ПРИНЯТО
Педагогическим Советом
МОУ «Средняя школа № 5»
протокол № 1 от «30» 08. 2023 г.

УТВЕРЖДЕНО
Приказом №75-ос от «01» 09. 2021 г.
Директор МОУ «Средняя школа №5»
_____М.Г. Аверкин
М.П.

СОГЛАСОВАНО
Председатель Управляющего
Совета МОУ «Средняя школа № 5»
_____/ Е.В. Маланьина
протокол № 8 от «25» 08. 2023 г.

Учтено мнение Совета обучающихся
Протокол № 2 от «25» 08. 2023 г.

Учтено мнение Совета родителей
Протокол № 2 от «25» 08. 2023 г.

Дополнительная общеобразовательная (дополнительная общеразвивающая) программа «КИБЕРБЕЗОПАСНОСТЬ»

на 2023-2024 учебный год

Направленность: социально-педагогическая
Уровень программы: ознакомительный
Возраст обучающихся: 11-16 лет
Срок реализации программы: 1 год (34 часа)
Форма обучения: очная
Язык обучения: русский

Автор-составитель:
Чернавский А.В.,
учитель информатики

Саранск, 2023

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Актуальность

Социальная среда, в которой растут современные дети, сильно отличается от той, что формировала их родителей. Цифровые технологии проникают во все сферы жизни. На наших глазах формируется цифровое общество, и одним из важных факторов социализации в нём становится Интернет.

Компьютер, подключённый к Сети, — влиятельный посредник между взрослым миром и детьми. Сегодня в значительной степени благодаря ему расширяется зона ближайшего развития ребёнка — область не созревших, а только созревающих психических функций, его образовательный потенциал. Понятие зоны ближайшего развития было предложено известным отечественным психологом Л.С. Выготским и активно используется как в российской, так и в зарубежной детской психологии. В условиях цифрового общества зона ближайшего развития определяется не только непосредственным взаимодействием ребёнка со взрослым, но и многочисленными взаимодействиями с миром, представленным в Интернете.

Отличительной особенностью социализации в Интернете является её стихийный, неконтролируемый характер. Зачастую современные дети осваивают цифровые технологии самостоятельно, без присмотра со стороны взрослого. Родители чувствуют себя гораздо спокойнее, когда их ребёнок сидит за компьютером в соседней комнате, нежели когда он «пропадает неизвестно где»; они полагают, что таким образом он избегает негативного влияния «улицы», недооценивая при этом риски, связанные с цифровой социализацией. Однако Интернет — это та же «улица» протяжённостью в миллионы гигабайтов, и там ребёнок, предоставленный самому себе, может повстречаться с разными ситуациями.

Попадая в Интернет из самых защищённых и безопасных мест — из дома или школы, — дети и подростки относятся к киберпространству с большим доверием. Способность оценить степень опасности той или иной среды приходит с жизненным опытом, это он учит нас предвосхищать нежелательные последствия тех или иных действий, вовремя оценивать разного рода угрозы. Юный пользователь, захваченный безграничными возможностями современных технологий, подобен очарованному страннику: он не может разглядеть риски, которые встречаются в Сети, и оказывается одним из самых незащищённых и уязвимых её пользователей. Когда он понимает, что столкнулся в Сети

с непосредственной опасностью, то часто не знает, как поступить и к кому обратиться за помощью, и вынужден учиться на собственных ошибках.

Взрослым важно понимать, что риски онлайн-среды связаны не только с содержанием тех или иных интернет-сайтов, от знакомства с которыми ребёнка следует уберечь. Немалую опасность представляет сам стихийный и неконтролируемый процесс освоения цифрового мира. Как отмечал Л.С. Выготский, обучение должно идти впереди развития. Для того чтобы ребёнок мог безопасно осваиваться в киберпространстве, ему нужен проводник, и стать такими проводниками должны в первую очередь родители и учителя. Только в совместной деятельности со взрослыми (и в школе, и дома) процесс цифровой социализации детей может приобрести систематический целенаправленный характер.

В соответствии с Федеральными государственными образовательными стандартами обучение в школе осуществляется с использованием современных технологий. На школе лежит ответственность за развитие у детей цифровой компетентности и обучение их навыкам безопасной работы в киберпространстве. Эти направления работы — необходимое условие развития в школе информационной образовательной среды. Стимулируя детей к освоению разных видов деятельности в Сети и одновременно обучая их критически оценивать интернет-ресурсы, развивая навыки безопасного поведения в киберпространстве, мы увеличиваем преимущества, которые даёт обучение с использованием Интернета.

В широком смысле задача взрослых состоит в воспитании «цифрового гражданина*, который, с одной стороны, обладает определёнными техническими навыками и компетенциями, с помощью которых он может осуществлять поиск и работу с информацией, налаживать эффективную коммуникацию с другими пользователями Сети, а с другой — использует цифровые технологии безопасно, ответственно и критично.

