МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОЕКТИРОВАНИЕ БЕЗОПАСНОЙ ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ В СРЕДНЕЙ ШКОЛЕ

Выпускная квалификационная работа по направлению
44.04.01 Педагогическое образование
Направленность программы магистратуры
«Образовательный менеджмент»
Форма обучения заочная

Проверка на объем заимствований:
74,92 % авторского текста
Работа допущена к защите
«10» февраля 2021 г.
зав. кафедрой педагогики и
психологии д.п.н., доцент
_____Гнатышина Е.В.

Выполнил(а):
Магистрант группы № ЗФ-318-158-2-1
Климов Евгений Викторович
Научный руководитель:
д.п.н., доцент, зав. кафедрой педагогики и психологии ФГБОУ ВО ЮУрГГПУ

Челябинск
2021

Оглавление

ВВЕДЕНИЕ

Актуальность исследования обусловлена кардинальными переменами в социальной, политической и экономической жизни общества под влиянием всемирной глобальной цифровизации. В современном мире происходит так называемый процесс перехода общества к более новому состоянию, которое ученые назвали как информационное или цифровое общество.

Когда сто лет назад в 1920 году Карел Чапек впервые употребил слово «робот» что означало «искусственный рабочий» в его научно-фантастической драме «R.U.R» (полное название «Россумские Универсальные Роботы»), он, вероятно, не догадывался, что десятилетиями тема робототехники и автоматизации будет настолько актуальной и распространенной, что затронет повседневную жизнь всех людей на Земле.

Мы живем в современном XXI веке, и первоначальная идея робототехники, и автоматизации, в попытках помощи людям от тяжелой и напряженной работы, все еще продолжается. Развитие в данном направлении не останавливается ни на секунду и с каждым днем мы видим, как появляются новые проекты развития данных направлений. Но с развитием новых технологий появилась и обратная сторона медали с негативными эффектами.

С развитием информационных и коммуникационных технологий скорость передачи и объем передаваемых данных увеличился в несколько тысяч раз и продолжает расти в геометрической прогрессии. В то же время благодаря массовому производству и дешевизне новых современных гаджетов их теперь может позволить приобрести себе практически каждый взрослый человек. Также данные современные устройства легкодоступны и современным детям. Сейчас ребенок в возрасте 5 лет не может толком завязать шнурки, но уже свободно и спокойно владеет современными электронными гаджетами, подключенными к сети Интернет.

При не правильном использовании ресурсов сети интернет как детьми, так и взрослыми может легко произойти утечка личной информации в сторону

злоумышленников. Поэтому повышенная осведомленность о безопасности – есть эффективная защита от неправомерного использования информации.

В нашем современном мире развитие систем информационной безопасности в образовательных организациях должно стоять на высоком уровне.

Современная система информационной безопасности школы – это в первую очередь совокупность различных управленческих решений, использование программных и аппаратных разработок, а также методические рекомендации для защиты информации внутри образовательной организации.

В наше развитое время отсутствие таких систем, разработок и решений может привести к потере важной годами наработанной информации вплоть до удаления ее с компьютера, а также к потере персональных данных, которыми могут воспользоваться третьи лица для собственной выгоды. Поэтому сейчас мы как никогда должны уделять этому особое внимание.

В современной отечественной и зарубежной литературе в наше время большое внимание уделяется различным проблемам информационной безопасности во всем мире.

В работах: В. Д. Попова, М. С. Вершинина, К. В. Ветрова, А. И. Ракитова, С. Э. Зуева более подробно раскрыты проблемы исследования в сфере информационного пространства.

Значительный вклад в сфере информационной безопасности внесли и другие ученые и исследователи. Это А. В. Возженников, А. Б. Агапов, А. С. Алексеев, И. Л. Бачило, Н. В. Данилов, Ю. М. Горский, И. С. Даниленко, С. А. Дятлов, Г. Г. Феоктистов, А. М. Яновский и другие. В их работах указаны взаимосвязи различных категорий информационной безопасности, а также разные приемы исследований в этой сфере.

В наше время системы хранения, обработки и передачи информации в различных организациях являются почти жизненно важными, особенно когда мы говорим о государственных организациях (администрации, школы, больницы и т.д.). Где должна соблюдаться политика конфиденциальности,

целостности, доступности.

Сейчас мы не должны смотреть на проблему информационной безопасности в одностороннем порядке. Нужно всегда действовать на опережение тем действиям третьих лиц, которые могут привести к различным ненужным потерям в сфере утечки информации как внутри, так и с наружи организации.

Для этого необходимо на уровне руководящего состава более серьезно подходить к данной проблематике в сфере защиты информации. Соответственно должно быть осознание о выделении значительных ресурсов и соблюдения определенного режима.

Таким образом, потребность в создании системы эффективной защиты от различных новейших угроз и атак в сфере информационной безопасности, а также разработка методик обеспечения информационной безопасности в образовательной организации определили объект, предмет, цель и основные задачи исследования.

Цель исследования: на основе теоретического анализа разработать модель безопасной цифровой среды школы в области обеспечения информационной безопасности учащихся.

Объектом исследования является система информационной безопасности общеобразовательной организации.

Предмет исследования: особенность обеспечения безопасной цифровой среды учащихся в условиях образовательной организации.

Гипотеза исследования: безопасная цифровая образовательная среда обеспечивается реализацией модели, состоящей из следующих 4-х компонентов:

1. организационно-управленческий компонент;
2. методический компонент;
3. образовательный компонент;
4. технологический компонент.

Задачи исследования:

– Анализ и выявление основных угроз и рисков информационной безопасности в современной школе;

– Рассмотреть понятия и социально-педагогический аспект безопасной цифровой среды образовательной организации;

– Разработать модель управления безопасной цифровой образовательной среды современной школы

– Внедрить модель безопасной цифровой образовательной среды в образовательную организацию.

Для реализации поставленной цели используются следующие **методы исследования:**

теоретические – изучение и анализ литературы и научных статей в области информационной безопасности образовательных организаций;

эмпирические – анализ средств и методов по информационной безопасности образовательных организаций, которые отражены в работах современных ученых и педагогов.

Теоретическая база исследования – это работы и исследования в области информационной безопасности образовательных учреждений, следующих ученых А. В. Возженников, А. Б. Агапов, А. С. Алексеев, И. Л. Бачило, Н. В. Данилов, Л. П. Владимировой, Т. А. Малых, Е. С. Полат, Н. И. Саттаровой и др.

Теоретическая значимость в обобщении материала по вопросам создания безопасной цифровой среды образовательной организации.

Практическая значимость: представлены модель и программа по развитию безопасной цифровой образовательной среды, которые могут применяться на в практике работы образовательных организаций.

База исследования: МОУ Архангельская СОШ.

Структура исследования: работа состоит из введения, теоретической и практической глав, заключения, списка использованных источников, приложений.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЩЕОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1 Анализ и выявление основных угроз и рисков информационной безопасности в современной школе

Информационно-коммуникационные технологии (ИКТ) занимают ведущие места в наше время. Умение работы с современными гаджетами и компьютерами, умение применять современные технологии в работе, умение использовать различные информационные ресурсы, дают современному человеку использовать так называемый современный (новый) стиль работы. На данный момент становится понятным, что в образовательных организациях практически все сотрудники должны внедрять информационные технологии в свою профессиональную деятельность [6].

Развитие образовательной организации в сфере цифровизации сейчас зависит во многом от политики администрации в данном направлении. А также от внедрения различных информационных технологий в процесс обучения и развития самой школы. Причем большую роль в этом выделяют не только сотрудникам школ, но и детям с родителями. Т.к. они тоже являются участниками образовательного процесса и жизни школы.

Цифровизация современного мира помимо положительной стороны имеет и обратную сторону медали. Так современный человек, не зависимо от возраста, без труда имея свободный доступ к любой информации в сети Интернет, мало защищен от ее негативного воздействия. Большинство детей не владеют культурой поведения в сети Интернет. Поэтому в первую очередь требуется сделать анализ факторов риска и угроз на ребенка в современной школе при работе на компьютере. Нужно выяснить влияют ли современные разработки обучения детей информационной безопасности к пониманию что делать можно, а что категорически не стоит делать. Или как вести себя в той

или иной ситуации при возникновении проблемы в информационном пространстве.

Современные проблемы безопасности детей в цифровом мире постоянно изменяются и становятся все более совершенными. С каждым разом происходит так называемый рывок в развитии и появлении источников угроз и опасности (нежелательные информационные ресурсы Интернет, жестокие компьютерные игры, некачественное программное обеспечение, ресурсы порнографического содержания, незакономерные действия мошенников в сети Интернет, люди, которые пытаются подействовать на психику ребенка давлением или унижением, либо призывая его (ребенка) на какие-то противоправные, а иногда и суицидные действия и т.д.) [10].

Тем не менее в наше время развиваются системы и методы безопасности информационного пространства. На уровне государства создаются новые законы по обеспечению безопасности в цифровом пространстве, по привлечению лиц осуществляющие противоправные действия к административным и уголовным наказаниям. Коммерческие организации создают и совершенствуют созданное ранее программное обеспечение для предотвращения угроз со стороны всемирной сети Интернет и хакеров. Интернет-провайдеры блокируют нежелательные интернет ресурсы, создают фильтры с так называемым детским интернетом где блокируется определенный контент. В образовательных организациях сейчас используются данные фильтры. Так же в школах разрабатываются нормативы и режимы по работе с и использованием информационных технологий.

Более распространенные факторы риска, которые влияют на психическое, нравственное, физическое здоровье ребенка – это в первую очередь компьютерные игры и социальные сети. На данный момент к этим ресурсам дети имеют свободный доступ без каких-либо ограничений. И если на школьном уровне происходит так называемая фильтрация ресурсов, которыми ребенок может пользоваться, то имея собственный гаджет (смартфон, планшет, ноутбук) с доступом в сеть Интернет он

беспрепятственно может пользоваться ресурсами с нежелательным для детей контентом.

Негативные влияния социальных сетей и компьютерных игр раскрыты в публикациях А. А. Веряева, Д. А. Журавлева, Н.И. Саттаровой, Т. Л Шишовой и других авторов. Ведь на самом деле сейчас много компьютерных и интернет игр направлены на то, чтобы убивать. Причем убивать не только каких-то монстров, но и убивать героев реальных людей, которые так же играют онлайн. В наше время это доходит до того, что дети одного класса могут играть онлайн в стрелялку друг против друга убивая своих персонажей. Причем данные игры реалистично воспроизводят кровь, отрезанные части тел человека, отстрелянную голову и тд. В играх дети могут играть за преступников и убийц совершая различные преступления хоть и виртуальные. Ребенок под влиянием компьютерных игр может чувствовать себя всемогущим и бессмертным. Игра на него влияет как наркотик, от которой он становится зависимым [3].

Общаясь в социальных сетях и современных мессенджерах, зная, что их оппонент находится где-то далеко могут оскорблять и угрожать друг другу вплоть до расправы. Сейчас даже взрослые не сдерживают своих эмоций и оскорблений при общении в социальных сетях и мессенджерах. Что говорить тогда о детях, которым современная культура поведения в информационном пространстве вообще не знакома. Дети, общаясь в социальных сетях подвержены воздействиям различных противозаконных групп и движений. Такие группы (Синий кит, АУЕ, свободу Навальному и т.п.) психологически воздействуют на ребенка толкая его к необдуманным и противозаконным действиям и поступкам, которые обычно направлены на насилие перед человеком.

Время провождения ребенка в виртуальном мире становится основным. Забывая о реальном мире, реальных делах и проблемах ребенок все больше предоставляет себя виртуальному компьютерному миру, в котором все проще

решается. Сейчас дети, находясь в одном здании школы предпочитают общаться посредством современных мессенджеров игнорируя реальное «живое» общение.

Поэтому поведение современных детей меняется в реальной жизни. Занятия спортом, реальные встречи и общения со сверстниками, учеба, участие в реальных делах, уходят на второй план. Ребенок перестает видеть реальные проблемы т.к. в виртуальном мире для него их решать более комфортно. Формируется поведение ребенка, которое направлено на стремление уйти из реальности и полностью погрузиться в виртуальный мир. Такое аддиктивное поведение пагубно влияет на психику ребенка и в дальнейшем может привести к другим формам зависимости таким, как алкоголь, наркотики и т.д. [3].

Помимо психологического воздействия у ребенка такое времяпрепровождение оказывает пагубное влияние и на физическое здоровье ребенка. Появляются проблемы со зрением, проблемы с позвоночником. У более эмоциональных детей может расти артериальное давление. Низкая двигательная активность приводит к плохому физическому развитию детей.

Причинами такого негативного воздействия на ребенка являются бесконтрольность доступа к современным цифровым ресурсам, непонимание информационной культуры поведения в сети, полное отсутствие помощи со стороны старшего поколения (родители, старшие братья и сестры и т.д.) и учителей.

Современная цифровая среда общества приводит к современным угрозам и проблемам в образовательной организации в сфере информационной безопасности. Сейчас требуется усовершенствовать сферу преподавания с учетом вопросов информационной безопасности школьников. Соблюдения политики правил и норм использования личных данных всех участников образовательного процесса. Поэтому в наше время цифровизации со стороны педагогике тоже проходят исследования соблюдения условий

информационной безопасности школьника.

Для учителей, школьников и их родителей сейчас существуют множество различных интернет ресурсов, а также разрабатываются и реализуются рекомендации для профилактики и предупреждению негативного воздействия на детей со стороны виртуального мира как в стенах школы, так и за пределами.

Все чаще на просторах интернета стали появляться ресурсы регулируемые на уровне государства, содержащие уроки информационной безопасности и культуры поведения ребенка в сети Интернет основанные в более понятной для детей – игровой форме. Стали проводится Единые уроки по информационной безопасности во всех школах страны.

В школьных программах по информатике тоже существуют некоторые основы по проблемам безопасности при работе за компьютером:

– техника безопасности работы за компьютером;

– правовая форма охраны информации с использованием личных данных;

– защита информации от действий третьих лиц, способность отличать ложь от истины;

– безопасность в сети Интернет;

– свобода слова и цензура в информационном пространстве;

– антивирусная защита от угроз из вне;

– искусственный интеллект;

– зависимость человечества от современных гаджетов;

– использование лицензионного программного обеспечения;

– соблюдение законодательных норм поведения в информационном пространстве.

Такие виды методических материалов раскрывают суть проблемы безопасности цифровой среды, информационных ресурсов, безопасность и защиту интересов и прав людей [3].

Цифровая информационная среда образовательного учреждения – это

целая система, где задействованы и на информационном уровне связаны все участники образовательного процесса. Это и администрация школы, педагоги и обслуживающий персонал, школьник и его родители.

Полный анализ источников проблемы цифровой образовательной среды информационного пространства позволил выделить следующее:

– при формировании цифровой образовательной среды средней школы необходимо внедрять новые информационные технологии в существующие образовательные программы по нормам государственных стандартов. Строить учебный процесс по схеме преподаватель-ученик-цифровая образовательная среда;

– цифровая образовательная среда имеет сложную педагогическую структуру, которая включает информационные, организационные, технические средства и ресурсы;

– при непосредственном создании цифровой образовательной среды в образовательной организации большое значение имеет компетентность педагогов в сфере информационных технологий, которые могут быть применимы как для обучения детей, так и для собственного развития в данном направлении [6].

Для реализации задач по построению цифровой образовательной среды образовательные организации стараются приобретать готовые программные продукты либо использовать бесплатные государственные ресурсы, которые уже имеют в своей структуре целый комплекс информационных систем («Кирилл и Мефодий – школа», «Сетевой город. Образование», «1С: Образование», «Федеральный центр информационно-образовательных ресурсов» и др.) [14].

Например, современный онлайн ресурс «Сетевой город. Образование», который используют практически все школы Челябинской области, в последние годы стал популярным среди администрации школ, педагогов и учеников. Данный онлайн ресурс выводит систему образования на более

современный уровень в сфере информационных технологий. Этот ресурс позволяет успешно применять информационные технологии в образовательном процессе не только учителям, но и школьникам и их родителям.

Такое внедрение данного сетевого ресурса в образовательный процесс позволяет решить ряд следующих проблем:

– хранение личных дел учащихся и учителей в электронном виде. Создается общая база данных с распределением ролей участников данного ресурса;

– обеспечение коммуникаций между всеми участниками образовательного процесса (администрация, учитель, школьник, родитель);

– наличие встроенных цифровых образовательных ресурсов в режиме онлайн доступа (рабочие тетради по предметам, готовые интерактивные уроки и курсы, автоматические проверки самостоятельных работ и тестов);

– индивидуальная доступность и открытость результатов учебного процесса для учеников и их родителей. Общая успеваемость класса;

– мониторинг качества образования (формирование различных отчетов по результатам обучения);

– автоматизация практически всех процессов управления учебным пространством школы (распределение нагрузки учителей, создание расписание, занятость кабинетов, составление учебных программ и планов и др.);

– использование онлайн ресурсов, формирующей школьное информационное пространство;

– наличие качественной и достоверной информации (обеспечивается защита школьников от доступа к вредной информации или информации сомнительного содержания).

