ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
(Н И У « Б е л Г У »)

ИНСТИТУТ ОБЩЕСТВЕННЫХ НАУК И МАССОВЫХ КОММУНИКАЦИЙ

КАФЕДРА СОЦИОЛОГИИ И ОРГАНИЗАЦИИ РАБОТЫ С МОЛОДЕЖЬЮ

СОЦИАЛЬНЫЕ МЕХАНИЗМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ШКОЛЬНИКОВ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

Выпускная квалификационная работа
направления подготовки 39.04.01 Социология
2 курса группы 10001726
Демяненко Анны Владимировны

Научный руководитель
кандидат социологических
наук, доцент
С. В. Хашаева

БЕЛГОРОД 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы выпускной квалификационной работы. В настоящее время во всех сферах жизни общества продолжают происходить глобальные перемены, вызванные развитием информационных технологий. Образование в 21 веке в условиях информационного общества – не просто способ усвоения стандартизированного массива знаний, а один из методов информационного обмена человека с окружающим миром. Различие между информацией и знанием, относительность последнего вследствие быстрого устаревания данных, трансформация образовательного процесса в непрерывный круг ведут к тому, что основной единицей образовательного процесса становится информация, а не знание. Следовательно, одной из задач современного образования становится обучение работе с информацией.

Актуальность безопасности школьника в сфере информации можно определить, с одной стороны, действием возникающих в современном обществе цивилизационных изменений, влияющих на формирование и развитие личности подрастающего человека как субъекта социального поведения. В то же время существует необходимость изменения в образовании, науке, общественном сознании и социальной практике приоритета безопасности личности перед общественной безопасностью.

Более половины респондентов исследования, которое проводили Г. Солдатова, Е. Рассказова, Е. Зотова, М. Лебешева, П. Роггендорф для международного проекта EU Kids Online среди российских детей, осознают, что Интернет все-таки содержит контент, который должен быть запрещен к просмотру в их возрасте. Около четверти детей имеет отрицательный опыт столкновения с негативом в сети. Стоит заметить, что 14% родителей считают, что их ребенок мог расстроиться из-за столкновения с чем-либо негативным в Интернете. На самом деле детей, попадавших в подобные

ситуации, в два раза больше (26%). Это говорит нам о том, что ситуация разнится с детей и с точки зрения родителей[1].

На сегодняшний день остро стоит проблема отсутствия чётко сформулированной и отражённой в нормативных актах теории информационной безопасности.

Базовым документом, определяющим государственную политику в этой области, является «Доктрина информационной безопасности Российской Федерации», утвержденная 5 декабря 2016 года. В качестве интересов личности, определяющих состояние её безопасности, выделяются реализация конституционных прав и свобод, обеспечение личной безопасности, повышение качества и уровня жизни, духовное, интеллектуальное и свободное развитие человека и гражданина[2].

В настоящее время уголовный кодекс РФ не предусматривает меры борьбы с ресурсами, опрашивающими несовершеннолетних без согласия родителей, а также содержащими информацию, способную негативно повлиять на духовное и психическое развитие школьников.

Таким образом, актуальность изучения проблемы заключается в следующем:

1. Современное состояние информационного пространства не позволяет назвать Интернет безопасным источником знаний для школьников.

2. Рост значимости использования информационных технологий, в частности Интернета, в образовательном и воспитательном процессе.

3. Несовершенство законодательной системы, отсутствие достаточного контроля со стороны родителей и государства, способное привести к нарушению информационной безопасности незрелой личности школьника.

---

[1] Солдатова Г., Зотова Е. Агрессоры и жертвы // Дети в информационном обществе. М., 2012. № 11.

[2] Указ Президента Российской Федерации «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 г. № 646 // Собрание законодательства Российской Федерации (СЗ РФ). 2016. № 50. Ст. 7074.

Степень научной разработанности темы. Тема информационной безопасности является относительно новой, но при этом активно изучается как российскими, так и зарубежными авторами. С точки зрения права и юриспруденции информационную безопасность рассматривали И. Л. Бачило в труде «Информационные ресурсы развития Российской Федерации: правовые проблемы» и Е.К. Волчинская в двух трудах: «Коммерческая тайна в системе конфиденциальной информации. Информационное право» и «Место персональных данных в системе информации ограниченного доступа»[1].

Теоретико-методологические подходы социологического анализа структуры и функций информационного пространства рассматривались В. С. Игнатовым и Д. В. Пименовой в работе «Информационное пространство. Структура и функции», а также А. С. Круль в работе «Социологические исследования информационных структур социальных систем»[2].

Процесс интеграции Интернета в различные сферы жизни, в том числе и образование, изучали И. В. Мелик-Гайказян в работе «Критерии определения границ в образовательном пространстве» и М.С. Мельникова в труде «Социальные аспекты Интернета: Постановка проблемы»[3].

---

[1] Бачило И. Л. Информационные ресурсы развития Российской Федерации: правовые проблемы. М., 2003; Волчинская Е. К. Место персональных данных в системе информации ограниченного доступа. URL: http://cyberleninka.ru/article/n/mesto-personalnyh-dannyh-v-sisteme-informatsii-ogranichennogo-dostupa (дата обращения: 20.04.2019).

[2] Игнатов В. С. Пименова Д. В. Информационное пространство. Структура и функции // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2007. № 3. URL: http://cyberleninka.ru/article/n/informatsionnoe-prostranstvo-struktura-i-funktsii (дата обращения: 27.04.2019); Круль А. С. Социологические исследования информационных структур социальных систем // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2009. № 4 (12). URL: http://cyberleninka.ru/article/n/sotsiologicheskie-issledovaniya-informatsionnyh-struktur-sotsialnyh-sistem (дата обращения: 30.04.2019).

[3] Мелик-Гайказян И. В. Критерии определения границ в образовательном пространстве. URL: http://cyberleninka.ru/article/n/kriterii-opredeleniya-granits-v-obrazovatelnom-prostranstve (дата обращения: 11.04. 2019); Мельникова М. С. Социальные аспекты интернета: постановка проблемы. URL: http://cyberleninka.ru/article/n/sotsialnye-aspekty-interneta-postanovka-problemy (дата обращения: 11.03. 2019).

В труде «Принципы классификации моделей коммуникации» Л. Р. Тухватулина даёт анализ наиболее важных моделей коммуникации, а также способ их упорядочивания в рамках информационно-синергетического подхода[1].

Проблема выпускной квалификационной работы заключается в противоречии между появившимся у школьников свободным доступом к информационным ресурсам сети Интернет и необходимостью комплексного контроля контента, опасного для лиц, не достигших совершеннолетнего возраста.

Объект выпускной квалификационной работы – информационная безопасность школьников в глобальной сети Интернет.

Предмет выпускной квалификационной работы – социальные механизмы управления информационной безопасностью школьников в глобальной сети Интернет.

Цель выпускной квалификационной работы – изучить актуальное состояние действенных социальных механизмов управления информационной безопасностью школьников, использующих глобальную сеть Интернет.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. Изучить сущность социальных механизмов управления информационной безопасности личности.

2. Проанализировать современное состояние развития социальных механизмов управления информационной безопасностью личности.

3. Выявить пути совершенствования социальных механизмов управления информационной безопасностью личности.

Теоретико-методологическая база выпускной квалификационной работы. Теоретической основой исследования являются общедидактические

[1] Тухватулина Л. Р. Принципы классификации моделей коммуникации. URL: http://cyberleninka.ru/article/n/printsipy-klassifikatsii-modeley-kommunikatsii (дата обращения: 22.03. 2019).

принципы и критерии оптимизации организации обучения (Ю. К. Бабанский, В. П. Беспалько, Г. А. Бордовский, В. С. Леднев, В. Н. Слободчиков и др.[1]), теория информации, кибернетика (Н. Винер, В. М. Глушков, В. А. Извозчиков, К. Шеннон и др.[2]). Кроме того, была рассмотрена теория безопасности (Г. В. Грачев, В. Н. Кузнецов, А. Д. Урсул и др.[3]).

Так же были изучены результаты гуманитарных исследований Интернет-ресурсов (А. Е. Войскунский и др.[4]) и эволюция концепций информатизации образования (А. А. Веряев, А. П. Ершов, И. В. Роберт, А.Ю. Уваров и др.[5]).

Методологической основой исследования стали такие методы научного познания, как общетеоретические (формализация, изучение и анализ литературы, нормативно-правовых актов, индукция, дедукция), эмпирические (экспертное интервью, опрос, фокус-группа).

Эмпирическую базу выпускной квалификационной работы составили результаты социологических исследований, проведенные в разное время различными научными коллективами. В том числе:

---

[1] Бабанский Ю. К. Методы обучения в современной общеобразовательной школе. М., 2003; Беспалько В. П. Основы теории педагогических систем. Воронеж, 1977; Бордовский В. А. Инновационные процессы в современной системе высшего педагогического образования. СПб., 2010; Леднев В. С. Основы теории содержания профессионально-педагогического образования: монография. М., 2006; Слободчиков В. И. Образовательная среда: реализация целей образования в пространстве культуры. М., 1997. Вып. 7.

[2] Винер Н. Кибернетика и общество. М., 1958; Глушков В. М. Основы безбумажной информатики. М., 1987; Бордовский Г. А., Извозчиков В. А., Исаев Ю. В., Морозов В. В. Информатика в понятиях и терминах. М., 2006; Шеннон К. Э. Работы по теории информации и кибернетике (сборник статей). М., 1963.

[3] Грачев Г. В. Информационно-психологическая безопасность личности: теория и технология психологической защиты: дис. … д-ра психол. наук. М., 2000; Кузнецов В. Н. Культура безопасности. Тезисы к докладу «Культура безопасности в трансформирующемся обществе». М., 2002; Урсул А. Д. Информатизация общества и переход к устойчивому развитию цивилизации // Вестник РОИВТ. 1993. № 1-3.

[4] Войскунский А. Е., Бабаева Ю. Д., Смыслова О. В. Интернет и личность. Санкт-Петербург. // Тезисы докладов Международной конференции «Интернет.Общество.Личность». СПб, 1999.

[5] Веряев А. А. Семиотический подход к образованию в информационном обществе. Монография. Барнаул., 2000; Ершов А. П. Информатизация: от компьютерной грамотности учащихся к информационной культуре общества // Коммунист. 1988. № 22; Роберт И. В. Современные информационные технологии в образовании. М., 1994; Уваров А. Ю. ИНТЕРНЕТ в школе: Смена парадигмы. Информатика и образование. 2001. № 3. URL: http://center.fio.ru/vio/VIO01 /Articlel 6.htm (дата обращения: 19.03.2019).

1. «Дети России онлайн». Руководители – Г. Солдатова, Е. Рассказова, Е. Зотова, М. Лебешева. Число участников опроса – 2050 респондентов. Анкетный опрос пар «родитель-ребенок», включающих детей 9-16 лет и одного из их родителей, 11 регионов России: Забайкальский край, Кемеровская, Кировская области, Москва, Московская область, Республика Дагестан, Республика Коми, Ростовская область, Санкт-Петербург, Саратовская, Челябинская области. Ноябрь 2010 г.[1]

2. Исследование «Растим детей в эпоху Интернета» проведено специально для «Лаборатории Касперского» организацией IconKids&Youth. Число участников опроса – 3780 семей с детьми от 8 до 16 лет (один родитель и один ребенок из семьи) в России, США, Великобритании, Германии, Франции, Испании, Италии. В России было опрошено 540 семей. 2016 г[2].

3. Так же были использованы данные администрации города при реализации программы «Развитие солидарного общества и информационного пространства городского округа города Белгорода на 2017-2020 годы»[3].

4. Было проведено авторское исследование «Социальные механизмы управления информационной безопасностью школьников в глобальной сети Интернет г. Белгорода». Первый этап – массовый опрос. Выборка смешанная. Число участников опроса – 716 и 402 респондента. Анкетный опрос населения г. Белгорода. Второй этап – проведение двух интервью и двух фокус-групп с использованием кейсов. Число участников 8 и 9 человек. Третий этап – проведение контент-анализа. Май 2019 г.

5. Использовались так же данные Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. N 149-ФЗ с дальнейшими дополнениями и др.

---

[1] Солдатова Г., Рассказова Е. Роль родителей в повышении безопасности ребенка в интернете: классификация и сопоставительный анализ // Вопросы психологии. 2013. № 2.
[2] URL: https://www.kaspersky.ru/about/press-releases/2016_actions-of-children-on-the-web (дата обращения: 18.04.2019).
[3] URL: http://www.beladm.ru/publications/publication/informatizaciya-municipalnogo-upravleniya-na-2015-/ (дата обращения: 17.04.2019).

Научно-практическая значимость выпускной квалификационной работы заключается в том, что в работе выявлен информационный контекст безопасности школьников, комплексные варианты защиты школьников от информационного воздействия сети Интернет в современных условиях развития постиндустриального общества.

Под основными интересами учащихся в данном контексте понимается реализация конституционных прав на получение качественного образования и информации, направленных на формирование информационной культуры учащихся, их физического, духовного и интеллектуального развития, на обеспечение личной безопасности, на повышение качества и уровня жизни. Разработана концепция, включающая понятийный аппарат проблемы, основные источники информационной опасности и виды угроз, обобщенную алгоритмическую модель системы обеспечения информационной безопасности школьников, вариативные модели и целостную систему педагогических условий ее реализации в школе и домашних условиях.

Структура ВКР. Выпускная квалификационная работа содержит введение, три раздела, заключение, список источников и литературы, приложения.

РАЗДЕЛ I. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКОЕ ОБОСНОВАНИЕ СОВРЕМЕННОГО СОСТОЯНИЯ РАЗВИТИЯ СОЦИАЛЬНЫХ МЕХАНИЗМОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ШКОЛЬНИКОВ

С каждым годом поток информации, оказывающий непосредственное влияние на современное общество, увеличивается в объемах, посредством возникновения новых информационных каналов. На сегодняшний день самым распространенным и передовым каналом является система Интернет – компьютерная паутина, позволяющая людям из разных уголков Земли за считанные секунды получить различного рода информацию, от обычного прочтения книги до создания виртуальной реальности. Именно благодаря такому темпу информационного развития, объем суммарных знаний человечества, по сравнению с 70-ми и 80-ми годами XX в., удваивается практически каждый год.

Интернет во втором десятилетии XXI века можно полноправно назвать целым социальным институтом, поскольку, будучи социокультурным феноменом, он демонстрирует, главным образом, возрастающую социальную значимость для жизнедеятельности человека. Однако при этом не стоит упускать из вида и технико-технологическую и экономическую важность. Ведь возможности информатики и вычислительной техники сейчас во многом определяют научно-технические возможности страны, уровень формирования ее народного хозяйства и социума. Поэтому с уверенностью можно сказать, что анализ информации и обмен ею является обязательным условием жизнедеятельности общества[1].

Поскольку информация уже давно стала активом, имеющим необозримую ценность, она должна быть защищена надлежащим образом, независимо от ее вида, а также форм хранения и распространения. Для этого используется определение «информационная безопасность», то есть политика мер, реализуемая для обеспечения контроля над рисками

[1] Лопатин В. Н. Информационная безопасность России: Человек, общество, государство. М., 2000.

информационной стабильности и безопасности. Получается, что информационная безопасность ограждает от обширного диапазона угроз для того, чтобы обеспечить людей уверенностью в своем психологическом состоянии, минимизации ущерба, получения максимальной отдачи от работы в глобальной Сети и реализации потенциальных возможностей социума.

Согласно определениям ученых, в настоящий момент область информации можно поделить на две составные части: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую, иными словами психофизическую (человек, коллектив). В данной работе будет рассматриваться информационная безопасность для школьников как психофизическая[1].

На сегодняшний день совершенно очевидно, что родители и преподаватели обязательно должны владеть основами информационных технологий и методикой их использования, так как их основной задачей является передача этих знаний детям школьного возраста. А также это помогает контролировать и бороться с распространением угроз в сети Интернет по отношению к несовершеннолетним детям, поскольку время, проведенное ими в Сети, с каждым годом увеличивается[2].

Такая зависимость объясняется несколькими причинами. В первую очередь стоит учитывать, что Интернет – это неиссякаемый источник и распространитель знаний, как платных, так и бесплатных, по всевозможным и вседоступным предметам. Второй причиной можно с уверенностью назвать индустрию развлечений и общения, от игровых просторов, до социальных сетей и общения с единомышленниками. Плюсом ко всему Интернет дает доступ к огромной платформе финансовых операций.

Однако самая большая проблема виртуальной сети Интернет, это ее свойство стирать границы между реальным и виртуальным миром.

---

[1] Асанович В. Я. Информационная безопасность: анализ и прогноз информационного воздействия. Минск, 2006.

[2] Воронов Р. В., Гусев О. В., Поляков В. В. О проблеме обеспечения безопасного взаимодействия с сетевыми образовательными ресурсами // Открытое образование. 2008. № 3.

Безмерные возможности Интернета, как самой современной технологии, захватывают детей настолько, что они автоматически становятся самой уязвимой возрастной группой пользователей, так как не в состоянии распознать всех опасностей и рисков глобальной Сети.

Информационная безопасность – многосторонняя сфера деятельности, в которой добиться положительных результатов можно только при комплексном подходе[1].

Интересы субъектов, связанных с использованием информационных систем, заключаются в обеспечении доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Стоит отметить, что помимо глобальных опасностей требуют особого внимание угрозы, которым подвергается каждый человек ежедневно в условиях информационного общества.

Информационная безопасность личности – это состояние и условия жизнедеятельности личности, при которых реализуются ее информационные права и свободы.

А угроза – это потенциальная возможность каким-либо способом нарушить информационную безопасность[2].

К угрозам, которые могут нанести непосредственный психофизический вред школьникам, относятся:

- кибербуллинг;
- секстинг;
- овершеринг;
- секты;
- наркотики;
- вписки;

[1] Родичев Ю. А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. СПб., 2008.
[2] Привалов А. Н. Основные угрозы информационной безопасности субъектов образовательного процесса // Известия ТулГУ. Гуманитарные науки. Тула, 2012. № 3.

- педофилия;
- мошенничество.

В 1993 году ученые И. Уитни и П. Смит в своем исследовании определяют «буллинг» как долговременные проявления агрессии, угрозы, оскорбления, диффамации, которые направлены от одного человека или группы лиц в адрес жертвы, не способной защититься[1].

С появлением сети Интернет появилось и дополнительное определение данному виду агрессии – кибербуллинг. В переводе с английского языка это обозначает Интернет-травля. В отличие от обычного запугивания, здесь используются различные средства коммуникации: компьютеры, планшеты, мобильные телефоны.

На сегодня существует несколько возможных классификаций кибербуллинга. Например, по способу взаимодействия между пользователями, степенью вовлеченности участников коммуникации и тяжестью вероятных последствий данной коммуникации.

В феврале 2015 года на образовательном портале www.kids.kaspersky.com была опубликовании статья под названием «10 forms of cyberbullying» (десять видов кибербуллинга)[2]. Она максимально наполнена «свежем» контентом, охватывающим всевозможные виды травли в Интернете. Рассмотрим некоторые представленные в ней виды:

1. «Издевательство» – неуклонные и целенаправленные угрозы и оскорбления в сообщениях, которые отправляются человеку. Они оказывают сильное влияние на объект, особенно на школьника с несформированной самооценкой, заставляют испытывать страх и неуверенность в себе.

2. «Аутинг» – публикация в Интернете личной или конфиденциальной информации о человеке без его согласия с целью публичного унижения жертвы.

---

[1] Уитни И., Смит П. Обследование характера и степени издевательств в младших, средних и средних школах // Образовательные исследования. 1993. №35.
[2] URL: www.kids.kaspersky.com (дата обращения: 11.02.2019).

3. «Фрэпинг» – это использование постороннего аккаунта в Интернете без разрешения владельца с целью публикации нежелательной информации от его лица, часто направленного против знакомых людей.

4. Обман – форма Интернет-травли, оказывающее особое влияние на психологическое состояние подростка. Он состоит в том, что инициатор завоевывает доверие жертвы и мотивирует поделиться с ним личной информацией, которую затем публикует онлайн, а общение с жертвой прекращает. Жертва, особенно ребенок с обостренным чувством восприятия, испытывает разочарование, обиду, чувствует себя преданным.

5. «Троллинг» – высмеивание, оскорбление и обесценивание личности человека. Данный вид так же оказывает сильное воздействие на уязвимых и неуверенных в себе детей[1].

Опасность кибербуллинга в школьной среде заключается так же в том, что его сложно заметить на этапе возникновения[2]. Причин, по которым в школе может возникнуть ситуация Интернет-травли, несколько:

1. Плохая психологическая атмосфера в классе.
2. Прерывание дружественных отношений между учениками.
3. Проблемы, проявляющиеся во время школьных мероприятий: конкурсов, состязаний, экскурсий.

По данным исследования 2010 года, 45% жертв сообщили, что они испытали злобу, 28% подростков испытали чувства раздосадованности и разбитости, 27% признались, что оскорбления расстроили их очень сильно. Менее 30% жертв сообщили, что столкновение с кибербуллингом никак на них не повлияло[3].

Стоит упомянуть еще один факт, касающийся последствий, к которым может привести кибербуллинг – взаимосвязь участия в Интернет-травли в

---

[1] Солдатова Г., Зотова Е. Агрессоры и жертвы // Дети в информационном обществе. 2012. № 11.
[2] Лучинкина А. И. Информационно-психологическая безопасность детей и подростков в интернет-пространстве // Ученые записки Крымского инженерно-педагогического университета. 2015. № 1.
[3] Бордовский В. А. Инновационные процессы в современной системе высшего педагогического образования. СПб., 2010.

качестве жертвы и склонности к суициду. Результаты исследования 2010 года показывают, что жертвы кибербуллинга предпринимали попытки суицида в два раза чаще, чем их ровесники, не становившиеся жертвами травли в Интернете. Эта статистика регулярно подтверждается материалами в медиа. Обычно кибербуллинг не является единственной причиной суицида, но может выступать как катализатор к данному действию.

Исходя из вышесказанного, ясно, что кибербуллинг является современной разновидностью Интернет-коммуникации, встречающийся среди слоев населения разного возраста, однако наиболее характерный для подростков в возрасте от 12 до 15 лет, ведущих активную виртуальную жизнь.

Желание людей рассказывать или размещать информацию личного характера, перебарщивая с откровенностью и не обращая внимания на границы приватности, получило название овершеринг. Термин появился в 2013 году[1].

К отличительным чертам овершеринга на Интернет-страницах школьников относятся:

- стремление поделиться подробностями личной жизни;
- наличие чрезмерно большого количества селфи;
- регулярное обновление статусов только «о себе»;
- неподдельный интерес только к темам, касающимся собственной персоны[2].

Овершеринг является одной из самых больших опасностей, подстерегающих детей в Интернете. Это относится и к информации, которую дети помещают в сеть сами, а также и к помещенной туда кем-то другим, например, даже родителями. Фото во время купания в младенчестве могут стать причиной насмешек в школьном возрасте. Информацию, которую люди публикуют самостоятельно, на сегодняшний день изучает целый ряд

[1] Зверева Е. А. Информация как объект неимущественных гражданских прав // Право и экономика. 2013. № 9.
[2] Кирмайер М. Информационные технологии. СПб., 2013.

совершенно незнакомых людей: исследователи, рекламные агентства, журналисты, спецслужбы, секты и экстремистские организации, преступники самых разных мастей и потенциальные работодатели.

Существует информация, которая, попав в Интернет, может нанести школьнику вред. С особой осторожностью стоит указывать такие данные, как:

1. Настоящие имя и фамилию.
2. Год рождения.
3. Домашний адрес.
4. Номер школы, в которой ты учишься.
5. Информацию о родителях и других родственниках.
6. Номер телефона.
7. Текущую геолокацию.
8. Эротические селфи.
9. Фотографии с дорогими подарками.
10. Компрометирующие снимки других людей.
11. Особое мнение.

Дети школьного возраста могут не замечать опасности наличия личной информации в Интернете, которая может быть использована в дальнейшем против них посредствам мошенничества, шантажа, извращений.

С появлением технологий, позволяющих обмениваться сообщениями по телефону, электронной почте или соцсетям, люди стали присылать друг другу письма разного рода, в том числе и интимного содержания[1]. Такая пересылка личных фотографий и сообщений получила название секстинг. Если переводить дословно – переписка сексуального характера.

Впервые этот термин был упомянут в 2005 году, как новая тенденция среди молодежи в Британской газете Sunday Telegraph Magazine[2]. А в 2008 году слово было добавлено в Новый Оксфордский Американский словарь,

---

[1] Юшина О. Л. Информационно-психологическая безопасность: библиотековедческий аспект (по материалам зарубежной литературы) // Науч. и техн. б-ки. 2003. № 11.
[2] URL: https://www.telegraph.co.uk/ (дата обращения: 21.01.2019).

как обозначение процесса, во время которого участники беседы обмениваются сообщениями, фотографиями и видеофайлами интимного содержания.

Профессор Йоркского университета в Торонто П. Камминг утверждает, что сексинг является вполне безопасным средством коммуникации в подростковом возрасте, который помогает постигнуть свою сексуальность, без негативных воздействий на психику ребенка. Основная опасность от секстинга это его возможные последствия, такие как скандал или самоубийство из-за обнародования чьих-то интимных файлов[1].

В некоторых странах секстинг относится к уголовным преступлениям. Например, в Австралии и США фотографии несовершеннолетних сексуального характера относятся к детской порнографии или лицу, отправляющему интимные фотографии, может быть предъявлено обвинение в сексуальном домогательстве.

Ученые Мичиганского университета выявили, что секстинг по своей сути безопасен. Выборку их исследования составили 3447 человек в возрасте от 18 до 24 лет.

Так же результаты исследования в журнале о подростковом здоровье говорят, что чрезмерного риска в секстинге нет, так же он сам по себе не является источником психологических проблем. Это подтверждает доцент Хосе Бормейстер, который заметил, что представление секстинга в СМИ и медицинских службах нельзя сопоставить с реальной картиной, так как оно не является девиантным или преступным поведением.

В 2015 году, было проведено новое исследование учеными университета Индианы[2]. Результаты их исследования отличаются от предыдущего: секстинг не всегда является взаимным и безопасным. Один из авторов исследования и специалист в области возрастной психологии

---

[1] Ефимова Л. Л. Информационная безопасность детей. Российский и зарубежный опыт: монография. М., 2015.

[2] Пушкарева Н. Л. Повседневная жизнь в России: междисциплинарный подход // Антропологический форум. 2011. №14.

Мишель Друин считает, что занятие секстингом по принуждению партнера при помощи манипуляций и угроз может оказаться негативным и травмирующим опытом (20% респондентов), а также стать новым видом партнерского насилия. Выборку данного исследования составили 480 молодых людей, из которых 71% пробовали заниматься секстингом.

Исследователи Индианского университета советуют обратить внимание на эту проблему: «Так как секстинг сейчас очень распространен среди молодых людей, многие могут думать, что принуждать заниматься им нормально и даже безобидно», а это не совсем так.

Времяпрепровождение с друзьями и сверстниками играет важную роль в жизни ребенка. Один из современных способов для молодежи собраться вместе называется вписка.

Вписка – это вечеринка для малознакомых или вообще незнакомых подростков, которые устраиваются в квартире или частном доме в отсутствие взрослых и часто с наличием алкоголя.

Основная цель вписки – это весело провести время вне дома и без взрослых. В зависимости от характера встречи, можно выделить несколько видов вписок: флэт, легион, подводная лодка, хасл, роуд пати[1].

Чаще всего школьники становятся участниками такого рода развлечений через социальные сети, приложения и «сарафанное радио». В большинстве случаев вечеринки неконтролируемы, количество участников неограниченно, а в большинстве случаев еще и являются незнакомцами. Все чаще СМИ оглашает случаи о чрезмерном распитии алкоголя, употреблении наркотических веществ и беспорядочных половых связях.

Этот вид досуга стал популярен не только среди студентов, но и среди школьников старших, иногда даже и средних классов. «Ой, тебе 16, и ты ещё ни разу не бывала на вписках? Я не могу ни одного моего одноклассника найти, кто бы на них ни бывал», – приводит слова 15-летней постоянной участницы вписок корреспондент издания «Комсомольская правда»

[1] URL: http://www.safor.ru/ (дата обращения: 27.02.2019).

Д. Карпицкая. Насчитывается 561274 человека в возрасте до 18 лет среди участников подобных групп[1].

Кроме предложений посетить вписку, в группах принято выкладывать фото или видео «отчеты» о том, как прошла вечеринка. На этих материалах можно встретить молодых людей, которые не достигли совершеннолетия, в нетрезвом состоянии или обнаженном виде.

Опасность для школьников состоит в том, что в силу своего возраста они не могут адекватно оценить степень опасности нахождения на подобной вписке с незнакомыми людьми, переоценивают свои возможности, предпочитают идти против правил безопасного поведения.

Вторая угроза идет от Интернета. Многие подростки стараются заснять свои «подвиги» на вписках и выложить их в Сеть по двум основным причинам: стремление заслужить славу, так как ролики с аморальным поведением набирают большое количество просмотров, и уверенность в своей безнаказанности.

Одними из самых опасных психоактивных веществ являются наркотики. На первый взгляд сложно связать их с всемирной паутиной, но в настоящее время очень распространены случаи продажи и распространения наркотических веществ через Интернет[2].

Специалисты, работающие над данной темой в «Лаборатории Касперского», проанализировали сайты и различные Интернет-порталы в различных регионах России[3]. Было выявлено, что чаще всего, а это 73%, дети посещают всевозможные соцсети, форумы, чаты, которые позволяют поддерживать коммуникацию с другими людьми. Второе место в этом исследовании заняли Интернет-страницы, на которых располагалась информация об алкоголе, табакокурении и наркотиках. Так как дети проводят огромное количество времени в Интернете, запрещенный контент

---

[1] URL: http://www.webwisekids.com (дата обращения: 13.01.2019).
[2] Игер Б. Работа в Internet. М.,1996.
[3] URL: https://www.kaspersky.ru/about/press-releases/2016_actions-of-children-on-the-web (дата обращения: 18.04.2019).

на сайтах становится особой угрозой, которой не было до появления Интернета.

Доступность данного контента знакомит детей с местами приобретения и способами употребления наркотических веществ, с описанием опыта других детей, обменом опытом. Широко обсуждается положительный эффект от приема наркотиков, их лекарственные свойства. Существует множество натуральных и химических заменителей, лекарств, которые обладают аналогичными свойствами. Многие из них легко приобрести, так как она имеются в свободной продаже.

Продажа данного вида наркотиков осуществляется, например, через форум Legal.RC. Несмотря на то, что в РФ Роскомнадзор ограничил доступ к нему, существует несколько обходных способов его посещения через различные браузеры и т.п. Все препараты на данном сайте считаются «легальными», их состав периодически меняется для этого[1].

Помимо такой опасности, что ребенок будет употреблять наркотические вещества, существуют случаи, при которых дети вербуются в качестве распространителей наркотиков. Это еще один хорошо отлаженный механизм, «бизнес» в Интернете.

