МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖИ
РЕСПУБЛИКИ КРЫМ
Государственное бюджетное образовательное учреждение
высшего образования Республики Крым
«КРЫМСКИЙ ИНЖЕНЕРНО-ПЕДАГОГИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ ФЕВЗИ ЯКУБОВА»

На правах рукописи

БЕКИРОВА Мария Александровна

ПЕДАГОГИЧЕСКОЕ СОПРОВОЖДЕНИЕ ОБУЧАЮЩИХСЯ ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ В УСЛОВИЯХ КИБЕРРИСКОВ И КИБЕРУГРОЗ

Специальность
5.8.1. Общая педагогика, история педагогики и образования
(педагогические науки)

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата педагогических наук

Научный руководитель:
доктор педагогических наук, доцент
Мыхнюк Мария Ивановна

Симферополь-2024

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность проблемы исследования. На современном этапе развития информационных технологий возникает проблема безопасного взаимодействия человека в Глобальной сети. Технические возможности Интернета способствует поиску, систематизации, обработки и использования различной информации в социальном пространстве, но вместе с тем возникает вопрос обеспечения информационной безопасности личности обучающегося, которая зачастую имеет негативный и агрессивный характер, что влияет на уровень сформированности духовно-нравственных ценностей школьников. А поэтому проблема формирования кибербезопасности обучающихся является актуальной, так как способствует противостоянию киберрискам и киберугрозам, исходящим из Интернет-сети, в том числе, утечке персональных данных, кибербуллингу, интернет-мошенничеству, киберэкстремизму.

Следует отметить, что под киберрисками подразумевают нарушения безопасности пользователя в финансовой, репутационной и других сферах деятельности в Сети, а под киберугрозами в правовом поле понимается нанесение вреда личности пользователя [Цирлов В.Л., 2013; Хлопов О.А., 2020].

Меры борьбы с негативными тенденциями влияния негативной информации на детей, подростков и молодежь указаны в доктрине информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 г. № 646), Федеральном законе «О защите детей от информации, причиняющей вред здоровью и развитию» (Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с изменениями и дополнениями)); Федеральном образовательном стандарте основного общего образования (Приказ Министерства просвещения Российской Федерации от 31 мая 2021 г. № 287).

Несмотря на принимаемые меры, ежегодно школьники оказываются вовлеченными в ситуации интернет-мошенничества, киберпедофилии, кибербуллинга. В то же время формирование кибербезопасности обучающихся должно

обеспечиваться системой мер, направленных на духовное, нравственное развитие, созданием условий для результативной информационно-просветительской деятельности по вопросам безопасного поведения обучающихся в интернет-пространстве несовершеннолетних подростков.

Обобщение результатов диссертационных исследований и психолого-педагогической литературы позволяет сделать вывод, что проблема изучения педагогического сопровождения обучающихся образовательных организаций в условиях киберрисков и киберугроз является актуальной, однако требует дополнительного исследования, что подтверждается и выявленными противоречиями:

– *на социально-педагогическом уровне*: между потребностью общества в результативной работе с подрастающим поколением по противодействию киберрискам и киберугрозам, и недостаточной разработанностью педагогического сопровождения по формированию готовности обучающихся к их противодействию;

– *на научно-теоретическом уровне* – между наличием теоретико-методологических предпосылок разработки педагогического сопровождения кибербезопасности обучающихся и отсутствием комплексного подхода к сопровождению этого процесса в общеобразовательных организациях;

– *на практическом уровне* – между необходимостью в повышении уровня готовности обучающихся образовательных организаций к противодействию киберрискам и киберугрозам, и недостаточной разработанностью средств сопровождения, обеспечивающих их безопасность в Интернет-сети.

Степень научной разработанности проблемы исследования. Различные теоретические аспекты педагогического сопровождения рассмотрены в трудах Л.В. Байбородовой [2014], Н.В. Кузьминой [2016], Н.С. Кривцовой [2018], В.С. Сухоруковой [2022], А.А. Стерхова [2016], Е.В. Юшкевич [2020] и др.; вопросы информационной безопасности изучали М.М. Бескоровайный [2011], Т.В. Владимирова [2016], Г.В. Грачев [2000], Г.М. Киселев [2012], И.Н. Курносов [2009], А.Я. Минин [2017], Е.Э. Серебряник [2011], Д.С. Синицын [2005];

становление и реализации личности как субъекта педагогической деятельности изучались В.А. Сластениным [1997], Л.К. Фортовой [2014] и др.; использование инновационных процессов в образовании рассмотрены О.Н. Троицкой [2021], А.В. Хуторским [2005] и др.

Проблема безопасности личности в сети Интернет освещалась в работах Г.У. Солдатовой [2014], А.И. Лучинкиной [2016], В.А. Плешакова [2018] и др.; различные аспекты кибербезопасности обучающихся изучали: А.С. Доколин [2017], Д.Б. Дубинина [2019], Ю. Диогенес [2020], О.С. Рыбакова [2020], А.И. Белоус [2021], Т.С. Ширикова [2021] и др.; правила безопасности детей в Интернете изучали Р.М. Алигулиев [2011], Н.И. Саттарова [2016], А.Н. Шеремет [2004] и др.

Существование данной проблемы, необходимость ее научного обоснованного решения свидетельствует об актуальности исследования и позволяют сформулировать тему научного исследования: *«Педагогическое сопровождение обучающихся образовательных организаций в условиях киберрисков и киберугроз».*

Цель исследования – выявить и изучить особенности педагогического сопровождения обучающихся в условиях киберрисков и киберугроз.

Объект исследования – педагогическое сопровождение обучающихся в условиях киберрисков и киберугроз.

Предмет исследования – особенности педагогического сопровождения обучающихся в условиях киберрисков и киберугроз.

Гипотезы исследования.

1. Педагогическое сопровождение обучающихся общеобразовательных организаций в условиях киберрисков и киберугроз может быть представлено как системная педагогическая деятельность, организованная в рамках мотивационно-целевого, теоретико-методологического, содержательно-процессуального и оценочно-рефлексивного направлений, каждое из которых направлено на формирование навыков кибербезопасности у обучающихся.

2. Формирование навыков кибербезопасности обучающихся общеобразовательных организаций может быть обусловлено созданием определенных педагогических условий в учебной и внеурочной деятельности на основе субъект-субъектного взаимодействия через интерактивные формы, технологии и средства педагогического сопровождения.

3. Педагогическое сопровождение может быть успешным, если будут повышены: уровень сформированности компонентов кибербезопасности обучающихся, построенной с учетом их личностных потребностей, в противостоянии киберрискам и киберугрозам, исходящих из Интернет-сети, а именно: уровень знаний о киберугрозах и способах противостояния им; уровень развития критического мышления, уровень рефлексии обучающихся.

Задачи исследования.

1. Уточнить понятия «кибербезопасность», «педагогическое сопровождение обучающихся образовательных организаций в условиях киберрисков и киберугроз» на основе комплексного анализа научной и методологической литературы.

2. Разработать модель педагогического сопровождения обучающихся образовательных организаций в условиях киберрисков и киберугроз, и определить оптимальные педагогические условия ее реализации.

3. Обосновать особенности организации процесса по противостоянию обучающимися образовательных организаций киберрискам и киберугрозам.

4. Экспериментально проверить уровень сформированности компонентов модели вследствие применения разработанных форм, технологий и средств педагогического сопровождения.

Теоретико-методологическая основа исследования представлена:

положениями: системного подхода (В.И. Андреев, И.В. Блауберг, Б.С. Гершунский, А.М. Новиков, В.В. Сериков и др.), деятельностного подхода (Л.С. Выготский, И.А. Зимняя, А.Н. Леонтьев, Т.Д. Овсянникова), субъектно-ориентированного подхода (Е.В. Бондаревская, К.К. Платонов, В.В. Сериков,

И.С. Якиманская и др.), рефлексивного подхода (С.Я. Рубинштейн, А.Л. Уманский, Т.М. Усманов, А.В. Хуторской и др.);

теориями: развития, обучения и воспитания личности (Т.В. Кудрявцев, Б.С. Лихачев, В.А. Сластенин и др.); педагогического сопровождения (О.С. Газман, Э.Ф. Зеер, И.А. Зимняя, А.В. Мудрик, М.И. Мыхнюк, Л.И. Пономарева, И.В. Уварина, Л.К. Фортова и др.); концепциями: формирования информационной безопасности (М.С. Иванов, А.И. Лучинкина, Г.Ю. Маклаков, В.А. Плешаков и др.); противостояния киберрискам и киберугрозам школьниками (Д.Б. Гудкова, Д.Б. Дубинина, К.С. Интенсон, А.Я. Мишин, О.И. Троицкая, Т.С. Ширикова и др.).

Методы и методики исследования.

Теоретические: теоретический анализ научной литературы по проблеме исследования педагогического сопровождения обучающихся в современном образовательном пространстве.

Эмпирические: наблюдение, беседа, анкетирование, педагогический эксперимент, диагностические методики, а именно: авторский опросник «Риски киберпространства» – для выявления группы рисков, к которым склонен подросток и определение уровня сформированности у подростка способов защиты; опросник определения уровня критического мышления – для изучения деятельностно-поведенческого критерия, а именно: умения подростка оценивать и обрабатывать информацию, полученную из интернет-источников, авторский опросник информационной этики; авторский опросник инструментальных навыков в области кибербезопасности – для изучения когнитивно-содержательного критерия; методика Дембо-Рубинштейн для реального и виртуального пространства – для изучения эмоционально-волевого критерия.

Методы математической статистики для обработки результатов педагогических экспериментов и их сравнение.

Этапы исследования.

Первый этап (2020-2021 гг.) был связан с теоретическим анализом научных и литературных источников по проблеме кибербезопасности школьников, определением методологических подходов; изучением состояния сформированности навыков кибербезопасности в образовательных организациях.

Второй этап (2021-2023 гг.) характеризовался разработкой, внедрением и апробацией модели педагогического сопровождения формирования кибербезопасности обучающихся общеобразовательных организаций в условиях киберрисков и киберугроз, экспериментальной проверкой комплекса педагогических условий, обработкой результатов формирующего этапа педагогического эксперимента.

Третий этап (2023-2024 гг.) связан с анализом полученных результатов констатирующего и формирующего этапов, формулировкой выводов, оформлением материалов исследования, определением перспективных направлений дальнейших исследований.

Основные научные результаты, полученные автором, и их научная новизна.

Уточнены сущность и содержание понятия «кибербезопасность обучающихся общеобразовательных организаций»; определены проблемные зоны в формировании кибербезопасности старшеклассника (несформированность мотивов безопасной деятельности в Сети; отсутствие или недостаточность знаний о киберугрозах и способах борьбы с ними; несформированность умений, определяющих критическое мышление подростка; легкомысленное отношение к проблеме кибербезопасности в целом, свойственное подросткам; особенности подросткового возраста в области определения авторитетов и референтных групп); выделены типы киберрисков («ложная информация», «посягательство на доброе имя», «деструктивное воздействие на здоровье»), характерных современным обучающимся.

Расширено понятие «педагогическое сопровождение обучающихся в условиях киберрисков и киберугроз»; эмпирически выявлены признаки опасной ситуации для обучающихся (навязчивость собеседника; прямые угрозы, требование персональных данных, уговоры со стороны собеседника, многократный переход по ссылкам и требование предварительной оплаты); определены особенности организации педагогического процесса и личностные характеристики обучающихся, позволяющие противостоять киберрискам и киберугрозам.

Разработана и эмпирически проверена модель педагогического сопровождения обучающихся общеобразовательных организаций в условиях киберрисков и киберугроз. Выделены критерии сформированности навыков кибербезопасности (мотивационно-стимулирующий, когнитивно-содержательный, деятельностно-поведенческий; эмоционально-волевой).

Определены оптимальные педагогические условия, способствующие реализации модели педагогического сопровождения обучающихся общеобразовательных организаций в условиях киберрисков и киберугроз (формирование положительной мотивации обучающихся к учебной и внеклассной деятельности; развитие критического мышления при столкновении с информацией в интернете, требующей принятия решения; использование интерактивной среды при решении ситуаций, связанных с кибербезопасностью обучающихся; осуществление рефлексии на основе применения механизмов самопознания, самоанализа и самоконтроля).

Разработана и апробирована программа педагогического сопровождения обучающихся общеобразовательных организаций в условиях киберрисков и киберугроз.

Теоретическая значимость исследования состоит в создании теоретической модели «педагогического сопровождения кибербезопасности обучающихся»; полученные результаты исследования дополняют представления о процессе формирования кибербезопасности обучающихся на основе оптимального

педагогического сопровождения при условии комплекса мер по созданию положительной мотивации обучающихся в области кибербезопасности, развитию у них критического мышления, рефлексивной позиции; подтверждают перспективность дальнейших исследований, касающихся самосовершенствования и саморазвития личности обучающегося в процессе противостояния киберугрозам.

Практическая значимость исследования заключается во внедрении в учебно-воспитательный процесс авторской модели педагогического сопровождения, что может позволить общеобразовательной организации целенаправленно осуществлять процесс формирования кибербезопасности обучающихся как в реальном, так и виртуальном пространстве с применением интерактивных и активных форм взаимодействия с обучающимися.

Эмпирический объект и база исследования. В экспериментально-исследовательской работе приняли участие 412 обучающихся 9-х классов общеобразовательных школ г. Симферополя.

Положения, выносимые на защиту.

1. Педагогическое сопровождение обучающихся образовательных организаций в условиях киберрисков и киберугроз представляет собою системную педагогическую деятельность, целью которой является подготовка обучающихся к безопасному взаимодействию в киберсреде, распознаванию киберугроз и умению противостоять им. Педагогическое сопровождение обучающихся образовательных организаций в условиях киберрисков и киберугроз обеспечивается мотивационно-целевым, теоретико-методологическим, содержательно-процессуальным и оценочно-рефлексивными блоками.

2. Уровень сформированности навыков кибербезопасности обучающихся образовательных организаций на основе предложенного педагогического сопровождения зависит от комплекса оптимальных условий (формирование положительной мотивации обучающихся к овладению навыками, обеспечивающими кибербезопасности; развития критического мышления; использование интерактив-

ной среды при решении ситуаций, связанных с кибербезопасностью обучающихся; осуществление рефлексии на основе применения механизмов самопознания, самоанализа и самоконтроля).

3. Эффективность педагогического сопровождения зависит от уровня сформированности компонентов кибербезопасности обучающихся, построенной с учетом их личностных потребностей, в противостоянии киберрискам и киберугрозам, исходящих из интернет-сети, а именно: уровня знаний о киберугрозах и способах противостояния им; уровня развития критического мышления, уровня рефлексии обучающихся.

Апробация и внедрение результатов исследования. Основные положения, выводы, результаты исследования обсуждались на заседаниях кафедры дошкольного образования и педагогики Крымского инженерно-педагогического университета имени Февзи Якубова (Симферополь, 2022-2024).

Результаты исследования были представлены на конференциях различного уровня: Международной научно-методической конференции «Актуальные вопросы науки и образования: теория и практика» (Симферополь, 2021); Международной научно-практической конференции «Проблемы совершенствования законодательства и правоприменительной практики» (Симферополь, 2022); Международной научно-практической конференции «Межотраслевые исследования как основа развития научной мысли» (Оренбург 2022); Международной конференции «Научные чтения памяти Февзи Якубова» (Симферополь, 2023); Международной научно-практической конференции «Информационные технологии как основа прогрессивных научных исследований» (Ижевск 2024); Международной научно-практической конференции «Планирование, проведение и толкование итогов научных исследований (Воронеж, 2024); II Всероссийской научной конференции «Актуальные вопросы науки и образования: теория и практика» (Симферополь, 2022); III Всероссийской научной конференции «Актуальные вопросы науки и образования: теория и практика» (Симферополь, 2023); XXII Все-

российской научно-практической конференции Январские педагогические чтения «Теоретико-методологические проблемы проектирования и моделирования содержания образования» (Симферополь, 2024); II Региональной научно-практической конференции «Инновационные технологии производства одежды и профессионального образования» (Симферополь, 2023); I Региональной научно-практической конференции «Образование в новых регионах Российской Федерации: реалии и перспективы» (Ялта, 2023); Научно-практической конференции для студентов и молодых ученых «Молодая наука» (Симферополь 2023).

Материалы исследования используются в деятельности Крымского инженерно-педагогического университета имени Февзи Якубова (Симферополь), Крымского федерального университета имени В.И. Вернадского (Симферополь), СОШ № 4 имени маршала Ф.И. Толбухина (Симферополь).

Публикации. По теме диссертационного исследования опубликовано 12 работ общим авторским объёмом 3,2 п.л., в том числе 6 статей – в журналах, рекомендованных ВАК РФ для публикации результатов диссертационных исследований.

Структура диссертации. Работа состоит из введения; трех глав; заключения, в котором содержатся основные вводы, практические рекомендации, а также перспективы дальнейшего изучения проблемы; списка литературы, состоящего из 212 источников; 5 приложений. Основной объем текста исследования составляет 157 страниц. Работа содержит 23 рисунка и 27 таблиц.

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПЕДАГОГИЧЕСКОГО СОПРОВОЖДЕНИЯ ФОРМИРОВАНИЯ КИБЕРБЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ

1.1. Кибербезопасность обучающихся как педагогическая проблема

Глобальная сеть Интернет заявила о себе с позиции важнейшего культурного события человечества. Само понятие «Интернет» – (inter – международная, net – сеть), имеет множество толкований, а по сути является сетью информационных потоков, где информация становится технологией, а технологии становятся информационными [17].

В настоящее время освоение основ кибербезопасности обучающихся, формирование информационной грамотности находится в центре научных интересов философов, социологов, психологов и педагогов. Существенный вклад в исследование проблемы кибербезопасности школьников внесли М.В. Бедник, Д.Б. Гудкова, Д.Б. Дубинина, К.С. Итинсон, О.Н. Троицкая, Т.С. Ширикова и др.; влияние информации на личность обучающегося рассматривалась в работах В.Г. Грачева, А.Б. Беляева, Н.И. Саттаровой и др.; использование эффективных форм, методов и технологий обучения для решения задач, связанных с противодействием кибербезопасности обучающихся исследовали А.В. Белоус, О.А. Воскрекасенко, М.А. Герасимова, Л.Н. Гришина, А.С. Кравченко, Л.К. Хаджиева и др. [1, 3, 4, 5, 11, 14, 25, 43, 51, 52, 97, 152, 172, 173, 182, 184, 194].

В современных литературных источниках рассматриваются различные подходы к определению содержания понятия «кибербезопасность». Прежде всего, отметим, что в основе дефиниции находится базовая единица – безопасность как отсутствие угрозы для жизни и здоровья человека. В законодательстве данное понятие рассматривается как «состояние защищенности жизненно важных интересов личности, общества и государства от угроз внешнего и внутреннего характера» [129].

Кибербезопасность, являясь частным случаем безопасности, может характеризовать состояние защищенности личности в киберпространстве при взаимодействии с техническими средствами и другими пользователями [122]: совокупность мер по защите информационно-коммуникативных технологий от цифровых атак [60, 89]. Так как наши личные данные доверены информационным системам, социальным сетям, цифровым устройствам, то основы кибербезопасности должен знать каждый пользователь, в том числе и обучающиеся.

В семантическом поле понятия кибербезопасность рассматривается дефиниция «информационная безопасность». При этом рядом ученых кибербезопасность рассматривается как частный случай информационной безопасности [21, 181].

И если категория «информационная безопасность» подразумевает состояние защищенности личности от угроз информационного воздействия [116, 122, 164], то в случае кибербезопасности мы имеем ввиду состояние защищенности личности от угроз информационного воздействия в киберсреде.

Современное положение информационного пространства сети можно назвать источником трансформации влияния информационной среды в угрозы информационной безопасности школьников. По этой причине, данный фактор не позволяет однозначно рассматривать Интернет как благополучную образовательную киберсреду (киберпространство).

Понятие «киберпространство» (от англ. «cuberspace») впервые было введено писателем У. Гибсоном в его новелле «Сожжение Хром», где он объединил понятие кибернетики и пространства [19, 56].

Китайский ученый Лю Ган указывал на то, что киберпространство, образуемое компьютерной сетью, является инструментом для исследования чувства и разума [114].

Ученые утверждают, что к факторам информационной среды, которые могут стать угрозами информационной безопасности школьников, относятся [116, 122]:

– общедоступность, неподконтрольность, неограниченный объем поступления циркулирующей информации школьникам;

– присутствие в информационной среде модифицированных физических носителей информации, воздействующих на физиологические системы подростка;

– наличие в информационных потоках специфических составляющих, целью которых является изменение психофизического состояние детей и подростков;

– наличие в информационной среде информации манипулятивного характера, дезориентирующей подростков, ограничивающей их возможности в условиях недостаточной правовой осведомленности, а также в силу возрастных особенностей подростков [116, 122].

На сегодняшний день проблемы кибербезопасности являются проблемами мирового масштаба и одновременно актуальным направлением для исследования и обеспечения безопасности информационных массивов в том числе и в образовательной сфере, а поэтому система кибербезопасности является защитой хранящейся и передаваемой информации, предназначенной для обмена.

По мнению многих исследователей к основным проблемам, связанных с обеспечением кибербезопасности образовательного процесса, является недостаточность информационно-просветительской деятельности по вопросам безопасного поведения в интернет-пространстве несовершеннолетних подростков, а также недостаточное учебно-методическое обеспечение в области информационной безопасности учебного процесса в образовательных организациях.

Значимой проблемой является несвоевременное совершенствование знаний и умений в области информационной безопасности самих педагогов. С этой целью образовательным организациям необходимо раскрыть проблему формирования навыков кибербезопасности при планировании содержания методических рекомендаций для педагогов и школьников, в системе повышения квалификации педагогов [23, 60, 122].

Следовательно, выполнив анализ содержания понятий «кибербезопасность» и «информационная безопасность» можно сделать вывод, что кибербезопасность не может быть полноценно направленной на защиту о множества киберугроз, а поэтому необходимо обеспечить максимально благоприятную для пользователей среду.

Изменение мировой образовательной системы, смешивание разных подходов, иногда диаметрально противоположных, приводит к глобальным изменениям не только идей образования, но и трансформации его субъектов. Как подчеркивает С.И. Жожикова это способствует формированию иного поведения, иных подходов, иного педагогического менталитета [66, С. 39]. Среди проблем, связанных с распространением киберпространства особое место занимает проблема информационной культуры, вызванной экспансией сети Интернет во все сферы общественной жизни.

Информационной культуре посвящены работы Р.А. Барышева, Ю.А. Минеева, А.В. Волокитой, Б.В. Кристального и др. Образовательные организации должны способствовать формированию информационной культуры личности обучающегося, предоставить ему фундаментальные знания в области ИКТ, сформировать практические навыки их применения, обеспечить безопасность их, в том числе и при встрече с киберугрозами и киберрисками [19, 25, 26, 27, 38, 39, 42, 47, 50, 51, 56, 57, 59, 63, 64, 67, 75, 80, 81, 93, 94, 95, 96, 97, 100]. Термин «информационная культура» рассматривается и как культуру и информацию, которые выступают составной частью общей культуры личности, а поэтому информационная культура в настоящее время становится обязательным компонентом общего образования.

В.А. Барышев в целом, рассматривает Интернет как явление культуры и как фактор социальных изменений [19]. Во-первых, интернет принес нам стирание культурных границ и упростил общение людей, говорящих на разных языках. Во-вторых, бестелесность и бездомность Интернета привели к изменению

ценностной системы личности и упрощению ее отношения к вечным дихотомиям добро-зло, жизнь-смерть [19].

Гипертекст как основная характеристика и личное свойство Интернета позволил создать новое пространство жизнедеятельности людей, опосредованное техническими средствами [44, 113, 121].

Так как Интернету присущи такие свойства как виртуальность, глобальность, гипертекстуальность и анонимность, эти же свойства формируют и виртуальную реальность [113, 121]. Тотальное погружение молодежи в информационное пространство Глобальной сети Интернет, что зачастую негативно влияет на физическое и психологическое состояние личности. Следовательно, чрезмерное увлечение различной информацией приводит к тому, что подростки, проводя за компьютером длительное время, виртуализируются и перестают воспринимать информацию критично [121, 141].

По мнению ученых, роль Интернета способствует не только развитию национальной культуры, но и оказанию негативного влияния на межкультурную коммуникацию в условиях глобального всероссийского информационного поля.

Одной из стратегических целей обеспечения безопасности в области образования является формирование у обучающихся *культуры личной информационной безопасности*. Для этого необходимо научить субъекта образования критически мыслить, а не потреблять весь контент, представленный в сети. Необходимо научить школьника оценивать информацию. Еще одной важной задачей является формирование у подростков иммунитета к негативным информационно-психологическим воздействиям, выработка алгоритма противостояния киберугрозам. Именно «взаимодействие с киберпространством развивает знание и культуру человека, культуру информационной безопасности, в то время как культура и знание человека, его знания информационной безопасности и культура информационной безопасности оптимизируют это взаимодействие» [2, С. 62].

Культура личной информационной безопасности [29, 43, 86] (О.А. Воскрекасенко, О.А. Киреевой, Н.А. Мойсеевым, Л.Ю. Монаховым, В.П. Топоровским и др.) рассматривается в контексте цифровой грамотности субъектов образовательного процесса; совершенствование обучающихся навыков безопасности работы в киберпространстве с целью формирования у них культуры безопасного поведения в сети Интернет. По мнению О.А. Воскрекасенко и А.А. Киреевой личная культура информационной безопасности включает знания о киберугрозах и способах реагирования на них [86] [Приложение 1].

В связи с этим педагогическое сопровождение формирования навыков кибербезопасности школьников должно включать обучение моделям поведения в случае опасной ситуации, алгоритмам реагирования на них. Особенно опасными становятся ресурсы террористов, сайты с порнографическими материалами, сайты агрессивных религиозных сект.

По результатам исследования фонда «Общественное мнение» 96% школьников, в возрасте 10-17 лет пользуются Интернетом и 51% из них не в полной мере ознакомлены об опасностях в сети. 52% детей выходит в Интернет, где оставляют персональные данные [37]. В связи с этим необходимо учесть, что формирование навыков кибербезопасности обучающихся возможно, как в рамках учебной, так и внеурочной деятельности.

Говоря о киберрисках, необходимо выделить несколько групп:

1. Риски, связанные с вредоносным программным обеспечением. Это и многочисленные вирусные программы, и файлы, ведущие к раскрытию персональных данных или поломке компьютера.

2. Риски, связанные с несоблюдением элементарных способов защиты: сообщение пароля от своих аккаунтов посторонним людям, например.

3. Киберкоммуникационные риски. К ним относятся разговоры с мошенниками, передача информации о себе в Сеть, перенос общения в Сети в реальное пространство.

4. Потребительские риски. Участие во сомнительных розыгрышах, отсылка денег незнакомым лицам, переводы.

5. Психологические риски, включая кибербуллинг, все виды зависимости [30, 37].

К потенциально опасным сайтам исследователи относят ресурсы со следующим контентом: пропаганда наркотиков, пропаганда суицидов и способов самоубийства, межнациональная рознь, порнография, агрессивные религиозные взгляды, пропагандирующие жертвоприношение и насилие [37].

Посещая различные сайты, школьники подвергаются различным киберугрозам и киберрискам. Под киберугрозами подразумевается неформативная лексика, анонимные прокси-сервисы, онлайн-игры, жестокость, насилие, эротика, порно.

К основным внешним киберугрозам специалисты в области кибербезопасности относят:

Вирусы. Считается, что подавляющее большинство киберпреступлений начинается с заражения компьютера вредоносным вирусом.

Спам. К спаму относится «сетевой мусор», который может содержать вредоносную информацию или перенаправлять на вредоносный ресурс [58]. В зоне риска Интернета находится и программное обеспечение. Это связано с мобильными устройствами. Часто пользователи выкладывают большой объем личной информации, которая может быть использована ему во вред. Угрозу несут и распространенные в интернете различного рода аферы через электронную почту или социальные сети, которые входят в доверие к потенциальной жертве. К основным видам интернет-афер можно отнести знакомства, лотерея, различного рода приглашения, звонки-ошибки и др.

Кибербуллинг – намеренная травля жертвы через интернет. На сегодняшний день кибертравля осуществляется даже учениками начальной школы. Как правило, буллеры оскорбляют и издеваются над жертвами используя прямой и

косвенный шантаж, фото и видео, наносят оскорбления как в личных сообщениях, так и на стене жертвы в социальной сети [122]. Школьники не всегда способны справляться с этой травлей, а поэтому обращаются за помощью к взрослым или близким людям. А поэтому, положительные отношения с педагогами, родителями, играют важную роль в защите подростков от кибербуллинга.

Киберэкстремизм как радикальность во взглядах и действиях [58]. Киберэкстремистические проявления оказывают влияние, прежде всего на неустойчивую молодежь, которая является наиболее активным пользователем интернет-сетей и прежде всего социальных сетей. С этой целью в последнее время в образовательных организациях особое внимание уделяется профилактике киберэкстремизма.

Киберсуицид – групповые или индивидуальные самоубийства, согласованные с помощью Интернет-ресурсов.

Угрозы для морали и нравственности через пропаганду информации, связанной с употреблением наркотиков, алкоголя, порнографии и др.

Угрозы интернет-зависимости – аддиктивная форма поведения, проявляющаяся в потере контроля над собой и неспособность вовремя справиться с собой по выходу из сети и противодействии киберзависимости.

Специалистами в области кибербезопасности выделены основные признаки, по которым определяется попадание подростка под влияние киберпреступников:

– переутомление, снижение трудоспособности, успеваемости;

– неоправданное желание похудеть, вступление в группы анорексии;

– нарушение сна, ранний утренний подъем, злоупотребление кофе;

– длительное времяпровождение за компьютером, мобильным телефоном, постоянный обмен сообщениями;

– снижение интереса к искусству, спорту;

– копирование на страницы музыки с символикой сатанизма, фашизма;

– окрашивание волос в различные яркие цвета;

– установление специальных браузеров для анонимного просмотра Интернета;

– игры в приложениях, в которых имеются внутренние чаты и др. [37].

Однако практикой доказано, что проследить всю информацию, попадавшую в Интернет невозможно, как и невозможно, по мнению ученых, предвидеть вход несовершеннолетних на сайты, где рекламируется употребление наркотиков, алкоголя и других вредных для детей веществ [181]. Следовательно, с целью защиты обучающихся от внешних киберугроз необходимо тесное и постоянное взаимодействие педагогов, родителей обучающихся и специалистов в области кибербезопасности, что позволит сформировать у обучающихся культуру личной информационной безопасности и подготовить их к противодействию киберугрозам.

Таким образом, на основе анализа различных источников в области кибербезопасности можно сделать вывод, что кибербезопасность обучающихся образовательных организаций может быть рассмотрена как система мер по обеспечению состояния защищенности школьника от киберрисков и киберугроз.

1.2. Сущность и содержание педагогического сопровождения формирования кибербезопасности обучающихся

Эффективная организация образовательного процесса, связанного с формированием кибербезопасности обучающихся, требует теоретического обоснования оптимального педагогического сопровождения и реализации его основных положений в практической деятельности общеобразовательных организаций.

Субъектами педагогического сопровождения по формированию кибербезопасности обучающихся образовательных организаций являются в первую очередь педагоги, родители подростков, а также специалисты в области кибербезопасности, которые привлекаются образовательными организациями для выполнения в основном консультативных функций. Поэтому каждый из этих субъек-

тов в процессе взаимодействия должен не только своевременно оказывать консультативную помощь обучающимся, но и помогать корректировать их действия, то есть сопровождать, поддерживать.

Различные аспекты теории и практики педагогического сопровождения и поддержку обучающихся рассматривали А.Г. Асмолов, О.С. Газман, В.И. Иванова, Н.С. Кравцова, А.В. Мудрик, В.И. Слободчикова, А.А. Стерхов, Я.И. Пономарев, Н.В. Уваркина, О.Н. Троицкая, А.П. Тряпицина, Т.С. Ширикова, С.Н. Чистякова, Е.В. Юшкевич и др. [32, 33, 34, 35, 36, 45, 99, 174, 181].

Выполним краткий анализ педагогических исследований образовательного процесса, которые, по нашему мнению, в достаточной мере раскрывают, теоретическую и практическую значимость, связанную с педагогическим сопровождением.

Следует отметить, что описания конкретно педагогического сопровождения процесса формирования кибербезопасности в научной и научно-методической литературе практически нет. Однако, в работах А.А. Стерхова мы находим модель педагогического сопровождения процесса духовно-нравственного развития обучающихся. В качестве основных блоков модели ученый выделяет мотивационно-целевой, содержательно-деятельностный и результативно-рефлексивный компоненты, а необходимыми и достаточными условиями успешной ее реализации обозначены социальные партнеры, включая общественные организации, вовлеченность семьи в дело воспитания школьников, создание системы самовоспитания детей и подростков [174, С. 7-8]. Применительно к проблеме нашего исследования отметим последнее условие, акцентируя внимания на необходимости рефлексии обучающегося. Следует отметить, что ученый представлял педагогическое сопровождение как смоделированный эксперимент.

В работах Е.В. Юшкевич дан глубокий анализ проблемы педагогического сопровождения саморазвития учащихся основной школы. Во главу угла исследовательница поставила субъект-субъектное взаимодействие и уделила особое внимание рефлексии школьников по результатам их деятельности. Несмотря на

отличие в названии целевых блоков модели педагогического сопровождения от модели А.А. Стерхова их суть остается той же [200, С. 15-17]. Для нашего исследования важным является именно организация субъект-субъектного взаимодействия и его интерактивный характер.

В словаре русского языка сопровождать – означает «следовать рядом, вместе с кем-либо» [132].

В работе Е.И. Казаковой феномен «сопровождение» рассматривается как педагогическая деятельность в целом, и как метод, обеспечивающий создание условий для принятия субъектом оптимальных решений в различных жизненных ситуаций, в частности [82, 83, 84].

По мнению Е.В. Шушаковой, педагогическое сопровождение процессов обучения и воспитания продиктовано логикой гуманистической парадигмы в образовании, личностно-ориентированным подходом в воспитании [197].

Таким образом, в данных исследованиях педагогическое сопровождение рассматривается как: *процесс развития личности; субъект-субъектное взаимодействие; динамическая структура сопровождения*.

В рамках нашего исследования наибольший интерес представляет концепция Л.В. Байбородовой, которая рассматривает педагогическое сопровождение как: педагогическую деятельность учителя по отношению к ребенку для обеспечения индивидуализации и дифференциации процесса бучения и воспитания; систему педагогических действий, направленных на помощь ребенку в ситуации выбора; интерактивное общение; совокупность форм, методов и технологий взаимодействия [16].

С этой позиции педагогическое сопровождение является комплексом действий педагога и обучающихся, направленных на удовлетворение актуальных потребностей, сопровождающихся в процессе непрерывного и эффективного взаимодействия с целью достижения поставленных целей и задач.

По утверждению Е.И. Казаковой педагогическое сопровождение, выступает в единстве четырех компонентов: диагностики, информации, консультации

и реализации [82, 83]. Диагностика уровня сформированности знаний и умений выявляет реально достижимые цели и задачи педагогической деятельности, связанные с отбором содержания, способов и средств с учетом зоны ближайшего развития изменяемых познавательных и социальных характеристик учащихся, отслеживания результатов и внесения необходимой коррекции; оказание поддержки обучающимся в виде консультаций при решении сложного комплекса действий [84].

На основе анализа значимости педагогического сопровождения в формировании кибербезопасности обучающихся позволило выделить функции и основные принципы данного процесса. С целью осуществления результативного образовательного процесса, связанного с формированием у подростков основ кибербезопасности, педагог способствует:

– формированию у школьников знаний в области кибербезопасности в ходе интерактивного взаимодействия;

– созданию условий для принятия школьниками грамотных решений в дилеммной ситуации.

Задачами педагога являются обеспечение консультативной помощи и коррекционной поддержи обучающимся на протяжении всего времени реализации педагогического сопровождения.

Для нашего исследования значимым является выделение принципов педагогического сопровождения формирования кибербезопасности обучающихся. В первую очередь, мы обращаем внимание на принцип системности педагогического сопровождения. Мы считаем, что в педагогическом сопровождении должен участвовать весь педагогический коллектив и все обучающиеся в рамках своей возрастной группы. Анализ состояния сформированности кибербезопасности в школах Республики Крым показал отсутствие знаний в этой области у самих педагогов и отсутствие мотивации к обучению. При этом взрослые легко поддавались на уловки кибермошенников. Мы считаем, что сопровождение и подготовка к нему должны быть единым процессом для всех.

Еще одним не менее важным принципом является принцип проблемности, обеспечивающий субъектную позицию педагога по отношению к подростку. В этом случае ребенок также воспринимается как субъект воздействия со своими мыслями и планами.

Можно отметить принципы ответственности и индивидуализации сопровождения. Однако, поддерживая идею ответственности, мы все же являемся сторонниками коллективного обучения и воспитания. В связи с этим, считаем, что педагогическое сопровождение процесса формирования навыков кибербезопасности должно проходить в интерактивной форме и в групповых занятиях.

Учитывая специфику процесса формирования кибербезопасности обучающихся, к основным принципам педагогического сопровождения можно отнести: принцип индивидуализации; принцип обеспечения субъектной позиции сопровождающего и сопровождаемого; принцип активного взаимодействия субъектов сопровождения на основе сотрудничества, принцип системности и вариативности сопровождения.

Так, принцип индивидуальности с позиции сопровождающего обеспечивает отбор содержания для формирования знаний, умений и навыков обучающихся общеобразовательной организации по основам кибербезопасности. С позиции сопровождаемых данный принцип обеспечивает осознание и принятие способов противостояния киберугрозам и киберрискам, исходящих из сети Интернет.

Принцип обеспечения субъектной позиции сопровождающего и сопровождаемого направлен на создание условий для формирования положительной мотивации в освоении системы знаний и практических действий, связанных с информационной и кибербезопасностью обучающихся. Сопровождаемый, в свою очередь, усваивает теоретические знания и демонстрирует практические действия как результат по противодействию киберрискам и киберугрозам.

Принцип системности и вариативности сопровождения. Деятельность сопровождаемого заключается в планировании и обеспечении системы знаний и

умений, необходимых обучающимся для защиты от вредоносной информации, исходящей от из различных сайтов, чатов; создании условий для осуществления выбора в совершенствовании практических умений и навыков обучающихся. Деятельность сопровождаемого предполагает осмысление и принятие системного и непрерывного саморазвития и самосовершенствования в области информационной и кибербезопасности сопровождаемым.

Принцип активного взаимодействия субъектов сопровождения на основе сотрудничества со стороны сопровождающего обеспечивает организацию и реализацию совместных действий по формированию кибербезопасности сопровождаемых в процессе учебной и внеурочной работы, а также поддержку инициативы сопровождаемого по принятию решений. Деятельность с позиции сопровождаемого заключается в осмыслении значимости сотрудничества с сопровождающим на основе диалогового общения; реализации учебных целей, связанных с противостоянием сопровождаемых с негативной, вредной информацией из сети Интернет.

Реализация педагогического сопровождения для кибербезопасности обучающихся общеобразовательных учреждений рассматривалась нами с позиции форм, технологий и средств сопровождения:

Применяя различные средства педагогического сопровождения в учебной и внеурочной деятельности, мы учитывали, что сопровождающий учит самостоятельно находить способы решения учебной проблемы, а не решает ее за обучающихся. В данном случае он выступает в роли наставника, коуча, тьютора и консультанта.

Педагог-коуч, тьютор в нашем исследовании используются как синонимичные понятия и предполагают диалогичность в общении с обучающимися, то есть использование интерактивных методов обучения и воспитания [7, 18, 20, 22, 28, 88].

Педагог-наставник играет немаловажную роль в процессе педагогического сопровождения, но следует учитывать, что в этом случае педагог должен быть

профессиональным в вопросах владения компьютером и иметь глубокие знания в сфере кибербезопасности.

Педагог-консультант может привлекаться в роли эксперта по тем или иным вопросам в ходе педагогического сопровождения. Например, в оценке степени сложности ситуации, отборе алгоритмов действий.

Деятельность педагога по оказанию поддержки обучающимся по противостоянию киберрискам и киберугрозам мы выстраивали с учетом требований субъектно-ориентированного подхода, который предполагает:

– учет индивидуальных особенностей личности обучающегося;

– проектирование индивидуальной траектории обучения и развития личности;

– создание ситуаций выбора средств педагогического сопровождения;

– предоставление обучающемуся возможности самостоятельного принятия решения учебной задачи;

– обеспечение возможности обучающемуся высказать собственное суждение.

В исследованиях Т.Б. Волобуевой, О.В. Давлетшаевой, Л.И. Петровой, В.Г. Решетникова и др., представлены различные формы, технологии и средства сопровождения, наиболее интересными для нас оказались деловые игры, мозговой штурм, квесты, ситуативные ролевые игры, конкурсы, олимпиады развивающие технологии, методические рекомендации, а также такие средства оценки сопровождения как мониторинг, оценка, рефлексия, коррекция [15, 41, 54, 61, 62, 90, 154].

Выбор оптимальных организационных форм, технологий и средств педагогического сопровождения и более детально будет обосновано в п. 2.2.

Таким образом, учитывая специфику научной проблемы мы рассматриваем педагогическое сопровождение формирования кибербезопасности обучающихся как *«специально организованный и контролируемый процесс взаимодей-*

ствия субъектов сопровождения, направленный на успешное усвоение основ кибербезопасности обучающимися с целью преодоления затруднений в противостоянии киберугрозам и киберрискам на основе применения оптимальных форм, технологий и средств сопровождения».

1.3. Педагогические условия сопровождения формирования кибербезопасности обучающихся

Прежде чем обосновать выбор оптимальных педагогических условий, обеспечивающих реализацию модели педагогического сопровождения обучающихся в условиях формирования кибербезопасности обучающихся, рассмотрим сущность понятий «условие», «педагогические условия».

В философии категория «условия» трактуется как «выраженное отношение предмета к явлениям действительности, без которых оно существовать не может» [188, 189]. В словаре С.И. Ожегова «условия» рассматриваются как «обстоятельство, от которого что-то зависит; требование, предъявляемое к одной из сторон, которые договариваются; правила, которые устанавливаются в соответствующей области деятельности; обстоятельства, при которых что-то осуществляется» [132, С. 62].