Современные ресурсы сети Интернет для образования требуют их

постоянного развития и не должны ограничиваться только стенами школы. У детей всегда должна быть возможность обучения на дому, например, в период карантина или непогоды. А педагог иметь возможность подготовиться к предстоящим занятиям. В связи с этим при использовании онлайн ресурсов и информационных технологий в учебном процессе, педагогами должны быть оценены и сокращены до минимума риски и угрозы при их использовании.

1.2 Основные понятия и социально-педагогический аспект безопасной цифровой среды в образовательной организации.

Информационная безопасность в образовательной организации – это понятие, которое включает в себя правовые, технические и этические аспекты.

Понятия «информационной безопасности» из различных источников представлены в Таблице 1.

Таблица 1 – Понятия информационной безопасности

Автор	Определение понятия
Доктрина информационной безопасности Российской Федерации	Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.
Федеральный Закон Об участии в международном информационном обмене	Информационная безопасность - состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства
Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию"	Информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.
А.И. Алексенцев	Информационная безопасность - состояние информационной» среды, обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений, безопасность информации и защиту субъектов от негативного информационного воздействия.

Продолжение таблицы 1

О.В. Азамов, К. Ю. Будылин, Е. Г. Бунев, С. А. Сакун, Д. Н. Шакин.	Достижение такого состояния развития общественных отношений, при котором обеспечена надежная и всесторонняя защита интересов субъектов этих отношений - человека, общества и государства - от угроз деструктивного информационного воздействия (информационных опасностей).
М. А. Стюгин.	Условия информационного превосходства свободной информационной системы (субъекта безопасности) в конфликте, позволяющие ему определить целевой режим функционирования, адекватный поставленный цели и реализовать его путем модификации состояния подсистем.
В.Ю.Статьев, В.А. Тиньков.	Защита информации и поддерживающей ее инфраструктуры с помощью совокупности программных, аппаратно-программных средств и методов с целью недопущения причинения вреда владельцам этой информации или поддерживающей его инфраструктуре.
А.В. Макеев, В. П. Петров.	Под "информационной безопасностью" следует понимать устойчивое состояние информационной сферы, сохраняющей, несмотря на неблагоприятные внешние и внутренние воздействия, свою целостность и способность к саморазвитию на основе осознания субъектами информационного взаимодействия своих ценностей, потребностей (жизненно важных интересов) и целей развития.
Г.А. Атаманов.	Информационная безопасность есть такое состояние объекта, при котором состояние информационной среды, в которой он находится, позволяет ему сохранять способность и возможность принимать и реализовывать решения сообразно своим целям, направленным на прогрессивное развитие.

Приведенные в таблице определения «информационной безопасности» постоянно подвергаются спорам, критике со стороны специалистов разных областей и со стороны ученых [11, с. 37; 15; с. 12;].

Как мы видим каждый автор по-своему видит и трактует значение понятия «Информационная безопасность». Происходит так называемая коллизия в понимание данного термина. Часто понятие этого термина берутся из разных источников, которые не согласуются между собой.

Часто под понятием информационной безопасности понимают область

в сфере защиты информации (целостность, правдивость, конфиденциальность). Если взять нормативно-правовые документы, например, Доктрина информационной безопасности РФ, то здесь понятие информационной безопасности рассматривается значительно шире:

– «безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз» [41];

– «информационная безопасность РФ — состояние защищенности ее национальных интересов в информационной сфере, определяющейся совокупностью сбалансированных интересов личности, общества и государства» [42].

Очевидно, что термин информационная безопасность и безопасность информации взаимосвязаны между собой. Но мы должны понимать, что безопасность не может существовать сама по себе, без определенного объекта к которому мы должны относить данное понятие. Без объекта понятие «безопасность» теряет свой смысл. В связи с этим если мы понятие безопасности относим непосредственно к какой-то информации тогда мы можем утверждать, что эти два понятия взаимосвязаны. И совсем другое, если мы термин «информационная» относим к какому-либо объекту защиты в информационном пространстве, то понятие информационной безопасности указывает на определенную деятельность и это понятие можно трактовать как защиту объекта от угроз со стороны информационного пространства.

В наше время учителя встают на одну ступень с работниками IT индустрии. Хорошо ориентируются цифровом пространстве на уровне учителей информатики. Помимо информатики цифровизация интегрируется и в другие школьные предметы. В наше время современный школьник больше информации получает уже не с помощью учебников, а средствами информационных и визуальных технологий как в кабинете, так и во всемирной сети Интернет. Также развивается самостоятельная работа школьника в сфере проектного исследования. Где школьник самостоятельно осуществляет поиск,

обработку и правильное структурирование данной информации [6].

Реализация национального проекта подключения всех образовательных организаций к высокоскоростному интернету без ограничений, позволяет педагогам и ученикам получить доступ ко всем современным ресурсам интернет пространства, включая электронные библиотеки, виртуальные музеи и галереи, учебные и мультимедиа ресурсы и многое другое. Создаются комплексные образовательные онлайн ресурсы, позволяющие детям проходить различные дополнительные курсы, не связанные со школьными уроками. Заниматься саморазвитием в интересующем направлении. Существуют интернет порталы и форумы по определенным направлениям и интересам, где школьник может получить консультацию на интересующий его вопрос [1].

Современные школы в наше время оснащены компьютерной техникой. Сейчас практически в каждом кабинете есть комплексная интерактивная система, состоящая из компьютера, проектора и интерактивной доски для наглядного и интересного проведения различных уроков. Разрабатываются различные национальные проекты нашего государства, направленные на цифровизацию образовательной среды в школах, а также ее безопасного использования в образовательном пространстве.

Глобальная цифровизация информационного пространства современной жизни нашего общества создала новые проблемы для развития личности. Сейчас благодаря развитию технических средств и сети Интернет информация по всему миру распространяется очень быстро, затрагивая все социальное пространство. Очень часто сама информация несет негативный и агрессивный характер влияя на социально-нравственные ориентиры общества. Деформация и деструктивные изменения духовной сферы общества в форме искаженных нравственных норм и критериев, неадекватных социальных стереотипов и установок, ложных ориентаций и ценностей, влияют на состояние и процессы во всех основных сферах общественной жизни. Поэтому в современном обществе возникает проблема информационной безопасности, без решения

которой не представляется возможным полноценное развитие не только личности, но и общества. Ребенок в наше время, который только познает этот мир оказывается незащищенным от больших потоков информации [4].

На просторах глобальной сети много жестокой пропаганды в отношении общества, которая легко доступна и для детского не окрепшего мозга. Эта проблема напрямую касается и образовательного пространства в школах. Так качество и уровень образованности подрастающего поколения, а также готовность к самореализации в обществе напрямую зависит и от роли учителя в этой подготовке. Поэтому сейчас и стоит необходимость введения новых компонентов в систему образования, которые позволяют обучить школьника информационной безопасности и культуре поведения в информационном пространстве. В наше время проблема безопасной цифровой образовательной среды для школьника и других участников данного процесса становится все более актуальной и требующей повышенного внимания.

Учителю информатики в решении данной задачи отводится особо важная роль. На сегодня в образовательной организации учитель информатики должен уметь не только владеть методикой преподавания уроков информатики, а еще владеть в совершенстве различными методами и системами в сфере информационной безопасности, иметь высокий уровень знаний о проблемах информационной безопасности школьников. Постоянно само развиваться в этих направлениях. Также требуется прямое содействие и полное понимание руководителя образовательной организации проблемы данной сферы безопасности.

Примерные требования к учителю:

– знание о негативных формах и способах воздействия на человека со стороны информационного пространства;

– знание о различных методах защиты;

– правила и нормы поведения в сетевом пространстве (правила сетевого этикета);

– знания методов по предупреждению и устранению проблемных или конфликтных ситуаций у школьников в информационном пространстве сети Интернет.

Первым этапом разрешения проблемы в сфере информационной безопасности встает обучение школьника адекватному восприятию и адекватной оценке полученной информации, ее осмыслению на основе нравственных и культурных ценностей. Педагогам, ученикам и их родителям нужно знать, что в цифровом пространстве всемирной паутины тоже существуют свои правила и законы, которые требуется соблюдать. Все чаще сейчас школьники показывают свое асоциальное поведение не зная, что в сети тоже есть свои правила и нормы поведения, этикет общения, которые необходимо соблюдать и сдерживать свои эмоции. Не зная реальных уголовно-наказуемых законов, дети часто совершают правонарушения с помощью Интернет пространства [3].

Ребенок, думая, что его никогда не найдут и не накажут, совершает противозаконные поступки, на которые в реальной жизни не способен. Причем совершая их, он не задумывается что его действия могут нанести реальный физический, моральный и экономический вред реальному человеку.

Поэтому преподаватель должен уделять особое внимание воспитательной работе с учениками в сфере информационной безопасности интернет пространства. Сейчас на уроках информатики раскрываются общие вопросы компьютерной безопасности, но к сожалению, не дадут ответа на вопрос как обеспечить личную безопасность в интернет пространстве.

Для рассмотрения в социально-педагогическом аспекте угрозы информационной безопасности как совокупности условий и факторов, воздействующих на здоровье личности, духовно-нравственную сферу, межличностные отношения, создающих опасность жизненно важным интересам личности, были использованы основные положения Доктрины информационной безопасности РФ. Информация представляет угрозу при

определенных условиях. Целью создания таких условий является манипуляция сознанием и психикой личности, в частности, личности ребенка.

В качестве классических средств воздействия на личность в информационном пространстве выделяют следующее:

– средства массовой информации (в том числе: использование глобальной сети Интернет, интернет-мессенджеры, мультимедиа приложения для смартфонов); литература различной направленности;

– современное искусство;

– образование (дошкольное, среднее и средне-специальное, высшее, система альтернативного образования и т.п.);

– воспитание (все разнообразные формы воспитания в системе образования, общественных организаций — формальных и неформальных, система организации социальной работы и т.п.);

– межличностное общение.

Любое из этих средств может быть использовано на благо или во вред личности. [10]

В условиях современной школы обеспечение информационной безопасности может быть рассмотрено как совокупность деятельности по недопущению вреда сознанию и психике ребёнка [7].

При этом же сам процесс обеспечения информационной безопасности ребенка основывается на умениях личности видеть и за ранее нейтрализовать эту угрозу со стороны информационного сообщества. Данное умение может приобретаться ребенком самостоятельно, либо в процессе обучения педагогом. В связи с этим перед нами стоит острая необходимость поиска путей решения проблемы информационной безопасности школьника [7].

Анализ изученной литературы и интернет ресурсов дает основание полагать, что процесс обучения информационной безопасности целесообразно начинать с начальных классов. В связи с этим необходимо рассматривать информационную безопасность ребенка, как социальную проблему, решение

которой есть педагогически направляемый процесс развития у ребенка знаний об интернет угрозе. Таким образом у ребенка должно вырабатываться умение противостоять такой угрозе для минимизации различных последствий.

Для решения таких проблем главную роль отводят педагогам, которые могут обучить детей информационной безопасности. Только педагог сможет научить ребенка выделять нужную информацию, блокируя некачественную. Подготовит ребенка к умению противостоять негативным информационным воздействиям. Поможет сформировать информационно-грамотную, личность которая в последствии будет помогать другим в противостоянии некорректного информационного фона сетевых ресурсов.

Когда мы говорим о интернет зависимости детей, то имеем ввиду влияние виртуального мира на сознание, ребенка которое несет на себе ряд проблем, связанных с психическим и физическим воздействием на здоровье ребенка. У ребенка появляются трудности в учебе (много лишней информации, снижение успеваемости, выделение малого количества времени), возникают этические проблемы (снижение интереса к чтению, искусству, перенос образа поведения из виртуального мира в реальный и т.д.) [12].

Опираясь на многочисленные труды исследователей проблемы в данной области (например, Л.Ф. Обуховой) можно утверждать, что определяющей для учащихся, особенно для младшего и среднего школьного возраста становится система взаимодействия «ученик – учитель», влияющая на отношения ребенка к родителям, к одноклассникам и самому себе. Для ученика в этом возрасте еще высок авторитет педагога, ребенок доверяет учителю и открыто может общаться с педагогом, доверяет информации, которую дает учитель. В ходе работы учителем в школе данные утверждения подкрепляются наблюдениями и работой с учащимися [12].

Основная деятельность школьника – это учебная деятельность, развитие умений в сфере информационной безопасности важно организовать в его процесс обучения.

В школьные годы на начальном этапе у ребенка начинает формироваться нравственное поведение. Он начинает понимать смысл слов «злой-добрый», «хорошо-плохо», но у него отсутствует субъективный взгляд на систему нравственных норм и ценностей. (В. Д. Ермоленко-Сайко)

Система нравственных норм и ценностей становится оценочным регулятором жизни и деятельности учащегося и реализуется в том случае, если эти правила и нормы поведения приняты и осмыслены ребенком. Следовательно, целесообразно формировать информационную безопасность, используя категории нравственных ценностей и норм, активизировать собственные внутренние силы ребенка по самоусовершенствованию.

Развивать школьника в сфере безопасности в информационном пространстве нельзя без учета его взаимодействия с другими учащимися. Процесс взаимодействия реализуется как кооперация (Г. А. Цукерман). в этом процессе идет постоянное преобразование ребенка в плане совершенствования. Появляются возможности для его культурно-познавательной жизни в информационном пространстве. Поэтому одно из условий при обучении школьника информационной безопасности должно быть взаимодействие детей в форме кооперации [7].

В школьном возрасте дети обладают мыслительной пластичностью, поэтому ее легко можно изменить в ходе учебно-познавательной деятельности школьника и качественно повлиять на формирование знаний в сфере информационной безопасности (Г.А. Цукерман, Л.В.Занков, В.В.Давыдов, Л.С. Выготский, Ю.М. Орлов, Г.К. Селевко, В.И. Андреев и др.) [7].

Анализируя выше изложенное можно говорить о том, что решение проблемы в сфере информационной безопасности ребенка должно проводиться под контролем грамотного педагога, который может без труда учитывать все необходимые составляющие этого процесса. Педагог, который без труда сможет внедрить в существующий педагогический процесс занятия по цифровой безопасности ребенка.

Реализация безопасной цифровой среды среди школьников нуждается в

условиях непосредственного взаимодействия и взаимопонимания между учителем и учеником. Педагог должен тщательно продумать содержание занятий по информационной безопасности, для полного и глубоко осмысления учеником. Школьник должен понимать большую значимость этого содержания.

Большую роль в успехе обучения информационной безопасности играет позиция самого учителя в этой области. Она должна быть направлена на поддержку ребенка в условиях саморазвития, на правильные взгляды и позиции в социуме, предупреждение от совершения неправильных поступков, показать правильный путь к адаптации в информационном пространстве.

Педагогическая работа должна реализовывать следующие принципы саморазвития:

– взаимная открытость между педагогом и учеником;

– свободосообразность;

– социосообразность;

– принцип идеологичности;

– неприемлемость насилия и непримиримость к насилию над другим субъектом [4].

Важным условием хорошего обучения в сфере информационной безопасности является осведомленность и развитие педагога в этом направлении:

– понимание что в нашем случае объектом защиты является ребенок;

– понимание характера угроз и рисков на школьника. Откуда они могут появиться;

– понимание необходимости предотвращения от внутренних и внешних угроз, которые неблагоприятно будут воздействовать на психику, самооценку, неправильный выбор в сложившейся ситуации, неадекватное

поведение в информационном пространстве и т.д.;

– предотвращении попадания ребенка в психологическую зависимость от других участников;

– иметь представление как своевременно избежать возможного ущерба. Какие средства и методы применять для защиты;

– дать понять, что на данный момент педагог является объективным помощником ребенка в сфере его безопасности в информационном пространстве. Опережая действия общества.

Условия, способствующие эффективному формированию информационной безопасности школы:

1) Содержательные. Реализует содержательный компонент учебной программы, направленный на систему внеурочных мероприятий, где изучается умение выявлять угрозу в информационном пространстве.

2) Процессуально-технологические. Направлено на эффективное использование средств, приемов и методов обучения учитывая различные особенности развития детей.

3) Психолого-педагогические условия. Основываются на доброжелательном взаимодействии между учителем и учеником. Дополнительное условие – это организация работы с родителями по профилактике угроз и рисков, исходящих из информационного пространства [4].

Давайте рассмотрим подробно данные условия. Первое условие направлено на реализацию программы внеурочной деятельности по изучению информационной безопасности. Целью данного обучения информационной безопасности школьника является правильное понимании и толкование рисков и угроз со стороны сетевого сообщества и информационного пространства. Так же правильный выбор методов и средств защиты исходящих из сети Интернет.