Предложения хорошего заработка и свободного графика часто привлекает подростков. Часто источником таких предложений является реклама: «Работа мечты. Всего 4 часа в день. Заработок 100000 рублей в месяц». Интернет источники описывают процесс «устройства» на такую работу следующим образом: кандидат направляется по гиперссылке на адрес ресурса, где он подробно знакомится со своими обязанностями, причем работу он получит после того, как оставит денежную сумму или копию паспорта в качестве залога.

[1] Борисов М. А. Основы организационно-правовой защиты информации. М., 2014.

Ребенок, который является слабой личностью или чьи взгляды и жизненные установки еще не сформированы, является потенциальной жертвой и для вербовки в секты[1].

Сектой называют организацию или группу лиц, сосредоточенных на своих интересах, в том числе и культах, которые отличаются от общепризнанных интересов общества или противоречат им. В понятие секта современный смысл вложил Мартин Лютер, немецкий реформатор и основоположник лютеранства.

До 2015 года в России, чтобы официально оформить секту религиозного уклона, ей необходимо было просуществовать на территории РФ 15 лет. После того, как данный законопроект отменили, количество сект, прикрывающихся молодыми религиозными объединениями, увеличилось. Так же развитие информационного общества поспособствовало тому, что у сект появилась новая площадка для зарождения и развития – Интернет.

Вступление в какую-либо секту, жизнь в ней, а также выход из нее оказывает негативное влияние на психику человека, особенно подростка, у которого она еще не окрепла. Часто этому способствуют разные психотропные препараты, психологические приемы, внушения. Опасность в том, что, даже выйдя из-под влияния секты, человек способен покончить жизнь самоубийством, так как не смог приспособиться к обычной социальной среде[2].

На сегодняшний день на территории РФ существует большое количество сект. В данной работе выделили четыре основных способа вовлечь подростка в секту:

- с помощью любви, повышенного внимания;
- влияние на восприятие человеком обстановки с помощью чтения специальной литературы;

[1] Березина Т. Н Об эмоциональной безопасности образовательной среды // Психология и психотехника. 2013. № 9.
[2] Леончиков В. Е. Информационная свобода и информационная безопасность в системе непрерывного образования // Информационная свобода и информационная безопасность: Материалы междунар. научно-практич. конференции. Краснодар, 2001.

- влияние на психику человека, гипноз;
- с помощью Интернета, который объединяет все вышеперечисленное.

В своем исследовании доктор психологических наук Л. Куликова выяснила, что самыми распространенными являются первый и второй способы. На улицах часто раздают брошюры, буклеты, книги. Изучение такой литературы или участливое внимание к персоне ребенка может показаться ему выходом из сложной жизненной ситуации, способом быть понятым и приняты. Таким образом, чувства и мысли ребенка отказываются под контролем секты[1].

Такие приемы, как вербовка, психологическое насилие, гипноз, которые увеличивают уровень внушаемости, относятся к незаконным способам. Кандидат юридических наук Е. Петрова утверждает, что данные приемы имеют особый эффект на психику человека за счёт определенных физических или психических воздействий: проповедей, ритуалов, песнопений, телодвижений.

Считается, что к лицам, наиболее подверженным негативному влиянию сект, относятся школьники, студенты выпускных курсов, а также молодые специалисты.

Интернет развивается, а вместе с ним, как было замечено выше, различные способы воздействия на подрастающее поколение. Ничего не предвещающие разговоры с незнакомцами в Сети могут привести к реальным физическим и психологическим увечьям. Возможность анонимной коммуникации увеличивает количество преступлений, связанных с педофилией[2].

Педофилия – это девиация полового влечения, при которой человека сексуально привлекают дети. Педофилами называют людей, страдающих

---

[1] Сатарова Н. И. Информационная безопасность школьников в образовательном учреждении: дис. … канд. пед. наук. СПб., 2003.
[2] Городов О. А. Информация как объект гражданского права // Правоведение. 2011. № 5.

этим расстройством. Можно выделить два основных типа педофилов в сети Интернет:

- педофилы, ищущие встречи;
- педофилы, ищущие контент.

Первый тип педофилов стремится обманным путем склонить ребенка к встрече с последующей интимной связью. Они используют фэйковые аккаунты в соцсетях, сближаются с детьми, притворяясь их друзьями, и предлагают встретиться. Второй тип совершает виртуальные знакомства с детьми для получения фото- или видеоматериалов, чтобы использовать его в собственных целях или для дальнейшего размещения на порнографических сайтах.

Россия занимает второе место после США по распространению в Интернете детской порнографии. Размещение в Интернете фотографий и видео со сценами сексуального характера, в которых участвуют дети и подростки, контролируется законом, ч. 3 ст. 242 УК РФ «Распространение, публичная демонстрация или рекламирование порнографических материалов с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей, включая сеть «Интернет»[1].

Так же распространенная угроза для школьников в Интернете – мошенничество, которое может проявляться различными способами: обманом, хищением средств или личных данных. Мошенником называют лицо, занимающееся подобной деятельностью.

Мошенничество в сети Интернет представлено несколькими разновидностями:

- фишинг;
- вишинг;
- кликфрод;
- скримминг;

[1] URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 19.03.2019).

- шимминг;
- клавиатурный шпион;
- фарминг;
- «нигерийские письма»;
- мошенничества с помощью служб знакомств, секс-услуг, интернет-магазинов, легкого заработка (бинарные опционы, Интернет-казино, лже-коучинг), продаж дипломов, военных билетов и т.п[1].

Стоит обратить внимание на самые распространенные виды мошенничества.

Целью такого вида мошенничества, как фишинг, является получения доступа к конфиденциальным данным человека, таким как пароли. Для этого применяются рассылки электронных писем от известных банков или магазинов, социальных сетей. В данных письмах может содержаться гиперссылка, по которой осуществляется переход на поддельную страницу, где пользователь введет свои настоящие логин и пароль. Таким образом, мошенники получают доступ к аккаунтам, сайтам и счетам людей.

Вишинг – еще один метод обмана в Интернет-пространстве. При данном виде мошенничества конфиденциальная информация выманивается с помощью личного контакта. Мошенник играет определенную роль. Он может быть заинтересованным покупателем, сотрудником банка, юристом с места работы или учебы человека, и, строя диалог определенным образом, старается выяснить реквизиты карты или паспортные данные, или другую важную информацию[2].

Определение деструктивной возможности угроз в сети Интернет есть одна из основных проблем при определении термина «информационная безопасность». П. Корниш, бывший специалист Лондонского Королевского

[1] URL: https://ru.wikipedia.org/wiki/ (дата обращения: 24.01.2019).
[2] Галицкий А. В. Защита информации в сети – анализ технологий и синтез решений. М., 2004.

Института Иностранных Дел, предлагает придерживаться такой классификации угроз[1]:

- незаконная деятельность взломщиков (хакеров);
- преступные группировки, организованно действующие в Сети;
- различные виды экстремизма;
- информационная агрессия на уровне своего государства и на международном уровне.

По словам Д. Белуева и А. Новоселова, «серая зона» выглядит как «черный ящик», на входе в который мы имеем риски весьма низкого уровня, вызываемого новыми субъектами. «На выходе же появляются серьезные угрозы существованию традиционных акторов-государств»[2].

Отталкиваясь от предыдущих слов, заметим, что при раскрытии сути понятия информационной безопасности как в общем, так и в частном смысле, эксперты сталкиваются с вопросом о ее правовом статусе.

В конце 20 века внимание общественности привлекли вопросы о правовой защите несовершеннолетних. Особую значимость к этой проблеме обусловило принятие Конвенции о правах ребенка на сессии Генеральной Ассамблеи ООН в 1989 году. Что касается нашей страны, то в 1990 году она присоединилась к этому международно-правовому акту и приняла на себя обязательство согласовать свое законодательство в соответствии с принципами Конвенции. Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» стал тому подтверждением[3].

Данный Закон является основополагающим по отношению к правам детей, а также определяет цели государства относительно интересов детей. Например, к целям относятся: противодействие дискриминации детей,

---

[1] Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks // Directorate-General for External Policies of the Union/Policy Department. Brussels, 2015.
[2] Балуев Д. Г. «Серые зоны» мировой политики. Очерки текущей политики. М., 2016.
[3] Федеральный закон «Об основных гарантиях прав ребенка в Российской Федерации» от 24.07.1998. г. № 124-ФЗ. URL: http://ivo.garant.ru/#/document/179146:0 (дата обращения: 23.01.2019).

гарантировать нормативных основы прав ребенка, поддерживать духовное, физическое, психическое, нравственное, интеллектуальное их развитие, воспитать в них чувство патриотизма и ответственности человека перед гражданским коллективом, к которому он принадлежит.

Одним из требований относительно прав несовершеннолетних – это право детей на информационную безопасность. Это предполагает государственную и общественную защиту ребенка от информации, которая представляет опасность для его жизни, здоровья и развития. Вплоть до сегодняшнего времени законодательство ускоренно развивалось и продолжает развиваться в информационной сфере. Ключевым является принятый Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[1].

Данным законом закреплены основные понятия, сопутствующие данной сфере, виды информации, причиняющей вред здоровью или развитию детей, а также рядовые требования к информационному продукту. Полномочия федерального органа исполнительной власти и органов государственной власти субъектов РФ, оказывающих влияние на уровень защиты детей от информации, причиняющей им вред, закреплены Законом.

Так же утвержден и вступил в силу приказ Министерства связи и массовых коммуникаций Российской Федерации от 29.08.2012 № 217 «Об утверждении порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей».

В Законе «О защите детей» указаны основные требования к информации, транслируемой по радио и телевидению: запрет на распространение данного вида информации с 4 часов до 23 часов по местному времени, на бранную речь и другую информацию, предусмотренную пунктами 4 и 5 статьи 10 Закона, с 7 часов до 21 часа по

[1] Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010. г. № 436-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 23.01.2019).

местному времени. Единственным исключением являются платные каналы и каналы с ограниченным доступом.

Созданный в РФ фонд «Общественное мнение», базируясь на информации проекта «Интернет в России/Россия в Интернете», констатирует, что Российская Федерация опережает такие европейские страны как Испанию, Францию, Италию, а также Великобританию, Бразилию и Австралию по такому критерию, как количество пользователей Сети. Но все же Россия занимает в мире третье место по этому вопросу. За семь лет с 2002 по 2009 годы число пользователей выросло с 8% (8,7 млн. человек) до 36% (42 млн. человек). Основываясь на этих данных, можно сказать, что третья часть людей, проживающих в РФ, становится пользователем Интернета. Так же был еще такой вывод: каждый седьмой житель посещает Интернет каждый день[1].

В 2000 году в России был создан «Фонд Развития Интернет», который в свою очередь создал информационный портал «Дети России Онлайн», а также линию помощи «Дети Онлайн» с целью защитить подрастающее поколение от опасной информации. По его данным 89% школьников в возрасте от 12 до 17 лет ежедневно выходят в Сеть, 17% тратят на Интернет по 5-8 часов в выходные дни, 56% пользуются Интернетом на мобильных устройствах, 76% уверены, что имеют представление обо всех процессах, происходящих в Сети, 48% испытывают чувство радости при использовании Интернета,43% предпочитают быть другом в виртуальной, а не реальной жизни, 44% не замечают различий между собой в реальном мире и в Интернете, 65% чувствуют себя более независимыми и коммуникабельными[2].

[1] URL: http://www.detionline.com (дата обращения: 12.02.2019).
[2] URL: http://www.detionline.com (дата обращения: 13.02.2019).

Диаграмма 1. Распределение ответов респондентов о том, как они проводят время в Интернете и что при этом испытывают

На основе данных исследований можно выделить основные категории Интернет-угроз:

1. Контентные риски, которые включают у себя материалы с противозаконной, вредоносной и просто неэтической информацией, начиная от эротики и порнографии, заканчивая насилием и суицидом.

2. Коммуникационные риски, которые включают в себя коммуникацию между Интернет-пользователями такую как вредоносные или незаконные контакты (кибербуллинг, склонение к встрече с незнакомцами, овершеринг, секстинг и др.)

3. Потребительские риски, к которым относятся приобретение товара низкого качества, подделок, контрафактной, фальсифицированной продукции и различного рода мошенничества.

На линию помощи «Дети Онлайн» совершались обращения среди пользователей по данным причинам в таком процентном соотношении: 41% – коммуникационные, 12% – контентные, 5% – потребительские[1].

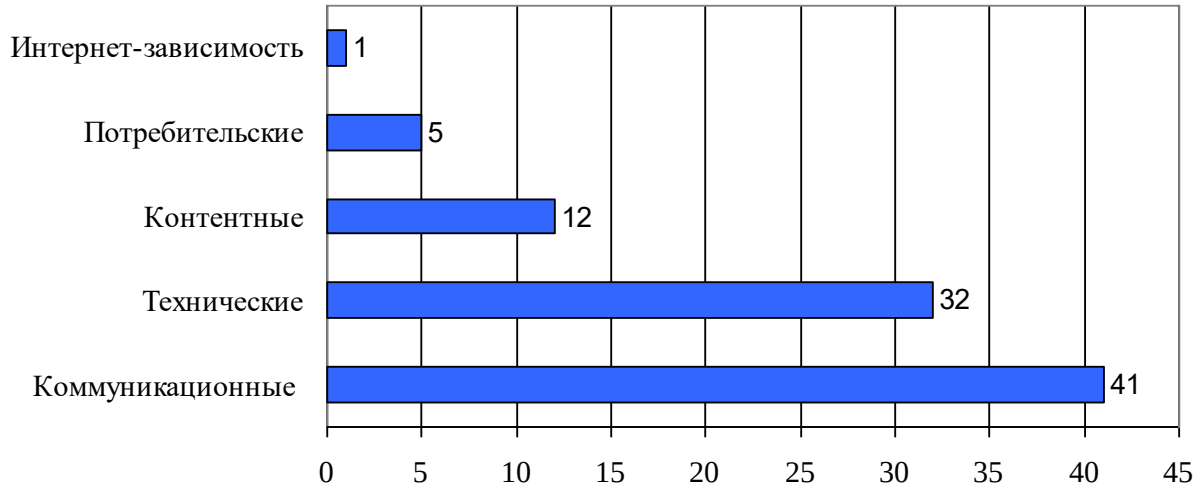

Диаграмма 2. Распределение ответов респондентов на вопрос о том, какие категории Интернет-угроз можно выделить

С вредоносным контентом на сайтах сталкивается каждый второй школьник. По данным фонда 29% сталкиваются с ненавистническим контентом, 28% с сайтами о чрезмерном похудении, 14% со способами причинения себе вреда и боли, 13% с информацией о наркотиках и способах их употребления, 11% со способами совершения самоубийства. В общей сложности 46% сталкивалось с чем-нибудь из перечисленного.

[1] URL: http://www.detionline.com (дата обращения: 12.02.2019).

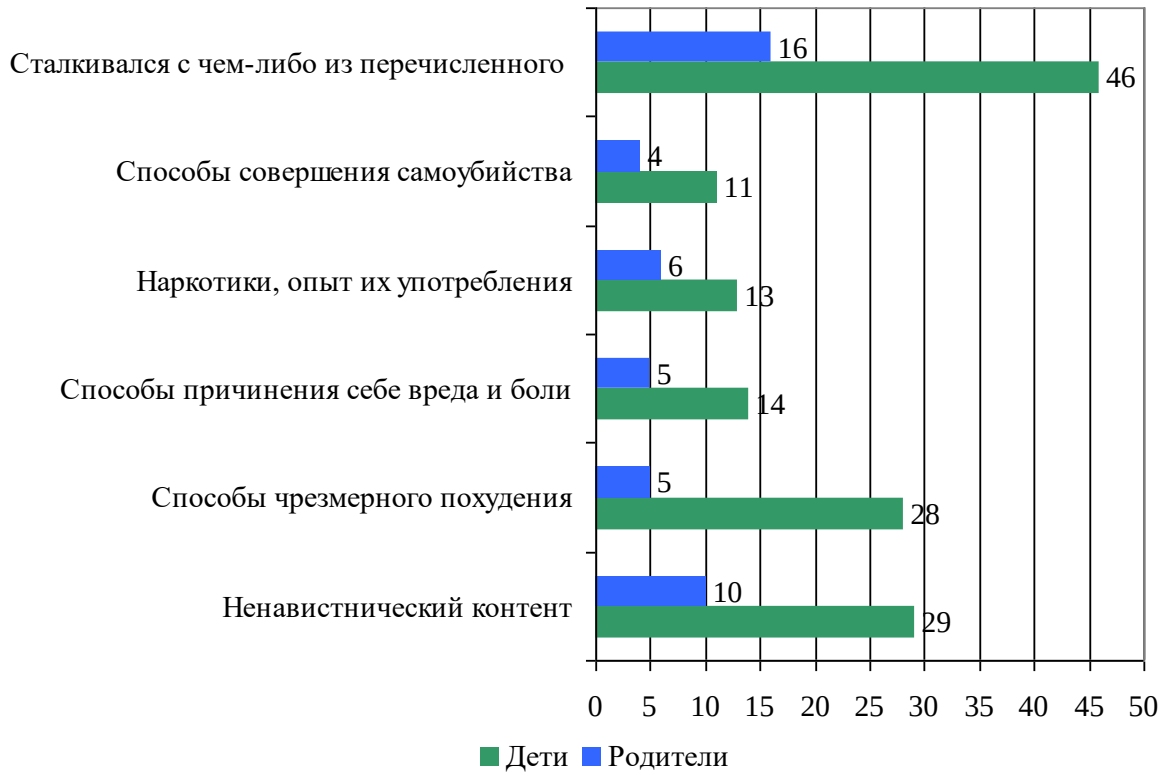

Диаграмма 3. Распределение ответов респондентов на вопрос о том, с каким вредоносным контентом они сталкивались в Интернете

Результаты исследования фонда свидетельствуют о том, что на 2016 год выросло количество профилей с открытым доступом. Оно составляет более 60%, что превышает показатель 2010 года более чем в два раза[1].

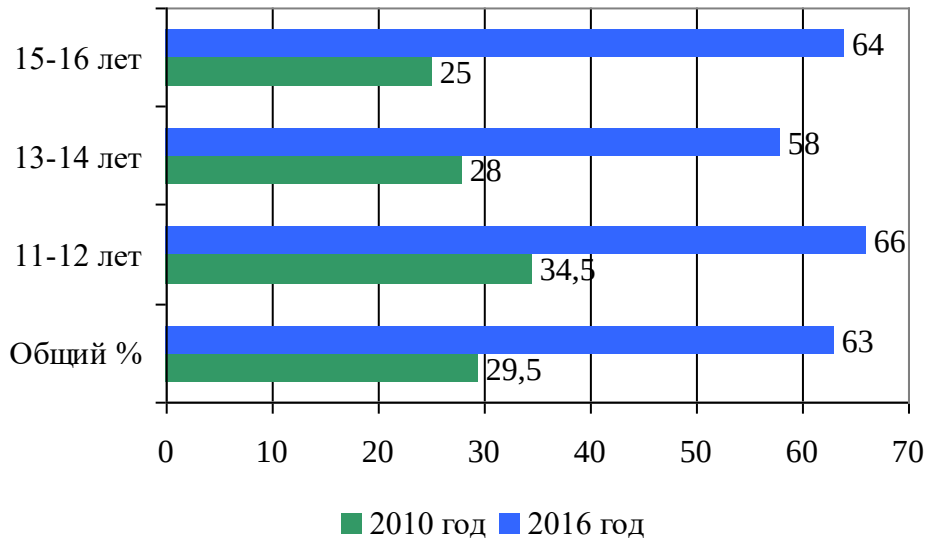

Диаграмма 4. Распределение количества открытых профилей за 2010-2016 года

[1] URL: http://www.detionline.com (дата обращения: 12.02.2019).

Необходимо отметить такое понятие, как «число Данбара», ограничение на количество долговременных отношений, которые поддерживает человек[1]. У взрослого человека оно лежит в диапазоне от 100 до 230, чаще всего считается равным 150. В настоящий момент круг Интернет-друзей 50% подростков 15-16 лет и 43% 13-14 лет составляет более 100 человек, что по числу почти сопоставимо с количеством социальных связей взрослого человека. Примерно 50% подростков имеет виртуальных друзей, с которыми он ни разу не встречался в реальной жизни. Показатели, как часто обращается за помощью или советом школьник к реальному или виртуальному другу, различаются меньше, чем вдвое. Например, делятся своими переживаниями с реальным другом 89%, а с виртуальным 54%, помогают в решении проблем 98% и 77%.

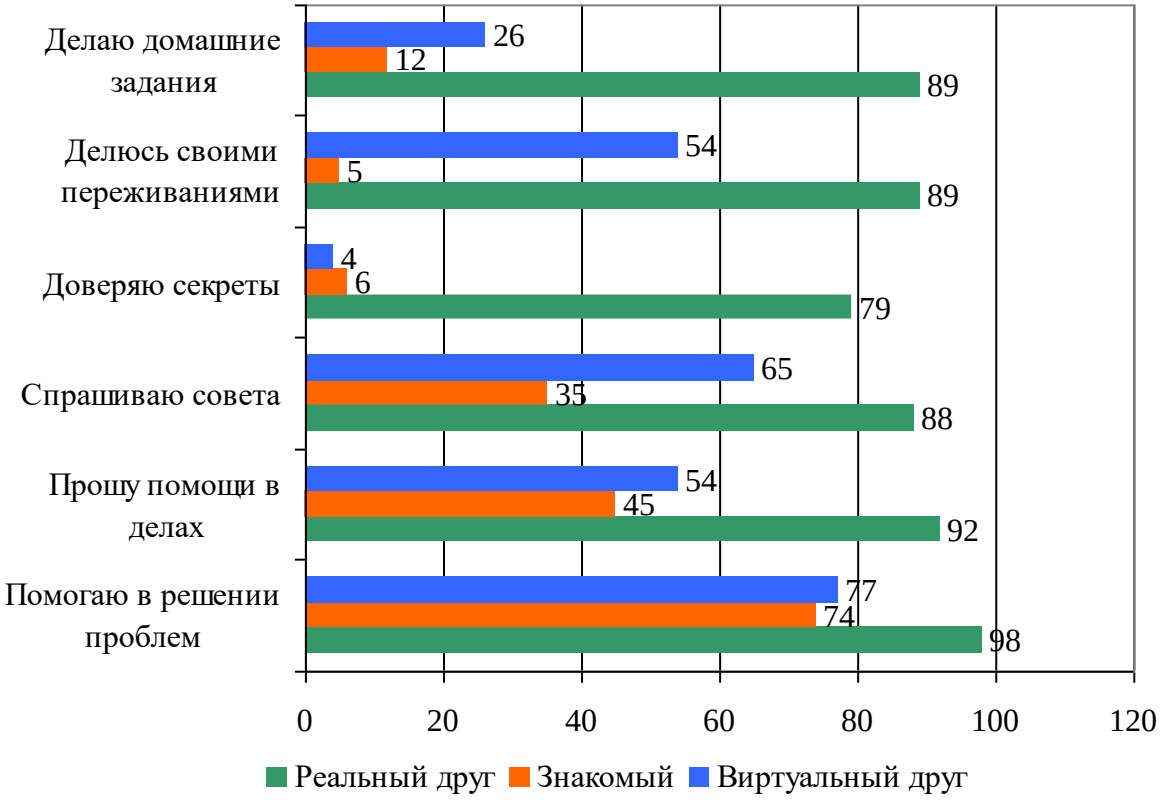

Диаграмма 5. Распределение ответов респондентов об их отношении к реальным и виртуальным друзьям

[1] Самоделова Л. А. Изучение основ информационной безопасности в системе дополнительного образования: автореф. … канд. пед. наук. М., 2005.

Было проведено исследование сотрудниками ФГБУ «Центральный научно-исследовательский институт организации и информатизации здравоохранения» Минздрава России Е. С. Скворцова, Л. К. Постникова среди городских 15-17 летних школьников России в 2010-2011 годах. В выборку вошли: 13 городов (Архангельск, Великий Новгород, Волгоград, Воронеж, Ижевск, Казань, Калининград, Калуга, Кемерово, Красноярск, Москва, Мурманск, Чебоксары), Московская область и Ненецкий автономный округ, представляющие 6 Федеральных округов Российской Федерации. В целом анкетированием было охвачено 16 574 учащихся 9-11 классов, в том числе 54,7% мальчиков и 45,3% девочек[1].

При анализе исследований, проведенным в РФ, заметно бесспорное омоложение людей, использующих Интернет. К примеру, А. Егоров и соавторы приводят данные мониторинга пользователей Сети: количество подростков, пользующихся Интернетом, в процентном соотношении изменилось с 2% на 25% за период с 1992 по 2004 гг. А уже в 2009 году их число достигло 90%. В странах Евросоюза это количество школьников достигает 86%, что практически сопоставимо с Российскими показателями.

Большое внимание в исследовании также было уделено и показателям пользовательской Интернет-активности школьниками: частота и длительность пользования Интернетом, выбор Интернета, как источника информации и др. Уровень распространенности пользования Интернетом среди подростков-школьников 9-11 классов составил в среднем по России 95,0 на 100 мальчиков и 95,4 на 100 девочек. Такие же данные получены и в ранее проведенных исследованиях. Наши данные показали, что 88,9% мальчиков и 89,7% девочек каждый день пользуются Интернетом. Часть из них ежедневно тратит на это по 2 часа (61,8% мальчиков и 59,7% девочек), а некоторые более 5 часов (7,3% мальчиков и 7,4% девочек). Значительно реже

[1] Майорова-Щеглова С. Н. Социологические концепты детства и проблемы информационной безопасности детей // Безопасность детей в информационном пространстве. М., 2014.

(от 2 дней в неделю до 2 часов в месяц) используют Интернет 6,1% мальчиков и 6,6% девочек.

Важные мотивы высокой пользовательской активности российских школьников – средства общения и источник информации. Девочки чаще, чем мальчики используют Интернет для общения с друзьями и заведения новых знакомств (54,9 и 42,9%), поиска нужных материалов для подготовки к школе (17,4% и 14,5%). В то время как мальчики чаще, чем девочки, используют его для поиска информации, касающейся хобби (17,4% и 11,6%), компьютерных игр (12,1% и 4,7%), т.к. нечем больше заняться (6,0% и 4,5%). Что касается покупок в Интернет-магазинах, то 3,7% мальчики и 4,3% девочки одинаково посещают Интернет-сайты.

Более половины школьников (51,6% мальчиков и 55,3% девочек) ничего не пропускают из-за пользования Интернетом. Однако практически одинаковое количество мальчиков и девочек пропускают прогулки с друзьями (22,5% и 22,9%), общение с родителями и праздники (3,8% и 3,8%). Следует отметить, что мальчики (10,5%) чаще, чем девочки (8,3%) пропускают занятия в секциях и кружках; не спят по ночам из-за пользования Интернетом (0,9% и 0,5%), а девочки пропускают прием пищи (0,4% и 0,3% соответственно).

Что касается системы образования, то для управления информационной безопасностью школьников в сети Интернет принимаются различные меры для устранения или профилактики безопасности: программно-технические, административные, организационные. Их основная цель – сформировать информационную культуру и навыки, необходимые для ограничения нежелательной информации за стенами образовательного учреждения[1].

Профессиональная компетентность современных учителей играет здесь важную роль. Чтобы быть осведомленным в вопросах информационной

[1] Бочаров М. И. Комплексное обеспечение информационной безопасности школьников. М., 2009.

безопасности педагог должен осваивать информационные технологии, видеть перспективу их развития, осознавать риски, связанные с нарушением правил информационной безопасности в учебном заведении.

В общеобразовательных организациях активно применяются меры двух видов: административные, организационные. К ним относят:

- назначение ответственного лица за организацию работы с ресурсами Интернета и ограничение доступа;
- создание локального приказа «Об информационной безопасности»;
- утверждение и ознакомления, обучающихся и педагогического коллектива с правилами организации доступа в Интернет ОУ, с информацией, запрещенной законодательством РФ;
- инструктирование штата сотрудников об их действиях во время осуществления контроля использования обучающимися сети Интернет;
- содействие в повышении квалификации сотрудников ОУ по вопросам защиты детей от причиняющей вред их здоровью и развитию информации;
- составление договорных обязательств с провайдером, касающихся предоставления фильтрации информации для трафика учебного заведения;
- проведение регулярного мониторинга использования контентной фильтрации;
- внесение отдельного положения в договор об оказании образовательных услуг, по которому родители берут на себя ответственность за предоставление при посещении учебного заведения своему ребенку личного средства связи, в котором есть выход в Интернет[1].

Помимо вышеперечисленных механизмов управления информационной безопасностью в школе, важной частью являются организационные и административные меры по соблюдению законодательства в области защиты персональных данных. Внутренняя

[1] Коротенков Ю. Г. Информационная образовательная среда основной школы. М., 2011.

политика их обработки должна отвечать требованиям Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», так же к этом относится ограничение доступа к информации, содержащей персональные данные.

В общеобразовательных организациях это осуществляется с помощью:

- создание локальной сети и ограничение доступа в Сеть в зависимости от выполняемой задачи;
- установка систем контентной фильтрации на персональные компьютеры либо сервер;
- настройка и обновление установок контентной фильтрации, блокирующей выход к ресурсам Интернета с причиняющей вред развитию и здоровью детей информацией;
- установка и обновление антивирусного программного обеспечения;
- осуществление педагогическим коллективом визуального контроля работы учеников в Сети;
- отсутствие доступа к Wi-Fi для учеников.

Несмотря на все правила пользования, ответственность за факты доступа со школьных компьютеров или устройств к нежелательной информации, лежит на руководителе образовательной организации[1].

Для сравнения рассмотрим работу над обеспечением информационной безопасности школьников в Сибирском федеральном округе, Алтайском крае. Еще с 2016 года акт приемки общеобразовательных организаций края включает в себя пункт о степени обеспечения информационной безопасности в учреждении, в том числе в обязательном наличии контент-фильтра. Так же КГБУО «краевой информационной-аналитический центр» разработал методические рекомендации, по которым ОУ проводят самообследование на

[1] Левин В. К. Защита информации в информационно-вычислительных системах и сетях // Программирование. 1994. № 5.

наличие комплекса мер, которые защищают детей от информации, причиняющей вред здоровью и развитию детей[1].

В соответствии с этим все учреждения сферы образования установили собственные программно-технические, административные и организационные меры, которые способствуют ограничению доступа школьников к информации, пагубно влияющей на их здоровье и развитие.

Помимо этого, Министерство образования и науки совместно с КГБОУ «краевой информационно-аналитический центр» с декабря 2016 года по январь 2017 года провело мониторинг того, как выполняется комплекс мер по защите школьников от нежелательной информации.

В мониторинге приняли участие 954 общеобразовательные организации и их филиалы (99% от общего числа общеобразовательных организаций). Мониторинг показал, что административные и организационные меры, содействующие ограничению доступа школьников к информации, пагубно влияющей на их физическое и психическое состояния, полностью реализованы 89% общеобразовательных организаций, а технические меры применяются в 97% учреждений.