Таким образом, высокая востребованность методических пособий и обучающих программ по формированию и повышению цифровой компетентности определяется следующими факторами:

• Интернет — неотъемлемая часть жизни нового поколения и важный фактор социализации современных детей и подростков;

• дети и подростки активно используют Интернет в образовательных целях, и значительная часть родителей осознаёт образовательный потенциал Интернета;

• требования современной технологически оснащённой среды мотивируют детей и

подростков к повышению своей цифровой компетентности;

• уровень цифровой компетентности современных подростков не может обеспечить эффективное, ответственное и безопасное использование Интернета;

• абсолютное большинство детей и подростков учатся использовать Интернет самостоятельно и бессистемно;

• современная школа естественным образом становится местом, где происходит цифровая социализация детей и подростков, овладение навыками безопасного использования Интернета.

Цели и задачи курса

Цель курса «Кибербезопасность» — повышение цифровой компетентности школьников и расширение возможностей полезного, критичного, ответственного и безопасного использования Интернета.

Данный курс предполагает решение следующих задач:

• расширить у обучающихся 5-9 классов диапазон возможностей, связанных с использованием цифровых технологий;

• способствовать осознанию школьниками влияния, которое цифровые технологии оказывают на их образ жизни;

• расширить представления обучающихся о возможностях Интернета как источника информации, инструмента коммуникации и потребления;

• познакомить обучающихся с возможными онлайн-рисками (техническими, контентными, коммуникационными, потребительскими и риском интернет-зависимости);

• способствовать формированию устойчивых стратегий своевременного распознавания онлайн-рисков и безопасного поведения при столкновении с ними, сформировать навыки успешного разрешения проблемных ситуаций в Сети, защиты своих персональных данных и управления ими;

• способствовать формированию у обучающихся адекватного образа цифровых технологий, предлолагающего, с одной стороны, понимание их позитивной роли в развитии человеческой цивилизации, а с другой — критическую оценку влияния цифровых технологий на разные стороны жизнедеятельности человека;

• способствовать формированию критического мышления, творческого мышления и креативности, способности к рефлексии, навыков сотрудничества.

Нормативно-правовая база курса

1. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».
2. Федеральный закон от 27 июля 2006 г. 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон № 152-ФЗ от 27 июля 2006 г. «О персональных данных».
4. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
5. Указ Президента Российской Федерации от 29 мая 2017 г. № 240 «Об объявлении в Российской Федерации Десятилетия детства».
6. Указ Президента Российской Федерации от 1 декабря 2016 г. № 642 «О Стратегии научно-технологического развития Российской Федерации».
7. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 гг.».

Формы деятельности

Курс «Кибербезопасность» организован в соответствии с системно-деятельностным подходом к обучению, предполагает применение активных методов, совместную работу обучающихся и учителя, поиск информации в разных источниках, творческий подход к решению учебных задач.

Занятия включают аудиторную и самостоятельную работу. В рамках каждого тематического модуля предполагается вступительная лекционная часть, подготовленная учителем (ведущим курса) на основе информации, которую он сможет найти в методических рекомендациях, дополнительной литературе и интернет-источниках (см. список литературы и интернет-источников).

На занятиях используются учебные пособия — тренажёры. Задания, представленные в учебных пособиях, рассчитаны на разные формы работы — индивидуальную, в парах, в малых и больших группах. Задания могут выполняться в тетради, с использованием цифровых устройств и в интерактивной форме. По усмотрению учителя некоторые задания могут быть выполнены в формате конференций, круглых столов, выставок, конкурсов. Каждое задание в тренажёре обозначено иконкой, соответствующей его формату.

Для создания позитивной атмосферы и повышения мотивации обучающихся при

освоении курса в учебные пособия введён сквозной персонаж — «персональный помощник» (в 5-6 классах это Кибернешка, в 7-8 классах — магистр Кибер Нетов, в 9 классе — профессор Кибер Нетович). Текст тренажёров оформлен как «посты» персонального помощника в социальной сети. В начале каждого тренажёра персональный помощник даёт информационно-мотивационную справку об Интернете и о курсе «Кибербезопасность» и знакомит читателей с основными рубриками своих «постов». Названия рубрик оформлены как хэштеги в социальной сети. В задания также введены сквозные персонажи — школьники: Гоша Геймеров, Рита Картинкина и Игорь Неюзеров. Характеры этих персонажей соответствуют разным типам пользователей. Гоша Геймеров — «любитель игр», для него Интернет в первую очередь место для онлайн-игр. Рита Картинкина — «общительный пользователь», для неё Интернет — место для общения и самопрезентапии. Игорь Неюзеров — «любознательный пользователь», для него Интернет прежде всего служит источником информации.

Внеурочный курс «Кибербезопасность» могут вести учителя, классные руководители, педагоги-психологи, социальные педагоги, педагоги дополнительного образования.

Предполагаемые результаты

Курс позволяет формировать *универсальные учебные действия* (УУД) в соответствии с требованиями Федерального государственного образовательного стандарта основного общего образования, а именно: личностные, регулятивные, коммуникативные, познавательные.

В блок *личностных УУД* входят когнитивный, эмоционально-ценностный и деятельностный компоненты.