Далее необходимо выделить методы проведения внеурочной работы по

обучению информационной безопасности. Первый метод самый важный, так как это начальный этап занятий, где ребенку будет интересно и понятно. Поэтому предлагается использование готового материала с использованием наглядных или мультимедийных пособий. Проведение занятия в игровой форме. Данный метод поможет учащимся правильно усвоить и воспроизвести полученную информацию [6].

Второй метод, который можно выделить – это метод проблемного изложения материала. На этом этапе учащиеся не являются участниками, а лишь наблюдают за размышлениями преподавателя. Третий метод – поисковый. На следующих этапах он становится одним из основных в обучении информационной безопасности. становится основным методом обучения на последующих этапах. Здесь преподаватель помогает ученику найти новые знаний с помощью различных средств обучения. Под руководством преподавателя дети разбирают различные проблемные ситуации, проводят анализ, делают выводы. Так как это внеурочная деятельность, то для преподавателя и учащихся открываются большие возможности по изучению информационной безопасности с помощью экскурсий, работы с электронными гаджетами, творческими проектами. Создание реальных ситуаций, предполагающих выбор из сложившейся проблемной ситуации, с дальнейшим анализом и выводами школьников. Самоанализ и самооценка учеников. Правильное отношение к критике от других участников.

Когда мы говорим о безопасной цифровой образовательной среде в школе. Мы не должны сужать круг и смотреть только на знания школьников. Важная роль в этом образовательном процессе отделена педагогам и родителям. В современном обществе педагоги и родители так же подвержены угрозам со стороны информационного пространства. Часто случается, что ребенок придерживается взглядов взрослых людей, которые его окружают. Поэтому сейчас очень важно, когда, педагоги и родители придерживаются правильных позиций по отношению к защите себя и ребенка в сетевом

пространстве. На данный момент многие педагоги и родители малокомпетентны в вопросах информационной безопасности. Поэтому на сегодня актуально проведение отдельных занятий, семинаров, вэбинаров, практических занятий по теме «информационной безопасности» для преподавателей и родителей учащихся [8, с. 38].

1.3 Описание и модель безопасной цифровой образовательной среды в современной школе.

В современной школе использование информационно-коммуникационных технологий является неотъемлемой частью всего образовательного процесса. В первую очередь это касается педагогов. Такие вспомогательные средства помогают при организации занятий. Заметное влияние оказывают на формы и методы обучения. Применение интерактивных и мультимедийных разработок делает уроки намного интересными, дети могут глубже погрузиться в изучение новых тем. По-другому посмотреть на различные физические процессы, явления. Позволяют повысить эффективность обучения [2].

Использование интерактивных технологий в обучении позволяет:

– значительно повысить активность школьников на уроке;

– проводить тестирование и проверочные работы с оперативным выводом результатов этих работ;

– экономить время на решение определенных задач;

– соблюдать принцип дидактики – наглядность. Происходит лучшее освоение учебного материала.

Стремительное развитие технологий и скоростного интернета позволяет использование интернет ресурсов для оперативного получения информации. Которая может быть так же представлена в форме презентаций, видеороликов, интерактивных разработок.

С другой стороны, стремительное развитие информационных

технологий кардинально изменило нашу жизнь и породило множество новых проблем. В том числе и проблему информационной культуры и безопасности в информационном пространстве среди подрастающего поколения.

На сегодняшний день взрослое поколение старается ограничивать по времени нахождение детей в сети Интернет. Но специалисты говорят о том, что это метод запрета может действовать до тех пор, пока это не начнет ограничивать ребенка в сфере образования и самостоятельной деятельности по обучению в определенных областях. Современные образовательные организации подключены к скоростному Интернету, школьникам сегодня задаются индивидуальные проекты, которые они реализуют самостоятельно с использованием интернет технологий. Информатика зачастую преподается уже с начальных классов с использованием практических работ, которые предполагают непосредственное участие детей в работе за компьютером, подключенным к глобальной сети Интернет. Наряду с преимуществами использования высокотехнологических продуктов существует и угроза нанесения вреда ребенку. Изучение влияния современных гаджетов и компьютера на организм и психическое состояние ребенка, является одним из главных вопросов современной цифровизации образовательных организаций [10].

Если раньше считалось, что на здоровье человека влияет так называемое излучение от компьютерной техники и периферии, то на сегодняшний день – это нервное и умственное переутомление со стороны информационного пространства и сетевого общества.

В книге Заряны и Нины Некрасовых «Как оттащить ребенка от компьютера и что с ним делать» сказано, что дети прирастают к «розетке», когда в реальном мире им становиться уже не интересно и они не могут найти себе полноценного занятия в реальности. Что не нужно бороться с компьютером и электронными гаджетами, это не укрепит взаимопонимание между родителями и детьми. Нужно просто попробовать посмотреть на все эти устройства глазами ребенка и направить его в нужное направление, пускай

даже если это будут компьютерные игры. Многие онлайн ресурсы на сегодня устроены так, чтобы через мультфильмы или игры научить ребенка полезным делам. Позволяют расширить мировоззрение ребенка в различных областях науки и творчества. Тогда виртуальный мир станет не угрозой, а помощником в семье.

Взрослые всегда должны помнить, что дети не видят угрозы и опасность исходящей от использования Интернета. В силу особенностей психологического развития детей направленной на постоянное познание всего нового появляется проблема правильного использования информационного пространства. Ребенка нельзя оставлять один на один с виртуальным миром. Это равнозначно, что мы бросаем его одного посреди большого незнакомого города. Требуется постоянный, но правильный контроль нахождения ребенка в сети Интернет. Когда ребенок понимает, что при любой сложной ситуации он может обратиться к педагогу или родителю за помощью. Иначе он может еще больше закрыться от реальности. Для того, чтобы дать ребенку правильную информацию по его безопасности в сетевом пространстве педагог и родитель в первую очередь должны сами для себя пройти обучение в данном направлении. Показав ребенку свободное владение по этой теме [10].

В связи с этим нужна продуманная модель организации безопасной цифровой среды в образовательном учреждении. А также методика обучения основным методам информационной безопасности:

– инструктаж среди педагогов и учеников по правильному доступу к образовательным ресурсам сети Интернет;

– создание методического пособия «Безопасный образовательный процесс с помощью интернет ресурсов»;

– установка программного обеспечения для фильтрации нежелательного интернет контента;

– проведение занятия для родителей по доступу детей к различным онлайн образовательным ресурсам сети Интернет;

– памятка родителям «Что нужно знать ребенку при работе с глобальной сетью Интернет».

На сегодняшний день существует множество готовых решений, программных продуктов, которые позволяют обезопасить нахождение ребенка в сети Интернет, ограничить его время просиживания за компьютером. Программы-фильтры нежелательного для детей контента позволяют обезопасить ребенка от ненужной информации.

Например, в современных операционных системах Windows уже присутствуют встроенные функции Родительского контроля, которые без труда может настроить любой пользователь. Что позволяет контролировать работу ребенка за компьютером:

– возможность ограничить время работы ребенка за компьютером;

– блокировать доступ к нежелательным интернет сайтам и другим онлайн ресурсам, в том числе и интернет мессенджерам;

– блокировать запуск определенных программ и игр, либо ограничивать по времени их использование.

Многие Интернет-провайдеры предлагают отдельную услугу, которая называется «Детский интернет». Её можно без труда подключить из личного кабинета пользователя. Она позволяет предоставлять ребенку использовать только те интернет ресурсы и онлайн игры, которые разрешены для детей (существует так называемый «белый список» интернет ресурсов на которые могут заходить дети, утвержденный Роскомнадзором) и блокируют ресурсы сомнительного содержания. У большинства компаний данная услуга совершено бесплатна.

На сегодня для школ существуют определенные требования работы детей за компьютером и в сети Интернет. Которые регулируются на законодательном уровне и проверяются прокуратурой на соблюдение этих требований. Вся серьезность этих требований подразумевает работу детей в сети Интернет только на очень узком пространстве и только на ресурсах,

связанных с образованием. Полностью запрещая использование социальных сетей. Что показало в последние годы не совершенность и неправильность этих требований по отношению к взаимодействию учитель-ученик. Когда все школы находились на дистанционном обучении как раз многие запрещенные ресурсы и помогали взаимодействию между учеником и учителем. Позволяя организовывать образовательный процесс дистанционно.

Поэтому видеть только зло от использования современной техники – это крайности, которые нужно избегать. Это всего лишь инструмент в наших руках, который позволяет нам помочь достигнуть тех или иных задач и целей.

В связи с этим возникает потребность не в полном запрете всех интернет ресурсов, в том числе и социальных сетей, а в разработке и внедрению педагогических программ и рекомендаций в образовательном процессе по правильному использованию этих онлайн ресурсов с точки зрения безопасности ребенка. Нужно подготовить ребенка адекватности работы с данными онлайн ресурсами. Научить культуре поведение в сетевом пространстве.

Основой проектирования безопасной цифровой среды школы в первую очередь выступает политика информационной безопасности [10].

В формировании и реализации политики информационной безопасности образовательного учреждения принимают непосредственное участие все заинтересованные лица образовательного процесса: директор, педагоги, ученики и их родители.

Документально политика информационной безопасности образовательного учреждения фиксируется в локально-нормативных актах и приказах школы, а также в «Типовых правилах использования сети Интернет в общеобразовательных организациях». В этих документах должны отражаться вопросы регламента и режима доступа учащихся при работе в сети Интернет не только в стенах школ, но и за ее пределами. Это необходимо для того, чтобы, когда преподаватель дает домашние самостоятельные задания с использованием глобальной сети Интернет, эти требования тоже

соблюдались, а угрозы и риски ребенку со стороны информационного пространства сводились к минимуму.

В образовательной организации для выполнения требований политики информационной безопасности должно быть ответственное лицо, компетентное в вопросах защиты детей в цифровом пространстве: заместитель директора по безопасности, заместитель директора по информационно-коммуникационным технологиям либо учитель информатики.

Соответственно политика информационной безопасности образовательного учреждения подразумевает разработку и внедрение целого пакета документов для создания условий по защите ребенка в условиях образовательного процесса:

– приказ директора «Об утверждении Плана работы по обеспечению информационной безопасности детей при использовании ресурсов сети Интернет в образовательной организации»;

– приказ директора «Об утверждении перечня локальных актов, регламентирующих деятельность образовательной организации по защите детей от распространения информации, наносящей вред их нравственному и духовному развитию при работе с Интернет-ресурсами»;

– правила использования сети Интернет в образовательной организации, утверждены приказом директора школы;

– инструкция для сотрудников школы и членов общественного Совета образовательной организации о порядке действий при осуществлении контроля за использованием учащимися сети Интернет, утверждена приказом директора школы;

– положение об общественном Совете образовательной организации по вопросам регламентации доступа к информации в сети Интернет, утверждено приказом директора школы;

– положение о политике в сфере персональных данных.

Для проведения классных часов и беседы с родителями классным руководителям разрабатываются памятки для учеников и их родителей «Что

нужно знать ребенку при работе с глобальной сетью Интернет» и «Как контролировать работу ребенка в условиях сетевого пространства с точки зрения безопасности».

Учителям предметникам выдаются методические рекомендации:

– памятка для преподавателей образовательного учреждения по обеспечению информационной безопасности учащихся;

– рекомендации по использованию правильных интернет ресурсов в образовательном процессе;

– памятка по правильному размещению информации на сайте образовательной организации с учетом размещения персональных данных как учащихся, так и сотрудников школы [10].

Сегодня на первый план мы должны вынести вопросы формирования культуры сетевого поведения и информационной грамотности всех участников педагогического процесса. Только комплексное решение, когда педагог курирует воспитание информационной культуры школьника через обучение, а родитель консультирует и организовывает детский контроль через программное обеспечение поможет воспитать правильное поведение ребенка в сети Интернет. В этом и должна стоять задача взрослого поколения – воспитание разносторонней личности, имеющей высокий нравственный и культурный уровень дающий полное понимание о собственной безопасности в современном цифровом мире.

Формирование культуры безопасного сетевого поведения и информационной грамотности процесс сложный и длительный. Но мы должны понимать всю важность этого процесса.

При разработке модели безопасной цифровой образовательной среды школы были ранее проанализированы источники различной литературы и СМИ, с целью выяснения точек зрения ученых и специалистов в сфере защиты от угроз в информационном пространстве, которые занимаются вопросами информационной безопасности в образовательных организациях, на

возможную структуру безопасной цифровой среды образовательной организации. В ходе проведенного анализа были выделены основные компоненты, являющиеся успешным формированием реализуемого проекта. В первых – это готовые программно-технические комплексы, во-вторых – это педагогическая система, основанная на компетентности преподавателей образовательного учреждения в сфере защиты детей от угроз со стороны информационного пространства.

Следовательно, при организации безопасной цифровой среды школы в модель необходимо заложить методы и элементы, которые будут отражать эти компоненты, и способствовать их дальнейшему развитию. На момент проведения исследования выяснили, что большинство преподавателей обладают базовыми знаниями в сфере информационных технологий и используют в педагогическом процессе современные информационно-коммуникационные средства с выходом в сеть Интернет. Кроме того, большая часть преподавателей и учащихся школы хоть раз сталкивались с угрозами, исходящими из сетевого пространства. В связи с этим были выделены и рассмотрены следующие положения:

– новая безопасная цифровая образовательная среда должна являться инструментом управления защиты учащихся исходящих из сетевого пространства;

– будет инструментом управленческих решений в сфере информационной безопасности учащихся в условиях школы и дома;

– гарантировать помощь и обучение преподавателей и учащихся в сфере безопасности при работе в сети Интернет.

Разработанная модель безопасной цифровой образовательной среды имеет следующие компоненты:

– организационно-управленческий;

– методический;

– образовательный

– технологический.

Все эти условия модели взаимосвязаны и не допускают изменение содержание одного не меняя другого. Что приведет к изменению всей модели в целом. На Рисунке 1 представлена схема первоначальной модели безопасной цифровой образовательной среды школы.

Рисунок 1 – Модель безопасной цифровой образовательной среды школы

Ожидаемые результаты внедрения модели:

1. Функционирование образовательной организации в сфере информационной безопасности в соответствии с моделью «безопасной цифровой образовательной среды средней школы.

2. Появление новых образовательных результатов и повышение

качества культуры поведения в сетевом пространстве.

3. Признание профессиональном сообществе, что школа является передовой в сфере защиты учащихся в информационном пространстве.

4. Непосредственное участие большинства родителей в изучении проблем безопасности детей в информационном пространстве.

Двигаясь дальше рассмотрим каждый компонент модели по отдельности.

Организационно-управленческий.

Цель: создание локально – нормативных актов в сфере информационной безопасности образовательной организации на основании законодательства Российской Федерации. Привлечение компетентных специалистов данной области. Разработка документа режима доступа учащихся в сети Интернет. Назначение ответственного лица за организацию защиты информационной безопасности. Планирования деятельности преподавателей с учетом применения онлайн ресурсов и регулирования образовательных процессов внутришкольного взаимодействия коллектива и учащихся.

Задачи:

1) создание школьного сайта для более оперативного оповещения и размещения документальной и методической информации. Размещение учебной информации по безопасности учащихся при работе в сети Интернет;

2) разработка нормативно-правовых документов, регулирующие использование компьютерной техники с выходом в интернет в условиях школы;

3) выделение дополнительных ресурсов для обеспечения безопасности сотрудников и учащихся при работе на компьютерной технике, подключенной к сети Интернет в условиях школы;

4) обеспечение эффективного управления образовательной организацией за счет прозрачности работы коллектива в области информационных технологий и персональных данных;

5) соблюдение законодательства РФ в сфере безопасности информационного образовательного пространства и персональных данных;

6) наладить систему взаимосвязи «школа – родители».

Процесс изменения деятельности и организационной культуры образовательного учреждения возможен при следующих условиях:

– идеология изменений должна быть понятна всем участникам образовательной организации и принята большинством;

– требуется создать оптимальные условия поддержки и сопровождения преподавателей и учеников в изучении основ по безопасности при работе в сетевом пространстве;

– необходимо постоянно осуществлять мониторинг и анализ на предмет новых угроз и рисков со стороны информационного пространства;

– инновационная деятельность среди участников образовательного процесса должна давать дополнительные возможности в сфере развития и саморазвития, но максимально безопасно.

Реализация организационно-управленческого компонента модели безопасной цифровой образовательной среды образовательной организации предполагает создание в школе безопасных условий работы всех участников образовательного процесса в сфере информационных технологий. В первую очередь это касается работы с использованием глобальной сети Интернет.