Выяснилось, что общеобразовательные организации Алтайского края осуществляют фильтрацию опасной информации тремя способами:

- с помощью провайдера;
- с помощью локальных программных пакетов;
- с помощью централизованной фильтрации через ресурсы КГБУО «краевой информационно-аналитический центр».

Вопросы информационной безопасности затрагиваются в школьных учебных пособиях, а также в рамках некоторых предметов, например, информатики и обеспечения безопасности жизнедеятельности. Но при этом затрагиваются только определенные составляющие всей проблемы, а не она целиком. На уроке информатики акцент делается на технические угрозы, на

[1] Моисеев А. М. Проблемы и пути совершенствования внутришкольного управления. Пособие для руководителей образовательных учреждений. Тамбов, 2012.

ОБЖ упоминаются опасности, лишь связанные с Интернетом. Можно сделать вывод, что этого недостаточно. Поэтому очень часто преподавание детям материала по информационной безопасности отводится на часы, предназначенные для внеурочной деятельности и различных воспитательных мероприятий. Чтобы детям было интересно постигать правила надлежащего использования Интернета, их привлекают к участию в конкурсах или онлайн-играм по информационной безопасности[1].

Рассмотрим очередной пример на Алтайском крае. Третий год подряд на базе школ проводится онлайн-квест для школьников «Сетевичок», который посвящен цифровой грамотности. Эта игра национальная и проводится по всей стране. Алтайский край был представлен в Национальном рейтинге школьниками из Барнаула, Бийска, Новоалтайска, Благовещенского и Калманского районов.

Каждый год проходит акция «Единый урок безопасного Интернета» по всей России. Именно в Алтайском районе в 2016 году в ней приняло участие более 150 тысяч человек, к которым относятся и школьники, и педагоги, и родители. В рамках данной акции по школам проводятся классные часы по предложенной теме, игры, конкурсы, беседы с сотрудниками органов и здравоохранения, встречи со специалистами коммерческих компаний и детских библиотек.

На примере Алтайского края можно рассмотреть хороший вариант работы с родительской общественностью. Раз году там проводится мероприятие для родителей, посвященное безопасному использованию Интернета детям и самим родителям. В 2015 году там проводилась родительская академия «Интернет: возможности и опасности. Как защитить семью и ребенка?». В 2016 году это была онлайн-конференция «Информационные угрозы и здоровье детей»[2].

---

[1] Малых Т. А. Проблемы информационной безопасности личности // Актуальные проблемы права, экономики и управления: материалы междунар.науч.-практ. конф. Иркутск, 2007.

[2] URL: http://www.microsoft.com/rus/childsafety (дата обращения: 12.02.2019).

Рассмотрев подобные систему осведомления по всей стране, можно сказать, что в образовательных организациях по всей России проводятся родительские собрания, где обсуждается необходимость ограждать детей от вредоносной информации. Также особое внимание уделяется соблюдению требований Федерального закона от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред здоровью и развитию» в школьных библиотеках-медиатеках[1].

Существует установленный ряд мер, обязательных для исполнения, по обеспечению информационной безопасности обучающихся, который контролируется муниципальными и региональными органами управления в образовательной сфере. Еще контроль осуществляют органы прокуратуры и другие[2].

Помимо стремления государства создать систему, которая оградит детей от ненадлежащей информации, все принимаемые ими меры должны в той или иной мере соответствовать ожиданиям родительской общественности. Родители должны быть уверены, что меры эффективны и ребенку ничего не угрожает.

Проанализировав различные виды документов (нормативные, научно-методические, технологические и иные), мы можем утверждать, что вопросу управления информационной безопасностью школьников уделяется большое внимание со стороны органов власти и образовательных организаций.

Несмотря на неоспоримый вклад государственных органов в данный вид безопасности, этого все равно недостаточно. На данной стадии в развитии глобальных информационных технологий и коммуникаций, учителя и родители сталкиваются со сложностью обеспечения защиты школьников от отрицательных и вредоносных для них данных[3].

---

[1] Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М., 2009.

[2] Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М., 2008.

[3] Рогаткин Д. В. Службы примирения в системе школьного самоуправления // Вестник восстановительной юстиции. 2012. № 4.

Стоит заметить, что на информационную безопасность школьника оказывают влияние два фактора. Первый – это цивилизованные изменения в обществе, которые воздействуют на формирование и развитие личности ребенка. Второй – изменение позиции самой личности человека в общественном сознании, так как теперь личность является центральным объектом в науке, образовании[1].

Исходя из этих исследований, можно заметить, что:

- пользователи Интернета с каждым года становятся все моложе, и их количество увеличивается;
- увеличивается количество Интернет-угроз;
- школьники проводят много времени в Сети, большинство из них лично сталкиваются с Интернет-угрозами.

Основным вопросом остается, кто и как защитит детей от негативного воздействия Интернета. Сегодня список главных навыков 21 века пополняет цифровая компетентность, готовность и способность человека использовать ИКТ уверенно, результативно, критично и безопасно во всевозможных областях жизни на основе усвоения им таких компетенций, как знания, навыки, умения, ответственность и мотивация.

Научить ребенка цифровой компетенции могут родители и учителя. На данный момент разрыв в знаниях, связанных с использованием Интернета, между родителями и детьми больше, чем между учителями и учениками. За последние пять лет доля учителей, использующих Интернет, выросло с 56% до 95%. Учителя обучаются ИКТ-компетенции самостоятельно и на курсах. В школах проводятся различные мероприятия для детей, которые знакомят их с правильным использованием информации из Сети, а также семинары для учителей, посвященные Интернет-безопосности, как с технической, так и с психофизической точки зрения.

[1] Саймон Д. «Как защитить детей от опасностей Интернета». М., 2006.

РАЗДЕЛ II. АНАЛИТИЧЕСКИЙ ОТЧЕТ ПО РЕЗУЛЬТАТАМ ИССЛЕДОВАНИЯ «СОЦИАЛЬНЫЕ МЕХАНИЗМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ШКОЛЬНИКОВ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ»

Для того чтобы выявить основные социальные механизмы управления информационной безопасностью школьников в глобальной сети Интернет, было проведено массовое анкетирование населения среди обучающихся начальных, средних и старших классов, а также родителей школьников города Белгорода.

Для достижения достоверных результатов в исследовании было использовано несколько различных видов исследования: анкетирования школьников и родителей, две фокус-группы с использованием кейсов для учителей, а также экспертные интервью с педагогом-психологом и социальным педагогом (см. Приложение 1).

Были выделены основные проблемные аспекты исследования:

1. Регулярность использования школьником глобальной Сети, а также его цели.
2. Осведомленность школьника о проблеме исследования.
3. Наличие или отсутствие контроля со стороны родителей/учителей.
4. Уровень подверженности рискам ребенка.

Анкета для школьников состояла из 22 вопросов, включая 2 вопроса паспортички, анкета для родителей – из 17 вопросов, включая 3 вопроса паспортички.

Среди школьников в анкетировании приняли участие всего 716 человек.

Для выяснения действенных социальных механизмов управления информационной безопасностью школьников, необходимо было просмотреть несколько критериев общественного мнения населения. Первым исследуемым критерием выступила регулярность использования детьми глобальной сети Интернет, а также время, проводимое ими в Сети.

Для выявления факторов опасности в Сети, которым подвержены школьники, необходимо было узнать о возможности доступа к самой сети Интернет. У 97,9% респондентов домашний компьютер (или ноутбук) подключены к Интернету, у 1,5% не подключен, у 0,6 отсутствует само устройство.

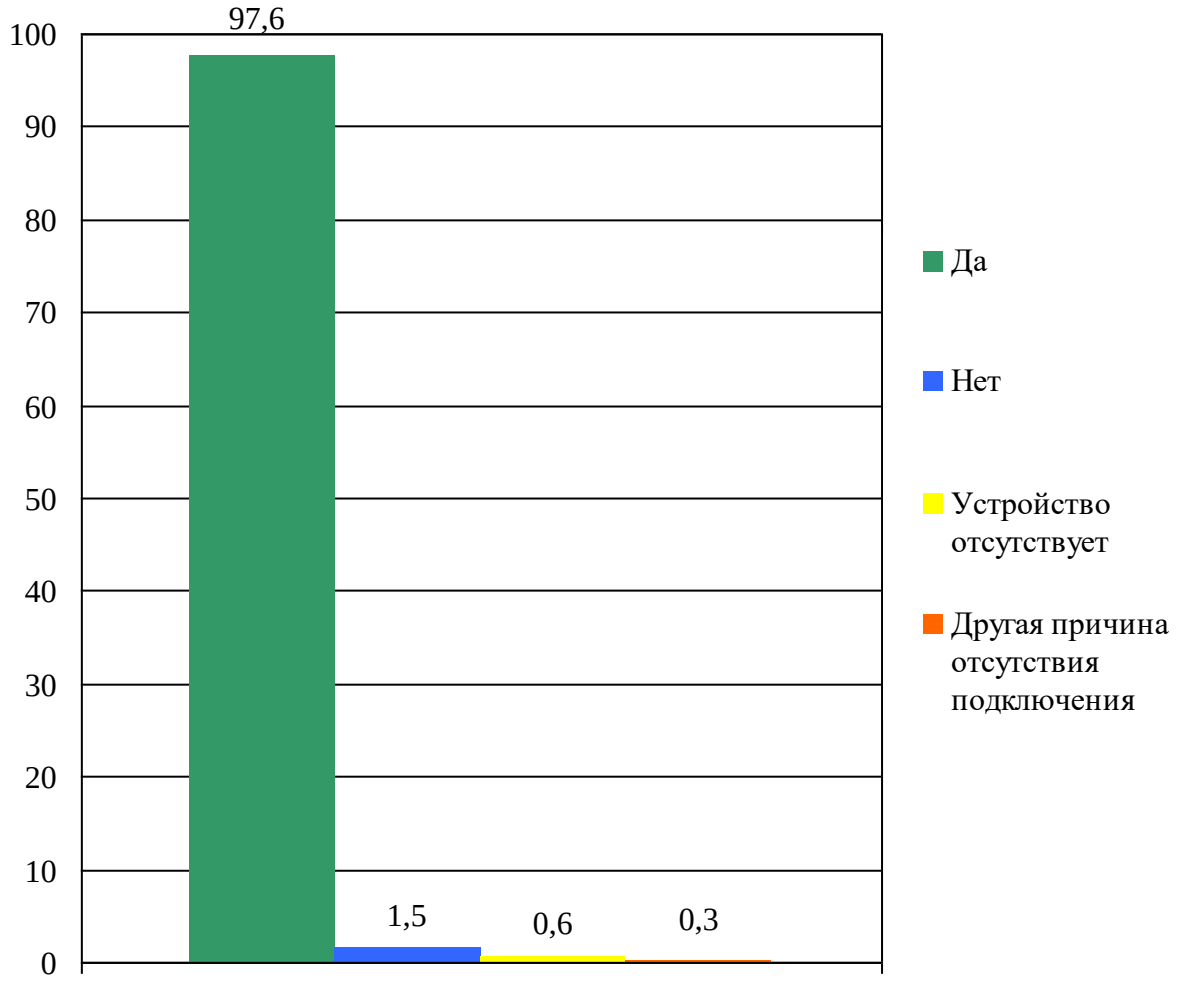

Диаграмма 6. Распределение ответов респондентов на вопрос о том, подключен ли их домашний компьютер (ноутбук) к Интернету

Мобильный телефон подключен к Интернету у 93% опрошенных, не подключен у 5,4%, устройство вообще отсутствует у 0,3%.

Результаты свидетельствуют о возможности ребенка выходить в Интернет как в дома, так и в школе. Основными причинами отсутствия Интернета на компьютере, ноутбуке или телефоне являются: отсутствие данного устройства.

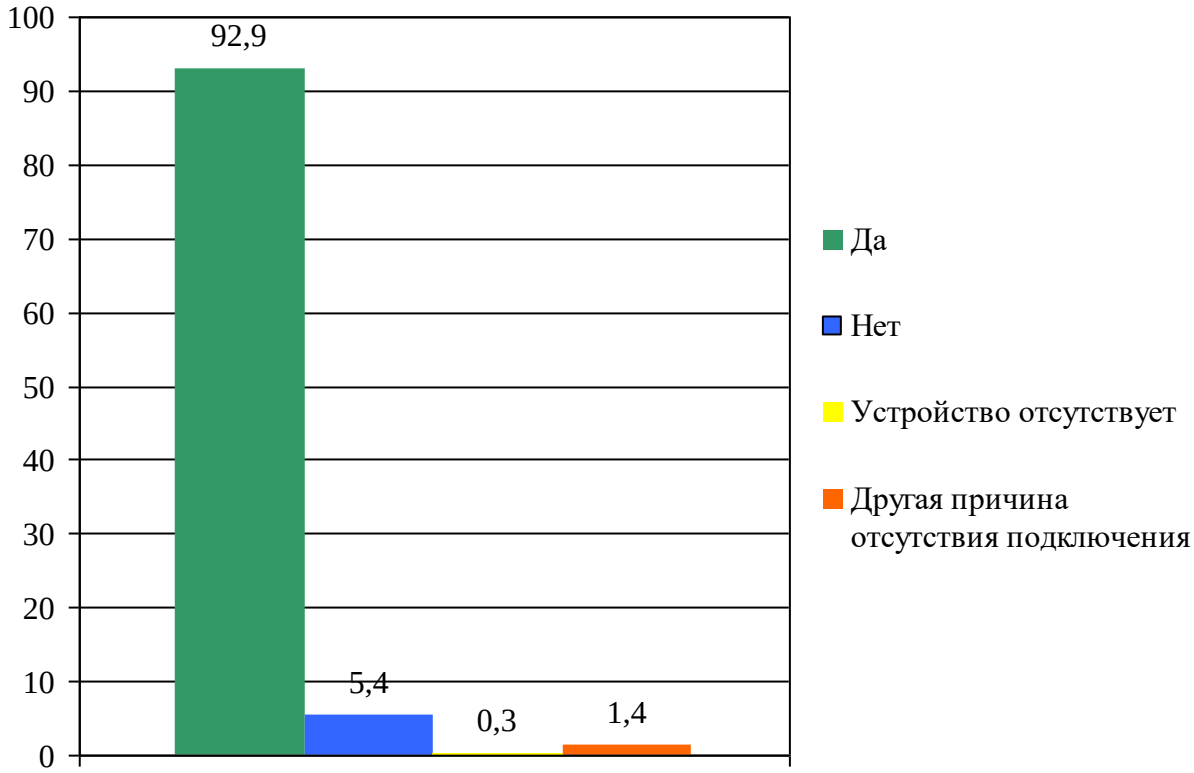

Диаграмма 7. Распределение ответов респондентов на вопрос о том, подключен ли их мобильный телефон к Интернету

Для корректных результатов нашего исследования необходимо было узнать о наличие доступа ребенка к Интернету, так как бывают ситуации, когда Интернет имеется в наличии, но ребенку им не разрешено пользоваться. Доступ к Интернету есть у 94% респондентов.

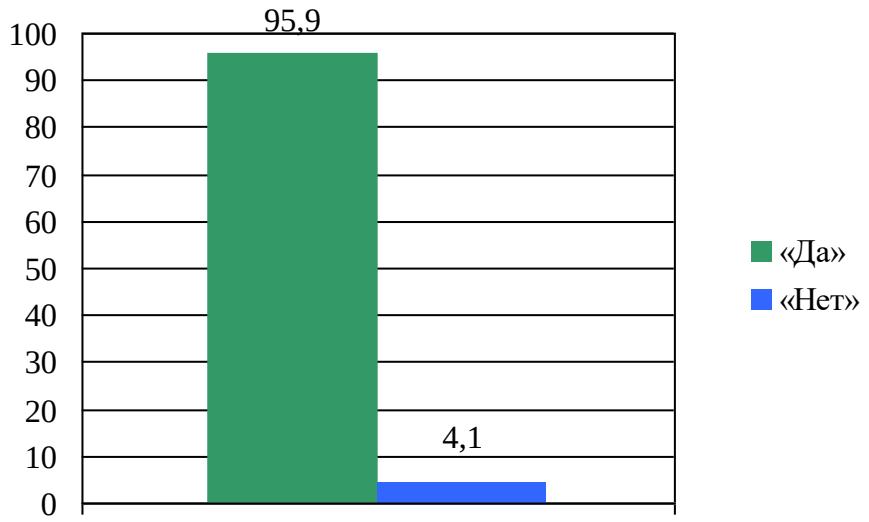

Диаграмма 8. Распределение ответов респондентов на вопрос о том, есть ли доступ у них доступ к Интернету на компьютере или телефоне

Регулярность использования Интернета является еще одним проблемным аспектом исследования. Так же школьник, у которого отсутствует подключение Интернета на компьютере или телефоне, может выходить в него через компьютерный класс или устройства друзей, или одноклассников, к примеру, проверить отметки в виртуальной школе или иной целью. Выяснилось, что 71,1% обучающихся заходит во всемирную паутину более одного раза в день, 24,7% делают это каждый день или почти каждый день, небольшое количество из опрошены, равное 3,8%, утверждают, что используют Интернет один или два раза в неделю, а 0,4% один-два раза в месяц или даже реже.

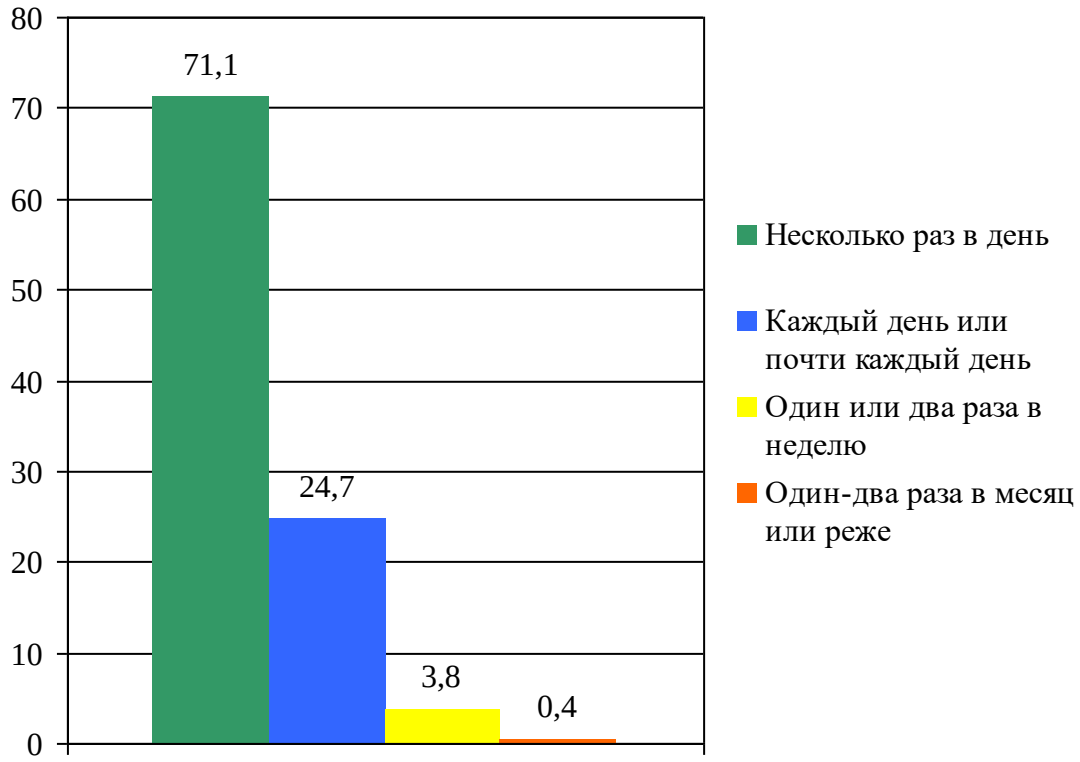

Диаграмма 9. Распределение ответов респондентов на вопрос о том, как часто они используют Интернет

При использовании Интернета в течение одних суток ученики в среднем тратят около 3 часов своего времени. Наибольшее количество времени, проводимого в Интернете, это 5-6 часов, а минимальное количество времени, указанное респондентом, – от 30 минут до 1 часа, в зависимости от четкости поставленной цели для ребенка.

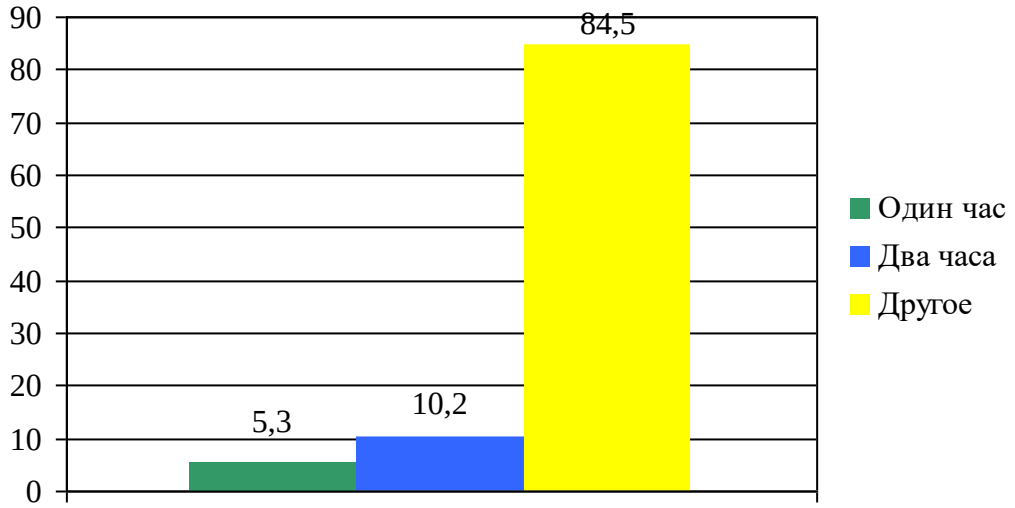

Диаграмма 10. Распределение ответов респондентов на вопрос о том, сколько времени в день они проводят в Интернете

Следующий вопрос давал возможность респондентам выбрать несколько вариантов ответа для выявления цели посещения Сети. Наиболее привлекательными занятиями для детей в Интернет-пространстве являются игры, в них играют 97,1% опрошенных, так же пользуются популярностью социальные сети для общения со сверстниками или друзьями по интересам, ими пользуются 93,9% учеников. Совершают покупки в Интернет-магазинах 47,6% школьников, крупнейший сайт для просмотра видео посещают 79,7%, сайты образовательной тематики просматривают 44,8%. Наименьшей популярностью пользуются сайты узкой направленности. При ответе на данный вопрос разрешалось выбрать несколько вариантов ответа.

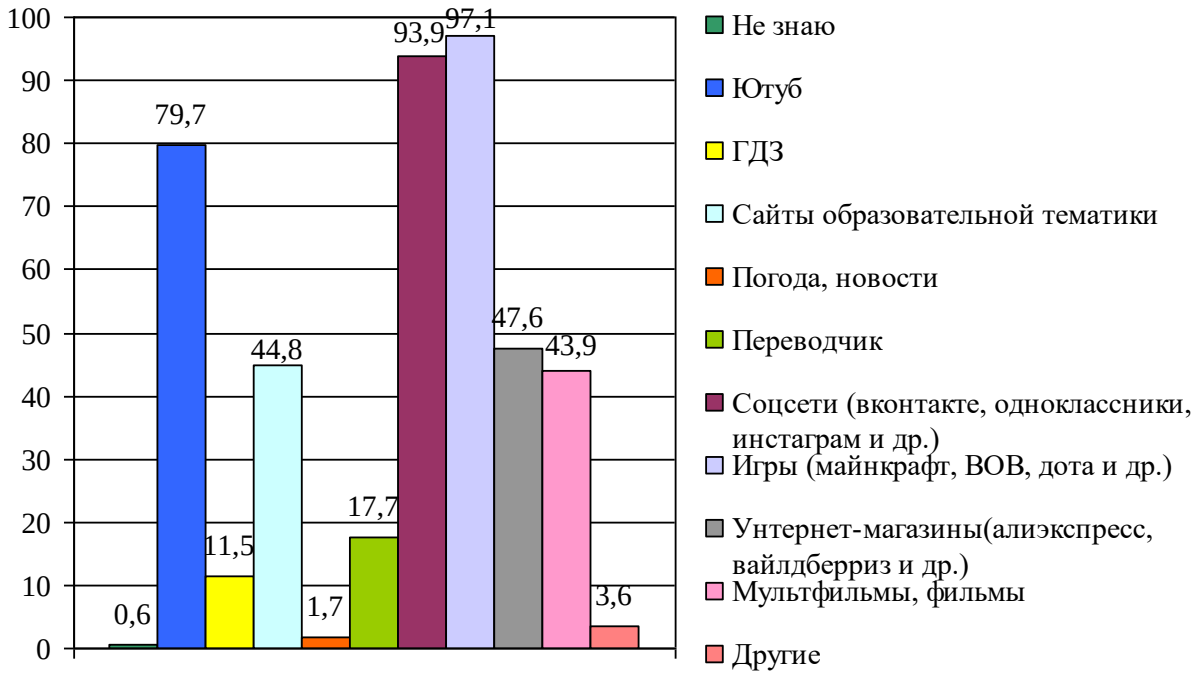

Диаграмма 11. Распределение ответов респондентов на вопрос о том, какие сайты посещают чаще всего

Далее мы исследовали наличие или отсутствие контроля со стороны родителей.

При достаточно большом нахождении детей в виртуальном мире наблюдается так же минимальная заинтересованность родителей в контроле данного процесса. У 89% школьников родители не следят за тем, чем занимается ребенок, сидя за компьютером, у 11% – редко, у 37% – никогда.

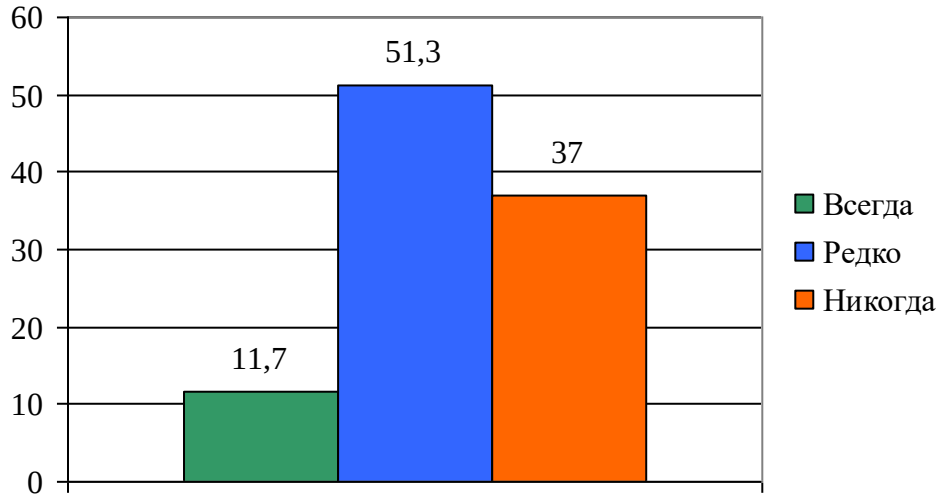

Диаграмма 12. Распределение ответов респондентов на вопрос о том, как часто родители следят за тем, чем они занимаются, сидя за компьютером

Помимо явного контроля, мы узнали некоторые косвенные методы со стороны родителей наблюдения за деятельностью ребенка в Сети: посещают ли они их страницы в социальных сетях и знают ли виртуальных «друзей» своего ребенка.

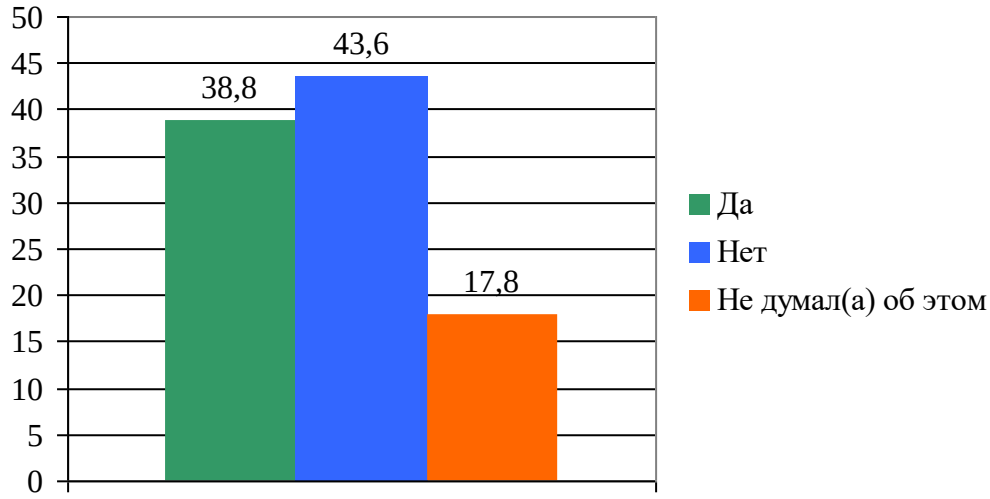

Диаграмма 13. Распределение ответов респондентов на вопрос о том, посещают ли родители их страницы в соцсетях

Среди опрошенных школьников у 38,8% родители посещают их существующую страницу в соцсетях, при этом 22,6% родителей знают виртуальных «друзей» своего ребенка. 43,6% родителей, по мнению школьников, не посещают их странички в Сети, а оставшиеся 17,8% даже не задумывались об этом.

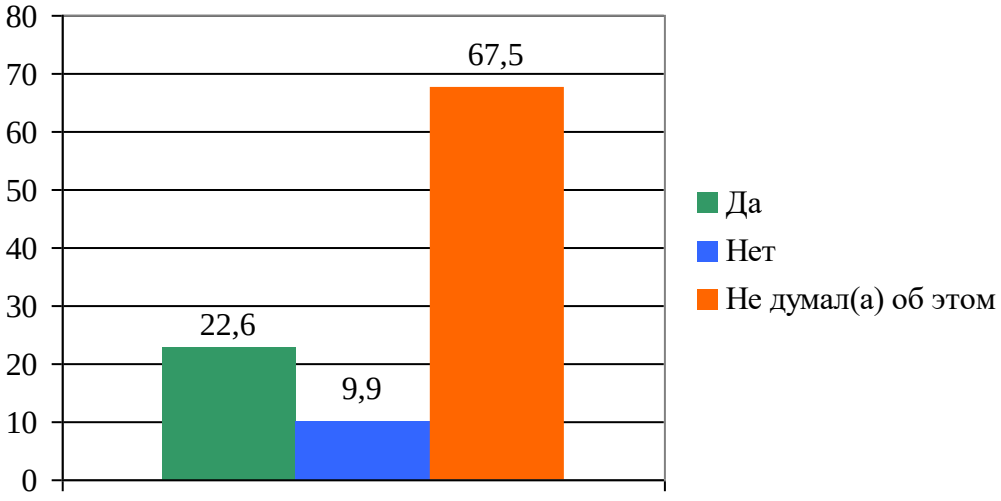

Диаграмма 14. Распределение ответов респондентов на вопрос о том, знают ли родители, с кем они «дружат» в соцсетях

Так же мы выяснили некоторые показатели стремления школьников скрыть свою деятельность в Интернете. У 8,3 % школьников существует страница под другим именем, о которой родители не знают, у 39,5% такой нет, 52,2% утверждают, что о таком не задумывались.