Под педагогическими условиями ученые подразумевают: определенные ресурсы (формы, методы, средства, технологии), направленные на решение педагогических задач [76, 125, 171].

При определении оптимальных педагогических условий педагогического сопровождения, обучающихся в условиях киберрисков и киберугроз мы основывались на критериях их выбора, предложенных Н.М. Яковлевой:

– зависимость эффективности условий от четкости определения конечного результата;

– наличие комплекса условий;

– педагогические условия могут выступать как механизм, включающий деятельность и как результат этой деятельности [201].

По мнению ученых, педагогические условия должны обладать свойствами *достаточности и необходимости* [201].

На основе анализа научных исследований и нашего практического опыта к значимым педагогическим условиям мы отнесли:

– обеспечение мотивированного включения обучающихся в деятельность, обеспечивающую их защиту от негативного воздействия на них информационной среды [190];

– развитие критического мышления обучающихся в процессе решения учебных задач по противодействию киберугрозам [104, 124, 137];

– формирование рефлексии обучающихся по противодействию киберугрозам [55, 61, 147, 174].

Раскроем содержание и обоснуем необходимость применения выявленных педагогических условий. *Обеспечение мотивированного включения обучающихся в деятельность, обеспечивающую их защиту от негативного воздействия на них информационной среды является первым педагогическим условием.* Выбор данного условия продиктован неоспоримой значимостью мотивации для осуществления любого вида деятельности. Понятие «мотивация» в современной педагогике используется как обозначающее систему факторов, детерминирующих поведение (потребности, мотивы, цели, намерения, стремления) и как характеристика процесса, который стимулирует поведенческую активность [115, 209, 210, 211, 212]. С.Л. Рубинштейн считает, что движущие силы человеческого поведения отражаются в мотивах его деятельности [158]. Мотивы, что входят в структуру самой деятельности исследовал А.А. Леонтьев [108]. В свою очередь Л.С. Выготский определял мотивационную сферу как аффектную и вольную сферу личности [44].

Мы рассматривали мотивацию как совокупность мотивов, интересов, потребностей, содержательной характеристикой которых является наличие личностного смысла развития личности через анализ, рефлексию и принятие решений [115].

В рамках нашего исследования для нас представляют интерес учебно-познавательные мотивы, ориентированные на получение дополнительных знаний и умений; мотивы самообразования, ориентированные на получение дополнительных (недостающих) знаний и умений [142].

Считается, что заинтересованность в овладении основами кибербезопасности является одним из наиболее важных мотивов и заключается в удовлетворении как личной, так и общественной потребности. Одним из важных аспектов мотивации является интерес, который выступает положительной составляющей образовательной деятельности.

Г.И. Щукина рассматривает интерес в трех аспектах, а именно [199]:

– проявления интереса к новым фактам и явлениям через изучение учебного содержания проблемного характера;

– проявления интереса к познанию существенно-значимых свойств явлений;

– проявление интереса к логическим умозаключениям с учетом активизации учебного процесса на основе применения принципов и методов логики развития мышления [199].

Для формирования кибербезопасности обучающихся в урочное и внеурочное время необходима внутренняя мотивация, желание узнавать новое и преодолевать трудности по противодействию киберугрозам, исходящим из сети Интернет, активная познавательная деятельность.

По мнению А.Н. Леонтьева, при стимулировании активной деятельности обучающихся необходимо учитывать, что на этот процесс значительно влияет эмоциональная сфера личности через положительные эмоции, удовлетворенности результатом своей деятельности, осознание важности сформированных знаний, ценностей и ценностных ориентаций в области кибербезопасности [109].

Таким образом, реализация первого условия способствует удовлетворению личностных мотивов, потребностей, интересов, направленных на противостояние подростками киберрискам и киберугрозам, исходящим из Глобальных сетей.

Развитие критического мышления обучающихся в процессе решения учебных задач по противостоянию киберрискам и киберугрозам является следующим педагогическим условием. Данное условие способствует критическому восприятию представленной информации, противостоянию киберугрозам, на основе анализа способов безопасной работы с информацией.

Под критическим мышлением подразумевается способность анализировать информацию с позиции логики и находить противоречие в ней, умение выносить обоснованные суждения, решения и принимать полученные результаты в различных ситуациях, в том числе и в нестандартных [115, С. 299; 140, С. 338].

Критичность мышления обучающихся заключается в том, насколько успешно выявляются их суждения и суждения других людей. Однако необходимо учитывать тот факт, что не всегда практические действия обучающихся при встрече с киберугрозами будут носить осознанный характер. Часто это могут быть необдуманные поступки или же использованный ранее уже примененный поведенческий стереотип. То есть, применяются варианты решения проблемных ситуаций без учета изменившихся условий деятельности [68, 162, 166, 194, 205].

Для результативных суждений обучающихся по принятию решений по противодействию киберрискам и киберугрозам у них должны быть выработаны умения, связанные с выполнением таких умственных операций как: сравнение, анализ, синтез, индукцию и дедукцию. В большой педагогической энциклопедии сравнение рассматривается как один из логических приемов познания внешнего мира и духовных ценностей. Познание есть процесс, в котором различение и сходство находятся в неразрывном единстве [140, С. 554].

Считается, что успех сравнения зависит от того, насколько правильно выбраны показатели для сравнения. Поэтому непременным условием для успешного осуществления операции сравнения является необходимость выделения существенных признаков сравниваемых явлений, предметов, фактов. Анализ – это мысленное расчленение чего-либо на части, а затем анализирование этих частей каждую в отдельности, что позволит понять структуру и содержание того, что

мы воспринимаем. Противоположный анализ мыслительной операции является синтез, рассматриваемый как мысленное соединение частей, явлений, предметов, а также мысленное сочетание отдельных их свойств.

Значимым для нашего исследования педагогическим условием является формирование рефлексивной позиции обучающихся по противодействию киберррискам и киберугрозам. Роль рефлексии в развитии личности исследовали С.Ф. Анисимов, А.А. Деркач, С.Я. Рубинштейн и др. [8, 55, 158]; педагогическую рефлексию изучали И.А. Зязюн, И.П. Подласый, А.В. Хуторской и др. [142].

Понятие «рефлексия» происходит от латинского слова «reflexio» – обращение назад. Данная категория возникла в философии и означала процесс размышления индивида о происходящем в его собственном сознании. В социальной психологии рефлексия рассматривается как форма осознания действующим субъектом как он в действительности воспринимается и оценивается другими субъектами. В большой педагогической энциклопедии рефлексия рассматривается как «процесс самопознания субъектом внутренних психических актов и состояний, а рефлексивное отношение личности к собственной деятельности является одним из важнейших психологических условий ее глубокого осознания, критического анализа и в результате самосовершенствования» [140, 147, 153].

По утверждению ученых рефлексия может рассматриваться в качестве механизма ценностно-смыслового уровня саморегуляции, превращающего личность в активный субъект жизнедеятельности [70, 145].

Рефлексия рассматривается и как механизм самопознания и самопонимания. По мнению В.В. Знакова, результатом самопознания является понимание мотивов своего поведения, умения обнаруживать смысл своих поступков, обоснование отношения к другим людям [74]. Как считает В.П. Зинченко, рефлексия – это «способность человека к самоанализу самоосмыслению и переосмыслению своих действий, с помощью которых стимулируются процессы самопознания» [72].

В исследованиях А.В. Хуторского анализируется понятие «педагогическая рефлексия». Ученый видит ее функции в способности педагога определить стратегию и тактику педагогического сопровождения, адекватно оценить собственные ресурсы, умении выбирать адекватные способы достижения цели и устанавливать обратную связь в ходе самосубъектного взаимодействия [142].

Рефлексия учебной деятельности может проявляться в ситуациях практического взаимодействия педагога и обучающегося в процессе взаимопонимания друг друга; проектирования практических видов деятельности по противостоянию киберугрозам с учетом как возрастных, так и индивидуальных особенностей личности обучающегося; в процессе самоанализа и самооценки собственной деятельности; осуществление анализа решения нестандартных ситуаций, по кибербезопасности обучающимися и др. С этой целью необходимо создать такую информационную образовательную среду, в которой будет возможность саморазвития обучающегося через включенность его в активную учебную и внеурочную деятельность.

Рефлексия может рассматриваться в качестве механизмов самопознания, самопонимания, самоанализа, самореализации и самоорганизации. Результатом самопознания является понимание мотивов своих достижений, своего поведения и поступков, отношения к другим людям. По мнению В.Г. Маралова, самопознание – это процесс обнаружения в себе каких-либо качеств, личностных и поведенческих характеристик, фиксация их, всесторонний анализ и оценка [79, 117, С. 28; 118].

Наиболее распространенными способами самопознания являются самонаблюдение (самонаблюдение за своими действиями, событиями внутреннего мира), а также самоанализ как то, что подвергается анализу с целью установления причинно-следственных связей, процесс размышления о себе.

С этой целью необходимо создать такую информационную образовательную среду, в которой будет возможность саморазвития обучающегося через включенность его в активную учебную и внеурочную деятельность. Основной

целью рефлексивной среды заключается в построении совместных действий педагогов и обучающихся как субъектов образования.

Рефлексивная среда, по мнению И.А. Стеценко, представляет собой динамическую структуру, в которой развивается личность; система условий развития личности, открывающая возможность самоисследования и самокоррекции социально-психологических ресурсов, способствующая возникновению потребности к рефлексии [175].

Для формирования кибербезопасности обучающихся общеобразовательных организаций необходима такая рефлексивная среда, которая обеспечит:

– стимулирование личности обучающегося к противостоянию киберрискам и киберугрозам, исходящих из Глобальной сети Интернет;

– предоставление дидактического обеспечения, способствующего оказать реальную помощь обучающимся в процессе решения выполнения самостоятельных действий;

– осуществление субъект-субъектного взаимодействия при решении сложных ситуаций, связанных с противостоянием киберугрозам;

– корректировку действий обучающихся на основе самоанализа и самооценки уровня сформированности практических умений;

– привлечение обучающихся к участию в мероприятиях по кибербезопасности через использование рефлексивных форм.

Считается, что рефлексия связана с уровнем сформированности определенных способностей обучающихся: самосозерцание, сотрудничество, эмпатия, самоорганизация, творческая способность, рассматриваемая как синтез свойств и особенностей личности, характеризующих степень их соответствия требованиям конкретного вида творческой деятельности; способность генерировать идеи, направленные на формирование творческой личности, на основе обоснования и прогнозирования результатов деятельности; способность к рефлексии, рассматриваемая как способность к самопознанию в виде размышлений над собственными переживаниями, ощущениями и мыслями.

Таким образом, рефлексию мы будем понимать, как процесс самосубъектного взаимодействия, обучающийся оценивает свои знания, умения, навыки и ресурсы для их развития [140].

Задача рефлексии, связанная с противостоянием киберрискам и киберугрозам состоит в том, чтобы оказать обучающимся поддержку в ситуациях, требующих устойчивости эмоционального состояния, на основе создания благоприятного климата и эмоционального комфорта в коллективе.

Поэтому необходимо создание такой рефлексивной среды, в которой происходит развитие интеллекта обучающихся, в которой анализируется его опят, создаются положительные продуктивные взаимоотношения педагога и обучающихся, направленные на развитие рефлексивных умений и навыков.

Важным инструментом развития навыков рефлексии является самооценивание достижений обучающимися с помощью ведения Дневников личностного роста. Процесс ведения дневника включает в себя: осознание собственной индивидуальности в определенном роде деятельности; стимулирование учебной и самообразовательной деятельности; выработка рефлексивных умений, связанных с самопознанием, самопониманием, самонаблюдением. В данных дневниках фиксируются способы, приемы и техники решения задач по противодействию киберугрозам, результаты сформированности практических действий в различных ситуациях информационной безопасности, осознания успехов и недостатков при решении учебных задач с помощью сети Интернет.

Фиксирования, анализ и оценку индивидуальных достижений обучающимися можно рефлексировать и с помощью различных видов портфолио, которые можно назвать диагностическим инструментом самопознания и самопонимания самого себя.

С помощью портфолио можно проследить:

– динамику сформированности умений и навыков в области кибербезопасности через призму предпочтений, ценностных установок и устремлений;

– изменения, произошедшие в своем отношении к решению нестандартных задач;

– оценку своих собственных возможностей в преодолении трудностей, связанных с киберугрозами;

– планирование перспективных мероприятий по реализации поставленных целей и задач.

Таким образом, вышеизложенное свидетельствует о том, что рефлексивный компонент будет способствовать созданию рефлексивной среды, способствующей формированию кибербезопасности обучающихся общеобразовательных организаций на основе использования механизмов самопознания, самопонимания, самоанализа своих достижений, действий и поступков.

В данном случае средствами педагогической поддержки формирования рефлексивных умений могут быть:

– «Дневники личностного роста», где фиксируются способы, приемы и техники решения задач по противодействию киберугрозам, результаты сформированности практических действий в различных ситуациях по информационной безопасности, осознания успехов и недостатков при работе в сетях Интернета, обоснование причин неуспешной деятельности и др.;

– «Портфолио результатов саморазвития и самосовершенствования обучающихся», где фиксируются результаты, полученные на разных этапах совершенствования практических действий, результаты самонаблюдения и самооценки своих действий;

– «Портфолио по информационной защите обучающегося». В качестве педагогического сопровождения здесь используются инструкции, алгоритмы действий, методические рекомендации. В таких портфолио подросток записывает основные правила поведения в киберпространстве и свои достижения в этой области.

Следовательно, реализация данного педагогического условия направлена на формирование рефлексивных механизмов самосознания, что позволяет анализировать свои действия и прогнозировать различные альтернативные варианты действий для достижения поставленных целей и задач.

Таким образом, комплекс выбранных и обоснованных педагогических условий результативно влияет на формирование кибербезопасности обучающихся через применение различных средств педагогической поддержки в процессе учебной и внеурочной деятельности.

Выводы по Главе 1

Теоретический анализ научных и психолого-педагогических источников по проблеме исследования позволили сформулировать основные положения кибербезопасности обучающихся. Раскрыта сущность понятий информационная безопасность и кибербезопасность обучающихся образовательных организаций. Проанализированы нормативно-правовые акты Российской Федерации, раскрывающие сущность информационной безопасности детей.

На основе анализа различных источников в области кибербезопасности мы определили, что «кибербезопасность обучающихся образовательных организаций может быть рассмотрена как система мер по обеспечению состояния защищенности школьника от киберрисков и киберугроз».

Изучена сущность и содержание различных аспектов педагогического сопровождения в образовательных организациях, которое рассматривалось как процесс, взаимодействие сопровождающего и сопровождаемого, технологию, метод, систему, основанных на принципах педагогического сопровождения.

Учитывая специфику научной проблемы, мы рассматриваем педагогическое сопровождение формирования кибербезопасности как «специально организованный и контролируемый процесс взаимодействия субъектов сопровожде-

ния, направленный на успешное усвоение основ кибербезопасности обучающихся с целью преодоления затруднений в противостоянии киберугрозам и киберрискам».

Результативному формированию основ кибербезопасности с учетом психологовозрастных особенностей обучающихся способствует комплекс педагогических условий, в том числе: обеспечение мотивационного включения обучающихся в деятельность, обеспечивающую их защиту от негативного воздействия на них информационной среды; развитие критического мышления обучающихся в процессе решения учебных задач по противодействию киберугрозам; формирование рефлексивной позиции обучающихся по противодействию киберрискам и киберугрозам.

ГЛАВА 2. МОДЕЛИРОВАНИЕ ПЕДАГОГИЧЕСКОГО СОПРОВОЖДЕНИЯ ОБУЧАЮЩИХСЯ В УСЛОВИЯХ КИБЕРРИСКОВ И КИБЕРУГРОЗ

2.1. Модель педагогического сопровождения обучающихся в условиях киберрисков и киберугроз

Для того чтобы процесс педагогического сопровождения, связанного с формированием основ кибербезопасности обучающихся образовательных организаций, носил системный характер, возникла необходимость разработки модели как структурно-логического ориентира образовательного процесса. Понятие «модель» в общем виде рассматривается как мера, образ, норма, способ; аналог какого-либо объекта, процесса или явления; искусственный объект, представленный в виде схемы, знаков, формул [140, 142]. В.В. Краевский рассматривает модель как теоретическое представление о явлении, в котором отражаются содержание управления, методы, показатели управленческой деятельности, при этом модель выступает основой диагностирования состояния педагогического процесса [98].

В педагогике модели подразделяются на: описательные, что позволяет представить цели, форму и содержание образовательной практики; функциональные, которые отображают связи данной модели с социальной средой; прогностические [133, С. 88].

Моделирование объектов и явлений педагогической действительности рассматривается в работах С.И. Архангельского, В.Г. Афанасьева, Ю.А. Конаржевского, В.И. Михеева, Н.В. Кузьминой, В.В. Серикова, Н.Ф. Талызиной и др. [12, 13, 54, 92, 103, 167].

Моделируя процесс педагогического сопровождения кибербезопасности обучающихся, мы учитывали, что она будет направлена на реализацию различных функций. Так, функция *научного обеспечения*, направлена на выявление теоретических основ, способствующих противодействию обучающихся различным киберугрозам и опасностям; *функция нормативного обеспечения*, реализуется

через определение целей модели, принципов и условий ее реализации; *функция методического обеспечения*, основанная на обосновании необходимого педагогического сопровождения процесса кибербезопасности обучающихся образовательных организаций; *диагностическая функция* направлена на выявление уровней сформированности знаний и умений по противодействию киберугрозам [58].

В рамках нашего моделирования предложенная модель педагогического сопровождения обучающихся в условиях киберрисков и киберугроз раскрывает авторское видение взаимосвязи компонентов, средств сопровождения, педагогических условий как целостной системы по противодействию обучающимися киберрискам и киберугрозам.

Модель имеет прогностический характер и в тоже время отражает реальные проблемы образовательного процесса по формированию кибербезопасности обучающихся на основе предложенного комплекса педагогического сопровождения.

Моделирование процесса педагогического сопровождения обучающихся в условиях киберрисков и киберугроз прослеживается в следующей логической последовательности:

1. Определение целей и задач, методологии и структуры педагогического сопровождения.

2. Определение оптимальных педагогических условий реализации модели, соотнесение цели, задач и желаемого результата.

3. Создание и апробация диагностического инструментария для решения научной проблемы.

Модель педагогического сопровождения обучающихся в условиях киберрисков и киберугроз состоит из: мотивационно-целевого блока, теоретико-методологического, содержательно-процессуального и оценочно-результативного блоков [Рисунок 1].

Мотивационно-целевой блок педагогического сопровождения обучающихся в условиях киберрисков и киберугроз является основным системно-образующим компонентом, определяющим потребности общества и образовательных организаций в противостоянии киберугрозам и опасностям обучающихся в Интернет-сетях. Цели задают определенную направленность компонентам модели, с учетом создание условий для достижения конечных результатов.

На основе теоретического анализа и изучения различных аспектов педагогического сопровождения образовательного процесса мы определили, что стратегическая цель обеспечивала формирование навыков обучающихся по противостоянию киберрискам и киберугрозам, а тактические и оперативные цели предполагали освоение субъектами основ информационной кибербезопасности.

Достижение данных целей предполагает: формирование потребностей в овладении обучающимися комплексом знаний и умений, овладение способами противостоящие киберугрозам и киберрискам, развитие навыков рефлексии.

Теоретико-методологический блок представлен в модели методическими подходами и принципами. К методологическим подходам педагогического сопровождения обучающихся образовательных организаций мы отнесли: системный, деятельностный, личностно-ориентированный и рефлексивный.

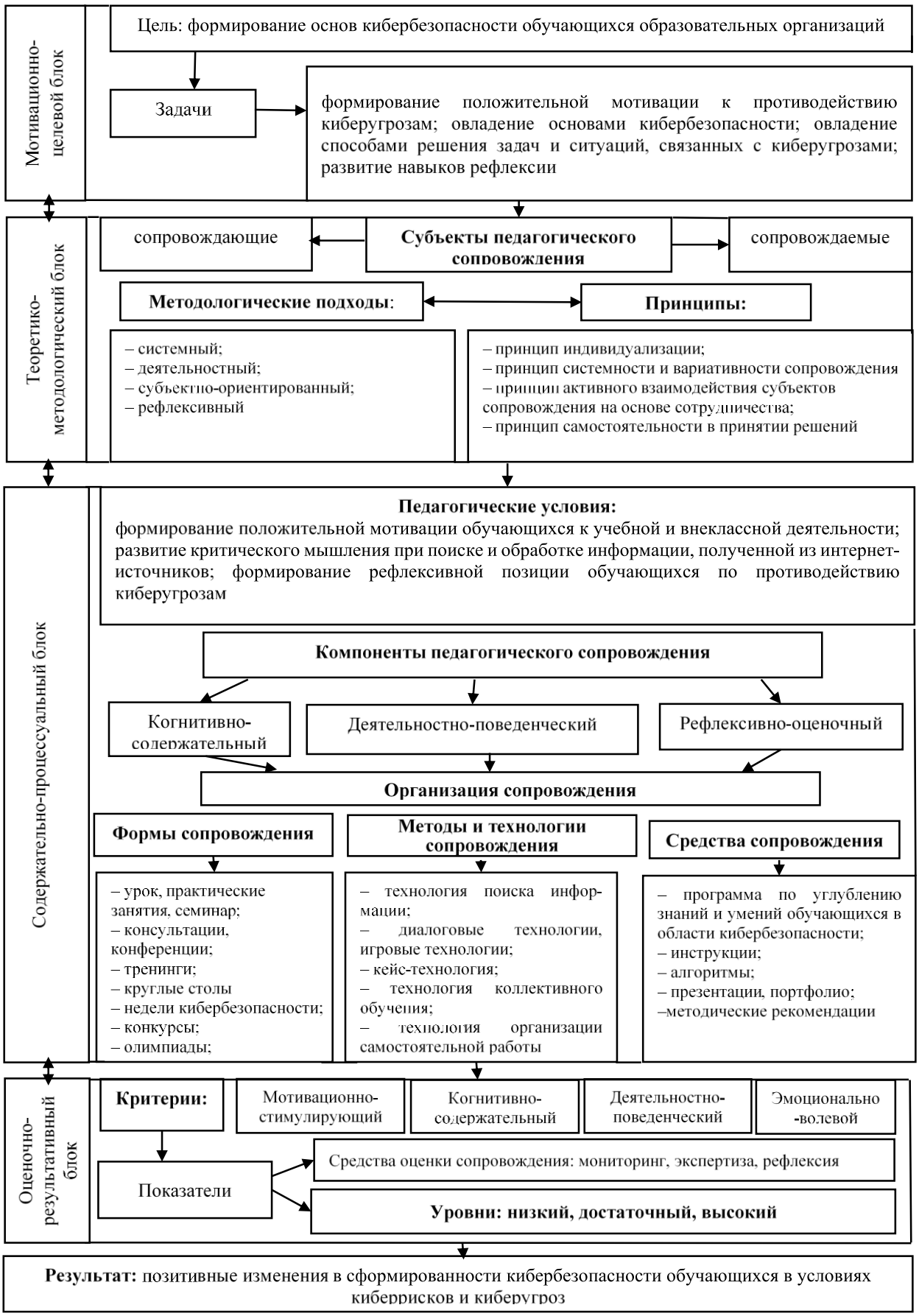


Рисунок 1. Модель педагогического сопровождения обучающихся в условиях киберрисков и киберугроз

В общепринятом понимании понятие «подход» предполагает устойчивую методологическую ориентацию личности при осуществлении своих действий в процессе познания, побуждающий к использованию определённой совокупности взаимосвязанных понятий, идей, способов, приемов и методов [31, 161].

Системный подход в педагогике рассматривается как организованный процесс передачи и усвоения социального опыта; процесс взаимодействия педагога и обучающегося в рамках педагогической системы. В научной литературе системный подход рассматривается как одно из направлений в методологии научного познания, основанное на рассмотрении объекта как системы, то есть комплекса взаимосвязанных элементов. Для системного подхода характерно целостное рассмотрение определенной совокупности элементов, компонентов, объектов. Базовым понятием системного подхода является понятие «система», которое, по мнению Т.А. Ильиной, представляет собой «выделенное на основе определенных признаков упорядоченное множество взаимосвязанных элементов, объединенных общей целью функционирования и единства управления выступающих во взаимодействии со средой как целостное явление» [76, С. 157].

В практике массовой школы до недавнего времени выделялись две системы: дидактическая и методическая. Первая относилась исключительно к учебному процессу, в то время как вторая направлена на разъяснение методов и технологий педагогами и воспитателям [85]. Многие ученые к основным элементам педагогической системы относят: цели, содержание, формы, методы и средства обучения и воспитания. Для педагогической системы установлены общие свойства: гибкость, динамичность, вариативность, адаптивность, целостность, прочность [142]. Основными принципами системного подхода являются принцип конечной цели; принцип целостности; принцип связанности элементов; принцип модульного построения; принцип иерархии; принцип развития. Системный подход в педагогике позволяет выделить, изучить и проанализировать элементы педагогической системы как единого целого.

Мы предлагаем рассматривать систему педагогического сопровождения по формированию кибербезопасности обучающихся образовательных организаций с позиции: проблема сопровождающий – сопровождаемый.

Деятельностный подход. Считается, что деятельность является основой, средством и решающим условием развития личности так как выступает в роли практической направленности, способствующей определению механизмов и процедур организации процесса в образовательной организации по противостоянию обучающимися киберрискам и киберугрозам [140]. Принципами деятельностного подхода являются: принцип сотрудничества; принцип субъектности; принцип самостоятельности.

*Субъектно-ориентированный подх*од предполагает естественный процесс саморазвития личности, опору на обучающегося на основе создания оптимальных условий для самореализации, самоанализа и самооценки уровня сформированности знаний и умений в области кибербезопасности.

Теоретической основой построения ориентированного образовательного процесса, по мнению Э.Ф. Зеера, является признание субъектности, где основными ценностями является саморазвитие и самореализация [69]. Субъектно-ориентированный подход подразумевает незаметное, ненавязчивое сопровождение процесса по формированию кибербезопасности обучающихся. Необходимым и достаточным основанием для реализации субъектно-ориентированного подхода является создание условий для личностного развития обучающихся; индивидуализация обучения при реализации поставленных задач; целесообразность использования информационных и коммуникационных средств развития.

Рефлексивный подход, основанный на положении о том, что представляет собой взаимодействие субъектов обучения, при котором учитываются личностные качества обучающихся, необходимые для формирования и развития рефлексивных умений и навыков. Основными особенностями рефлексивного подхода к формированию навыка по противостоянию обучающимися кибербезопасностям и киберугрозам являются: понимание сущности киберрисков и киберугроз для

личности обучающегося; целенаправленное противодействие кибербезопасности; мотивация предстоящей деятельности; прогнозирование последствий, исходящих из Глобальной сети; готовность обучающихся к противодействию киберугрозам.

А.С. Доколин предложил следующие принципы рефлексивного подхода: принцип самоопределения; принцип самореализации; принцип самоконтроля [58, С. 46-47].

К основным принципам педагогического сопровождения по формированию у обучающихся основ кибербезопасности мы отнесли:

1. *Принцип индивидуализации* предусматривает, что сопровождение со стороны педагога должно оказывать поддержку сопровождающего в соответствии с его потребностями при формировании системы знаний и умений в области кибербезопасности, а также обеспечения самореализации обучающихся в процессе их противостояния киберрискам и киберугрозам.

2. *Принцип системности и вариативности сопровождения* предполагает, что сопровождающий должен оказывать постоянную помощь и поддержку сопровождающему, используя различные практические способы и приемы по противодействию негативным последствиям, исходящим из сети Интернет.

3. *Принцип активного взаимодействия субъектов сопровождения* на основе сотрудничества предусматривает, что действия обучающихся по противостоянию киберугрозам будет более эффективной, если применить технологии сотрудничества в виде малых групп или работы в парах, которые позволяют анализировать и коллективно обсуждать проблемы, обосновать свою точку зрения на решение конкретных ситуаций.

4. *Принцип самостоятельности в принятии решений,* направленных на обеспечение условий для формирования самостоятельных действий обучающимися в различных ситуациях для осуществления оперативного принятия решений в зависимости от вида киберугроз и характера его воздействия на личность обучающегося.

Содержательно-процессуальный блок представлен в модели компонентами, средствами сопровождения и педагогическими условиями.

К основным компонентам педагогического сопровождения обучающихся образовательных организаций мы отнесли: когнитивно-содержательный, деятельностно-поведенческий и рефлексивно-оценочный.

Когнитивно-содержательный компонент, направленный на формирование системы знаний в области информационной и кибербезопасности. Данный компонент предполагает: наличие у обучающихся знаний об источниках внешних и внутренних угроз, связанных с кибербезопасностью; ознакомление с основными видами киберугроз и правилами поведения в сети Интернет, способами противостояния при встрече с ними; обоснование негативного влияния следствие киберугроз на физическое и психологическое состояние подростков, снижение уровня духовного и нравственного потенциала личности.

Деятельностно-поведенческий компонент рассматривается в двух аспектах: деятельность сопровождающего и деятельность сопровождающегося. Деятельность сопровождающего заключается в оказании консультативной помощи и поддержки обучающегося при формировании практических умений и навыков, необходимых обучающимся для противодействия киберугрозам. В данном случае сопровождающий выступает в роли коуча, тьютора, консультанта. В свою очередь, деятельность сопровождаемого предполагает освоение способов противостояния киберугрозам и выработки умений безопасного взаимодействия в сети Интернет в процессе поиска, копирования и обмена информацией.

Рефлексивно-оценочный компонент тесно взаимосвязан с когнитивно-содержательным и деятельностно-поведенческим. Данный компонент позволяет определить цель учебной деятельности, осознать свою индивидуальность и уникальность, обеспечить анализ и результаты собственной деятельности и определить способы коррекции этих действий. Вместе с тем, с помощью рефлексии вырабатываются умения контроля и самоконтроля действий обучающимися в том

числе и осуществления контроля собственного эмоционального состояния, эмоциональных реакций на негативные процессы.

В содержательно-процессуальный блок входит и *организация педагогического сопровождения по формированию знаний и умений обучающихся* образовательных организаций в области кибербезопасности, представленная формами, технологиями и средствами, направленными на противодействие вовлечению подростков в различные виды кибербезопасностей и рисков. К основным формам, применяемым как в процессе учебной, так и внеурочной деятельности мы отнесли консультации, дискуссии, тренинги, недели кибербезопасности, классные часы, викторины, конкурсы, олимпиады, а также круглые столы с участием обучающихся. В качестве педагогических технологий, способствующих развитию личностных качеств обучающегося по противодействию киберугрозам мы предлагаем: технологию поиска информации, технологию портфолио, кейс-технологию, технологию коллективного обучения, технологию организации самостоятельной работы.

Средствами поддержки обучающихся для решения учебных задач и проблемных ситуаций по кибербезопасности являются: инструкции и алгоритмы, презентации, портфолио, методические рекомендации.

Оценочно-результативный блок выполняет оценочную функцию. Данный блок представлен в модели критериями, показателями и уровнями сформированности противодействия обучающимися кибербезопасностям. К основным критериям мы отнесли: мотивационно-стимулирующий, когнитивно-содержательный, деятельностно-поведенческий и эмоционально-волевой.

При выборе показателей сформированности кибербезопасности у обучающихся образовательных организаций мы учитывали: автономность показателей; их достоверность; надежность, релевантность [58]. К уровням противодействия киберугрозам обучающимися, мы отнесли низкий, достаточный, высокий. Данные уровни характеризуют степень сформированности кибербезопасности обучающимися по противостоянию киберугрозам и киберрискам.

Таким образом, представленная модель характеризуется целостностью и системностью, так как ее блоки взаимосвязаны и отражают все процессы, которые направлены на формирование у обучающихся способов и приемов по противодействию киберрискам и киберугрозам.

2.2. Организация педагогического сопровождения по формированию кибербезопасности обучающихся общеобразовательных организаций

Современное информационное пространство создает новые проблемы для развития личности обучающегося, так как сама информация часто носит противоречивый, а иногда и агрессивный характер, негативно влияющая на подростков. Развитие личности обучающегося в условиях информационного пространства основана на идеях гуманистической педагогики, главной целью которой является самоактуализация личности на основе осознания обучающимися особенностей собственного отношения к миру и себя в этом мире. Гуманизация педагогического процесса предъявляет значительные требования как к педагогу, так и к обучающемуся. В связи с этим, К. Роджерс считает, что:

– личность находится в центре постоянно меняющегося мира. У каждой личности есть свой собственный мир, через который она воспринимает окружающую действительность;

– личность воспринимает окружающую действительность через призму собственных установок и понимания;

– личность стремится к самопознанию и самореализации, имеет внутреннее стремление к самосовершенствованию;

– развитие и самосовершенствование происходят на основе взаимодействия с окружающей средой и другими людьми [66, с. 39].

Анализ исследований, касающихся педагогического сопровождения различных аспектов деятельности педагога, в том числе и по кибербезопасности обучающихся выявил, что акцент делается на взаимодействие сопровождаемого и сопровождающих в процессе урочной и внеурочной деятельности [Рисунок 2].

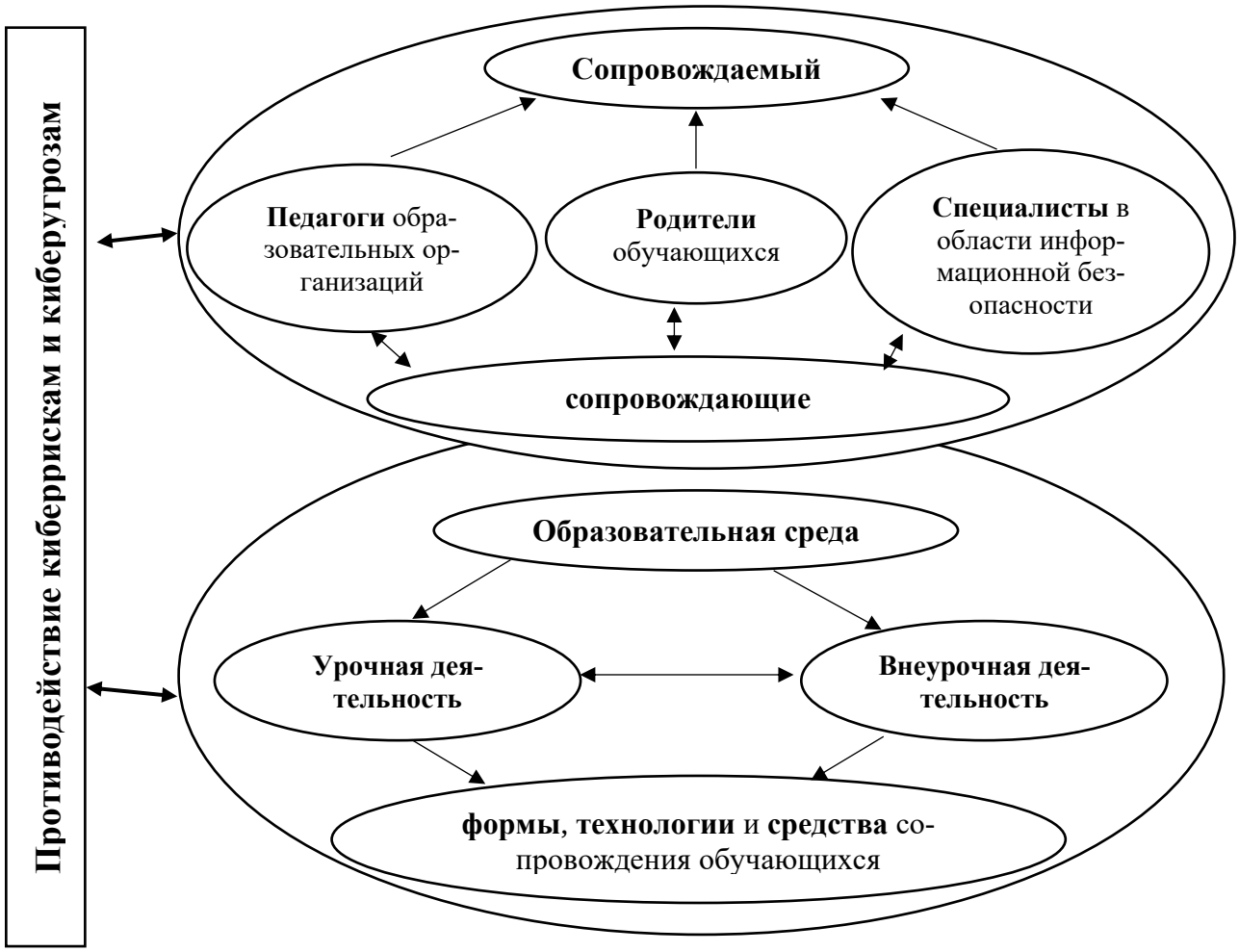


Рисунок 2. Организация педагогического сопровождения обучающихся общеобразовательных учреждений по противодействию киберрискам и киберугрозам

По нашему мнению, целесообразным является разработка аспектов сопровождения, связанных с обеспечением субъектной позиции обучающегося и индивидуализации педагогического сопровождения. С этой целью мы анализировали: какие специфические средства педагогического сопровождения будут эффективными в процессе учебной и воспитательной работы используемой педагогами; какие организационные формы целесообразно применять при формировании кибербезопасности обучающихся; какие методы и приемы будут способствовать результативной организации взаимодействия субъектов сопровождения; какая поддержка необходима обучающимся при поиске учебной информации при выполнении домашних заданий; какие затруднения испытывают обучающиеся при противостоянии киберугрозам.

Для противодействия различным киберрискам и киберугрозам необходим комплекс мер проводимых образовательными организациями в процессе учебной и внеурочной деятельности, а также при взаимодействии образовательных организаций с родителями обучающихся с организациями в области кибербезопасности, а также при оказании информационной и консультативной поддержки педагогами обучающихся [Таблица 1].

Таблица 1

Виды и содержание деятельности по формированию кибербезопасности обучающихся

Виды деятельности	Содержание деятельности	Дидактическое обеспечение
Учебная деятельность	– ознакомление с законодательной базой в области кибербезопасности; – формирование системы знаний обучающихся по основам кибербезопасности; – интеграция теоретической информации и навыков поведения обучающихся для защиты личностных данных в Глобальной сети; – использование способов и приемов интерактивного обучения при создании и решении ситуационных задач, связанных с кибербезопасностью.	– учебные кейсы по основам кибербезопасности; – инструкции по правилам поведения в интернете; –алгоритмы создания ситуационных задач; –методические рекомендации по применению интерактивных методов и технологий обучения.
Внеурочная деятельность	– углубление знаний в области киберугроз и рисков во внеурочное время; – участие обучающихся в различных организационных формах внеурочной работы по кибербезопасности; –совершенствование навыков по противостоянию киберугроз в процессе самостоятельной практической деятельности.	– алгоритмы подготовки обучающихся к участию в коллективных и групповых формах внеурочной деятельности по кибербезопасности; –инструкции по выполнению практических заданий, связанных с поведением обучающихся в киберпространстве; –методические рекомендации по принятию решений в ситуации встречи с киберугрозой.

Продолжение Таблицы 1

1	2	3
Взаимодействие образовательных организаций с организациями в области кибербезопасности	– использование диалогового общения с целью углубления знаний, умений и навыков по защите от информационных угроз; – проведение тренингов по противостоянию киберугроз и рисков	– памятки поведения обучающихся при использовании программного обеспечения; – рекомендации по сохранению психического и физического здоровья обучающихся; – инструкции по проведению различного рода тренингов в области кибербезопасности.

Таким образом, педагогическое сопровождение формирования кибербезопасности обучающихся включает в себя приобретение базовых знаний в области кибербезопасности, выработки комплекса умений по противодействию киберугрозам на основе ознакомления с законодательными актами в данной отрасли, изучении инструкций, алгоритмов действий, связанных с оказанием сопротивления негативному воздействию информационной среды. Важную роль в решении проблемы отводится созданию и решению ситуационных задач, связанных с киберугрозами.

В свою очередь, внеурочная деятельность предполагает углубление знаний обучающихся в области кибербезопасности через организацию коллективных и групповых форм педагогического сопровождения, участия в обсуждении возникших проблем. С этой целью использовались дискуссионные методы, стимулирующие познавательный интерес обучающихся, обеспечивающие переосмысление принятых решений по противодействию киберугроз и опасностей. Обоснованные виды деятельности по противодействию опасностям и киберугрозам позволяют педагогам обеспечить подростков знаниями, связанными с цифровой грамотностью кибербезопасности, а учитывая возрастные особенности, влиять на их поведение в киберпространстве. Противодействию рискам и киберугрозам способствует и взаимодействие образовательных организаций с организациями в области кибербезопасности через проведение разъяснительной работы среди обучающихся о причинах и последствиях киберугроз, организацию учебных тренингов по противодействию опасностей в киберпространстве, ознакомление

обучающихся с инструкционной информацией о правилах поведения в экстремальных ситуациях [Приложение 2].

В ходе учебной и воспитательной деятельности педагога по формированию основ кибербезопасности обучающихся формируются мораль и нравственность школьников через урок, воспитательное мероприятие. Урок является основной организационной формой в образовательных организациях. По мнению М.Н. Скаткина и других ученых [142, 169, 170], в уроке концентрируется если не вся, то значимая часть педагогики. Основные показатели современного урока представлены в таблице 2.