Сформированный *когнитивный компонент* обеспечивает наличие у обучающихся знаний основных прав и обязанностей пользователя Интернета в соответствии с законами РФ. Обучающиеся должны научиться ориентироваться в системе моральных норм и ценностей, а также в особенностях взаимоотношений и культуры поведения в онлайн-среде. Обучающиеся осваивают культуру общения в Интернете, учатся способствовать формированию культуры поведения в онлайн-среде среди сверстников. Обучающиеся смогут оценивать поступающую онлайн-информацию, исходя из нравственных и этических норм. Они смогут проводить рефлексию своей деятельности и осознают ответственность за результаты этой деятельности.

Сформированность *эмоционально-ценностного компонента* проявляется в

доброжелательном отношении к другим пользователям Интернета, нетерпимости к любым формам агрессивного и противоправного поведения в Интернете и готовности противостоять им, а также уважении к общечеловеческим ценностям, готовности к распространению их в онлайн-среде. У обучающихся развивается потребность в развитии своей личности, самореализации в соответствии с ценностями и нормами, в том числе в онлайн-среде, чему способствует разработка, реализация и участие Е различных социальных проектах, а также в других видах деятельности, предлагаемых в рамках курса. Обучающиеся осознают смысл овладения цифровыми технологиями.

Деятельностный компонент выражается в готовности и способности обучающегося к участию в различных видах онлайн-деятельности, способствующих личностному развитию; в осознанном соответствии социально одобряемым нормам поведения по отношению к взрослым и сверстникам в различных онлайн-контекстах. У школьников появляется потребность участвовать в онлайн-деятельности, способствующей личностному развитию.

К блоку личностных УУД также относятся *основы социальных компетенций*, включая ценностно-смысловые и моральные установки, опыт социальных и межличностных отношений с учётом особенностей онлайн-среды.

К *регулятивным, УУД* относятся сформированные у обучающихся в результате освоения данного курса умение ставить цели, задачи, планировать их реализацию и выбирать эффективные пути их достижения; умение выбирать оптимальные способы разрешения проблемных ситуаций, возникающих при использовании Интернета, что особенно важно при осуществлении деятельности, направленной на обеспечение личной безопасности в Интернете.

К *коммуникативным УУД* в контексте данного курса относятся умение учитывать мнение других пользователей при взаимодействии с ними в онлайн-среде; стремление к кооперации, компромиссу, конструктивному взаимодействию; умение устанавливать контакт в онлайн-общении; умение конструктивно разрешать конфликтные ситуации (выявлять, идентифицировать проблемы, искать и оценивать способы разрешения конфликта, принимать решения и реализовывать их); умение планировать взаимодействие (определять цели, способы взаимодействия) с учётом особенностей онлайн-коммуникации.

В рамках курса формируются такие *познавательные УУД*, как умение формулировать

познавательную цель при пользовании Интернетом и цифровыми технологиями; умение искать информацию; умение анализировать информацию с целою выделения существенных и несущественных признаков; умение синтезировать информацию; умение критически оценивать достоверность информации; умение выбирать основания и критерии для сравнения информации, устанавливать причинно-следственные связи, выстраивать логические цепи рассуждений, выдвигать гипотезы и их обоснование.

В логике достижения образовательных результатов, соответствующих требованиям ФГОС, по итогам освоения курса у обучающихся должен появиться опыт учебно-исследовательской и проектной деятельности в онлайн-среде. У обучающихся возникнут познавательные интересы в области цифровых технологий.

Во время изучения внеурочного курса «Кибербезопасность» формируются *ИКТ-компетенции:* умение строить поисковые запросы в онлайн-источниках и находить релевантную информацию, анализировать, сопоставлять, обобщать, интерпретировать и систематизировать информацию, оценивать её достоверность, умение сохранять и передавать информацию, в том числе в форме гипермедиа (текст, изображение, звук, ссылки между разными информационными компонентами), при соблюдении правил кибербезопасности. Приобретённые компетенции позволят более эффективно осваивать программы основных учебных курсов.

Курс состоит из семи смысловых модулей, которые представлены в каждом классе. Работа над каждым модулем способствует формированию определённого набора компетенций.

Модуль 1. Цифровой мир и интернет-зависимость. Формируется способность и готовность к *осознанному, ответственному и безопасному освоению и использованию Интернета и цифровых устройств,* а именно способность и готовность:

• ответственно выбирать оптимальные и безопасные пути освоения цифровых технологий, Интернета и цифровых устройств;

• понимать и адекватно использовать возможности, предоставляемые Интернетом и цифровыми технологиями, в соответствии с этическими нормами и текущим законодательством РФ;

• понимать и адекватно оценивать риски, возникающие в процессе освоения Интернета и цифровых технологий;

• находить оптимальные способы решения проблем, возникающих в процессе освоения

Интернета и цифровых технологий;

• оценивать количество личного времени, проводимого за использованием Интернета и цифровых устройств, и качество содержательного наполнения этого времени;

• ответственно и сбалансированно распределять личное время, в том числе отводимое на использование цифровых технологий;

• оценивать наличие признаков чрезмерного использования Интернета и цифровых устройств;

• находить адекватные, оптимальные пути решения проблемы чрезмерного использования Интернета и цифровых устройств.