Методический компонент модели

В процессе современного образования с использованием информационных технологий именно преподаватель является основным фактором, поскольку преподаватель ориентирован на сохранении

существующей системы образования в условиях новизны используемых технологий. Переориентация преподавателя на новую систему образования, основанную на использование современных цифровых технологий в процессе обучения детей – большая проблема как для него самого, так и для всего общества. В связи с этим, для успешной работы в режиме использования информационных технологий в образовательном процессе важно подготовить в первую очередь учительский состав, обучая их, осуществляя всевозможную поддержку в познании новых возможностей в образовательном процессе, создавая благоприятные условия для успешной деятельности.

Цель:

Создание системы внутришкольного обучения и поддержки преподавательского коллектива по вопросам безопасности учащихся при работе с информационными технологиями. В связи с этим поставлены следующие задачи:

1) на школьном сайте для преподавателей разместить методические рекомендации по правильной работе с информационными технологиями в учебном процессе;

2) расширить возможности повышения квалификации преподавателей школы в сфере защиты от угроз при работе с сетью Интернет;

3) изучить возможности различные онлайн сервисов по обучению информационной безопасности для использования в образовательном процессе;

4) организовать обучение для педагогов в сфере защиты информации от внешнего воздействия;

5) разработать систему проведения онлайн семинаров, вэбинаров, онлайн педсоветов и онлайн взаимодействия «учитель-ученик»;

Основными содержательными компонентами обучения педагогов работе в безопасной информационной среде являются:

– понимание специфики новых образовательных результатов и роли безопасного использования информационных технологий в образовательном процессе, как важного инструмента при достижении этих результатов;

– формирование понимания современных возможностей Интернет-ресурсов и использование их в образовательном процессе;

– технологические умения, связанные с работой в цифровой среде (освоение работы с образовательными Интернет-ресурсами).

Для достижения результата, обучение должно носить деятельностный характер. Результат обучения – проект, буклет, рекомендации, выдаваемые детям.

Основные компетенции, которыми должен овладеть учитель по итогам обучения:

– понимание возможностей и ограничений использования интернет- ресурсов в педагогической практике, понимание ответственности за неправомерное использование этих ресурсов учащимися в условиях школы;

формирование «сценарного мышления» - готовности педагога соотносить возможности интернет ресурсов и педагогических задач

Образовательный компонент модели

Современная цифровая образовательная среда должна строиться на использовании различных сетевых инструментов: образовательных онлайн платформах, блогах, сервисах видео контента и др. Что может стать критерием отбора сетевых и онлайн сервисов для безопасной цифровой образовательной среды средней школы? Способность учителя изучать и внедрять возможности сетевых и онлайн сервисов с конкретными педагогическими задачами, применять так называемые «педагогические сценарии» использования безопасной образовательной среды онлайн сервисов в образовательной практике.

Цель: Внедрение и реализация педагогических практик,

ориентированных на получение современных образовательных результатов.

Задачи:

1) создать максимально возможные условия для использования в образовательном процессе школы интернет технологии: в учебный процесс, внеурочная деятельность в условиях образовательной организации, воспитательный процесс;

2) создать условия для реализации предметных, метапредметных, социальных проектов в рамках урочной, внеурочной деятельности, а также в рамках работы детских объединений классов и школы;

3) развивать саморазвитие и самообразование педагогов и учащихся образовательной организации;

4) создать или использовать максимально безопасный для учащихся интерактивный электронный онлайн контент по учебным предметам в помощь преподавателям для организации более интересного образовательного процесса;

5) создать условия для расширения зоны дистанционного и онлайн обучения в условиях безопасной цифровой образовательной среды;

6) обеспечить онлайн и дистанционное взаимодействие всех участников образовательного процесса: учащихся и их родителей (законных представителей), преподавателей школы, специалистов органов управления в сфере образования, представителей общественности;

7) организовать взаимодействие школы с другими образовательными организациями, учреждениями культуры, учреждениями дополнительного образования, учреждениями спорта;

8) обеспечить мониторинг и анализ результатов образовательного процесса в условиях цифровизации образовательной организации.

Технологический компонент модели

Реализация инновационной современной модели цифровой образовательной среды школы невозможна без современных технологических средств.

При формировании безопасной цифровой образовательной среды школы иметь следующее технологическое оснащение:

– информационный экран в главном холле образовательной организации для трансляции последней актуальной информацией и новостей школы;

– компьютерная техника (компьютер, ноутбук, планшет) с доступом к высокоскоростному интернету с установленной защитой запрещенного контента для детей. С возможностью использования онлайн образовательных ресурсов;

– кабинеты администрации образовательной организации с компьютерной техникой, на которую установлены современные средства защиты от внешних угроз из сетевого пространства.

– актовый зал (мультимедийное оборудование: компьютер, проектор, экран);

– учебные кабинеты в том числе и кабинет информатики (компьютер, проектор, интерактивная доска);

– мобильный класс (ноутбук, планшет с выходом в Интернет, контент фильтрацией запрещенного для детей контента);

– сервер (автоматизация образовательных процессов, фильтр запрещенного контента для детей);

– системы видеонаблюдения образовательной организации с возможностью трансляции через Интернет;

– цифровые лаборатории по предметам с возможностью использования образовательных онлайн ресурсов.

Цель: обеспечение технико-технологической стороны

образовательного процесса.

Задачи:

1) обеспечить информационную открытость образовательной организации;

2) обеспечить безлимитный высокоскоростной канал работы в сети Интернет;

3) поддерживать в рабочем состоянии безопасное использование компьютерной техники в условиях школы;

4) проводить мероприятия по организации безопасной работы учащихся, родителей и работников школы в сети Интернет;

5) осуществлять контентную фильтрацию всех компьютеров, подключенных к интернету;

6) обеспечить заключение договоров со сторонними организациями.

Таким образом данная модель предполагает правильное функционирование безопасной цифровой образовательной среды в учебном процессе и открывает новые возможности в использовании онлайн ресурсов для повышения качества образования. Моделирование позволяет построить желательный образ организации безопасной цифровой среды в школе. В ходе чего все участники образовательного процесса будут обладать необходимым уровнем компетентности в области информационной безопасности.

Выводы по первой главе

В главе 1 мы рассмотрели различные риски и угрозы, которые могут возникать в сетевом пространстве и неправильном поведении детей в этом пространстве, что способствуют деформации развития современного поколения. Но вместе с тем проведя анализ мы определили, что если ребенку указать правильное направление поведения в сети Интернет, то можно добиться успехов как в саморазвитии, так и в учебном процессе.

Продолжая свои исследования, мы изучили понятийный аппарат

информационной безопасной среды.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационная безопасность детей – состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Управление безопасной цифровой образовательной средой – это взаимодействие всех субъектов образовательного процесса, сконцентрированное на обеспечении становления, стабилизации, оптимального функционирования и обязательного развития образовательной организации и создания безопасной цифровой образовательной среды.

В связи с этим проведя исследования и проанализировав все вышеизложенное, нами было предложено внедрить модель безопасной цифровой образовательной среды в среднюю школу.

ГЛАВА 2. ВНЕДРЕНИЕ МОДЕЛИ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ В МОУ АРХАНГЕЛЬСКАЯ СОШ

2.1 Анализ состояния цифровой образовательной и безопасной информационной МОУ Архангельская СОШ

Базой исследования выступила МОУ Архангельская СОШ. В исследовании приняли участие 15 учителей, 60 учеников с 7 по 11 классы, 47 родителей (законные представители) учащихся. Всего учащихся с 1 по 11 классы 153 ученика.

Образовательное учреждение - Архангельская средняя общеобразовательная школа организовано в 1986 году по Решению исполкома № 225 от 22.07.1986г

Сведения о реорганизации и переименовании:

1995г. МОУ Архангельская средняя школа. Постановление Главы администрации Сосновского района № 592 от 27.06.1995г.

2000г. МОУ Архангельская средняя общеобразовательная школа Сосновского района Челябинской области. Постановление № 840 от 05.09.2000г.

2002г. МОУ Архангельская средняя общеобразовательная школа. Постановление № 294 от 02.04.2002г.

Учредитель: Муниципальное образование Сосновский муниципальный район

Адреса места осуществления образовательной деятельности: 456537, Челябинская область, Сосновский район, с. Архангельское, ул. Набережная, 1А

Учреждение осуществляет образовательную деятельность в соответствии с Уставом образовательного учреждения, утвержденным Постановлением Администрации Сосновского муниципального района

№3301 от 28 декабря 2015 года;

- Лицензией серии 74ЛО2 № 00000597 выданной Министерством образования и науки Челябинской области № 11468 от 3 июня 2015 года бессрочно:

1. Начальное общее образование - основная образовательная программа – 4 года

2. Основное общее образование – основная образовательная программа – 5 лет

3.Среднее общее образование - основная образовательная программа – 2 года

Образовательное учреждение имеет свидетельство о государственной аккредитации № 1524 от 21 декабря 2012 года, выданное Министерством образовании и науки Челябинской области на срок действия по 21 декабря 2024 года.

МОУ Архангельская СОШ имеет лицензию на право ведения образовательной деятельности по следующим образовательным программам: образовательная программа начального общего образования, образовательная программа основного общего образования, образовательная программа среднего общего образования, образовательная программа дополнительного образования.

Школа укомплектована компьютерным классом в количестве – 4 компьютера. Так же у каждого преподавателя есть свой рабочий компьютер или ноутбук. Ведется закуп лицензионного программного обеспечения, в том числе и для защиты от внешних угроз.

Основным условием обеспечения качества образования в современной школе является эффективно развивающаяся и функционирующая безопасная цифровая образовательная среда.

Цель: провести анализ состояния цифровой образовательной и безопасной информационной среды МОУ Архангельская СОШ.

Задачи:

1) провести анализ состояния цифровой образовательной и безопасной информационной среды МОУ Архангельская СОШ;

2) определить уровень компетентности участников образовательного процесса (учителя, учащиеся, родители) в области познания информационной безопасности;

3) сравнить результаты, сделать вывод;

В исследовании были использованы следующие методы:

– беседа с преподавателями, анкетирование и анализ полученных данных;

– беседа с учащимися и их родителями, анкетирование и анализ полученных данных;

– изучение существующей документации в области цифровизации и обеспечения информационной безопасности МОУ Архангельская СОШ школы.

Исследование проводилось в период с сентября 2018 года по май 2019 года.

На первом этапе был проведен констатирующий эксперимент, в ходе которого изучена документация школы, локальные нормативные акты, проведен общий анализ цифровой образовательной среды в том числе и в области информационной безопасности. В связи с этим можно было выстроить критерии оценивания уровня безопасности использования информационных технологий в образовательном процессе школы:

4 балла – оптимальный уровень. В школе созданы условия, которые можно считать модельными.

3 балла – высокий уровень. В школе созданы и функционируют все требуемые условия безопасной цифровой образовательной среды.

2 балла – средний уровень. В школе созданы условия, но по каким-то причинам не исполняются требования по организации безопасной цифровой среды.

1 балл – низкий уровень. В школе частично созданы условия, но они не позволяют реализовать деятельность в полной мере.

0 баллов – нулевой уровень. Отсутствие условий для реализации деятельности.

Следующим этапом было проведено анкетирование, с помощью которого определили:

– Уровень грамотности учителей в области изучения информационной безопасности, а также умения применять современные информационные технологии в учебном процессе.

Соответствующая анкета была размещена на компьютерах организации для удобства обработки информации. Анкета оценивалась по следующим критериям:

85-100% – Высокий уровень;

55-84% – Средний уровень;

0-54% – Низкий уровень.

– Уровень образованности детей при работе в сети Интернет. Детям была представлена анкета блиц-опрос «Я и моя информационная безопасность». Анкета оценивалась по следующим критериям:

8-10 «Б» – Высокий уровень;

5-7 «Б» – Средний уровень;

0-4 «Б» – Низкий уровень.

– Уровень знаний родителей (законных представителей) учащихся школы в области информационной безопасности и культуре поведения в сетевом пространстве. Критерии оценивая анкеты:

85-100% – Высокий уровень;

55-84% – Средний уровень;

0-54% – Низкий уровень.

Анализ состояния информационной безопасной образовательной среды МОУ Архангельская СОШ представлен в Таблице 2.

Таблица 2 – Анализ состояния информационной безопасной образовательной среды

№ п/п	Деятельность участников образовательного процесса	Обеспечение деятельности	Уровень
Технологические средства, информационные ресурсы, формы информационного взаимодействия. Средний балл:			**1**
	Создание и использование информации (в том числе запись и обработка изображений и звука, выступления с аудио-, видео сопровождением и графическим сопровождением, общение в сети Интернет и др.)	Компьютеры, интерактивные доски, презентационное оборудование, акустические системы, микрофоны, веб-камеры, видео и фото камеры, сетевое оборудование, документ-камера. Различное специализированное ПО для осуществления телекоммуникации, доступа в Интернет, редактирования аудио и видео информации. Расходные материалы. Методические материалы и рекомендации	1
	Получение информации различными способами (поиск информации в сети Интернет, работа в библиотеке и др.)	Локальная компьютерная сеть с доступом в Интернет, компьютеры, система контентной фильтрации, электронные библиотечные каталоги. Расходные материалы	1
	Использование безопасных цифровых образовательных онлайн ресурсов в учебном процессе.	ПО для организации планирования «Сетевой город. Образование. Якласс. Учи.ру и тд.	1
	Использование онлайн ресурсов для изучения информационной безопасности подростков.	Онлайн ресурсы с гос. поддержкой Сетевичек.рф, единыйурок.рф, урокцифры.рф	1
	Использование контент фильтрации образовательной организации.	ПО для реализации: skydns, Интернет цензор usergate прокси сервер, маршрутизаторы с использование белых списков разрешенного контента через ДНС средства, детский интернет регулируемый интернет провайдером и т.д.	1
	Использование антивирусной защиты на компьютерах школы.	Разнообразное бесплатное и платное программное обеспечение для антивирусной защиты систем Windows.	1
	Специализированное программное обеспечение защиты информации.	Программное обеспечение организующее защищенные каналы передачи данных для безопасного документооборота.	1

Продолжение таблицы 2

	Проектирования и организации своей индивидуальной и групповой деятельности, организации своего времени с использованием ИКТ	Автоматизированная информационная система (Сетевой город. Образование»). Онлайн ресурсы образовательного процесса. Онлайн ресурсы с достоверной информацией. Компьютеры, ПО (планировщики). Расходные материалы. Методические материалы и рекомендации	1
	Планирования учебного процесса, фиксации его динамики, промежуточных и итоговых результатов	Автоматизированная информационная система (Сетевой город. Образование»).	1
	Обеспечения доступа в школьной библиотеке к информационным ресурсам Интернета, учебной и художественной литературе, коллекциям медиа-ресурсов на электронных носителях, к множительной технике для тиражирования учебных и методических тексто-графических и аудиовидеоматериалов, результатов творческой, научно-исследовательской и проектной деятельности учащихся	Компьютеры с доступом в Интернет, возможностью работы с различной мультимедийной информацией.	1
	Дистанционное взаимодействие всех участников образовательного процесса	Автоматизированная информационная система (Сетевой город. Образование»). Социальные сети и интернет мессенджеры. Компьютеры, доступ в Интернет, веб-камеры.	1
	Дистанционное взаимодействие образовательного учреждения с другими организациями социальной сферы	Компьютеры, доступ в Интернет, сетевое оборудование, веб-камеры, ПО для телекоммуникации и расходные материалы. Автоматизированная информационная система (Сетевой город. Образование»).	1
	Реализация безопасной цифровой образовательной деятельности в целом	Наличие локальной компьютерной сети и безопасного доступа в сеть Интернет. Наличие компьютеров с ЭОРами и доступом в Интернет на рабочих местах педагогов. Наличие компьютеров с ЭОРами и доступом в Интернет на уроках и во внеурочное время у обучающихся (мобильный компьютерный класс, компьютеры в информационно-библиотечном центре). Расходные материалы.	1

На основании анализа состояния безопасной цифровой образовательной среды МОУ Архангельская СОШ можем сделать вывод, что в школе частично созданы условия, но они не позволяют реализовать деятельность в полной мере.

Так же был изучен уровень компетентности педагогов в области информационной безопасности и защите персональных данных при применении в учебном процессе информационных технологий. Было проведено анкетирование учителей школы на онлайн ресурсе https://www.survio.com/survey/d/V0M5M8A9V9M5K8V1Z

Анкета для учителей представлена в Приложении 1.

Обработав результаты анкетирования, выяснили:

Владеют знаниями в области информационной безопасности – 30% опрошенных. Следят за развитием новых цифровых технологий в области информационной безопасности детей 20% учителей. Используют онлайн ресурсы в педагогическом процессе 20% учителей. Применяют онлайн ресурсы для саморазвития – 30% учителей. Знакомы с законом «О персональных данных» – 40% учителей. Знакомы со специализированными информационными порталами и поисковыми системами для детей – 20%. Сетевое взаимодействие с учениками слабо развито.