Таблица 2

Основные характеристики урока

Показатели эффективности урока	**Действия сопровождающих**	**Действия сопровождаемых**
1	2	3
Высокий уровень учебно-воспитательных результатов	– использование комплекса педагогической поддержки сопровождаемых в процессе урока	– овладение глубокими и прочными знаниями и умениями в области кибербезопасности
Высокий уровень познавательной активности обучающихся	– развитие творческого потенциала обучающихся; – применение оптимальных интерактивных форм, методов и технологий; – формирование критического мышления обучающихся	– формирование и развитие познавательных интересов, стремление к активному мыслительному процессу; – творческий поиск решения познавательных задач; – применение нравственно-волевых усилий на достижение поставленных целей и задач
Высокий уровень самостоятельности обучающихся в процессе учебно-познавательной деятельности	– организация процесса по выполнению обучающимися различного рода самостоятельных работ	– способность к самостоятельному принятию решений по противодействию киберугрозам
Высокий уровень индивидуализации процесса обучения	– создание условий для выполнения обучающимися индивидуальных заданий; – чередование методов, методических приемов и способов решения обучающимися учебных задач; – исполнение функций консультанта, тьютора, коуча	– выполнение заданий в соответствии с интеллектуальными возможностями; – использование инструктивной информации и учебных кейсов при выполнении самостоятельных работ

Продолжение Таблицы 2

1	2	3
Высокий уровень коммуникативной культуры	– создание условий для результативного субъект-субъектного взаимодействия на уроке; – использование диалоговых методов в виде эвристической беседы, деловых игр, мозгового штурма и др.	– участие в обсуждении способов решения проблемных ситуаций; – участие в решении учебных задач в виде игры, обсуждения способов решения учебных задач и ситуаций
Высокий уровень обеспечения визуализации учебного содержания	–предоставление обучающимся учебной информации с использованием медиасредств; – демонстрация сложных явлений и процессов с дополнительными комментариями педагога	– анализ предлагаемой визуализации явлений и процессов; – обоснование конкретных действий, представленных в виде презентаций, видеозаписей

С целью активизации учебно-познавательной деятельности обучающихся и развития у них творческого и критического мышления мы использовали такие активные формы сопровождения как: игровые уроки, уроки, построенные на разборе конкретных ситуаций, уроки консультация-диалог.

Результативность проведения игрового урока зависит от методической подготовленности педагога к организации и управлению игровой деятельностью. На организационном этапе происходит ознакомление обучающихся с целями, задачами, со сценарием и основными этапами игры и критериями оценивания каждого из этапов, распределение обучающихся на команды, выбор капитанов команд. Основной этап предполагает работу команд над предложенными заданиями, в том числе: анализ предложенных заданий в выдвижение гипотезы по их реализации, доказательство фактов, явлений в процессе дискуссии, выбор оптимальных средств при выполнении практических действий; активное участие в обсуждении альтернативных способов действий. Заключительный этап игры предполагает работу экспертов по результатам каждого этапа игры, обобщения командных зачетов. В данном случае педагог выполняет функцию коуча, модератора [134].

Мозговой штурм, как разновидность игры–дискуссии, направленный на развитие критического мышления обучающихся в процессе решения актуальных

задач по противодействию киберугрозам, исходящих с сайтов с негативной информацией, формирование аналитических умений, связанных с поиском, анализом, обобщением большого потока учебной информации.

Уроки, построенные на разборе конкретных ситуаций, в нашем случае по противодействию обучающимися киберугрозам, предполагает интеграцию содержания теоретического материала с самостоятельным решением проблемных ситуаций. С этой целью используются фронтальная форма для изложения теоретического материала, групповая или индивидуальная организационные формы для выполнения самостоятельных заданий обучающимися.

Результативному решению ситуаций и задач способствует выбор оптимальных методов обучения, то есть такой деятельности педагогов, которая обеспечит достижение нужных результатов в максимально сжатые сроки.

С.И. Змеев акцентирует свое внимание на применение проблемных методов, которые направленные на поисковую деятельность, необходимую для решения конкретных задач, а также активные и интерактивные методы с применением компьютерных технологий [73].

Учеными установлено, что процесс усвоения знаний наиболее эффективно происходит в ходе решения проблемных заданий. Педагогические основы проблемного обучения разрабатывались И.Я. Лернером, Т.В. Кудрявцевым, А.М. Матюшкиным, М.И. Махмутовым, и др. [110, 102, 119, 120]. Л.М. Фридман утверждает, что проблемная ситуация и задача в структурном отношении одинаковы так как элементами проблемной ситуации являются реальный объект и реальный субъект действий, а частями задачи являются знаковые формы, в которых отображаются элементы проблемной ситуации [101].

Считается, что проблемная ситуация является основой проблемного обучения, поскольку она характеризует уровень развития критического мышления ребенка и способствует формированию его самостоятельности обучающегося, формированию убеждений и развитию коммуникативных навыков [101].

Еще одним способом взаимодействия с ребенком является *беседа,* В идеале, беседа должна иметь как заранее подготовленные вопросы и проходить в форме структурированного интервью, так и носить спонтанный характер. К преимуществам беседы можно отнести: обеспечение активной позиции обучающихся; включение в беседу многих обучающихся; с помощью беседы осуществляется проблемное решение учебной задачи.

Дискуссия, как средство педагогической поддержки сопровождаемых обеспечивает обмен мнениями, идеями, своей позицией и установками, в процессе интенсивной и продуктивной работы по решению учебных задач и проблемных ситуаций [88].

Урок консультация-диалог способствует активному обсуждению основных проблем, а в случае необходимости оказание консультативной помощи при выходе из сложных проблемных ситуаций, связанных с вопросами кибербезопасности.

Педагогическое сопровождение при проведении практических занятий предполагает:

– организацию выполнения практической работы обучающихся;

– оказание консультативной помощи и корректировки действий обучающихся в случае необходимости;

– организацию обсуждения результатов выполненных заданий;

– подведение общих и индивидуальных итогов по результатам выполнения практического занятия.

В процессе практических занятий решаются различные виды учебных задач. С позиции нашего исследования к основным задачам можно отнести спектр различных рисков киберпространства и способов поведения обучающихся при встрече с киберугрозами.

Для нашего исследования значимым был предложенный О.Н. Троицкой, О.Л. Безумовой и Т.С. Шириковой комплекс учебных задач по кибербезопасно-

сти с учетом возрастных особенностей обучающихся. Следует отметить, что уровень задач усложнялся для каждой возрастной категории: от осуществления покупок в инетрент-магазинах до раскрытия киберпреступлений [179].

В работе А.И. Лучинкиной, Т.В. Юдеевой по информационно-психологической безопасности авторами предложен еще один интересный вариант психолого-педагогического сопровождения процесса формирования безопасности поведения в виртуальном пространстве. Авторы используют игровые оболочки для вовлечения и мотивации школьников. Для каждой возрастной группы игровая оболочка учитывает особенности возраста: для школьников 1-4 классов – это сказка, для 5-6 классов – увлекательное приключение, квест. Для старшеклассников – детектив [112].

Следующей формой педагогического сопровождения по формированию кибербезопасности обучающихся являются семинары. По мнению А.В. Хуторского, с*еминар* обеспечивает обсуждение различного рода образовательных проблем в процессе коллективно-групповой коммуникации [А.В.Хуторской]. Семинары обеспечивают плюрализм мысли, которые выдвигаются участниками данного мероприятия во время обсуждения различных проблем; уяснения положительных результатов достижения или их недостатков; обсуждение актуальной информации, необходимой обучающимся для решения практических задач.

Значительное внимание в своем исследовании мы уделяли *семинарам-практикумам*, содержание которых предполагало не только обсуждение актуальных вопросов в области кибербезопасности, но и выполнение практических задач, связанных с проблемой противостояния киберугрозам.

При проведении данного мероприятия в 9-х классах в качестве консультантов принимали участие обучающихся 10-11-х классов, что способствовало не только передачи практического опыта менее опытным пользователям компьютерных операций, но и детальное объяснение практических действий в процессе тренинговых упражнений. С целью формирования практических навыков по

противодействию киберрискам и киберугрозам второй составляющей семинаров-практикумов является решение проблемных задач и ситуаций.

Консультация используется в образовательном процессе с целью ликвидации пробелов в знаниях, осуществляемых в форме самостоятельных индивидуальных ил групповых занятий учащихся. Применение консультаций обеспечивает преодоление трудностей в освоении учебного содержания отдельных тем, разделов программы, а также с целью оказания поддержки обучающимся в углубленном изучении дисциплины.

Тренинг. Ученые рассматривают тренинг как результативный метод педагогического сопровождения, так как он способствует овладению способами активного овладения действиями в практически условиях. Одним из достоинств тренинга является вовлечение всех участников в процесс взаимодействия. При проведении тренингов осуществляется развитие познавательной деятельности обучающихся через развитие памяти, внимания, мышления, формируется положительная мотивация к самопознанию и саморазвитию личности обучающегося [142].

К тренингам развития Е.Ф. Зеер относит: тренинги командной согласованности, тренинги рефлексии [194]. Целью тренинга командной согласованности является формирование межличностной сгруппированности коллектива, развития умений и навыков самоанализа, совершенствования процессов саморазвития и самосовершенствования. Тренинг рефлексии является способом развития личности, механизмом самопознания в процессе общения, в основе которого находится способность личности представлять, как она воспринимается партнером по общению. Целью данного тренинга является выявление результатов саморазвития и осознание сильных и слабых сторон своего поведения, деятельности в целом [194].

К организационным формам педагогического сопровождения формирования кибербезопасности обучающихся во внеурочной деятельности мы отнесли:

теоретические конференции, круглый стол, конкурсы, викторины, олимпиады, недели кибербезопасности.

Практиковалось проведение такой формы педагогического сопровождения как *теоретические конференции*, в которых принимали участие обучающиеся 9-11-х классов. Вопросы, выносимые на обсуждение, должны были способствовать теоретическому обоснованию проблем, информационной и кибербезопасности, причем участие в обсуждении данных проблем принимали все желающие обучающиеся.

В качестве примера предлагаем некоторые из тех проблем, которые были вынесены на обсуждение в процессе конференции:

– роль интенсивности негативного информационного воздействия на личность обучающегося;

– виды киберугроз исходящих из сети Интернет и их влияние на формирование духовно-нравственных ценностей подростков;

– виды информации, причиняющей вред здоровью и развитию детей;

– средства защиты и способы отражения возникающих киберугроз для обучающихся.

Круглый стол, как организационная форма, направлена на обсуждение проблем информационной и кибербезопасности обучающихся с целью поиска путей и способов совершенствования знаний и умений для противодействия киберугрозам и рискам.

В своем исследовании мы использовали следующие темы, выносимые на обсуждение круглых столов:

– проблемы, связанные с информатизацией общества и погружение молодежи в пространство Интернета;

– факторы, оказывающие негативное влияние информационно-коммуникационной среды на личность обучающегося;

– причины, влияющие на снижение духовно-нравственного потенциала обучающихся, исходящих от Глобальных сетей.

Проведение *недели кибербезопасности* предполагает комплекс мероприятий, в которые были вовлечены обучающиеся как одной, так и разных возрастных групп:

– классный час в виде лекции-игры «Кибербезопасность и «Я»» способствовала привлечению обучающихся к решению ситуаций, связанных с их поведением и действиями по противодействию киберугрозам;

– конкурс рефератов, эссе обучающихся под девизом «Безопасность в Интернете»;

– соревнование обучающихся в виде принятия оптимальных решений по предложенным нестандартным ситуациям в киберпространстве;

– проведение викторины «Прогулка в Интернете» на знание обучающихся правил поведения в Глобальных сетях;

– участие в тренинговых мероприятиях по совершенствованию практических умений обучающихся 9-х классов под руководством обучающихся 10-11-х классов под девизом «Наставник-модератор»;

– участие в теоретической конференции по результатам проведения кибернедели, в которой принимали участие педагоги, родители обучающихся, специалисты в области кибербезопасности, обучающиеся.

Достаточно значимыми для решения образовательных проблем, связанных с кибербезопасностью является использование в учебном процессе образовательных организаций интерактивных технологий, а именно: совместной проектной деятельности, квестов [142].

В качестве педагогического сопровождения формирования кибербезопасности обучающихся мы использовали субъектно-ориентированные технологии, в том числе: технология, связанная с поиском информации, технология портфолио, кейс-технология, технология коллективного обучения, технология организации самостоятельной деятельности обучающихся [Таблица 3].

Таблица 3

Субъектно-ориентированные технологии поддержки сопровождающего

Виды педагогических технологий	**Содержание поддержки сопровождающего**
Технология поиска информации	– сведение об объектах и явлениях окружающей действительности; – сведения о свойствах информации (актуальность, точность, достоверность, адресность, компактность, доступность, защищенность); – структура работы с информацией (источники информации, поиск информаций, анализ информации, представление информации); – виды работы с информацией (тезирование, реферирование, составление граф-схемы, разработка схем-таблиц)
Технология портфолио	– информационное портфолио (поиск, систематизация информации, поиск новой информации, подготовка информации к использованию, разработка инструктивной информации); – проблемно-ориентированное портфолио (учебное, научное, профессиональное, социальное); рефлексивное портфолио (анализ и оценка субъектом целей и результатов киберактивности, особенности работы с источниками информации); – портфолио развития критического мышления обучающихся на уровне анализа-оценивания-сравнивания; критерии оценивания (гибкость, рациональность, оригинальность мышления, способность решать практические проблемы, уровень сформированности самоконтроля и самооценки).
Кейс-технология	– представление учебной информации в виде текста, графики, таблиц, диаграмм; – представление учебной информации в виде мультимедиа; – работа над анализом и сравнением полученной информацией; – поиск необходимой дополнительной информации для решения учебной задачи; – определение рациональности используемой информации для решения конкретной ситуации.
Технология коллективного обучения	– работа с информацией в парах сменного характера; – работа с информацией в малых группах (изучение представленной информацией, взаимообмен знаниями и практическими умениями, обсуждение результатов выполненного задания); – применение метода микрообучения по формированию отдельных умений и навыков на основе представленной инструктивной информации.
Технология организации самостоятельной работы	– ориентация обучающихся на поиск учебной информации; – ориентация на поиск, анализ и обобщение основной и дополнительной информации; – структурирование учебной информации и ее использование для выполнения самостоятельной работы.

В таблице 4 представлены наиболее распространенные средства педагогического сопровождения по формированию кибербезопасности обучающихся.

Таблица 4

Средства педагогического сопровождения по формированию кибербезопасности обучающихся

Виды средств педагогического сопровождения	Деятельность сопровождающего	Деятельность сопровождаемого
Алгоритмы	Разработка алгоритмов по формированию первоначальных действий обучающихся, связанных с информационной безопасностью. Алгоритмы создания ситуационных задач. Алгоритмы подготовки обучающихся к участию в коллективных и групповых формах внеурочной деятельности по кибербезопасности.	Четкость и последовательность выполнения практических действий обучающихся на основе алгоритма действий.
Инструкции	Разъяснительная и рациональная практическая деятельность со стороны преподавателя. Демонстрация способов выполнения сложных практических действий. Поддержка обучающихся в нестандартных ситуациях.	Анализ содержания инструктивного материала по проведению различного рода тренингов. Самоубеждение в необходимости выполнения действий в соответствии с предложенной инструкцией. Изучение инструкций по правилам поведения в Интернете. Ознакомление с памятками поведения обучающихся при использовании программного обеспечения.
Методические рекомендации	Рекомендации по использованию различных приемов и способов, связанных с анализом ситуаций и поиском рациональных путей выхода из затруднительного состояния. Рекомендации по переключению действий обучающихся при решении сложных учебных задач	Ознакомление обучающихся с рекомендациями по противостоянию киберугрозам. Анализ ситуаций и поиск способов выполнения рациональных действий. Ознакомление с рекомендациями по сохранению психического и физического здоровья обучающихся.
Программы по углублению знаний обучающихся по кибербезопасности	Разработка содержания программы, нацеленной на углубление базовых знаний и навыков обучающихся в области информационной безопасности и кибербезопасности.	Анализ содержания знаний. Поиск наилучшего способа действий при встрече с киберугрозами. Решение обучающимися нестандартных учебных задач по кибербезопасности.

В настоящее время в Интернет-сетях предложены различные образовательные программы, направленные на формирование основ информационной и кибербезопасности. Одной из таких является программа по информационной безопасности, разработанная на основе ФГОС среднего и общего образования. Программа может быть реализована в рамках внеурочной деятельности в виде отдельных блоков – модулей. Преимущество программы в том, что подросток может выбрать эти модули самостоятельно. Каждый из них представляет собою аутентичный материал с логичной и завершенной структурой.

Для нас представляют интерес методические рекомендации для подростков, предложенные «Kaspercky Satekids». Рекомендации представлены в виде слайд-шоу, что дает возможность детям и их родителям быстрее схватить суть проблемы и прокачать навыки при работе в сети Интернет. Учитывая индивидуальные особенности школьников и уровень их подготовленности к использованию ИКТ, нами были разработаны инструкции и алгоритмы действий для пользователей ИКТ в различных ситуациях.

С.Н. Вангородским представлен перечень небезопасных интернет-сервисов для детей [37]:

– сервисы, пропагандирующие нездоровые сексуальные отношения;

– сервисы, предполагающие общение ребенка в виртуальном мире, что зачастую влияет на общение со сверстниками;

– сервисы с онлайн-играми, когда после длительного участия в игровой деятельности ребенку трудно приспосабливаться к реальным отношениям со сверстниками;

– сервисы, распространяющие информацию о терроризме, сектантстве, фашизме;

– сервисы с азартными играми, которые пагубно сказываются на психике ребенка [37].

Достаточно важным фактором, влияющим на формирование кибербезопасности обучающихся, является взаимодействие между педагогом и родителями обучающегося образовательных организаций. Формами педагогического сопровождения, связанного с нормативно-правовым просвещением родителей по проблемам кибербезопасности являются консультации, родительские собрания, круглые столы, участие родителей в неделях кибербезопасности и других мероприятиях.

Выводы по Главе 2

Предложенная модель педагогического сопровождения обучающихся в условиях киберрисков и киберугроз, раскрывает авторское видение содержания, форм, технологий и средств педагогического сопровождения, комплекса педагогических условий, оценки результативности уровней сформированности кибербезопасности обучающихся. Модель рассматривается как целостная система, состоящая из: мотивационно-целевого (цели и задачи); теоретико-методологического (методологические подходы и принципы); содержательно-процессуального и оценочно-результативного (критерии, показатели, уровни) блоков; рассматриваемого как компонентов педагогического сопровождения (когнитивно-содержательного, деятельностно-поведенческого, рефлексивно-оценочного); организации сопровождения, включающего комплекс форм, технологий и средств поддержки, способствующих результативному формированию кибербезопасности обучающихся.

Модель реализует основную идею исследования, которая заключается в том, что повышению результативности педагогического сопровождения обучающихся в условиях киберрисков и киберугроз зависит от создания условий для личностных преобразований, формирования субъектного и рефлексивного опыта.

Формирование кибербезопасности обучающихся образовательных организаций способствует результативная организация учебно-воспитательного процесса, на основе применения интерактивных форм, технологий и средств педагогического сопровождения.

В ходе исследования было выявлено, что основными формами педагогического сопровождения формирования кибербезопасности обучающихся являются различные типы уроков, практические занятия, семинары, тренинги. К формам педагогического сопровождения внеурочной деятельности относятся: недели кибербезопасности, круглые столы, конкурсы, олимпиады, теоретические конференции, классные часы и др. Все это направлено на формирование кибербезопасности обучающихся общеобразовательных организаций.

ГЛАВА 3. ОПЫТНО-ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО ФОРМИРОВАНИЮ КИБЕРБЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ В УСЛОВИЯХ КИБЕРРИСКОВ И КИБЕРУГРОЗ

3.1. Программа и методика организации педагогического эксперимента

Педагогический эксперимент проводился на базе образовательных организаций общего образования г. Симферополь, обучающимися предпрофессиональных классов на базе ГБОУ ВО РК «Крымский инженерно-педагогический университет имени Февзи Якубова».

На этапе констатирующего эксперимента нами были разосланы приглашения в реальном и виртуальном пространстве к участию в эксперименте, направленном на изучение отношения к угрозам киберпространства.

В результате проделанной работы к участию в эксперименте дали согласие 412 человек (разослано приглашений – 650). Эти респонденты и принимали участие в констатирующем эксперименте.

Теоретический анализ проблемы исследования позволил выделить основные критерии сформированности навыков кибербезопасности обучающихся: мотивационно-стимулирующий, когнитивно-содержательный, деятельностно-поведенческий, эмоционально-волевой.

В рамках каждого критерия нами были отмечены основные показатели, определяющие уровень его сформированности. Так, мотивационно-стимулирующий критерий описывается показателями понимания социальной и личностной значимости кибербезопасности; стимулирования поведения обучающихся к соблюдению информационной безопасности; сформированностью мотивов по противодействию подростков киберугрозам и киберрискам; проявлением у обучающихся интереса к информационной безопасности. Когнитивно-содержательный критерий включает знания в области кибербезопасности; – знания обучающихся о методах и средствах противостоянию киберугрозам и киберрискам; ценностные ориентации по противодействию кибербезопасности.

К деятельностно-поведенческому критерию относятся умения по соблюдению информационной этики; аналитические умения по отбору информации; творческая активность при решении проблемных ситуаций; критическое мышления обучающихся при выборе способов противостоянию киберугрозам; способы защиты при встрече с киберугрозами и рисками; системность и гибкость использования теоретических знаний; – умение находить причинно-следственные связи и обосновывать практические действия.

Эмоционально-волевой критерий основывается на рефлексивной позиции обучающихся по противодействию киберугрозам; самооценкой волевых качеств подростками с подключением механизмов самоанализа, самопознания и самоконтроля; уровнем саморегуляции подростка в интернет-пространстве.

Проведенный теоретический анализ научной литературы по проблеме исследования позволил сформировать эмпирическую модель исследования [Таблица 5] и обозначить его задачи.

Таблица 5

Эмпирическая модель диагностики кибербезопасности обучающихся

Критерии	Измеряемые показатели	Методики
1	2	3
Мотивационно-стимулирующий	понимание социальной и личностной значимости кибербезопасности, проявление у обучающихся интереса к информационной безопасности	Опросник «Риски в киберпространстве» (авторский)
	стимулирование поведения обучающихся к соблюдению информационной безопасности	Дилеммы в интернет-пространстве (авторская)
	сформированность мотивов по противодействию подростков киберугрозам и киберрискам	Фокус-группы по выявлению мотивов противодействия киберугрозам и киберрискам
Когнитивно-содержательный	уровень сформированности знаний в области кибербезопасности	Опросник инструментальных навыков в области кибербезопасности (авторский)
	уровень знаний обучающихся о методах и средствах противостоянию киберугрозам и киберрискам	
	уровень сформированности ценностных ориентаций по кибербезопасности	Ассоциативные ряды

Продолжение Таблицы 5

1	2	3
Деятельностно-поведенческий	уровень сформированности умений по соблюдению информационной этики	Опросник на знание информационной этики
	уровень развития критического мышления обучающихся при выборе способов противостоянию киберугрозам, уровень сформированности аналитических умений по отбору информации	Опросник определения уровня критического мышления (Методика Ю.Ю. Гущина)
	уровень развития творческой активности обучающихся в противостоянии киберугрозам и выбора способов защиты при встрече с киберугрозами и рисками	Самоотчеты, сочинения «Я знаю как…»
Эмоционально-волевой	уровень сформированности рефлексивной позиции по противодействию киберугрозам	Методика определения самооценки (Дембо-Рубинштейн), самоотчеты

Как видно с таблицы 5, часть анкет и методик является авторскими. Так, при изучении мотивационно-стимулирующего критерия кибербезопасности обучающихся выявилась недостаточность доказательного диагностического инструментария. В связи с этим нами была разработан опросник «Риски киберпространства». Целью опросника является выявление группы рисков, к которым склонен подросток и определение уровня сформированности у подростка способов защиты. В основу опросника положена типология рисков киберпространства, предложенная О.С. Рыбаковой. Исследовательница выделила три группы рисков:

1. Риски, связанные с получением деструктивной информации. К ним относятся:

– разжигание вражды, ненависти и насилия;

– ложная информация;

– посягательства на доброе имя, честь и достоинство;

– непристойная информация;

– информация, оказывающая деструктивное воздействие на здоровье людей.

2. Риски, связанные с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет. К ним относятся:

– кибербуллинг;

– деятельность экстремистских сообществ;

– популяризация и распространение способов деструктивного поведения;

– пропаганда самоповреждающего (анорексия, селфхарм) и суицидального поведения;

– целенаправленное распространение негативного поведения онлайн и призыв к асоциальному поведению офлайн [37, 182].

3. Риски для несовершеннолетнего самому стать жертвой правонарушений (преступлений) [86].

По каждому типу рисков был составлен ряд утверждений, которые нужно было оценить по пятибалльной шкале: нет; скорее нет, чем да; иногда; скорее да, чем нет; да. Респондентам предлагалась инструкция по оценке каждого утверждения по пятибалльной шкале (нет; скорее нет, чем да; иногда; скорее да, чем нет; да).

Опросник «Риски киберпространства»

№ п/п	Утверждение	нет	скорее нет, чем да	иногда	скорее да, чем нет	да
1	2	3	4	5	6	7
1.	Я поддерживаю мнения людей, которые призывают в Сети к очищению страны от приезжих и иноверцев					
2	Не вижу ничего зазорного в проявлении ненависти к кому-либо в постах и комментариях					
3.	Я могу написать негативный пост или комментарий о личных качествах человека, который мне не нравится					
4.	Я считаю нормальным распространение сцен секса, сексуального насилия в Сети или описания этих эпизодов.					
5.	Мне нравится сообщать в Сети информацию, которая вызывает страх у моих подписчиков					
6.	Мне приходилось быть жертвой травли в Сети					
7.	Я просматриваю страницы сообществ с экстремистскими взглядами					

1	2	3	4	5	6	7
8.	Я интересуюсь информацией о способах совершения преступлений или самоубийства					
9.	Мне интересны сообщества, где можно получить информацию о селфхарме, анорексии и др.					
10.	В Сети любое поведение, даже призывы к нарушению закона, правильное.					
11.	О систематических оскорблениях в Сети в свой адрес я сообщаю взрослым (родителям, педагогам)					
12.	О предложениях к встрече от незнакомых людей в Сети я сообщаю взрослым (родителям, педагогам)					
13.	Я не сообщаю свои персональные данные и своих близких по просьбе в Сети или по телефону					
14	Если меня шантажируют фотографиями или текстами, размещенными мною ранее с Сети, то я сообщаю об этом взрослым (родителям, педагогам)					
15.	Если мне предлагают участие (оплачиваемое или неоплачиваемое) в митингах, съемках фильма, акциях, то я сообщаю об этом взрослым (родителям, педагогам)					

Как видно из текста опросника первые 10 утверждений позволяют выявить отношение подростка к рискованным мероприятиям в Сети, а последние 5 утверждений направлены на выявление способов противодействия этим рискам и угрозам [Приложение 3].

В апробации опросника принимали участие 243 учащихся 9 классов г. Симферополя. В ходе апробации нами была проверена валидность и надежность опросника [Приложения 4, 5].

На основе кривой распределения нами были выявлены достоверные значения для каждой из шкал.

Таблица 6

Результаты изучения кривой распределения ответов

Шкала/уровень	Номера утверждений	Низкий уровень	Достаточный уровень	Высокий уровень
Риски, связанные с получением деструктивной информации	1, 2, 3, 4, 5	0-6	7-13	14-20
Риски, связанные с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет	6, 7, 8, 9, 10	0-6	7-13	14-20
Осознание рисков киберпространства	11, 12, 13, 14, 15	0-6	7-13	14-20

Низкий уровень рисков, связанных с получением деструктивной информации, соответствует подростку, который проверяет полученную информацию по разным источникам. Средний уровень рисков, связанных с получением деструктивной информации, соответствует подростку, который эпизодически проверяет полученную информацию по разным источникам. Высокий уровень рисков, связанных с получением деструктивной информации, соответствует подростку, который принимает на веру всю информацию в интернет-пространстве, включается в нее и следует предписаниям незнакомых людей.

Низкий уровень рисков, связанных с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет, предполагает устойчивость подростка к влиянию сообществ и отдельных людей на его поведение и мысли. Средний уровень рисков, связанных с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет, предполагает средний уровень устойчивости подростка к влиянию сообществ и отдельных людей на его поведение и мысли. Высокий уровень рисков, связанных с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет, предполагает подверженность подростка влиянию сообществ и отдельных людей на его поведение и мысли.

Осознание рисков киберпространства связано с поиском выхода из ситуации и привлечении взрослых к решению проблемы.

Склонность к рискам киберпространства рассчитывалась путем сложения результатов следующим образом: **Склонность к рискам киберпространства** = ∑ Риски, связанные с получением деструктивной информации +∑ Риски, связанные с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет -∑ Осознание рисков киберпространства

Склонность к рискам киберпространства также в процессе апробации оказалась трехуровневой: низкий уровень – 0-14 баллов. Подросток не склонен к рискованным действиям в киберпространстве; средний уровень – 15-29 баллов. Подросток иногда склонен к рискованным действиям в киберпространстве; высокий уровень – 30-40 баллов. Подросток направлен на рискованные действия в киберпространстве.

Таким образом, результаты по предложенным методикам и анкетам дают представление об уровне сформированности мотивационно-стимулирующего критерия.

Для изучения сформированности мотивов по противодействию подростков киберугрозам и киберрискам нами проводились фокус-группы. Для участия в фокус-группе в соответствии с целями были приглашены подростки 9-х классов с учетом пропорционального представительства по следующим параметрам: пол, возраст. Такой подход обеспечил репрезентативность выборки.

Респондентам предлагались следующие вопросы для обсуждения:

1. Какие риски киберпространства вы можете назвать?

2. Какой риск в Интернет кажется вам наиболее угрожающим?

3. Как вы понимаете, что ситуация опасная?

4. С кем Вы обсуждаете опасные ситуации, которые возникают в Интернете? Кто или что помогает вам?

Сценарий проведения фокус-группы.

Во вводной части участникам сообщается цель работы группы и принимаются правила работы группы. На следующем этапе происходит погружение в проблему. На третьем этапе выявляются основные понятия и смыслы. В нашем случае мы использовали метод ассоциаций. В качестве слова-триггера были использованы словосочетания «киберриск», «киберугроза». В этом случае проводилась количественная и качественная обработка данных ассоциативного эксперимента. Такой подход позволил определить субъективную значимость выделенных направлений для участников. На четвертом этапе мы использовали метод дискуссии по предлагаемым вопросам без выработки общего мнения. С этой целью была применена форма деловой игры «Кафе «Дилемма»». Участники были объединены в мини-группы для обсуждения дилеммных ситуаций с открытыми ответами. Для работы над ситуациями участники фокус-группы объединялись в мини-группы по 7-10 человек.

Дилеммные ситуации включали в себя весь возможный спектр проблем, связанный с киберпространством. В качестве примера приведем несколько ситуативных задач, предложенных респондентам:

1. При выходе в социальную Сеть можно увидеть предложение о переходе по ссылке для получения для участия в розыгрыше айфона или получения другого ценного подарка. Ваши действия. Проведите анализ имеющихся рисков и возможностей.

2. Со страницы вашего виртуального друга или подписчика поступило предложение о фотосессии 18+ за солидное вознаграждение. Вы согласились с предложением и стали жертвой шантажа. Теперь ваш заказчик обещает разместить эти фото в социальной сети, если вы не выплатите ему определенную сумму или не сделаете еще несколько подобных фото, но более откровенных. Ваши действия.

3. Во время поиска учебного материала ваше внимание привлекло всплывающее окно с новой игрой. Ваши действия. Проведите анализ имеющихся рисков и возможностей.

Всего было проведено 12 фокус-групп, в работе которых прияли участие 142 школьника. Заканчивалась работа в фокус-группах ответом на вопросы анкеты о мотивах экстремального поведения подростков в Сети. Анкета содержала вопросы открытого типа.

Анкета о мотивах экстремального поведения подростков в Сети.

1. Почему подростки часто становятся жертвами кибер-мошенников?

2. Почему подростки часто верят ложной информации, полученной в Сети?

3. Почему подростки чаще, чем остальные, оказываются вовлеченными в киберпреступления?

Изучение *когнитивно-содержательного критерия* предполагало прежде всего получение информации об уровне сформированности знаний в области кибербезопасности и уровне знаний школьников о методах и средствах противостоянию киберугрозам и киберрискам.

Для получения информации об уровне сформированности знаний в области кибербезопасности нами предлагались следующие вопросы:

1. Что такое кибербезопасность?

2. Что такое киберриск, киберугроза?

3. Назовите известные вам киберугрозы и кибериски?

4. Для чего нужны логины и пароли?

5. Для чего нужен пин-код?

6. Почему нельзя переходить по непроверенным ссылкам?

7. Почему нельзя открывать письма и сообщения от незнакомых отправителей?

8. Почему специалисты не рекомендуют давать свою геолокацию в социальных сетях?

9. Что такое персональные данные? Почему их нельзя разглашать?

10. Что такое кибербуллинг?

11. Что делать если ты стал жертвой кибербуллинга?

12. Что такое цифровая репутация?

13. Что такое спам?

14. Что такое флуд?

15. Что такое компьютерный вирус?

16.Как обеспечить наилучшую безопасность вашего ПК?

17. Есть ли закон, определяющий меру ответственности гражданина за создание и распространение вредоносных программ (в том числе вирусов)?

18. Какой из браузеров считается менее безопасным, чем остальные?

19. Зачем необходимо делать резервные копии?

20. Согласно какому документу в России проводится правовое обучение по вопросам защиты информации?

Правильный ответ на каждый вопрос оценивался в 1 балл, неправильный – 0 баллов. Проведенный опрос рандомно выбранных 100 респондентов показал, что возможно следующее распределение по шкале ответов:

0-5 – низкий уровень знаний в области кибербезопасности

6-10 – средний уровень знаний в области кибербезопасности

11-15 – достаточный уровень знаний в области кибербезопасности

16-20 – высокий уровень знаний в области кибербезопасности

Для получения информации об уровне знаний школьников о методах и средствах противостоянию киберугрозам и киберрискам предлагались следующие вопросы:

1. Назовите методы защиты от вредоносных программ.

2. Как обезопасить свое общение в Wi-Fi? Назовите не менее 5 способов.

3. Назовите не менее 10 способов безопасного общения в социальных сетях.

4. Назовите способ безопасного использования электронных денег.

5. Перечислите способы поведения в случае, если вы стали жертвой или свидетелем кибербуллинга.

6. Перечислите способы сохранения своей цифровой репутации.

Правильный полный ответ по каждому пункту оценивался в 2 балла. Неполный ответ – 1 балл. Неправильный или отсутствующий ответ – 0 баллов.

Проведенный опрос рандомно выбранных 100 респондентов показал, что возможно следующее распределение по шкале ответов:

0-4 – низкий уровень знаний в области кибербезопасности

5-8 – достаточный уровень знаний в области кибербезопасности

9-12 – высокий уровень знаний в области кибербезопасности

Сформированность ценностных ориентаций по кибербезопасности определялась при помощи ассоциативных рядов. Респондентам давалась следующая инструкция: «Уважаемый респондент, напишите в центре листа слово кибербезопасность. А теперь напишите те слова, с которыми ассоциируется у Вас это понятие. Чем ближе к центру Вы запишите слово, тем большая степень ассоциации с источником. Нужно разместить на листе не менее 10 ассоциативных слов».

На следующем этапе полученные ассоциативные ряды обрабатывались при помощи интент-анализа для выделения групп ценностей, связанных с кибербезопасностью.

Таким образом, результаты по предложенным методикам и анкетам дают представление об уровне сформированности когнитивно-содержательного критерия.

Исследование деятельностно-поведенческого критерия предполагало выявление уровней сформированности: умений по соблюдению информационной этики, аналитических умений по отбору информации, развития творческой активности обучающихся в противостоянии киберугрозам и развития критического мышления обучающихся при выборе способов противостоянию киберугрозам.

В основе исследовательского опросника для определения умений по соблюдению информационной этики лежали правила сетевого этикета, опубликованные на сайте лаборатории Kaspersky.

Вопросы по правилам сетевого этикета

1. Почему При общении в сети нужно придерживаться тех же правил поведения, которым вы следуете в реальной жизни?

2. Почему важно понимать с кем вы общаетесь?

3. Почему не стоит использовать при общении заглавные буквы?

4. Почему при участии в чате нужно сначала прочитать сообщение и комментарии к нему, а потом задать вопрос?

5. Почему нужно следить за орфографией и пунктуацией в сообщениях?

6. Почему нельзя предавать огласке полученную информацию без предварительного разрешения ее отправителя?

7. Почему письма должны быть краткими и информативными?

8. Почему не стоит подписываться на информационные рассылки и регистрироваться на форумах с использованием чужого имени и адреса электронной почты?

9. Почему не стоит злоупотреблять техническими возможностями для слежки за участниками чата?

10. Почему лучше избегать словесных войн?

11. Почему нужно перед началом общения разобраться с правилами конкретного сообщества?

12. Как противодействовать дискриминационным высказываниям в Сети?

13. К чему может привести разглашение личной информации?

14. Почему лучше использовать нейтральные псевдонимы, не раскрывающие личность?

15. Почему следует избегать общения с ботами?

16. Почему не следует доверять виртуальным знакомым?

17. Почему при общении в закрытой группе, следует воздержаться от шуток «для посвященных»?

18. С чем связано требование «изъясняйтесь кратко и по делу»?

Опросник носил исследовательский характер. Каждый правильный ответ оценивался в 1 балл. Таким образом, максимальное количество баллов – 18.

Проведённая апробация на 187 школьниках показала, что:

Низкий уровень – 0-8 баллов.

Достаточный уровень – 9-13 баллов

Высокий уровень – 14-18 баллов.

Уровень сформированности аналитических умений по отбору информации, развития творческой активности обучающихся в противостоянии киберугрозам и развития критического мышления обучающихся при выборе способов противостоянию киберугрозам выявлялся при помощи основной методики Ю.Ф. Гущина «Тест-опросник критического мышления» и адаптированной нами.

Респондентам давалась инструкция, с помощью которой предлагалось решение ряда задач, которые не являются традиционными и не имеют стандартных решений [Приложение 2].

В апробации опросника принимали участие 221 учащихся 9-х классов г. Симферополя. В ходе апробации нами была проверена валидность и надежность опросника [Приложение 2].

Изучение *эмоционально-волевого критерия* сформированности рефлексивной позиции по противодействию киберугрозам включало определение степени самооценки волевых качеств подростками с подключением механизмов самоанализа, самопознания и самоконтроля и уровень сформированности саморегуляции подростка в интернет-пространстве.

Для изучения этих показателей использовались самоотчеты респондентов, которые подвергались процедурам контент- и интент-анализа и адаптированный вариант методики Дембо-Рубинштейн для реального и виртуального пространства. Диагностика проходила под контролем педагога-психолога.

Нами были выбраны 3 шкалы: уверенность-неуверенность, безопасность-опасность, доверие – недоверие. Сначала для реального пространства, а потом для виртуального нужно было отметить по десятибалльной шкале совет состояние при нахождении в указанном пространстве. Затем полученные результаты сравнивались и подвергались анализу.

Таким образом, грамотно подобранный инструментарий охватывал весь спектр деятельности подростка в интернете и описывал его отношение к кибербезопасности.

3.2. Обсуждение результатов констатирующего этапа педагогического эксперимента

Мотивационно-стимулирующий критерий. Эмпирическое исследование мотивационно-стимулирующего критерия сформированности кибербезопасности обучающихся показало наличие определенных проблем в мотивации и определении места безопасности в киберпространстве со стороны обучающихся.

Результаты исследования понимания социальной и личностной значимости кибербезопасности, умение выделять киберриски приведены на рисунках 3-5 и в таблице 7.

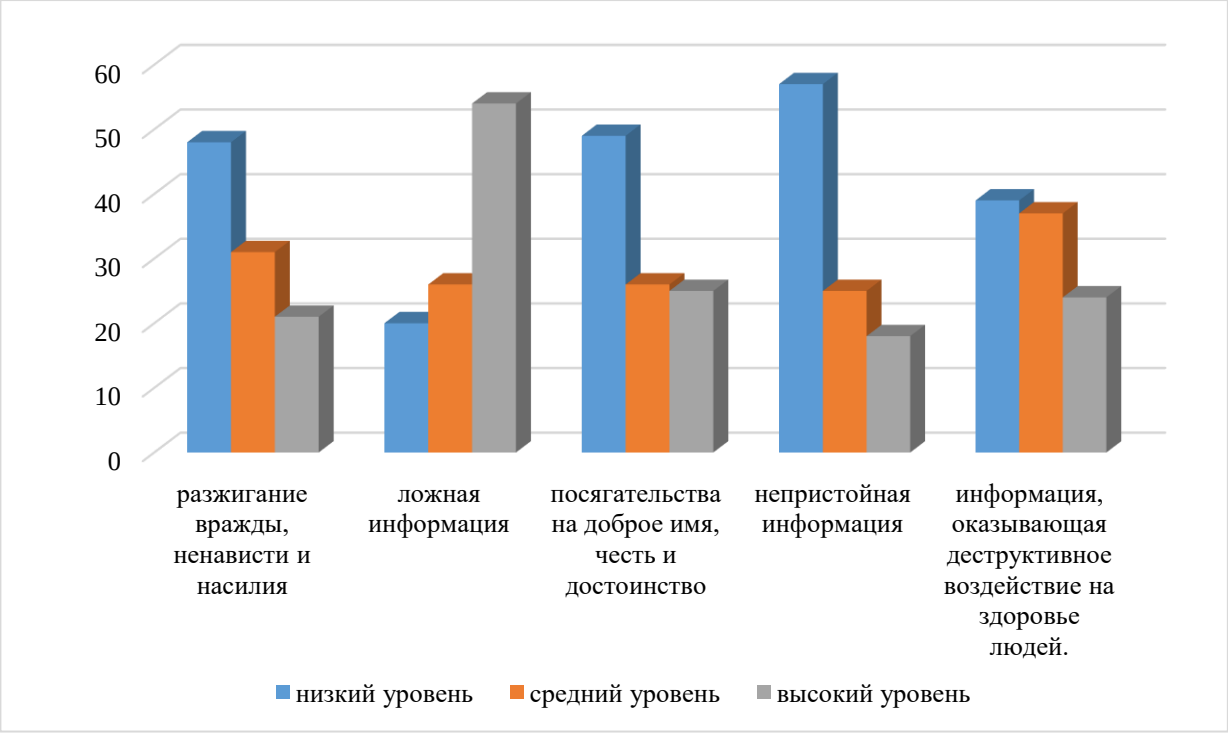


Рисунок 3. Склонность подростков к рискам, связанным с получением деструктивной информации

На основе данных рисунка 2, наиболее частым риском, связанным с получением деструктивной информации, является ложная информация. Более 54%

респондентов принимают ее за достоверную и не видят ничего удивительного в том, чтобы солгать в Сети. Высокие значения выявлены и по шкалам «посягательство на доброе имя», «деструктивное воздействие на здоровье». По сути, эти показатели входят в ТОП-10 самых распространённых рисков.

