующие её определённым образом, а не редко и отправляющие собранные данные по электронной почте или другим методом? *(шпионы)*

Ведущий:

Слово независимому эксперту. С каким счетом закончили I гейм команды?

Независимый эксперт: - *(озвучивает результаты)*

II гейм “Заморочки из бочки”

Ведущий:

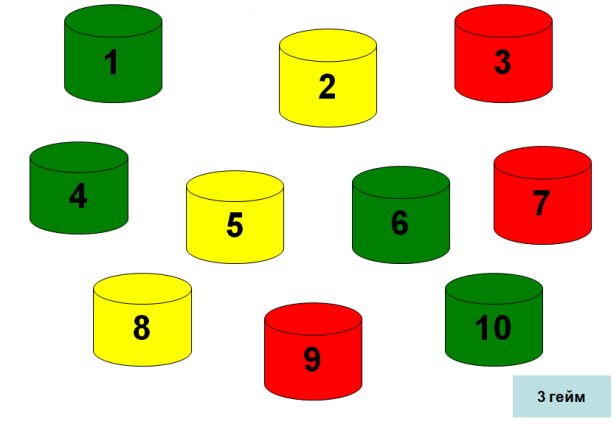
Для этого задания

Приложите все старания.

И победу тот возьмёт,

У кого счастливый лот.

Представители команд по очереди выбирают бочонки и отвечают на вопрос, который содержится в нем. На обсуждение вопроса отводится одна минута.



Если команда ответила неверно, дается возможность ответить другой команде.

В одном из бочонков видео вопрос. Это так называемый “счастливый случай”.

Вопросы в бочонках:

№ 1 (зелёный) – Найди почтовый червь: IM-Worm, IRC-Worm, Email-Worm, Net-Worm, P2P-Worm. *(Email-Worm)*

№ 2 (жёлтый) – Первый компьютерный вирус? Игра Дарвин, Creeper, Reaper, EP – Win 5.10c. *(Игра Дарвин)*

№ 3 (красный) – Что не относится к файловым вирусам? Link-вирусы, Parasitic-вирусы, Файловые черви, LAN-черви. *(LAN-черви)*

№ 4 (зелёный) – Какие черви для файлообменных сетей: IM-Worm, IRC-Worm, Email-Worm, Net-Worm, P2P-Worm. *(P2P-Worm)*

№ 5 (жёлтый) - Кто создатель программы игра Дарвин? В.А.Высотский, Г.Д.Макилрой, Роберт Морис, Алан Соломон. *(Роберт Морис)*

№ 6 (зелёный) - Черви в IRC-каналах? IM-Worm, IRC-Worm, Email-Worm, Net-Worm, P2P-Worm. *(IRC-Worm)*

№ 7 (красный) – *видеовопрос*

№ 8 (жёлтый) – Первый вирус для Windows, заражающий исполняемые файлы назывался: Win.Vir_1_4, «Homer», EP – Win 5.10c. *(Win.Vir_1_4)*

№ 9 (красный) – Что не относится к троянским программам? Утилиты несанкционированного удаленного управления; Overwriting-вирусы; Дропперы; Эммуляторы DDOS-атак. *(Overwriting-вирусы)*

№ 10 (зелёный) – Черви, использующие интернет-пейджеры? IM-Worm, IRC-Worm, Email-Worm, Net-Worm, P2P-Worm. *(IM-Worm)*

Ведущий:

Слово независимому эксперту: С каким счетом закончили 2 гейм команды?

Независимый эксперт: - *(озвучивает результаты II гейма и общего счета)*

Звучит музыка “ Счастливого случая”

III гейм “Темная лошадка”

Ведущий:

Этот гейм самый интересный, таинственный. Наша жизнь устроена так, что все тайное когда-нибудь становится явным. Мы говорим о «темной лошадке».

В гости к нам пришёл

Человек из прошлого.

Угадайте, кто же он?

Ведущий:

Перед вами сейчас будет представлена фотография “темной лошадки” - известного человека. Но эта фотография будет закрыта. Чтобы открыть фотографию необходимо будет угадать, кто на ней изображен. Сделать это можно будет с помощью подсказок, но с каждой подсказкой количество баллов уменьшается. Максимальное количество балов – 4. Чья команда быстрее поднимет руку, та и отвечает.

“Темная лошадка” *(Евгений Касперский)*

Подсказки:

Родился 4 октября 1965 г. в Новороссийске. Окончил Институт криптографии, связи и информатики и до 1991 г. работал в многопрофильном научно-исследовательском институте.

Начал изучение феномена компьютерных вирусов в октябре 1989 г., когда на его компьютере был обнаружен вирус "Cascade".

С 1991 по 1997 гг. работал в НТЦ "КАМИ", где вместе с группой единомышленников развивал антивирусный проект "AVP".