Среди школьников 28% не говорят родителям, сколько они на самом деле проводят времени в Интернете, 15% не задумывались над данным вопросом, остальные говорят, что не скрывают.

Из опрошенных 1% сталкивались с настораживающей информацией на страницах своих «друзей». Их встревожили люди, которые находятся в «друзьях» у человека, паблики, на которые подписан человек, посты, которые публикует.

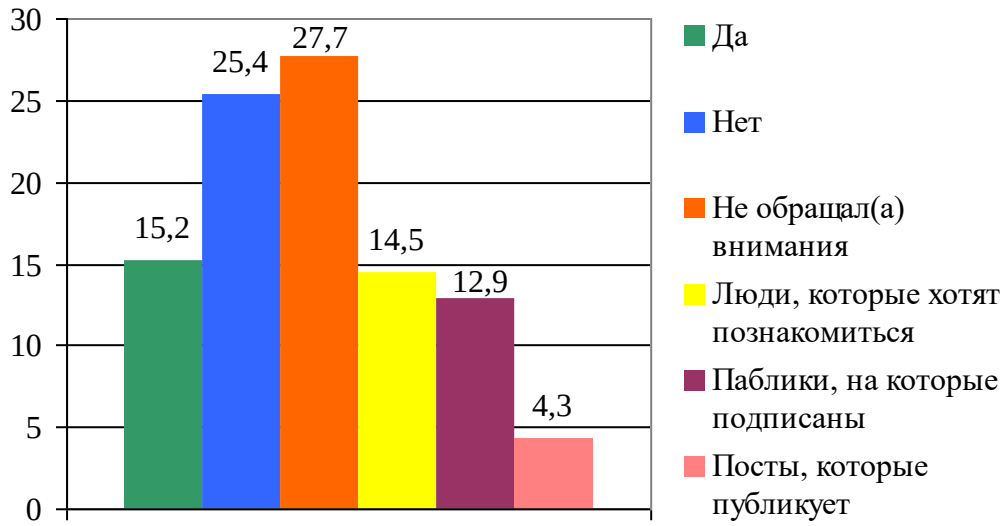

Диаграмма 15. Распределение ответов респондентов о наличии настораживающей информации на страницах друзей

Следующим вопросом мы узнали, насколько школьники осведомлены о проблеме исследования.

Вопрос о том, о каких понятиях Интернет-угроз вы слышали, был задан в зависимости от возраста респондента. В старших классах был дан полный перечень угроз и школьникам предлагалось выбрать известные, в средней и младше школе было дано несколько вариантов ответов и предлагалось так же написать самостоятельно то, о чем ребенок знает или слышал. Большинству школьников известно о таких существующих угрозах, как кибербуллинг

(51,5%), наркотики (73,6%), секты (44%), мошенничество (86,2%), вписки (35,1%).

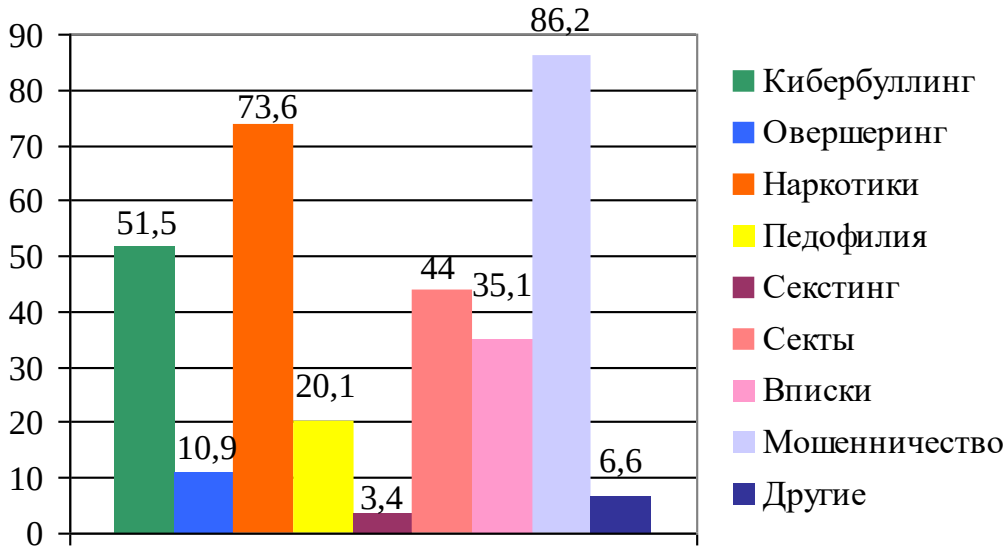

Диаграмма 16. Распределение ответов респондентов на вопрос о том, какие виды Интернет-угроз им знакомы

Так же в анкете была представлены, позволяющие проверить уровень подверженности рискам ребенка

Для поиска наличия конкретных рисков, которым могли подвергнуться школьники, им были заданы вопросы, связанные с кибербуллингом, запрещенной информацией, личными данными, незнакомцами в Сети.

Сам по себе буллинг, без использования сети Интернет, знаком многим детям и родителям вне зависимости от возраста, пола. Среди опрошенных школьников 12 школьников (1,4%) признались, что были жертвой травли, 17 учеников (1,9%) ответили, что один из их друзей был жертвой травли, 9 человек (1%) утверждают, что были случаи среди детей школы, 2 человека (0,2%) выбрали вариант, что они участвовали в травле другого человека, остальные респонденты выбрали варианты «таких случаев не было» или «не знаю».

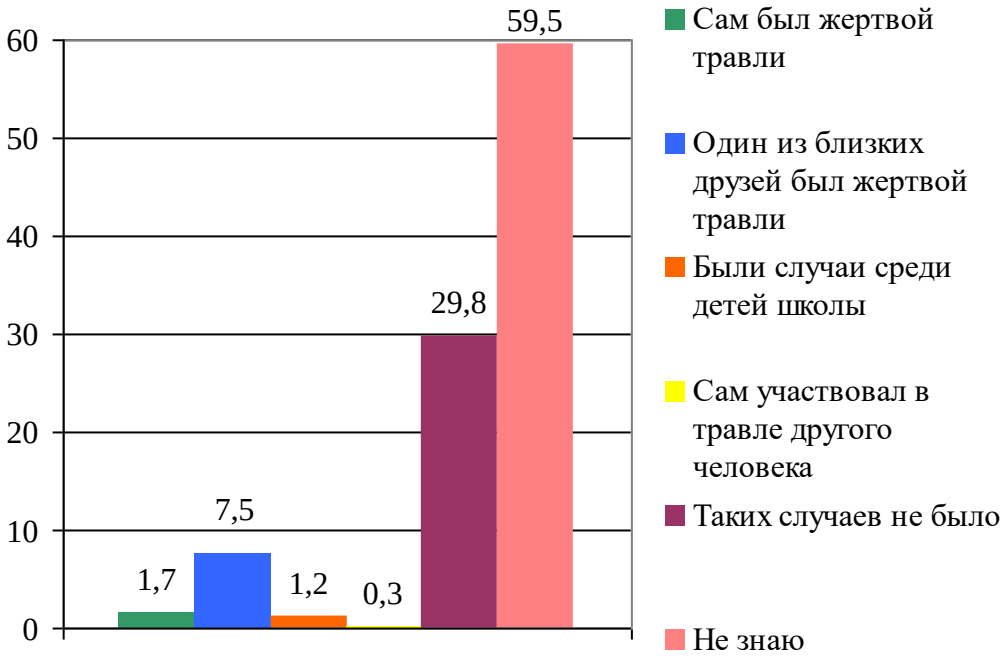

Диаграмма 17. Распределение ответов респондентов на вопрос о том, сталкивались ли они с травлей в Интернете

Среди школьников 55,2% часто пренебрегают запретом на прочтение/просмотр информации, которая им запрещена (ограничение по возрасту), 7,8% делают это всегда, 32,3% иногда. Всего лишь 4,7% опрошенных утверждают, что прислушиваются к предостерегающим подсказкам.

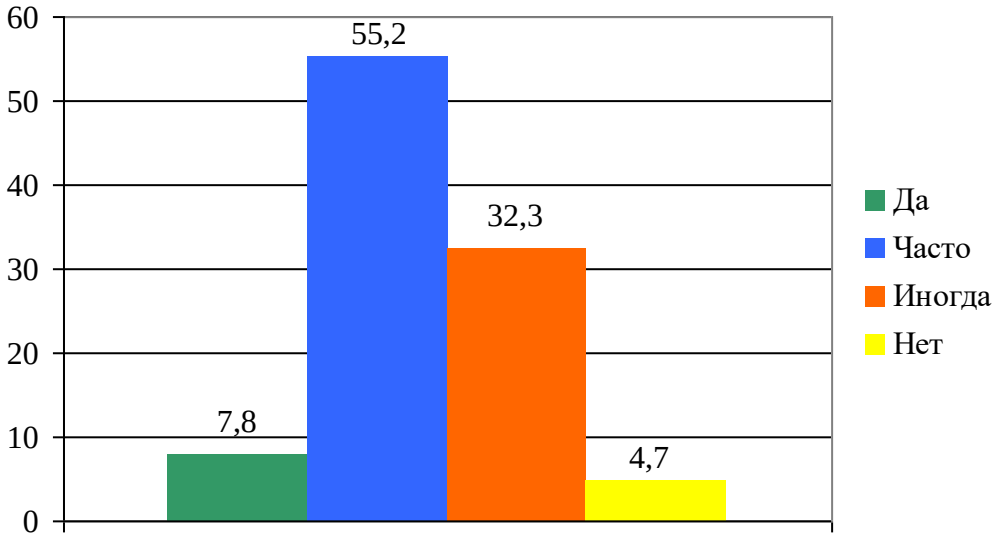

Диаграмма 18. Распределение ответов респондентов на вопрос о том, пренебрегают ли они возрастным ограничением в Сети

Так же 40,6% частично сообщали своим виртуальным друзьям, с которыми не знакомы в реальной жизни, личную информацию о себе, 5,9% почти всю, остальные не сообщали.

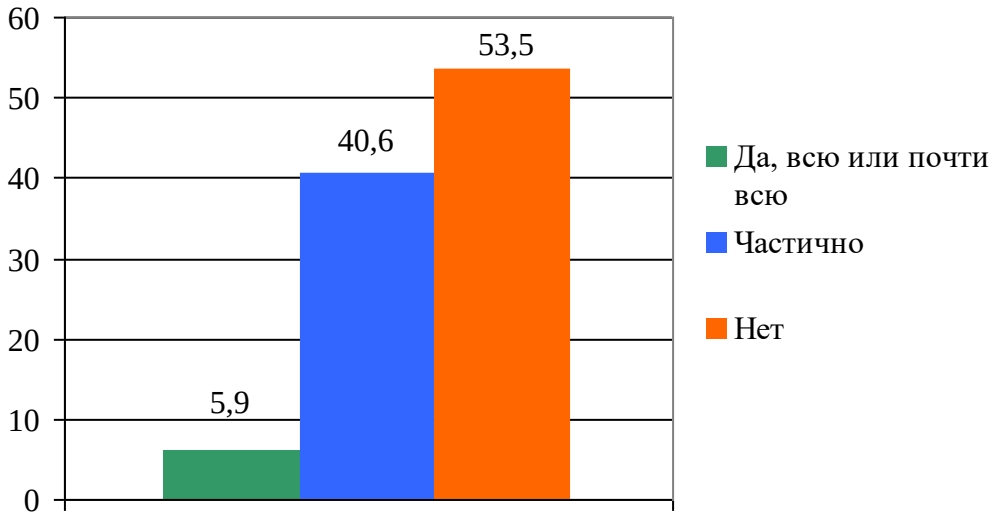

Диаграмма 19. Распределение ответов респондентов на вопрос о том, сообщают ли они личную информацию виртуальным друзьям

Помимо этого, 12,2% встречались лично с людьми, с которыми познакомились в Интернете, 26,8% встречались только с теми людьми, кто вызывал доверие, остальные не встречались.

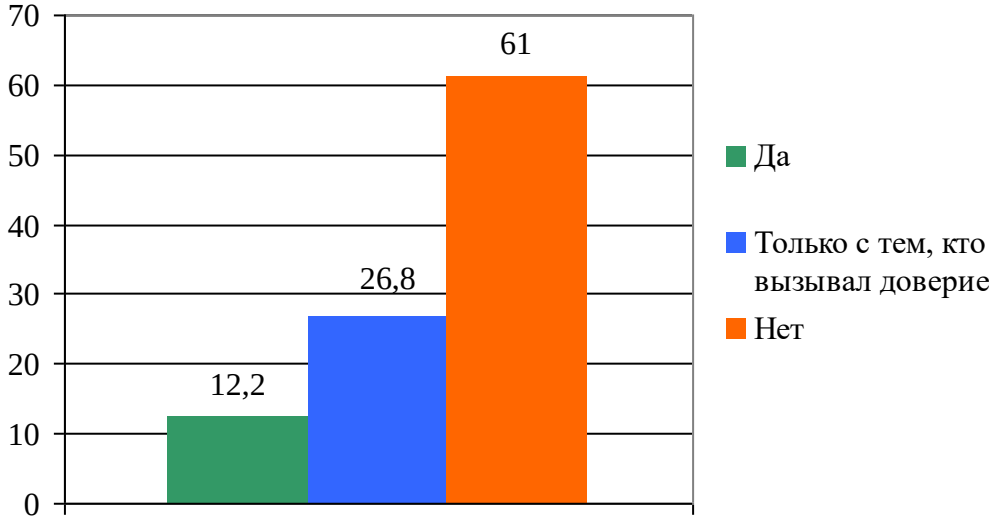

Диаграмма 20. Распределение ответов респондентов на вопрос о том, встречались ли они с людьми, с которыми познакомились через Интернет

Чтобы проанализировать причины полученных процентных показателей, необходимо исследовать, то, как происходит донесение до детей

информации о возможной опасности. О том, как безопасно пользоваться Интернетом, 36,9% учеников объясняли родители.

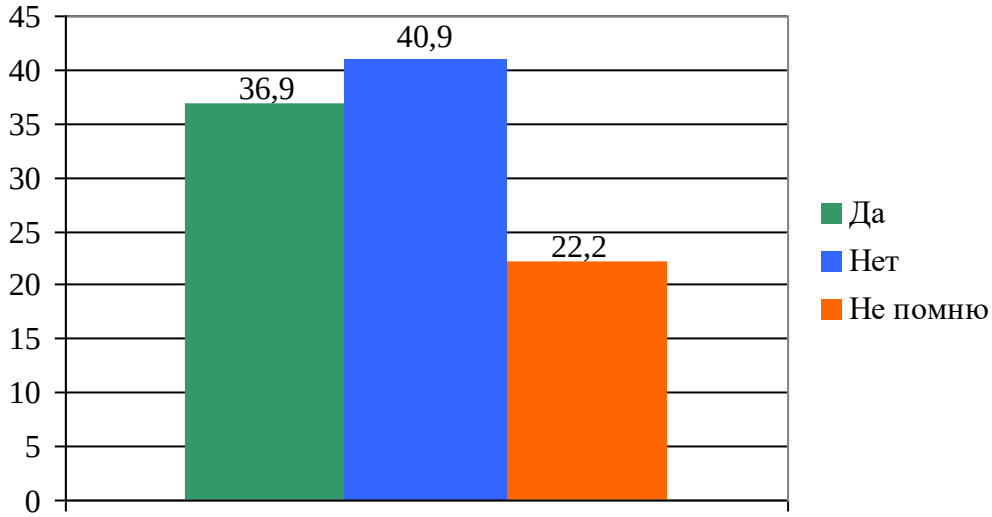

Диаграмма 21. Распределение ответов респондентов на вопрос о наличии бесед по безопасному использованию Интернета со стороны родителей

Подобного рода сведения 80,9% респондентов получали в школе от учителей или классных руководителей.

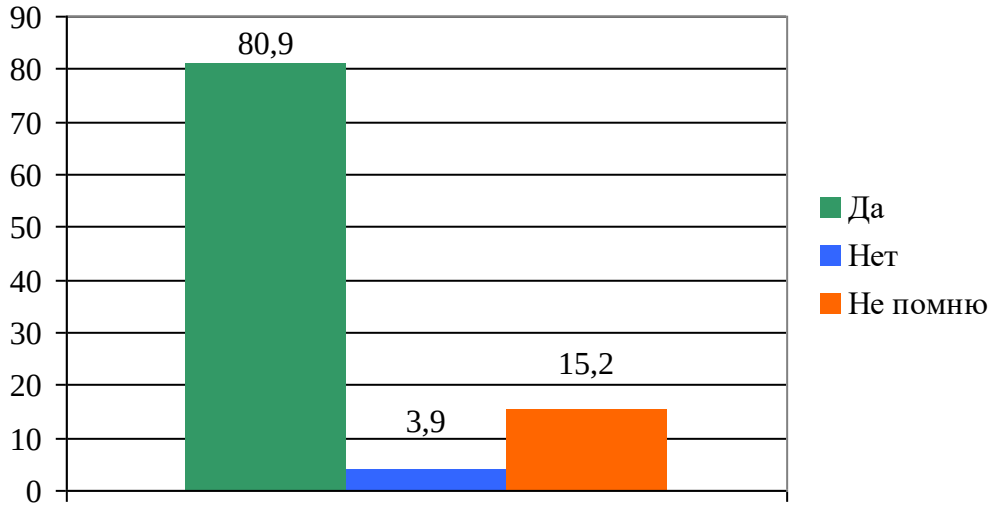

Диаграмма 22. Распределение ответов респондентов на вопрос о наличии бесед по безопасному использованию Интернета со стороны учителей

Помимо основных аспектов в нашем исследовании мы узнали о технической оснащенности домашних компьютеров детей. Необходимости подобного вопроса касаемо школ нет, так как все школьные компьютеры оборудованы фильтрами. 20,1% школьников ответили, что на домашнем

компьютере у них имеется фильтр, 27,7% высказали обратное, 52,2% не знают о наличии или отсутствии подобных программ дома.

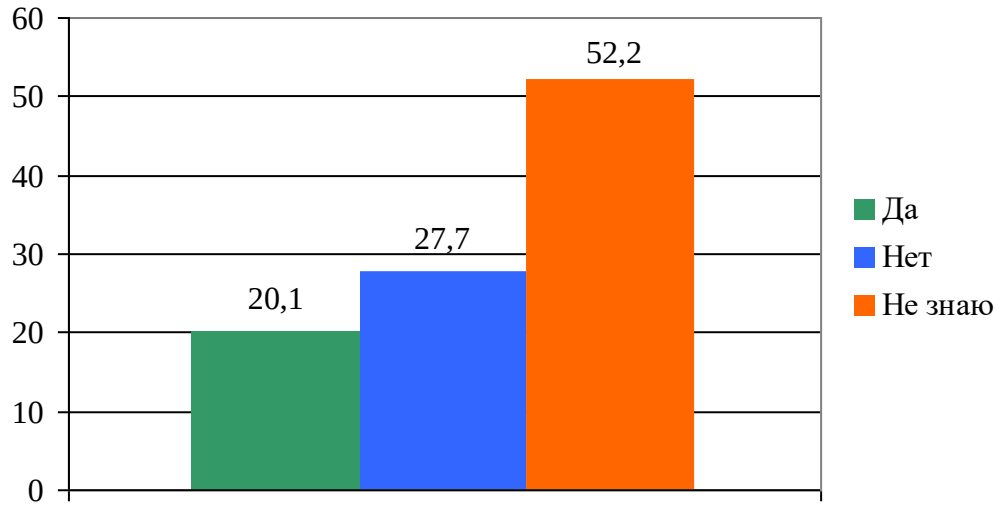

Диаграмма 23. Распределение ответов респондентов о наличии фильтров дома

В анкетировании приняли участие 51,5% женщин и 48,5% мужчин.

Респонденты в возрасте 9-10 лет составили 30,7%; 11-15 лет – 39,7%; 16-18 лет – 29,6%.

Аналогичное анкетирование было проведено среди родителей школьников. Всего в опросе приняло участие 402 человека.

В анкетировании родителей школьников были затронуты схожие проблемные аспекты.

У всех опрошенных респондентов оказался дома компьютер или ноутбук с подключенным к нему Интернетом (100%). О подключении мобильного телефона своего ребенка к Интернету говорят 98% опрошенных, об отсутствии подключения 2%. 91,3% родителей подтверждают факт, что у их детей есть свободный доступ к сети Интернет, 8,7%, что его нет.

Среди опрошенных 74,9% утверждают, что их ребенок использует Интернет несколько раз в день, 20,6% родителей – каждый или почти каждый день, 4% родителей – один или два раза в неделю.

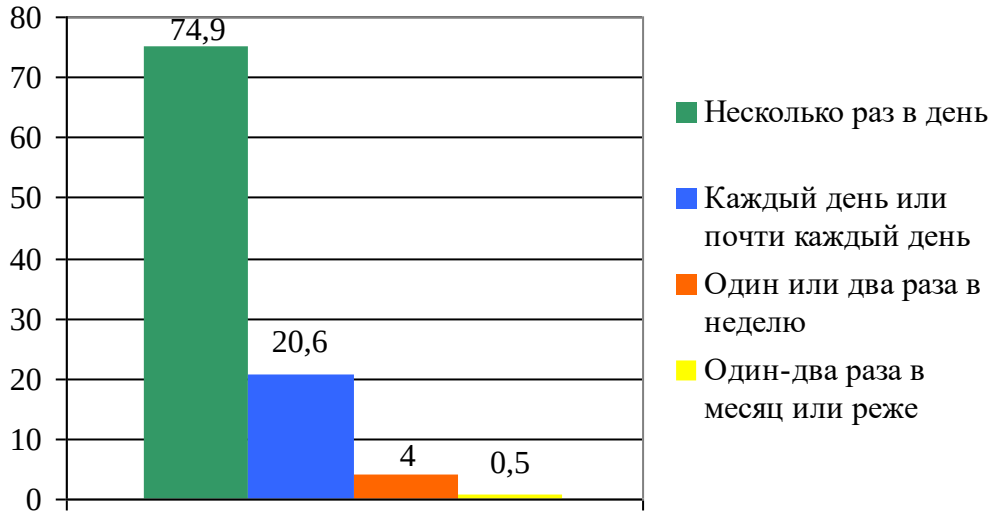

Диаграмма 24. Распределение ответов респондентов на вопрос о регулярности использования Интернета их детьми

При этом дети проводят в Интернете или за компьютером в среднем 2 часа.

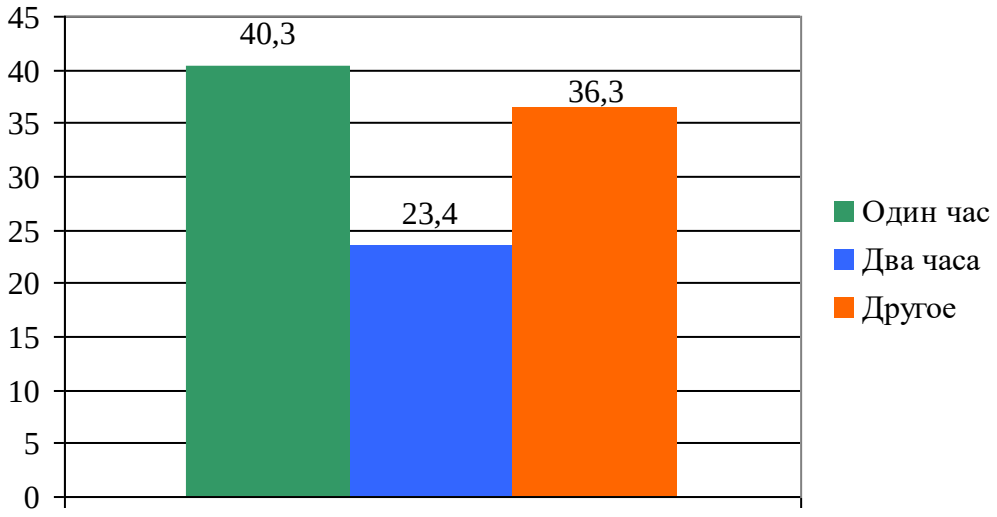

Диаграмма 25. Распределение ответов респондентов на вопрос о количестве времени, которое проводит их ребенок в Интернете

Среди наиболее посещаемых детьми сайтов, по мнению родителей, можно выделить: соцсети (считают 96,8%), игры (считают 93,3%), Интернет-магазины (считают 36,1%), ГДЗ (считают 29,9%), переводчик (считают 26,1%).

В то время, пока ребенок использует Интернет, родители следят за этим в следующем соотношении: 14,9% всегда, 47% редко, 38,1% никогда.

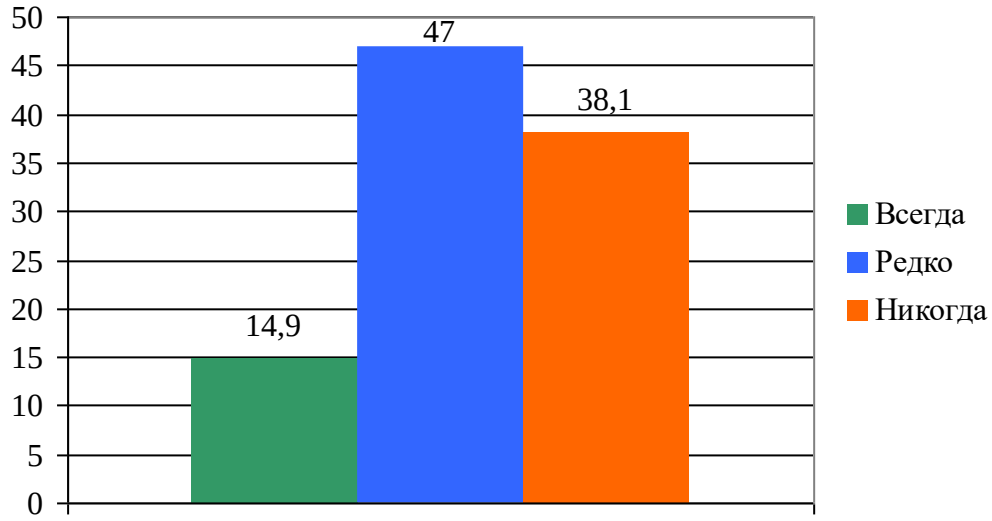

Диаграмма 26. Распределение ответов респондентов на вопрос о частоте наблюдения за тем, чем занимается их ребенок за компьютером

Заходят на страницы детей в социальных сетях всего 74,9% из опрошенных (301 родитель). 52,2% (210 человек) их них знают, с кем «дружит» в соцсетях их ребенок. 4,7% (19 респондентов) встречали что-то настораживающее на социальной странице своего ребенка.

Анкетирование показало, что родители хорошо осведомлены только о некоторых видах Интернет-угроз, которые в основном являются известными им аналогами опасностей в реальной жизни.

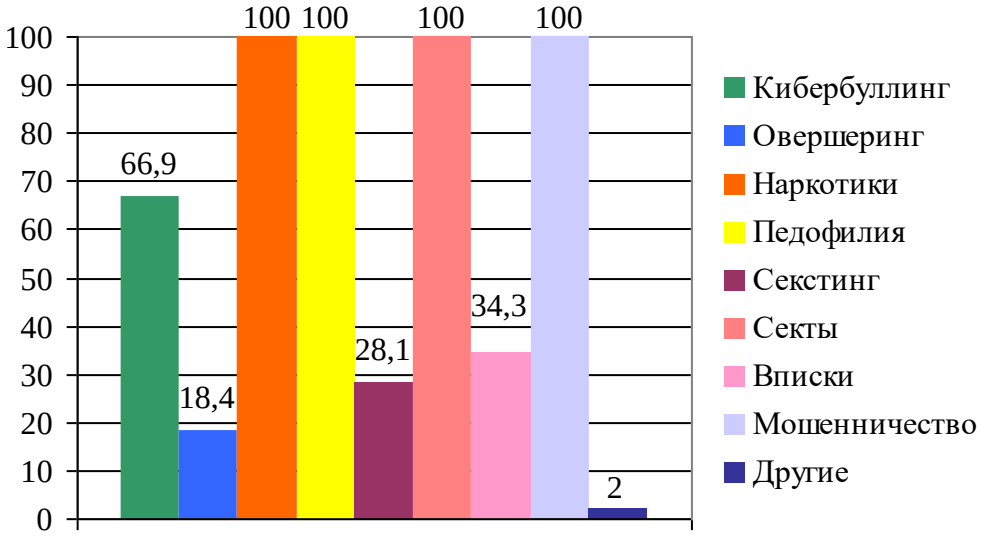

Диаграмма 27. Распределение ответов респондентов на вопрос о существовании различных видов угроз в Сети

К данным угрозам относятся: наркотики – 100%, педофилия – 100%, секты – 100%, мошенничество – 100%. Осведомленность о других видах угроз составила: кибербуллинг – 66,9%, вписки – 34,3%, секстинг – 28,1%, овершеринг – 18,4%, другие – 2%.

Только 2,1% с уверенность сказали, что их ребенок был жертвой травли в Интернете. Так же небольшая часть респондентов, а именно 2,2% говорят, что были случаи среди детей школы. Один из близких друзей ребенка был жертвой травли по мнению 6,7% родителей. Так же 1,2% опрошенных родителей взяли на себя ответственность, указав, что именно их ребенок участвовал в чьей-то травле. Остальные же респонденты выбрали такие варианты ответов, как «таких случаев не было» или «не знаю».