Следует отметить, что более 20% респондентов имеет высокий уровень склонности к рискам, связанным с получением деструктивной информации. При этом подростки не считают нарушением запугивание или рассылку информации, оказывающей вред психическому здоровью человека (24 % респондентов).

Результаты исследования склонности подростков к рискам, связанными с вовлечением несовершеннолетних в противоправную деятельность посредством сети Интернет, приведены на рисунке 4.

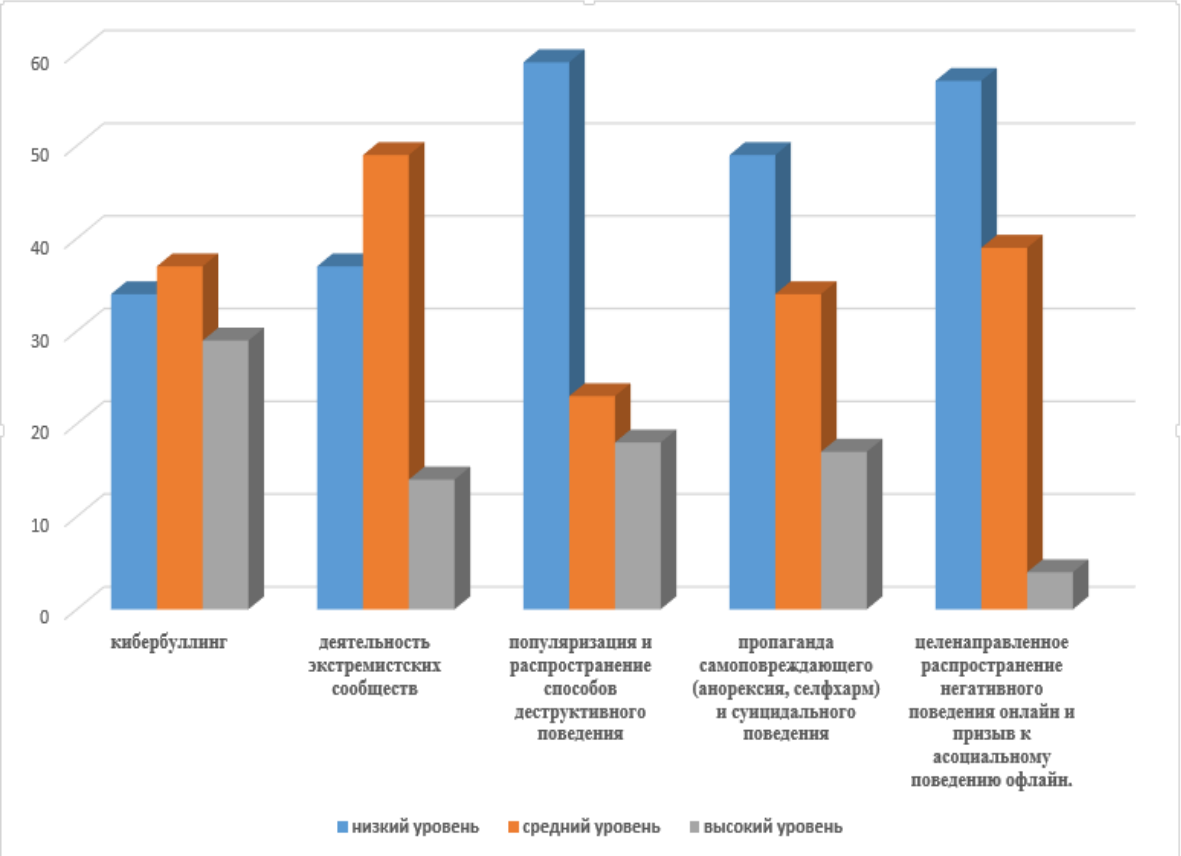


Рисунок 4. Склонность подростков к рискам, связанным с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет

Результаты исследования, представленные на рисунке 4 выявили, что 29% респондентов склонны к кибербуллингу и участвуют в нем в разных ролевых по-

зициях; около 4% старшеклассников с интересом относятся к деятельности экстремистских сообществ; около 17% школьников склонны к самоповреждающему поведению, а 17% респондентов готовы пропагандировать деструктивные способы поведения. Следует отметить, что только пятая часть респондентов представленной выборки осознанно относится к рискам киберпространства и в случае необходимости сообщают об этом взрослым [Рисунок 5].

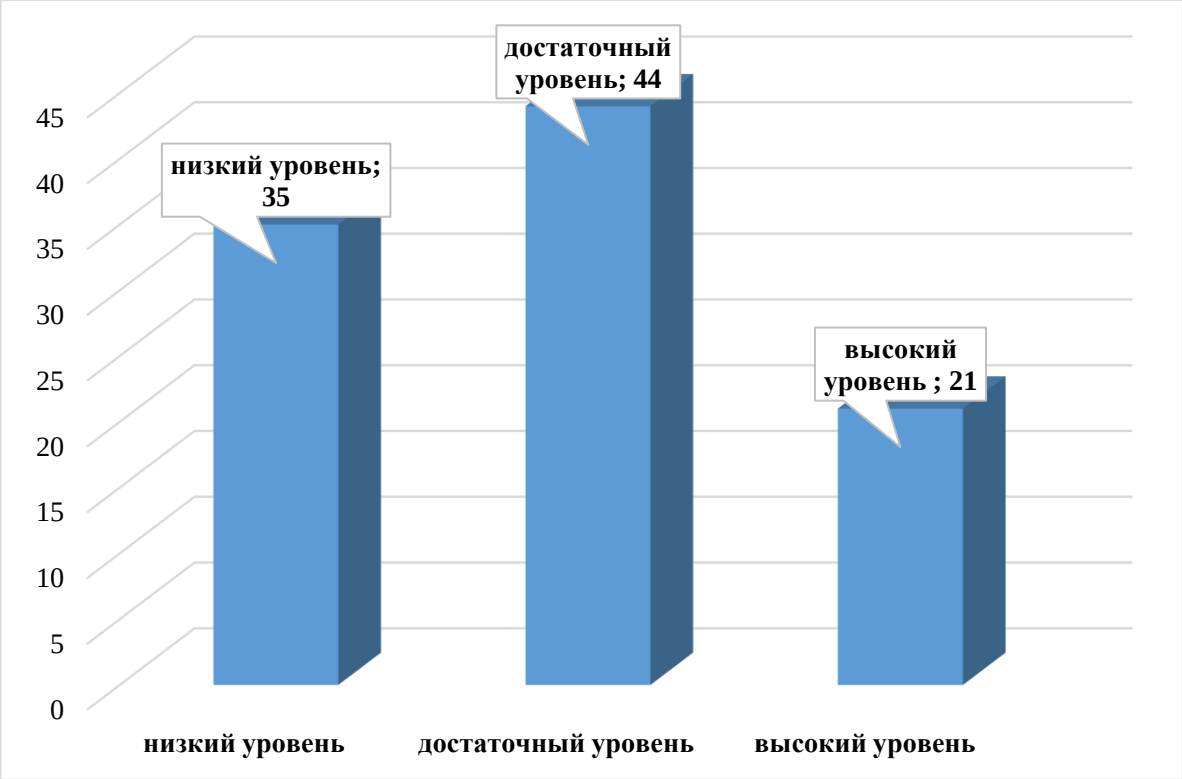


Рисунок 5. Склонность подростков к осознанию рисков кибепространства

Более 35% подростков не воспринимают деструктивные действия в сети как угрозу своей безопасности. Безусловно, такие результаты связаны не только с особенностями подросткового возраста, но и с низким уровнем знаний о киберпространстве.

Таким образом, проведенное исследование позволило выделить склонность к рискам у всех подростков выборки [Таблица 7].

Как видно, по результатам, приведенным в таблице 7, высокой склонность к рискам в киберпространстве остается у 34% респондентов, что требует дополнительных исследований причин этого явления.

Таблица 7

Результаты исследования склонности к киберрискам

Виды рисков	Низкий уровень	Достаточный уровень	Высокий уровень
Риски, связанные с получением деструктивной информации	39	44	27
Риски, связанные с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет	51	27	22
Осознание рисков киберпространства	35	44	21
Склонность к рискам	32	32	34

При проведении фокус-групп анализировались ответы на заранее запланированные вопросы.

1. Какие риски киберпространства вы можете назвать?

Таблица 8

Риски киберпространства

Риск	Травля	Одиночество	Кража денег	Бессмысленная трата денег	Взлом ПК	Секты	Секс	Шантаж
Частота	346	189	397	196	401	121	209	398

Как видно по результатам, приведённым в таблице 14, наиболее часто как угрозу подростки воспринимают взлом ПК, шантаж и кражу денег. Привлекает внимание тот факт, что подростки выделяют в качестве риска – бессмысленную трату денег, что может свидетельствовать о их рефлексивной позиции по отношению киберпространства.

Интересны ответы на вопрос, связанный с признаками опасной ситуации [Таблица 9].

Таблица 9

Признаки опасной ситуации

Признак	Навязчивость собеседника	Требование персональных данных	Многократный переход по ссылкам	Требование предварительной оплаты	Прямые угрозы	Уговоры
Частота	412	397	289	278	410	179

Так, для всех опрошенных подростков общим признаком опасной ситуации является навязчивость собеседника. Практически все респонденты отметили в качестве признака опасности – прямые угрозы, требование персональных данных. Интересно, что около 25% выборки к признакам опасности относят уговоры со стороны собеседника. И хотя подростки не относят их к явным признакам, но уговоры вызывают недоверие. Только 70% выборки к признакам опасной ситуации относят многократный переход по ссылкам и требование предварительной оплаты. Такие результаты говорят о ведущейся, но мало эффективной работе с подростками в области кибербезопасности.

Для нашего исследования представляют интерес с кем обсуждают подростки опасные ситуации. Результаты ответов на вопрос, с кем Вы обсуждаете опасные ситуации, которые возникают в Интернете? Кто или что помогает вам представлены в таблице 10.

Таблица 10

Референтная группа
(было предложено назвать тех, к кому обращаются в первую очередь)

Признак	**Родители**	**Учителя**	**Друзья**	**Интернет-сообщества**	**Никто**
Частота	67	56	124	120	45

Как видно по результатам, приведенным в таблице 16, подавляющее большинство подростков при идентификации ситуации как опасной обращаются за помощью или просто рассказывают об этом в интернет-сообществах, в чатах и к друзьям. 11% выборки не делится со своей проблемой ни с кем. Несмотря на то, в школах активно идут уроки кибербезопасности, и педагоги должны быть готовы к разговору с подростками, количество возможных обращений – 12,4%. Аналогичная ситуация и обращением к родителям.

Таким образом, результаты исследования показали малоэффективность проводимой работы с подростками в области кибербезопасности. Следующим этапом работы в фокус-группах было выявление понятий и смыслов. Ребята в

индивидуальном формате составляли ассоциативные ряды к понятиям киберриск и киберугроза. В качестве примера приведем ассоциативный ряд Али, ученицы 9-го класса [Рисунок 5].

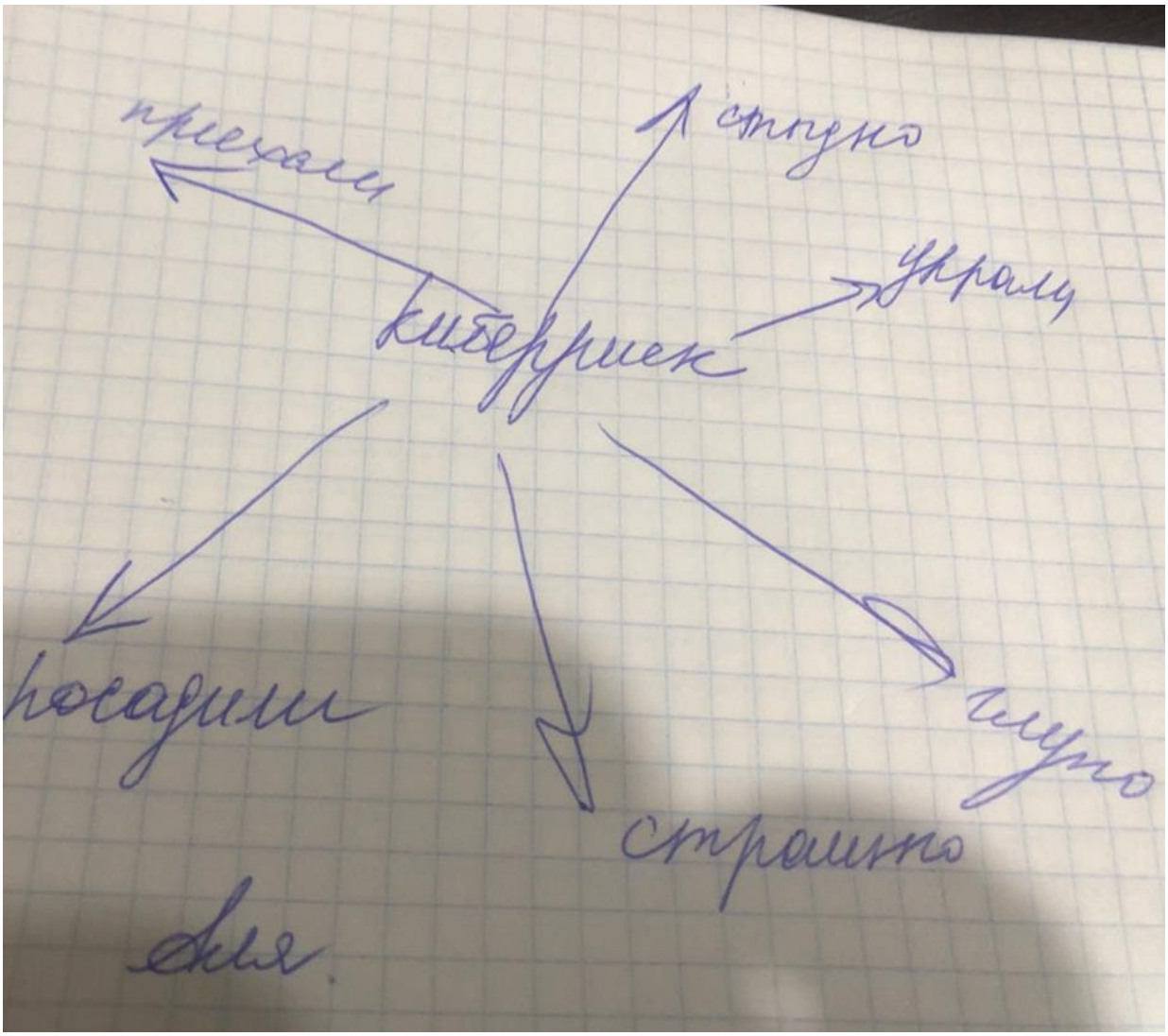


Рисунок 6. Ассоциативный ряд Али

Как видно с рисунка 6, ассоциации имеют разный характер. Так, приехали, украли, посадили, глупо, стыдно – синтагматические ассоциации, то есть имеют класс, отличный от слова-триггера. Страшно – парадигматическая ассоциация. Имеет сходный с триггером класс.

Частотное распределение слов-реакций на слово-стимул представлено в таблице 11.

Таблица 11

Частотное распределение слов-реакций на слово-стимул

Слово-реакция киберриск	**Частота**	**Слово-реакция киберугроза**	**Частота**
Угроза	**378**	Бандитизм	**56**
Шантаж	**271**	Опасность	**302**
Насилие	**132**	Взлом	**129**
Уголовная ответственность	**112**	Кража	**304**
Опасность	**365**	Шантаж	**221**
Экстрим	**98**	Горе	**79**
Смелость	**49**	Страх	**162**
Глупость	**78**	Жертва	**78**
Взлом	**209**	Атака	**101**
Драйв	**46**	Тюрьма	**67**

В своем исследовании мы брали только первых 10 позиций. В ходе обработки нами были объединены некоторые слова в единую группу с общим названием. В данном процессе нас волновали результаты частотного распределения и направления высказывания. Как показывают результаты, представленные в таблице 11, для подростков слова киберриск и киберугроза являются синонимичными, однако киберугроза – драматичнее.

Так, при описании наиболее значимых ассоциаций к понятию киберриск выявлены такие ассоциации как смелость, глупость, драйв. экстрим, что создает картину легкомысленного отношения к киберрискам. В тоже время ассоциативный ряд для понятия киберугроза содержит такие слова как: горе, страх, жертва, что позволяет думать о киберугрозах как более опасных, чем риски.

Полученные результаты легли в основу составления текстов по кибербезопасности для подростков. Интерес представляла работа в фокус-группах при решении дилеммных ситуаций. Каждому старшекласснику предлагалось написать выход из предложенной ситуации. Следует отметить, что в ходе работы выявлено, что 67% девятиклассников не могут определить путь выхода из проблемной ситуации в киберпространстве. Всего было предложено 15 дилемм: 5 из них относилось к определению выхода из ситуации, связанной с получением де-

структивной информации; 5 – с участием подростка в противоправной деятельности. 5 ситуаций – с личностными особенностями подростка. Целью работы с дилеммами являлось определение личных способов сохранения безопасности в Сети.

С первой группой дилемм справились полностью 24% подростков. 69% респондентов не знают, как себя вести в ситуации получения деструктивной информации; 14 подростков в ходе работы над дилеммами старались привлечь к ответам окружающих или списать у них их ответы.

Вторая группа дилемм была полностью отработана 21% подростков, выбрали неконструктивный путь решения проблемы – 65% подростков. Так, в ситуации буллинга подросток, выступающий жертвой, предлагает никому не говорить и попросить буллера не трогать его.

Третья группа дилемм была решена успешно 45% подростков. Только 34% не справились. Основная проблема неуспеха подростков – боязнь одиночества в Сети.

Следующим этапом работы стало анкетирование с открытыми вопросами о мотивах экстремального поведения подростков в Сети. Все подростки получили бланки с вопросами.

Ниже приведены варианты ответов и частоты [Таблица 12-14].

Так, при ответе на первый вопрос был собран массив из 3045 ответов. Синонимичные слова или слова, находящиеся в одинаковом смысловом поле, были объединены в группы с одним названием. Всего было выделено 6 групп. Частота рассчитывалась по совокупности встречаемости слов в группе [Таблица 12].

Таблица 12

Вопрос: Почему подростки часто становятся жертвами кибермошенников?

Мотивы	**Азарт**	**Власть**	**Безысходность**	**Агрессия**	**Интерес**	**Доверие**
Частота	587	754	489	726	310	179

Как видно по результатам, приведенным в таблице 12, основными мотивами подростков в общении с киберпреступниками являются азарт, власть,

безысходность, агрессия, интерес, доверие. Описывая свой негативный опыт общения с кибермошенниками, подростки отмечают, что «особенно в розыгрышах все так по-настоящему». Девятиклассники отмечают, что они были уверены, что их не коснется обман. И хотя полученные результаты представляют интерес для психологов, но они подчеркивают несовершенство педагогического процесса прежде всего в плоскости субъект-субъектных отношений. Ответ на второй вопрос собрал массив длиною в 1023 слова. Нами были выделены 5 смысловых групп [Таблица 13].

Таблица 13

Вопрос: Почему подростки часто верят ложной информации, полученной в Сети?

Мотивы	**Вера в сказку**	**Власть**	**Азарт**	**Безысходность**	**Глупость**
Частота	226	171	174	216	236

На основе результатов, приведенных в таблице 13 можно сделать вывод, что наиболее актуальной причиной доверия ложной информации подростки считают глупость и веру в сказку. Это разнополюсные мотивы, однако такой разброс характерен для подросткового возраста. Настораживает такой мотив как безысходность. Эта группа содержит такие ответы как: нет выхода, никто не поможет, последний шанс.

Следует отметить, что мотивы вовлечения подростков в киберпреступления повторяют уже выделенные ранее [Таблица 14]. В ходе обработки массива данных, состоящего из 1245 слов, нами выделено 5 смысловых групп.

Таблица 14

Вопрос: Почему подростки чаще, чем остальные, оказываются вовлеченными в киберпреступления?

Мотивы	**Азарт**	**Власть**	**Одиночество**	**Агрессия**	**Интерес**
Частота	226	171	174	216	236

Результаты, приведенные в таблице 14 выявили, что наиболее часто в качестве мотива или причины вовлечения в киберпреступления подростки указывают интерес, азарт, агрессия. Следует отметить, что группа азарт представлена понятиями риск, скорость, драйв, полет. В то время, как группа интерес представлена понятиями увлеченность, по приколу, нравится и др.

Мы считаем, что результаты исследования мотивов подростков, вовлеченных в рискованную деятельность, позволили выделить основные проблемы, вокруг которых может строиться педагогическая работа с обучающимися, а именно: привлечение интереса подростка, удовлетворение его потребности во власти, перенос агрессии с человека на объект, создание команды.

Когнитивно-содержательный критерий. Результаты исследования уровня сформированности знаний в области кибербезопасности приведены на рисунке 7.

Как видно на рисунке 7, 74% респондентов имеет достаточный и высокий уровень сформированности знаний в области кибербезопасности. Однако, стоит обратить внимание, что 40 школьников из 412 не ориентируются или плохо ориентируются в киберпространстве.

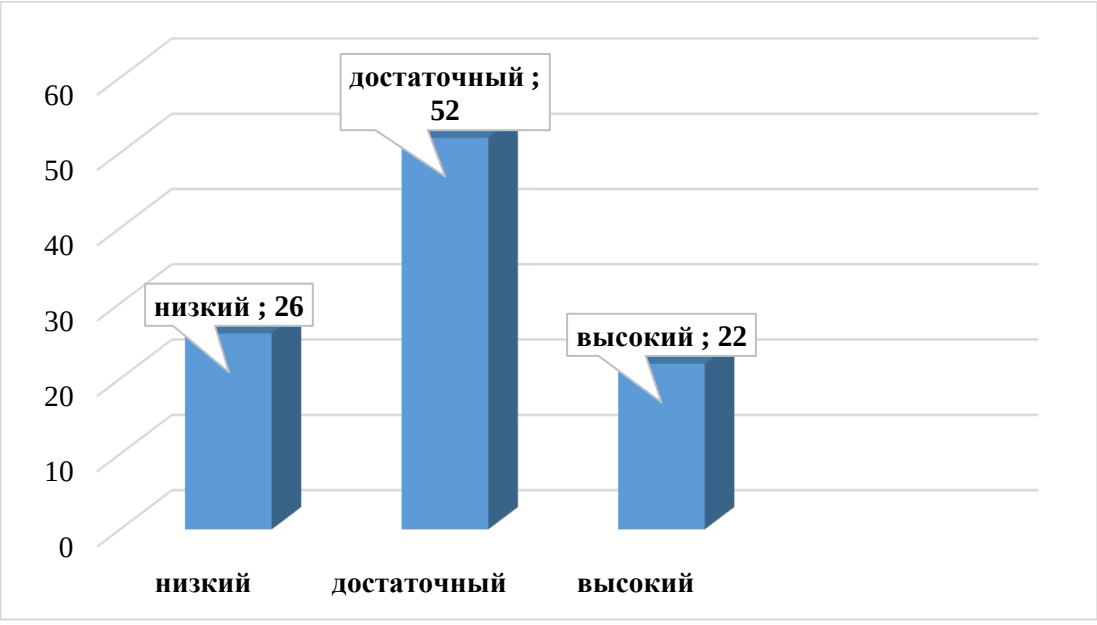


Рисунок 7. Результаты исследования уровня сформированности знаний

Анализ допущенных ошибок позволил выделить наиболее проблемные области знаний по кибербезопасности. Так, 54% школьников ответило неправильно на вопрос о цифровой репутации. 23% респондентов этой группы в своих ответах опираются на ошибочные суждения – мифы. Более 31% старшеклассников выборки дают неполные ответы в отношении персональных данных, отмечая только одну сторону проблемы. 71% обучающихся выборки не смог назвать и закон, определяющий меру ответственности гражданина за создание и распространение вредоносных программ (в том числе вирусов). Следовательно, школьники не уделяют внимание ответственности за участие в схемах кибермошенников. Кроме того, хаккинг в подростковых кругах считается социально одобряемой деятельность, так как быть хакером модно.

Результаты исследования уровня знаний школьников о методах и средствах противостоянию киберугрозам и киберрискам приведены в таблице 15.

Результаты, приведенные в таблице 15, при ответе на все вопросы у подростков есть некоторые затруднения. Так, среди способов безопасного общения в социальных сетях только у 22 подростков отмечено, что нужно ограничить объем личной информации в социальных сетях. При перечислении способов сохранения цифровой репутации только 9% подростков смогли дать правильные ответы. По нашему мнению, такие результаты связаны с тем, что ребята малознакома с самим термином «цифровая репутация». При этом, даже продвинутые пользователи не выполнили мониторинг отзывов и обучение цифровой грамотности как способы сохранения цифровой репутации.

Таблица 15

Методы и средства противостоянию киберугрозам и киберрискам

Назовите методы защиты от вредоносных программ.					
Выключить ПК	**Поставить антивирус**	**Пробить ссылку по базе**	**Не знаю**		
342	**389**	**116**	**12**		
Как обезопасить свое соединение Wi-Fi? Назовите не менее 5 способов.					
Поставить пароль	**Скрыть**	**Поставить ограничения**	**Отключать**	**Проверять трафик**	**Не знаю**
353	**213**	**167**	**371**	**201**	**10**
Назовите не менее 5 способов безопасного общения в социальных сетях.					
Сложный пароль	**Страница не для всех**	**Сложная аутентификация**	**Отписаться от подписчиков**	**Не переходить по ссылкам**	
359	**873**	**101**	**102**	**234**	
Назовите способ безопасного использования электронных денег.					
Виртуальный кошелек	**С карты**				
64	**367**				
Перечислите способы поведения в случае, если вы стали жертвой или свидетелем кибербуллинга.					
Прекратить общение	**Рассказать взрослым**	**Ответить агрессией**	**Не знаю**		
308	**102**	**244**	**29**		
Перечислите способы сохранения своей цифровой репутации.					
Надежный пароль	**Управление профилями в социальных сетях**	**Использование VPN**			
29	**34**	**38**			

Результаты сформированность ценностных ориентаций в области кибербезопасности представлены в таблице 16. Респондентам предлагалось написать эссе на тему «Безопасность в Интернете: кому она нужна».

На следующем этапе полученные ассоциативные ряды обрабатывались при помощи интент-анализа для выделения групп ценностей, связанных с кибербезопасностью.

В таблице 16 приведены ценности, имеющие наибольшее количество выборов в данной группе респондентов. Следует отметить, что витальные и социальные ценности, несмотря на их значимость, занимают лишь третье и второе

место в иерархии ценностей данной выборки. Тем не менее все указанные ценности совпадают с теми, на подрыв которых направлены основные киберугрозы.

Таблица 16

Кибербезопасность как ценность

№ п/п	Ценность	Количество респондентов, указавших
1.	**Витальные ценности** (сохранение жизни, психического здоровья)	**157**
2.	**Социальные ценности** (сохранение репутации, сохранение круга друзей)	**268**
3.	**Материальные ценности** (сохранение денег, имущества, богатство)	**389**

В качестве примера приведем несколько выдержек из эссе респондентов.

Витальные ценности (сохранение жизни, психического здоровья).

Эльмира, 15 лет: «Безопасность в Интернете нужна, прежде всего, мне. Я хочу знать, как обезопасить свою жизнь и жизнь своих близких от преступников и просто негодяев. Недавно читала как девочку через социальные сети шантажировали ее фото. Девочка была на грани самоубийства. У моей подруги взломали страницу и написали всякую гадость о ней. Она не видела. А потом над ней смеялись. Это ужасно.»

Саша, 16 лет: «Я не хочу сходить с ума от тог, что кто-то решил надо мной поиздеваться. Я могу и должен научиться себя защищать».

Антон, 15 лет: «Интернет – это как реал. Мы же не бросаема под колеса и соблюдаем правила. Здесь нужно также».

Социальные ценности (сохранение репутации, сохранение круга друзей).

Оля, 15 лет: «Однажды мою страницу взломали и стали писать про меня пошлости. И самое страшное, что мне стали добавлять друзей таких же пошлых с ужасными аватарами. Мне было так стыдно как будто все это сделала я. Никогда больше не допущу такого. Я научилась охранять свою страницу».

Сердар, 14 лет: «Меня не все любят в классе. Так бывает. Было время, когда под моими постами в ВК анонимы писали всякую кринжатину. Некоторые меня оскорбляли. Я закрыл страницу для чужих и почистил друзей».

Материальные ценности (сохранение денег, имущества, богатство).

Рина, 15 лет: «У мамы увели все деньги с карты. Ей просто позвонили по телефону, и она все данные слила службе банка. Я так не хочу. Безопасность нужно соблюдать».

Гоша, 15 лет: «Мой брат повелся на розыгрыш айфонов. Короч нагрели его на 3000 за пересылку. Айфона нет до сих пор. Фирма исчезла. Безопасность в нете нужна для того, чтобы этого не было».

Эрика, 15 лет: «Мне нужен безопасный интернет потому, что я хочу зарабатывать деньги. Сейчас я думаю о своем деле. Ну и о безопасности, конечно».

Проведенное исследование показало, что когнитивно-содержательный критерий играет важную роль в формировании навыков кибербезопасности подростка.

Деятельностно-поведенческий критерий. Результаты эмпирического исследования умений по соблюдению информационной этики приведены на рисунке 8.

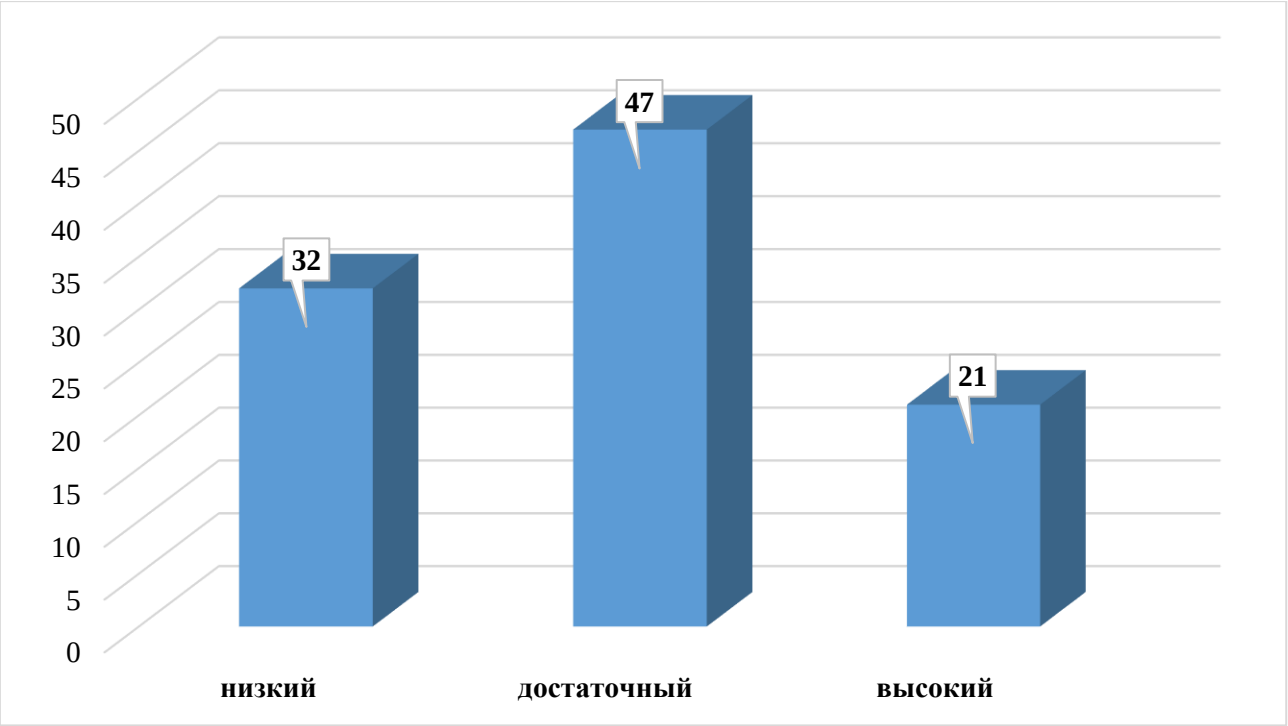


Рисунок 8. Результаты эмпирического исследования умений по соблюдению информационной этики

Результаты, представленные на рисунке 8 выявили, что подавляющее большинство респондентов (47%) имеет достаточный уровень сформированности умений по соблюдению информационной этики. Этим респондентам характерно поверхностное отношение к правилам сообщества. Нередко такие подростки удаляют страницы и заносят в черный список своих друзей; 21% респондентов имеют высокий уровень сформированности умений по соблюдению информационной этики, что выражается осмыслении правил и норм сообщества, уважении к другим; а около 32 % респондентов выборки не интересуются правилами действий в Интернете и предполагают, что «виртуальный мир прогнется под них».

Результаты сформированности критического мышления в области кибербезопасности отражают умения: делать логические умозаключения и обосновывать свой ответ; оценивать последовательности умозаключений; анализировать и делать заключение о причинах явлений; анализировать и оценивать содержание текстов; обнаруживать ошибки, связанные с неопределенностью и двусмысленностью выражений и терминов; обнаруживать существенную информацию на фоне избыточной [Рисунок 9].

Как видно на рисунке 9, наибольшее количество респондентов имеет достаточный уровень развития критического мышления, что соответствует развертыванию мыслительных операций в пределах элементарных суждений. Опыт приобретается путем проб и ошибок.

Респондентов с низким и высоким уровнем развития критического мышления соответственно 34% и 13%.

Следует отметить, что респондентам с низким уровнем развития критического мышления свойственно воспринимать на веру любую информацию. Причинно-следственные связи нарушены. Рефлексия, соответственно, снижена.

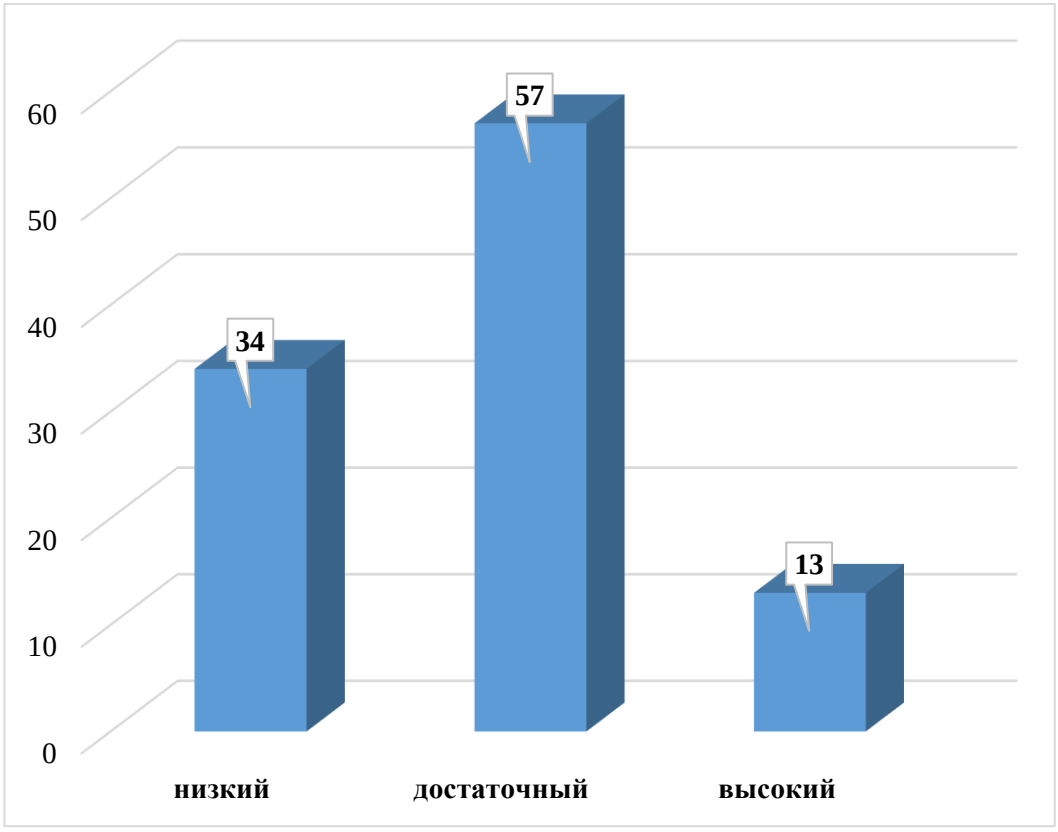


Рисунок 9. Распределение по уровням развития критического мышления в выборке

Высокий уровень развития критического мышления проявляется в устойчивых сформированных умениях делать логические умозаключения, оценивать последовательности умозаключений; устанавливать правильные причинно-следственные связи; выделять фигуру на фоне, рефлексировать. Таким респондентам

характерны возросшая скорость определения ошибок, высокий уровень рефлексии.

Детальный анализ по каждой шкале приведен в таблицах 17-22 и описании к ним.

Таблица 17

Умение делать логические умозаключения и обосновывать свой ответ

Количество респондентов/баллы	**0**	**1**	**2**	**3**
Задание 2	16	53	198	146
Задание 3	17	58	201	137
Задание 4	14	65	212	121

Как выявили результаты, приведенные в таблице 17, полностью выполнили задание только 30-35% респондентов. При этом в большинстве случаев проблема была не в построении логического умозаключения, в обосновании ответа. Следует отметить, что на неумение ответить правильно указывают подростки, ставшие жертвами кибермошенников. Ребята указывают, что они понимают с кем разговаривают, но не могут правильно сформулировать свою мысль и их доводы разбиваются о «контраргументы» мошенников.

Таблица 18

Умение оценивать последовательности умозаключений

Количество респондентов/баллы	**0**	**1**	**2**	**3**	**4**	**6**	**7**	**8**	**9**	**10**
Задание 5	0	0	3	8	15	49	49	94	87	107
Задание 6	0	42	370							

Как видно по результатам, приведенным в таблице 18, задание под № 6 выполнили практически все респонденты, а при выполнении задания № 5 – также возникла сложность с обоснованием ответа. Подростки не нашли нужные аргументы. Мы считаем, что проблема заключатся в том, что старшеклассники не имеют достаточного опыта дискуссий для того, чтобы аргументированно ответить собеседнику.

Безусловно, важную роль в развитии критического мышления играет умение анализировать и делать заключение о причинах явлений. Результаты исследования сформированности этого умения у подростков выборки приведены в таблице 19.

Таблица 19

Умение анализировать и делать заключение о причинах явлений

Количество респондентов/баллы	**0**	**1**	**2**	**3**	**4**
Задание 1	0	0	43	111	258
Задание 7	1	18	367	26	
Задание 8	0	412			

Результаты, приведенные в таблице 19 выявили, что возникли трудности с выполнением заданий 1 и 7, что указывает на недостаточную проработанность способности к причинно-следственной связи у подростков. Следует отметить, что несформированное умение анализировать и делать заключение о причинах явлений, может привести к повторным ошибкам во взаимодействии с мошенниками.

Умение анализировать и оценивать содержание текстов имеет огромное значение при попытке кибермошенников заключить клиентом договор или соглашение. Именно отделение главного от второстепенного позволяет не совершить ошибку в заключении договора.

Таблица 20

Умение анализировать и оценивать содержание текстов

Количество респондентов/баллы	**0**	**1**	**2**	**3**
Задание 9	0	21	187	204
Задание 10	0	14	176	222
Задание 11	0	15	187	210
Задание 12	0	13	187	212

Как видно по результатам, приведенным в таблице 20, полностью выполняет задания 49-50% респондентов. 4-5% респондентов не выполняет задания вообще. А около 45% подростков выполняет задания частично. Такие результаты

характерны для подростков, которые к документам относятся легкомысленно. При этом информация на сайтах тоже читается не полностью.

В качестве примера можно привести ситуацию Алины Н., заказавшей с поддержкой мамы себе сумочку. Сумка пришла. Однако не имела ничего общего с тем, что было заказано. В ответ на гневные обращения матери девочки представители продавца указали на то, что на сайте написано о том, что форма товара может быть другой. Конечно, ни Алина, ни ее мама этого текста не читали.

Умение обнаруживать ошибки, связанные с неопределенностью и двусмысленностью выражений и терминов, является крайне необходимым в киберпространстве, особенно при чтении рекламы.

Таблица 21

Умение обнаруживать ошибки, связанные с неопределенностью и двусмысленностью выражений и терминов

Количество респондентов/баллы	**0**	**1**	**2**	**3**
Задание 13	8	17	167	220
Задание 14	4	11	397	

Как видно по результатам, приведенным в таблице 21, задание 13 вызвало затруднение у 49% респондентов. Проблема взаимодействия с интернет-пространством – это и проблема семантическая. Появление новых слов и выражений может запутать подростка, если он не знает их значений.

Эмоционально-волевой критерий. Эмпирическое исследование сформированности рефлексивной позиции по противодействию киберугрозам включало определение степени самооценки волевых качеств подростками с подключением механизмов самоанализа, самопознания и самоконтроля и уровень сформированности саморегуляции подростка в интернет-пространстве.

Самоотчеты респондентов содержали сведения о том, как они заходят в Интернет, какие правила соблюдают, с какими проблемами сталкиваются, к кому обращались за помощью. Всего было рассмотрено 412 самоотчетов и составлен массив длиной в 9748 слов, относящимся к исследуемой проблеме.

Из этого массива методом интент-анализа были выделены основные группы проблем и рассчитана их доля в % [Рисунок 10].