Таким образом можем сделать вывод, что работа педагогов в области учения, развития и саморазвития в области информационной безопасности и защите персональных данных слабо развита и несет низкий потенциал. Общий уровень развития познания педагогов в области информационной безопасности представлен в Таблице 3.

Таблица 3 – Уровень развития знаний педагогов в области информационной безопасности

Уровень знаний педагогов	Количество	%
Высокий уровень	3	20
Средний уровень	4	26,67
Низкий уровень	8	53,33

Как видим большинство педагогов имеют средний и низкий уровни компетентности в области информационной безопасности. Наглядно результаты представлены на Рисунке 2.

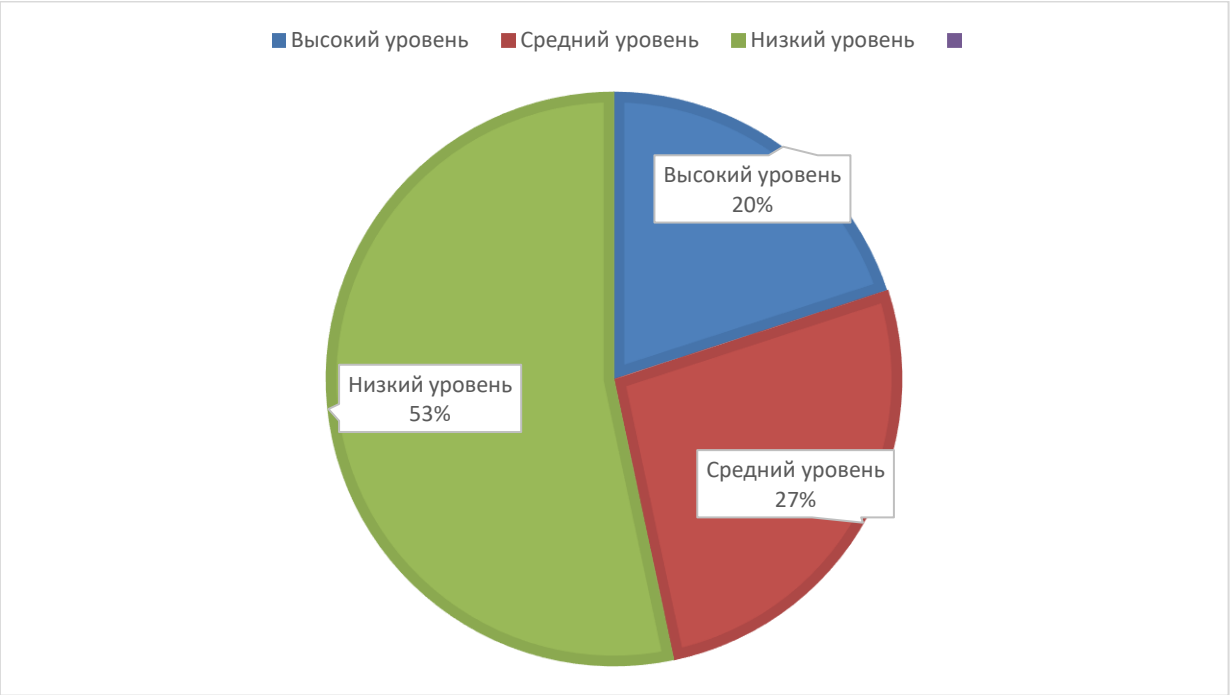

Рисунок 2 – Уровень компетентности педагогов в области информационной безопасности

Следующим шагом произвели анонимное анкетирование учащихся. Анкета представлена в Приложении 2.

Обработав и проанализировав результаты анкет (общее кол-во детей, прошедших анкетирование – 60 человек), выяснили следующее:

Таблица 4 – Уровень знаний поведения в сети Интернет учащихся

Уровень знаний правильного поведения в сети Интернет	Кол-во	%
Высокий уровень	8	13,33
Средний уровень	12	20
Низкий уровень	35	58,33
Не используют интернет	5	8,34

Наглядно результаты представлены на Рисунке 3.

Рисунок 3 – Уровень знаний поведения в сети Интернет учащихся

Из представленного результата видно, что большинство детей не знакомы с правильным пользованием сети Интернет и культурой поведения в сетевом пространстве. Так же имеется 1% учащихся, которые вообще по каким-либо причинам не используют интернет или косвенно знакомы с его использованием.

Следующий этап – анкетирование родителей (законных представителей) учащихся школы.

Анкета представлена в Приложении 3.

Анализ результатов анкет показал: Компьютер дома есть у 90% опрошенных. Дети, имеющие доступ в интернет с различных гаджетов, имеют 95%. За сайтами, которые посещают дети следят 38% родителей. Программы фильтрации нежелательного для детей контента используют 5% родителей. Беседы с ребенком о безопасной работе в сети интернет проводят 2% родителей. Таким образом можно сказать, что родители создали условия детям для использования онлайн ресурсов, но мало кто следит за работой детей в сети Интернет. И совсем маленький процент тех родителей, которые готовы проводить беседы с детьми по безопасной информационной культуре в

сетевом пространстве.

Наглядно результаты представлены на Рисунке 4.

Рисунок 4 – Результаты анкетирования родителей

По результатам исследования было определено, что защита учащихся в цифровом пространстве находится в зачаточной стадии и скорее всего существует частичная проблема знаний в этой области. В самой школе частично созданы условия для осуществления деятельности в данной области, но не все участники образовательного процесса готовы к развитию и работе в области информационной безопасности. Хотя использование свободного доступа сети Интернет учащимися находится на высоком уровне – 95%. В связи с этим мы апробировали разработанную нами модель для решения проблемы знаний в области информационной безопасности всех участников образовательного процесса.

2.2 Внедрение модели безопасной цифровой образовательной среды МОУ Архангельская СОШ

Для формирования и внедрения модели безопасной цифровой образовательной среды в сентябре 2019 года была создана проектная группа из числа административной команды школы. Проектной группе предстояло

решить следующие задачи:

– разработать элементы модели безопасной цифровой образовательной среды в МОУ Архангельская СОШ;

– наполнить элементы содержанием, которое способствовало бы развитию участников образовательного процесса в сфере защиты от угроз информационного пространства;

– ознакомить коллектив преподавателей образовательной организации с моделью безопасной цифровой образовательной среды МОУ Архангельская СОШ;

– создать условия для максимального включения преподавателей в процесс реализации данного проекта.

Соответственно в начале учебного 2019-2020 года на педагогическом совете было представлено развитие школы в направлении информационной безопасности учащихся на последующие 5 лет вперед – Внедрение модели безопасной цифровой образовательной среды. Так же была представлена сама модель безопасной цифровой образовательной среды МОУ Архангельская СОШ.

Получив одобрение преподавателей и руководителей подразделений школы, модель безопасной цифровой образовательной была вынесена на обсуждение родителям и учащимся, где так же получил одобрение на внедрение и реализацию. Ниже представлены планы мероприятий по всем компонентам внедряемой модели.

В целях реализации организационно-управленческого компонента был разработан следующий план мероприятий, представленный в Таблице 5.

Таблица 5 – План мероприятий по реализации организационно-управленческого компонента модели

Основные мероприятия	Сроки	Ответственные	Ожидаемый результат
1	2	3	4
Разработка локально-нормативной базы об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования. Защита и обработка персональных данных.	Октябрь 2019	Директор, заместители структур, учитель информатики.	Разработаны и приняты локальные акты необходимые для обеспечения информационной безопасности образовательной организации.
Назначении ответственного лица за информационную безопасность и защиту персональных данных образовательной организации.	Февраль 2020	Директор	Начало работы ответственного за информационную безопасность школы. Решение проблемы доведения административной информации до потенциальной аудитории.
Создание сайта школы.	Февраль-июль 2020	Директор, зам директора по информатизации, учитель информатики.	Размещение оперативной информации на сайте. Доведение информации до всех работников школы. Усиление контроля за исполнительской дисциплиной
Нормативно-правовое обеспечение о информационной безопасности и защите персональных данных.	Февраль 2020	Директор, заместители директора, секретарь школы	Внедрение внутришкольной документации по информационной безопасности. Ознакомление коллектива с разработаными локальными документами.

Продолжение таблицы 5

1	2	3	4
Повышение взаимодействия между всеми участниками образовательного процесса. В том числе и с помощью интернет ресурсов и мессенджеров.	Март 2020	Директор, заместители директора, классные руководители.	Организовать взаимодействие по схемам «учитель-ученик», «учитель-родители» с созданием групп по классам, предметам в социальных сетях и интернет мессенджерах
Использование принятых организационно-управленческих технологий среди преподавателей образовательной организации.	Май 2020 – май 2021	Директор, заместители директора.	Контроль за исполнением принятых положений и нормативных документов в области безопасного использования информационных технологий.
Соблюдение действующего законодательства РФ в области информационной безопасности и защите персональных данных.	Один раз в квартал	Заместитель директора по информатизации.	Контроль за исполнением Федеральный закон "О персональных данных" N 152-ФЗ среди администрации и учителей школы.

В целях реализации методического компонента был разработан следующий план мероприятий, представленный в Таблице 6.

Таблица 6 – План мероприятий по реализации методического компонента модели

Основные мероприятия	Сроки	Ответственные	Ожидаемый результат
1	2	3	4
Прохождение курсов повышения квалификации «Информационная безопасность в сети Интернет» в дистанционной форме: **https://solncesvet.ru/trainings/informacionnaya-bezopasnost-v-seti-internet/** или в очной форме обучения в	2021 – 2024гг.	Директор, заместители директора.	Курсы повышения квалификации для администрации и учителей школы – охват 95% сотрудников. Понимание специфики безопасной работы в сети Интернет.

Продолжение таблицы 6

1	2	3	4
Региональном центре оценки качества и информатизации образования (РЦОКИО): **https://rcokio.ru/events/obuchenie/obuchenie-po-ppk-obespechenie-informatsionnoj-bezopasnosti-organizatsi/**			
Изменение профессиональной позиции преподавателей в отношении использования онлайн ресурсов в педагогическом процессе	Весь период	Заместители директора, методист.	Понимание специфики новых образовательных результатов и роли использования безопасных информационных ресурсов у 100% учителей.
Обучение педагогов по программе «Дистанционное обучение» с использованием образовательных онлайн ресурсов.	Весь период	Директор, заместители директора.	Повышение ИКТ компетентности учителей в использовании онлайн ресурсов при дистанционном обучении кольников.
Создание системы онлайн консультации преподавателей по безопасной работе в сети Интернет.	Весь период	Заместители директора.	Создание и дальнейшее ведение группы в интернет мессенджере, для оперативного оказания консультаций между преподавателями, администрацией школы.

Продолжение таблицы 6

1	2	3	4
Участие преподавателей в онлайн мероприятиях, семинарах, вэбинарах.	Весь период	Заместители директора, учителя.	Повышенный интерес участия в онлайн мероприятиях среди учителей школы. Создание и реализация своих похожих проектов.
Освоение и внедрение современных безопасных образовательных онлайн технологий.	Весь период	Учителя, методист.	Повышение качества образования за счет внедрения онлайн ресурсов.
Организация своих онлайн-семинаров для учащихся и их родителей на школьной платформе сайта по темам информационной безопасности и защите персональных данных.	Весь период	Заместитель директора по информатизации, учителя.	Повышения уровня знаний среди учащихся и их родителей (законных представителей) в области информационных технологий, информационной безопасности, защите персональных данных.
Разработка и внедрение программы «Безопасный интернет»	Сентябрь 2020 – Май 2021 гг.	Директор, заместитель директора по информатизации.	На основе модели внедрить программу по обеспечению безопасной информационной среды в школе «Безопасный интернет».

Таким образом для полного функционирования методического компонента безопасной цифровой образовательной среды МОУ Архангельская СОШ была разработана и внедрена программа «Безопасный интернет». Примерная программа представлена в Приложении 4.

В целях реализации образовательного компонента был разработан следующий план мероприятий, представленный в Таблице 7.

Таблица 7 – План мероприятий по реализации образовательного компонента модели

Основные мероприятия	Сроки	Ответственные	Ожидаемый результат
1	2	3	4
Участие учеников в проектной деятельности школы, с использование интернет ресурсов.	Весь период	Заместители директора, учителя.	Повысить качество используемой информации в проектной деятельности. Самореализация учащихся в учебной деятельности.
Создание условий для использования онлайн ресурсов и цифрового контента по всем учебным предметам.	Весь период	Заместители директора, учителя.	Повышение интереса работы в сети интернет с образовательными онлайн ресурсами педагогов и учащихся.
Повышение образованности и компетентности у учащихся в сфере познания цифровых технологий и информационной безопасности	Весь период	Учителя	Повышение качества образования у учащихся в познаниях цифрового пространства и информационных технологий; участие в конкурсах, олимпиадах и др. в сфере информационных технологий.
Дистанционное и онлайн обучение учащихся образовательной организации с применением современных технологий (при необходимости) и для детей находящихся на домашнем обучение, а также для детей с ОВЗ.	Весь период	Учителя	Расширить использование онлайн ресурсов при дистанционном обучении. Организовать безопасное дистанционное обучение детей.
Привлечение учащихся в систему дополнительного образования на базе образовательной организации. Либо с привлечением дистанционного и онлайн обучения.	Весь период	Заместитель директора по информатизации, учитель информатики.	Повысить интерес учащихся к изучению современных информационных технологий и защиты информации во внеурочной деятельности.

Продолжение таблицы 7

1	2	3	4
Снижение числа безграмотности среди учащихся в области защиты от угроз информационного пространства сети Интернет.	Весь период	Учителя, заместители директора.	Внедрение в учебный процесс обязательного внеурочного занятия по теме «информационная безопасность» на весь учебный год
Привлечение родителей (законных представителей) учащихся к изучению вопроса защиты детей в информационном пространстве	Весь период	Заместитель директора по информатизации, учителя.	Повысить уровень родителей в вопросах защиты детей при работе в сети Интернет.
Привлечение всех участников образовательного процесса к использованию образовательного сетевого ресурса «Сетевой город. Образование»	Весь период	Администрация школы, учителя, родители.	Повышение интереса и контроль учащихся через онлайн ресурс «Сетевой город. Образование»
Ликвидация безграмотности родителей в вопросах воспитания детей в области информационной безопасности.	Весь период	Учителя	Снижение обоснованных жалоб со стороны педагогов, детей на действия родителей по вопросам воспитания. Способность родителей решать конфликтные ситуации самостоятельно,
Ежеквартальное размещение на сайте образовательной организации информации с появившимися вопросами от родителей по информационной безопасности детей.	С 2022 года на весь период.	Заместитель директора по информатизации, учителя.	Сбор информации и создание рубрики на школьном сайте «Часто задаваемые вопросы» в области информационной безопасности детей и защиты персональных данных.

Для реализации образовательного компонента представляем разработку одного из внеклассных мероприятий по изучению информационной безопасности в Приложении 5.

В целях реализации технологического компонента был разработан следующий план мероприятий, представленный в Таблице 8.

Таблица 8 – План мероприятий по реализации технологического компонента модели

Основные мероприятия	Сроки	Ответственные	Ожидаемый результат
Заключение договора с поставщиком интернет-услуг	Январь 2020 – весь период.	Директор, учитель информатики.	Стабильный высокоскоростной канал интернета.
Установка контент-фильтра на школьный сервер, компьютеры учебных классов и техническое обслуживание	Весь период	Директор, заместитель директора по информатизации.	Обеспечение безопасной работы учащихся в сети Интернет.
Покупка пакетов антивирусного ПО на всю компьютерную технику школы	Весь период	Директор	Обеспечение защиты компьютера от внешних угроз..
Покупка лицензионного ПО на компьютерную технику школы.	Весь период	Директор	Обеспечение комфортной работы на компьютерной технике.
Покупка новой компьютерной техники для комфортной работы учащихся и преподавателей	Весь период	Директор, заместитель директора по информатизации.	Обеспечение современной компьютерной техникой участников образовательного процесса. Повышение интереса работы с применением информационных технологий.
Разработка проекта «Серверная»	Февраль 2021	Директор, заместитель директора по информатизации	Создание серверной комнаты с соответствующим оборудованием для автоматизации образовательных процессов внутри школы.

Продолжение таблицы 8

1	2	3	4
Организация технической поддержки педагогов при проведении уроков с использованием современной цифровой техники	Весь период	Заместитель директора по информатизации, учителя.	Оперативная помощь учителям в учебном процессе при использовании компьютерной и мобильной техники.
Создание школьного «Центра тестирования» для проверки знаний учащихся и хранении результатов на сервере школы. Имеет выход в интернет.	Весь период	Администрация школы, учителя.	Проверка знаний учащихся, в том числе и при дистанционном обучении. Безопасное хранение информации на сервере внутри школы.
Разработать, утвердить и ознакомить всех работников школы с локальными актами, регулирующими работу в сети Интернет	Весь период	Директор, заместители директора	Формирование информационной культуры, обеспечение безопасной работы в сети интернет
Ежеквартальное размещение на сайте образовательной организации информации с появившимися вопросами от родителей по информационной безопасности детей.	С 2022 года на весь период.	Заместитель директора по информатизации, учителя.	Сбор информации и создание рубрики на школьном сайте «Часто задаваемые вопросы» в области информационной безопасности детей и защиты персональных данных.