Модуль 2. Техносфера и технические риски. Формируется способность и готовность к *ответственному и безопасному использованию средств подключения к Интернету и программного обеспечения, связанного с работой в Интернете, а именно способность и готовность:*

• ответственно и безопасно использовать различные способы подключения к Интернету и возможности их настройки в соответствии с текущими задачами, а также осваивать новые средства связи;

• ответственно и безопасно использовать современное программное обеспечение для работы в Интернете и возможности их настройки в соответствии с текущими задачами, а также осваивать новое программное обеспечение;

• ответственно и безопасно относиться к конфиденциальности личных данных в Интернете и уметь защищать их от несанкционированного доступа;

• ответственно и безопасно использовать программные средства для защиты технических устройств от вирусов;

• оценивать основные риски, связанные с различными способами подключения к Сети, использованием локальных и облачных приложений для работы в Интернете, аутентификацией в Интернете, использованием антивирусных средств для защиты технических устройств.

Модуль 3. **Информация и контентные риски.** Формируется способность и готовность *ответственно и безопасно обращаться с информацией в Интернете (искать. оценивать, создавать, размещать, потреблять и распространять информационный контент),* а именно способность и готовность:

• ответственно и безопасно использовать различные поисковые системы и их

возможности для поиска в Интернете информации, необходимой для решения различных жизненных задач, в том числе образовательных;

• оценивать качество информации и информационных ресурсов в Интернете, в том числе их достоверность, надёжность, безопасность, а также потенциальные риски, связанные с их использованием и распространением;

• ответственно и безопасно использовать различные интернет- ресурсы для создания и размещения в Интернете оригинальной позитивной информации (мультимедиа, текстов, сайтов и т.д.);

• ответственно и безопасно потреблять и распространять информацию в соответствии с этическими нормами, текущим законодательством РФ в области авторского права и защиты детей от информации, причиняющей вред их здоровью и развитию;

• оценивать основные риски использования информации в Интернете, связанные с поиском и оценкой достоверности и надёжности информации, созданием и размещением информационного контента, распространением в Сети противозаконной информации, угрожающей здоровью и развитию детей и подростков.

Модуль 4. Общение и коммуникационные риски. Формируется способность и готовность *использовать ресурсы Интернета для ответственной и безопасной коммуникации*, а именно способность и готовность:

• ответственно и безопасно взаимодействовать с другими пользователями на различных интернет-ресурсах (в социальных сетях) в соответствии с общечеловеческими нормами поведения, текущим законодательством РФ, правилами конкретного интернет-ресурса, а также в зависимости от оценки сложившейся ситуации:

• ответственно и безопасно выбирать стратегии коммуникации, в том числе самопрезентации, на различных интернет-ресурсах (в социальных сетях) в зависимости от вида ресурса, целей коммуникации и целевой аудитории;

• ответственно и безопасно управлять собственной репутацией (формировать, поддерживать, защищать) и социальным капиталом в Интернете;

• адекватно оценивать риски, возникающие в процессе коммуникации в Интернете (в случае встречи с незнакомцами, проявления агрессии и т.д.), а также выбирать безопасные стратегии поведения в ситуациях, связанных с этими рисками;

• ответственно и безопасно выбирать стратегии поведения при столкновении с проявлениями агрессии (с троллингом, кибербуллингом и т.д.) в Интернете.

Модуль 5. Цифровая экономика и потребительские риски. Формируется способность и готовность *ответственно и безопасно потреблять товары и услуги*, представленные на различных интернет-ресурсах, в соответствии с текущим законодательством РФ и правами потребителей, а именно способность и готовность:

- использовать различные интернет-ресурсы для поиска информации о необходимых товарах и услугах;
- оценивать качество продуктов, предоставляемых на различных интернет-ресурсах, а также потенциальные риски, связанные с их потреблением;
- оценивать достоверность информации, представленной на различных рекламных носителях в Интернете;
- ответственно и безопасно использовать интернет-ресурсы, соблюдая пользовательские соглашения и общие правила безопасности;
- изучать и реализовывать права потребителей в соответствии с текущим законодательством РФ.
- оценивать основные потребительские риски, связанные с приобретением и потреблением товаров и услуг, представленных на различных интернет-ресурсах, распространением рекламы в Интернете, различными видами мошенничества в Интернете (в том числе фишингом), различными видами онлайн-игр (многопользовательских, социальных, каузальных).

Модуль 6. Персональные данные. Формируется способность и готовность *самостоятельно, в соответствии с актуальными жизненными задачами, защищать персональные данные с помощью технических и программных приёмов и средств, устанавливать границы собственной приватности и управлять репутацией в Сети*, а именно способность и готовность:

- различать виды персональных данных и понимать последствия небрежного обращения с ними, способы их попадания в Интернет и дальнейшего распространения в Сети;
- уметь пользоваться различными средствами управления персональными данными и приватностью в Интернете;
- ответственно и безопасно использовать методы защиты конфиденциальных персональных данных от несанкционированного доступа;
- ответственно и безопасно использовать специальные безопасные режимы работы в

браузерах;

• ответственно и безопасно использовать приёмы, позволяющие контролировать распространение персональных данных в Интернете, а также удалять следы онлайн-активности с различных устройств и онлайн-ресурсов;

• ответственно и безопасно использовать настройки приватности в социальных сетях и на других онлайн-ресурсах;

• ответственно и безопасно использовать механизмы обращения в службу технической поддержки разработчиков устройств, приложений, онлайн-ресурсов, в общественные и государственные организации;

• оценивать основные риски, связанные с предоставлением и распространением персональных данных.