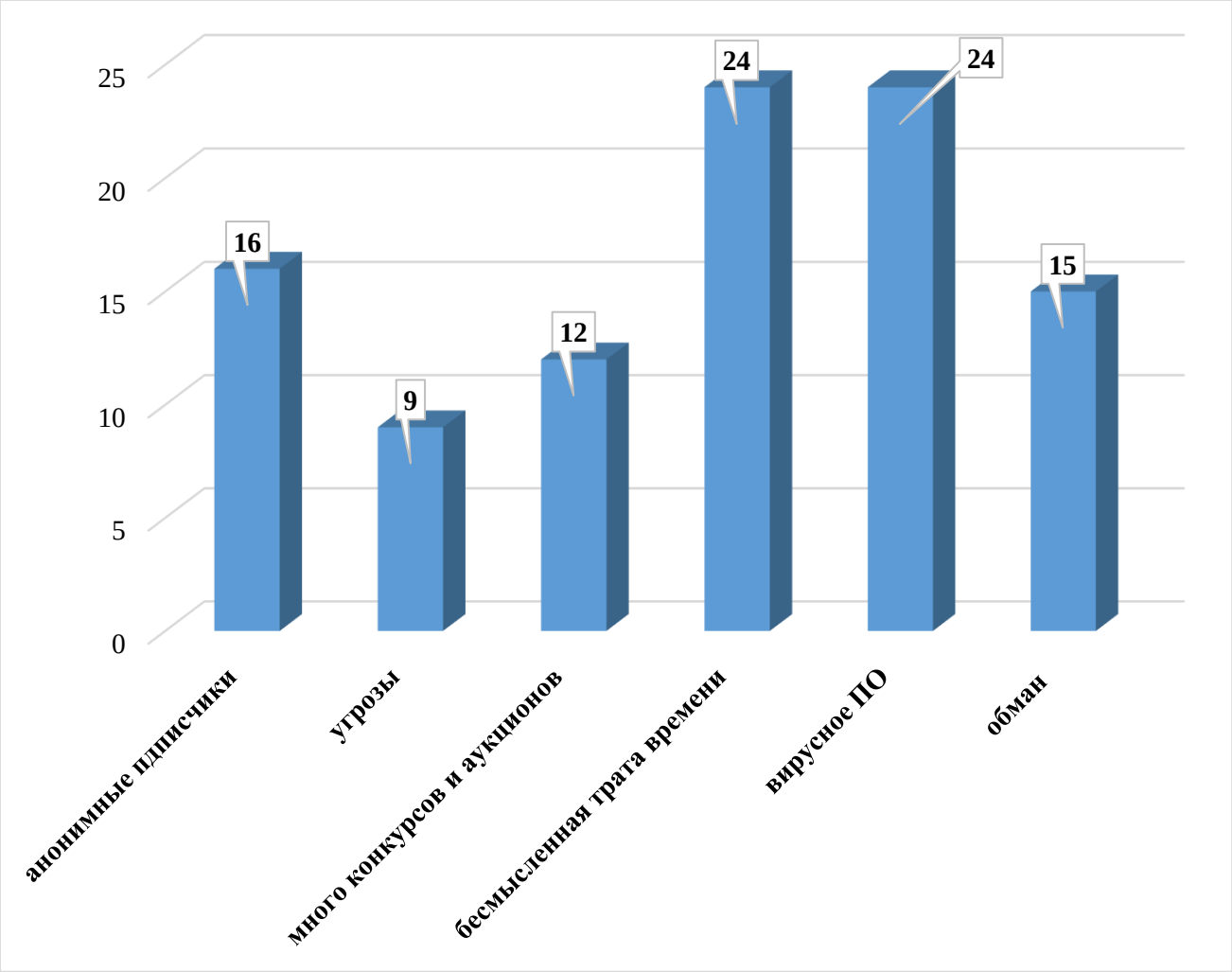


Рисунок 10. Проблемы, отмеченные в самоотчетах

Результаты диаграммы выявили, что школьники реалистично оценивают риски, с которыми они встречаются в киберпространстве. Однако чаще всего в самоотчетах встречается указание на бессмысленную трату времени (24%) и на то, что «можно цапнуть вирус» (24%).

В процессе самоанализа были выявлены и алгоритмы входа в Сеть, отмеченные школьниками [Рисунок 11].

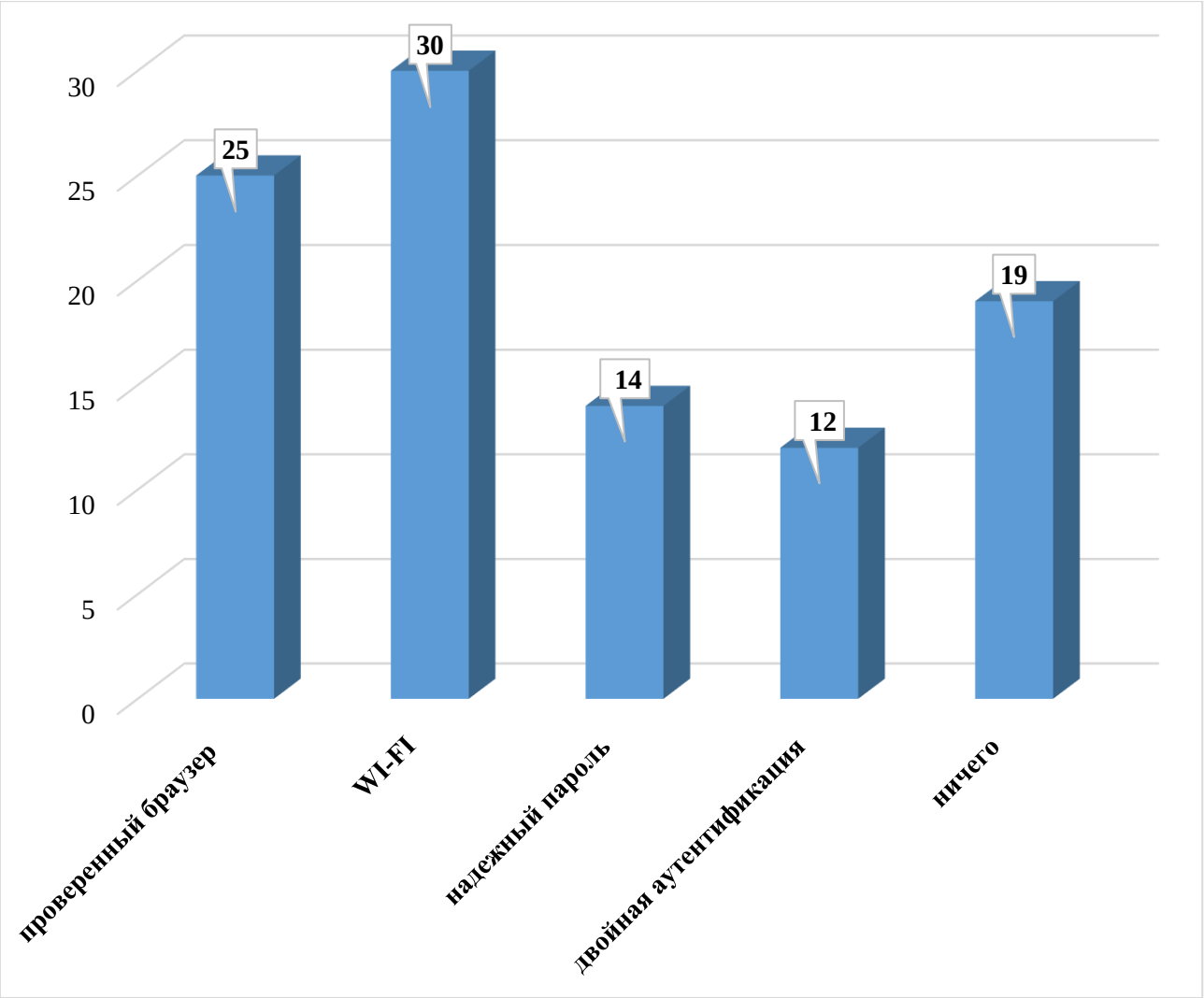


Рисунок 11. Алгоритмы входа, отмеченные в самоотчетах

Как видно с рисунка 10 – 19% массива содержит информацию о том, что школьники полагаются на волю случая и не предпринимают никаких действий для обеспечения безопасности в Сети. 30% от всего массива – предположения, что использование любого WI-FI может предотвратить киберугрозу. Около 25% массива содержит информацию об уверенности школьников в том, что их браузер надежный. И только 26% массива данных содержит информацию о защите соединения.

Такие результаты подтверждают необходимость педагогического воздействия на старшеклассников в области кибербезопасности.

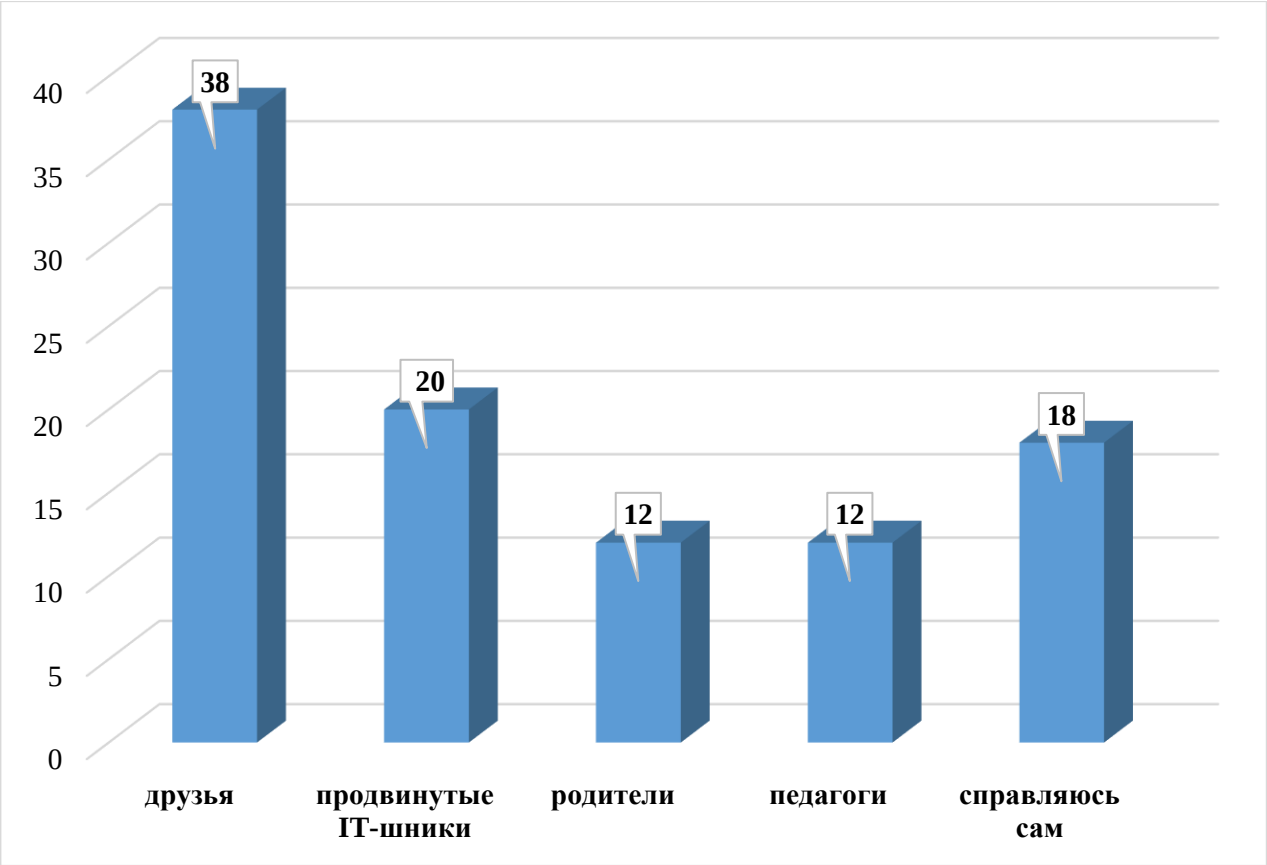


Рисунок 12. Обращение за помощью, отмеченное в самоотчетах

Как видно на рисунке 12, подтверждаются ранее полученные результаты о том, что наиболее референтными лицами для подростков являются их друзья, а педагоги и родители занимают последние места в рейтинге значимых лиц в этих вопросах.

Как указывалось, в п. 3.1, исследование эмоционально-волевой сферы школьников проводилось в реальном и виртуальном пространствах по трем шкалам: уверенность-неуверенность, безопасность-опасность, доверие – недоверие. Затем полученные результаты сравнивались и подвергались анализу.

Следует отметить, что существуют значимые различия по шкале уверенность-неуверенность в реальном и виртуальном пространстве. Так, более 27% школьников чувствуют себя увереннее в виртуальном пространстве, чем в реальном. А 46% школьников не ощущают разницы пребывания в обоих пространствах.

При этом 67% респондентов выборки считают киберпространство более безопасным, чем реальное.

Однако, полученные данные позволяют сделать вывод о том, что 82% выборки испытывает больше доверия в реальном пространстве, чем в виртуальном.

Таким образом, проведенное исследование позволило выявить ключевые точки в формировании кибербезопасности старшеклассника:

1. Несформированность мотивов безопасной деятельности в Сети.

2. Отсутствие или недостаточность знаний о киберугрозах и способах борьбы с ними.

3. Недостаточность сформированности умений, определяющих критическое мышление подростка.

4. Легкомысленное отношение к проблеме кибербезопасности в целом, свойственное подросткам.

5. Особенности подросткового возраста в области определения авторитетов и референтных групп.

Полученные результаты и сделанные на их основании выводы легли в основу формирующего эксперимента.

3.3 Обсуждение результатов формирующего этапа педагогического эксперимента

Как было указано в п. 2.2 модель педагогического сопровождения процесса формирования кибербезопасности старшеклассников построена с учетом следующих педагогических условий: формирование положительной мотивации обучающихся к учебной и внеклассной деятельности; развитие критического мышления при поиске и обработке информации, полученной из интернет-источников; осуществление рефлексии на основе применения механизмов самопознания, самоанализа и самоконтроля.

Характеристики ЭГ и КГ.

Для участия в формирующем этапе педагогического эксперимента привлекались те же обучающиеся, что и для участия в констатирующем, однако по рекомендации экспертов, нами были взяты всего 10 классов из экспериментальных школ, по 2 в параллели. Ребята из предпрофессиональных классов на базе университета не привлекались к формирующему эксперименты в связи с эпизодичностью встреч.

Таким образом были созданы контрольная и экспериментальная группы. В контрольную группу (КГ) вошли 128 обучающихся пяти 9-х классов. Следует отметить, что у 65% обучающихся КГ не были сформированы мотивы безопасной деятельности в Сети, 67% респондентов имели недостаточные знания о киберугрозах и способах борьбы с ними, у 63 % школьников недостаточно сформированы умения, определяющие критическое мышление, более 78 % респондентов наблюдалось легкомысленное отношение к проблеме кибербезопасности в целом [Рисунок 13].

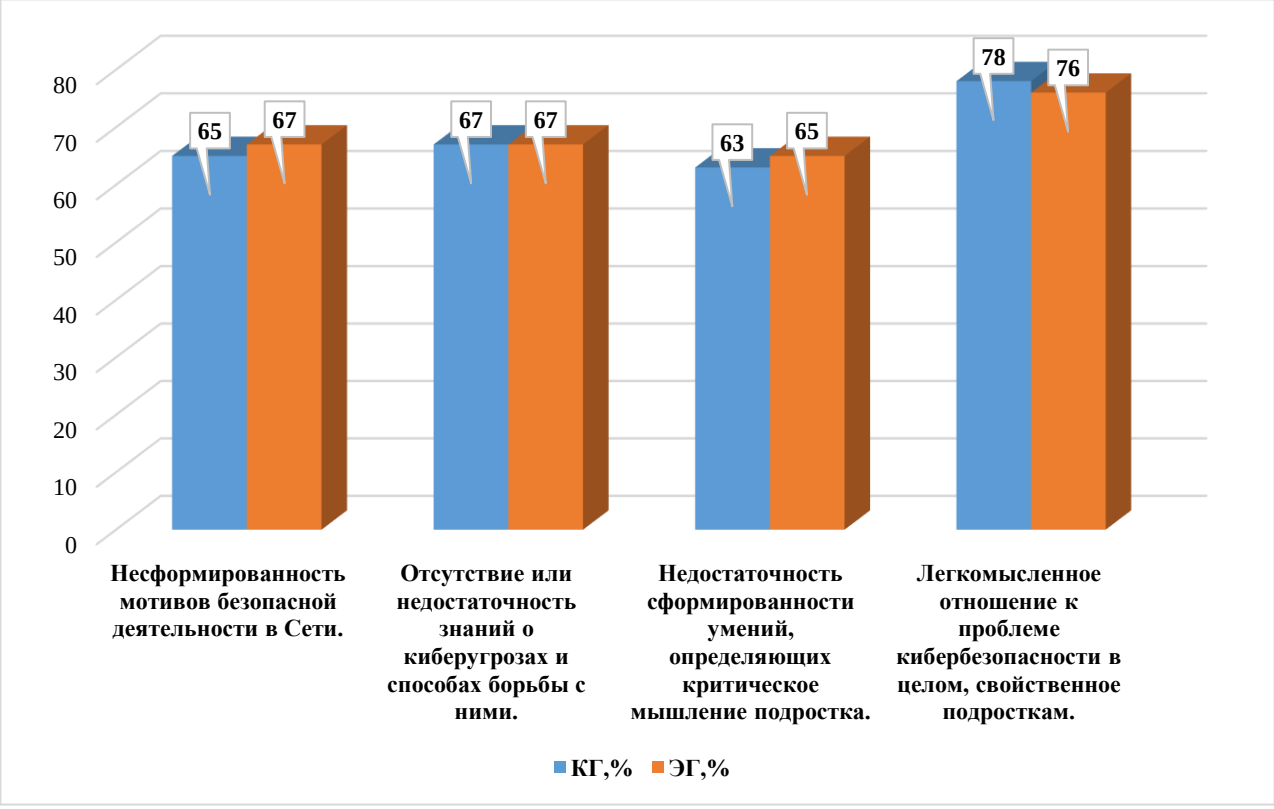


Рисунок 13. Характеристика контрольной и экспериментальной групп

В экспериментальную группу вошло 130 обучающихся пяти 9-х классов. Следует отметить, что у 67% обучающихся КГ не были сформированы мотивы безопасной деятельности в Сети, 67% респондентов имели недостаточные знания о киберугрозах и способах борьбы с ними, у 65 % школьников недостаточно сформированы умения, определяющие критическое мышление, более 75 % респондентов наблюдалось легкомысленное отношение к проблеме кибербезопасности в целом

При этом было выявлено, что уровень сформированности навыков кибербезопасности в обеих группах существенно не различался.

Для экспериментальной группы была разработана программа по формированию навыков безопасного проведения в Сети, а для респондентов контрольной группы такая работа не проводилась.

Рассмотрим результативность предложенных педагогических условий в рамках предложенной модели педагогического сопровождения формирования кибербезопасности старшеклассников.

В соответствии с *первым педагогическим условием*. *Формирование положительной мотивации обучающихся к учебной и внеклассной деятельности, способствующей совершенствованию навыков в области кибербезопасности.*

Таблица 22

Особенности формирования положительной мотивации обучающихся в области кибербезопасности

Компонент	**Содержание**	**Форма**	**Технология**	**Средства**
Когнитивный компонент	Формирование знаний по кибербезопасности	Лекции, дискуссии, беседы	кейс-технология	технологии коллективного обучения, интерактивные игры, инструкции, алгоритмы, методические рекомендации
Деятельностный компонент	Вовлечение школьников в социально одобряемую деятельность	Практические занятия, внеклассные мероприятия	Интерактивные задачи по формированию навыков кибербезопасности	
Рефлексивный компонент	Умение определять ситуации, в которых проявление навыков кибербезопасности необходимо	Квест	Задачи с несколькими решениями	

Нами была разработана мотивационная программа, включающая мероприятия, направленные на формирование интереса обучающихся к собственной кибербезопасности [Таблица 23]. Мы исходили из того, что для формирования навыка необходимо 10-12 закреплений.

Как видно из таблицы 30, все мероприятия предполагают интерактивную форму проведения. На первом мероприятии – проблемной лекции – сразу были озвучены проблемы, решение которых необходимо было найти в дальнейшем.

Таблица 23

Мероприятия, направленные на формирование положительной мотивации обучающихся в области кибербезопасности

№ п/п	Мероприятие	Цель	Форма проведения
1.	Лекция «Кибербезопасность – это о чем»	Систематизировать знания в области использования интернета	Проблемная лекция, лекция-диалог
2.	Кафе «Дилемма»	Сформировать навыки и осознанные подходы к противодействию интернет-угрозам	Кейс-технологии, интерактивные игры
3.	Кибер-квест	Сформировать навыки распознавания и реагирования на интернет-угрозы.	Кейс-технологии, технологии коллективной работы
4.	Киберумник	Систематизировать знания в области использования интернета в личном зачете	Кейс-технологии, технологии портфолио
5.	Олимпиада по кибербезопасности	Систематизировать знания в области использования интернета	Технологии индивидуальной работы

Проблемная лекция начиналась с предъявления записи реального телефонного разговора (кейс-технологии):

«Добрый день! Ирина Викторовна, Вам ранее приходило сообщение о том, что у Вас закончился договор с МТС. Вы хотите его продлить. Это совершенно бесплатно.

– хочу. А какие условия?

– От 1 года до 15 лет. На сколько лет хотите продлить договор об оказании услуг Вы?

– на год.

– отлично. Мы вышлем Вам продленный договор через Госуслуги. Сейчас Вам уже пришло сообщение с 4 цифрами для входа. Продиктуйте их мне, пожалуйста».

На этом запись останавливалась, и ребята обсуждали возможные действия обеих сторон. Следует отметить, что около 44% школьников предлагали все же заключить договор, но при личной встрече. И только 14% обучающихся отметили, что никакого договора с МТС быть не может, а предлагаемые действия – мошенничество.

Преподаватель после обсуждения переходил к информативной части, объясняя, как кроме уже названных школьниками способов, можно снизить киберриски не только в общении с мошенниками, но и на их собственных страницах в социальных сетях.

Еще одной эффективной формой работы со школьниками в области кибербезопасности стало обсуждение проблемных вопросов вместе с модератором в интерактивном кафе «Дилемма» (кейс-технологии). Школьники объединялись в группы по 7-10 человек для решения ситуативных задач, связанных с киберрисками. Целью игры являлось обсуждение альтернативных способов поведения и пополнение знаний учащихся о киберугрозах. В качестве примера приведем несколько ситуаций.

1. На пост девушки в социальных сетях откликнулось несколько пользователей с угрозами ее жизни и здоровью. Как поступить девушке в этом случае? Что делать, если она указала в профиле свой адрес и место обучения?

2. В личные сообщения в мессенджерах юноше поступило сообщение о том, что у написавшего есть фото – и видеоматериалы интимного плана с участием указанного молодого человека. И если он не выполнит то, что от него потребует написавший, то эти фото и видео станут достоянием всех. Что делать в такой ситуации? Выполнить требования шантажиста или…

3. От имени Кости Н. в мессенджеры его друзей и подписчиков стали расходиться сообщения с просьбой скинуть 200 руб. карту. Что делать в этом случае? Помочь другу или…

4. Ане поступило приглашение в неизвестную группу. Что делать: принять его или нет? Ведь можно пропустить, что-то, действительно интересное, а можно стать жертвой мошенников? Как быть?

5. Вы получили сообщение о том, что ваш номер телефона участвовал в розыгрыше автомобиля и вы выиграли, но для подтверждения нужно прислать копию паспорта своего или родителей. Ваши действия.

6. Вы получили сообщение со ссылкой на скачивание видеоконтента. Вши действия.

7. Оля К. познакомилась в социальных сетях с молодым человеком, долго переписывалась с ним. И наконец он назначил ей встречу. Чтобы вы посоветовали Оле?

8. Во время общения в социальной сети вам приходит сообщение от незнакомого человека, который ссылается на общих друзей, называя их по именам, и приглашает вечером погулять. Как вы поступите в этой ситуации? Почему?

После проведения обсуждений в микрогруппах учитель предлагал школьникам обсудить все решения в кругу. Такой подход давал возможность увидеть, услышать и оценить правильность и адекватность предложенных алгоритмов поведения в приведенных выше ситуациях.

Так при обсуждении ситуаций в общем кругу ребята приводили свои варианты решений, а учитель помогал проверить их реалистичность. Так, в первой ситуации, связанной с угрозами жизни и здоровью девушки было несколько решений:

– сообщить значимым взрослым;

– заблокировать сообщения с этих аккаунтов;

– не реагировать;

– ответить им в грубой форме.

Учитель вместе со школьниками разбирали каждое решение и оценивали его адекватность данной ситуации. В результате ребята пришли к выводу, что в подобной ситуации нужно немедленно сообщать значимым взрослым и ни в коем случае не вступать в общение с буллерами.

Проведение кибер-квеста возможно, как во время урока как один из его элементов и как отдельное внеклассное мероприятие. Нами использовались оба варианта. Кибер-квест предполагал прохождение от 1 до 7 этапов в зависимости от временного ресурса. Стоит отметить, что педагоги оценили эффективность этой формы работы и ими было составлено несколько вариантов кибер-квеста. Квест предполагал групповой формат работы. Формировались мини-группы по 5-7 человек, перед которыми ставились задачи на каждом из этапов. В нашем исследовании предлагался кибер-квест, включающий 7 этапов:

1. *Элементарные знания по кибербезопасности*. На этом этапе ребятам предлагалось вопросы и задания, требующие знания основных понятий, применяемых в данной области. Цель этапа; систематизация знаний по кибербезопасности. В нашем случае мы предлагали несколько наборов заданий. Выполнение каждого задания оценивалось в 1 балл. Всего было 5 заданий.

Пример кейса.

1. Почему при общении в сети нужно придерживаться тех же правил поведения, которым вы следуете в реальной жизни?

2. Что такое кибербезопасность?

3. Для чего нужны логины и пароли?

4. Для чего нужен пин-код?

5. Что такое цифровая репутация?

В целом было подготовлено 8 кейсов.

2. *Персональные данные.* На этом этапе школьникам предлагались вопросы, связанные с передачей персональный данных.

Пример кейса.

– Сергей зарегистрирован в «В-контакте». У него более 300 друзей, активная страница. В один из входов в ВК, система предложила ввести свои данные: логин и пароль, но войти все равно не получилось. После долгих мучений и ввода всех данных Сергей был перенаправлен на несуществующую страницу. А на следующий день друзья и подписчики Сергея получили с его страницы сообщения с просьбой выслать денег. Что произошло? [https://edu.cnppm.ru/mod/page/view.php?id=658]

– Эльнара воспользовалась ноутбуком своей подруги для входа в ВК. Что нужно сделать Эльнаре, чтобы оставить минимум личной информации на ноутбуке подруги?

– К чему может привести разглашение личной информации?

– Тонин аккаунт взломали и с ее страницы разослали порнофото и предложения эротического характера в личные сообщения Аня восстановила доступ к аккаунту и поменяла пароль, но было уже поздно. Многие удалили ее из друзей и добавили в черный список, а кто-то даже перестал разговаривать в школе. Что следует сделать Ане для того, чтобы восстановить свою репутацию? Почему следует избегать общения с ботами?

– Почему не следует доверять виртуальным знакомым?

3. *Угрозы киберпространства.* На этом этапе целью является актуализация знаний о киберугрозах и борьбе с ними.

– На сайте Газеты RU https://www.gazeta.ru/tech/2019/11/29/12839030/morris_worm.shtml есть забавная информация: «В ноябре 1988 г. случилась первая эпидемия, вызванная сетевым червем. Червь Морриса заразил от 6000 до 9000 компьютеров в США (включая Исследовательский центр NASA) и практически парализовал их работу сроком до пяти суток. На офисных компьютерах стояла операционная система Unix. Доступ в интернет имел один компьютер, остальные были связаны с ним по локальной сети. Это позволяло маскироваться под задачу легальных пользователей си-

стемы. Однако из-за ошибок в коде безвредная по замыслу программа неограниченно рассылала свои копии по другим компьютерам сети, запускала их на выполнение и таким образом забирала под себя все сетевые ресурсы».

– Какие действия сотрудников могли бы выявить причину заражения?

– Игорю около 2-х недель назад пришло сообщение со ссылкой от друга об онлайн-игре. Игорь перешел по ссылке. Игра оказалась интересной. Парень активно включился в нее. Но через несколько дней поступило сообщение, что игра платная и он играл в долг, который растет с каждым часом. На сегодняшний день его долг составляет около 1500000 рублей. Как поступить Игорю в данной ситуации?

– Какие основные типы киберугроз существуют?

– Какие меры безопасности нужно предпринять для защиты компьютерных систем?

– Какие последствия несут кибератаки для одного пользователя? Для организации?

4. Кибербуллинг. Для подростков угроза кибербуллинга наиболее актуальная, поэтому целью этого этапа является актуализация способов борьбы с кибербуллингом.

Пример кейса.

– Что такое кибербуллинг? Какие законы защищают жертв буллинга? Какое наказание ожидает буллера?

– Группа девятиклассников развлекалась фотосъемками в мужском туалете, а потом шантажировала ребят тем, что выложит фото в социальные сети или разошлет одноклассникам. Андрей оказался одним из тех, кого шантажировали фото. Как ему поступить в этой ситуации?

– Старшеклассники выкладывают в социальные сети короткие видео. Для того, чтобы «поймать сюжет» они придумывают сложные ситуации. Например, выкидывают чью-то сумку в мусорный бак и ждут, когда за ней придет хозяин.

Или назначают встречу двум людям от их имени и по выдуманной причине. Затем все это записывается и отправляется в ВК. А главные герои видео становятся объектами насмешек. Как классифицировать эти действия подростков и что делать тем, кто стал их жертвами?

– Всем известно, что подростки часто группируются по интересам. Вот и сейчас десятиклассники создали группу в ВК, в котрую вступил весь класс, кроме новенькой. Ежедневно все одноклассники обсуждают элитарность этой группы и пишут оскорбительные комментарии ко всем фото и постам новой ученицы. Как классифицировать эти действия подростков и что делать девочке в этой ситуации?

– Перечислите способы поведения в случае, если вы стали жертвой или свидетелем кибербуллинга.

Проведение интерактивной игры «Кибер-умник» позволило выявить индивидуальный уровень знаний и сформированность мотивации формирования навыков кибербезопасности для каждого старшеклассника. Школьникам предлагались индивидуальные задания в форме блиц-опроса. В течение 20 минут старшеклассники должны были ответить письменно на 20 вопросов. Вопросы были взяты из авторского опросника, приведенного в п. 3.1. Для школьной олимпиады задания составлялись учителями-предметниками с учетом уровней сложности.

Результаты исследования понимания социальной и личностной значимости кибербезопасности, умение выделять киберриски до и после эксперимента в контрольной и экспериментальной группах приведены на рисунках 13-14.

Анализ полученных результатов выявил, что в экспериментальной группе существенно снизилось количество респондентов, не осознающих необходимость безопасного поведения в интернет-пространстве. Достоверно возросло число респондентов с низким уровнем осознанности киберрисков (χ^2= 47,5 при $\rho < 0,05$). В тоже время количество респондентов с низким уровнем рискованного повеления возросло (χ^2= 51,6 при $\rho < 0,05$).

В контрольной группе существенных изменений не было [Рисунок 14].

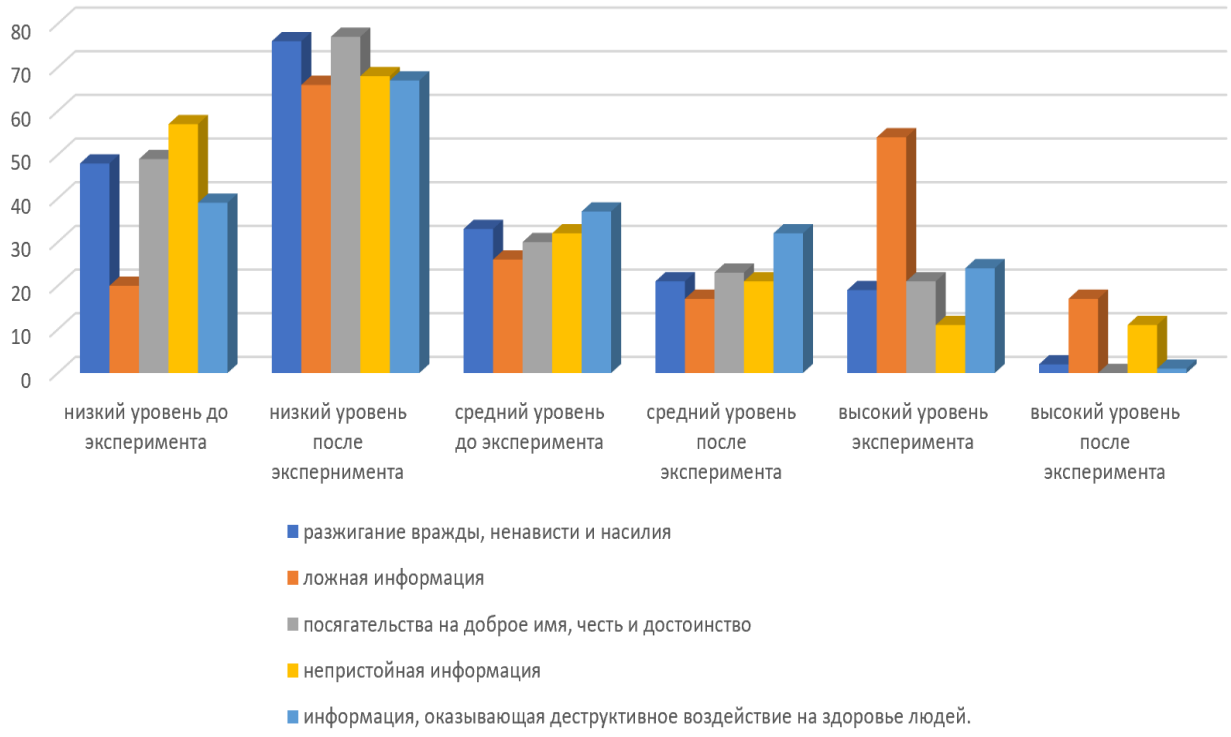


Рисунок 14. Динамика вовлеченности в риски киберпространства экспериментальной группы

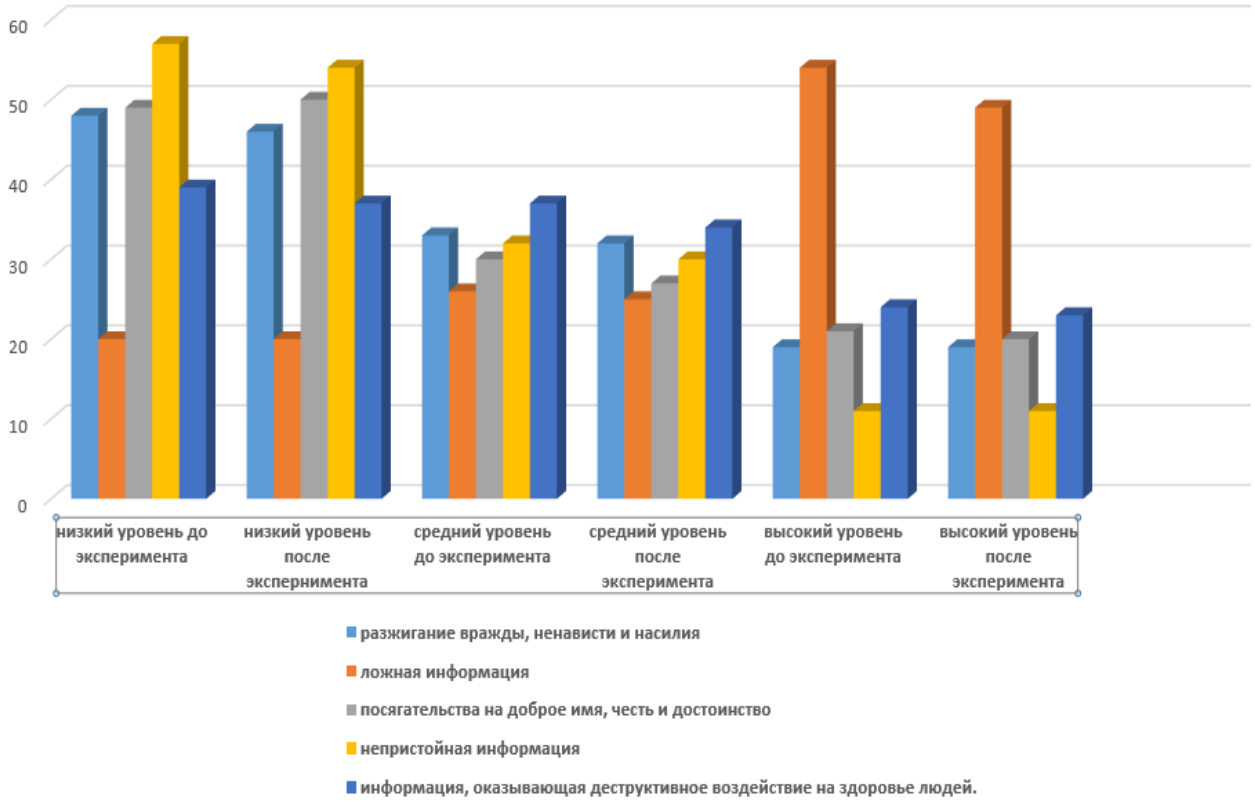


Рисунок 15. Динамика вовлеченности в риски киберпространства контрольной группы

Наблюдение за респондентами экспериментальной группы показало, что вовлечение ребят в групповую деятельность способствовало их интересу к проблеме кибербезопасности. Так, 26 старшеклассников записались в кибердружину, а 54 старшеклассника этой же группы вошли в группу киберволонтеров для работы с учениками младших классов по кибербезопасности. В то время, когда среди респондентов контрольной группы записались в кибердружину – 7 человек, а киберволонтеры – 6 человек.

Второе педагогическое условие связано с развитием критического мышления школьников при поиске и обработке информации, полученной из интернет-источников**.**

Компоненты и формы развития критического мышления при поиске и обработке информации, полученной из интернет-источников представлены в таблице 24.

Таблица 24

Развития критического мышления при поиске и обработке информации, полученной из интернет-источников

Компонент	Содержание	Форма	Технология	Средства
1	2	3	4	5
Когнитивный компонент	знание и умение делать логические умозаключения и обосновывать свой ответ; умение оценивать последовательности умозаключений	интерактивные игры, диалог, дискуссия	кейс-технология	модуль по развитию критического мышления, презентации, методические рекомендации
Деятельностный компонент	умение анализировать и делать заключение о причинах явлений умение анализировать и оценивать содержание текстов умение	семинары, конкурсы, практические занятия	технологии коллективного обучения, технология поиска информации	алгоритм, инструкции, методические рекомендации

Продолжение Таблицы 24

1	2	3	4	5
Рефлексивный компонент	обнаруживать ошибки, связанные с неопределенностью и двусмысленностью выражений и терминов умение обнаруживать релевантную (существенную в данном случае) информацию на фоне избыточной.	недели кибербезопасности, круглые столы, семинары	технологии самостоятельной работы	презентации, инструкции

Модуль по развитию критического мышления предполагал собою серию мероприятий, направленных на формирование и развитие умений делать логические умозаключения и обосновывать свой ответ; оценивать последовательности умозаключений, анализировать и делать заключение о причинах явлений, анализировать и оценивать содержание текстов, обнаруживать ошибки, связанные с неопределенностью и двусмысленностью выражений и терминов, обнаруживать релевантную (существенную в данном случае) информацию на фоне избыточной [Таблица 25].

Для развития навыков критического мышления нами использовались различные виды деятельности, в том числе «Детективные истории». Это интерактивная игра, позволяющая в индивидуальном и групповом формате, привлечь школьника к анализу информации. Школьникам предлагалось опровергнуть или подтвердить следующую информацию. Для этого ребятам на первом этапе предоставлялась возможность поискав Сети Интернет с последующим обсуждением полученной информации.

Таблица 25

Мероприятия, направленные на формирование критического мышления в области кибербезопасности

№ п/п	Мероприятие	Цель	Форма проведения
1.	Детективные истории	Сформировать умение делать логические умозаключения и обосновывать свой ответ; умение анализировать и делать заключение о причинах явлений; умение анализировать и оценивать содержание текстов	Кейс-технологии, интерактивные формы
2.	Тема из записной книжки	Сформировать умение оценивать последовательности умозаключений	Технологии самостоятельной работы, групповые технологии, активные методы, интерактив
3.	Мозговой штурм	Сформировать умение обнаруживать релевантную (существенную в данном случае) информацию на фоне избыточной	Кейс-технологии, интерактив, технологии коллективной работы
4.	Игра «Аналитики»	Сформировать умение обнаруживать релевантную (существенную в данном случае) информацию на фоне избыточной; умение обнаруживать ошибки, связанные с неопределенностью и двусмысленностью выражений и терминов	Технологии самостоятельной работы, групповые технологии, активные методы

Примеры возможных детективных историй, способствующих формированию критического мышления обучающихся.

1. Незнакомым людям нельзя говорить по телефону «Да» или «Нет».

2. Если сайт использует HTTPS – это гарантия того, что он официальный.

3. Жертвами кибербуллинга может стать любой человек.

4. Министерство может взломать один человек.

5. Цель любой кибератаки – получить данные.

6. Удалить всю информацию на смартфоне можно, откатившись до заводских настроек.

7. В суицидальных интернет-сообществах нет ничего опасного для тех, кто просто зашел из интереса.

8. Если на телефон или почту приходят незапрашиваемые коды подтверждения для авторизации, значит аккаунт взломали.

9. Режим «Инкогнито» в браузере обеспечивает полную анонимность в интернете.

10. Синдром Снежаны – исключение и никакого отношения не имеет к обычным пользователям социальных сетей.

11. Если устройство не подключено к интернету, его невозможно заразить вирусами.

12. Я пользуюсь антивирусом – этого вполне достаточно.

13. Сложные пароли – гарантия безопасности.

14. В моих данных нет ничего ценного.

15. Мошенничество и фишинг легко распознать.

16. Посещать известные сайты – безопасно.

17. USB-флешку нужно извлекать только через режим «безопасное извлечение».

18. Сидение близко к монитору портит зрение.

19. Камеру на устройствах нужно заклеивать, чтобы за мной не следили.

20. Разрядка до полного нуля и зарядка до 100% продлят жизнь аккумулятора телефона.

На втором этапе игры с помощью набора мифов школьникам предлагалось составить детективную историю. используя правдивую и ложную информацию в области кибербезопасности.

Примеры истории, составленные некоторыми группами респондентов.