В ходе реализации технологического компонента модели цифровой образовательной среды МОУ Архангельская СОШ планируется повысить качество использования современных информационных технологий в условиях образовательного процесса.

Таким образом внедрение модели безопасной цифровой образовательной среды МОУ Архангельская СОШ позволит реализовать функционирование информационной безопасности всех участников образовательного процесса в условиях школы.

2.3 Результаты внедрения модели безопасной цифровой образовательной среды МОУ Архангельская СОШ

Целью завершающего этапа работы было определить эффективность

внедрения модели безопасной цифровой образовательной среды в школе.

Задачи:

1. Провести анализ состояния цифровой образовательной и безопасной информационной среды школы.

2. Определить уровень компетентности участников образовательного процесса (учителя, учащиеся, родители) в области познания информационной безопасности.

3. Определить степень удовлетворенности участников образовательного процесса функционированием безопасной цифровой образовательной среды.

При внедрении модели безопасной цифровой образовательной среды школы были получены следующие результаты:

Анализ безопасной цифровой среды школы показал, что в школе постепенно создаются условия для осуществления данной деятельности в полном объёме. Постепенно расширяется комплекс мер по изучению информационной безопасности среди учителей и учащихся. Классными руководителями созданы группы в социальных сетях и интернет мессенджерах, для более оперативного взаимодействия с учениками и их родителями (законными представителями). В АИС «Сетевой город. Образование» свою деятельность в полной мере ведут 85% учителей. В учебный процесс введено внеурочное занятие для учеников 7 класса по теме «Информационная безопасность» на весь учебный год. Началась активная работа классных руководителей с родителями в области правильного поведения детей в сети Интернет, посредством онлайн ресурса квест по информационной безопасности «Сетевичек.рф». Педагоги постепенно проходят курсы повышения квалификации по информационным технологиям и безопасности в образовательном процессе школы. Создан сайт школы для информирования оперативной и актуальной информацией. Подключен стабильный высокоскоростной интернет. Постепенно идет закупка и оснащение компьютерной и интерактивной техникой кабинетов

образовательной организации. Заключены договора, куплены и уже внедрены на всю компьютерную технику школы пакеты программного обеспечения: антивирусные пакеты программ, программы контент-фильтрации, лицензионные операционные системы Windows и др. Для учащихся школы регулярно проводятся занятия по информационной безопасности, в том числе и с использование различных онлайн ресурсов (например, «Единыйурок.рф, Урокцифры.рф»). Ведется закупка серверного оборудования для реализации проекта «Серверная». Разработана и постепенно внедряется программа «Безопасная цифровая среда образовательной организации». После внедрения модели уровень вырос до 2,5 балла.

Анкетирование учителей показало, что уровень компетентности в области информационной безопасности повышается. Большая часть педагогов стали уделять внимание на проблему культуры поведения учащихся в сети Интернет. Повысилось применение образовательных онлайн ресурсов в учебном процессе. Создана система оперативного консультирования учителей по работе с онлайн-ресурсами и цифровыми инструментами.

Обработав результаты анкетирования, выяснили:

Владеют знаниями в области информационной безопасности – 70% опрошенных. Следят за развитием новых цифровых технологий в области информационной безопасности детей 50% учителей. Используют онлайн ресурсы в педагогическом процессе 70% учителей. Применяют онлайн ресурсы для саморазвития – 70% учителей. Знакомы с законом «О персональных данных» – 90% учителей. Знакомы со специализированными информационными порталами и поисковыми системами для детей – 90%. Сетевое взаимодействие с учениками налажено на 95%.

Таким образом можем сделать вывод, что после внедрения модели безопасной цифровой среды работа педагогов в области учения, развития и саморазвития в области информационной безопасности и защите персональных данных получила основательное развитие и повышение. Общий уровень развития познания педагогов в области информационной

безопасности представлен в таблице 9.

Таблица 9

	Количество	%
Высокий уровень	12	80
Средний уровень	3	20
Низкий уровень	0	0

Наглядно результаты представлены на рисунке 6.

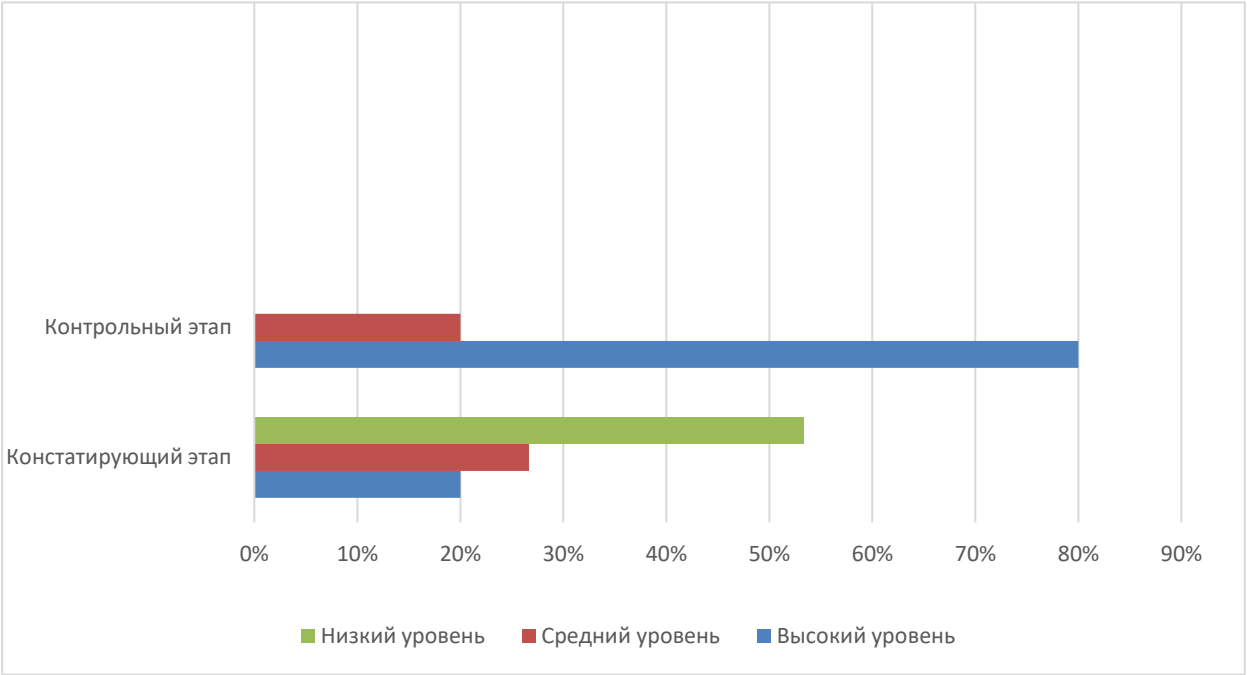

Рисунок 6 – Уровни компетентности педагогов в области информационной безопасности на констатирующем и контрольном этапах эксперимента.

Уровень знаний учащихся правильного поведения в сети Интернет представлен в Таблице 10.

Таблица 10

Уровень знаний правильного поведения в сети Интернет	Кол-во	%
Высокий уровень	40	66,67
Средний уровень	14	23,33
Низкий уровень	6	10
Не используют интернет	0	0

Из представленного результата видно, что большинство детей стали повышать уровень знаний правильного безопасного пользования сети Интернет и культуру поведения в сетевом пространстве. 1% детей, не использующих интернет, так же были привлечены в проведенные мероприятия по изучению информационной безопасности и были вовлечены в образовательную деятельность с использованием онлайн ресурсов в условиях школы, использованием школьной компьютерной техники.

Наглядно результаты представлены на Рисунке 7.

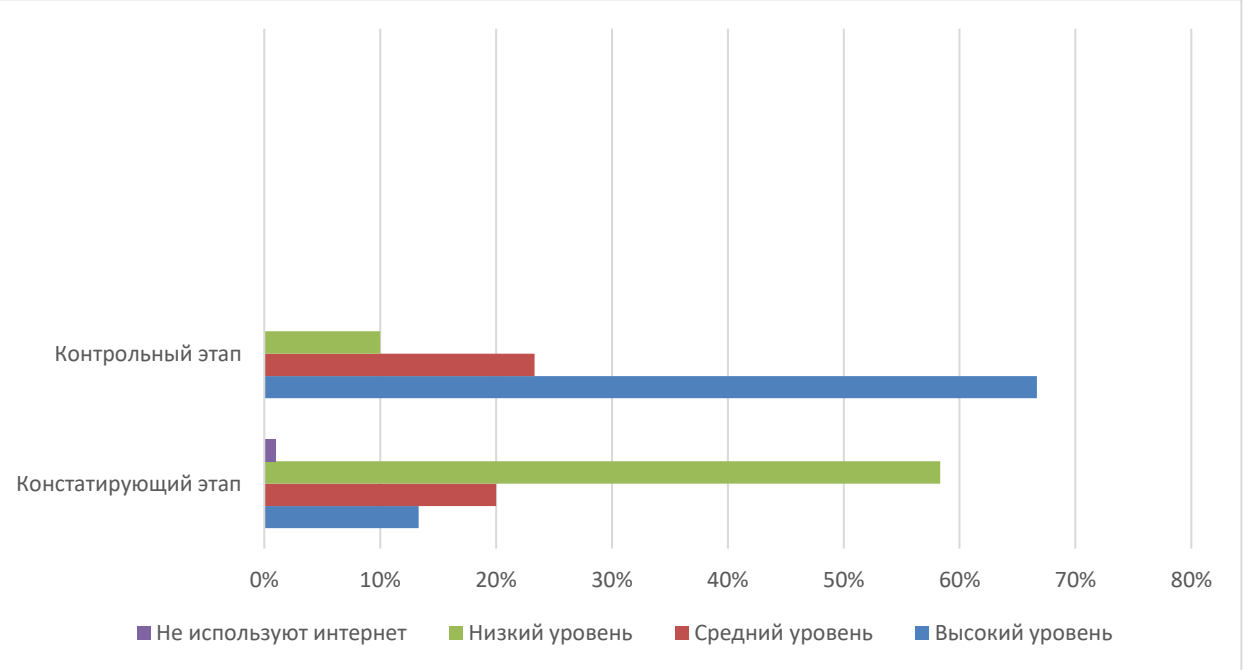

Рисунок 7 – Уровень знаний учащихся правильного поведения в сети Интернет на констатирующем и контрольном этапах.

Анализ результатов анкет показал: Компьютер дома есть у 90% опрошенных. Дети, имеющие доступ в интернет с различных гаджетов, имеют 95%. За сайтами, которые посещают дети следят 56% родителей. Программы фильтрации нежелательного для детей контента используют 35% родителей. Беседы с ребенком о безопасной работе в сети интернет проводят 70% родителей. Таким образом можно сказать, что родители создали условия детям для использования онлайн ресурсов, но мало кто следит за работой детей в сети Интернет. И совсем маленький процент тех родителей, которые готовы проводить беседы с детьми по безопасной информационной культуре в сетевом пространстве.

Наглядно результаты представлены на рисунке 8.

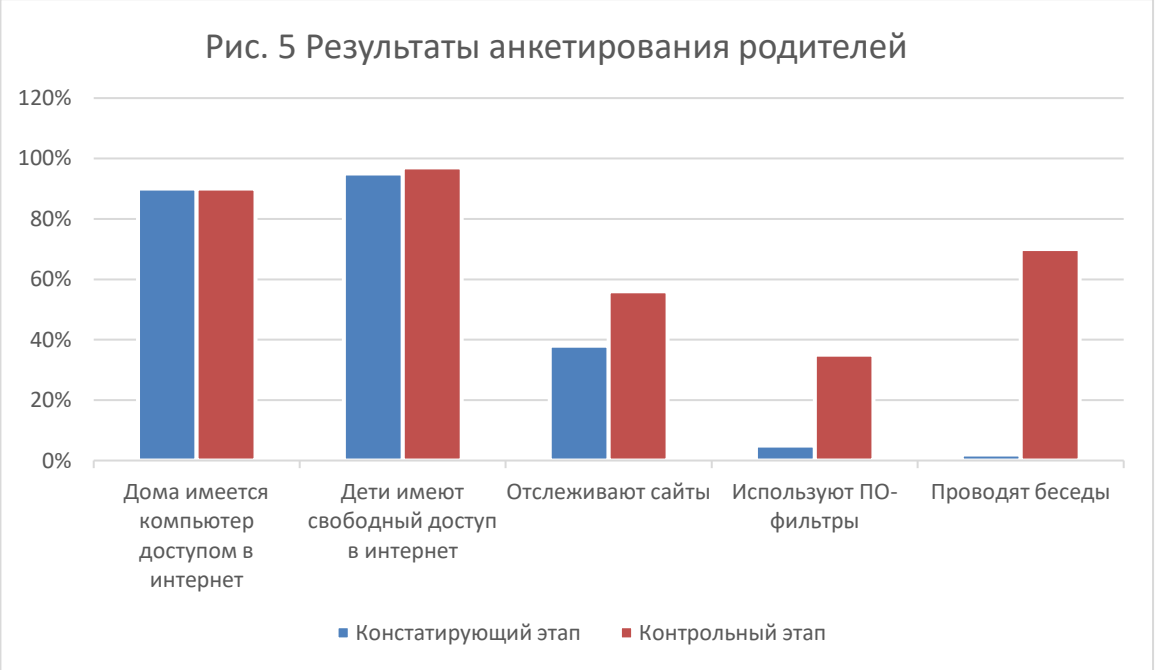

Рисунок 8 – Результаты анкетирования родителей на констатирующем и контрольном этапах

Кроме того, выяснили степень удовлетворенности родителей организацией образовательного процесса с использованием безопасной цифровой образовательной среды в школе:

Родителям задавались следующие вопросы:

1. Пользуетесь ли вы рекомендациями по контролю поведения ребенка в информационном пространстве? (Да– 2 балла, не всегда – 1 балл, не пользуюсь – 0 баллов)

2. Пользуетесь ли вы онлайн ресурсами «Сетевичёк.рф», «Единыйурок.рф»? (Да– 2 балла, частично – 1 балл, не пользуюсь – 0 баллов)

3. Удовлетворяет ли вас организация образовательного процесса с использованием современных цифровых технологий? Да– 2 балла, частично – 1 балл, нет – 0 баллов)

4. Удовлетворяют ли вас формы информационного взаимодействия с учителями? Да– 2 балла, частично – 1 балл, нет – 0 баллов)

Удовлетворенность качеством образовательного процесса с применением современных цифровых устройств в том числе и сети Интернет составила 80% родителей, частично – 15%. Рекомендациями пользуются 70% родителей, не всегда – 21%. Предложенными онлайн ресурсами в области информационной безопасности детей пользуются 58% родителей, частично – 22%. Форма взаимодействия с учителями посредством онлайн ресурсов удовлетворяет 85% родителей, остальные предпочитают очное общение.

Таким образом качество образовательного процесса с использованием безопасной цифровой среды как видим имеет положительную динамику развития.

Выводы по второй главе.

В ходе реализации задач практической части нашей работы:

1. Проведен анализ безопасной цифровой образовательной среды школы (1 балл).

2. С помощью анкетирования определен уровень знаний в области информационной безопасности среди педагогов, учащихся и их родителей (законных представителей).

Мы выяснили, что общий уровень знаний среди учителей, учащихся и

их родителей (законных представителей) в области информационной безопасности находится в начальной стадии и имеют низкий уровень компетентности.

Для повышения эффективности функционирования безопасной цифровой образовательной среды МОУ Архангельская СОШ была разработана и внедрена модель безопасной цифровой среды школы. Предложен ряд управленческих и педагогических действий и мероприятий.

На контрольном этапе мы провели анализ безопасной цифровой образовательной среды школы (2,5 балла). Определили уровень компетентности педагогов в области информационной безопасности (высокий уровень – 80%, средний уровень – 20%, низкий уровень – 0%); уровень знаний учащихся правильного поведения в сети Интернет (высокий уровень – 66,67%, средний уровень – 23,33%, низкий уровень – 10%); уровень контроля поведения ребенка в информационном пространстве (За сайтами, которые посещают дети следят 56% родителей. Программы фильтрации нежелательного для детей контента используют 35% родителей. Беседы с ребенком о безопасной работе в сети интернет проводят 70% родителей).

В связи с вышеизложенным, внедрение модели безопасной цифровой образовательной среды способствует повышению качества образовательного процесса в школе.