Модуль 7. Цифровое будущее. Формируются *позитивный образ цифровых технологий и цифрового будущего, активная субъектная позиция и ценностное отношение к личному будущему, а также способность и готовность к конструктивной социализации в условиях цифрового общества*, что выражается в способности и готовности:

• разбираться в изменениях, которые происходят в технологической и социальной сферах;

• понимать, адекватно и ответственно использовать возможности, которые появляются благодаря новым технологиям;

• понимать и адекватно оценивать риски, возникающие вследствие изменений в технологической и социальной сферах;

• находить личные жизненные ориентиры, соответствующие нравственным и этическим нормам;

• создавать и планировать жизненный план в условиях цифрового общества и с учётом происходящих изменений;

• реализовать личностный потенциал в условиях цифрового общества;

• выбирать и планировать адекватный и оптимальный путь реализации личностного потенциала и жизненного плана в условиях цифрового общества и с учётом происходящих изменений.

Литература

Основная литература

1. *Солдатова Г.У.* Цифровая социализация в культурно-исторической парадигме: изменяющийся ребёнок в изменяющемся мире // Социальная психология и общество. 2018. Т. 9. С. 71-80.

2. *Солдатова Г.У., Рассказова Е.И., Пестик ТЛ.* Цифровое по*коление России: компетентность и безопасность. М.: Смысл, 2017.*

URL:http://detionline.com/assets/files/research/2017cifrovoe_pokolenie_rossii.pdf (дата обращения: 18.06.2020).

3. *Солдатова Г.У., Пестик ТЛ., Рассказова Е.И., Зотова Е.Ю.* Цифровая компетентность подростков и родителей. Результаты всероссийского исследования. М.: Фонд Развития Интернет, 2013. URL: http://detionline.com/assets/files/research/ DigitalLiteracy.pdf (дата обращения: 18.06.2020).

4. *Солдатова Г., Рассказова Е., Зотова Е., Лебешева М., Роггендорф П.* Дети России онлайн: риски и безопасность. Результаты международного проекта EU Kids Online II в России. URL: http://detionline.com/assets/files/helpline/RussianKidsOnline_Final% 20ReportRussian.pdf (дата обращения: 18.06.2020).

5. *Солдатова Г.У., Чигарькова С.В.. Дренёва АЛ., Илюхина С.П.* Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодёжи в Интернете: учебно-методическое пособие. М.: Когито-Центр, 2019. URL: http://detionline. com/assets/files/research/my_v_otvete_za_cifrovoy_mir.pdf (дата обращения: 18.06.2020).

6. *Солдатова Г., Зотова Е., Лебешева М., Шляпников В.* Интернет: возможности, компетенции, безопасность: методическое пособие для работников системы общего образования. Ч. 1.

Лекции. М.: Центр книжной культуры «Гутенберг», 2013. URL: http://detionline.com/assets/files/research/BookTheorye.pdf (дата обращения: 18.06.2020).

7. *Солдатова Г., Зотова Е,, Лебешева М., Шляпников В.* Интернет: возможности, компетенции, безопасность: методическое пособие для работников системы общего образования. Ч. 2. Практикум. М.: Центр книжной культуры «Гутенберг», 2013. URL: http://detionline.com/assets/files/research/Book_Praktikum.pdf (дата обращения: 18.06.2020).

8. *Солдатова Г.У., Приезжева АА, Олькина О.И., Шляпников В.Н.* Практическая психология безопасности. Управление персональными данными в интернете: учебно-

методическое пособие для работников системы общего образования. 2-е. изд., испр. и доп. М.: Генезис, 2017. URL: http://detionline.com/assets/files/ research/Internet-bezopasnost.pdf (дата обращения: 18.06.2020).

Дополнительная литература

1. *Блау М.* Удивительный интернет. М.: Энас-книга, 2016. С. 432.

2. *Бочавер АА., Хломов К.Д.* Буллинг как объект исследований и культурный феномен // Психология. Журнал высшей школы экономики.2013. Т.10. № 3.

3. *Бочавер АА., Хломов КД.* Кибербуллинг: травля в пространстве современных технологий // Психология. Журнал высшей школы экономики. 2014. Т. 11. № 3.

4. *Голубева НА., Марцинковская Т.Д.* Информационная социализация: психологический подход // Психологические исследования: электронный научный журнал. 2011. № 6. С. 2.

5. *Голубева НА., Марцинковская ТД.* Социализация современных подростков: информационный контекст // Вопросы психологии. 2016. № 5. С. 15-28.

6. *Жичкина А.Е., Белинская Е.Н.* Самопрезентация в виртуальной коммуникации и особенности идентичности подростков — пользователей Интернета *IT* Образование и информационная культура. Социологические аспекты. Труды по социологии образования. 2000. С.431-460.

7. Информационные и коммуникационные технологии в образовании: монография / под ред. Б. Дендева. М.: ИИТО ЮНЕСКО, 2013.

8. *Карр Н.* Пустышка: Что Интернет делает с нашими мозгами. СПб.: Бест Бизнес Букс, 2012.