Детективная история № 1

«Агент Косинус попал в техногенный мир и всеми силами пытался освоиться в нем и стать своим. В его задачи входил технический шпионаж в пользу планеты Альфа-Бета-Гамма. Планета Земля и планета Альфа-Бета-Гамма находились не в лучших отношениях, поэтому разоблачение агента могло стать критичным как для самого Косинуса, так и для его планеты в целом. Первым шагом агента было погружение в пространство, которое земляне называли виртуальным. Агент сразу завел себе страницу в странной сети «ВК» и заполнил свой

профиль. Естественно, как настоящий шпион, он указал имя Константин, город проживания – Симферополь, возраст – 270 лет (Косинус был еще молод), Затем Косинус озаботился подборкой друзей. Во время подготовки агента предупреждали, что наличие друзей в социальных сетях – это именно то, что нужно сделать сразу. Они, по мнению, руководителей Косинуса, обладают всей необходимой информацией для выполнения его миссии. Косинус старался из всех сил. Уже к вечеру второго дня у него было более 1500 друзей. У них агент и уточнял все про виртуальные миры и покупку шпионского оборудования. Через три дня агент потратил половину выданных ему денег на покупку нужного шпионского оборудования по скидке в 99% на сайте, ссылку на который скинул ему один из виртуальных друзей. Еще через неделю он удивился техническому прогрессу землян, получив по почте России, две пары носков и переноску для кошки, ценою в 100 тыс. рублей. Очевидно, именно эти предметы и были нужным шпионским оборудованием. Чтобы не отличаться от других сограждан, Косинус активно участвовал во всех акциях и лотереях, которые обещали ему телефон в подарок, автомобиль в качестве выигрыша. Косинус поражался бестолковости землян, которые отдают такие дорогие вещи за сущие копейки предоплаты. Правда после предоплаты выигрыши не приходили, но Косинус догадывался, что почта России может быть перегружена рассылками выигрышей счастливчикам. За первый месяц агент растратил все деньги, влюбился в прекрасную Львицу, назначил ей встречу. Правда на встречу пришли три небритых мужика и полностью лишили Косинуса всех шпионских аксессуаров, обеспечивающих ему связь с Альфа-Бета-Гаммой. Львица на связь больше не выходила. Косинус страдал. Он стал бояться всего: общаться с незнакомыми людьми, покупать товары… Он даже заклеил камеру своего ноутбука, чтобы никто не мог подглядывать за ним. Именно это и стало последним пунктом его шпионской деятельности. Когда, сидя на лавочке в парке, он пытался с ноутбука с заклеенной камерой

отправить сообщение на Альфа-Бета-Гамму по подсказке бота Алисы, к нему подошли первоклашки и понаблюдав за его мучениями спросили: «Дядя, ты – шпион или инопланетянин?».

Косинус поднял руки вверх и обреченно сказал: «Инопланетянин». Скорую вызвали проходившие мимо люди.

Что не так делал Косинус, постигая виртуальный мир? Назовите его основные ошибки».

Детективная история № 2

«Агент Васья был давно завербован Моссадом и поэтому четко придерживался всех правил разведки. Васья никогда не говорил по телефону слов «Да» или «Нет» потому, что твердо знал: его согласие может привести к утечке личных данных через голосовое сообщение. Поэтому Васья предпочитал молчать в трубку.

Васья никогда не пользовался непроверенными сайтами, если они не использовали HTTPS. Агент знал, что HTTPS – это гарантия того, что сайт официальный.

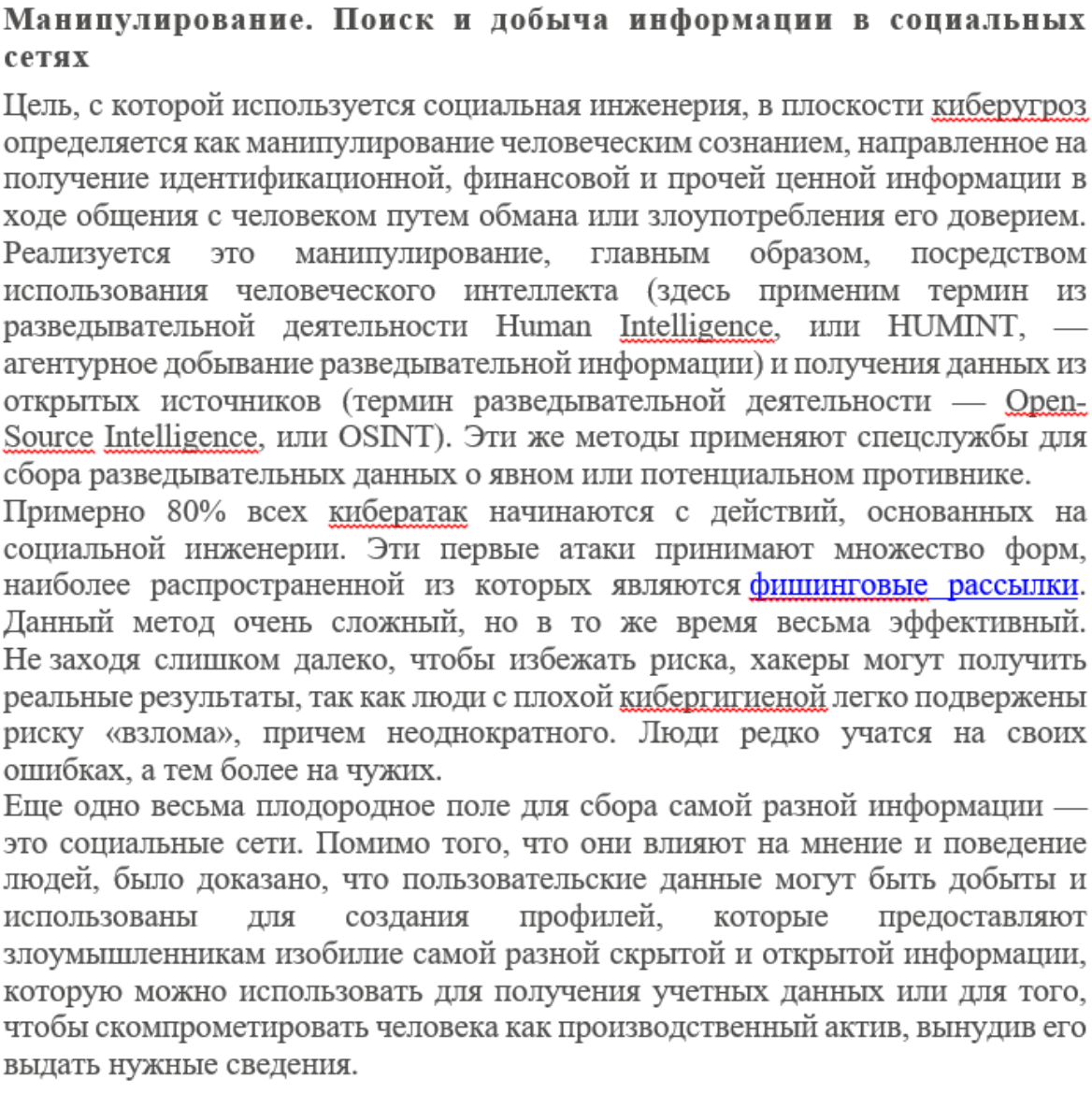
Осторожность – это второе имя Васьи. Чтобы не провалить поставленные задачи Васья ежечасно удалял всю информацию на смартфоне, откатившись от заводских настроек, а в браузер выходил только в режиме «Инкогнито» для обеспечения полной анонимности в интернете. Для предотвращения слежки Васья заклеил камеру на телефоне. Использовал сложные пароли. И был уверен, что ему ничего не грозит.

Когда ему на почту стали приходить незапрашиваемые коды подтверждения для авторизации, он понял, что аккаунт взломали. А когда ему в личку стали поступать письма от анонимов, которые знали про него все (они так и писали: «Знаю про Вас все или… мне известно, чем Вы занимаетесь, сидя у компьютера. Если Вы не отправите по указанному счету 1000000 рублей, то я размещу все это

в Интернете»), Васья понял, что он попал по-крупному. Уходил он через суицидальные сообщества. Навсегда. Хотя зашел просто посоветоваться».

Что не так делал Васья?

Кроме того, школьникам предлагались различные блоки информации для анализа и поиска несоответствий. Эффективным оказался метод анализа текстов с последующим разбором методов борьбы с явлением. В качестве примера приведем следующий фрагмент, взятый на сайте https://controleng.ru/programmnye-sredstva/bezopasnost-programmnye-sredstva/ugroza-kiberbezopasnosti/ [Рисунок 16].



Манипулирование. Поиск и добыча информации в социальных сетях

Цель, с которой используется социальная инженерия, в плоскости киберугроз определяется как манипулирование человеческим сознанием, направленное на получение идентификационной, финансовой и прочей ценной информации в ходе общения с человеком путем обмана или злоупотребления его доверием. Реализуется это манипулирование, главным образом, посредством использования человеческого интеллекта (здесь применим термин из разведывательной деятельности Human Intelligence, или HUMINT, — агентурное добывание разведывательной информации) и получения данных из открытых источников (термин разведывательной деятельности — Open-Source Intelligence, или OSINT). Эти же методы применяют спецслужбы для сбора разведывательных данных о явном или потенциальном противнике.

Примерно 80% всех кибератак начинаются с действий, основанных на социальной инженерии. Эти первые атаки принимают множество форм, наиболее распространенной из которых являются фишинговые рассылки. Данный метод очень сложный, но в то же время весьма эффективный. Не заходя слишком далеко, чтобы избежать риска, хакеры могут получить реальные результаты, так как люди с плохой кибергигиеной легко подвержены риску «взлома», причем неоднократного. Люди редко учатся на своих ошибках, а тем более на чужих.

Еще одно весьма плодородное поле для сбора самой разной информации — это социальные сети. Помимо того, что они влияют на мнение и поведение людей, было доказано, что пользовательские данные могут быть добыты и использованы для создания профилей, которые предоставляют злоумышленникам изобилие самой разной скрытой и открытой информации, которую можно использовать для получения учетных данных или для того, чтобы скомпрометировать человека как производственный актив, вынудив его выдать нужные сведения.

Рисунок 16. Фрагмент текста для анализа 1

В ходе анализа перед школьниками были поставлены следующие вопросы:

– Что лежит в основе нарушений людьми кибербезопасности? – умение делать логические умозаключения и обосновывать свой ответ;

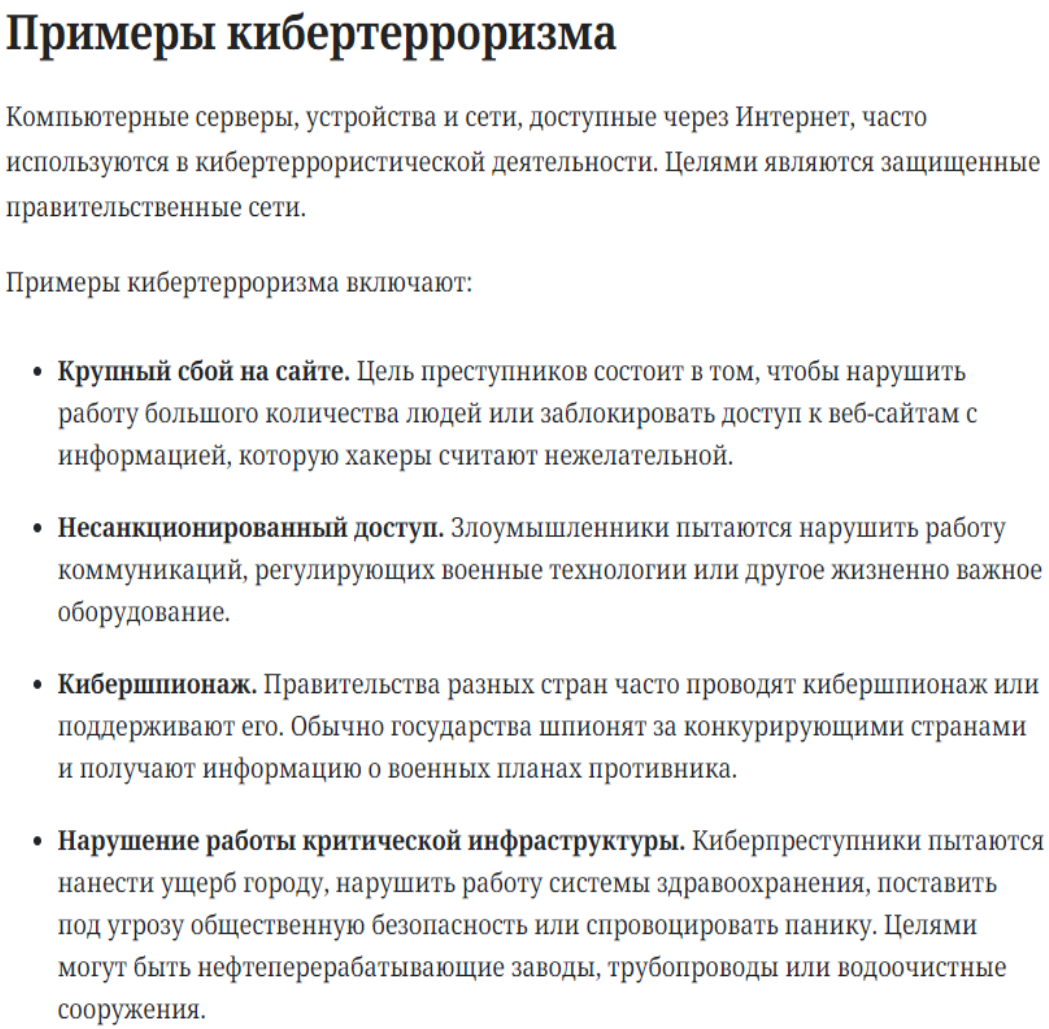
– Каким образом социальная инженерия добивается нарушений людьми кибербезопасности? – умение оценивать последовательности умозаключений;

– В чем причина киберрискованного поведения людей? – умение анализировать и делать заключение о причинах явлений;

– В чем заключается главный посыл текста? – умение анализировать и оценивать содержание текстов;

– умение обнаруживать ошибки, связанные с неопределенностью и двусмысленностью выражений и терминов;

– Какая информация в этом тексте является наиболее существенной, а какая второстепенной? – умение обнаруживать релевантную (существенную в данном случае) информацию на фоне избыточной.



Примеры кибертерроризма

Компьютерные серверы, устройства и сети, доступные через Интернет, часто используются в кибертеррористической деятельности. Целями являются защищенные правительственные сети.

Примеры кибертерроризма включают:

- **Крупный сбой на сайте.** Цель преступников состоит в том, чтобы нарушить работу большого количества людей или заблокировать доступ к веб-сайтам с информацией, которую хакеры считают нежелательной.
- **Несанкционированный доступ.** Злоумышленники пытаются нарушить работу коммуникаций, регулирующих военные технологии или другое жизненно важное оборудование.
- **Кибершпионаж.** Правительства разных стран часто проводят кибершпионаж или поддерживают его. Обычно государства шпионят за конкурирующими странами и получают информацию о военных планах противника.
- **Нарушение работы критической инфраструктуры.** Киберпреступники пытаются нанести ущерб городу, нарушить работу системы здравоохранения, поставить под угрозу общественную безопасность или спровоцировать панику. Целями могут быть нефтеперерабатывающие заводы, трубопроводы или водоочистные сооружения.

Рисунок 17. Фрагмент текста для анализа 2

Следует отметить, что всего было подобрано 30 фрагментов текста для анализа. Каждый из них нес информацию о киберугрозах и способах борьбы с ними.

На этом этапе нами широко использовались технологии самостоятельной работы при проведении анализе информации по схеме Фишбоун – школьникам предлагались ссылки на сайты с нужной для работы информацией. Задача ребят была в оценке, систематизации и иерархизации этой информации.

Еще одной формой с применением технологии самостоятельной работы стал метод записной книжки Хефеле. За неделю до мероприятия старшеклассникам выдавались записные книжки, в которых предлагалось собрать информацию по предложенной теме. Записей должно быть не менее 7-ми по дням недели. Это

может быть бытовая информация – одноклассники рассказали, что стали жертвами фишинга. Это может быть научная или научно-популярная информация.

Еще одной эффективной формой стал метод фокальных объектов. Школьникам предлагалось перенести на заданный объект новые свойства. Например, определить сходство между существующими киберугрозами и преступлениями в реальном пространстве. Следует отметить, что такая форма работы заставляет школьников задуматься о том, что из себя представляет киберугроза. В некоторых случаях школьники находили примеры мошенничества героев в художественных произведениях, например, в рассказе Николая Лескова «Старый гений» - должник не собирается отдавать долг женщине и оставляет ее без средств к существованию. Школьники, проанализировав произведение, находят его отражение в нынешних финансовых схемах и отмечают, что благополучный исход не всегда возможен. Такой подход позволяет выработать эффективный алгоритм поведения и понять мотивы злоумышленников.

Среди коллективных технологий нами была взята форма мозгового штурма, когда старшеклассники обсуждали тему «Защита персональных данных».

– Что грозит человеку, у которого произошла утечка персональных данных?

– От кого нужно защищать персональные данные?

– Как защитить персональные данные?

Результаты диагностики уровня сформированности критического мышления у школьников экспериментальной группы представлены на рисунке 18.

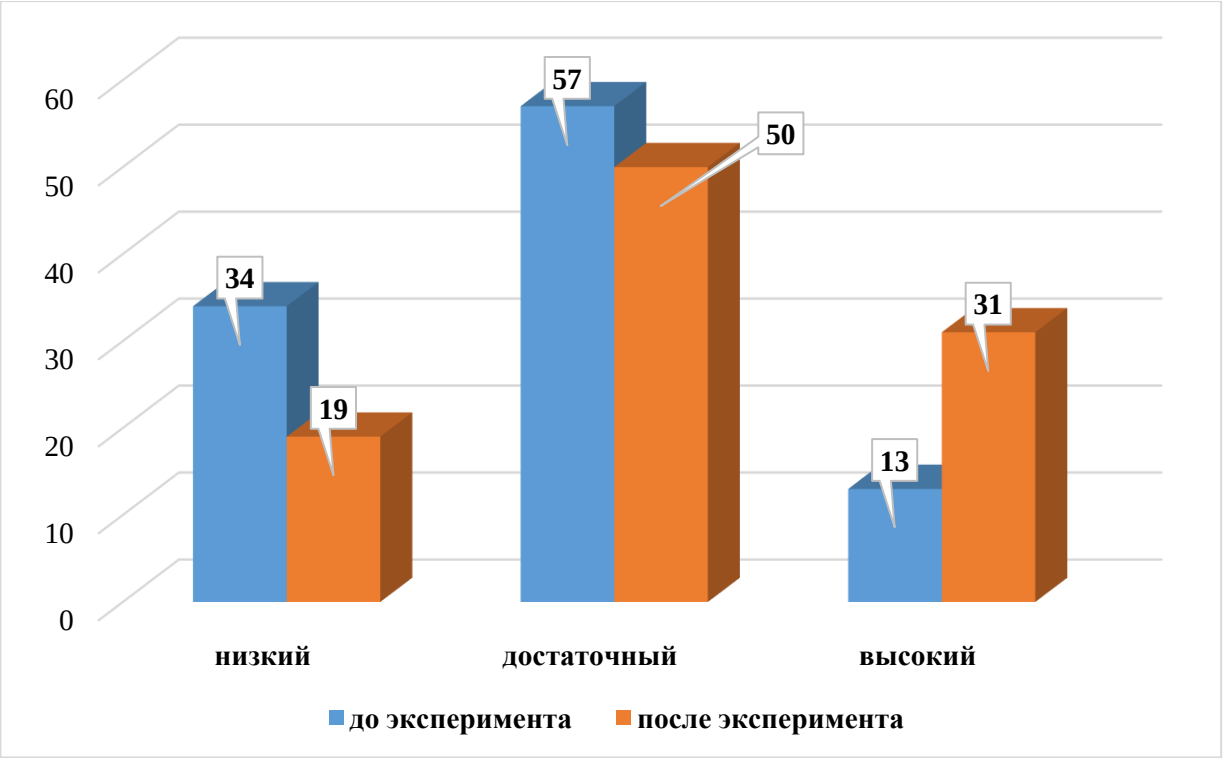


Рисунок 18. Динамика сформированности критического мышления в экспериментальной группе

Мы считаем, что такие результаты связаны созданием благоприятных условий для развития мыслительных операций.

В контрольной группе тоже происходили стихийные переходы с одного уровня на другой. Мы связываем это с тем, что школьников невозможно изолировать от цифровой среды и они стихийно получают знания, кроме того, информатика является обязательным предметом, прописанным во ФГОС СО. Однако существенных изменений зафиксировано не было [Рисунок 18].

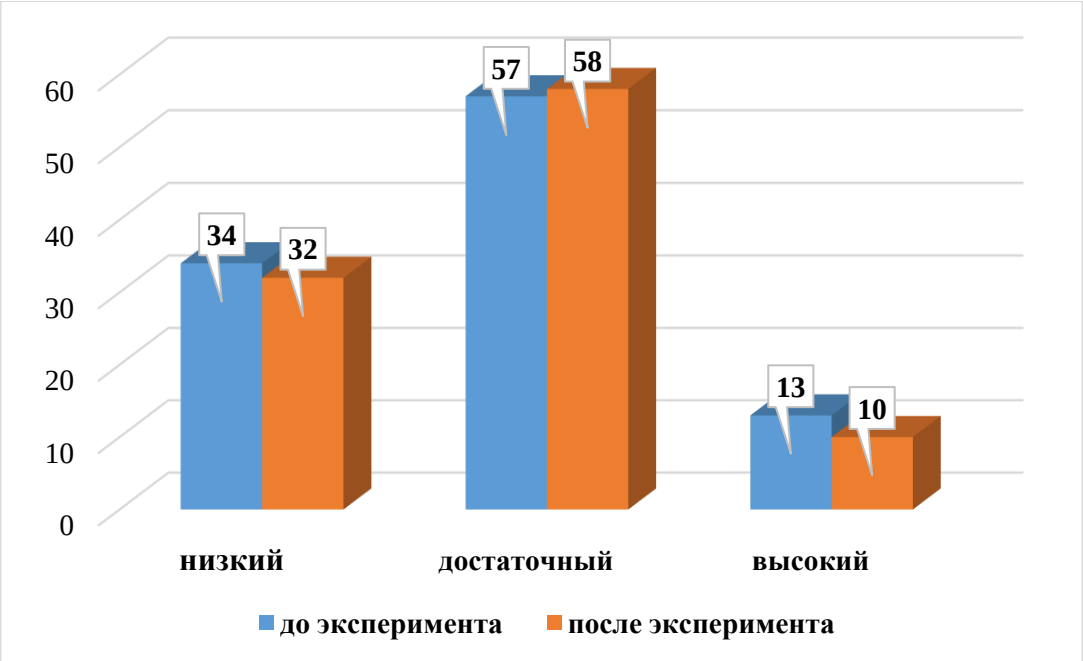


Рисунок 19. Динамика сформированности критического мышления в контрольной группе

Результаты диаграмм [Рисунки 18 и 19] выявили динамику сформированности критического мышления в ЭГ.

Третьим педагогическим условием, необходимым для эффективного формирования навыков кибербезопасности стало осуществление рефлексии на основе применения механизмов самопознания, самоанализа и самоконтроля.

С целью выявления уровня сформированности рефлексии респондентов контрольной и экспериментальной групп было предложено дать субъективную оценку своему уровню знаний в области кибербезопасности. Следует отметить, что полученные результаты не имели достоверных отличий. Школьники обеих групп показали, что их уровень знаний существенно вырос за последние 6 месяцев (именно столько длился эксперимент в экспериментальной группе).

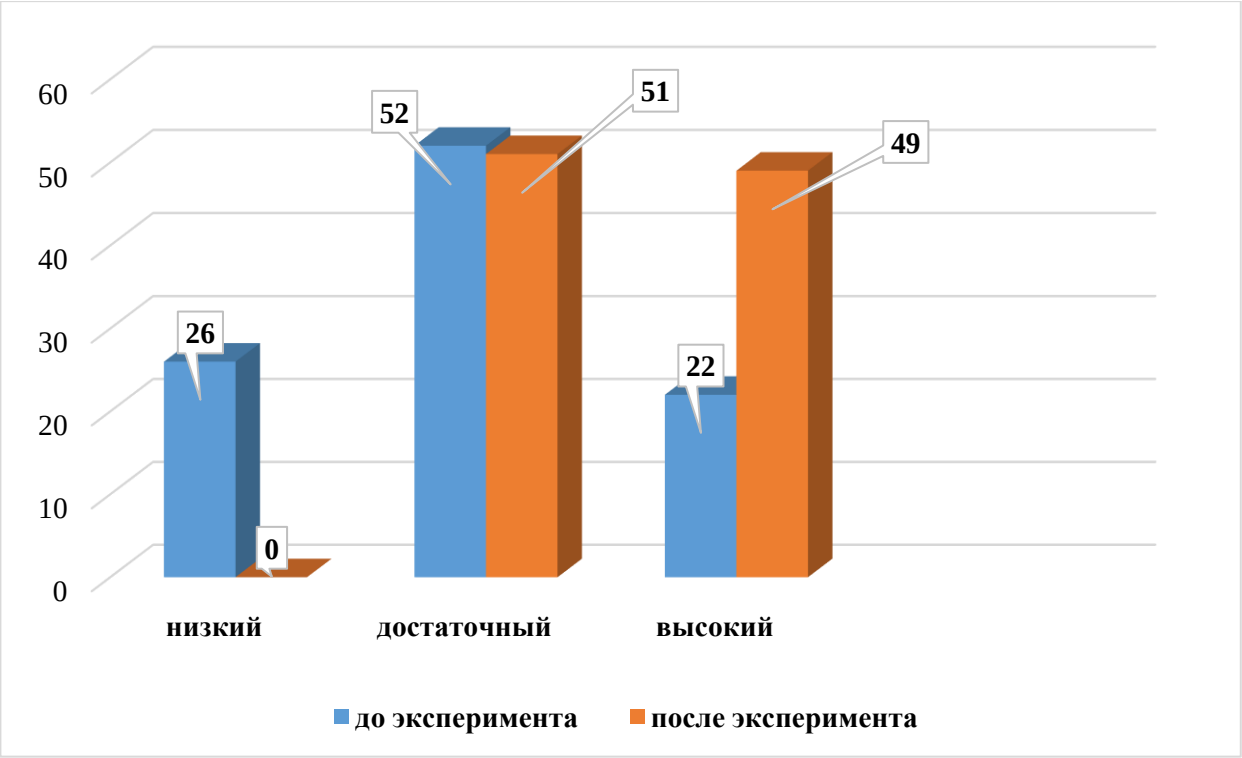


Рисунок 20. Результаты сформированности уровня знаний по кибербезопасности до и после эксперимента в экспериментальной группе

Однако проведенное следом диагностическое исследование показало, что возрастание уровня знаний произошло только в экспериментальной группе [Рисунок 20]. После эксперимента значительно увеличилось количество школьников с достаточным и высоким уровнями знаний.

В то же время в контрольной группе существенных изменений не произошло, но наблюдались единичные изменения уровня знаний. Мы связываем их со стихийным приобретением информации и учебной программой.

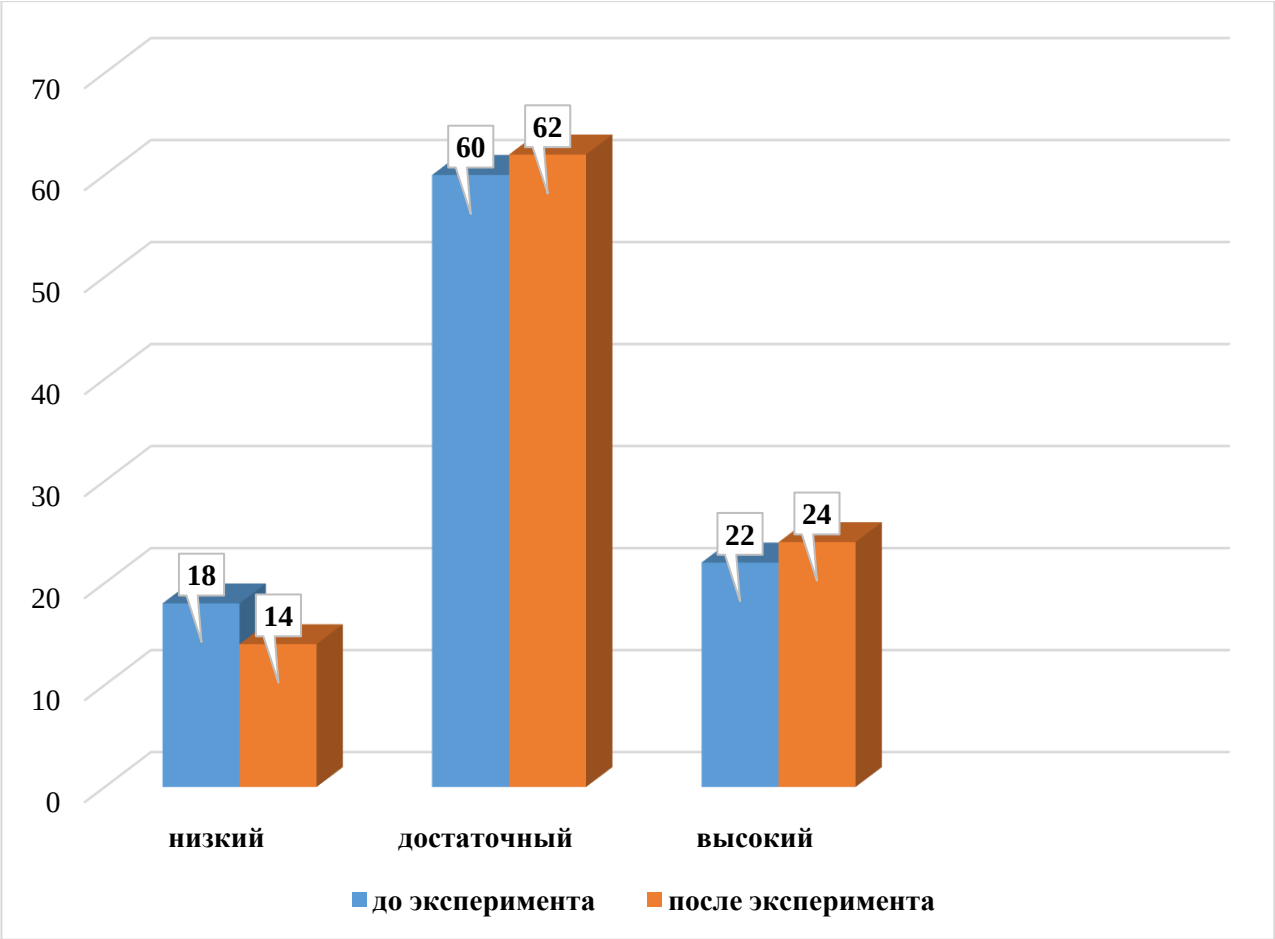


Рисунок 21. Результаты сформированности уровня знаний по кибербезопасности до и после эксперимента в контрольной группе

Значительные изменения произошли в представлениях старшеклассников о том, где можно получить помощь в случае сложной ситуации, связанной с киберугрозами.

Следует отметить, что в случае киберугроз старшеклассники экспериментальной группы после проведенных мероприятий предпочитают обращаться педагогам и родителям, что достоверно отличается от результатов той же группы до эксперимента (χ^2=48,2 и χ^2=49,7 соответственно при $\rho<0,05$). Мы считаем, что такие показатели указывают на высокую степень доверия взрослым в вопросах киберзащиты. Остаются неизменными показатели обращения школьников к продвинутым IT-специалистам, а вот количество обращения к друзьям сократилось. Ребята объясняют это тем, что друзья, в большинстве случаев, просто поддерживают, но решение ситуации порой лежит за пределами их возможностей.

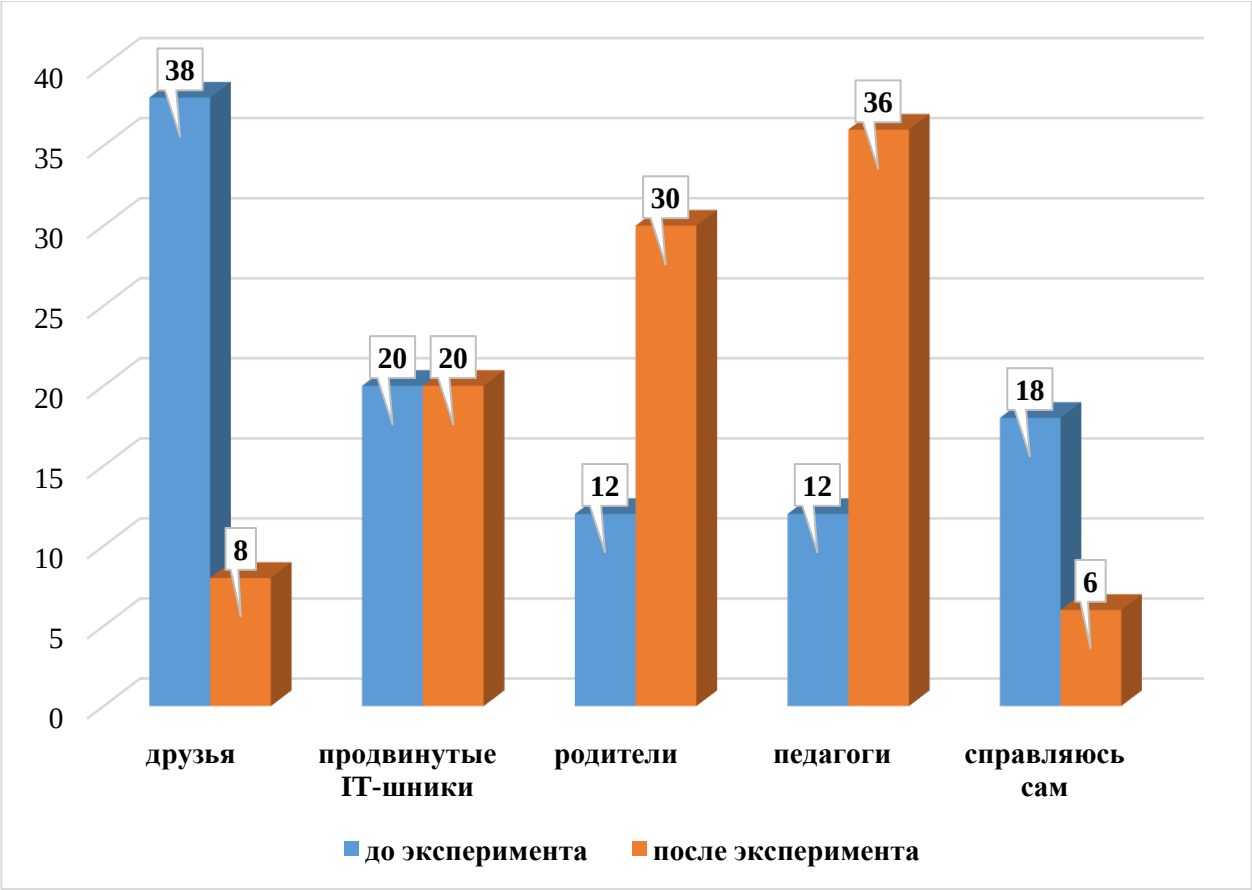


Рисунок 22. Динамика обращений за помощью в экспериментальной группе

В то же время респонденты экспериментальной группы стали меньше обращаться к друзьям и чаще искать помощь у IT-специалистов, однако количество самостоятельных решений существенно снизилось с 18% до 6%.

Динамика обращений за помощью в контрольной группе тоже претерпела изменения. Так ребята, по-прежнему, чаще всего за помощью обращаются к друзьям и продвинутым специалистам [Рисунок 23].

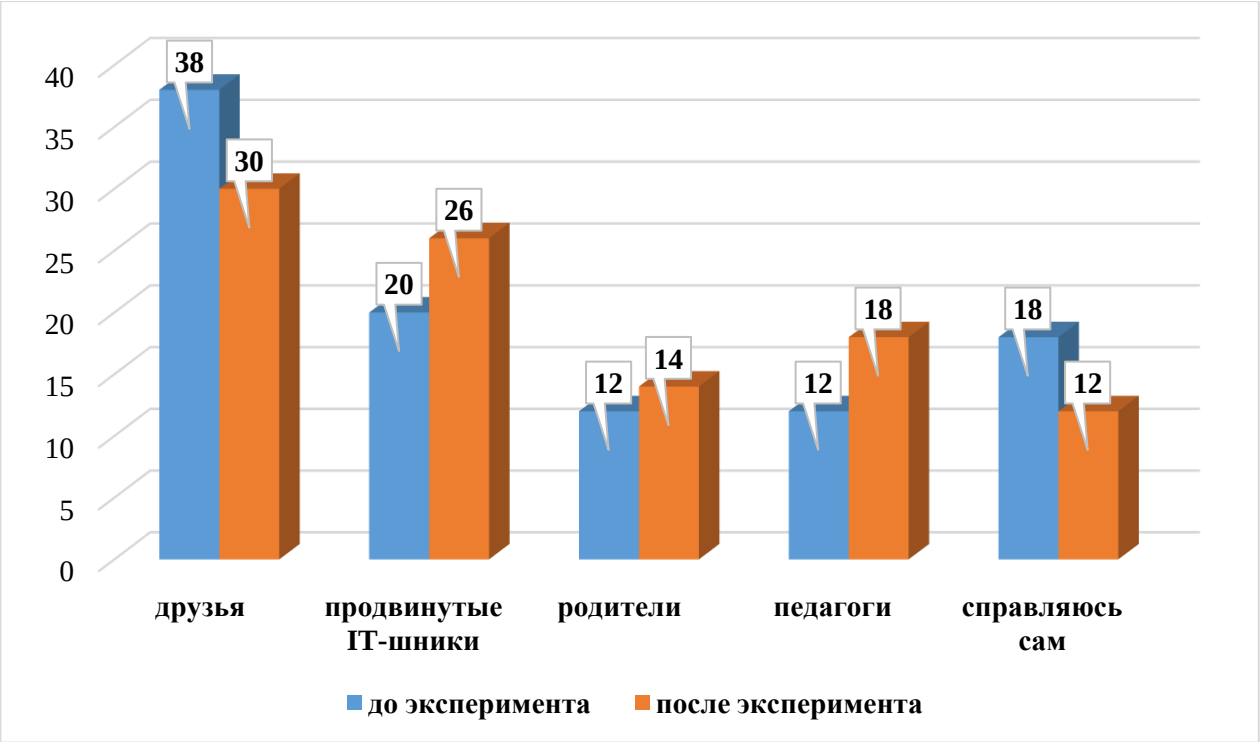


Рисунок 23. Динамика обращений за помощью в контрольной группе

Однако, количество обращений ко взрослым тоже возросло. Несколько уменьшилось количество ответов о том, что респондент справится сам. Возможно, пример параллельных классов, где учатся подростки, входящие в экспериментальную группу, позитивно повлиял на рефлексивное поведение школьников контрольной группы.

Результаты исследования динамики склонности к киберрискам у респондентов обеих групп до и после эксперимента приведены в таблицах 26-27.

Таблица 26

Результаты исследования склонности к киберрискам у респондентов экспериментальной группы

Тип риска	Низкий уровень		Достаточный уровень		Высокий уровень	
	до	после	до	после	до	после
1	2	3	4	5	6	7
Риски, связанные с получением деструктивной информации	39	67	44	19	27	14

Продолжение Таблицы 26

1	2	3	4	5	6	7
Риски, связанные с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет	51	89	27	11	22	0
Осознание рисков киберпространства	35	3	44	66	21	31
Склонность к рискам	32	76	32	14	34	10

Как видно по результатам, представленным в таблице 26, произошли достоверные изменения по всем шкалам в экспериментальной группе. Выросло осознание киберрисков как проблемы. Школьники стали серьезно относиться к проблемам фишинга, буллинга. В тоже время поведение старшеклассников экспериментальной группы стало рефлексивнее, чем до эксперимента. Достоверно уменьшилось количество респондентов, склонных к киберрискам (χ^2=48,54 при ρ<0,05).

Результаты исследования склонности к киберрискам у респондентов контрольной группы приведены в таблице 27.

Таблица 27

Результаты исследования склонности к киберрискам у респондентов контрольной группы

Тип риска	Низкий уровень		Достаточный уровень		Высокий уровень	
	до	после	до	после	до	после
Риски, связанные с получением деструктивной информации	39	42	44	41	27	17
Риски, связанные с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет	51	48	27	22	22	30
Осознание рисков киберпространства	35	35	44	47	21	18
Склонность к рискам	32	34	32	33	34	33

Как видно по результатам, приведенным в таблице 27, существенных изменений не произошло. Таким образом проведенное исследование показало эффективность предлагаемой модели.

Выводы по Главе 3

Основными критериями сформированности навыков кибербезопасности обучающихся выступают: мотивационно-стимулирующий (показатели понимания социальной и личностной значимости кибербезопасности; стимулирования поведения обучающихся к соблюдению информационной безопасности; сформированность мотивов по противодействию подростков киберугрозам и киберрискам; проявление у обучающихся интереса к информационной безопасности), когнитивно-содержательный (знания в области кибербезопасности; знания обучающихся о методах и средствах противостоянию киберугрозам и киберрискам; ценностные ориентации по противодействию кибербезопасности), деятельностно-поведенческий (умения по соблюдению информационной этики; аналитические умения по отбору информации; творческая активность при решении проблемных ситуаций; критическое мышления обучающихся при выборе способов противостоянию киберугрозам; способы защиты при встрече с киберугрозами и рисками; системность и гибкость использования теоретических знаний; умение находить причинно-следственные связи и обосновывать практические действия); эмоционально-волевой (самооценка волевых качеств подростками с подключением механизмов самоанализа, самопознания и самоконтроля; уровень саморегуляции подростка в интернет-пространстве).

При изучении критериев сформированности навыков кибербезопасности обучающихся выявилась недостаточность доказательного диагностического инструментария. В связи с этим для проверки мотивационно-стимулирующего критерия кибербезопасности обучающихся разработан опросник «Риски киберпространства», целью которого является выявление группы рисков, к которым склонен подросток и определение уровня сформированности у подростка способов защиты; для изучения деятельностно-поведенческого критерия адаптирован опросник определения уровня критического мышления, составлен опросник информационной этики; для изучения когнитивно-содержательного критерия раз-

работан авторский опросник опросник инструментальных навыков в области кибербезопасности. В основе исследовательского опросника для определения умений по соблюдению информационной этики лежали правила сетевого этикета, опубликованные на сайте лаборатории Kaspersky; для изучения эмоционально-волевого критерия адаптирована методика Дембо-Рубинштейн для реального и виртуального пространства по шкалам: уверенность-неуверенность, безопасность – опасность, доверие – недоверие.