ЗАКЛЮЧЕНИЕ

К выполнению работы привела необходимость создания новой модели устройства безопасной цифровой образовательной среды МОУ Архангельская СОШ, которая должна обеспечить безопасное использование современных информационных технологий при достижение новых образовательных результатов. Целью работы являлось определение текущего состояния безопасной цифровой образовательной среды МОУ Архангельская СОШ, а также разработка и внедрение модели безопасная цифровая образовательная среда школы, которая позволит найти результативные механизмы управления данной средой.

В результате выполнения исследования:

1. Проведен анализ рисков и угроз информационной безопасности в современной школе.
2. Рассмотрены понятия и социально-педагогический аспект безопасной цифровой среды в образовательной организации.
3. Описана модель безопасной цифровой образовательной среды в современной школе.

В практической части работы нами проведён анализ безопасной цифровой образовательной среды МОУ Архангельская СОШ. Определен уровень компетентности участников образовательного процесса в области информационной безопасности.

Выявлено, что безопасная цифровая образовательная среда школы имеет низкий уровень развития и находится на начальном этапе использования. Создаются не достаточные условия для ее полного функционирования.

Для повышения эффективности функционирования безопасной цифровой образовательной среды школы была разработана и внедрена модель БЦОС и предложен ряд управленческих и педагогических мероприятий и действий.

Анализ результатов внедрения модели показал:

1. повысился уровень безопасной цифровой образовательной среды школы;
2. повысилась компетентность учителей в области информационной безопасности;
3. повысилась культура поведения учащихся в информационном пространстве;
4. повысился контроль родителей за детьми при работе в сети Интернет;
5. большинство родителей поддерживают политику развития безопасности учащихся в сетевом пространстве.

В связи с этим, выдвинутая гипотеза, что безопасная цифровая образовательная среда обеспечивается реализацией модели – подтвердилась. Следовательно, цель работы достигнута, а намеченные задачи решены.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Галатенко, В.А. Основы информационной безопасности [Текст] / В. А. Галатенко. - М.: Интуит, 2013.

2. Зубакина О.В. Сетевая поддержка профессионального самоопределения старших школьников // Открытое образование [Текст]. — 2008. —№ 2. — С. 77—85.

3. Леончиков В.Е. Информационная свобода и информационная безопасность в системе непрерывного образования // Информационная свобода и информационная безопасность [Текст]: Материалы междунар. научно- практич. конференции. — Краснодар, 2001. — С. 336—338

4. Малых Т.А. Педагогические условия развития информационной безопасности младшего школьника [Текст]: Автореф. дисс. ... канд. пед. наук. — Иркутск, 2008.

5. Саттарова Н.И. Информационная безопасность школьников в образовательном учреждении [Текст]: Дисс. ... канд. пед. наук. — СПб., 2003.

6. Старикова Л.Д. Современная трактовка непрерывности образования // Высшее образование сегодня [Текст]. — 2008. — № 10. — С. 76—79.

7. Стратегия развития информационного общества в российской федерации // Российская газета [Текст]: Федеральный выпуск № 4591 от 16 февраля 2008 г.

8. Утробина Е.В. О формировании сетевых профессиональных педагогических сообществ // Педагогическое образование и наука [Текст]. — 2007. — № 3. — С. 64—66.

9. Эльконин Б.Д. Круглый стол / Парадоксальные результаты международных исследований оценки качества образования // Вопросы образования [Текст]. — 2008. — № 1. — С. 170—171.

10. Ясенев В.Н. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Учебное пособие. /Ясенев В.Н. - Нижний Новгород: 2017. –198с

11. Ажмухамедов, И.М., Ханжина, Т.Б. Определение оптимального набора мер по обеспечению информационной безопасности [Текст] / И.М. Ажмухамедов, Т.Б. Ханжина // «Актуальные вопросы современной информатики»: материалы Международной заочной научно-практической конференции (1-15 апреля 2011г.). Коломна, ГОУ ВПО «Московский гос. областной социально-гуманитарный институт», 2011, Т.1, С.8-12.

12. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 9 с.

13. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 7 с.

14. ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.

15. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

16. Доктрина информационной безопасности Российской Федерации, № Пр-1895 от 9 сентября 2000 г.

17. Домарев, В.В. Безопасность информационных технологий. Системный подход [Текст] / В.В. Домарев. – Киев: «ТИД», 2012. – 912 с.

18. Завгородний, В.И. Комплексная защита информации в компьютерных системах[Текст] / В.И. Завгородний. - М.: «Логос», 2001.

19. Зегжда, Д.П. Основы безопасности информационных систем[Текст]: учеб. пособие для вузов / Д. П. Зегжда, А. М. Ивашко. - М.: Горячая линия Телеком, 2000. - 452 с.

20. Концепция обеспечения информационной безопасности предприятия [Электронный ресурс]. - Режим доступа: www.securitypolicy.ru. Дата обращения: 12.05.2017.

21. Таирова Н.Ю. Развитие информационно-исследовательской компетентности преподавателя педагогического университета [Текст]: Автореф. дис. канд. пед. наук / Н.Ю.Таирова. - Калининград, 2001. - 19 с.

22. О безопасности [Электронный ресурс]: [федеральный закон: от 05.03.1992 г. № 2446-I, в ред. от 25.12.1992 г. № 4235-I, от 24.12.1993 г. №2288, от 25.07.2002 г. № 116-ФЗ, от 07.03.2005 г. № 15-ФЗ]. - Режим доступа: www.consultant.ru.

23. О персональных данных [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. № 152-ФЗ, в ред. от 04.06.2014 г. № 152-ФЗ]. - Режим доступа: www.consultant.ru.

24. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. №149-ФЗ, в ред. от 06.04.2011 г. № 149-ФЗ]. – Режим доступа: www.consultant.ru.

25. Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: [п. 2 Постановления Правительства Российской Федерации: от 17.11.2007 г. № 781, в ред. От 01.11.2012 г. № 1119]. - Режим доступа: www.consultant.ru.

26. Тришина С.В. Информационная компетентность как педагогическая категория / Интернет-журнал [Электронный ресурс] "Эйдос".2005. 10 сент. http://www.eidos.ru/journal/2005/0910-11 .htm.

27. Бармен С. Разработка правил информационной безопасности. - М.: Издательский дом "Вильямс", 2002.

28. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право. - Спб.: Изд-во «Юридический центр Пресс», 2001.

29. Сидоров, А.О. Модель и метод структурированной оценки риска при анализе информационной безопасности [Текст]: диссертация ... кандидата технических наук: 05.13.19 / А.О. Сидоров; [Место защиты: С.-Петерб. гос. ун-т информац. технологий, механики и оптики]. - Санкт-

Петербург, 2008. - 134 с.: ил. РГБ ОД, 61 09-5/1295.

30. Черкашена Л.С. Внутришкольное управление процессом формирования информационной компетентности учащихся [Текст]: диссертация кандидата педагогических наук: 13.00.01 Белгород, 2007, 223 е., Библиогр.: с. 147-167 РГБ ОД, 61:07-13/2658

31. Структура системы защиты информации от угроз нарушения целостности [Электронный ресурс]. - URL: www.shadanis.narod.ru.

32. Шишов С.Е., Агапов И.И. Компетентностный подход к образованию как необходимость / Мир образования - образование в мире. 2005, №4. - с.41-43.

33. Бождай А.С., Финогеев А.Г. Сетевые технологии. Часть 1 [Текст]: Учебное пособие. Пенза: Изд-во ПГУ, 2005.

34. Симонович С., Евсеев Г. Эффективная работа: познай свой компьютер [Текст]. – СПб.: Питер, 2005.

35. Указ Президента Российской Федерации от 17.12.97 г. № 1300«Концепция национальной безопасности Российской Федерации» в редакции указа Президента Российской Федерации от 10.01.2000 г. №24.

36. Шубинский М.И. Информационная безопасность для работников бюджетной сферы [Текст]. Учебное пособие / НИУ ИТМО. СПб., 2012.

37. Воронов Р.В., Гусев О.В., Поляков В.В. О проблеме обеспечения безопасного взаимодействия с сетевыми образовательными ресурсами // Открытое образование [Текст]. — 2008. — № 3. — С. 20—23.

38. Грачев Г.В. Информационно-психологическая безопасность личности: теория и технология психологической защиты [Текст]: Автореф. дисс. ... д-ра психол. наук. — М., 2000.

39. Акупень Т. Понятие и сущность информационной безопасности, и ее место в системе обеспечения национальной безопасности РФ // Информационные ресурсы России. 2009. №4

40. Закон Российской Федерации «О государственной тайне» от 21.07.93 №5485-1.

41. Закон Российской Федерации «О международном информационном обмене» от 04.07.96 №85-ФЗ.

42. Закон Российской Федерации «О персональных данных» от 27.07.2006г. № 152-ФЗ.

43. Дорофеев А.В. «Менеджмент информационной безопасности» Журнал «Вопросы кибербезопасности выпуск» № 3 (4) / 2014Пилипенко В. Ф., Ерков Н. В., Парфенов А. А. Обеспечение комплексной безопасности в образовательном учреждении. Теория и практика /М.: Из-во «Айрис-пресс», 2006. 192 с.

44. Бармен С. Разработка правил информационной безопасности. - М.: Издательский дом "Вильямс", 2002.

45. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право. - Спб.: Изд-во «Юридический центр Пресс», 2001.

46. Белов Е.Б., Лось В.П. Основы информационной безопасности. Учебное пособие для вузов, Гелиос АРВ, 2006.

47. «Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 9.09.2000 г. № Пр.-1895.

48. А. Бабаш, Е. Баранова, Д. Ларин «Информационная безопасность. История защиты информации в России», СПб.: Питер, 2015

49. О персональных данных [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. № 152-ФЗ, в ред. от 04.06.2014 г. № 152-ФЗ]. - Режим доступа: www.consultant.ru.

ПРИЛОЖЕНИЕ 1

Анкета учителям

Как Вы считаете, на какой вид деятельности в интернете школьники тратят наибольшее количество времени?

1. ○ Общение в социальных сетях
2. ○ Онлайн игры
3. ○ Поиск информации для образовательных нужд
4. ○ Просмотр фильмов
5. ○ Затрудняюсь ответить
6. ○ Другое: _____

Назовите три наиболее важных, на Ваш взгляд, критерия оценки Интернет-ресурса для детей и подростков Просьба отметить не более трех пунктов

- ☐ Красивое оформление ресурса
- ☐ Ресурс повышает уровень образованности пользователя
- ☐ Ресурс не содержит рекламы и отвечает требованиям интернет безопасности и фильтрации контента (содержимого)
- ☐ На ресурсе присутствуют элементы интерактивности и игровой формы подачи материала
- ☐ Возможность бесплатно скачать с ресурса интересующие материалы без регистрации
- ☐ Другое: _____

Как Вы думаете, может ли школа помочь в освоении культуры безопасного поведения в Сети? Вы можете выбрать не более 3-х вариантов

- ☐ Да, при использовании сетевых технологий на уроках учителя будут обращать внимание на вопросы безопасности
- ☐ Нет, т.к. даже при большом желании учителя не являются квалифицированными специалистами в этом вопросе
- ☐ Нет, у учителей просто нет времени этим заниматься
- ☐ Да, классные руководители могут проводить классные часы по вопросам информационной безопасности
- ☐ Да, но только на уроках информатики
- ☐ Нет, это работа специализированных структур
- ☐ Нет, этим должны заниматься родители

- ☐ Да, подавая подавая пример своим позитивным представительством в социальных сетях
- ☐ Другое:

Знаете ли Вы о мероприятиях, проводимых с родителями по основам информационной безопасности детей в сети Интернет?

- ○ Нет, не знаю
- ○ Знаю, но на практике они не проводятся
- ○ Не знаю, но они были бы очень уместны
- ○ Знаю, проводятся раз в год
- ○ Другое:

Знакомы ли Вы с регламентом пользования личными средствами коммуникации (мобильными телефонами и т.п.) и личной компьютерной техникой в ОУ?

- ○ Да
- ○ Нет
- ○ Не понимаю, о чем речь

Как вы считаете, кто должен организовывать мероприятия с обучающимися по основам культуры работы и информационной безопасности в сети Интернет?

- ○ Учителя предметники
- ○ Компетентные специалисты из соответствующих организаций
- ○ Учителя информатики
- ○ Ответственные за информационную безопасность вместе с заместителем директора по воспитательной работе
- ○ Другое:

Знакомы ли Вы с инструкцией по обеспечению безопасного доступа к Интернету

- ○ Да
- ○ Нет
- ○ Не понимаю, о чем речь

Работает ли в Вашей школе контент-фильтрация?

- Да
- Нет
- Не понимаю, о чем речь

Какой Вы взаимодействуете с детьми в сетевом пространстве?Вы можете выбрать несколько вариантов

- С помощью электронной почты
- В социальных сетях
- С помощью Skype
- С помощью персонального сайта
- Я не использую сетевые технологии для этих целей
- Представительство в сети - это личное пространство, я не впускаю в него детей
- С помощью школьного сайта / школьного журнала
- Другое:

Знакомы ли Вы с Федеральный закон Российской Федерации N 152

- Да
- Нет
- Не понимаю, о чем речь

Знакомы ли Вы со специализированными информационными порталами и поисковыми системами для детей?

- Да
- Нет
- Не понимаю, о чем речь

Если да, то с какими?Перечислите несколько основных

Как Вы думаете, кто в большей мере должен знакомить детей с основами

безопасного поведения в сети Интернет?
Проранжируйте от 1 до 5 степень участия в ознакомлении детей с основами безопасного поведения в сети (1 - должны участвовать в большей степени, 5 - должны участвовать в меньшей степени)

Учителя предметники

Специализированные организации

Родители

Учителя информатики

Окружение

Готово

ПРИЛОЖЕНИЕ 2

Анкета учащихся «Я и моя информационная безопасность»

1. Новый друг, в чьих данных указан тот же возраст, что и у тебя, предлагает тебе обменяться фотографиями.

А Попрошу его фото и потом отправлю свое.

Б Посоветуюсь с родителями.

2. В чате тебя обозвали очень грубыми словами.

А Скажу в ответ: «Сам дурак».

Б Прекращу разговор с этим человеком.

3. Знакомый предложил разослать телефон и адрес «плохой девочки», чтобы все знали о ней.

А Потребую доказательств, что она плохая.

Б Сразу откажусь.

4. Пришло сообщение с заголовком «От провайдера», запрашивают твой логин и пароль для входа в Интернет.

А Вышлю только пароль: они сами должны знать логин.

Б Отмечу письмо как спам.

5. Друг из Интернета предложил тебе встретиться.

А Конечно, приду.

Б Нет, не пойду, так как этот человек может оказаться не тем, за кого себя выдает.

6. Учительница дала домашнее задание: найти ответ на вопрос «Какие планеты входят в Солнечную систему?».

А Найду ответ в Интернете.

Б Проверю информацию в других источниках (книгах), так как не все, что пишут в Интернете — правда.

7. В Интернете на сайте пиратской продукции появилась новая песня

твоего любимого певца (новая книга, компьютерная игра).

А Обязательно скопирую ее в свой плей-лист.

Б Приобрету лицензионную версию песни на официальном сайте, потому что чужую собственность надо уважать.

8. Тебе угрожают по Интернету.

А Я настолько испуган, что боюсь сообщать об этом кому-нибудь.

Б Я сразу расскажу об угрозах родителям.

9. Антивирусная защита на компьютере не рекомендует заходить на сайт, который тебе нужен.

А Проигнорирую предупреждение, может быть, программа ошибается.

Б Не буду заходить на «подозрительный» сайт, потому что опасаюсь вирусов, которые могут повредить моему компьютеру.

10. На фильме, который ты хочешь посмотреть, стоит возрастная маркировка 18+, а тебе еще нет 18.

А Меня не остановит маркировка, если я хочу посмотреть фильм, я его посмотрю.

Б Я спрошу совета у родителей и посмотрю фильм, если они разрешат.

11. Пользуешься ли ты глобальной сетью Интернет в учебных или развлекательных целях?

А Да, использую.

Б Нет, предпочитаю обходить его стороной.

ПРИЛОЖЕНИЕ 3

Анкета для родителей «Безопасный интернет для детей»

- **Есть ли у Вас дома компьютер?**

  ☐ Да
  ☐ Нет
- **Кто пользуется компьютером у Вас дома?**

  ☐ Только родители
  ☐ Только ребенок
  ☐ Все члены семьи
- **Имеет ли Ваш ребенок доступ к сети Интернет?**

  ☐ Да
  ☐ Нет
- **Следите ли Вы за тем, на какие сайты заходит ребенок? Каким образом?**

  ☐ Да
  ☐ Нет
- **Установлены ли у Вас программы, которые фильтруют содержание сайтов?**

  ☐ Да
  ☐ Нет
- **Сколько Ваш ребенок проводит времени в сети Интернет?**

  ☐ До 1 часа
  ☐ Больше 1 часа
  ☐ Не пользуется Интернетом

- **Беседуете ли вы с ребёнком о безопасности в сети Интернет?**

  ☐ Да
  ☐ Нет
- **На какие сайты заходит Ваш ребенок?**

  ☐ Образовательные
  ☐ Социальные сети
  ☐ Разные

Спасибо за участие в анкетировании.