9. *Кин Э.* Ничего личного. М.: Альпина паблишер, 2016.

10. *Манович Л.* Язык новых медиа / Л. Манович; (перевод Дианы Кульчицкой). М.: Ад Маргинем Пресс, 2018.

11. *Марцинковская Т.Д.* Информационная социализация в изменяющемся информационном пространстве // Психологические исследования: электронный научный журнал. 2012. Т. 5. №26. С. 7.

12. Медийная и информационная грамотность: программа обучения педагогов. М.: Институт ЮНЕСКО по информационным технологиям в образовании, 2012.

13. *Палфри Дж., Гассер* У. Дети цифровой эры. М.: Эксмо, 2011.

14. *Скиннер К.* Человек цифровой: Четвёртая революция в истории человечества, которая затронет каждого / Крис Скиннер, пер. с англ.; [науч. ред. К. Щеглова]. М.: Маип,

Иванов и Фербер, 2019.

15. *Солдатова Г.У., Вишнева А.Е.* Особенности развития когнитивной сферы у детей с разной онлайн-активностью: есть ли золотая середина? // Консультативная психология и психотерапия. 2019. Т. 27. №3. С. 97-118. URL: https://psyjournals.ru/files/108516/cpp_2019_n3_Soldatova_Vishneva.pdf (дата обращения: 18.06.2020).

16. *Солдатова Г.У., Рассказова Е.И.* «Оборотная сторона» цифровой компетентности российских подростков: иллюзия компетентности и рискованное поведение онлайн // Вопросы психологии. 2017. № 3. С. 3-15.

17. *Солдатова Г.У., Рассказова Е.И.* Неосведомлённость родителей о столкновении подростков с рисками в интернете: содержание и психологические факторы // Психологический журнал. 2019. Т. 40. С. 71-83.

18. *Солдатова Г.У., Рассказова Е.И.* Цифровая ситуация развития межпоколенческих отношений: разрыв и взаимодействие между подростками и родителями в Интернете // Мир психологии. 2017. № 1 (89). С. 134-143.

19. *Солдатова Г.У.. Рассказова Е.И., Чигарькова С.В., Львова Е.П.* Цифровая культура: правила, ответственность и регуляция // Цифровое общество как культурно-исторический контекст развития человека: сборник научных статей и материалов международной конференции, 14-17 февраля 2018, Коломна / под общ. ред. Р.В. Ершовой. Коломна: Государственный социально-гуманитарный университет, 2018. С. 374-379.

20. *Солдатова Г.У., Шляпников В.И.* Цифровая компетентность российских педагогов // Психологическая наука и образование. 2015. Т. 20. N° 4. С. 5-18.

21. *Солдатова Г.У., Ярмина АН.* Кибербуллинг: особенности, ролевая структура, детско-родительские отношения и стратегии совладания // National Psychological Journal. 2019. Т. 12. № 3.

22. *Солдатова Г.. Зотова Е., Чекалина А., Гостимская О.* Пойманные одной сетью // Социально-психологическое исследование восприятия интернета детьми и подростками. М., 2011.

23. *Цимбаленко С.Б.* Подросток в информационном мире: практика социального проектирования. М.: НИИ Школьных технологий, 2010.

24. Digital Competence Framework for Educators (DigCompEdu). Published on EU Science Hub. URL: https://ec.europa.eu/jrc/en/ printpdf/137812 (дата обращения: 18.06.2020).

25. *Mossberger K., Tolbert C.J., McNeal R.S.* Digital Citizenship. The Internet, Society and

Participation. Cambridge, Maooachuocttc: MIT Press, 2007.

26. *Smahel D.,* et al. EU Kids Online 2020: survey results from 19 countries. 2020.

Интернет-ресурсы

1. Дети России онлайн — сайт проектов Фонда Развития Интернет [Электронный ресурс]: [сайт]. [2020]. URL: http://detionline.com (дата обращения: 18.06.2020).

2. Образовательный портал для родителей от Лаборатории Касперского [Электронный ресурс]: [сайт]. [2017]. URL: https://kids.kaspersky.ru (дата обращения: 18.06.2020).

3. Электронные версии выпусков журнала «Дети в информационном обществе» [Электронный ресурс]: [сайт]. [2017]. URL: http:// detionline.com/journal/numbers (дата обращения: 18.06.2020).

СОДЕРЖАНИЕ КУРСА

5 КЛАСС

Занятие 1. Зачем нам нужен Интернет

Создание современного Ингернета. Тим Бернерс Ли. Всемирная паутина. Новые возможности Интернета в осуществлении традиционных социально-культурных практик. Типы интернет-пользователей. Проблема интернет-зависимости. Сбалансированный распорядок дня.

Занятие 2. Как устроен Интернет

Компьютерная программа. Первая в мире компьютерная программа. Браузер. Программное обеспечение, софт. Профессия программист. Техносфера. Виды цифровых устройств. Три кита Интернета: «железо», софт, сети. Компьютерные вирусы. Правила защиты цифрового устройства от компьютерных вирусов.