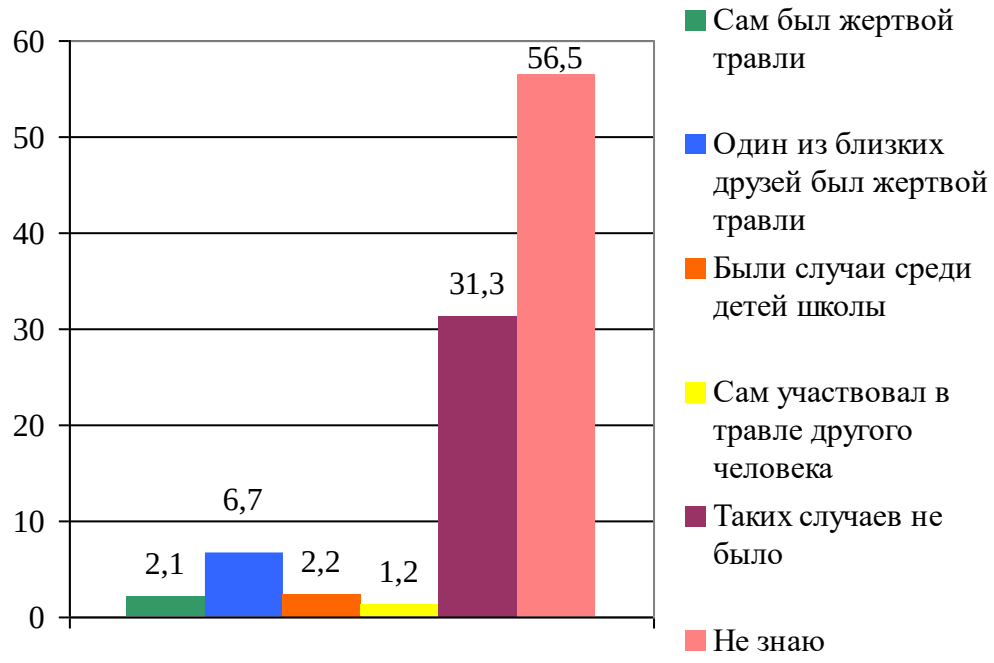

Диаграмма 28. Распределение ответов респондентов на вопрос о том, сталкивался ли их ребенок с кибербуллингом

Подготавливают своего ребенка к правильному и безопасному использованию Интернета 46% опрошенных, остальные либо не делают этого (30,1%), либо конкретно не задумывались о необходимости этого (23,9%).

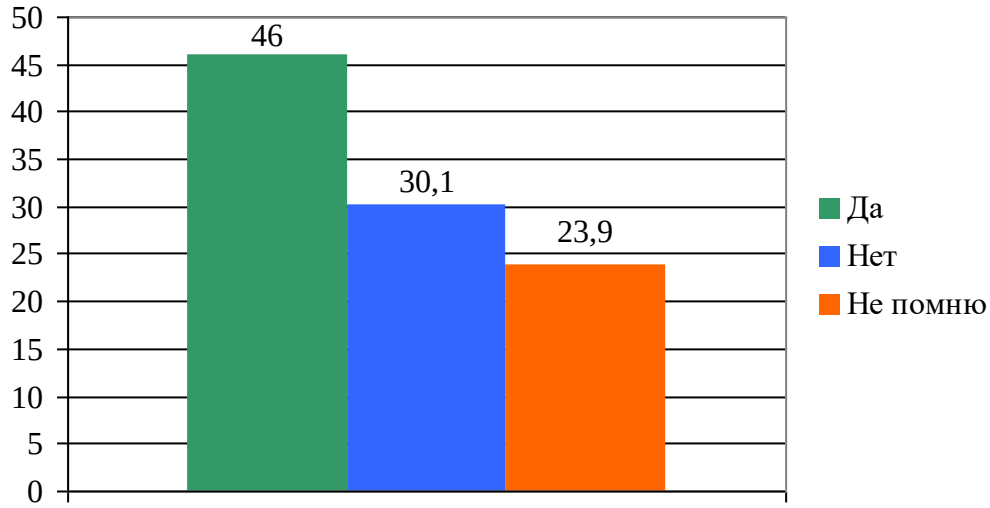

Диаграмма 29. Распределение ответов респондентов на вопрос о проведении бесед с ребенком на тему безопасного использования Интернета

У 33,6 %, а это у 135 человек, дома стоит фильтр от посещения нежелательных и опасных сайтов.

Из них 154 человек мужского пола, 248 – женского. 23,9% (96 человек) в возрасте от 20 до 30 лет, 28,4% (114 человека) – от 31 до 40, 39,1% (157 человек) – от 41 до 50, 8,7% (35 человек) – от 51 и старше. 33,3% (134 человека) имеют высшее образование, 44,5% (179 человека) – среднее профессиональное образование, 22,1% (89 человек) – основное общее образование.

Так же распределение ответов на вопросы анкет представлено в Приложении 7.

Теперь перейдем к анализу результатов, полученных в ходе проведения двух фокус-групп с использованием кейсов.

Фокус-группы по теме «Социологический анализ информационной безопасности школьников в глобальной сети Интернет» были проведены с учителями, которые так же являются классными руководителями.

Всего было проведено 2 групповые дискуссии, длительность которых составила 46 и 57 минут. Групповые дискуссии проводились по заранее разработанному сценарию – гайду (см. Приложение 3).

Количество участников первой и второй дискуссий с классными руководителями составило 8 и 9 человек соответственно.

Перед началом дискуссии участникам был задан вопрос о том, как они понимают понятия «Интернет-угроза» и «Интернет-безопасность». Все ответы оказались верными. Респондентам был задан вопрос: «Насколько сильно влияет активное использование Интернета школьниками на их жизнь, учебу, поведение, на ваш взгляд?» Учителя отметили, что, чем чаще ребенок использует возможности Интернета, тем по нему заметнее. Причем они отмечают, что «всегда по-разному влияет». Так как в некоторых случаях школьник использует возможности всемирной паутины для учебы или нахождения полезной и актуальной информации, а в других просто «тратит своё драгоценное время! На игры, например», а «некоторые даже умудряются играть в онлайн-казино, не осознавая всех последствий».

Хорошим показателем является то, что сами учителя осведомлены почти обо всех опасностях, подстерегающих детей в Интернете.

«Каждый месяц на базе партии Единая Россия проводятся видео-селекторы, посвященные Интернет-безопасности. Нас знакомят со статистикой в других городах по данному вопросу» (реплика участника С., дискуссия от 21 февраля).

«Верно. Например, что 70% школьников получают в социальных сетях приглашения дружить от незнакомых людей. А 18% школьников получают приглашения от незнакомых взрослых. А возрасте 10-12 лет количество таких детей возрастает! Вот какие мы продвинутые!» (реплика участника И., дискуссия от 21 февраля).

«Мы сами часто проводим классные часы или беседы, посвященные этой проблеме» (реплика участника М., дискуссия от 21 февраля).

Видно, что учителя деликатно подходят к вопросам детской безопасности. Помимо общего обзора Интернет-угроз учителей знакомят со статистикой на государственном уровне.

«Дети часто очень, ну просто очень наивны! Найдя в Сети друга по интересам, который их понимает и поддерживает, они считают, что он самый замечательный человек. Но при этом они не видели его в реальности и не подозревают, что это может оказаться взрослый человек с дурными намерениями» (реплика участника С., дискуссия от 21 февраля).

В данной дискуссии отмечаются в большей степени отрицательные стороны использования Интернета. Первая и одна из самых важных вещей – это то, что чрезмерное увлечение Интернетом может оказать пагубное воздействие на бытовую, учебную, социальную, рабочую, семейную, финансовую и психологическую сферы нашей жизни.

Самый большой минус для молодых людей и детей сети Интернета это то, что в нем содержится информация сомнительного содержания. Также стоит еще раз отметить, что существует информационное воздействие, угрожающее физическому и психическому здоровью человека.

«*Существует множество сайтов, где ребенок может прочитать про наркотики, алкоголь и табак, как сделать взрывчатки, выйти на сайт начинающих террористов. Можно с легкость посетить сайт, где показывают видеоролики с детской порнографией, видео с суицидом, многое другое»* (реплика участника И., дискуссия от 21 февраля).

«В такой социальной сети как «ВКонтаке» и в различных чатах, каждый подросток, добавляя незнакомцев, может наткнуться на обман» (реплика участника Н., дискуссия от 4 марта).

Кроме того, отмечается, что никто не застрахован от кражи личной информации. Использование Интернета для банковских операций, социальных сетей или других услуг, часто делает личную информацию уязвимой для кражи.

«Еще одна из хорошо знакомых пользователю вещей – спам. Ээм…Спам относится к отправке нежелательных сообщений электронной почты, которые не служат никакой цели и засоряют ваш ящик. Такие

незаконные действия могут быть очень докучающими» (реплика участника Е., дискуссия от 21 февраля).

«И если бы спам был самым страшным! Так там есть и порнография и прочее, с ней связанное» (реплика участника И., дискуссия от 21 февраля).

«Так бывает и такое, что у детей вымогают их фотографии в ненадлежащем виде! Угрожают и запугивают» (реплика участника К., дискуссия от 4 марта).

Порнография доступная детям является, по мнению участников фокус-группы, одним из самых больших недостатков Интернета. Отсутствие контроля и неограниченный доступ порнографических материалов, отрицательно сказывается на детях. Все, что родители могут сделать, это заблокировать вредные сайты и вести мониторинг сайтов, которые просматривают их дети. Интернет дает доступ к материалам шокирующего содержания настолько легко, что часто попадается на глаза.

«Хорошо, что сейчас в школах работают над этими вопросами» (реплика участника А., дискуссия от 21 февраля).

«Немного помощи не помешало бы со стороны родителей, конечно» (реплика участника Е., дискуссия от 4 марта).

В ответах участников исследования заметен явный призыв к тому, чтобы родители дома так же знакомили своих детей с миром Интернета.

Далее участникам дискуссий был задан вопрос о том, какие угрозы в Интернете они бы назвали самыми опасными.

«Определенно кибербуллинг! Из-за его распространенности, легкости возникновения» (реплика участника М., дискуссия от 4 марта).

«Кибербуллинг, наркотики и педофилию. Очень сложно поймать преступника, доказать его вину…Они могут привести к летальному исходу» (реплика участника С., дискуссия от 21 февраля).

«Я согласна с Вами, но нельзя недооценивать овершеинг и секты. Слишком часто уж дети стали искать поддержки у друзей в Интернете» (реплика участника Т., дискуссия от 21 февраля).

Участники фокус-группы сошлись во мнении, что наибольший вред физическому и психологическому здоровью школьника могут нанести кибербуллинг, наркотики и педофилию, так как злоумышленники в этих ситуациях используют очень хитрые и изощренные приемы вовлечения или запугивания. И единственный способ оградить школьников от их воздействия это комплексная работа со стороны учителей и родителей, а также служб безопасности.

Далее респондентам были предложены кейсы (см. Приложение 4). В первом кейсе была история мальчика Алексея, который увлекался играми в онлайн-казино.

«Конечно, ситуация на грани…Он может как наиграться и бросить, так и попасть в зависимость от игр» (реплика участника Е., дискуссия от 4 марта).

«Школьникам свойственно желание выделиться. Вот и ему, вероятно, хочется отличаться за счет своего увлечения, а если он еще и выиграет деньги на кроссовки, будет очень горд. Многие могут самовыражаться за счет этого» (реплика участника А., дискуссия от 21 февраля).

Идея того, что это может быть временным увлечение и пройти, как детская игра в куклы, оживила дискуссию и вызвала недоумение коллег, так как большинство считало, что «такие увлечения обманчивы. И он, сам того не замечая, постепенно оказывается в долгах».

«Такого ребенка нужно контролировать. Видно, что у него есть энтузиазм и амбиции, значит, ему нужно хобби и временная работа, за которую он может получать деньги. Но не легкие, а заработанные свои трудом» (реплика участника Т., дискуссия от 4 марта).

«Верно. Ему нужно объяснить, что от реального заработка он получит больше уважения от сверстников» (реплика участника А., дискуссия от 4 марта).

Из дискуссии видно, что участники беседы сразу начинают искать решение данной проблеме, а не только обсуждать ее.

Далее участникам был предоставлен еще один кейс, в котором говорилось о встрече пятнадцатилетней девочки Маши с виртуальным другом.

В начале обсуждения особой критики или опасений в сторону героини истории не было сказано. Участники исследования даже отметили положительный момент данной истории:

«А почему нет? Дружба по интересам – самая крепкая и продолжительная» (реплика участника М., дискуссия от 4 марта).

Когда тема перешла к обсуждению встречи с человеком, которого знаешь, мнения разделились. Одни выказали недовольство по отношению к поступку девочки, другие поддержали.

«Группа интеллектуальная, вероятность попасть на мошенника мала» (реплика участника И., дискуссия от 21 февраля).

«Данная история только кажется хорошей и невинной, потому что мы знаем развязку. А если поставить троеточие после слов, где она пошла на встречу, то можно предположить любой финал, вплоть до летального исхода» (реплика участника И., дискуссия от 21 февраля).

«Виртуальный 15-летний Даниил мог оказаться на самом деле 40-летнм мужиком с аморальными намерениями» (реплика участника И., дискуссия от 21 февраля).

«Ну…в таких случаях всегда можно попросить друга или родителя походить рядом при первой встрече» (реплика участника Н., дискуссия от 21 февраля).

«Но…послушайте меня! С другой стороны, мы не можем практически жить в Интернете и бояться его. Наша жизнь уже стала во многом виртуальной» (реплика участника А., дискуссия от 21 февраля).

Важно, что респонденты при обсуждении данного вопроса пришли к выводу о том, что, несмотря на все плюсы и минусы Интернета, он «помогает детям развиваться». Если раньше эта роль была предоставлена родителям,

учителям или книгам, то в настоящее время Интернет является еще одной социальной средой для подрастающего школьника.

Для получения достоверных результатов исследования было взято два интервью по теме «Социальные механизмы управления информационной безопасностью школьников в глобальной сети Интернет» у социального педагога МБОУ СОШ № 7 Сорокиной Дарьи Геннадьевны и у педагога-психолога МБОУ СОШ № 7 Коробенко Юлии Витальевны.

Вопросы, задаваемые во время беседы практически идентичны. Интервью проводились отдельно, но далее будут одновременно приводиться ответы педагогов для дальнейшего их сопоставления.

Приведем несколько высказываний, характеризующих проблему Интернет-безопасности в школе.

«О!..Конечно, данный вопрос актуален как никогда. В последние годы все больше и больше детей осваивают бескрайние просторы Интернета. И… все чаще возникают если споры и сомнения: нужно ли разрешать детям пользоваться всемирной паутиной?..Большинство исследователей м специалистов отвечают на этот вопрос утвердительно» (Д.Г.).

«Детская аудитория интернета насчитывает сейчас 8-10 млн. пользователей до 14 лет…Если это не повод обратить внимание взрослых педагогов и ученых на данный вопрос, то что» (Ю.В.).

«Социальные отношения в Интернете выстраиваются так, как их интерпретируют пользователи из реальной жизни…эм…Можно сказать, что там возникает еще одно общество, параллельное нашему…Естественно со своими опасностями» (Ю.В.).

Мы видим, педагоги считают проблему исследования актуальной. Они так же определяют Интернет, как иное, обособленное общество, со своими законами и проблемами, которые только частично пересекаются с реальными. Проблема им видится и в том, что Интернет создавался взрослыми людьми для таких же взрослых. А неподготовленные психологически дети могут «оступиться» в нем.

Детская и подростковая аудитория пользователей всемирной сети все расширяется. Им интересно узнавать мир нового и неопознанного, общаться с людьми в разных концах света, играть в веселые игры и делиться с другими своими мыслями и увлечениями.

Из беседы ясно, что очень часто дети действительно не осознают опасности. *«Случайный клик»* или *«давно знакомый, добрый виртуальный друг»* оказываются ловушками.

Далее экспертов попросили уточнить, каким угрозам школьники подвержены больше всего, на их взгляд, а также какие школьники могут оказаться агрессорами, а какие жертвой в подобной ситуации.

«*В последнее время наиболее часто дети страдают от кибербуллинга, овершеринга и разных видов мошенничества»* (Д.Г.).

«*Причиной кибербуллинга может стать внешность, национальность или какой-то случай на уроке. Отличники и дети из малообеспеченных семей также потенциальные жертвы»* (Ю.В.).

«*Те, кто является агрессорами зачастую самоутверждаются»* (Ю.В.).

Помимо установления ролей (жертва и агрессор) в процессе кибератаки, важно знать, как часто происходят подобные случаи с данными видами угроз.

«Хм…смотря каким. Вот, например, с мошенничествами реже немного, чем с остальными двумя, может быть раз в 2-3 месяца. Вот от кибербуллинга могут пострадать несколько детей за год, если вовремя не заметить и не предотвратить. А об опасности овершеринга можно повторять хоть каждый день! Это ведь очень коварная угроза» (Д.Г.).

Крайне важным моментом экспертного интервью было выявление реальных примеров из практики экспертов, когда детям приходилось сталкиваться с опасностями в Интернете.

«Да…в моей практики были такие случаи. Например, одиннадцатилетняя школьница Мария (назовем ее так) пришла однажды в слезах. На вопрос о том, что случилось, она показала мне группу

«Вконтакте», созданную её одноклассниками. Там они выкладывали фотографии Марии и подписывали их самыми неприятными словами. Сложилась такая ситуация, что Маша и другая девочка соперничали за лидерство. Из-за того, что травля продолжалась уже месяцев, девочка чувствовала себя совсем беспомощной и одинокой. Я узнала, что классный руководитель проводил беседу с детьми, но это не повлияло на ситуацию. Вот…Я собрала в итоге виновников у себя, открыла перед ними их сайт и попросила объяснить. Я очень доходчиво пояснила, к каким последствиям это все может привести. В беседе так же участвовал завуч» (Д.Г.).

«Пару лет назад учился у нас мальчик Саша, который еще с 8 лет школы занимался бальными танцами. В начальной школе другие мальчишки постоянно подшучивали над ним из-за этого, что приводило часто к дракам. А когда они перешли в 5 класс, у многих появились современные телефоны и доступ в Интернет…тут два одноклассника и пару мальчиков из параллели начали постоянно писать ему обидные сообщения, шутки.ну..в общем …как сейчас называется, тролили его» (Ю.В.).

Завершающей точкой в историях экспертов стали показатели того, удалось или не удалось школьникам избежать последствий в сложившихся ситуациях.

«*Беседа с обидчиками Маши подействовала на ребят. Как только они начали осознавать все последствия данного поступка, сами захотели прекратить травлю. Я бы сказала..мм..что это случай с хорошим концом»* (Д.Г.).

«Поначалу Саша отшучивался в ответ, но через несколько месяцев бросил танцы. Родители его уговаривали этого не делать, но он настоял на своем. И только к концу учебного года выяснилась причина ухода с танцев. Родители рассказали, что частенько Саша чуть ли не в истерике дома бился и со слезами и криками просил их не отводить его туда. Но родители считали, что он хочет просто погулять или посмотреть телевизор. А так как внешние атаки в школе он отбивал, никто и не подозревал, что в Сети

он подвергается сильному моральному давлению…со стороны тех, чье мнение имеет особо важное значение для подростка» (Ю.В.).

Из историй педагогов видно, что самостоятельно дети почти не могут себя защитить, особенно если они подвергаются жесткой неконструктивной критике со стороны не одного, а нескольких сверстников. У взрослого человека уже хорошо сформированы психологические установки, он знает, что делать в подобных ситуациях с травлей. Он может подать в суд на обидчика, предоставив доказательства или просто не обращать на исходящий от кого-то «негатив» внимание и не отвечать обидчику или просто заблокировать его.

Со слов педагогов понятно, что так же невозможно представить наших подростков без социальных сетей. Все чаще распространенные социальные сети стали: «Одноклассники», «ВКонтакте», «Фэйсбук». Регистрируясь и заполняя свои страницы, подростки, показывают окружающим свой внутренний мир, что является их «визитной карточкой».

Использование Интернета подрастающим поколением – один из важных показателей уровня развития информационного общества. Безусловно, сегодня тяжело представить, что какая-либо область деятельности будет обходиться без использования ИКТ, особенно у молодежи. Так, школьники в процессе своего обучения с начальных классов активно начинают использовать компьютеры и Интернет: готовят проекты, рефераты, презентации, изучают дополнительную литературу и электронные приложения к учебникам. И это приводит к следующему умозаключению, о котором говорят педагоги.

«*Обязательно в школе должны проводиться мероприятия, чтобы защитить молодое поколение! В классах с 1 по 6 это могут быть тематические игры, сказки, урока-путешествия с страну Интернет. Я даже уже мультфильму видела на эту тему. Вот их тоже можно показывать детям. С 7 по 11 класс это уже должны быть серьезные и*

основательные беседы, с подробным разъяснением о последствиях…Вот тогда школьники будут максимально защищены» (Ю.В.).

«Если вовремя не принимать меры или не объяснять детям, что в Интернете, как и в жизни что-то хорошо, а что-то плохо, то случаи мошенничеств и прочего могут возрасти…увы…Нужно при этом, чтобы не только в школе, но и дома поднималась эта тема» (Д.Г.).

Следует подчеркнуть, что успех информатизации школьников во многом зависит от наличия технологических (аппаратных и программных), информационных и организационных ресурсов, от продуманной политики области по формированию информационного образовательного пространства, от степени участия учителей и родителей в наполнении информационного пространства.

Так как мы завершили первый этап линейного анализа данных, можно преступить к анализу значимых сопряжений.

Для начала, построим таблицы сопряженности между вопросами, которые были связаны с основными проблемными аспектами исследования и для выявления социально-демографических характеристик, как пол и возраст респондента.

Сопоставив пол респондента и ответы на вопрос анкеты «Как часто Вы используете Интернет?», видно, что чаще (несколько раз в день) Интернетом пользуются мальчики, а именно 37,4%. Для девочек показатель составляет 33,7%. Каждый день или почти каждый день Интернетом пользуются 9,9% мальчиков и 14,8% девочек. Из опрошенных один или два раза в неделю, а также один-два раза в месяц или реже, в совокупности пользуются Интернетом менее 5% всех опрошенных. При этом разница между показателями респондентов разного пола небольшая, следовательно, можно сделать вывод, что частота использования Сети имеет минимальную зависимость от пола.

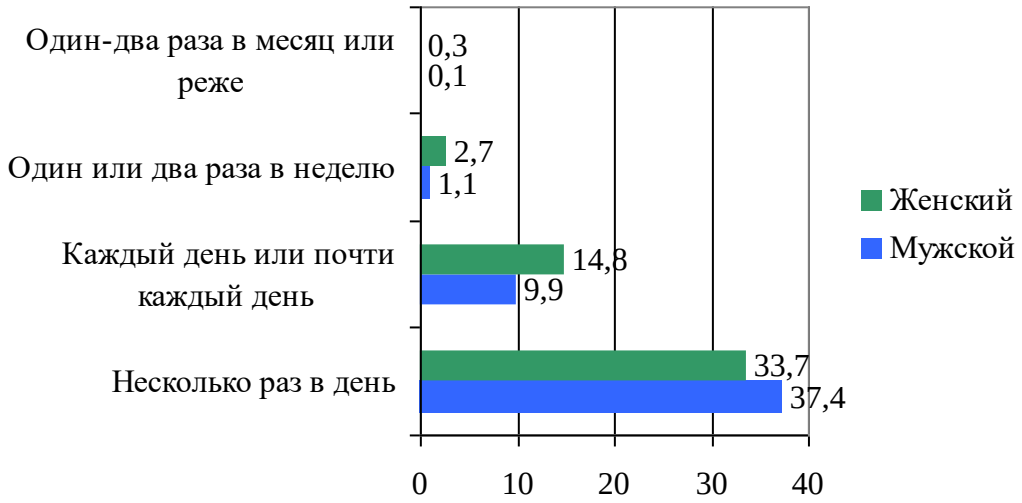

Диаграмма 30. Распределение ответов респондентов на вопрос о регулярности использования Интернета в зависимости от пола

Теперь рассмотрим связь пола респондента и его осведомленность о различных видах угроз в Сети. По ответам на вопрос «О каких из приведенных понятиях Интернет-угроз Вы слышали?» видно, что мальчики и девочки ознакомлены с опасностями примерно на одном уровне, но при этом разница зависит от определенного вида угрозы.

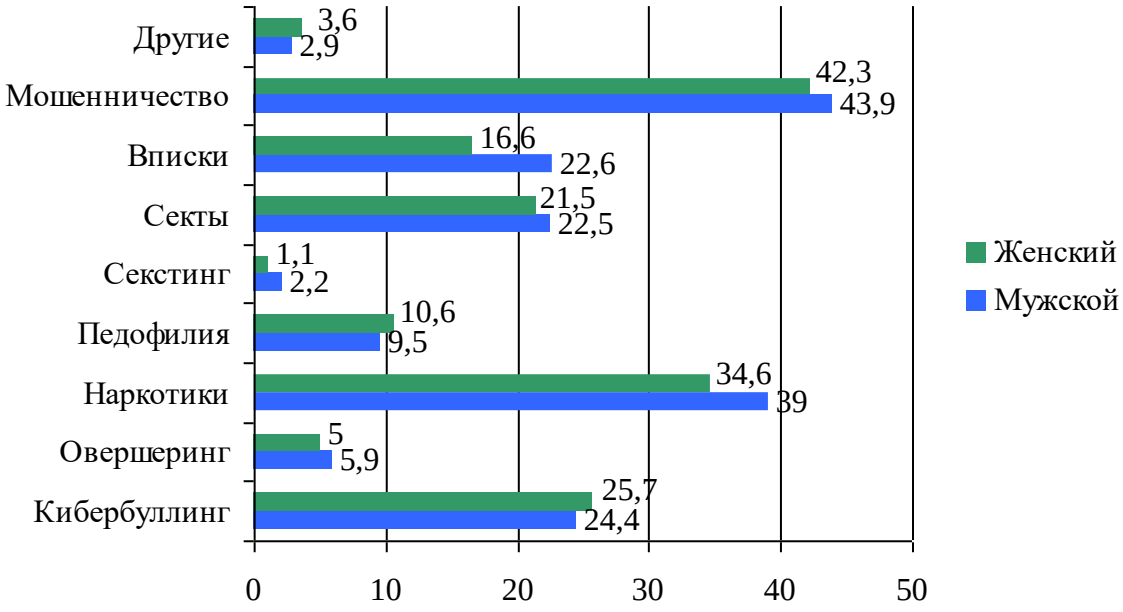

Диаграмма 31. Распределение ответов респондентов на вопрос об их осведомленности в зависимости от пола

Мальчики лучше осведомлены о: овершеринге (5,9%), наркотиках (39%), секстинге (2,2%), сектах (22,5%), списках (22,6), мошенничестве

(43,9%) Девочки лучше осведомлены о: кибербуллинге (25,7%), педофилии (10,6%), а также чаще выбирают наличие альтернативных опасностей (3,6%).

Далее, рассмотрим сопряжение между полом и вероятностью наличия уже существующей угрозы. Больше девочек признается, что сами (1%) или один из их близких друзей (4,3%) являлись жертвой травли. Мальчики чаще, чем девочки, говорят о том, что сами могли участвовать в травле другого человека (0,3%). Большинство респондентов мужского (13,1%) и женского (16,7%) пола утверждают, что таких случаев не было.

По ответам респондентов на вопрос «Объясняли ли Вам родители, как безопасно пользоваться Интернетом?» очевидно, что девочки чаще получают рекомендации от родителей на тему пользования Сетью. Вариант ответа «Да» выбрало 14,8% мальчиков и 22,1% девочек, а вариант ответа «Нет» выбрало 21,4% мальчиков и 19,5% девочек. Остальные утверждают, что не помнят о наличие бесед подобной тематики.

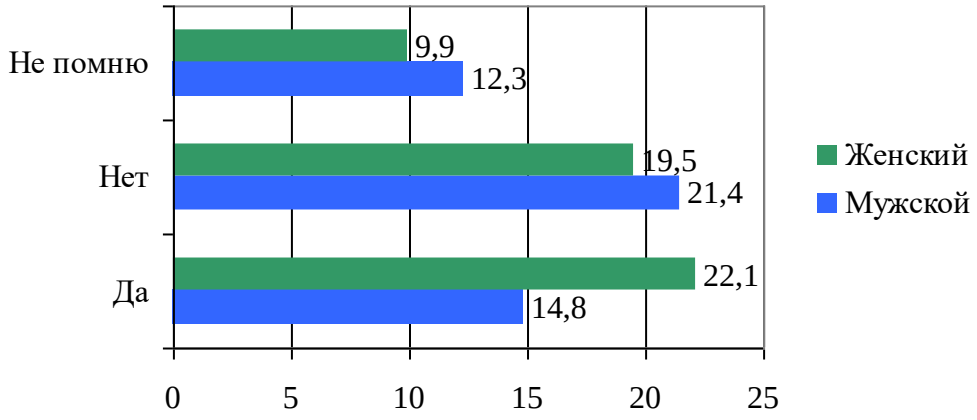

Диаграмма 32. Распределение ответов респондентов на вопрос о том, объясняли ли им родители, как безопасно пользоваться Интернетом, в зависимости от пола

Аналогично проведем анализ зависимости основных проблемных аспектов от возраста школьника. По результатам легко заметить, что наиболее частыми пользователями Сети являются дети в возрасте от 16 до 17 лет. 27,8% из них утверждают, что используют Интерне несколько раз в день, 0,1% – один или два раза в неделю, реже Интернетом никто из опрошенных данного возраста не пользуется. Реже всех пользуются Интернетом дети 9-10 лет: 16,3% несколько раз в день, а 0,3% один-два раза в месяц или реже.

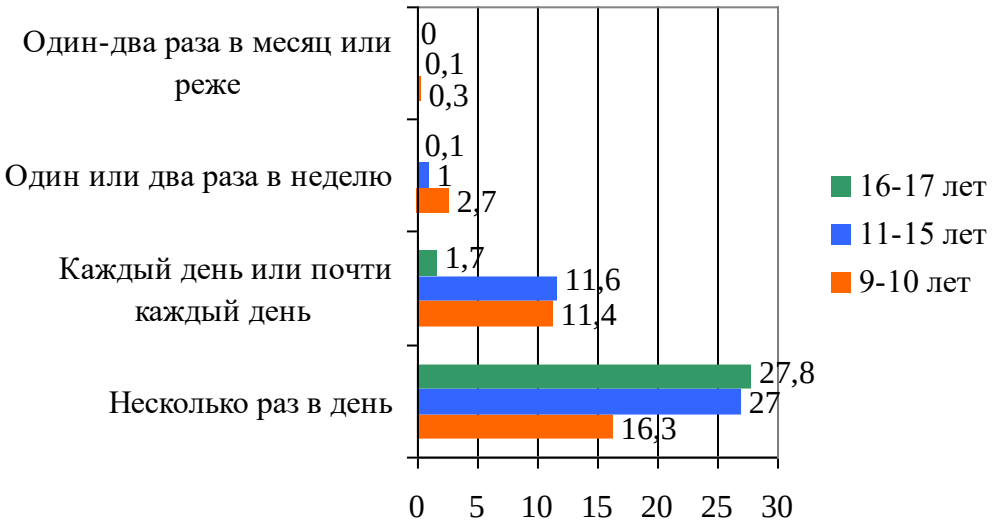

Диаграмма 33. Распределение ответов респондентов на вопрос о регулярности использования Интернета в зависимости от возраста

Таким же образом была выявлена взаимосвязь между возрастом детей и их осведомленности о Интернет-угрозах: чем старше школьники, тем о большем количестве подстерегающих их опасностей они знают. К примеру, о кибербуллинге слышало 25,4% старших школьников, 17,2% обучающихся в средней школе и 8,9% – ученики начальных классов. Только в вариантах ответа «Мошенничество» и «Другие» показатели обучающихся в средней школе были наивысшими, но при этом разница показателей незначительна.