ПРИЛОЖЕНИЕ 4

Программа безопасной информационной среды МОУ Архангельская СОШ «Безопасный Интернет»

Муниципальное общеобразовательное учреждение
Архангельская средняя общеобразовательная школа

Согласовано
На заседании
педагогического совета
Протокол № 5 от 31.08.2020

Утверждено
Директор школы
Р.В. Насыров
Приказ № 111 от 31.08.2020

ПРОГРАММА БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СРЕДЫ МОУ АРХАНГЕЛЬСКАЯ СОШ «БЕЗОПАСНЫЙ ИНТЕРНЕТ»

с. Архангельское 2020

СОДЕРЖАНИЕ

ПАСПОРТ ПРОГРАММЫ

Название раздела программы	Содержание
Тема	Безопасная цифровая образовательная среда средней школы
Ответственные исполнители	Заместитель директора по ИКТ, ответственный за информатизацию. Заместитель директора по УВР, ответственный за деятельность по информационной безопасности. Заместитель директора по безопасности.
Научный руководитель (консультант) эксперимента	Должность: Заместитель директора по информационным и коммуникационным технологиям. Учитель информатики
Актуальность и замысел темы	В настоящее время наблюдается процесс перехода общества к качественно новому состоянию, названными учёными информационным обществом. Информатизация массированно воздействует на психику, модификацию поведения человека, с другой стороны, она выступает фактором модернизации во всех сферах человеческой деятельности. **Актуальность программы** обусловлена радикальными переменами в социальной, политической и экономической жизни общества под влиянием информатизации. Одной из основных задач образования становится не только обучение работе с информацией, но и **комплексноеобеспечение** безопасности участников образовательного процесса при работе с информацией в информационной системе. Под информационной безопасностью ОУ следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Уже сегодня назрела необходимость рассматривать **информационную безопасность как одну из основных составляющих безопасности ОУ.** Важнейшим элементом информационной безопасности ОУ является формирование информационной культуры участников

	образовательного процесса и обеспечение и безопасности школьника в информационной сфере. В программу вовлечены все участники образовательного процесса. Дети рассматриваются как активные пользователи Сети и будущие родители-трансляторы позитивного опыта для новых поколений.
Предмет инновации	Комплексные: организационно-педагогические и технические условия обеспечения информационной безопасности участников образовательного процесса в образовательной организации.
Цель	разработка механизма обеспечения информационной безопасности в
	образовательном процессе.
Практическая значимость	заключается в разработке конкретных рекомендаций по обеспечению информационной безопасности в образовательной организации.
Задачи	Разработать документацию по организации и реализации темы ресурсной площадки. Создать материально-технические и организационно методические, педагогические условия. Продолжить обучение участников образовательного процесса основам безопасного и легитимного использования интернет ресурсов. Разработать методические рекомендации, инструкции, методические пособия, сценарии мероприятий и уроков и иные материалы для обобщения и распространения опыта. Провести открытые мероприятия в рамках образовательного пространства по распространению опыта между учащимися.
Гипотеза	Будет создан инструментарий для обеспечения безопасной информационной среды в школе и, в дальнейшем, в образовательном пространстве района.
Продолжительность:	Продолжительность: 2020 – 2021 учебный год

Состав участников	Учителя информатики, классные руководители, администрация и учебно-вспомогательный персонал: 1. социальный педагог 2. психологи 3. библиотекарь 4. медицинский работник, сотрудники гимназии (бухгалтеры, лаборанты, системный администратор, секретарь) обучающиеся 1-11классов, родители учащихся.
База	МОУ Архангельская СОШ
Этапы, содержание каждого этапа	Реализацию программы предполагается осуществить за 1учебный год. **Подготовительный этап** • Подготовка документов для организации работы на базе МОУ Архангельская СОШ • Обучение консультативно-методической группы для реализации обучения педагогов МОУ Архангельская СОШ **Внедренческий этап** Организация постоянно действующего обучения для педагогов гимназии и города: семинары, консультации, мастер-классы, открытые родительские собрания для педагогов и родителей. Проведение занятий (классные часы, игры, тренинги, викторины, конкурсы, уроки информатики и информационной технологии) с учащимися с целью формирования информационной культуры Участие учителей и учащихся в интернет проектах по проблеме формирования безопасного поведения в сети. **Аналитико-обобщающий этап**. Сбор, анализ информации, подготовка методических продуктов, публикация материалов.
Прогноз возможных негативных последствий, способы коррекции таких последствий	1 Сопротивление инновациям при ведении программы. 2 Недостаточность кадровых ресурсов. 3 Проблема преодоления сопротивления и равнодушия родительской общественности к проблеме интернет- безопасности. 4 Недостаточное материально-техническое обеспечение программы.

Критерии оценки ожидаемых результатов	-снижение количества правонарушений в области информационной безопасности; - снижение количества правонарушений среди учащихся, в том числе проявлений агрессивного поведения; -увеличение количества родителей, установивших программы контент-фильтрации на домашних ПК; -увеличение количества родителей, осуществляющих контроль за использованием сети интернет детьми;
Ожидаемые результаты, формы их представления	1 Формирование у учащихся информационной культуры как одной из важнейших компетенций. (информационных, коммуникативных). 2 Обеспечение безопасного образовательного пространства 3 Повышение качества профессиональных компетенций педагогов. 4 Расширение сферы сотрудничества с образовательными учреждениями, партнерами, заинтересованными организациями. 5 Повышение престижа школы за счет внедрения в работу инновационных программ. 6 Обеспечение сохранности персональных данных и информации в школе. 7 Улучшение материально-технической базы школы.

ПРИЛОЖЕНИЕ 5

Внеурочное занятие по безопасному поведению детей в сети интернет «Безопасность в сети Интернет»

Цель: обратить внимание учащихся на возможные угрозы в сети Интернет, повысить грамотность учащихся в вопросах безопасности в сети, формировать общепринятые нормы поведения в сети.

Задачи:

1. Знакомство учащихся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет.
2. Выработка правила безопасного поведения в сети.
3. Выработка необходимости использования в сети общепринятых нравственных норм поведения.

Планируемые результаты:

Предметные*:* Формирование представлений о безопасном поведении детей в Интернете, организация усвоения основных понятий по данной теме, формирование мировоззрения учащихся, формирование умения распознавать опасные явление в сети Интернет, формирование навыков правильно оценивать степень безопасности ресурсов сети Интернет и основных приемов безопасного поведения в сети.

Метапредметные*:*

***Личностные*:** формирование умений управлять своей учебной деятельностью, развитие внимания, памяти, логического и творческого мышления; воспитание гуманизма, положительного отношения к труду, целеустремлённости, формирование умения управлять своей познавательной деятельностью.

Регулятивные: умеют оценивать правильность выполнения действий при работе в Интернете.

Познавательные: общеучебные – осуществляют поиск и выделение необходимой информации.

Логические: – выстраивают логическую цепь рассуждений

Коммуникативные: научиться высказывать свое мнение, обосновывать его, приводить аргументы

Формы организации познавательной деятельности учащихся: коллективная, индивидуальная, групповая.

Оборудование: компьютер, проектор, интерактивная доска, памятка учащимся;

Ожидаемые результаты:

– повышение уровня осведомленности учащихся о проблемах безопасности при использовании сети Интернет, потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз.

– формирование культуры ответственного, этичного и безопасного использования Интернета.

Тип урока

Открытия нового знания

План и этапы урока:

1. Введение
2. Объявление темы. Постановка задач
3. Просмотр социального ролика «Безопасность школьников в сети Интернет»
4. Сказка о золотых правилах безопасного поведения в Интернет
5. Физкультминутка
6. Рефлексия

Приложение

Памятка по безопасному поведению в интернете

1. Введение.

Создание проблемной ситуации

А сейчас я предлагаю вам отгадать загадки, чтобы понять, о чем пойдет речь на уроке.

Игра «Угадай-ка».

Что за чудо-агрегат
Может делать все подряд -
Петь, играть, читать, считать,
Самым лучшим другом стать? (*Компьютер.*)

На столе он перед нами, на него направлен взор,
подчиняется программе, носит имя... (*монитор*).

Не зверушка, не летаешь, а по коврику скользишь
и курсором управляешь. Ты – компьютерная... (*мышь*).

Нет, она – не пианино, только клавиш в ней – не счесть! Алфавита там картина, знаки, цифры тоже есть.
Очень тонкая натура. Имя ей ... (*клавиатура*).

Сохраняет все секреты «ящик» справа, возле ног,
и слегка шумит при этом. Что за «зверь?». (*Системный блок*).

Есть такая сеть на свете
Ею рыбу не поймать.
В неё входят даже дети,
Чтоб общаться, иль
играть.
Информацию черпают,

И чего здесь только нет!

Как же сеть ту называют?

Ну, конечно ж...

(Интернет)

2. Объявление темы. Постановка задач.

Как вы думаете, о чём мы сегодня будем говорить?

Правильно, мы с вами поговорим об интернете, точнее о безопасности в интернете. Мы живём в эпоху Интернета, без которого, увы, сейчас трудно справиться. Интернет заменил у нас многое. Это нам облегчило жизнь. Сейчас всего лишь при помощи одного небольшого устройства мы можем обмениваться мгновенными сообщениями, покупать книги или музыку, получать любую необходимую информацию и многое другое. Интернет ворвался в нашу жизнь.

У кого дома есть компьютер?

Как вы им пользуетесь?

А у кого дома есть Интернет?

*А как вы думаете, какая опасность может подстерегать пользователей интернета? (*ответы детей*).*

Мы можем найти в интернете любую информацию, но некоторые сайты могут быть заражены, и наш компьютер может «заболеть».

Поэтому постарайтесь запомнить основные правила безопасного интернета.

3. Просмотр социального ролика «Безопасность школьников в сети Интернет»

Описание ролика: Сегодня Интернет является одним из самых мощных инструментов в мире и действительно удивительной частью нашей жизни. Каждый день в нём появляется что-то новое и очень удобное, что делает жизнь легче для многих людей. Но кроме пользы он таит в себе массу опасностей, особенно для детей. Поэтому им просто необходимо знать правила безопасного поведения в сети Интернет, которые подробно рассмотрены в данном уроке.

https://www.youtube.com/watch?v=9OVdJydDMbg

4. А сейчас послушайте сказку о золотых правилах безопасного поведения в Интернет

СКАЗКА

В некотором царстве, Интернет - государстве жил-был Смайл-царевич-королевич, который правил славным городом.

И была у него невеста – прекрасная Смайл-царевна-Королевна, день и ночь проводившая в виртуальных забавах.

Сколько раз предупреждал её царевич об опасностях, подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл-царевич, возводя город, заботился об охране своих границ и обучая жителей города основам безопасности жизнедеятельности в Интернет-государстве.

И не заметил он, как Интернет-паутина всё-таки затянула Смайл-царевну в свои коварные сети.

Погоревал – да делать нечего: надо спасать невесту.

Собрал он королевскую – дружину. Стали думать головы мудрые, как вызволить царевну из плена виртуального. И придумали они «Семь золотых правил безопасного поведения в Интернет», сложили их в котомку Смайл-царевичу, и отправился он невесту искать.

Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: сообщества Змея-искусителя-Горыныча, стрелялки-убивалки Соловья-разбойника, товары заморские купцов шаповских, сети знакомств - зазывалок русалочьи… Как же найти-отыскать Смайл-царевну?

Крепко задумался Смайл-королевич, надел щит антивирусный, взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную. Долго бродил он, и остановился на распутье игрища молодецкого трёхуровневого, стал читать надпись на камне: на первый уровень попадёшь – времени счёт потеряешь, до второго уровня доберёшься – от родных-близких отвернёшься, а на третий пойдёшь - имя своё забудешь. И понял Смайл-царевич, что здесь надо искать невесту.

Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей, разомкнувшихся Смайл-царевна, осенила себя паролем честным и бросилась в объятия своего суженого. Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными: «Вот тебе оберег от козней виртуальных, свято соблюдай наказы безопасные!»

1. **Спрашивай взрослых**

Если что-то непонятно
страшно или неприятно,
Быстро к взрослым поспеши,
Расскажи и покажи.

Всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

2. **Установи фильтр**

Как и всюду на планете,
Есть опасность в интернете.

Мы опасность исключаем,

Если фильтры подключаем.

Чтобы не сталкиваться с неприятной и огорчительной информацией в интернете, установи на свой браузер фильтр, или попроси сделать это взрослых — тогда можешь смело пользоваться интересными тебе страничками в интернете.

3. Не открывай файлы

Не хочу попасть в беду —

Антивирус заведу!

Всем, кто ходит в интернет,

Пригодится наш совет.

Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус!

4. Не спеши отправлять SMS

Иногда тебе в сети,

Вдруг встречаются вруны.

Ты мошенникам не верь,

Информацию проверь!

Если хочешь скачать картинку или мелодию, но тебя просят отправить смс - не спеши! Сначала проверь этот номер в интернете – безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.

5. Осторожно с незнакомцами

Злые люди в Интернете,

Расставляют свои сети.

С незнакомыми людьми

Ты на встречу не иди!

Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

6. **Будь дружелюбен**

С грубиянами в сети,

Разговор не заводи.

Ну и сам не оплошай –

Никого не обижай.

Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека, читать грубости так же неприятно, как и слышать.

7. **Не рассказывай о себе**

Чтобы вор к нам не пришёл,

И чужой нас не нашёл,

Телефон свой, адрес, фото,

В интернет не помещай,

И другим не сообщай.

Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

Залилась совестливыми слезами дева красная, дала своему наречённому слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа города своего, сама начнёт обучаться и помогать будет люду заблудшему и погрязшему в трясине сетевой. И зажили они дружно и счастливо с мечтою расширить границы образования.

Тут и сказочке конец, а кто слушал - МОЛОДЕЦ!

Учитель: Какова мораль этой сказки?

А сейчас немного отдохнём и поиграем.

5. Физкультминутка

Игра «Вирусы»

Цель игры: Эмоциональная разрядка, снятие напряжения.

Вспомогательные материалы: Листы А4 двух цветов и лента, которой можно будет обозначить линию, разделяющую две команды.

Процедура проведения: Листы А4 нужно скомкать и сделать из них снежки двух разных цветов. Снежки одного цвета обозначают, например, вирусы, спам, зараженные файлы, снежки другого цвета – безопасная информация, безопасные файлы. Участники делятся на две команды так, чтобы расстояние между командами составляло примерно 3 м. В руках каждой команды снежки двух цветов, которые они, по команде ведущего, бросают другой команде. Задача: как можно быстрее закидать противоположную команду снежками, при этом успевая откидывать все «опасные» снежки и сохранять у себя все «безопасные». Ведущий засекает 10 секунд и, услышав команду «Стоп!», участники должны прекратить игру. Выигрывает та команда, на чьей стороне оказалось меньше «опасных» и больше «безопасных» снежков. Перебегать разделительную линию запрещено.

Учитель: - Ребята, давайте попробуем почувствовать на себе вирусную атаку и постараться защититься от нее! Правила будут такие. Вам нужно разбиться на 2 команды. Но сначала из листочков бумаги черного и белого цвета сделаем снежки! Каждый должен сделать по 2 снежка белого и черного цвета. Черные снежки – «опасные», а белые – «безопасные». По моей команде начинаем бросать друг в друга снежки! Задача одной команды – как можно быстрее закидать противоположную команду снежками.

Также задача каждой команды – успеть откидывать все черные снежки и сохранять у себя белые.

Сейчас я вручу каждому памятку с правилами. Прочитайте правила и постарайтесь их выполнять (*вручение памяток)*.

6. Рефлексия

Подведём итог нашего урока. Прочитайте предложение и продолжите.

Мне было интересно узнать…

Мне понравилось…

Меня удивило…

Мне захотелось…

Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!

Желаю, чтобы и в жизни, и на просторах Интернета у вас было всё просто отлично!

Памятки о правилах безопасного пользования интернетом остаются вам.

Памятка по безопасному поведению в Интернете

Это важно знать!

- Я не скажу о себе ничего (ни адреса, ни телефона, ни других сведений) без разрешения родителей.

- Я никогда не передам по Интернет своей фотографии.

- Я никогда не встречусь ни с кем, кого знаю только по Интернет, без разрешения родителей. На встречу я пойду с отцом или с матерью.

- Я никогда не отвечу на сообщение, которое заставляет меня краснеть, будь то электронное письмо или общение в чате.

- Я буду разговаривать об Интернет с родителями.

- Я буду работать только тогда, когда они разрешат мне, и расскажу им обо всем, что я делал в Интернет.