Занятие 3. Какая бывает информация

Что такое информация. Цифровая информация. Контент. Ценность информации. Каналы восприятия информации. Возможности использования каналов восприятия информации в Интернете. Единицы измерения цифровой информации. Формы представления цифровой информации в Интернете.

Занятие 4. Как работает поиск в Интернете

Поиск информации. Поисковая система. Полезные ресурсы в Интернете. Контентные риски: столкновение с неприятным онлайн-контентом. Способы защиты от контентных рисков: настройки безопасного поиска и кнопка «пожаловаться на контент».

Занятие 5. Как люди общаются в Интернете

Сервисы для общения в Интернете. Возможности общения в Интернете. Рэй Томлинсон. Первое в мире электронное сообщение. Плюсы и минусы цифрового общения. Правила онлайн-общения.

Занятие 6. Как совершать покупки в Интернете

Цифровая экономика. Реальные и виртуальные товары. Первый в мире интернет-магазин. Критерии надёжности интернет-магазина. Плюсы и минусы интернет-магазинов. Баннеры, реклама. Правила безопасности при совершении покупок в Интернете.

Занятие 7. Что такое персональные данные

Общедоступная и персональная информация. Персональные данные. Виды персональных данных.

Занятие 8. Какие следы мы оставляем в Интернете

Виды персональных данных, выкладываемых в открытый доступ. Риски размещения персональной информации в открытом доступе. Настройки приватности.

Занятие 9. Урок в школе будущего

Современные технологии, используемые в процессе обучения.

6 КЛАСС

Занятие 1. Мы в цифровом мире

Информационные революции, история средств связи. Функции и роль Интернета в повседневной жизни. Возможности и риски, связанные с Интернетом. Интернет-зависимость. Варианты организации свободного времени без использования гаджетов и Интернета.

Занятие 2. Почему важны пароли в Интернете

История паролей. Всемирный день пароля. Аккаунт, логин, пароль, аутентификация, авторизация. Способы защиты аккаунта (пароль, отпечаток пальца, одноразовый код, USB-ключ, двухфакторная аутентификация). Правила безопасности при защите аккаунта (создание, использование и хранение надёжных паролей). Алгоритмы создания паролей.

Занятие 3. Полезные интернет-ресурсы

Виды информационных ресурсов. Что такое контент. Контент в Интернете. Полезные онлайн-ресурсы. Цифровые образовательные ресурсы. Контентные риски. Способы защиты от нежелательного контента в Интернете.

Занятие 4. Как искать и распознавать правдивую информацию

Потребность в информации. Информационная социализация. Инструменты для быстрого поиска в Интернете. Достоверность информации. Что такое фейк. Пост и репост в социальной сети. Способы определения достоверности информации.

Занятие 5. Как общаться в Интернете

Самопрезентация. Особенности самопрезентации в Интернете. Общение в Интернете. История смайлика. Преимущества и недостатки общения в Интернете. Вербальное и невербальное общение. Эмодзи. Особенности передачи и восприятия информации, выраженной при помощи смайликов и эмодзи и при помощи текста. Уместное и

неуместное использование смайликов и эмодзи в онлайн-общении.

Занятие 6. Как избежать конфликтов в Интернете

Агрессивное и неагрессивное общение. Причины агрессии в Интернете. Правила безопасности при общении в Интернете. Троллинг. Стратегии поведения при столкновении с троллингом. Пути решения проблемы агрессии в Интернете. Возможности бесконфликтного общения в Интернете. Способы поддержки человека, столкнувшегося с агрессией в Интернете. Флешмобы. Правила бесконфликтного общения в Интернете.

Занятие 7. Как избежать онлайн-мошенничества

Цифровая экономика. Преимущества и риски покупок онлайн. Интернет-мошенничество. Фишинг. Виды интернет-мошенничества и их последствия. Спам. Способы защиты от спама. Смс-мошенничество. Способы защиты от интернет- и смс-мошенничества.

Занятие 8. Что такое персональные данные

Персональные данные. Публичная и персональная информация. Идентификатор личности. Виды персональных данных.

Занятие 9. Что нужно знать о цифровых следах

Цифровой след. Понятие приватности. Настройки приватности в цифровых устройствах. Виды кодов (линейный штрихкод и qr- код). Источники приватных сведений о человеке. Рекомендации по управлению приватностью в Интернете.

Занятие 10. Дома будущего

Новшества в архитектуре и строительстве, связанные с цифровыми технологиями. Применение цифровых технологий в быту.

7 КЛАСС

Занятие 1. Как не заблудиться в Интернете

Место Интернета в жизни современного человека. Домен и доменное имя. Виды доменов. Требования к доменным именам. Проблема интернет-зависимости. Всплывающие уведомления. Профилактика чрезмерной увлечённости Интернетом.

Занятие 2. Как безопасно подключаться к Интернету

Способы подключения к Интернету. Проводное и беспроводное соединение. Правила безопасности при беспроводном подключении к Интернету. Правила и алгоритмы составления надёжного пароля.

Занятие 3. Как искать полезную информацию в Интернете

Потребность в информации как одна из базовых потребностей человека. Контент сайта. Механизм работы поисковых систем. Возможности и правила поиска в поисковых системах Google и Яндекс. Функция «поиск по картинке». Информационная перегрузка.