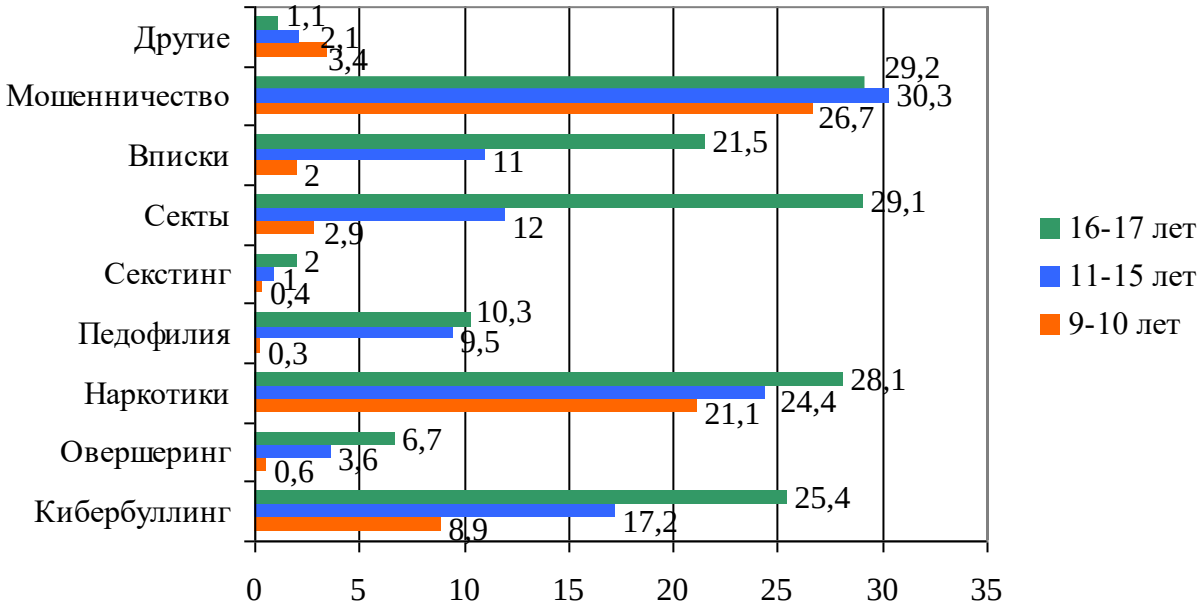

Диаграмма 34. Распределение ответов респондентов на вопрос об их осведомленности в зависимости от возраста

Теперь рассмотрим связь вопроса «Сталкивались ли Вы с травлей в Интернете?» и возраста. О причастности в роли жертвы или агрессора к подобной ситуации охотнее сознаются ученики 11-15 лет. Самые низкие показатели принадлежат ученикам старшей школы. Можно сделать вывод, что, чем старше становится ребенок, тем разумнее он реагирует на агрессию в Интернете.

Помимо этого, расчеты показали, что существует связь между возрастом ребенка и контролем со стороны родителя: чем младше ребенок, тем чаще родители объясняют ему как безопасно пользоваться Интернетом. При этом суммарные показатели на ответы «Нет» и «Не помню» превышают количество ответов «Да», что свидетельствует о низком уровне контроля со стороны родителей.

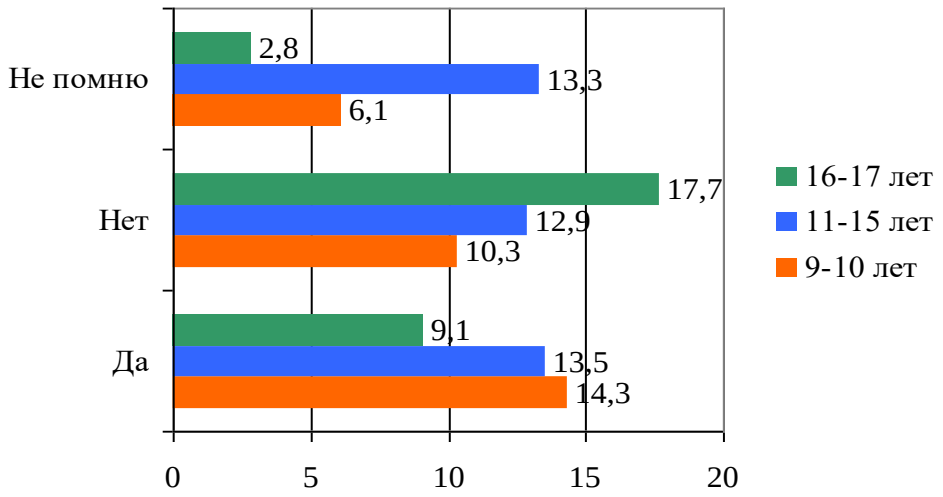

Диаграмма 35. Распределение ответов респондентов на вопрос о том, объясняли ли им родители, как безопасно пользоваться Интернетом, в зависимости от возраста

Проанализировав вопросы, в которых была найдена статистическая связь, можно сказать, что в некоторых из них существует очевидная взаимозависимость между переменными. Например, мы выявили зависимость проблемных аспектов исследования от возраста школьников, она выражена наиболее явно, в отличие от зависимости от пола респондентов.

Далее в нашем исследовании рассмотрим связь меду основными проблемными аспектами в ответах школьников и родителей.

Регулярность использования школьниками Интернета подтверждается как результатами опроса самих детей (71,1%), так и родителей (74,9%). Показатели указывают на то, что дети по сравнению с родителями не считают, что они проводят много времени в Интернете.

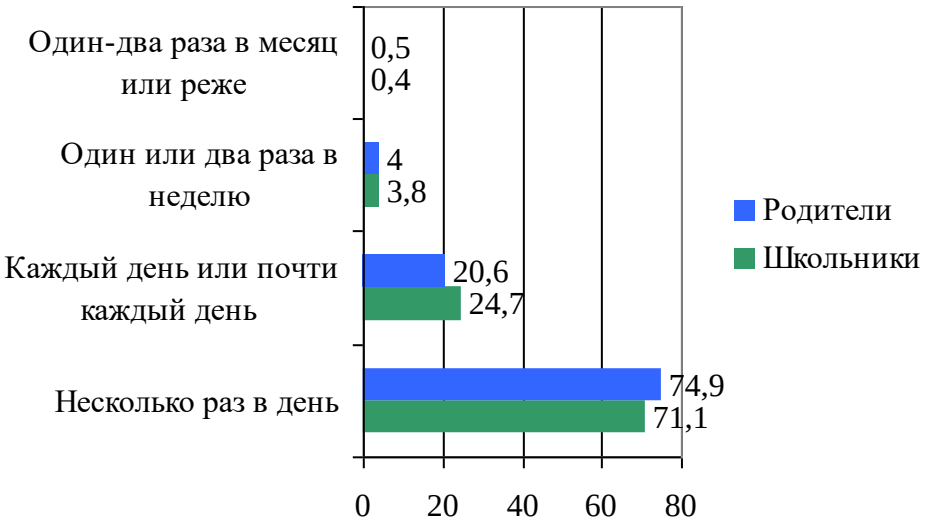

Диаграмма 36. Распределение ответов респондентов на вопрос о регулярности использования Интернета школьниками

Степень осведомленности родителей об опасностях Сети выше, чем у детей.

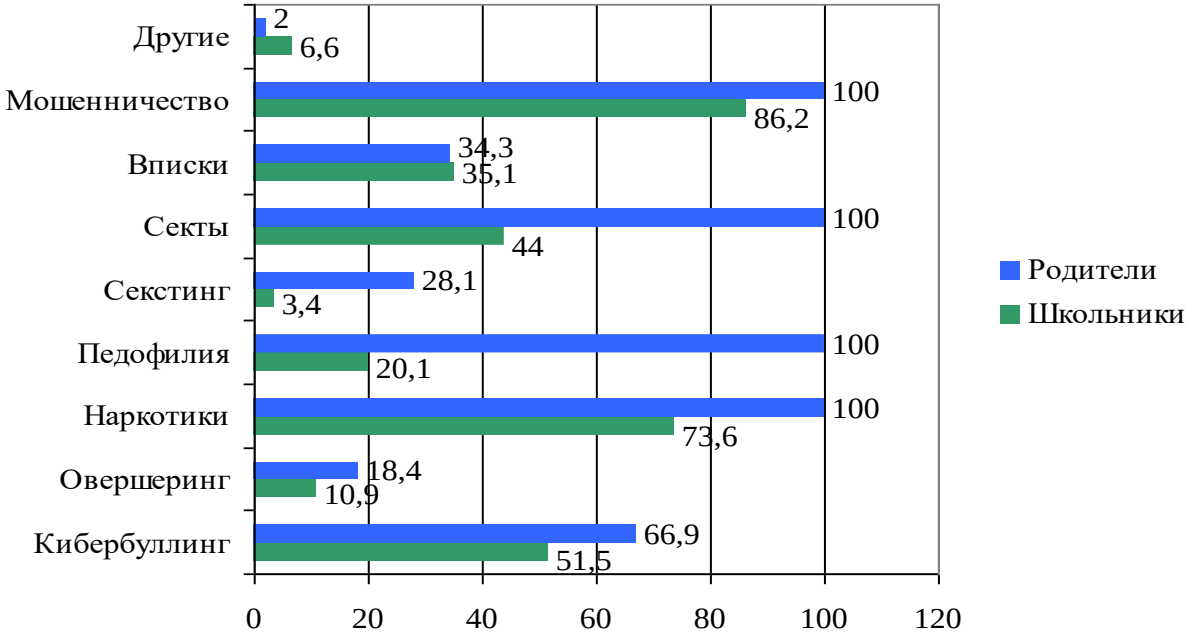

Диаграмма 37. Распределение ответов респондентов на вопрос об их осведомленности в различных видах Интернет-угроз

Показатели в ответах родителей достигают 100% в случае угроз, которые могут возникнуть не только в Интернете, например, наркотики, секты, педофилия, мошенничество.

Так же мы проанализировали вероятность риска на примере кибербулинга для ребенка или наличие этого риска в окружении ребенка. 7,5% школьников и 6,7% родителей говорят о наличии подобной опасности в окружении ребенка. Так же очень низкими показателями отмечены такие варианты ответов, как «сам был жертвой травли», «сам участвовал в травле другого человека».

Уровень контроля, осуществляемый со стороны родителей, оказался ниже среднего. Всего лишь 36,9% школьников и 46% родителей говорят о его присутствии. Причем наличие разницы при выборе варианта ответа «Да» в 9,1% свидетельствует о вероятной неэффективности предпринимаемых некоторыми родителями мер.

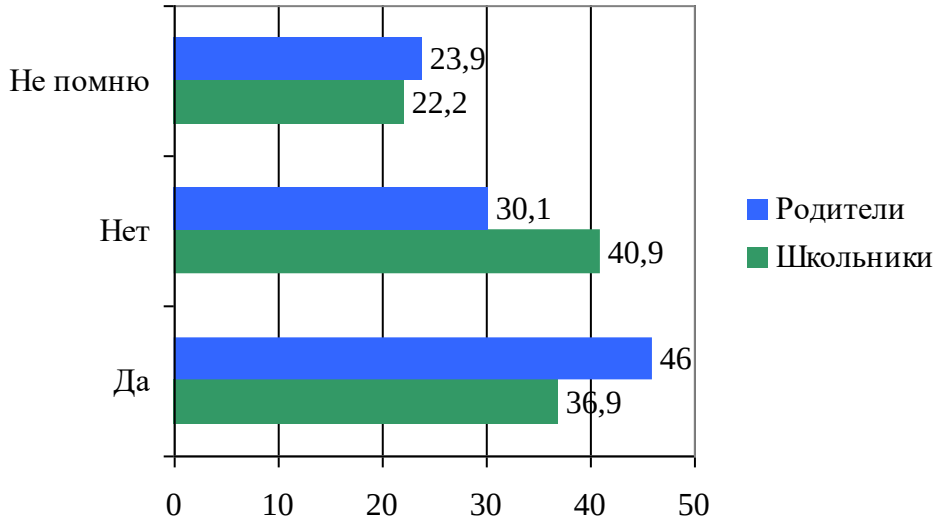

Диаграмма 38. Распределение ответов респондентов на вопрос о том, объясняют ли родители школьникам, как безопасно пользоваться Интернетом

Итак, мы приходим к следующим выводам.

В ходе проведенного исследования было выявлено, что вторая и третья гипотезы подтвердились лишь наполовину, остальные гипотезы полностью подтвердились. Результаты социологического исследования показали, что большинство школьников города Белгорода проводят чрезмерное количество

времени в Интернете, а именно они используют Интернет несколько раз в день и в среднем проводят около 2-3 часов свободного времени в нем, тем самым, подвергая себя опасности. Особой популярностью у детей пользуются социальные сети и различные игры, что является площадкой для активной деятельности мошенников и агрессоров.

Говоря об осведомленности школьников, родителей и учителей, исследование показало, что наиболее осведомленной социальной группой являются учителя, а наименее осведомленной – школьники. Причем сведения, которыми обладают школьники, ранжируются в зависимости от их возраста. Самыми известными угрозами для школьников, а также родителей, являются те, которые не возникли в Интернете, а лишь расширили границы воздействия с его помощью, например, мошенничества, наркотики, педофилия. О таких угрозах, как овершеринг и секстинг, респондентам опроса было известно меньше всего. Поэтому данная гипотеза подтвердилась частично.

Еще одна гипотеза, подтвердившаяся частично, связана с контролем выхода школьников в Сеть. По результатам опросов и фокус-групп очевидно, что родители и учителя использую различные методы контроля. Контроль со стороны учителей обусловлен постановлениями государства и внутренней политикой школ. Родительский контроль в свою очередь является менее эффективным, так как не вписан в конкретные рамки и имеет рекомендательный характер.

Наша последняя гипотеза тоже нашла подтверждение. По мнению относительного большинства респондентов, школьники не сталкивались с ситуациями травли в Интернете или же не слышали о подобных. Это свидетельствует о невысоком уровне угрозы по отношению к школьникам в городе Белгороде. Но стоит все же учитывать факт недостаточной осведомленности школьников и вероятность умалчивания по каким-либо причинам информации.

РАЗДЕЛ III. ВЫВОДЫ И РЕКОМЕНДАЦИИ ПО РЕЗУЛЬТАТАМ ИССЛЕДОВАНИЯ СОЦИАЛЬНЫХ МЕХАНИЗМОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ШКОЛЬНИКОВ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

Потоки информации, которую глобальная сеть Интернет пропускает через себя, увеличиваются вдвое практически каждый год. Посредством информатизации общества все больше школьников пользуются информацией, полученной из Всемирной паутины. Исследования показали, что пользователи сети Интернет молодеют с каждым годом. Зачастую активное использование информации из Сети сказывается на интеллектуальном, нравственном развитии детей, их психическом и физическом здоровье.

В постиндустриальном обществе особую ценность приобретает такой актив, как информация. Она должна быть защищена надлежащим образом, независимо от ее вида, а также форм хранения и распространения. Защитой информации занимается такая сфера как «информационная безопасность».

Кроме того, появляется еще одно новое понятие – Интернет-угроза, которое требует к себе особого внимания. Угрозы в сети Интернет бывают двух видов: информационно-технические и информационно-психологические.

К самым распространенным информационно-психологическим угрозам мы отнесли кибербуллинг, секстинг, овершеринг, секты, наркотики, вписки, педофилию, мошенничество. Основной группой риска по отношению к данным видам угроз или их различным проявлениям являются школьники.

Исследования показали, что многие школьники не осведомлены об опасности или же просто не понимают, что могут оказаться в опасной ситуации. Так, например, желания активно общаться, опубликовывать свои фотографии или завести новых друзей могут стать причиной овершеринга или секстинга.

Как видно из анализа фокус-групп, а также интервью и результатов анкетирования, что проблема наличия большого количества угроз для

незащищенной личности школьников остается открытой и актуальной. Возрастает необходимость комплексного воздействия на проблему: со стороны учителей, родителей, а также государства. Если убрать из этой цепочки одно звено, то проблема не решится окончательно: резкое противоречие в воспитательной работе между домом и школой может оказать пагубное влияние на ребенка, а также отсутствие активных действий государства в сфере Интернет-безопасности подвергает подрастающее поколение к еще большей опасности.

Государство старается регулировать этот процесс посредством законов «О персональных данных», «О защите детей от информации, причиняющей вред их здоровью и развитию», «Об информации, информационных технологиях и о защите информации», администрация города – посредством реализации программы «Развитие солидарного общества и информационного пространства городского округа города Белгорода на 2017-2020 годы».

Со стороны школы для решения проблемы обеспечения информационной безопасности проводятся комплексные меры, которые включают, как административные, организационные, программно-технические меры, так и профилактические, для формирования информационной культуры и навыков учащихся в целях ограничения доступа к негативной информации вне учебного заведения.

Многие родители осознают свою ответственность перед ребенком и обществом. Они проводят беседы с детьми, знакомят их с сетевым этикетом. Но как показывают исследования, что принимаемых мер со стороны родителей недостаточно, особенно с учетом низких количественных показателей.

В нашем исследовании мы отталкивались от таких проблемных аспектов, как регулярность использования школьником глобальной Сети, цели его использования, осведомленность школьника о проблеме исследования, наличие или отсутствие контроля со стороны родителей/учителей, уровень подверженности рискам ребенка.

Проведенное нами исследование, состоящее из двух опросов, двух фокус-групп и двух экспертных интервью, показало, что:

Во-первых, школьники города Белгорода проводят большое количество времени в Сети. Из всех респондентов около 50 % сообщали кому-либо свою личную информацию, а более половины опрошенных игнорируют сообщения о возрастном ограничении. Это снижает их уровень защищенности перед Интернет-угрозами.

Во-вторых, высокий уровень осведомленности о проблеме только у учителей города Белгорода. Это связано с тем, что по отношению школ ведется активная государственная политика на федеральном и локальном уровнях. Школьники и родители города Белгорода в свою очередь недостаточно осведомлены о существующем широком спектре Интернет-угроз.

Кроме того, возникает проблема контроля информации, получаемой школьниками из Сети. В школе это возникает по причине наличия у детей личных мобильных устройств, дома же из-за отсутствия достаточного контроля со стороны родителей, которые не придают особое значение информационному воспитанию ребенка.

Все же наше исследование показало, что, уровень угрозы со стороны агрессоров и мошенников в сети Интернет по отношению к школьникам города Белгорода относительно невысок. Исходя из общемировых тенденций их развития, возникает угроза распространения опасности в Сети.

В связи эти мы считаем необходимым разработку комплексных социальных механизмов управления информационной безопасностью школьников для родителей, школ, а также администрации города.

Последовательному формированию у школьников самостоятельного критического мышления может способствовать введение администрацией города в школьные программы курса медиаобразования.

Медиаобразованием называется область знаний, направленная на разработку совокупности системных операций по анализу и изучению

специфику работы таких средств массовой информации, как пресса, радио, телевидение, Интернет. Поскольку возраст, с которого дети становятся пользователями Сети, уменьшается, необходимо вводить данную дисциплину еще в начальной школе. Работа, проводимая по данному предмету должна быть системной и направленной на формирование базовых умений при работе с информацией.

Мировая педагогическая общественность давно осознала значимость этой проблемы не только для интеллектуального развития человека, но и для его информационной безопасности. Так, проблема информационной безопасности ребенка перерастает в проблему концепции системы образования, системы подготовки педагогических кадров.

В процессе непрерывного образования личность должна получить знания, выработать умения и навыки работы с новыми информационными технологиями и средствами телекоммуникации, позволяющими выполнять социальные роли создателя и потребителя информации.

Данный процесс не ограничивается только реализацией технологических проблем, он включает в себя овладение эффективными методами обучения и познания, деятельности и мышления, стоящими на верхушке пирамиды непрерывного образования, а именно: анализа, синтеза, абстрагирования, формализации, обобщения информации, связанных с креативным уровнем образования, позволяющим из множества информации строить свое представление о мире или, иначе, сформировать информационный стиль мышления и информационное мировоззрение.

Кроме того, необходимо осведомить родителей школьников о наличии различного программного обеспечения, с помощью которого можно осуществлять контроль нежелательной для ребенка информации (см. Таблица 1). Веб-фильтр родительского контроля оценивает содержимое веб-узлов и может блокировать те из них, содержимое которых определено как нежелательное.

Таблица 1

Перечень программ-фильтров контента

Название	Описание	Сайт разработчиков
Kaspersky Internet Security	Kaspersky Internet Security предлагает запретить доступ к нежелательным сайтам.	www.kav.ru
KinderGate (Родительский Контроль)	С помощью KinderGate Родительский Контроль родители смогут не только запрещать сайты взрослого содержания, но и блокировать массу других категорий по своему усмотрению.	www.usergate.ru
Фильтр «Семейная Безопасность»	Веб-фильтр в Семейной безопасности Windows Live помогает защитить вашего ребенка путем ограничения доступа к определенным веб-сайтам.	download.ru.msn.com
StaffCop Home Edition	Программа сохраняет сайты, посещаемые пользователями.	www.staffcop.ru/home/
«Один Дома»	Данное ПО предназначено специально для защиты детей от просмотра нежелательного контента.	www.odindoma.org
«Интернет Цензор»	Главная задача пакета – сделать пребывание детей и подростков в Интернете безопасным, оградив их от вредных ресурсов.	www.icensor.ru
Avira Premium Security Suite	Пакет программ, которые будучи используемыми в комплексе, позволяет защитить личный компьютер от большинства современных угроз.	www.avira.com
BitDefender Internet Security 2011	BitDefender Internet Security 2011 защищает ПК от вирусов, хакеров, взлома и попытки кражи персональных данных	www.bitdefender.ru
Dr.Web Security Space	Помимо сильного модуля родительского контроля, это также комплексное решение проблемы защиты ПК	www.drweb.com
F-Secure Internet Security 2009	Комплексное решение защиты от всех видов интернет-угроз.	www.f-secure.com

Рассмотрим функции, решаемые с помощью родительского контроля:

1. Ограничение времени, проводимого ребенком за компьютером.
2. Установка запрета на доступ детей к отдельным играм.
3. Ограничение активности детей в Интернете.
4. Установка запретов на использование детьми отдельных программ.
5. Ведение отчетов о работе ребенка за компьютером.

Перед общеобразовательными организациями как государственного, так и частного характера должны стоять следующие задачи по управлению информационной безопасностью школьников:

1. Выявление уровней обучения информационной безопасности школьников. В школе можно выделить три уровня обучения информационной безопасности, соответствующие возрастным категориям обучающихся: начальной школе (6-9 лет), средней (10-15 лет), старшей (16-18).

2. Классификация угроз на каждом этапе обучения информационной безопасности. На первом этапе можно выделить угрозы личной безопасности школьника, не связанные с использованием технических средств. На втором этапе выделяют угрозы личности, семье, окружающему ученика социуму, возникающие при работе с информацией на компьютере и в Интернете. На третьем этапе – изучение основ профессиональной безопасности по выбранному профилю с использованием специальных средств записи и обработки информации. Второй и третий этапы обучения информационной безопасности непосредственно связаны с медиаобразованием.

3. Обеспечение непрерывности в изучении информационной безопасности при переходе от одного этапа обучения к другому. Обеспечение непрерывного обучения за счет четкого выделения понятийного аппарата на каждом этапе и построении на его основе системы последующих положений с учетом возрастных особенностей развития и использования технических средств работы с информацией. Определение роли угроз, исходящих от сообществ, в которые могут входить школьники на каждом этапе непрерывного образования.

4. Определение содержания обучения на каждом этапе. В зависимости от возникающих угроз необходимо определить содержание обучения на каждом этапе и разработать условия безопасного использования соответствующих сервисов работы с образовательным контентом. Особенностью обучения информационной безопасности является то, что

недостаточно изучить только организационные и технические средства обеспечения, но и необходимо привить нравственность и воспитать ответственность за использование информации, которая может причинить ущерб не только личности, неумело с ней обращающейся, но и другим людям.

5. Установление способов согласования действий и распределение меры ответственности семьи, школы, системы дополнительного образования по обеспечению информационной безопосностью школьников в учебно-воспитательном процессе. Необходимо разработать методические рекомендации для родителей по обеспечению информационной безопасности семьи. Они должны содержать классификацию возможных информационных угроз. Рекомендации по ограничению доступа ребенка к информации и по обеспечению информационной безопасности для детей, находящихся за пределами школы, – в зоне ответственности родителей. Организационными формами взаимодействия школы с родителями по вопросам обеспечения ИБ как учащихся, так и семьи в целом могут быть как традиционные (родительские собрания, заседания родительских комитетов, индивидуальные беседы учителей с родителями), так и специально организованные лекции, и семинары с участием педагогов, правоохранительных органов, специалистов по защите информации.

6. Определение форм внедрения мер по обеспечению информационной безопасности в учебно-воспитательный процесс школы. Необходимо разработать систему дидактических средств для учащихся на каждом этапе обучения, включающую в себя систему понятий, способы поведения, законодательство в области, и другие аспекты. Внедрение знаний по информационной безопасности в учебный процесс школы может быть, как в рамках существующих предметов, например, информатики или ОБЖ, так и на специально организуемых занятиях, например, классных часах, ролевых играх, проектной деятельности учащихся.

Комплексное решение рассмотренных задач информационной безопасности со стороны семьи и школы позволит значительно уменьшить риски причинения различного рода ущербов (морального, материального, здоровью и др.) ребенку. Поэтому обеспечение информационной безопасности школьников должно стать одним из первоочередных направлений работы современной школы.

Практические советы родителям необходимо так же ранжировать вв зависимости от возраста их детей.

Как считают психологи, для детей, обучающихся в начальной школе, а также осваивающие программу первого или второго класса средней школы, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Правила по безопасности в данном возрасте:

1. Завести домашний список правил посещения и использования Сети Интернет, одновременно действующий и для детей, и для родителей, соблюдать записанные в него правила и условия.

2. Определить строгие временные рамки при нахождении за компьютером в течение дня.

3. Пояснить ребенку, что периодическая проверка его действий за компьютером не является вашей прихотью или способом развлечься, это способ обезопасить его.

4. Переместите домашний компьютер в общую комнату или комнату родителей, чтобы он находился под контролем.

5. Помимо собственного контроля, необходимо установить программу, позволяющую осуществлять фильтрацию контента.

6. Периодически заводите разговор об их виртуальных друзьях.

7. Объясните об опасности личных встреч с незнакомыми друзьями из Интернета либо предложите свою помощь при организации их знакомства.

8. Создайте совместно с ребенком сайты «белого» списка, на которые он потом будет заходить, и следите за исполнением.

9. Научите детей не раскрывать личную информацию в Сети при регистрации на сайтах или при общении с кем-то: свой адрес, телефон, номер школы.

10. Загружайте все программы вместе, чтобы какой-нибудь вирус не попал в компьютер.

11. Можете создать вашему ребенку личную учетную запись с ограниченным доступом для работы на компьютере.

12. Наладьте доверительные взаимоотношения с ребенком.

13. Научите или мотивируйте ребенка рассказывать вам об угрозах в Сети и обращаться к вам при личном столкновении с ними. Не отчитывайте ребенка, а, наоборот, похвалите и посоветуйте подойти еще раз в подобных случаях.

14. Предлагайте завести общий почтовый ящик или же узнайте у детей пароль от их ящика, чтобы оградить от общения с подозрительными незнакомцами.

15. Воспитывайте в детях культуру общения в Сети, объясните им, что использовать сеть для хулиганства, распространения сплетен или угроз недопустимо и опасно.

В возрасте 13-17 лет, когда дети обучаются в средних или старших классах, приоритетной для них становится своя точка зрения или сверстников. Родительские пожелания и наставления становятся второстепенными. Поэтому контролировать ситуацию родителям становится сложнее. Иногда Интернет становится и другом, и учителем, и советником.

В данном возрасте родителям необходимо сделать упор на соглашение между ними и ребенком о домашнем пользовании Интернетом, проверять историю посещаемых ребенком сайтов, создать учетную запись на правах администратора, о паролях доступа к которой будут знать только родители.

Для организации безопасной работы с Интернетом в данном возрасте необходимо придерживаться следующих рекомендаций:

1. Определите четко количество времени, которое ребенок должен проводить в Сети, список «белых» сайтов и другие правила пользования.

2. Домашнее устройство с выходом в Интернет также должно находиться в общей комнате, что позволяет негласно контролировать соблюдение домашних правил.

3. Разговаривайте с детьми не только об их виртуальных друзьях и мошенниках, а еще и о более серьезных опасностях.

4. Приучите ребенка сразу рассказывать вам о столкновении с Интернет-угрозами, чтобы была возможность вовремя предотвратить их.

5. Пользуйтесь контент-фильтрацией, родительским контрлем.

6. Необходимо знать, какими социальными сетями пользуются ваши дети.

7. Контролируйте общение с виртуальными незнакомцами и по-возможности отговаривайте от личной встречи с ними.

8. Напоминайте о неразглашении личной информации, объясните, какие последствия могут быть, если она попадет в руки к злоумышленникам.

9. Контролируйте установку новых программ, следите, чтобы они были загружены с официальных сайтов, во избежание заражения компьютера вирусами.

10. Держите под контролем эмоциональное состояние ребенка, чтобы он не искал утешения в сектах или вписках, так популярных в Интернете.

11. Научите ребенка давать реальный электронный адрес только по делу, чтобы оградить его от большого количества спама в Сети, а также не отвечать на подозрительные ил нежданные письма.

12. Заинтересуйтесь виртуальной жизнью ребенка, зарегистрируйтесь в соцсетях, которыми он пользуется, посетите сайты, которые нравятся вашему ребенку.

13. Обсудите различные виды мошенничеств, которые распространены в Интернете, например, покупка ответов на экзамены, высокооплачиваемые подработки.

14. Расскажите о последствиях онлайн-игр, в особенности азартных.

15. Расскажите о правовой стороне ситуации, наказании за мошенничество, кибербуллинг, разглашения частной информации в виде фото или видео.

С момента поступления ребенка в школу угроза информационной безопасности в отношении ребенка возрастает, поскольку у него появляется свобода от наблюдения и контроля со стороны родителей, а также начинает разграничиваться сфера влияния семьи, школы, системы дополнительного образования, социума.

Вследствие актуальности проблемы отсутствия комплексных социальных механизмов управления информационной безопасностью школьников в будущем необходимо рассматривать как данную проблему в общем, так и отдельные ее составляющие.

С целью реализации вышесказанного, мы предлагаем:

1. Проведение постоянного мониторинга общественного мнения, в который необходимо включить оценку информированности населения о текущей проблеме по городу Белгороду и Белгородской области.

2. Изучить поставленную проблему посредством интегрированного социологического метода – фокус-группа в виде проведения онлайн-конференции по теме.

3. Провести исследования отдельно по каждому виду угроз в Сети по городу Белгороду и Белгородской области в которое необходимо включить оценку информативности, степень и частоту подверженности или, наоборот, участия. Необходимо, в целом, повышать уровень компетентности населения, борясь с основными угрозами в Интернете.