В 1997г. Евгений стал одним из основателей "Лаборатории Касперского".

Ведущий:

С каким счетом закончили 3 гейм команды?

Независимый эксперт: - *(озвучивает результаты III гейма и общего счета)*

Звучит музыка " Счастливого случая"

IV гейм "Ты – мне, я – тебе".

Ведущий:

Команды задают по 3 вопроса соперникам (поочередно). Вопросы готовились заранее. Кому адресовать вопрос выбирает сам участник. Кто ответил, тот и задает вопрос. За каждый правильный ответ - 1 балл. Отвечающему можно рассуждать вслух.

Начинает команда, у которой меньшее количество баллов.

Ведущий:

С каким счетом закончили 4 гейм команды?

Независимый эксперт: - *(озвучивает результаты IV гейма и общего счета)*

Звучит музыка " Счастливого случая"

Гейм V "Гонка за лидером"

Ведущий:

Итак, последний гейм! Кто же будет победителем?

5 гейм "Гонка за лидером" посвящен свободной тематике по предметам

Ведущий зачитывает вопросы, участники команд отвечают. Кто первый ответит, тот и получает балл, вопросы задаются быстро.

Вопросы гейма "Гонка за лидером":

1. По среде обитания вирусы классифицируют на:

1) резидентные, нерезидентные;

2) не опасные, опасные, очень опасные;

3) сетевые, файловые, загрузочные, макровирусы;

4) паразиты, репликаторы, невидимки, мутанты, троянские.

2. Герундий – это:

1) резидентный вирус;

2) нерезидентный вирус;

3) неличная форма глагола;

4) третья форма глагола.

3. Наиболее опасные свойства компьютерного вируса — способность к:

1) удалению данных и модификации себя;

2) модификации себя и форматированию винчестера;

3) форматированию винчестера и внедрению в файлы;

4) внедрению в файлы и саморазмножению.

4. По особенностям алгоритма вирусы можно классифицировать на:

1) резидентные и нерезидентные;

2) не опасные, опасные, очень опасные;

3) сетевые, файловые, загрузочные, макровирусы;

4) паразиты, репликаторы, невидимки, мутанты, троянские.

5. Термин «информатизация общества» обозначает:

1) целенаправленное и эффективное использование информации во всех областях человеческой деятельности на основе современных информационных и коммуникационных технологий;

2) увеличение избыточной информации, циркулирующей в обществе;

3) увеличение роли средств массовой информации;

4) введение изучения информатики во все учебные заведения страны;

5) организацию свободного доступа каждого человека к информационным ресурсам человеческой цивилизации.

6. Развитый рынок информационных продуктов и услуг, изменения в структуре экономики, массовое использование информационных и коммуникационных технологий являются признаками:

1) информационной культуры;

2) высшей степени развития цивилизации;

3) информационного кризиса;

4) информационного общества;

5) информационной зависимости.

7. Компьютерные вирусы - это:

1) вредоносные программы, которые возникают в связи со сбоями в аппаратных средствах компьютера;

2) программы, которые пишутся хакерами специально для нанесения ущерба пользователям ПК;

3) программы, являющиеся следствием ошибок в операционной системе;

4) пункты а) и в);

5) вирусы, сходные по природе с биологическими вирусами.

8. Какой законодательный акт регламентирует отношения в области защиты авторских и имущественных прав в области информатизации?

1) Доктрина информационной безопасности РК;

2) Закон «О правовой охране программ для ЭВМ и баз данных»;

3) раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РК;

4) Указ Президента РК;

5) Закон «Об информации, информатизации и защите информации».

9. Для написания самостоятельной работы вы скопировали из Интернета полный текст нормативно-правового акта. Нарушили ли вы при этом авторское право?

1) Да, нарушено авторское право владельца сайта;

2) нет, так как нормативно-правовые акты не являются объектом авторского права;

3) нет, если есть разрешение владельца сайта;

4) да, нарушено авторское право автора документа;

5) нет, если истек срок действия авторского права.

10. Можно ли разместить на своем сайте в Интернете опубликованную в печати статью какого-нибудь автора?

1) Можно, с указанием имени автора и источника заимствования;

2) можно, с разрешения и автора статьи и издателя;

3) можно, но исключительно с ведома автора и с выплатой ему авторского вознаграждения;

4) можно, поскольку опубликованные статьи не охраняются авторским правом;

5) можно, с разрешения издателя, выпустившего в свет данную статью, или автора статьи.

Учитель:

Сегодня мы с вами вспомнили многое об информационной безопасности, о вирусах. Кто-то узнал что-то новое для себя. Говорить о защите информации можно бесконечно. У нас еще будут “Счастливые случаи”, когда мы сможем поделиться знаниями о новых вирусах и способах защиты от них.

Игра закончена. До новых встреч!!!

Звучит музыка “ Счастливого случая”