Эмпирическое исследование мотивационно-стимулирующего критерия сформированности кибербезопасности обучающихся показало наличие определенных проблем в мотивации и определении места безопасности в киберпространстве со стороны обучающихся: наиболее частым риском, связанным с получением деструктивной информации, является «ложная информация», «посягательство на доброе имя», «деструктивное воздействие на здоровье». Только 20% респондентов осознанно относится к рискам киберпространства и в случае необходимости сообщают об этом взрослым

Эмпирически выявлены признаки опасной ситуации по мнению подростков: навязчивость собеседника; прямые угрозы, требование персональных данных, уговоры со стороны собеседника, многократный переход по ссылкам и требование предварительной оплаты. Более 80% подростков при идентификации ситуации как опасной обращаются за помощью или просто рассказывают об этом в интернет-сообществах, в чатах и к друзьям, а 11% выборки не делится со своей проблемой ни с кем. Основными мотивами подростков в общении с киберпреступниками являются азарт, власть, безысходность, агрессия, интерес, доверие.

Результаты изучения когнитивно-содержательного критерия показало, что наиболее проблемными областями знаний по кибербезопасности являются: знания в области цифровой репутации, о методах и средствах противостоянию киберугрозам и киберрискам, правовые нормы ответственности за участие в схемах кибермошенников. Витальные и социальные ценности занимают третье и второе место соответственно в иерархии ценностей данной выборки.

Результаты эмпирического исследования деятельностно-поведенческого критерия показали, что: 47% выборки имеет достаточный уровень сформированности умений по соблюдению информационной этики; у 34% и 13% респондентов начальный (низкий) и высокий уровень развития критического мышления соответственно. Эмпирическое исследование деятельностно-поведенческого критерия показало наличие трудностей, связанных с осознанными поступками в области обеспечения собственной безопасности в интернет-пространстве у ряда подростков.

Проблемными зонами в формировании кибербезопасности старшеклассника являются: несформированность мотивов безопасной деятельности в Сети; отсутствие или недостаточность знаний о киберугрозах и способах борьбы с ними; несформированность умений, определяющих критическое мышление подростка; легкомысленное отношение к проблеме кибербезопасности в целом, свойственное подросткам; особенности подросткового возраста в области определения авторитетов и референтных групп.

Модель педагогического сопровождения процесса формирования кибербезопасности старшеклассников построена с учетом следующих педагогических условий: формирование положительной мотивации обучающихся к учебной и внеклассной деятельности; развитие критического мышления при поиске и обработке информации, полученной из интернет-источников; использование интерактивной среды при решении ситуаций, связанных с кибербезопасностью обучающихся; осуществление рефлексии на основе применения механизмов самопознания, самоанализа и самоконтроля.

Для участия в формирующем эксперимента привлекались те же обучающиеся, что и для участия в констатирующем. В контрольную группу (КГ) вошли 128 обучающихся 9-х классов, из них 77 девочек, 51 мальчик. В экспериментальную группу вошло 130 обучающихся 9-х классов, из них 58 мальчиков и 72 девочки. Уровень сформированности навыков кибербезопасности в обеих группах существенно не различался.

Реализация педагогического условия, заключающегося в формировании положительной мотивации обучающихся к учебной и внеклассной деятельности, способствующей формированию навыков кибербезопасности, позволила в экспериментальной группе существенно снизить количество респондентов, не осознающих необходимость безопасного поведения винтернет-пространстве, способствовало их интересу к теме кибербезопасности. В контрольной группе существенных изменений не произошло.

Реализация педагогического условия, связанного с развитием критического мышления школьников при поиске и обработке информации, полученной из интернет-источников, позволила повысить уровень сформированности критического мышления у 35% школьников ЭГ.

Использование интерактивной среды стало сквозным элементом, проходящим через все мероприятия по кибербезопасности, Большую роль в подготовке школьников по вопросам кибербезопасности сыграли учителя информатики, разработавшие целый цикл занятий в этом направлении с использованием ИКТ.

Реализация педагогического условия, заключающегося в осуществлении рефлексии на основе применения механизмов самопознания, самоанализа и самоконтроля, позволила сформировать адекватное отношение к киберрискам и киберугрозам со стороны старшеклассников. Старшеклассники экспериментальной группы после проведенных мероприятий предпочитают обращаться педагогам и родителям, что достоверно отличается от результатов той же группы до эксперимента (χ^2=48,2 и χ^2=49,7 соответственно при $\rho<0,05$).

ЗАКЛЮЧЕНИЕ

В ходе анализа научных исследований выявлено, что вопросы кибербезопасности обучающихся и умения их противостоять киберрискам и киберугрозам занимают центральное место в системе государственных приоритетов и привлекают внимание образовательных структур.

1. Теоретический анализ научной литературы позволил определить кибербезопасность обучающихся образовательных организаций как составляющую информационной безопасности, направленную на выявление угроз информационного воздействия на личность, поступающих из Интернет-сети и реализации мер по обеспечению ее безопасности в ситуациях риска.

2. Теоретически определено, что педагогическое сопровождение обучающихся в условиях киберрисков и киберугроз представляет специально организованный и контролируемый процесс взаимодействия субъектов сопровождения, направленный на успешное освоение основ кибербезопасности обучающихся.

3. Теоретически обоснована структура модели педагогического сопровождения обучающихся образовательных организаций в условиях киберрисков и киберугроз, включающая мотивационно-целевой, теоретико-методологический, содержательно-процессуальный и оценочно-результативный блоки.

4. Эмпирически выявлены педагогические особенности педагогического сопровождения обучающихся образовательных организаций в условиях киберрисков и киберугроз, а именно:

а. Разработаны и обоснованы оптимальные педагогические условия: обеспечение мотивированного включения обучающихся в деятельность, обеспечивающую их защиту от негативного воздействия информационной среды; развитие критического мышления обучающихся в процессе решения учебных задач по противостоянию киберрискам и киберугрозам; использование интерактивной среды при решении ситуаций, связанных с кибербезопасностью обучающихся;

формирование рефлексивной позиции обучающихся по противодействию киберрискам и киберугрозам) и составляющие педагогического сопровождения обучающихся (формы, технологии и средства).

b. Обоснована необходимость организации педагогического сопровождения обучающихся образовательных организаций в условиях киберрисков и киберугроз на основе применения интерактивных форм, методов и технологий обучения, направленных на обеспечение системы знаний и умений, необходимых сопровождаемым для защиты от вредоносной информации, исходящей из различных сайтов, чатов и других Интернет-ресурсов. Основная поддержка сопровождаемых в условиях противостояния киберрискам и киберугрозам осуществляется педагогом, который выступает в роли коуча, тьютора, наставника, консультанта.

5. Результаты эксперимента выявили позитивную динамику сформированности когнитивно-содержательного, деятельностно-поведенческого и рефлексивно-оценочного компонентов, тем самым, подтвердив эффективность предложенной модели педагогического сопровождения обучающихся образовательных организаций в условиях киберрисков и киберугроз.

Практические рекомендации. Материалы исследования могут быть использованы педагогами для работы по формированию навыков кибербезопасности школьников, профилактики кибербуллинга, попадания в суицидальные группы.

Перспективы дальнейшего исследования видятся в изучении способов формирования навыков кибербезопасности у школьников разных возрастов, склонных к рискованному поведению.

СПИСОК ЛИТЕРАТУРЫ

1. Абдеев, Р.Ф. Философия информационной цивилизации / Р.Ф. Абдеев. – Москва : ВЛАДОС, 1994. – 336 с.: 58 ил.

2. Абдуразаков, М.М. Современные проблемы обеспечения информационной безопасности в образовательно-педагогической сфере / М.М. Абдуразаков, З.О. Батычов // Информатика и образование. – 2021. – Т. 36 (№10). – С. 57–64.

3. Айсина, Р.М. Киберсоциализация молодежи в информационнокоммуникационном пространстве современного мира: эффекты и риски / Р.М. Айсина // Социальная психология и общество. – 2019. – Т. 10. – № 4. – С. 42–57.

4. Алескеров, В.И. Международный опыт противодействия проявлениям экстремизма в сети Интернет / В.И. Алескеров, В.В. Баранов // Академическая мысль. – 2021. – № 2 (15). – С. 122–128.

5. Алигулиев, Р.М. Вопросы защиты детей школьного возраста от интернет-зависимости / Р.М. Алигулиев, Р.Ш. Махмудова, Р.Ш. Махмудов // Дистанционное и виртуальное обучение. – 2011. – № 5. – С. 97–107.

6. Алпеев, А.С. Терминология безопасности: кибербезопасность, информационная безопасность / А.С. Алпеев. – 2014. – № 5. – С. 39–42.

7. Амонашвили, Ш.А. Личностно-гуманная основа педагогического процесса / Ш.А. Амонашвили. – Минск : Университетское, 1990. – 559 с.

8. Анисимов, С.Ф. Духовные ценности: производство и потребление / С.Ф. Анисимов. – Москва : Мысль, 1988. – 253 с.

9. Антология мировой философии : в 4-х т. – Т. 1. – Москва, 1969. – 760 с.

10. Самоорганизующаяся информационная среда с децентрализованным управлением для взаимодействия образовательных учреждений / С.М. Аракелян, А.В. Духанов, В.Г. Прокошев, С.В. Рощин // Сборник научных статей. Интернет-порталы. Содержание и технологии. Выпуск 4 / редкол. : А.Н. Тихонов и др. ; ФГУ ГНИЙ ИТТ «Информика». – Москва : Просвещение, 2007. – С. 440–464.

11. Артамонов, В.А. Кибербезопасность в условиях цифровой трансформации / В.А. Артамонов, Е.В. Артамонова // Цифровая трансформация. – 2021. – №

4 (17). – С. 42–51.

12. Архангельский, С.И. О моделировании и методике обработки данных педагогического эксперимента : материалы лекций, прочит. в Политехн. музее на фак. программиров. обучения / С.И. Архангельский, В.И. Михеев, С.А. Машников ; Всесоюз. о-во «Знание». Политехн. музей. Межведомств. науч. совет по проблеме «Программиров. обучение». – Москва : Знание, 1974. – 48 с. : ил.; 20 см.

13. Афанасьев, В.Г. Системность и общество : монография / В.Г. Афанасьев. – Москва : Политиздат, 1980. – 368 с.

14. Афонин, А.Ю. Образовательные Интернет-ресурсы / А.Ю. Афонин, В.Н. Бабешко ; ГНИЙ ИТТ «Информика». – Москва : Просвещение, 2004. – 287 с.

15. Бабанский, Ю.К. Избранные педагогические труды / Ю.К. Бабанский. – Москва : Педагогика, 1989. – 560 с.

16. Байбородова, Л.В. Индивидуализация и сопровождение в образовательном процессе педагогического вуза : монография / Л.В. Байбородова, Л.Н. Артемьева, М.П. Кривунь. – Ярославль : РИО ЯГПУ, Канцеляр, 2014. – 220 с.

17. Ключевые идеи субъектно-ориентированной технологии индивидуализации образовательного процесса в педагогическом вузе / Л.В. Байбородова, В.Н. Белкина, М.В. Груздев, Т.Н. Гущина // Вестник Новосибирского государственного педагогического университета. – 2018. – Т. 8. – № 5. – С. 7–21.

18. Барахсанова, Е. А. Информационные технологии в сфере образования : учебное пособие / Е.А. Барахсанова. – Москва : Академия, 2003. – 240 с.

19. Барышев, Р.А. Киберпространство и проблема отчуждения : автореферат дис. кандидата философских наук : 09.00.11 / Барышев Руслан Александрович; [Место защиты: Сиб. федер. ун-т]. – Красноярск, 2009. – 16 с.

20. Башмаков М.И. Информационная среда обучения / М.И. Башмаков, С.Н. Поздняков, Н.А. Резник. – Санкт-Петербург : СВЕТ, 1997. – 400 с.

21. Безкоровайный, М.М. Кибербезопасность – подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. –

2014. – № 1 (2). – С. 22–27.

22. Безрукова, В.С. Проективная педагогика : учебное пособие для инж.-пед. ин-тов и индустриально-пед. техникумов / В.С. Безрукова. – Екатеринбург : Деловая книга, 1996. – 344 с.

23. Беленов, Н.В. Формирование навыков информационной безопасности в сети интернет у обучающихся 5–9 классов / Н.В. Беленов, О.С. Самсонова // Проблемы современной науки и образования. – 2020. – № 7 (37). – С. 54–57.

24. Беликов, В.А. Философия образования личности: деятельностный аспект : монография / В.А. Беликов. – Москва : ВЛАДОС, 2004. – 357 с.

25. Белоус, А.И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А.И. Белоус, В.А. Солодуха. – Москва: ТЕХНОСФЕРА, 2021. – 482 с.

26. Белякова, О.С. Исследование навыков кибербезопасности стандарта SFIA8 / О.С. Белякова, В.А. Сухомлин // International Journal of Open Information Technologies. – 2022. – Vol. 10. – №7. – С 156–164.

27. Белякова, Е.Г. Информационная культура и информационная безопасность школьников / Е.Г. Белякова, Э.В. Загвязинская, А.И. Березенцева // Образование и наука. – 2017. – Т. 19. – № 8. – С. 147–162.

28. Березова, Н.А. К вопросу о технологиях тьюторского сопровождения будущих педагогов / Н.А. Березова // Экономические и гуманитарные исследования регионов. – 2020. – № 1. – С. 25–30.

29. Бескоровайный, М.М. Информационная безопасность в сфере образования и науки / М.М. Бескоровайный, А.П. Тутузов // Информационная безопасность в сфере образования и науки // Информатизация и связь. – 2011. – № 6. – С. 34–39.

30. Бешенков, С.А. Информатика. Систематический курс : учебник для 10 класса / С.А. Бешенков, Е.А. Ракитина. – Москва : Лаборатория Базовых Знаний, 2001. – 432 с.

31. Блауберг, И.В. Становление и сущность системного подхода / И.В.

Блауберг, Э.Г. Юден. – Москва : Наука, 1973. – 270 с.

32. Богословский, В.И. Научное сопровождение образовательного процесса в педагогическом университете: методологические характеристики : монография / В.И. Богословский. – Санкт-Петербург : Изд-во РГПУ им. Герцена, 2000. – 144 с.

33. Бондаревская, Е.В. Ценностные основания личностного ориентированного образования / Е.В. Бондаревская // Педагогика. – 1995. – № 4. – С. 29–36.

34. Будунов, Г.М. Компьютерные технологии в образовательной среде: «за» и «против» / Г.М. Будунов. – Москва : Аркти, 2006. – 192 с.

35. Буряк, В.В. Проблематика кибербезопасности в информационном обществе / В.В. Буряк // Юридический факт. – 2018. – № 32. – С. 99–102.

36. Быкова, Е.В. Информационная безопасность в школе / Е.В. Быкова // Образование и информационная культура: теория и практика : материалы Межрегионального форума, Ульяновск, 03 декабря 2017 года / под редакцией В.Г. Шубовича. – Ульяновск : Ульяновский государственный педагогический университет им. И.Н. Ульянова, 2017. – С. 19–21.

37. Вангородский, С.Н. Основы кибербезопасности : учебно-методическое пособие. 5–11 классы / С.Н. Вангородский. – Москва : Дрофа, 2019. – 238 с.

38. Векшарева, Д.М. Человек IT-цивилизация. Крупнейшие кибератаки / Д.М. Векшарева // Россия и мир в новое и новейшее время - из прошлого в будущее : материалы XXV Юбилейной ежегодной международной научной конференции : в 4 т. – Санкт-Петербург : Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2019. – Т. 3. – С. 101–102.

39. Владимирова, Т.В. Обеспечение безопасности в условиях информационной не стабильности общества : автореф. дис. докт. философ. наук : 09.00.11 – социальная философия / Татьяна Валерьевна Владимирова. – Красноярск, 2016. – 41 с.

40. Волкова, М.Н. Деятельностный подход и категория деятельности в психологии : учебное пособие / М.Н. Волкова. – Владивосток : Мор. гос. ун-т, 2007.

– 78 с.

41. Волобуева, Т.Б. Конструирование сетевой модели повышения квалификации педагогических кадров / Т.Б. Волобуева // Нижегородское образование. – 2017. – № 3. – С. 72–80.

42. Волокита, А.В. Россия: от информации - к информационному обществу / А.В. Волокитой, Б.В. Кристальный, Д.С. Черешин. – М., 1989. – С. 12–15.

43. Воскрекасенко, О.А. Формирование культуры кибербезопасности в системе профессиональной подготовки обучающихся колледжа как педагогическая система / О.А. Воскрекасенко, А.А. Киреева, Т.Т. Щелина // Современные наукоемкие технологии. – 2022. – № 10-1. – С. 125–129.

44. Выготский, Л.С. Педагогическая психология / Лев Семенович Выготский ; под. ред. В.В. Давидова. – Москва : Педагогика, 1996. – 536 с.

45. Газман, О.С. Новые ценности образования: содержание гуманистического образования / О.С. Газман, Р.М. Вейсс, Н.Б. Крылова. – Москва : Инноватор, 1995. – С. 28–43.

46. Герасимов, И.В. Информатика: Применение сетевых компьютерных технологий : учебное пособие / И.В. Герасимов, В.А. Калмычков, Л.А. Чугунов. – Санкт-Петербург : СПГЭТЛЭТИ, 2004. – 72 с.

47. Герасимова, М.А. Роль дидактической игры в процессе обучения детей основам кибербезопасности / М.А. Герасимова // Наука и образование: сохраняя прошлое, создаём будущее : сборник статей XXVIII Международной научно-практической конференции : в 2-х частях. Часть 2. – Санкт-Петербург, 2020. – С. 68–70.

48. Гершунский, Б.С. Прогностический подход к компьютеризации / Б.С. Гершунский // Советская педагогика. – 1986. – № 7. – С. 43–48.

49. Горюнова, Л.В. Тьюторское сопровождение профессионального самоопределения обучающихся в условиях интеграции основного и дополнительного образования / Л.В. Горюнова, М.А. Дорохманова // Научнометодический электронный журнал «Концепт». – 2020. – № 12. – С. 106–110.

50. Грамаков, Д.А. Об использовании Web 2.0 и других Интернет сервисов в молодежных информационных Интернет-порталах / Д.А. Грамаков // Педагогическая информатика. – 2008. – № 2. – С. 53–60.

51. Грачев, Г.В. Информационно-психологическая безопасность личности: теория и технология психологической защиты : дис. … д-ра психол. наук : 19.00.12 – политическая психология / Грачев Георгий Васильевич. – Москва, 2000. – 360 с.

52. Гришина, Л.Н. ч Особенности представлений подростков о правах ребенка / А.В. Черная, Л.Н. Гришина // Российский психологический журнал. – 2018. – Т. 15. – № 2. – С. 60–82.

53. Гущин, Ю.Ф. Оценка уровня развития критического мышления учащихся / Ю.Ф. Гущин, Н.В. Смирнова [Электронный ресурс]. – Режим доступа : http://psyhoinfo.ru/ocenka-urovnya-razvitiya-kriticheskogo-myshleniya-uchash-chihsya/.

54. Давлятшиева, О.В. Сущность, структура и содержание научнометодического сопровождения в современных условиях развития общеобразовательных организаций / О.В. Давлятшиева // Современная наука: актуальные проблемы теории и практики. Серия: Гуманитарные науки. – 2017. – № 3. – С. 35–47.

55. Деркач, А.А. Рефлексивная акмеология творческой индивидуальности : учебно-методическое пособие / А.А. Деркач, И.Н. Семенов, А.В. Балаева ; под общ. ред. проф. А.А. Деркача ; Рос. акад. гос. службы при Президенте Рос. Федерации. – Москва : РАГС, 2005. – 194, [1] с. : ил.; 20 см.

56. Диденко, К.В. Некоторые проблемы выявления и предупреждения киберпреступлений / К.В. Диденко // Вестник Белгородского юридического института МВД России им. И.П. Путилина. – 2020. – № 3. – С. 20–24.

57. Диогенес, Ю. Кибербезопасность. Стратегии атак и обороны / Ю. Диогенес, Э. Озкайя. – Москва : ДМК-Пресс, 2020. – 326 с.

58. Доколин, А.С. Формирование готовности студентов вуза к противодействию вовлечению в киберэкстремистскую деятельность : автореф. дис. … канд.

пед. наук : спец. 13.00.08 – Теория и методика профессионального образования / Доколин, Андрей Сергеевич. – Магнитогорск, 2017. – 24 с.

59. Доктрина информационной безопасности Российской Федерации : утв. Указом Президента РФ от 5декабря 2016 года [Электронный ресурс]. – Режим доступа : https://www.garant.ru/products/ipo/prime/doc/71456224.

60. Дубинина, Д.Б. Проблема медиабезопасности и кибербезопасности личности школьника и студента в современном информационном пространстве / Д.Б. Дубинина // Экология медиасреды : материалы IV Открытой межвузовской научно-практической конференции (Москва, 25 апреля 2019 года). – Москва, 2019. – С. 96–101.

61. Духанина, Л.Н. Вынужденная цифровизация школьного образования в России: родительская рефлексия / Л.Н. Духанина, А.А. Максименко // Научный результат. Социология и управление. – 2021. – Т. 7. – № 2. – С. 116–131.

62. Ершов, А.П. Информатизация: от компьютерной грамотности учащихся к информационной культуре общества / А.П. Ершов // Коммунист. – 1989. – № 2. – С. 82–92.

63. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт / Л.Л. Ефимова, С.А. Кочерга. – Москва : ЮНИТИ-ДАНА, 2013. – 239 с.

64. Жидкова, А.В. Понятие «информационная безопасность» на пропедевтическом этапе обучения информатике в школе / А.В. Жидкова. – 2017. – № 10. – С. 31–34.

65. Жичкина, А. Социально-психологические аспекты общения в Интернете [Электронный ресурс] / А. Жичкина. – Режим доступа : http://flogiston.ruprojects/articles/refmf.shtml

66. Жожикова, С.И. Формирование информационной культуры и саморазвития личности при использовании глобальной сети Интернет / С.И. Жожикова // Вестник Северо-Восточного федерального университета им. М.К. Аммосова. – 2009. – № 1. – С. 84–89.

67. Жолобова, С.И. Информационная безопасность современного школьника [Электронный ресурс] / С.И. Жолобова // Социальная сеть работников образования [сайт]. – 2013. – Режим доступа : http:nsportal.ru/shkola/klassnoe-rukovodstvo/library/2013/10/26/informatsionnaya-bezopasnost-sovremennogo-shkolnika.

68. Загашев, И.О. Критическое мышление: технологии развития / И.О. Загашев, С.И. Заир-Бэк. – Санкт-Петербург : Альянс-Дельта, 2018. – 192 с.

69. Зеер, Э.Ф. Психология взрослости : учебное пособие / Э.Ф. Зеер, Э.Э. Сыманюк ; Российская акад. образования, Московский психолого-социальный институт. – Москва : Московский психолого-социальный институт ; Воронеж : МОДЭК, 2011. – 207 с. : табл.; 21 см. Зейгарник, Б.В. Опосредствования и саморегуляция в норме и патологии / Б.В. Зейгарник // Вестник МГУ. Серия 14 Психология. – 1981. – № 2 апрель-июнь. – С. 9–15.

70. Зимняя, И.А. Педагогическая психология : учебник для вузов / И.А. Зимняя. – Изд. второе, доп., испр. и перераб. – Москва : Издательская корпорация «ЛОГОС», 1999. – 384 с.

71. Зинченко, В.П. Человек развивающийся. Очерки российской психологии / В.П. Зинченко, Е.Б. Моргунов. – Москва : Тривола, 1994. – 304 с.

72. Змеев С.И. Технологии обучения взрослых : учебное пособие для студ. высш. учеб. завед. / Сергей Иванович Змеев. – Москва : Академия, 2002. – 128 с.

73. Знаков, В.В. Самопонимание субъекта как когнитивная и экзистенциальная проблема / В.В. Знаков // Психологический журнал. – 2008. – Т. 26. – № 1. – С. 18–28.

74. Зубалова, О.А. Проблемы информационной безопасности образовательной среды в современных условиях / О.А. Зубалова // Мир науки, культуры, образования. – 2018. – № 3 (70). – С. 36–38.

75. Педагогика : учебное пособие для студентов педагогических учебных заведений / В.А. Сластенин, Н.Ф. Исаев, А.И. Мищенко, Е.Н. Шиянов. – 4-е изд. – Москва : Школьная Пресса, 2004. – 512 с.

76. Интернет-порталы: содержание и технологии : сборник научных статей. Выпуск 1 / редкол. : А.Н. Тихонов (пред.) и др. ; ГНИЙ ИТТ «Информика». – Москва : Просвещение, 2003. – 720 с.

77. Информатизация общего среднего образования : научно-методическое пособие / под ред. Д.Ш. Матроса. – Москва : Педагогическое общество России, 2004. – 384 с.

78. Исаев, И.Ф. Технология тьюторского сопровождения учебнопрофессиональной самореализации студентов вуза / И.Ф. Исаев, В.Н. Кормакова // Научные ведомости Белгородского государственного университета. Серия: Медицина. Фармация. – 2018. – № 12 (131). – С. 160–167.

79. Итинсон, К.С. Обеспечение кибербезопасности в образовательных учреждениях: осведомлённость, правила, стратегия / К.С. Итинсон, В.М. Чиркова. – Балтийский гуманитарный журнал. – 2021. – Т. 10. – № 4 (37). – С. 99–102.

80. Ищенко, А.Н. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности Росси в информационной сфере / А.Н. Ищенко, А.Н. Прокопенко, А.А. Страхов // Проблемы правоохранительной деятельности. – 2017. – № 2. – С. 55–62.

81. Казакина, М.Г. Ценностные ориентации школьников и их формирование в коллективе / М.Г. Казакина. – Ленинград : Изд-во ЛГПИ, 1989. – 85 с.

82. Казакова, Е.И. Педагогическое сопровождение. Опыт международного сотрудничества / Е.И. Казакова. – Санкт-Петербург : На путях к новой школе, 1995. – 186 с.

83. Казакова, Е.И. Системно-ориентационный подход к развитию общеобразовательной школы / Е.И. Казакова. - Санкт-Петербург : Образование, 1995. – 66 с.

84. Камалеева, А.Р. Системный подход в педагогике / А.Р. Камалеева // Научно-педагогическое обозрение. – 2015. – № 3 (9). – С. 13–22.

85. Киреева, О.А. Коммуникационный консалтинг как средство обеспечения информационной безопасности в современном обществе: социологический аспект : автореферат дис … канд. социол. наук : 22.00.08 / Киреева Ольга Фелик-совна; [Место защиты: Моск. пед. гос. ун-т]. – Москва, 2015. – 30 с.

86. Киселев, Г.М. Информационные технологии в педагогическом образовании : учебник / Г.М. Киселев, Р.В. Бочкова. – Москва : Дашков и К, 2012. – 308 с.

87. Коджаспирова, Г.М. Педагогика : учебник для академического бакалавриата / Г.М. Коджаспирова. – 4-е изд. перераб. и доп. – Москва : ЮРАЙТ, 2016. – 719 с.

88. Козьминых, С.И. Обеспечение комплексной защиты объектов информатизации : учебное пособие / С.И. Козьминых. – Москва : Юнити-Дана, 2020. – 543 с.

89. Колокольникова, З.У. Технология активных методов обучения в профессиональном образовании : учебное пособие / З.У. Колокольникова, С.В. Митросенко, Т.И. Петрова. – Красноярск : Сибирский федеральный ун-т ; Институт естественных и гуманитарных наук, 2007. – 176 с.

90. Коменский, Я.А. Великая дидактика, содержащая универсальное искусство учить всех всему / Я.А. Коменский // Избранные педагогические сочинения : в 2 т. / под. ред. А.И. Пискунова. – Москва : Педагогика, 1982. – Т. 1. – С. 242–476.

91. Конаржевский, Ю.А. Педагогический анализ учебно-воспитательного процесса и управление школой / Ю. А. Конаржевский. – Москва : Педагогика, 1986. – 143, [2] с.; 20 см.

92. Конвенция об обеспечении международной информационной безопасности (концепция) [прин. Ген. Ассамблеей ООН: по состоянию на 8 дек. 2010 г.] [Электронный ресурс]. – Режим доступа : http://www.scrf.gov.ru/documents/6/112.html (дата обращения: 11.08.2024).

93. Концепция информационной безопасности детей в Российской Федерации : утв. расп. Правительства РФ от 28 апреля 2023 г. № 1105-р [Электронный ресурс]. – Режим доступа : https://lyceum15.gosuslugi.ru/netcat fLles/168/2854/Rasporyazhenie Pravitel stva RF ot 28.04.2023 N 1105 r.pdf (дата обращения: 11.08.2024).

94. Концепция стратегии кибербезопасности Российской Федерации. Проект [Электронный ресурс] // Проект [сайт]. – 2020. – Режим доступа : http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 11.08.2024).

95. Кордобовский, О.С. Человек в информационном пространстве / О.С. Кордобовский // Человек. – 1998. – № 6. – С. 12–18.

96. Кравченко, А.С. Современные технологии формирования культуры кибербезопасности / А.С. Кравченко, А.В. Калач // Ведомости УИС. – 2019. – № 11 (210). – Режим доступа : https://cyberleninka.ru/article/n/sovremennye-tehnologii-formirovaniya-kultury-kiberbezopasnosti (дата обращения: 11.08.2024).

97. Краевский, В.В. Моделирование в педагогическом процессе / В.В. Краевский // Введение в научное исследование по педагогике. – Москва : Просвещение, 1988. – 120 с.

98. Кривцова, Н.С. Педагогическое сопровождение формирования положительного образа профессии у старшеклассников : автореф. дис. канд. пед. наук : 13.00.01 / Кривцова Наталья Сергеевна; [Место защиты: Сарат. нац. исслед. гос. ун-т им. Н.Г. Чернышевского]. – Саратов, 2018. – 23 с.

99. Государственная политика Российской Федерации в области развития информационного общества / Б.В. Кристальный, О.Л. Алферов, А.В. Коротков, И.Н. Курносов. – Москва : Трейн, 2007. – 470 с // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право: Реферативный журнал. – 2009. – №3. – С. 65–67.

100. Кувалдыкова, Л.З. Развитие правовой компетентности будущего бакалавра педагогики средствами проблемных ситуаций / Л.З. Кувалдыкова. – Оренбург : ООО ИПК «Университет», 2012. –119 с.

101. Кудрявцев, Т.В. Психология технического мышления : автореф. дис. на соискание ученой степени д-ра психол. наук. (962) / Кудрявцев, Т.В. [АПН СССР. Науч.-исслед. ин-т общей и пед. психологии]. – Москва : [б. и.], 1971. – 31 с.

102. Кузьмина, М.В. Как формировать медиакультуру учащихся / М.В. Кузьмина // Управление начальной школой. – 2016. – № 9. – С. 12–16.

103. Кулаева, О.А. Тьюторство и развитие критического мышления при организации научно-исследовательской деятельности учащихся в современной школе-лицее / О.А. Кулаева // Поволжский педагогический вестник. – 2019. – Т. 7. – № 4 (25). – С. 161–166.

104. Кулик, С. Тупики кибербезопасности / С. Кулик // Европейская безопасность: события, оценки, прогнозы. – 2018. – № 48 (64). – С. 2–4.

105. Кулумбегов, Ян.М. Использование технологий виртуальной и дополненной реальности в образовании и других сферах деятельности / Ян.М. Кулумбегов, Е.Д. Зуккель, Е.В. Коробейникова // Инновационный конвент «Кузбасс: образование, наука, инновации» : материалы Инновационного конвента / Департамент молодежной политики и спорта Кемеровской области. – Кемерово, 2019. – С. 570–571.

106. Курносов, И.Н. Информационное общество и глобальные информационные сети: вопросы государственной политики / И.Н. Курносов // Информационное общество. – 1988. – № 6. – С. 29–41.

107. Леонтьев, А.А. Педагогическое общение / Алексей Алексеевич Леонтьев. – Москва : Знание, 1979. – 47 с.

108. Леонтьев, А.Н. Деятельность, сознание, личность / А.Н. Леонтьев. – Москва : Политиздат, 1977. – 304 с.

109. Лернер, И.Я. Проблемное обучение / И.Я. Лернер. – Москва : Знание, 1974. – 62, [2] с. : ил.

110. Лопатин, И.Д. Экстремизм как социально-политическое явление современного мира: особенности его возникновения и развития в России : дис. ...

канд. полит. наук : 23.00.02 / Лопатин Иван Дмитриевич. – Ярославль, 2007. – 192 с.

111. Лучшев, Б.С. Психологическая безопасность обучающихся в информационной среде школы / Б.С. Лучшев // Казанский педагогический журнал. – 2019. – № 3 (134). – С. 52–56.

112. Лучинкина, А.И. Информационно-психологическая безопасность личности в интернет-пространстве : учебное пособие / А. Лучинкина, Т. Юдеева, В. Ушакова ; М-во образования, науки и молодежи Республики Крым, Гос. бюджетное образовательное учреждение высш. образования Респ. Крым «Крымский инженерно-педагогический университет». – Симферополь : ДИАЙПИ, 2015. – 151 с.

113. Лю Ган. Философия информации и основы будущей китайской философии науки и техники / Лю Ган // Вопросы философии. – 2007. – № (5). – С. 45–57.

114. Маклаков, А.Г. Общая психология : учеб. пособие для студ. вузов / Аннатолий Геннадиевич Маклаков. – Санкт-Петербург : Питер, 2008. – 582 с.

115. Малых, Т.А. Педагогические условия развития информационной безопасности младшего школьника : автореф. дис. … канд. пед. наук 13.00.01 – общая педагогика, история педагогики и образования / Малых Татьяна Александровна. – Москва, 2008. – 22 с.

116. Маралов, В.Г. Основы самопознания и саморазвития : учебное пособие для студ. сред. пед. учеб. завед. / Владимир Георгиевич Маралов. – Москва : Академия, 2002. – 256 с.

117. Маслоу, А.Г. Дальние пределы человеческой психики / А.Г. Маслоу ; пер. с англ. А.М. Татлыбаевой ; ред. вступ. ст. и коммент. Н.Н. Акулиной. – Санкт-Петербург : Евразия, 1999. – 430 с.

118. Матюшкин, А.М. Проблемные ситуации в мышлении и обучении / А.М. Матюшкин. – Москва : Директ-Медиа, 2014. – 274 с.

119. Махмутов, М.И. Организация проблемного обучения в школе / М.И.

Махмутов. – Москва : Просвещение, 1977. – 240 с.; 20 см. – (Книга для учителей).

120. Меньчиков, Г.П. Виртуальная реальность: понятия, новация, применение / Г.П. Меньчиков // Философия науки. – 1998. – № 3-4. – С. 170–175.

121. Минин, А.Я. Информационная безопасность в образовании обучающихся и обучающих / А.Я. Минин // Правовое обеспечение социокультурного развития. Наука и школа. – 2017. – № 1. – С. 29–36.

122. Миронов, А.В. Оперативно-профилактические меры противодействия молодежному экстремизму / А.В. Миронов // Вестник КРУ МВД России. – 2011. – № 2 (12). – С. 51–55.

123. Муштавинская, И.В. Технология развития критического мышления на уроке в системе подготовки учителя / И.В. Муштавинская. – Санкт-Петербург, 2017. – 144 с.

124. Найн, А.Я. Педагогический эксперимент: методика и его организация : учебное пособие / А.Я. Найн, З.М. Уметбаев. – Магнитогорск : МаГУ, 2002. – 127 с.

125. Нечай, А.А. Актуальные проблемы защиты информации в современных автоматических телефонных станциях / А.А. Нечай, П.Е. Котиков // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2015. – № 2. – С. 65–69.

126. Никитаева, М.В. Как обеспечить информационную безопасность образовательной среды в школе / М.В. Никитаева // Безопасная образовательная среда в современной школе : материалы научно-практической конференции, Москва, 23 марта 2017 года. – Москва : Московский городской педагогический университет, 2017. – С. 111–114.

127. О защите детей от информации, причиняющей вред их здоровью и развитию : фед. закон от 29.12.2010 г. № 436-ФЗ (ред. от 12.06.2024) [Электронный ресурс]. – Режим доступа : https://legalacts.ru/doc/federalnyi-zakon- ot-29122010-n-436-fz-o/.

128. Об информации, информационных технологиях и о защите информации : фед. закон ; принят ГосДумой 8 июля 2006 г. ; ред. от 12.12.2023 г. [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons doc LAW 61798.

129. Об образовании в Российской Федерации : фед. закон ; принят Гос. Думой 21 декабря 2012 г.: по состоянию на 29 декабря 2012 г. [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons doc LAW 140174.

130. Обухова, Л.Ф. Возрастная психология : учебник для бакалавров / Л.Ф. Обухова. – Москва : ЮРАЙТ, 2013. – 460 с.

131. Ожегов, С.И. Словарь русского языка: 70000 слов / под ред. Н.Ю. Шведовой. – 23-е изд., испр. – Москва : Русский язык, 1990. – 917 с.

132. Онушкин, В.Г. Образование взрослых: междисциплинарный словарь / В.Г. Онушкин, Е.И. Очарев. – Санкт-Петербург – Воронеж : ИОВ РАО, 1995. – 232 с.

133. Организация и контрольно-методическая деятельность преподавателя высшей школ : учебно-методическое пособие / Л.З. Тархан, М.И. Мыхнюк. – Симферополь : ИТ «АРИАЛ», 2018. – 212 с.

134. Остапова, А.В. Психологические особенности подросткового возраста / А.В. Остапова // Евразийский научный журнал. – 2019. – № 7. – С. 109–110.

135. Остроушко, А.В. Защита информационной безопасности несовершеннолетних в КНР / А.В. Остроушко, А.А. Букалеров, С.А. Букалеров // LegalBulletin. – 2018. – Т. 3. – № 1-2. – С. 56–60.

136. Остроцкая, С.В. К вопросу анализа угроз безопасности критическим информационным инфраструктурам / С.В. Остроцкая, И.В. Калуцкий // Информационные технологии в моделировании и управлении: подходы, методы, решения : материалы II Всероссийской научной конференции с международным участием : в 2 частях. – Курск, 2019. – С. 212–217.

137. Панюкова, С.В. Информационные и коммуникационные технологии в

личностно-ориентированном обучении / С.В. Панюкова. – Москва : Изд-во ИОСО РАО, 1998. – 225 с.

138. Педагогика : учебное пособие для студ. пед. учеб. заведений / В.А. Сластенин и др. – Москва : Школа-Пресс, 1997. – 512 с.

139. Педагогика: большая современная энциклопедия / сост. Е.С. Рапацевич. – Минск : Современное слово, 2005. – 720 с.

140. Плешаков В.А. Киберсоциализация человека: от Homo Sapiens'a до Homo Cyberus'a : монография / В.А. Плешаков ; М-во образования и науки Российской Федерации, Федеральное гос. бюджетное образовательное учреждение высш. проф. образования «Московский пед. гос. ун-т». – Москва : МГПУ : Прометей, 2012. – 211 с. : ил., табл.; 20 см.; ISBN 978-5-7042-2368-9

141. Подласый, И.П. Педагогика : в 2 кн. : учебник для студ. вузов, обуч. по пед. спец. / Иван Павлович Подласый. – Москва : ВЛАДОС, 1999. – Книга 1: Общие основы процесса обучения : новый курс. – 1999. – 574 с.

142. Полат, Е.С. Новые педагогические и информационные технологии в системе образования / Е.С. Полат. – М. : Академия, 2001. – 272 с.

143. Помощь родителям в воспитании детей / общ. ред. и предисл. В.Я. Пелиповского ; пер. с англ. – Москва : Прогресс, 1992. – 256 с.

144. Практическая психология : учебник / под ред. М.К. Тутушкиной. – Санкт-Петербург : Дидактика Плюс, 2001. – 368 с.

145. Психология тренинговой работы: содержательные, организационные и методические аспекты ведения тренинговой группы / И.В. Вачков. – Москва : Эксмо, 2007. – 416 с.

146. Пьянкова, Г.С. Развитие профессиональной рефлексии : учебное пособие для вузов / Г.С. Пьянкова. – Красноярск : КГПУ им. Астафьева, 2009. – 280 с.

147. Радкевич, И.О. О компьютере без дифирамбов / И.О. Радкевич // Литературная газета. – 1986, 17 сент. – С. 6.

148. Ракитов, А.И. Информация, паука, технология в глобальных исторических измерениях / А.И. Ракитов. – Москва : Изд-во ИНИОН РАН, 1998. – 104 с.

149. Об утверждении Стратегии развития отрасли информационных технологий в РФ на 2014–2020 гг. и на перспективу до 2025 г. : распоряжение Правительства от 1 ноября 2013 г. № 2036-р [Электронный ресурс]. – Режим доступа : http://base.garant.ru/70498122.

150. Об утверждении Стратегии развития информационного общества в Российской Федерации : распоряжение Правительства от 7 февраля 2008 г. № Пр.-212 [Электронный ресурс]. – Режим доступа : http://base.garant.ru/productse/ipo/prime/doc/92762.

151. Ревенков, В.П. Минимизация риска воздействия кибератак в условиях применения технологий дистанционного банковского обслуживания : учебное пособие / В.П. Ревенков, А.А. Бердюгин, И.В. Ожерез. – Москва : Прометей, 2020. – 214 с.

152. Рекина, Ю.В. Условия развития критического мышления учащихся основной школы / Ю.В. Рекина // Современной педагогическое образование. – 2022. – № 6. – С. 305–307.

153. Решетников, В.Г. Организационно-методическое сопровождение и методическая поддержка деятельности педагогов в условиях модернизации образования / В.Г. Решетников, // Омский научный вестник. – 2013. – № 5 (122). – С. 174–177.

154. Рихтер, Т.В. Использование интерактивных методов обучения при формировании профессиональных компетенций педагогов по обеспечению кибербезопасности подрастающего поколения / Т.В. Рихтер // Активные и интерактивные методы обучения в естественно-математическом образовании : коллективная монография. – Соликамск, 2018. – С. 13–21.

155. Роберт, И.В. Информационное взаимодействие в информационнокоммуникационной предметной среде / И.В. Роберт // Информационные и коммуникационные технологии в системе непрерывного образования. Ученые записки

(сб. статей) / РАО Ин-т информ. образования. – Москва, 2001. – С. 3–30.