4. Увеличить количество мероприятий, предоставляющих объективную информацию об опасностях для несовершеннолетних детей в сети Интернет, а так же рекомендации по снижению уровня угрозы.

5. Организация и проведение тематических научных и научно-практических конференций, семинаров, круглых столов, симпозиумов, посвященных механизмам управления информационной безопасностью школьников в Интернете, что позволит более глубоко изучить конкретные факторы.

6. Взаимодействие с организациями, институтами, изучающими опыт других стран по данной проблеме, для более объективного понимания и грамотного построения дальнейших путей решения выявленных проблем.

Только так, социальные механизмы управления информационной безопасностью школьников в глобальной сети Интернет могут быть действительно выведены на новый уровень. При следовании вышеуказанным рекомендациям и дальнейшей изученности проблемы станет возможным рост уровня информационной безопасности школьников.

Таким образом, подводя итоги данного раздела, можно сказать следующее. В разделе были предложены, по нашему мнению, наиболее эффективные профилактические мероприятия. К ним относятся:

1. Введение в школьную программу новой дисциплины, в качестве предметной области или же части другого предмета, к примеру, информатики.

2. Популяризация среди родителей всевозможное программное обеспечение, с помощью которого можно осуществлять контроль нежелательной для ребенка информации

3. Проведение личных бесед с детьми и увеличение количества мероприятий, предоставляющих объективную информацию об опасностях для несовершеннолетних детей в сети Интернет, тем самым комплексно воздействовать на проблему.

4. Организация и проведение дальнейших исследований по данному вопросу, которые будут затрагивать одновременно проблему и в общем, и в частном, например, исследование статистического индикатора в динамике 3-5 лет на территории города Белгорода и исследование воздействия конкретных Интернет-угроз на школьников города Белгорода.

ЗАКЛЮЧЕНИЕ

Информационная безопасность школьников в глобальной сети Интернет не только, отражение личностного благополучия человека, но и мощный экономический, трудовой, оборонный потенциал общества и важный индикатор общественного и культурного развития.

В данном исследовании было изучено актуальное состояние действенных социальных механизмов управления информационной безопасностью школьников, использующих глобальную сеть Интернет.

В ходе исследования мы:

1. Изучили сущность социальных механизмов управления информационной безопасности личности.

2. Проанализировали современное состояние развития социальных механизмов управления информационной безопасностью личности.

3. Выявили пути совершенствования социальных механизмов управления информационной безопасностью личности

Таким образом, можно сказать, что основные поставленные цель и задачи были выполнены. Это так же обосновано полученными результатами.

Выяснилось, что школьники по большей части не защищены от опасностей Интернета. Чем ниже возраст ученика, тем он менее осведомлён об угрозах. При этом, чем школьник старше, тем ниже уровень контроля над процессом его выходом в Интернет. Так же существует проблема быстрого роста сайтов, содержащих Интернет-угрозы, их не успевают вовремя блокировать. В обще сложности выход детей в Интернет контролируется менее, чем на 50%. У единиц присутствуют дома фильтры. При этом школьники проводят большое количество времени в Сети. Чаще всего они посещают социальные сети и игры, что является так же самым вероятным местом, где ребенок может быть подвергнут опасности.

Анализ фокус-групп показал, что учителя являются группой лиц, которые хорошо осведомлены о разных видах Интернет-угроз в отличие от

школьников и их родителей. Чтобы это исправить, проводится минимум воспитательных мероприятий и бесед.

При составлении исследования был проведен теоретический анализ педагогической, социологической, психологической литературы по проблемам развития личности и ее социализации в эпоху Интернета. Так же был изучен отечественный и зарубежный опыт обеспечения информационной безопасности школьника. Была изучена готовность современного учителя и родителя к контролю и своевременной ликвидации опасности, возникающей при использовании ресурсов Интернета. Кроме того, проанализированы и обобщены результаты исследовательской работы, определены видов Интернет-угроз, причины их возникновения, меры по профилактике и устранению на уровне школы и родительского контроля.

Анализ анкетирований показал, что пол школьника не сильно влияет на наличие вероятной угрозы по отношению к нему. При этом достаточно сильная связь присутствует между основными проблемными аспектами исследования и возрастом детей.

По итогам экспертных интервью видно, что школьники являются основной возрастной категорией, подверженной сетевым опасностям. Дети, захваченные беспредельными ресурсами современных технологий, оказываются в ситуации, когда не могут идентифицировать виртуальные риски с реальными. Истории, которые чаще всего доходят до социального педагога и педагога-психолога, связаны с виртуальной агрессией, кибербуллингом. В совокупности с низким уровнем осведомленности детей и их родителей конкретные опасность в Сети представляют скрытую угрозу для школьников.

Каждое учебное заведение (то же можно сказать о воспитании школьников родителями) имеет свои особенности и механизмы управления, которые необходимо учитывать при разработке комплексных механизмов управления информационной безопасностью. Процесс создания системы управления рассматриваемого масштаба носит не самый затяжной характер,

так как начинается не с нуля. Рассмотренный в данной работе подход позволяет существенно ускорить и оптимизировать указанный процесс за счет использования готовых адаптируемых программно-технических решений.

В результате нами были даны рекомендации о проведении различных мероприятий, которые мы разделили на несколько категорий: для администрации города, общеобразовательных организаций и родителей. Каждая из них направлена на решение определенных задач на своем уровне.

Для предотвращения и профилактики Интернет-угроз необходимо:

1. Администрации города ввести особую дисциплину в образовательную программу – медиаобразование, а также популяризировать среди родителей программы-фильтры, созданные для ограничения доступа к информации ненадлежащего содержания. Так же удачным решением будет активное информирование населения через средства массовой информации.

2. Общеобразовательной организации, или конкретнее учителям, выделить три уровня обучения информационной безопасности, соответствующие возрастным категориям обучающихся, для выбора правильных форм и методов воспитания.

3. Родителям создать индивидуальные домашние правила пользования Интернетом, контролировать количество времени, проведенного ребенком в Сети, проводить информативно-воспитательные беседы. Так же стоит контролировать время пребывания в Сети, блокировать нежелательный контент, наладить доверительные отношения с ребенком, чтобы он сам захотел сообщать о любых угрозах и тревогах, связанных с Интернетом.

Помимо этого, неотъемлемой частью успешной ликвидации проблемы является проведение постоянного мониторинга общественного мнения, тематических научных и научно-практических конференций, семинаров, круглых столов, симпозиумов, посвященных механизмам управления информационной безопасностью школьников в Интернете.

В ходе исследования выяснилось, что гипотезы 1, 4 подтвердились полностью. Гипотезы 2, 3 подтвердились частично – низкий уровень осведомленностью проблемой наблюдается у школьников и родителей, а также меры, осуществляемые родителями, по защите ребенка от опасностей в Сети проводятся, но их недостаточно.

Проблема существования действенных социальных механизмов управления информационной безопасностью школьников носит особый, социально значимый характер. Проблема сохранения безопасного информационно-психологического состояния является актуальной как в личностном, так и в общественном плане – именно от вклада в потенциальное формирование каждого гражданина России зависит дальнейшее развитие всей нации.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Федеральный закон от 24.07.1998 г. № 124-ФЗ (ред. от 27.12.2018) «Об основных гарантиях прав ребенка в Российской Федерации» [Электронный ресурс] // Режим доступа к изд.: https://legalacts.ru/doc/federalnyi-zakon-ot-24071998-n-124-fz-ob/. – Систем. требования: IBM PC, Internet Explorer.

2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // Режим доступа к изд.: http://www.consultant.ru/document/cons_doc_LAW_61798/. – Систем. требования: IBM PC, Internet Explorer.

3. Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс] // Режим доступа к изд.: http://www.consultant.ru/document/cons_doc_LAW_108808/. – Систем. требования: IBM PC, Internet Explorer.

4. Стратегия развития информационного общества в Российской Федерации // Российская газета. Федеральный выпуск. – 2008. – № 4591. – С. 37-39.

5. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»: // Собрание законодательства РФ. – 2016. – № 50. – С. 70-74.

6. Асанович, В. Я. Информационная безопасность: анализ и прогноз информационного воздействия [Текст] / В. Я. Асанович, Г. Г. Меньшин. – Минск : Амадея, 2006. – 204 с.

7. Бабанский, Ю. К. Методы обучения в современной общеобразовательной школе [Текст] / Ю. К. Бабанский. – М. : Просвещение, 2003. – 208 с.

8. Балуев, Д. Г. «Серые зоны» мировой политики. Очерки текущей политики [Текст] / Д. Г. Балуев, А. А. Новоселов; отв. ред. М. А. Троицкий. –

М. : Научно-образовательный форум по международным отношениям, 2016. – Вып. 3. – С. 14-15.

9. Бармен, С. Разработка правил информационной безопасности [Текст] / С. Бармен. – М. : Вильямс, 2002. – 208 с.

10. Бачило, И. Л. Информационные ресурсы развития Российской Федерации: правовые проблемы [Текст] / И. Л. Бачило. – М., 2003. – 26 с.

11. Березина, Т. Н. Об эмоциональной безопасности образовательной среды [Текст] / Т. Н. Березина // Психология и психотехника. – 2013. – № 9. – С. 897-902.

12. Беспалько, В. П. Основы теории педагогических систем [Текст] / В. П. Беспалько. – Воронеж : Изд-во Воронежского университета, 1977. – 240 с.

13. Бордовский, В. А. Инновационные процессы в современной системе высшего педагогического образования [Текст] / В. А. Бордовский. – СПб. : Изд-во РГПУ, 2010. – 52 с.

14. Борисов, М. А. Основы организационно-правовой защиты информации [Текст] / М. А. Борисов, О. А. Романов. – М. : Книжный дом «ЛЕНАНД», 2014. – 248 с.

15. Бочаров, М. И. Комплексное обеспечение информационной безопасности школьников [Текст] / М. И. Бочаров. – М. : ДМК Пресс, 2009. – 310 с.

16. Браун, С. «Мозаика» и «Всемирная паутина» для доступа к Internet: пер. с англ. [Текст] / С. Браун. – М. : Мир, Малип, СК Пресс, 1996. – 167 с.

17. Веряев, А. А. Семиотический подход к образованию в информационном обществе : монография [Текст] / А. А. Веряев. – Барнаул : Изд-во БГПУ, 2000. – 298 с.

18. Винер, Н. Кибернетика и общество [Текст] / Н. Винер. – М. : ИЛ, 1958. – 200 с.

19. Войскунский, А. Е. Интернет и личность [Текст] / А. Е. Войскунский, Ю. Д. Бабаева, О. В. Смыслова. – СПб. : Тезисы докладов Международной конференции «Интернет.Общество.Личность», 1999. – 376 с.

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

21. Гаврилов, Э. П. Коммерческая тайна и результаты интеллектуальной деятельности [Текст] / Э. П. Гаврилов // Патенты и лицензии. – 2012. – № 4. – С. 19-23.

22. Галицкий, А. В. Защита информации в сети – анализ технологий и синтез решений [Текст] / А.В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – М. : ДМК Пресс, 2004. – 616 с.

23. Гилстер, П. Новый навигатор Internet; пер. с англ. [Текст] / П. Гилстер – Киев : Диалектика, 1996. – 495 с.

24. Глушков, В. М. Основы безбумажной информатики [Текст] / В. М. Глушков. – М. : Наука, 1987. – 552 с.

25. Городов, О. А. Информация как объект гражданского права [Текст] / О. А. Городов // Правоведение. – 2011. – № 5. – С. 80-82.

26. Грачев, Г. В. Информационно-психологическая безопасность личности: теория и технология психологической защиты [Текст]: автореф. дис. … д-ра психол. наук / Г. В. Грачев. – М., 2000. – 56 с.

27. Ершов, А. П. Информатизация: от компьютерной грамотности учащихся к информационной культуре общества [Текст] / А. П. Ершов // Коммунист. – 1988. – №2. – С. 82-92.

28. Ефимова, Л. Л. Информационная безопасность детей. Российский и зарубежный опыт : монография [Текст] / Л. Л. Ефимова, С. А. Кочерга – М. : ЮНИТИ-ДАНА, 2015. – 239 с.

29. Зверева, Е. А. Информация как объект неимущественных гражданских прав [Текст] / Е. А. Зверева // Право и экономика. – 2013. – № 9. – С. 28-33.

30. Игер, Б. Работа в Internet [Текст] / Б. Игер ; под ред. А. Тихонова ; пер. с англ. – М. : БИНОМ, 1996. – 313 с.

31. Информатика в понятиях и терминах [Текст] / Г. А. Бордовский и др. ; под ред. В.А. Извозчикова. – М. : Норма, 2006. – 204 с.

32. Кирмайер, М. Информационные технологии [Текст] / М. Кирмайер. – СПб. : Питер, 2013. – 443 с.

33. Колесников, О. Э. Интернет для делового человека [Текст] / О. Э. Колесников. – М. : МЦФ. Издат. фирма «Яуза», 1996. – 281 с.

34. Коротенков, Ю. Г. Информационная образовательная среда основной школы [Текст] / Ю. Г. Коротенков. – М. : Академия АйТи, 2011. – 152 с.

35. Крол, Э. Все об Internet: Руководство и каталог [Текст] / Э. Крол ; пер. с англ. С.М. Тимачева. – Киев: BNV, 1995. – 591 с.

36. Кузнецов, В. Н. Культура безопасности : тезисы к докладу «Культура безопасности в трансформирующемся обществе» [Текст] / В. Н. Кузнецов // Безопасность Евразии. – М. : октябрь 2002. – 2002. – № 1 (январь-март). – С.126-141.

37. Левин, В. К. Защита информации в информационно-вычислительных системах и сетях [Текст] / В. К. Левин // Программирование. – 1994. – №5. – С. 5-16.

38. Леднев, В. С. Основы теории содержания профессионально-педагогического образования : монография [Текст] / В. С. Леднев, П. Ф. Кубрушко. – М. : Эгвес, 2006. – 287 с.

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

40. Лопатин, В. Н. Информационная безопасность России: Человек, общество, государство [Текст] / В. Н. Лопатин. – М., 2000. – 428 с.

41. Лучинкина, А. И. Информационно-психологическая безопасность детей и подростков в интернет-пространстве [Текст] / А. И. Лучинкина, Т. В. Юдеева // Ученые записки Крымского инженерно-педагогического университета. Серия «Педагогика. Психология». – 2015. – №1. – С. 19-24.

42. Майорова-Щеглова, С. Н. Социологические концепты детства и проблемы информационной безопасности детей [Текст] / С. Н. Майорова-Щеглова // Безопасность детей в информационном пространстве. – М. : Российская гос. детская б-ка, 2014. – С. 43-49.

43. Малых, Т. А. Проблемы информационной безопасности личности [Текст] / Т. А. Малых // Актуальные проблемы права, экономики и управления: материалы междунар. науч.-практ. конф. – Иркутск : СИПЭУ, 2007. – 143 с.

44. Моисеев, А. М. Проблемы и пути совершенствования внутришкольного управления [Текст] / А. М. Моисеев : пособие для руководителей образовательных учреждений. – Тамбов : ТОИПКРО. – 2012. – 331 с.

45. Нольден, М. Ваш первый выход в Internet: Для начинающих пльзователей Internet и широкого круга пользователей PC [Текст] / М. Нольден ; гл. ред. Е. В. Кондукова ; пер. с нем. К. А. Шиндер. – СПб. : ИКС, 1996. – 238 с.

46. Петренко, С. А. Управление информационными рисками [Текст] / С. А. Петренко. – М. : Компания АйТи ; ДМК Пресс, 2004. – 384 с.

47. Привалов, А. Н. Основные угрозы информационной безопасности субъектов образовательного процесса [Текст] / А. Н. Привалов, Ю. И. Богатырева // Известия ТулГУ. Гуманитарные науки. – Тула, 2012. – №3. – С. 427-431.

48. Роберт, И. В. Современные информационные технологии в образовании [Текст] / И. В. Роберт. – М. : Школа-Пресс, 1994. – 41 с.

49. Рогаткин, Д. В. Службы примирения в системе школьного самоуправления [Текст] / Д. В. Рогаткин // Вестник восстановительной юстиции. – 2012. – № 4. – С. 12-33.

50. Родичев, Ю. А. Информационная безопасность: нормативно-правовые аспекты : учебное пособие [Текст] / Ю. А. Родичев. – СПб. : Питер, 2008. – 272 с.

51. Саймон, Д. Как защитить детей от опасностей Интернета [Текст] / Д. Саймон. – М. : НТ Пресс, 2006.

52. Самоделова, Л. А. Изучение основ информационной безопасности в системе дополнительного образования [Текст]: автореф. дис. … канд. пед. наук / Л. А. Самоделова. – М. : Институт содержания и методов обучения РАО, 2005. – 17 с.

53. Сатарова, Н. И. Информационная безопасность школьников в образовательном учреждении : дис. … канд. пед. наук [Текст] / Н. И. Саттарова. – СПб., 2003. – 120 с.

54. Слободчиков, В. И. Образовательная среда: реализация целей образования в пространстве культуры [Текст] / В. И. Слободчиков // Новые ценности образования : культурные модели школы. Вып. 7. Инноватор. Bennet colledge. – М., 1997. – 281 с.

55. Солдатова, Г. Агрессоры и жертвы [Текст] / Г. Солдатова, Е. Зотова // Дети в информационном обществе. – 2012. – №11. – С. 42-51.

56. Солдатова, Г. Роль родителей в повышении безопасности ребенка в интернете : классификация и сопоставительный анализ [Текст] / Г Солдатова, Е. Рассказова // Вопросы психологии. – 2013. – №2. – С. 3-14.

57. Урсул, А. Д. Информатизация общества и переход к устойчивому развитию цивилизации [Текст] / А. Д. Урсул // Вестник РОИВТ. – 1993. – №1-3.– С. 35-45.

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

59. Чашников, Л. А. Современные модели информационно – аналитического обеспечения школьного управления [Текст] / Л. А. Чашников // Вопросы психологии. – 2013. – №9. – С. 36-41.

60. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Текст] / В.Ф. Шаньгин. – М. : ДМК Пресс, 2008. – 544 с.

61. Шеннон, К. Э. Работы по теории информации и кибернетике : сборник статей [Текст] / К. Э. Шеннон ; пер. с англ. под ред. Р. Л. Добрушина, О. В. Лупанова. – М., 1963. – 829 с.

62. Щербаков, А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты [Текст] / А. Ю. Щербаков. – М. : Книжный мир, 2009. – 352 с.

63. Юшина, О. Л. Информационно-психологическая безопасность: библиотековедческий аспект (по материалам зарубежной литературы) [Текст] / О. Л. Юшина // Науч. и техн. б-ки. – 2003. – №11. – С. 32-45.

64. Cornish, P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks [Текст] / P. Cornish // Directorate-General for External Policies of the Union/Policy Department. – Brussels: European Parliament, 2015.

65. Волчинская, Е. К. Место персональных данных в системе информации ограниченного доступа [Электронный ресурс] / Е. К. Волчинская // Право. Журнал Высшей школы экономики. – 2014. – С. 193-205 (Государство и право. Юридические науки). – Научная электронная библиотека «КиберЛенинка» // Режим доступа к изд. : http://cyberleninka.ru/article/n/mesto-personalnyh-dannyh-v-sisteme-informatsii-ogranichennogo-dostupa. – Систем. требования: IBM PC, Internet Explorer.

66. Игнатов, В. С. Пименова, Д. В. Информационное пространство. Структура и функции [Электронный ресурс] / В. С. Игнатов, Д. В. Пименова // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2007. – №3. – С. 3-5 (Общество как система. Социальные отношения и процессы). – Научная электронная библиотека «КиберЛенинка» // Режим

доступа к изд. : http://cyberleninka.ru/article/n/informatsionnoe-prostranstvo-struktura-i-funktsii. – Систем. требования: IBM PC, Internet Explorer.

67. Круль, А. С. Социологические исследования информационных структур социальных систем [Электронный ресурс] / А. С. Круль // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2009. – №4(12). – С. 98-100 (Социология). – Научная электронная библиотека «КиберЛенинка» // Режим доступа к изд. : http://cyberleninka.ru/article/n/sotsiologicheskie-issledovaniya-informatsionnyh-struktur-sotsialnyh-sistem. – Систем. требования: IBM PC, Internet Explorer.

68. Мельникова, М. С. Социальные аспекты интернета : постановка проблемы [Электронный ресурс] / М. С. Мельникова // Известия Российского государственного педагогического университета им. А. И. Герцена. – 2012. – С. 78-81 (Социология). – Научная электронная библиотека «КиберЛенинка» // Режим доступа к изд. : http://cyberleninka.ru/article/n/sotsialnye-aspekty-interneta-postanovka-problemy. – Систем. требования: IBM PC, Internet Explorer.

69. Мелик-Гайказян, И. В. Критерии определения границ в образовательном пространстве [Электронный ресурс] / И. В. Мелик-Гайказян // Высшее образование в России. – 2009. – №10. – С. 81-83 (Философия). – Научная электронная библиотека «КиберЛенинка» // Режим доступа к изд. : http://cyberleninka.ru/article/n/kriterii-opredeleniya-granits-v-obrazovatelnom-prostranstve. – Систем. требования: IBM PC, Internet Explorer.

70. Тухватулина, Л. Р. Принципы классификации моделей коммуникации [Электронный ресурс] / Л. Р. Тухватулина // Вестник Томского педагогического университета. – 2006. – Вып. 7(58). – С. 49-53 (Социология). – Научная электронная библиотека «КиберЛенинка» // Режим доступа к изд. : http://cyberleninka.ru/article/n/printsipy-klassifikatsii-modeley-kommunikatsii. – Систем. требования: IBM PC, Internet Explorer.

ПРИЛОЖЕНИЯ

Приложение 1

ПРОГРАММНО-ИНСТРУМЕНТАЛЬНЫЙ КОМПЛЕКС ИССЛЕДОВАНИЯ «СОЦИАЛЬНЫЕ МЕХАНИЗМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ШКОЛЬНИКОВ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ»

1.1 Методологические основы исследования «Социальные механизмы управления информационной безопасностью школьников в глобальной сети Интернет»

Описание проблемной ситуации. В настоящее время школьники признаются одновременно и частью ноосферы, которая формируется в обществе, и результатом потребления информационного продукта в положительных и отрицательных его тенденциях. В связи с тем, что потребители информационного ресурса молодеют с каждым годом, школьники на данный момент могут выступать как эксперты в процессе всех новообразований, так как они быстрее и глубже осваивают информационную сферу деятельности и коммуникации. По словам специалистов, Интернет-активность пользователей является фундаментальным аспектом в процессе развития информационного общества.

Информатизация как старшего, так и молодого поколения в обществе приобретает тенденцию глобального развития. Фонд «Общественное мнение» провел исследование, по результатам которого выяснилось, что по количеству пользователей Интернета Россия обгоняет Австралию, Испанию, Италию, Францию, Великобританию и Бразилию, и занимает третье место в мире. По сравнению с 2002 годом, когда численность Интернет-пользователей в России составляла 8% (8,7 млн. человек), в 2009 году она увеличилась до 36% (42 млн. человек). А ежедневными пользователями Сети стали 23,9 млн. человек, которых в 2002 году было 2,1 млн. Таким образом, каждый третий житель России является пользователем Интернета, а каждый седьмой - посещает Интернет ежедневно.

Последствия от активного пользования сетью Интернет могут быть положительными и отрицательными по отношению к человеческому физическому и психическому состоянию. Негативное воздействие информационных технологий на психофизическое состояние человека может быть следующим: зависимость, виртуализация жизни, отсутствие круга интересов. Именно неоспоримо растущая информатизация общества в России делает выбранную тему актуальной.

Со сложностью в осознании многогранности влияния Интернета на жизнь сталкиваются в первую очередь школьники. Используя Интернет в основном для учебы и развлечений, несовершеннолетние дети не осознают полного спектра опасностей, исходящих от Сети для их здоровья и развития. В зависимости от количества времени, проведенного в Интернете, появляется вероятность ощутить и его негативное влияние. Но при этом школьникам характерна трудность идентифицировать информацию негативного характера.

Благодаря своим качествам: анонимности, доступности, невидимости, безопасности, простоты использования, Интернет оказывает неоценимую услугу людям, но в то же время может наносить вред детям, не достигшим совершеннолетнего возраста, которые вместо социализации в реальном мире, находят возможность социализации в мире виртуальном.

Проблема исследования заключается в противоречии между тенденцией распространения слабоконтролируемого количества Интернет-угроз и не достаточного числа эффективно организованных мероприятий по защите школьников от них.

Объектом исследования выступают школьники 3-11 классов, родители школьников и учителя города Белгорода.

Предметом исследования является социальные механизмы управления информационной безопасностью школьников в глобальной сети Интернет.

Цель исследования: выявить степень защищенности школьников, использующих глобальную сеть в повседневной жизни, от опасностей в глобальной сети Интернет.

Для достижения поставленной цели необходимо решить следующие **задачи:**

1. Определить уровень информированности школьниками, родителями и учителями об опасностях в Сети.
2. Выявить количество времени, проводимого школьниками в Сети, и цели его использования.
3. Проанализировать полученные данные.
4. Выделить основные формы существующего контроля при выходе ребенка в Интернет.
5. Выявить случаи возникновения и предотвращения Интернет-угроз среди школьников.

Гипотезы исследования:

1. Школьники города Белгорода проводят чрезмерное количество времени в Интернете, тем самым, подвергая себя опасности.
2. Школьники, родители и учителя города Белгорода недостаточно осведомлены о видах Интернет-угроз.
3. Родители и учителя города Белгорода недостаточно контролируют выход школьников в Сеть.
4. Уровень угрозы со стороны агрессоров и мошенников в сети Интернет по отношению к школьникам города Белгорода относительно невысок.

Интерпретация основных понятий.

1. Информация – сведения независимо от формы их представления, получаемые из Интернет-пространства.
2. Интернет – всемирная информационная компьютерная сеть, связывающая между собой как пользователей компьютерных сетей, так и пользователей индивидуальных компьютеров для обмена информацией.
3. Интернет-пространство – это открытое целостное образование, не имеющее четких границ, создаваемое взаимодействующими индивидами, акторами, социальными группами и организациями, объединенными опосредованными социальными взаимосвязями и отношениями при помощи компьютерных и аналогичных им коммуникационных технологий, и соответствующих средств поддержки.
4. Интернет-угроза – вред, нанесенный технике или человеку с помощью глобальной сети Интернет.
5. Интернет-безопасность – это отрасль компьютерной безопасности, связанная специальным образом не только с Интернетом, но и с сетевой безопасностью, поскольку она применяется к другим приложениям или операционным системам в целом. Её цель – установить правила и принять меры для предотвращения атак через Интернет.
6. Кибербуллиннг – это целенаправленный и повторяющийся вред, наносимый кому-то с использованием интернет-технологий, компьютеров, гаджетов и других электронных девайсов.
7. Овершеринг – стремление человека рассказывать окружающим больше, чем стоило бы, перебарщивая с откровенностью и забывая о приватности.
8. Контент – это абсолютно любое информационно значимое либо содержательное наполнение информационного ресурса или веб-сайта.
9. Онлайн – «деятельность», которая доступна исключительно через Интернет.
10. Спам – массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получать.

Операционализация основных понятий.

Таблица 2

Операционализация основных понятий для проведения массового опроса школьников

Качественный показатель	Понятие-индикатор	Вопрос-индикатор
Регулярность и цели использования Сети	Наличие доступа	1. Подключен ли Ваш компьютер (ноутбук) к Интернету? 2. Подключен ли Ваш мобильный телефон к Интернету? 3. Есть ли у Вас доступ к Интернету на компьютере или телефоне?
	Регулярность использования	1. Как часто Вы используете Интернет? 2. Сколько времени Вы проводите за компьютером в день?
	Цели использования	1. Какие сайты Вы посещаете чаще всего?
Осведомленность	Знание понятий	1. Встречали ли вы что-то настораживающее на страницах своих «друзей»?
	Идентификация опасностей	2. О каких из приведенных понятиях Интернет-угроз Вы слышали?
Контроль	Контроль со стороны родителей и учителей	1. Как часто родители следят за тем, чем Вы занимаетесь в Интернете? 2. Заходят ли родители на Вашу страницу в соцсетях? 3. Знают ли родители, с кем Вы «дружите» в соцсетях? 4. Есть ли у Вас скрытая от родителей страница в Интернете? 5. Скрываете ли Вы от родителей, сколько времени проводите в Интернете на самом деле? 6. Объясняли ли Вам в школе, как безопасно пользоваться Интернетом? 7. Объясняли ли Вам родители, как безопасно пользоваться Интернетом? 8. Стоит ли на Вашем компьютере дома фильтр?
Вероятность рисков	1. Кибербуллинг 2. Овершеринг 3. Прочие риски	1. Сталкивались ли Вы с травлей в Интернете? 2. Пренебрегаете ли вы запретом на прочтение/просмотр информации, которая вам запрещена (ограничение по возрасту)? 3. Сообщали ли Вы друзьям, с которыми знакомы только по сети (не в реальной жизни) личную информацию о себе (фамилию, возраст, адрес, номер школы и т.п.)? 4. Встречались ли Вы лично с людьми, с которыми познакомились в Интернете?
Социально-демографический блок	1. Пол 2. Возраст	1. Укажите Ваш пол 2. Укажите Ваш возраст

Таблица 3

Операционализация основных понятий для проведения массового опроса родителей

Качественный показатель	Понятие-индикатор	Вопрос-индикатор
Регулярность и цели использования Сети	Наличие доступа у ребенка	1. Подключен ли компьютер (ноутбук) Вашего ребенка к Интернету? 2. Подключен ли мобильный телефон Вашего ребенка к Интернету? 3. Есть ли у Вашего ребенка доступ к Интернету на компьютере или телефоне?
	Регулярность использования ребенком	1. Как часто Ваш ребенок использует Интернет? 2. Сколько времени Ваш ребенок проводит за компьютером в день?
	Цели использования	1. Какие сайты Ваш ребенок посещает чаще всего?
Осведомленность	Знание понятий	1. О каких из приведенных понятиях Интернет-угроз Вы слышали?
	Идентификация опасностей	2. Встречали ли вы что-то настораживающее на страницах «друзей» ребенка?
Контроль	Контроль со стороны родителей	1. Как часто Вы следите за тем, чем занимается Ваш ребенок в Интернете? 2. Заходите ли Вы на страницу ребенка в соцсетях? 3. Знаете ли Вы, с кем ребенок «дружит» в соцсетях? 4. Объясняли ли Вы ребенку, как безопасно пользоваться Интернетом? 5. Стоит ли на Вашем компьютере дома фильтр?
Вероятность рисков	Наличие рисков	1. Сталкивался ли Ваш ребенок с травлей в Интернете?
Социально-демографический блок	1. Пол 2. Возраст 3. Образование	1. Укажите Ваш пол 2. Укажите Ваш возраст 3. Укажите Ваш уровень образования

1.2 Методические основы исследования «Социальные механизмы управления информационной безопасностью школьников в глобальной сети Интернет»

Определение выборочной совокупности исследования. В ходе исследования было проведено 2 анкетирования, 2 фокус-группы с использованием кейсов и 2 интервью.

При проведении анкетирования в нашем исследовании применялась квотная выборка. Отбор респондентов осуществлялся по методу двухступенчатой квотной выборки, репрезентативной по отношению к социально-демографической структуре населения.

Квотными признаками выступают пол и возраст.

Участниками анкетирования являлись школьники 3-11 классов в возрасте от 9 до 18 лет. Среди школьников в анкетировании приняли участие всего 716 человек. Из них 220 человека учащиеся начальных классов в возрасте 9-10 лет, 284 человек учащиеся

средних классов в возрасте 11-15 лет, 212 человек учащиеся старших классов в возрасте 16-18 лет.

Генеральная совокупность составляет 83739 человек (население области в возрасте от 19 до 17 лет). Объем выборочной совокупности составляет 716 человек.

Таблица 4

Описание генеральной и выборочной совокупности

Генеральная совокупность		Выборочная совокупность	
человек	%	человек	%
83739	100	716	100

Таблица 5

Описание выборочной совокупности по квотному признаку – пол

Генеральная совокупность				Выборочная совокупность			
мужчины		женщины		мужчины		женщины	
человек	%	человек	%	человек	%	человек	%
42728	51	41011	49	347	48	369	52

Таблица 6

Описание выборочной совокупности по квотному признаку – возраст

	Генеральная совокупность		Выборочная совокупность	
	человек	%	человек	%
9-10	20286	24	220	31
11-15	45885	55	284	40
16-17	17568	21	212	29
Итого	83739	100	716	100

Участники фокус-групп были выбраны в соответствии со следующими условиями:

1. Участники принадлежали к одному социальному слою (имели приблизительно равное экономическое положение). Тема информационной безопасностью школьников в глобальной сети Интернет была знакома участникам по повседневному общению или по собственному опыту.

2. Соблюдалась однородность группы по возрасту и образованию.

3. Фокус-группы состояли из 8 и 9 человек в возрасте от 25 до 35 лет.

4. Участники фокус-групп преподавали максимально разные предметные области. Так же они не были знакомы с процедурой проведения данного метода, среди них не было тех, кто получил или получал дополнительное образование социолога, журналиста или психолога.

Участниками интервью стали:

1. Социальный педагог МБОУ СОШ № 7 Сорокина Дарья Геннадьевна, находящаяся на этой должности более 5 лет.

2. Педагог-психолог МБОУ СОШ № 7 Коробенко Юлия Витальевна, находящаяся на этой должности более 10 лет.

Обоснование методов сбора эмпирических данных. Для более детального изучения явления защищенности школьников от угрозы в Сети мы решили использовать проверенные и устоявшиеся в социологии методы исследования: опрос (анкетирование), фокус-группу, интервью.

Опрос – метод социологического исследования, заключающийся в сборе и получении первичных эмпирических сведений об определённых мнениях, знаниях и социальных фактах, составляющих предмет исследования, путём устного или письменного взаимодействия исследователя (интервьюера) и заданной совокупности опрашиваемых (интервьюируемые, респонденты). При проведении исследования будет применяться раздаточный материал в виде анкет. Анкетирования проводятся во внеурочное время со школьниками, на родительских собраниях с родителями. Анкеты не занимают у респондентов слишком много времени, что позволяет им отвечать на вопросы спокойно и полно.

Использование фоку-группы необходимо для того, чтобы респонденты могли не просто отвечать на заранее заготовленные вопросы, но и активно обсуждать заданную тему. Респондентам будут задаваться открытые и закрытые вопросы, при ответе на которые начнется активная дискуссия с участием модератора, который будет направлять ход беседы и следить, чтобы заданная тема не менялась. Данный метод нужно использовать в исследовании для того, чтобы его участники в процессе грамотно направленной дискуссии могли выразить собственное мнение по теме. Данный метод принадлежит к третьему уровню инновационности, поскольку содержит в себе междисциплинарный подход.

Экспертное интервью – метод качественного исследования, одна из разновидностей глубинного интервью, беседа с компетентным специалистом отрасли (экспертом) по определенной теме и интервьюером (модератором). Метод интервью необходим, чтобы подробно заглянуть в глубь проблемы, узнать определенные детали или спорные моменты.

Методы обработки информации.

1. Подготовка данных для обработки:
- выявление и отбор бракованных анкет;
- создание базы данных в программе MS Excel;
- подготовка к расшифровке информации, полученной в ходе проведения фокус-групп и бэкспертного интервью.

2. Обработка данных:
- ввод данных в компьютер посредством программы MS Excel;
- создание таблиц и графиков для последующего анализа данных;
- перенос информации, полученной в ходе фокус-групп и интервью, с аудионосителя в электронный вид.

3. Анализ данных:
- описание полученных данных;
- интерпретация результатов;
- разработка рекомендаций.

Организационный план исследования

Таблица 7

Организационный план исследования

Вид работы	Исполнитель	Сроки выполнения
Выявить мнение школьников о проблеме исследования посредством анкетирования	Опросная группа	Январь, 2019 г.

Продолжение Табл. 7

Вид работы	Исполнитель	Сроки выполнения
Выявить мнение родителей школьников о проблеме исследования посредством анкетирования	Опросная группа	Февраль, 2019 г.
Выявить мнение экспертов о проблеме исследования посредством интервью с экспертами	Опросная группа	Февраль, 2019 г.
Провести фокус-группу с целью выявления мнения населения о проблеме исследования	Руководитель опросной группы	Март, 2019 г.
Проанализировать данные, полученные в ходе контент-анализа и качественного анализа данных	Руководитель опросной группы	Март, 2019 г.
Проанализировать полученные данные	Руководитель опросной группы	Март – апрель, 2019 г.
Интерпретировать результаты	Руководитель опросной группы	Апрель, 2019 г.
Разработать предложения и рекомендации по профилактике Интернет-угроз	Руководитель опросной группы	Апрель – май, 2019 г.

1.3 Апробация инструментария и менеджмент исследования

Пилотажное исследование (апробация инструментария).

Для уточнения формулировок вопросов и ответов опросника, а также для проверки понимания формулировок опросника у целевой группы и нормирования опроса, нами было проведено пилотажное исследование по теме «Социальные механизмы управления информационной безопасностью школьников в глобальной сети Интернет». Был проведен полевой опрос 30 респондентов. В проведении опроса принимал участие 1 анкетер. Далее был произведен анализ результатов интервью с последующим обсуждением реакций респондентов с анкетером.

В ходе пилотажного исследования была выявлена такая проблема как отсутствие конкретики в формулировке вопроса. Вследствие этого были внесены изменения в инструментарий.

Во-первых, вопрос № 1 был разделен на два вопроса, чтобы узнать наличие Интернета и на компьютере, и на мобильном устройстве.

Во-вторых, изменена форма вопроса № 13. Это обосновано тем, что не рекомендуется предлагать детям начальных и средних классов вопрос о конкретных угрозах, как наркотики или педофилия.

В-третьих, вопросы № 12 и № 13 были объединены в один, чтобы исключить пропуск респондентов вопроса.

Протокол пилотажного исследования приведен в Приложении 2. Окончательный список вопросов анкетирование приведен в Приложении 5 и Приложении 6.

Менеджмент исследования. Перед началом исследования необходимо обеспечить для него организационные условия.

Затраты времени. Так как фокус-группа проводится среди сотрудников школ, это сокращает поиски людей. Затраты времени на поиск одного человека – приблизительно полчаса в день.

Учитывая занятость учителей время скорее понадобится на поиск удобного дня для проведения беседы, это еще полчаса в день. Необходимое количество участников наберется через 1×60 мин. = 60мин. (7 ч.). Если учесть возможные отказы, нужно

увеличить время поиска 60×1.1=66 мин. Поиск респондента, соответствующего участию в фокус-группе еще в 1,2 раза: 66×1,2= 79 минут.

Таким образом, ориентировочно 79 минут понадобится на поиск одного человека в день для участия в фокус-группе.

Количество респондентов – 8 и 9 человек. В общей сложности понадобится около 1-2 недели для того, чтобы найти всех подходящих участников. Предполагается провести каждую фокус-группу ориентировочно на 40-50 минут.

Для анкетирования необходимо найти более 700 респондентов среди школьников, более 50 среди родителей и более 30 среди учителей. Анкетирования планируется проводить в строго отведенное для них время: ученикам после уроков 20 минут в день на один класс, родителям на родительских собраниях, учителям во внерабочее время. Примерный срок получения нужного количества анкет равен 1-1,5 месяца.

Поиск участников интервью предположительно занимает 1 неделю, с учетом отказа и загруженности.

Тиражирование материала.

Для проведения фокус-группы и интервью были составлены вопросы в текстовом документе, анкетирования были заранее подготовлены и напечатаны.

Распечатка анкет: для одной анкеты необходимо затратить 0,5 страницы. Печать одной страницы составляет 4 рубля, для одной анкеты необходимо затратить 2 рубль.

1200 х 2 = 2400 – сумма для распечатки анкет для массового опроса школьников и родителей.

Управление рисками исследования.

В ходе любого социологического исследования необходимо предусмотреть возможные риски:

1. Ресурсные риски. Данный вид рисков подразумевает трудности с поиском респондентов, которые отвечают критериям выборки. Для участия в фокус-группах, анкетировании, интервью необходимо найти определенное количество человек, которые могли бы подойти для обсуждения исследуемой темы, на это уйдет достаточное количество временных и трудовых ресурсов.

2. Риски, связанные с технической частью. При проведении фокус-групп или интервью может не сработать диктофон, либо при транскрибировании текста могут возникнуть технические неполадки, которые помешают грамотно расшифровать текст.

3. Риски, связанные с человеческим фактором. Некоторые респонденты могут отвечать на вопросы фокус-групп или анкет неправдиво, поверхностно, не задумываясь, таким образом, давая социально-значимые ответы. В связи с этим, есть риск, что результаты исследования будут не соответствовать реальной картине по проблеме исследования.

4. Риски, связанные с природными факторами. Природные риски не зависят от деятельности человека, в связи с этим мы не можем их предотвратить или избежать.

Приложение 2

ПРОТОКОЛ ПИЛОТАЖНОГО ИССЛЕДОВАНИЯ ПО ТЕМЕ «СОЦИАЛЬНЫЕ МЕХАНИЗМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ШКОЛЬНИКОВ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ»
17.01.2019

Цель проведения пилотажного исследования:

1. Уточнение формулировок вопросов и ответов анкетирования.
2. Проверка понимания формулировок анкетирования у целевой группы.
3. Нормирование опроса (количество респондентов, время одного интервью, количество отказов и т.д.).

Способ проведения пилотажного исследования:

Полевой опрос 30 респондентов с участием 1 анкетера, анализ результатов интервью с последующим обсуждением реакций респондентов с анкетерами.

Основные проблемы, выявленные в ходе пилотажного исследования:

1. Неполная формулировка вопроса
2. Наличие вопросов с недостаточным количеством вариантов ответа

Изменение в инструментарии по итогам пилотажного исследования:

1. Вопрос № 1 «Подключены ли Ваши компьютер и телефон к Интернету?» был разделен на два вопроса: «Подключен ли Ваш компьютер (ноутбук) к Интернету?» и «Подключен ли Ваш мобильный телефон к Интернету?»
2. Из вопроса № 13 для респондентов начальной и средней школы были убраны варианты ответа: наркотики, педофилия, секстинг.
3. Вопросы № 12 «Встречали ли Вы что-то настораживающее на страницах своих друзей?» и № 13 «Что именно Вас встревожило?» были объединены в один: «Встречали ли вы что-то настораживающее на страницах своих «друзей»?», с объединением вариантов ответов.

Приложение 3

ГАЙД ГРУППОВОЙ ДИСКУССИИ ПО ПРОБЛЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ШКОЛЬНИКОВ ГОРОДА БЕЛГОРОДА В СЕТИ ИНТЕРНЕТ

Введение. *Здравствуйте, уважаемые участники беседы! В целях написания выпускной квалификационной работы мы проводим исследование по изучению информационной безопасности школ в глобальной сети Интернет.*

Правила. Теперь давайте определим несколько простых правил для нашей беседы.

1. Не допускать критики в адрес лично кого-то из участников беседы.

2. Не перебивать выступающих, так как говорящим должен быть только один человек.

3. При несогласии с чьей-то точкой зрения необходимо аргументировать свою альтернативную точку зрения, желательно по нескольким пунктам.

4. Ограничивать эгоцентричные высказывания, так как в ходе беседы приветствуются различные точки зрения, причем каждая из которых может быть интересна и иметь научно-практическую значимость.

Мы надеемся, что вы будите придерживаться данных правил и не забывать, что цель нашего исследования выявить многообразие мнений и взглядов на проблему в противоречии между тенденцией распространения слабоконтролируемого количества Интернет-угроз и не достаточного числа эффективно организованных мероприятий по защите школьников от них.

Предполагаемые вопросы для дискуссии, которые могут задаваться модератором после обсуждения кейсов:

I. Какое место занимает Интернет в жизни школьников? *(Вводная дискуссия; длительность – не более 10-15 минут)*

II. Дискуссия по проблемам (40-50 минут)

Эта часть дискуссии посвящена обсуждению конкретных вопросов о влиянии Интернета на школьников.

Вопрос 1. Влияет ли Интернет на образовательный процесс?

Вопрос 2. Определите, какие Интернет-угрозы являются наиболее опасными и почему?

Вопрос 3. Осуществляются ли в школе какие-либо попытки оградить детей от подобного рода опасностей?

Вопрос 4. Влияет ли количество времени, проведенного в Интернете, на уровень опасности ребенка?

Вопрос 5. Посещая какие сайты, школьник наиболее подвержен опасности?

После обсуждения всех вопросов следует дать всем участникам возможность еще раз высказаться в целом по теме исследования. После чего поблагодарить за участие в беседе.

Благодарим за участие в дискуссии!

Приложение 4

КЕКСЫ ДЛЯ ОБСУЖДЕНИЯ В РАМКАХ ФОКУС-ГРУПП

Кейс № 1: в среднеобразовательной школе г. Белгорода в 9 классе учится молодой человек по имени Алексей (имя мальчика изменено из этических соображений), ему 15 лет. Он очень любит онлайн-игры и уже несколько месяцев делает ставки в онлайн-казино. Его привлекает возможность легкого выигрыша, так как он хочет приобрести много молодежных товаров. Первый месяц, делая ставки, он выигрывал по 50, 100 и один раз даже 500 рублей. Но череда удач прошла, и за последние 2 месяца он стал часто проигрывать деньги, которые дают ему родители, а также занимать у своих одноклассников с условием, что он отыграется и вернет, суммы-то небольшие. Подведя подсчеты, одноклассники недовольны безответственность друга и обижаются на то, что долги он еще не вернул. Что вы думаете о сложившейся ситуации? Будут ли какие-либо последствия увлечения Алексея?

Кейс № 2: Маше (имя девочки и название группы изменено из этических соображений) 14 лет, она очень любит читать книги, даже добавилась в группу «КнигоЕд» в социальной сети в Вконтакте. На ее комментарий к посту ответил молодой человек 15 лет, что привело к продолжению общения в личной переписке. Спустя неделю активного общения и обсуждения литературы Данил (имя мальчика изменено из этических соображений) пригласил Машу встретиться недалеко от места, где будет проходить собрание клуба. Маша согласилась и пошла на встречу, её привлекла возможность завести реального друга с такими же интересами как у нее. После встречи ребята подружились и стали хорошо общаться. Как вы думаете, нужно ли делать реальных друзей из виртуальных? Какие причины подтолкнули Машу встретиться с незнакомым человеком?

Приложение 5

АНКЕТА ДЛЯ ПРОВЕДЕНИЯ МАССОВОГО ОПРОСА ШКОЛЬНИКОВ

Участнику исследования!

Уважаемый респондент! Просим Вас принять участие в исследовании на тему «Социальные механизмы управления информационной безопасностью школьников в сети Интернет». Просим Вас ответить на вопросы предложенной анкеты. Для этого следует внимательно прочитать вопрос и варианты ответов, поставить галочку в нужной ячейке.

1. Подключен ли Ваш компьютер (ноутбук) к Интернету?
- Да
- Нет
- Устройство отсутствует
- Другая причина отсутствия подключения

2. Подключен ли Ваш мобильный телефон к Интернету?
- Да
- Нет
- Устройство отсутствует
- Другая причина отсутствия подключения

3. Есть ли у Вас доступ к Интернету на компьютере или телефоне?
- Да
- Нет

4. Как часто Вы используете Интернет?
- Несколько раз в день
- Каждый день или почти каждый день
- Один или два раза в неделю
- Один-два раза в месяц или реже

5. Сколько времени Вы проводите за компьютером в день?
- Один час
- Два часа
- Другое ___

6. Какие сайты Вы посещаете чаще всего? (выберете несколько вариантов ответа)
- Не знаю
- Ютуб
- ГДЗ
- Сайты образовательной тематики
- Погода, новости
- Переводчик
- Соцсети (вконтакте, одноклассники, инстаграм и др.)
- Игры (майнкрафт, ВОВ, дота и др.)
- Унтернет-магазины (алиэкспресс, вайлдберриз и др.)
- Мультфильмы, фильмы

7. Как часто родители следят за тем, чем Вы занимаетесь в Интернете?
- Всегда
- Редко
- Никогда

8. Заходят ли родители на Вашу страницу в соцсетях?
- Да
- Нет
- Не думал(а) об этом

9. Знают ли родители, с кем Вы «дружите» в соцсетях?
- Да
- Нет
- Не думал(а) об этом

10. Есть ли у Вас скрытая от родителей страница в Интернете?
- Да
- Нет
- Не думал(а) об этом

11. Скрываете ли Вы от родителей, сколько времени проводите в Интернете на самом деле?
- Да
- Нет
- Не думал(а) об этом

12. Встречали ли вы что-то настораживающее на страницах своих «друзей»?
- Да
- Нет
- Не обращал(а) внимания
- Люди, которые хотят познакомиться
- Паблики, на которые подписаны
- Посты, которые публикует

13. О каких из приведенных понятиях Интернет-угроз Вы слышали? (выберете несколько вариантов ответа)
- Кибербуллинг
- Овершеринг
- Наркотики
- Педофилия
- Секстинг
- Секты
- Вписки
- Мошенничество
- Другие

14. Сталкивались ли Вы с травлей в Интернете?
- Сам был жертвой травли
- Один из близких друзей был жертвой травли

- Были случаи среди детей школы
- Сам участвовал в травле другого человека
- Таких случаев не было
- Не знаю

15. Пренебрегаете ли вы запретом на прочтение/просмотр информации, которая вам запрещена (ограничение по возрасту)?

- Да
- Часто
- Иногда
- Нет

16. Сообщали ли Вы друзьям, с которыми знакомы только по сети(не в реальной жизни) личную информацию о себе (фамилию, возраст, адрес, номер школы и т.п.)?

- Да, всю или почти всю
- Частично
- Нет

17. Встречались ли Вы лично с людьми, с которыми познакомились в Интернете?

- Да
- Только с тем, кто вызывал доверие
- Нет

18. Объясняли ли Вам родители, как безопасно пользоваться Интернетом?

- Да
- Нет
- Не помню

19. Объясняли ли Вам в школе, как безопасно пользоваться Интернетом?

- Да
- Нет
- Не помню

20. Стоит ли на Вашем компьютере дома фильтр?

- Да
- Нет
- Не знаю

21. Укажите Ваш пол ___

22. Укажите Ваш возраст___

Благодарим Вас за участие в исследовании!

Приложение 6

АНКЕТА ДЛЯ ПРОВЕДЕНИЯ МАССОВОГО ОПРОСА РОДИТЕЛЕЙ ШКОЛЬНИКОВ

Участнику исследования!

Уважаемый респондент! Просим Вас принять участие в исследовании на тему «Социальные механизмы управления информационной безопасностью школьников в сети Интернет». Просим Вас ответить на вопросы предложенной анкеты. Для этого следует внимательно прочитать вопрос и варианты ответов, поставить галочку в нужной ячейке.

1. Подключен ли компьютер (ноутбук) Вашего ребенка к Интернету?
- Да
- Нет
- Устройство отсутствует
- Другая причина отсутствия подключения

2. Подключен ли мобильный телефон Вашего ребенка к Интернету?
- Да
- Нет
- Устройство отсутствует
- Другая причина отсутствия подключения

3. Есть ли у Вашего ребенка доступ к Интернету на компьютере или телефоне?
- Да
- Нет

4. Как часто Ваш ребенок использует Интернет?
- Несколько раз в день
- Каждый день или почти каждый день
- Один или два раза в неделю
- Один-два раза в месяц или реже

5. Сколько времени Ваш ребенок проводит за компьютером в день?
- Один час
- Два часа
- Другое ___

6. Какие сайты Ваш ребенок посещает чаще всего? (выберете несколько вариантов ответа)
- Не знаю
- Ютуб
- ГДЗ
- Сайты образовательной тематики
- Погода, новости
- Переводчик
- Соцсети (вконтакте, одноклассники, инстаграм и др.)
- Игры (майнкрафт, ВОВ, дота и др.)
- Унтернет-магазины (алиэкспресс, вайлдберриз и др.)

- Мультфильмы, фильмы

7. О каких из приведенных понятиях Интернет-угроз Вы слышали? (выберете несколько вариантов ответа)

- Кибербуллинг
- Овершеринг
- Наркотики
- Педофилия
- Секстинг
- Секты
- Вписки
- Мошенничество
- Другие

8. Встречали ли вы что-то настораживающее на страницах «друзей» ребенка?

- Да
- Нет
- Не обращал(а) внимания
- Люди, которые хотят познакомиться
- Паблики, на которые подписаны
- Посты, которые публикует

9. Как часто Вы следите за тем, чем занимается Ваш ребенок в Интернете?

- Всегда
- Редко
- Никогда

10. Заходите ли Вы на страницу ребенка в соцсетях?

- Да
- Нет
- Не думал(а) об этом

11. Знаете ли Вы, с кем ребенок «дружит» в соцсетях?

- Да
- Нет
- Не думал(а) об этом

12. Объясняли ли Вы ребенку, как безопасно пользоваться Интернетом?

- Да
- Нет
- Не помню

13. Стоит ли на Вашем компьютере дома фильтр?

- Да
- Нет
- Не знаю

14. Сталкивался ли Ваш ребенок с травлей в Интернете?

- Сам был жертвой травли
- Один из близких друзей был жертвой травли

- Были случаи среди детей школы
- Сам участвовал в травле другого человека
- Таких случаев не было
- Не знаю

15. Укажите Ваш пол __

16. Укажите Ваш возраст__

17. Укажите Ваш уровень образования_____

Благодарим Вас за участие в исследовании!

Приложение 7

Таблица 8

Распределение ответов на вопрос: «Подключен ли Ваш компьютер (ноутбук) к Интернету?»

Варианты ответов	Абс. число	%
Да	699	97,6
Нет	11	1,5
Устройство отсутствует	4	0,6
Другая причина отсутствия подключения	2	0,3

Таблица9

Распределение ответов на вопрос: «Подключен ли Ваш мобильный телефон к Интернету?»

Варианты ответов	Абс. число	%
Да	665	92,9
Нет	39	5,4
Устройство отсутствует	2	0,3
Другая причина отсутствия подключения	10	1,4

Таблица 10

Распределение ответов на вопрос: «Есть ли у Вас доступ к Интернету на компьютере или телефоне?»

Варианты ответов	Абс. число	%
Да	687	95,9
Нет	29	4,1

Таблица 11

Распределение ответов на вопрос: «Как часто Вы используете Интернет?»

Варианты ответов	Абс. число	%
Несколько раз в день	509	71,1
Каждый день или почти каждый день	177	24,7
Один или два раза в неделю	27	3,8
Один-два раза в месяц или реже	3	0,4

Таблица 12

Распределение ответов на вопрос: «Сколько времени Вы проводите за компьютером в день?»

Варианты ответов	Абс. число	%
Один час	38	5,3
Два часа	73	10,2
Другое	605	84,5

Таблица 13

Распределение ответов на вопрос: «Какие сайты Вы посещаете чаще всего?»

Варианты ответов	Абс. число	%
Не знаю	4	0,6
Ютуб	571	79,7
ГДЗ	82	11,5
Сайты образовательной тематики	321	44,8
Погода, новости	12	1,7
Переводчик	127	17,7
Соцсети (вконтакте, одноклассники, инстаграм и др.)	672	93,9
Игры (майнкрафт, ВОВ, дота и др.)	695	97,1
Унтернет-магазины(алиэкспресс, вайлдберриз и др.)	341	47,6
Мультфильмы, фильмы	314	43,9
Другие	26	3,6

Таблица 14

Распределение ответов на вопрос: «Как часто родители следят за тем, чем Вы занимаетесь в Интернете?»

Варианты ответов	Абс. число	%
Всегда	84	11,7
Редко	367	51,3
Никогда	265	37,0

Таблица 15

Распределение ответов на вопрос: «Заходят ли родители на Вашу страницу в соцсетях?»

Варианты ответов	Абс. число	%
Да	278	38,8
Нет	312	43,6
Не думал(а) об этом	126	17,8

Таблица 16

Распределение ответов на вопрос: «Знают ли родители, с кем Вы «дружите» в соцсетях?»

Варианты ответов	Абс. число	%
Да	162	22,6
Нет	71	9,9
Не думал(а) об этом	483	67,5

Таблица 17

Распределение ответов на вопрос: «Есть ли у Вас скрытая от родителей страница в Интернете?»

Варианты ответов	Абс. число	%
Да	59	8,3
Нет	283	39,5
Не думал(а) об этом	374	52,2

Таблица 18

Распределение ответов на вопрос: «Скрываете ли Вы от родителей, сколько времени проводите в Интернете на самом деле?»

Варианты ответов	Абс. число	%
Да	164	22,9
Нет	445	62,2
Не думал(а) об этом	107	14,9

Таблица 19

Распределение ответов на вопрос: «Встречали ли вы что-то настораживающее на страницах своих «друзей»?»

Варианты ответов	Абс. число	%
Да	109	15,2
Нет	182	25,4
Не обращал(а) внимания	198	27,7
Люди, которые хотят познакомиться	104	14,5
Паблики, на которые подписаны	92	12,9
Посты, которые публикует	31	4,3

Таблица 20

Распределение ответов на вопрос: «О каких из приведенных понятиях Интернет-угроз Вы слышали?»

Варианты ответов	Абс. число	%
Кибербуллинг	369	51,5
Овершеринг	78	10,9
Наркотики	527	73,6
Педофилия	144	20,1
Секстинг	24	3,4
Секты	315	44,0
Вписки	251	35,1
Мошенничество	617	86,2
Другие	47	6,6

Таблица 21

Распределение ответов на вопрос: «Сталкивались ли Вы с травлей в Интернете?»

Варианты ответов	Абс. число	%
Сам был жертвой травли	12	1,7
Один из близких друзей был жертвой травли	54	7,5
Были случаи среди детей школы	9	1,2
Сам участвовал в травле другого человека	2	0,3
Таких случаев не было	213	29,8
Не знаю	426	59,5

Таблица 22

Распределение ответов на вопрос: «Пренебрегаете ли вы запретом на прочтение/просмотр информации, которая вам запрещена (ограничение по возрасту)?»

Варианты ответов	Абс. число	%
Да	56	7,8
Часто	395	55,2
Иногда	231	32,3
Нет	34	4,7

Таблица 23

Распределение ответов на вопрос: «Сообщали ли Вы друзьям, с которыми знакомы только по сети(не в реальной жизни) личную информацию о себе (фамилию, возраст, адрес, номер школы и т.п.)?»

Варианты ответов	Абс. число	%
Да, всю или почти всю	42	5,9
Частично	291	40,6
Нет	383	53,5

Таблица 24

Распределение ответов на вопрос: «Встречались ли Вы лично с людьми, с которыми познакомились в Интернете?»

Варианты ответов	Абс. число	%
Да	87	12,2
Только с тем, кто вызывал доверие	192	26,8
Нет	437	61,0

Таблица 25

Распределение ответов на вопрос: «Объясняли ли Вам родители, как безопасно пользоваться Интернетом?»

Варианты ответов	Абс. число	%
Да	264	36,9
Нет	293	40,9
Не помню	159	22,2

Таблица 26

Распределение ответов на вопрос: «Объясняли ли Вам в школе, как безопасно пользоваться Интернетом?»

Варианты ответов	Абс. число	%
Да	579	80,9
Нет	28	3,9
Не помню	109	15,2

Таблица 27

Распределение ответов на вопрос: «Стоит ли на Вашем компьютере дома фильтр?»

Варианты ответов	Абс. число	%
Да	144	20,1
Нет	198	27,7
Не знаю	374	52,2

Таблица 28

Распределение ответов на вопрос: «Укажите Ваш пол»

Варианты ответов	Абс. число	%
Женский	369	51,5
Мужской	347	48,5

Таблица 29

Распределение ответов на вопрос: «Укажите Ваш возраст»

Варианты ответов	Абс. число	%
9-10 лет	220	30,7
11-15 лет	284	39,7
16-17 лет	212	29,6

Таблица 30

Распределение ответов на вопрос: «Как часто Ваш ребенок использует Интернет?»

Варианты ответов	Абс. число	%
Несколько раз в день	301	74,9
Каждый день или почти каждый день	83	20,6
Один или два раза в неделю	16	4,0
Один-два раза в месяц или реже	2	0,5

Таблица 31

Распределение ответов на вопрос: «Сколько времени Ваш ребенок проводит за компьютером в день?»

Варианты ответов	Абс. число	%
Один час	162	40,3
Два часа	94	23,4
Другое	146	36,3

Таблица 32

Распределение ответов на вопрос: «Как часто Вы следите за тем, чем занимается Ваш ребенок в Интернете?»

Варианты ответов	Абс. число	%
Всегда	60	14,9
Редко	189	47,0
Никогда	153	38,1

Таблица 33

Распределение ответов на вопрос: «О каких из приведенных понятиях Интернет-угроз Вы слышали?»

Варианты ответов	Абс. число	%
Кибербуллинг	269	66,9
Овершеринг	74	18,4
Наркотики	402	100,0
Педофилия	402	100,0
Секстинг	113	28,1
Секты	402	100,0
Вписки	138	34,3
Мошенничество	402	100,0
Другие	8	2,0

Таблица 34

Распределение ответов на вопрос: «Сталкивался ли Ваш ребенок с травлей в Интернете?»

Варианты ответов	Абс. число	%
Сам был жертвой травли	8	2,1
Один из близких друзей был жертвой травли	27	6,7
Были случаи среди детей школы	9	2,2
Сам участвовал в травле другого человека	5	1,2
Таких случаев не было	126	31,3
Не знаю	227	56,5

Таблица 35

Распределение ответов на вопрос: «Объясняли ли Вы ребенку, как безопасно пользоваться Интернетом?»

Варианты ответов	Абс. число	%
Да	185	46,0
Нет	121	30,1
Не помню	96	23,9