156. Романов, А.А. Потенциал информационно-образовательной среды университета в обучении будущих педагогов / А.А. Романов, Е.Ю. Лунькова // Образовательное пространство в информационную эпоху – 2019 : сборник научных трудов ; материалы Международной научно-практической конференции / под редакцией С.В. Ивановой. – Москва, 2019. – С. 631–645.

157. Рубинштейн, С.Л. Основы обшей психологии / Сергей Леонидович Рубинштейн / сост., авторы комментариев и послесловия А.В. Брушлинский, К.А. Абульханова-Славская. – Санкт-Петербург : Питер, 2002. – 720 с.

158. Ручка, А.А. Моральные ценности личности / А.А. Ручка / под ред. А.А. Татаренко. – Москва : МГУ, 1994. – 176 с.

159. Рыбакова, О.С. Безопасность несовершеннолетних в информационном обществе: анализ киберрисков и угроз / О.С. Рыбакова // Мониторинг правоприменения. – 2020. – № 2 (35). – С. 65–73. DOI: 10.21681/2226-0692-2020-2-65-73.

160. Условия гуманитаризации высшего профессионального образования : коллективная монография / под. общ. ред. Л.И. Савва. – Магнитогорск : МаГУ, 2008. – 463 с.

161. Садовский, В.М. Системный подход и общая теория системы: статус, основные проблемы и перспективы развития / В.М. Садовский. – Москва : Наука, 1980.

162. Саидов, Ж.А. Причины использования виртуальной реальности в образовательных и обучающих курсах, и модель определяющая, когда использовать виртуальную реальность / Ж.А. Саидов, Ф.А. Жулибекова // Студенческие научные достижения : сборник статей VI Международного научно-исследовательского конкурса. – Пенза : МЦНС «Наука и Просвещение», 2019. – С. 30–35.

163. Саттарова, Н.И. О формировании культуры безопасности обучающихся в информационном пространстве / Н.И. Саттарова // Проблемы современного педагогического образования. – 2018. – № 58-4. – С. 242–245.

164. Сенстерова, К.П. Понятие «сопровождение» как педагогическая категория / К.П. Сенстерова // Известия Саратовского Университета. Серия Акмеологического образования. Психология развития. – 2020. – Т. 9. Вып. 1 (33). – С. 289–293.

165. Серебряник, Е.Э. Формирование информационно-личностной безопасности учащихся основной школы : автореф. дис. … канд пед. наук: 13.00.01 – общая педагогика, история педагогики и образование / Евгений Эммануилович Серебряник. – Калининград, 2011. – 21 с.

166. Сериков, В.В. Образование и личность. Теория и практика проектирования педагогических систем : монография / В.В. Сериков. – Москва : Издательская корпорация «ЛОГОС», 1999. – 272 с.

167. Синицын, Д.С. Психолого-педагогические условия обучения информационно-психологической безопасности подростков : дис. … канд. пед. наук : 13.00.01 / Дмитрий Сергеевич Синицын ; Рос. гос. пед. ун-т им. А.И. Герцена. – Санкт-Петербург, 2005. – 169 с.

168. Скаткин, М.Н. Проблемы современной дидактики / Михаил Николаевич Скаткин. – 2-е изд. – Москва : Педагогика, 1984. – 95 с.

169. Скаткин, М.Н. Активизация познавательной деятельности учащихся в обучении / Михаил Николаевич Скаткин. – Москва : [б. и.], 1965. – 48 с.; 20 см. – (Материал к Научной конференции по дидактике 11-13 мая / Науч.-исслед. ин-т общего и политехн. образования Акад. пед. наук РСФСР).

170. Сластенин, В.А. Педагогика: инновационная деятельность / В.А. Сластенин, Л.С. Подымова. – Москва : Магистр, 1997. – 224 с.

171. Создание глобальной культуры кибербезопасности и защиты важнейших информационных инфраструктур [резол. Ген. Ассамблеи ООН: утв. 30 янв. 2004 г.] [Электронный ресурс]. – Режим доступа : http://www.ifap.ru/ofdocs/un/58199.pdf.

172. Солдатова, Г.У. Безопасность подростков в Интернете: риски, совла-

дение и родительская медитация / Г.У. Солдатова, Е.И. Рассказова // Национальный психологический журнал. – 2014. – № 3 (15). – С. 36–48.

173. Стерхов, А.А. Педагогическое сопровождение и поддержка учащихся воспитательной службой православной гимназии [Электронный ресурс] / А.А. Стерхов // Филологические науки. Вопросы теории и практики. – 2016. – № 1-2 (55). – Режим доступа : https://cyberleninka.ru/article/n/pedagogicheskoe-soprovozhdenie-i-podderzhka-uchaschihsya-vospitatelnoy-sluzhboy-pravoslavnoy-gimnazii (дата обращения: 11.08.2024).

174. Стеценко, И.А. Теория и практика формирования рефлексивной компетентности студентов / И.А. Стеценко ; под ред. Е.А. Михайлычева ; М-во образования и науки Российской Федерации, Федеральное гос. бюджетное образовательное учреждение высш. проф. образования «Таганрогский гос. педагогический ин-т им. А. П. Чехова». – Таганрог : Таганрогский гос. педагогический ин-т им. А.П. Чехова, 2013. – 127 с.

175. Сухорукова, В.С. Понятие «сопровождение» как педагогическая категория / В.С. Сухорукова // Наука, технологии, общество - НТО-П-2022 : сборник научных статей по материалам II Всероссийской научной конференции, Красноярск, 28-30 июля 2022 года. – Красноярск : Общественное учреждение «Красноярский краевой Дом науки и техники Российского союза научных и инженерных общественных объединений», 2022. – С. 271–276.

176. Тархан, Л.З. Организационная и контрольно-методическая деятельность преподавателя высшей школы / Л.З. Тархан, М.И. Мыхнюк. – Симферополь : ИТ «АРИАЛ», 2018. – 212 с.

177. Толковый словарь русского языка: около 100 000 слов, терминов и фразеологических выражений / С.И. Ожегов ; под общ. ред. Л.И. Скворцова. – 28-е изд., перераб. – Москва : Мир и Образование: ОНИКС, 2012. – 1375 с.

178. Троицкая О.Н. Особенности организации и проведения конкурса задач по кибербезопасности / О.Н. Троицкая, О.Л. Безумова, Т.С. Ширикова // Информатика в школе. – 2019. – № 6. – С. 5–9. https://doi.org/10.32517/2221-1993-

2019-18-6-5-9

179. Троицкая, О.Н. Конкурс «кибербезопасность в образовании» в системе средств подготовки будущих учителей к обучению школьников основам кибербезопасности / О.Н. Троицкая, Е.Д. Вохтомина // Актуальные проблемы обучения математике и информатике в школе и вузе : материалы VI Международной научной интернет-конференции, Москва, 11-12 декабря 2020 года / под общей редакцией Л.И. Боженковой, М.В. Егуповой. – Москва : Московский педагогический государственный университет, 2021. – С. 349–356.

180. Концептуальная модель обучения основам кибербезопасности в основной школе [Электронный ресурс] / О.Н. Троицкая, Т.С. Ширикова, О.Л. Безумова, Е.А. Лыткина // Современные проблемы науки и образования. – 2018. – № 5. – Режим доступа : https://science-education.ru/ru/article/view?id=28073

181. Тропинина, Т.Л. Кибербезопасность и киберэкстремизм: поговорим о понятийном аппарате / Т.Л. Тропинина // Информационные технологии и безопасность : сборник научных трудов междунар. конф. Выпуск 3. – Киев : Национальная академия наук Украины, 2003. – С. 173–181.

182. О Национальной стратегии действий в интересах детей на 2012–2017 годы : указ Президента РФ от 01.06.2012 г. № 761 [Электронный ресурс] // [сайт]. – Режим доступа : http://base.garant.ru/70183566.

183. Фарниев, С.А. Теоретико-концептуальные аспекты изучения феномена информационной безопасности / С.А. Фарниев // Азимут научных исследований: экономика и управление. – 2018. – Т. 7. – № 3 (24). – С. 397–399.

184. О рекламе : фед. закон от 13.03.2006 г. № 38-ФЗ ; принят Гос. Думой 22 февраля 2006 года, одобрен Советом Федерации 3 марта 2006 года, в ред. Приказов от 1 мая 2019 г. № 89-ФЗ [Электронный ресурс] // [сайт] [2014]. – Режим доступа : http://base.garant.ru/12145525.

185. О защите детей от информации, причиняющей вред их здоровью и развитию : фед. закон от 29 декабря 2010 г № 436-ФЗ // Собрание законодательства РФ. – 2011. – № 1. – Ст. 48.

186. Федеральный образовательный стандарт основного общего образования : утв. приказом Минпрома России от 31.05.2021 г. № 287 // Учебный год. – 2021. – 89 с.

187. Философский словарь / под ред. И.Т. Фролова. – 5-е изд. – Москва : Политиздат, 19987. – 590 с.

188. Философский энциклопедический словарь / глав. ред.: Л.Ф. Ильичев, П.Н. Федосеев, С.М, Ковалев, В.Г. Панов. – Москва : Советская энциклопедия, 1983. – 840 с.

189. Фроликова, О.А. Мотивация как фактор развития личностнопрофессиональных качеств студентов-психологов : монография / О.А. Фроликова. – Орел : Изд. Александр Воробьев, 2010. – 180 с.

190. Фунтиков, М.С. Педагогические условия формирования интегративной среды процесса профессиональной подготовки бакалавров информационной безопасности : автореф. дис. … канд. пед. наук : 13.00.08 – теория и методика профессионального образования / Максим Николаевич Фунтиков. – Донецк, 2020. – 23 с.

191. Хаджиева, Л.К. Анализ модели развития электронных информационных технологий / Л.К. Хаджиева, Б.Э. Элежбиев, М.А. Джамалдинова // Journal of Monetary Economics and Management. – 2023. – № 1. – С. 160–164.

192. Храмцов, П.Б. Лабиринт Интернет. Практическое руководство / П.Б. Храмцов. – Москва : Электроинформ, 1996. – 256 с.

193. Хуторской, А.В. Методика личностно-ориентированного обучения. Как обучать всех по-разному. Пособие для учителя / А.В. Хуторской. – Москва : ВЛАДОС, 2005. – 383 с.

194. Зеер, Э.Ф. Психология взрослости : учебное пособие / Э.Ф. Зеер, Э.Э. Сыманюк ; Российская акад. образования, Московский психолого-социальный институт. – Москва : Московский психолого-социальный ин-т ; Воронеж : МОДЭК, 2011. – 207 с. : табл.; 21 см. – (Библиотека психолога).; ISBN 978-5-99360036-9 (МПСИ)

195. Ченушкина, С.В. Защита прав ребенка от кибербуллинга в образовательной организации / С.В. Ченушкина // 30 лет Конвенции о правах ребенка: современные вызовы и пути решения проблем в сфере защиты прав детей : сборник материалов Международной научно-практической конференции, 17 ноября 2020 г., Екатеринбург / Рос. гос. проф.-пед. ун-т. – Екатеринбург : РГППУ, 2020. – С. 282–286.

196. Шеремет, А.Н. Интернет как средство массовой коммуникации: социологический анализ : автореф. дис. … канд. соц. наук : 22.00.06 / Александр Николаевич Шеремет. – Екатеринбург, 2004. – 25 с.

197. Шушакова, Е.В. Научно-методическое сопровождение инновационных процессов в сельской школе : автореферат дис. … канд. пед. наук : 13.00.01 / Шушакова Евгения Васильевна ; [Место защиты: Ом. гос. пед. ун-т]. – Омск, 2008. – 22 с.

198. Щербакова, Г.В. Информатизация образования и проблемы кибербезопасности в образовательной среде / Г.В. Щербакова, А.В. Арухтина, С.С. Демура // Современное педагогическое образование. – 2020. – № 11. – С. 63–66.

199. Щукина, Г.И. Активизация познавательной деятельности учащихся в учебном процессе / Г.И. Щукина. – Москва, 2000. – 97 с.

200. Юшкевич, Е.В. Педагогическое сопровождение саморазвития учащихся основной школы : автореф. дис. … канд. пед. наук : 13.00.01 / Юшкевич Елена Викторовна ; [Место защиты: Новгородский государственный университет имени Ярослава Мудрого]. – Великий Новгород, 2020. – 24 с.

201. Якиманская, И.С. Личностно ориентированное обучение в современной школе / И.С. Якиманская. – Москва : Сентябрь, 2002. – 96 с.

202. Яковлев, Е.В. Педагогические исследования: содержание и представление результатов : монография / Е.В Яковлев, Н.О. Яковлева. – Челябинск : Изд-во РБИУ, 2010. – 317 с.

203. Якунин, В.А. Педагогическая психология : учеб. пособие / В.А. Якунин. – Санкт-Петербург : Изд-во В.А. Михайлова, 2000. – 349 с.

204. Яницкий, М.С. Ценностные ориентации личности как динамическая система : монография / М.С. Яницкий. – Кемерово : Кузбассвузиздат, 2000. – 203 с.

205. Янушок, Н.И. Фаза осмысления на уроках математики как основной элемент технологии критического мышления [Электронный ресурс] / Н.И. Янушок // Альманах мировой науки. – 2017. – № 1-1. – Режим доступа : https://nsportal.ru/shkola/matematika/library/2020/06/23/tehnologii-i-formy-razvitiya-kriticheskogo-myshleniya-na-urokah.

206. Atila Bostan. Impact of education on security practices in ICT / Atila Bostan // Tehnicki vjesnik. – 2017. – № 19. – P. 709–715.

207. Mobile learning and emerging mobile technologies in Preschool Education: perceptions of teachers in training / I. Aznar, M.P. Caceres, J.M. Trujillo, J.M. Romero // Espacios. – 2019. – Vol. 40. – № 5. – P. 14.

208. Hall, C. Security of the Internet and the Known Unknowns / C. Hall // Communications of the ACM. – 2018. – № 55 (6). – P. 35–37.

209. Muniandy, L. Cyber security behavior among higher education students in Malaysia / L. Muniandy, B. Muniandy, Z. Samsudin // Journal of Information Assurance & Cybersecurity. – 2017. – P. 1-13.

210. The Importance of Cybersecurity Education in School / N.A.A. Rahman, I.H. Sairi, N.A.M. Zizi, F. Khalid // International Journal of Information and Education Technology. – 2020. – Vol. 10. – № 5. – P. 378–382.

211. Tekerek, M. A Research on Students' Information Security Awareness / M. Tekerek, A. Tekerek // Turkish Journal of Education. – 2016. – № 3. – P. 61–70.

212. Toni Hunt Cyber Security Awareness in Higher Education / Toni Hunt // Central Washington University. – 2017. – P. 1–13.

ПРИЛОЖЕНИЯ

ОГЛАВЛЕНИЕ ПРИЛОЖЕНИЙ

стр.

Приложение 1

В помощь обучающимся.
Информация о видах киберугроз исходящих из сети-Интернет

Вирусы скрытно проникают в компьютерные системы, и без эффективной защиты бороться с ними невозможно. Чтобы вирусы проникли в компьютер, достаточно всего лишь открыть вложение в электронном письме (при этом совершенно не обязательно, чтобы письмо было отправлено неизвестным адресатом, хорошо известный компаньон также может прислать вирус, если ранее его компьютер был заражен). Некоторым вирусам достаточно уже того, что компьютер просто подключен к локальной сети, к которой подключен и зараженный компьютер. Для распространения значительного числа вирусов используют съемные накопители информации (флешки, мобильные жесткие диски и оптические носители). Вирусы могут нарушить работоспособность компьютеров и программ, уничтожить файлы.

Спам – это массовая рассылка на большое число адресов, содержащие рекламу или коммерческое предложение; электронный эквивалент бумажной рекламы, которую бросают в ваш почтовый ящик. Однако спам не просто надоедает и раздражает. Он опасен, особенно если является частью фишинга

Фишинг – это обман пользователя с целью получения его личных данных, таких как логин, пароль, номер телефона или банковской карты.

Кибербуллинг – намеренная травля жертвы через интернет. К таким травлям можно отнести нанесение оскорблений через личные сообщения, публикации провокационных материалов, распространения конфиденциальной информации о жертве. В данном случае агрессоры задействуют такие каналы общения как социальные сети, чаты, мессенджеры, которые приводят к психологической травле. Школьники не всегда способны справляться с этой травлей, а поэтому обращаются за помощью к взрослым или близким людям. Участниками кибербуллинга являются буллеры, жертвы, зрители. Жертвой буллинга может стать любой школьник, зрители буллинга – это дети, поддающиеся влиянию не умеющие сопереживать и сочувствовать, принимающие травлю за развлечение.

К основным видам кибербуллинга можно отнести: физическое насилие в виде нанесения телесных повреждений; эмоциональное насилие в виде насмешек, угроз, унижений в присутствии других, анонимные звонки оскорбляющего или унижающего характера, публикация видеоматериалов в сети с целью травли конкретной личности распространение слухов и сплетен; экономическое насилие проявляется в отнятии личных вещей, денег, вымогательства.

Киберэкстремизм рассматривается как приверженность к крайним взглядам, мерам и действиям, которая может иметь место в любой сфере общественной жизни. Это приверженность к крайним взглядам, идеям и действиям, направленным на распространение принципов нетерпимости с использованием совокупности различных средств и методов сбора, обработки и передачи информации в киберпространстве.

Киберэкстремистические проявления оказывают влияние, прежде всего на неустойчивую молодежь, которая является наиболее активным пользователем интернет-сетей и прежде всего социальных сетей. С этой целью в последнее время в образовательных организациях особое внимание уделяется профилактике киберэкстремизма.

Киберсуицид – групповые или индивидуальные самоубийства, согласованные с помощью Интернет-ресурсов.

Угрозы для морали и нравственности через пропаганду информации, связанной с употреблением наркотиков, алкоголя, порнографии и др.

Угрозы интернет-зависимости – аддиктивная форма поведения, проявляющаяся в потере контроля над собой и неспособность вовремя справиться с собой по выходу из сети и противодействии киберзависимости.

Игровая зависимость рассматривается как заболевание на ряду с наркоманией алкоголизмом. Разницу между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах, обычно, содержаться настольные и словесные игры, где не тратятся денежные средства; сайты с азартными играми допускают, что люди выигрывают или проигрывают конкретные деньги. Опасность игровой зависимости достаточно велика и отличается насилием, повышенной агрессивностью, жестокостью со стороны молодежи.

Интернет-зависимость обучающихся рассматривается как постоянное путешествие по интернету с целью поиска информации; пристрастия к виртуальному общению и виртуальному знакомству, характеризующимися большими объёмами переписки, постоянным участием в чатах, а, следовательно, избыточностью знакомы и друзей из интернета; просмотр и скачивание фильмов, клипов, аудиофайлов, программ, обмен файлами.

Овершеринг – это чрезмерное и необдуманное размещение личной информации о себе или других в сети, стремление человека рассказывать окружающим больше, чем стоило бы, перебарщивая с откровенностью забывая об опасности. К ним относятся: биографические данные, данные о здоровье, данные об уровне обеспеченности семьи и другие сведения.

Компьютерные программы:

Компьютерный вирус – это небольшая программа способная к саморазмножению и выполнению разных деструктивных действий. Вирусы действуют только программным путем. Они, как правило, присоединяются к файлу или, проникают в тело файла. В этом случае говорят, что файл заражен вирусом. Вирус попадает в компьютер только вместе с зараженным файлом. Для активизации вируса нужно загрузить зараженный файл, и только после этого, вирус начинает действовать самостоятельно. Некоторые вирусы во время запуска зараженного файла становятся резидентными (постоянно находятся в оперативной памяти компьютера) и могут заражать другие загружаемые файлы и программы. Другая разновидность вирусов сразу после активизации может быть причиной серьезных повреждений, например, форматировать жесткий диск. Действие вирусов

может проявляться по-разному: от разных визуальных эффектов, мешающих работать, до полной потери информации.

Червь - вредоносная программа, которая самостоятельно распространяется через локальные и глобальные компьютерные сети. Червь, в отличие от вируса, не оставляет своих копий и всегда присутствует на заражённом компьютере в единственном экземпляре.

Шпионская программа (spyware) — программа, установленная на компьютер пользователя, собирающая данные о нём. Такая программа не вредит файлам и программам, установленным на компьютере, однако относится к вредоносному программному обеспечению.

Шпионское и рекламное программное обеспечение попадает на компьютер несколькими путями, и один из них — согласие пользователя на принятие файлов cookie или согласие с Лицензионным соглашением сомнительного приложения. И вот уже ваш компьютер участвует в спам-рассылке, «раскручивает» сайт злоумышленников, рекламирует сомнительные товары. Вопрос противодействия шпионским программам очень важен для пользователей и поставщиков программного обеспечения. По мере развития угрозы шпионского программного обеспечения появился и ряд программ, предназначенных для его удаления и блокировки. Но иногда эффективнее бывает воспользоваться резервными копиями важных файлов после переустановки операционной системы

Рекламное программное обеспечение (adware) — нежелательное программное обеспечение, написанное для рекламирования того или иного товара или перенаправляющее на сайты, предлагающие эти товары и услуги.

Приложение 2

В помощь обучающимся.
Инструкция по защите персональных данных в Интернет-сети

1. Защитите свой компьютер

2. Постоянно обновляйте все программное обеспечение (включая веб-браузер)

3. Установите законное антивирусное программное обеспечение

4. Брандмауэр должен быть всегда включен.

5. Установите на беспроводном маршрутизаторе защиту с помощью пароля.

6. Всегда проверяйте флеш-накопители (или USB-накопители)

7. Не переходите по ссылкам и не нажимайте кнопки во всплывающих сообщениях, которые кажутся подозрительными.

8. Обеспечьте защиту секретной личной информации

9. Никогда не отвечайте на просьбы прислать деньги от «членов семьи», на сообщения о розыгрышах лотереи, в которых вы не участвовали, или другие мошеннические сообщения.

10. Используйте надежные пароли и храните их в секрете. Придумайте пароли, представляющие собой длинные фразы или предложения и содержащие сочетание строчных, прописных букв, цифр и символов. -

11. Используйте на разных сайтах разные пароли.

12. Позаботьтесь о своей безопасности и репутации в Интернете

13. Более безопасное использование социальных сетей

14. Никогда не публикуйте информацию, которую вы не хотели бы видеть на доске объявлений.

15. Периодически анализируйте, кто имеет доступ к вашим страницам, а также просматривайте информацию, которую эти пользователи публикуют о вас.

16. Настройте список пользователей, которые могут просматривать ваш профиль или фотографии.

17. Подходите избирательно к предложениям дружбы

Приложение 3

Тест для самопроверки знаний по информационной безопасности обучающихся

1. Какую информацию нельзя разглашать в Интернете?
1. Свои увлечения.
2. Свой псевдоним.
3. Домашний адрес.

2. Чем опасны социальные сети?
1. Личная информация может быть использована кем угодно в разных целях.
2. При просмотре неопознанных ссылок компьютер может быть взломан.
3. Все вышеперечисленное верно.

3. Виртуальный собеседник предлагает встретиться, как следует поступить?
1. Посоветоваться с родителями и ничего не предпринимать без их согласия.
2. Пойти на встречу одному.
3. Пригласить с собой друга.

4. Что в Интернете запрещено законом?
1. Размещать информацию о себе.
2. Размещать информацию других без их согласия.
3. Копировать файлы для личного использования.

5. Действуют ли правила этикета в Интернете?
1. Интернет-пространство свободное от правил.
2. В особых случаях.
3. Да, как и в реальной жизни.

6. Для чего используется антивирус?
1. Для периодической проверки компьютера.
2. Для обмена информацией.
3. Для уничтожения вирусов.
4. Для авторизации доступа к файлам.
5. Для нахождения вирусов.

7. Какими способами вирусы могут заразить ваш компьютер?
1. Через просмотр страниц в соцсетях.
2. Скачиванием неизвестных программ из интернета.
3. Использованием нелицензированной версией антивируса.
4. Переход по ссылке неизвестного происхождения.
5. Посредством спама.

Используемые Интернет-ресурсы:
1. Сайт «Азбука безопасности» (http://azbez.com/node/2017).

Приложение 4

Инструкция к тесту оценки критического мышления

1. Вначале внимательно прочтите задачу. Возможно, вам покажется, что некоторые из задач очень простые и не требуют долгих размышлений, так как ответ очевиден. Но все же не спешите с выводами, они могут оказаться ошибочными.

2. Не следует долго останавливаться на решении задач, в которых вы не можете достаточно быстро найти ответ. Помните, что время тестирования ограничено и нужно успеть порешать все задачки.

3. Кроме ответов на поставленные в задачах вопросы, просим вас кратко обосновать свой ответ (в том числе и в случаях, когда предлагается выбрать ответ из числа предложенных). Обоснование является обязательным, так как без этого нельзя будет понять основания ваших ответов и решений. А это в данном случае важно для оценки самого теста и отдельных задач в нем. Если вы затрудняетесь с ответом в какой-то из задач, то долго не задерживайтесь на ней и переходите к другой».

В процессе исследования мы планировали выявление уровня критического мышления обучающихся. С этой целью был предложен опросник, направленный на диагностику сформированности следующих умений: умение делать логические умозаключения и обосновывать свой ответ; умение оценивать последовательности умозаключений; умение анализировать и делать заключение о причинах явлений; умение анализировать и оценивать содержание текстов; умение обнаруживать ошибки, связанные с неопределенностью и двусмысленностью выражений и терминов; умение обнаруживать релевантную (существенную в данном случае) информацию на фоне избыточной.

Нами использовалась основная версия текста и адаптированная для нашего исследования. Обе формы приведены в таблице 1.

Таблица 1

Формы опросника критического мышления

№ п/п	Форма А исходная	Форма Б адаптированная
1.	Реши задачу. В темном и сыром подвале выросло растение с белыми листьями, потому что в подвале было темно. Вопрос 1. Правильно ли сделан этот вывод? Вопрос 2. При каких условиях можно было бы считать это утверждение правильным?	Реши задачу. Саша – блогер и зарабатывает много денег, потому что блогеры всегда много зарабатывают. Вопрос 1. Правильно ли сделан этот вывод? Вопрос 2. При каких условиях можно было бы считать это утверждение правильным?

2.	Даны два утверждения: 1. Все переводчики отлично владеют иностранным языком. 2. Некоторые писатели - переводчики. Какой вывод правильный? а) Некоторые писатели отлично владеют иностранным языком. б) Все писатели отлично владеют иностранным языком	Даны два утверждения: 1. Бесплатное антивирусное ПО охватывает меньше элементов безопасности, чем платное. 2. На некоторых ПК установлено бесплатное антивирусное ПО. а) ПК, на которых установлено бесплатное аннтивирусное ПО, находятся в полной безопасности. б) ПК, на которых установлено бесплатное аннтивирусное ПО, подвергаются опасности.
3.	Даны два утверждения и вывод. 1. Некоторые садовые растения имеют красивые цветы. 2. Некоторые деревья - садовые растения. Значит (вывод): некоторые деревья имеют красивые цветы. Правильно ли сделан этот вывод? Обоснуй свой ответ	Даны два утверждения и вывод. 1.Некоторые активные интернет-пользователи становятся жертвами кибермошенников 2. Некоторые мои одноклассники – активные интернет-пользователи. Значит (вывод): некоторые мои одноклассники становятся жертвами кибермошенников. Правильно ли сделан этот вывод? Обоснуй свой ответ.
4.	Рассмотрим два утверждения и вывод: «Некоторые звери – зайцы. Некоторые обитатели леса – звери». Вывод: Некоторые обитатели леса - зайцы. Правильно ли сделан этот вывод? Обоснуй свой ответ Скажи, это единственно возможный вывод?	Рассмотрим два утверждения и вывод: Некоторые Web-сайты – вирусные. Некоторые пользователи загружают Web-сайты на свои ПК Вывод: Некоторые пользователи загружают вирусные Web-сайты на свои ПК Правильно ли сделан этот вывод? Обоснуй свой ответ Скажи, это единственно возможный вывод?
5.	Реши задачу. «Коля темнее Сергея. Сергей младше, чем Вова. Вова ниже Коли. Коля старше, чем Вова. Вова светлее, чем Сергей, Сергей выше, чем Коля». Кто самый светлый, кто старше всех и кто самый высокий? Ответ: а) Самый светлый _____ потому что: б) Старше всех _____ потому, что _____ в) Самый высокий _____ потому, что _____ Обоснуй свой ответ	Реши задачу. «Коля темнее Сергея. Сергей младше, чем Вова. Вова ниже Коли. Коля старше, чем Вова. Вова светлее, чем Сергей, Сергей выше, чем Коля». Кто самый светлый, кто старше всех и кто самый высокий? Ответ: а) Самый светлый _____ потому что: б) Старше всех _____ потому, что _____ в) Самый высокий _____ потому, что _____ Обоснуй свой ответ
6.	Реши задачу. «Три бегуна Борисов, Волков, Григорьев в соревновании заняли один - первое место, и двое других – второе». Какое место занял каждый бегун, если Борисов и Волков, Григорьев и Волков заняли разные места?	Реши задачу. «Три бегуна Борисов, Волков, Григорьев в соревновании заняли один - первое место, и двое других – второе». Какое место занял каждый бегун, если Борисов и Волков, Григорьев и Волков заняли разные места?

	а) Первое место занял _____, потому что: б) Два вторых места заняли _____, так как	а) Первое место занял _____, потому что: б) Два вторых места заняли _____, так как
7.	Реши задачу: В лаборатории больных мышей стали усиленно кормить и заставляли немного двигаться. Очень скоро они поправились. При каких условиях можно считать, что мыши поправились? а) от усиленного питания, при условии… б) от движения, при условии ... _ в) от усиленного питания и движения вместе, при условии …	Реши задачу: В лаборатории больных мышей стали усиленно кормить и заставляли немного двигаться. Очень скоро они поправились. При каких условиях можно считать, что мыши поправились? а) от усиленного питания, при условии… б) от движения, при условии ... _ в) от усиленного питания и движения вместе, при условии …
8.	Две девочки и мальчик списывали с доски и сделали ошибки. Одна девочка сидела на второй парте, была невнимательна и много разговаривала с соседями, не знала правил правописания. Вторая - сидела на последней парте, много разговаривала с соседями, носила очки. Мальчик сидел на первой парте, носил очки, разговаривал с соседями, не знал правил правописания. Вопрос. Что было наиболее вероятной причиной того, что ученики сделали ошибки?	Трое подростков стали жертвами кибермошенников. Одна девочка пренебрегала правилами безопасности в интернете, познакомилась в социальной сети с режиссером, который предложил ей пройти пробу для съемки в фильме, но для этого нужно выслать ее фото топлес. Затем он стал шантажировать ее этим фото, настаивая на личной встрече и сексе. Вторая девочка была отличницей, не верила в то, что может стать жертвой мошенников. Перешла по ссылке на сайт с розыгрышем айфонов и дала личные данные для участия. Вскоре с маминой карты были списаны все средства. Мальчик у постоянно поступали угрозы со страниц его случайных знакомых и с анонимных страниц. Он стал нервным, начал хуже учиться. И все время заходил к себе на страницу, чтобы убедиться, что ничего страшного пока не случилось. Вопрос. Что было наиболее вероятной причиной того, что ребята стали жертвами кибермошенников?
9.	Прочти текст и определи, есть ли в нем предложение, не связанное с основной темой, не относящееся к ней. Обоснуйте свой ответ «Воет вьюга. Холодно. Лед. Во льду промоина. В промоине рыба ходит. Забрался мишка в промоину, шумит, лапищами воду толчет. Это он так рыбу ловит. Оглушит медведь рыбину, зацепит ее когтями и отправит в рот. Вкусно».	Прочти текст и определи, есть ли в нем предложение, не связанное с основной темой, не относящееся к ней. Обоснуйте свой ответ. «Интернет - зло. В обычной жизни мы пытаемся сохранить своё имущество и частную жизнь с помощью замков, камер охраны, сейфов для хранения ценных вещей. Защититься в интернете гораздо сложнее. Мошенники изобретают всё более изощрённые способы атаки. Помимо прямых угроз, преступники исполь-

		зуют так называемую социальную инженерию — проникают вам в доверие и выманивают личные данные и деньги.»
10.	«В зимнем тумане встает холодное, тусклое солнце. Спит заснеженный лес. На лесной поляне тихо. Жители леса попрятались от лютого холода. Вдруг веселая стайка клестов пронеслась над поляной. Эти птицы боятся мороза». Скажите, нет ли в данном тексте предложений, имеющих значение, которое не совпадает с содержанием остальных предложений и противоположны этому содержанию.	Вирусы на ПК попадают из зараженного электронного письма или файла, приложенного к письму – нельзя открывать письма, пришедшие из неизвестных источников, а особенно скачивать и запускать файлы, прикрепленные к этим письмам. Вирусы могут распространяться даже через текстовые файлы, например, в формате. pdf; через зараженный сайт – многие сайты способны самостоятельно устанавливать на компьютеры вирусы. Для этого бывает достаточно просто открыть страницу. Это особенно актуально для нелегальных сайтов, например, с пиратским контентом, через установку неизвестных приложений с неизвестного сайта – если вы скачиваете что-либо из Интернета, убедитесь, что источник надежен. Программы лучше скачивать с по тем ссылкам, которыми уже пользовались другие люди до вас.
11.	«Пеликана узнаешь сразу по большому мешку под клювом. Во время ловли рыбы птица набивает ею мешок до отказа, а потом на берегу спокойно съедает добычу. Чайки тоже съедают рыбу на берегу. Пеликаны не могут нырять. Рыбу они ловят только на мелких местах». Прочти текст и найди предложение, не соответствующее его основной теме.	Прочти текст и найди предложение, не соответствующее его основной теме. Не открывайте письма и сообщения от незнакомых отправителей; • Не скачивайте пиратский контент; • Внимательно проверяйте адреса веб-сайтов, которые вы посещаете; • Не устанавливайте на телефон или компьютер, приложение из непроверенного источника; • Не давайте приложениям разрешения, которые не нужны им для работы – приложению «калькулятор» не нужен доступ к микрофону смартфона; • Следите за своими расходами в сети и за тем, какие подписки оформляют приложения; • В настройках телефона отключите уведомления от приложений, которые вы не хотите получать; • Проводите меньше времени в сети, это плохо влияет на психику; • Установите на компьютер и телефон антивирус;

		• Храните на телефоне как можно меньше информации о себе. Так вы защититесь от утечки данных; • Подключите на телефоне функцию защиты от спама. На некоторых устройствах она доступна в настройках или ее можно подключить у мобильного оператора.
12.	«Дятел уселся на дерево. Он деловито передвигается вверх по стволу. Вот он откидывает назад голову и быстро начинает ударять клювом по дереву. А кругом стоит тишина». Подумай, нет ли в этом тексте предложения, противоположного по значению другим предложениям и, если есть, то каким?	Подумай, нет ли в этом тексте предложения, противоположного по значению другим предложениям и, если есть, то каким? «Желание быть лучшим порождает зависимость, которая проявляется в растрате денег на своих игровых персонажей для покупки виртуальных улучшений и предметов. Из соображений экономии игроки покупают виртуальные ценности у интернет-продавцов по самым низким ценам, что соответствует правилам кибербезопасности».
13.	В полемике против сенатора от штата Флорида К. Пеппера, его противник заявил: «…все ФБР и каждый член конгресса знают, что Клод Пеппер бесстыдный экстраверт. Более того, есть основания считать, что он практикует непотизм по отношению к своячнице, сестра его была феспианкой в греховном Нью-Йорке. Наконец, и этому трудно поверить, хорошо известно, что до женитьбы Пеппер практиковал целибат». В результате этого К. Пеппер потерпел поражение на очередных выборах. Вопрос: Что, на ваш взгляд, сыграло решающую роль в поражении сенатора К. Пеппера?	В полемике против сенатора от штата Флорида К. Пеппера, его противник заявил: «…все ФБР и каждый член конгресса знают, что Клод Пеппер бесстыдный экстраверт. Более того, есть основания считать, что он практикует непотизм по отношению к свояченице, сестра его была феспианкой в греховном Нью-Йорке. Наконец, и этому трудно поверить, хорошо известно, что до женитьбы Пеппер практиковал целибат». В результате этого К. Пеппер потерпел поражение на очередных выборах. Вопрос: Что, на ваш взгляд, сыграло решающую роль в поражении сенатора К. Пеппера?
14.	Судья Верховного суда США Бреннан решил внести ясность в вопрос, какие наказания считать жестокими и бесчеловечными. Как известно, во многих странах налагается запрет на такие наказания, которые являются жестокими и бесчеловечными. Судья Бреннан предложил следующий вариант: «Наказание является жестоким и бесчеловечным... если оно несовместимо с человеческим достоинством». Согласны вы с вариантом наказания, предложенным судьей Бреннаном?	Судья Верховного суда США Бреннан решил внести ясность в вопрос, какие наказания считать жестокими и бесчеловечными. Как известно, во многих странах налагается запрет на такие наказания, которые являются жестокими и бесчеловечными. Судья Бреннан предложил следующий вариант: «Наказание является жестоким и бесчеловечным... если оно несовместимо с человеческим достоинством». Согласны вы с вариантом наказания, предложенным судьей Бреннаном?
15.	Предположим, вы являетесь водителем автобуса. На первой остановке к вам в автобус вошли 6 мужчин и 2 женщины. На	Предположим, вы являетесь водителем автобуса. На первой остановке к вам в автобус вошли 6 мужчин и 2 женщины. На

	второй остановке 2 мужчин вышли из автобуса и 1 женщина вошла. На третьей остановке вышел 1 мужчина, а вошли 2 женщины. На четвертой — вошли 3 мужчин, а 3 женщины вышли из автобуса. На пятой остановке 2 мужчин вышли, 3 мужчин вошли, 1 женщина вышла и 2 женщины вошли. Как зовут водителя автобуса?	второй остановке 2 мужчин вышли из автобуса и 1 женщина вошла. На третьей остановке вышел 1 мужчина, а вошли 2 женщины. На четвертой — вошли 3 мужчин, а 3 женщины вышли из автобуса. На пятой остановке 2 мужчин вышли, 3 мужчин вошли, 1 женщина вышла и 2 женщины вошли. Как зовут водителя автобуса?

Таблица 2

Данные валидности и надежности авторского исследовательского опросника

№ п/п	Шкала	Валидность		Надежность		$\rho_{теор}$ 0,05	$\rho_{теор}$ 0,01
		Рэксп содержательная	Рэксп критериальная	Константность	Стабильность	0,79	0, 81
1.	умение делать логические умозаключения и обосновывать свой ответ;	0,96	0,90	0,91	0,92		
2.	умение оценивать последовательности умозаключений	0,94	0,93	0,93	0,97		
3.	умение анализировать и делать заключение о причинах явлений	0,89	0,94	0,92	0,89		
4.	умение анализировать и оценивать содержание текстов	0,96	0,89	0,93	0,91		
5.	умение обнаруживать ошибки, связанные с неопределенностью и двусмысленностью выражений и терминов	0,87	0,94	0,92	0,89		
6.	умение обнаруживать релевантную (существенную в данном случае) информацию на фоне избыточной	0,93	0,91	0,92	0,99		

Нами была изучена константность путем определения коэффициента корреляции параллельных форм опросника. Через два месяца после основного исследования нами была проведена повторная диагностика с использованием опросника для определения его стабильности. Все полученные коэффициенты подтверждают надежность диагностического инструмента.

Валидизация предполагала определение критериальной и содержательной валидности опросника. Благодаря экспертной помощи дополнены и изменены

все шкалы. Авторский исследовательский опросник проверялся на однородной выборке респондентов. Критериальная валидность проверялась по соответствующим шкалам основного опросника. Оценки по опроснику согласовывались с оценками экспертной комиссии. Экспертами были выбраны педагоги и психологи, имеющие опыт работы не менее 5 лет.

Как видно из таблицы 2, $\rho_{эксп}$ превышает $\rho_{теор}$ (уровни достоверности 0,05 и 0,01), что позволяет говорить о валидности авторского исследовательского опросника. Полученные коэффициенты стабильности и константности психодиагностического инструмента также превышают $\rho_{теор}$, что указывает на высокую надежность опросника.

Приложение 5

Коэффициент корреляции параллельных форм опросника

Таблица 1

Данные валидности и надежности авторского исследовательского опросника

№ п/п	Шкала	Валидность	Надежность		$\rho_{теор}$ 0,05	$\rho_{теор}$ 0,01
		Рэксп содержательная	Константность	Стабильность	0,79	0, 81
1.	Риски, связанные с получением деструктивной информации	0,89	0,81	0, 88		
2.	Риски, связанные с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет	0,84	0,94	0,87		
3.	Осознание рисков киберпространства	0,65	0,91	0,87		

Нами была изучена константность путем определения коэффициента корреляции параллельных форм опросника. Через два месяца после основного исследования нами была проведена повторная диагностика с использованием опросника для определения его стабильности. Все полученные коэффициенты подтверждают надежность диагностического инструмента.

Валидизация предполагала определение содержательной валидности опросника. Благодаря экспертной помощи дополнены и изменены шкалы «Риски, связанные с получением деструктивной информации», «Риски, связанные с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет», «Осознание рисков киберпространства»». Авторский исследовательский опросник проверялся на однородной выборке респондентов.

Оценки по опроснику согласовывались с оценками экспертной комиссии. Экспертами были выбраны педагоги и психологи, имеющие опыт работы не менее 5 лет.

Как видно из таблицы 1, $\rho_{эксп}$ превышает $\rho_{теор}$ (уровни достоверности 0,05 и 0,01), что позволяет говорить о валидности авторского исследовательского опросника. Полученные коэффициенты стабильности и константности психодиагностического инструмента также превышают $\rho_{теор}$, что указывает на высокую надежность опросника.

Нами было выбрано следующее присвоение численных ответов [Таблицы 2, 3].

Таблица 2

Присвоение баллов для шкал «Риски, связанные с получением деструктивной информации», «Риски, связанные с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет», «Осознание рисков кибепространства»

нет	скорее нет, чем да	иногда	скорее да, чем нет	да
4	3	2	1	0

Таблица 3

Присвоение баллов для шкалы «Осознание рисков кибепространства»

нет	скорее нет, чем да	иногда	скорее да, чем нет	да
0	4	3	2	1