Занятие 4. Почему нужно проверять информацию в Интернете

Достоверная и недостоверная информация. Фейковые новости. Признаки недостоверной, фейковой информации.

Занятие 5. Человек в Интернете: реальный или виртуальный?

Способы общения в Интернете. Форумы, чаты, мессенджеры. «Друзья» в социальных сетях и Интернете. Аватар — «лицо» человека в Интернете. Механизм формирования образа человека в Интернете. Риски общения с незнакомцами в Интернете. Правила безопасного общения с интернет-друзьями.

Занятие 6. Как противостоять агрессии в Интернете

Агрессия и конфликты в Интернете. Троллинг. Действия по профилактике агрессивного поведения в Интернете. Действия при столкновении с агрессией в Интернете.

Занятие 7. Как безопасно совершать покупки в Интернете

Цифровая экономика. Покупки в Интернете. Риски онлайн-шопинга. Правила безопасности при совершении покупок онлайн.

Занятие 8. Как персональные данные оказываются в Сети

Персональные данные. Конфиденциальность. Цифровые следы. Способы попадания персональных данных в Сеть. Куки-файлы. Правила защиты персональных данных. Режим «инкогнито». Три кита защиты персональных данных: надёжные пароли, настройки приватности, управление персональными данными.

Занятие 9. Для чего нужно управлять персональными данными

Значимость персональных данных. Способы управления персональными данными в Интернете. Рекомендации по предотвращению кражи персональных данных.

Занятие 10. Цифровой мир будущего

Интернет вещей. Цифровые технологии и предметы повседневного пользования.

8 КЛАСС

Занятие 1. Новая реальность — дополненная и виртуальная

Виртуальная реальность. Дополненная реальность. История развития технологий виртуальной и дополненной реальности. Применение виртуальной и дополненной реальности в разных сферах жизни. Видеоигры. Зависимость от видеоигр. Профилактика зависимости от видеоигр.

Занятие 2. Защита от вредоносных программ

Вредоносные программы: мифы и реальность. Компьютерный вирус. Виды вредоносных программ. Троянская программа. Способы защиты от технических рисков.

Занятие 3. Как стать мастером поиска в Интернете

Команды быстрого поиска в Интернете. Возможности строки поиска для решения математических задач. Нежелательный контент. Способы борьбы с нежелательным контентом.

Занятие 4. Как распознать фейки в Интернете

Фейковые новости. Фактчекинг. Признаки фейковых новостей. Способы определения фейковых видео и фотографий. База знаний Wolfram Alpha. Критерии оценки достоверности информации.

Занятие 5. Репутация в Интернете: как её сохранить

Репутация и самопрезентация в Интернете и офлайн. Риски, сопряжённые с самопрезентацией в Интернете. Негативное и положительное влияние поведения в Интернете на репутацию в жизни офлайн. Управление репутацией.

Занятие 6. Агрессия в Сети: способы предотвращения

Проявление агрессии в Интернете. Влияние столкновения с агрессией в Сети на пользователей. Профилактика агрессии в Сети. Технические средства защиты от агрессии в Сети. Социальная реклама. Правила безопасного общения в Интернете.

Занятие 7. Электронные платежи: правила безопасности

История денег. Банковские онлайн-операции. Интернет-платежи. Цифровая экономика. Платёжные карты. Виртуальные деньги. Криптовалюты. Риски при осуществлении интернет-платежей. Правила безопасности при осуществлении покупок в Интернете.

Занятие 8. Персональные данные в Сети: как их защитить

Государственный контроль над защитой персональных данных, Роскомнадзор. Сайт

«Персональныеданные.дети». Федеральный закон «О персональных данных*, персональные данные, оператор персонатьных данных, обработка персональных данных. Виды персональных данных. Признаки надёжного пароля. Способы создания надёжного пароля. Как пароли попадают к мошенникам. Правила хранения и защиты паролей.

Занятие 9. Оберегаем личное пространство в Интернете

Приватность. Личное пространство. Личные границы. Зоны общения. Распределение персональных данных по зонам общения. Шкала «открытости-закрытости*. Тест на степень открытости в Интернете. Настройки приватности в социальных сетях. Рекомендации по настройкам приватности в социальных сетях.

Занятие 10. Профессии будущего

Цифровые технологии и профессии. Изменения в мире профессий. Новые профессии, связанные с цифровыми технологиями.

9 КЛАСС

Занятие 1. Искусственный интеллект: что нас ждёт в будущем?

Искусственный интеллект, машинное обучение, нейросети, глубокое обучение. Применение искусственного интеллекта в различных сферах жизни. Тест Тьюринга. Чат-боты. Положительные и отрицательные последствия внедрения технологий искусственного интеллекта.

Занятие 2. Как безопасно искать и хранить информацию в Интернете

Браузер. Возможности и недостатки разных браузеров. Функции браузеров: сохранение паролей, сохранение истории посещений, запоминание введённых данных, функция защиты от фишинга и вредоносного программного обеспечения, управление всплывающими окнами, управление информацией о местоположении пользователя, управление доступом к камере и микрофону, управление загрузкой файлов. Облачные программы, облачные сервисы, облачные приложения для учёбы. Минусы и плюсы облачных и локальных сервисов.

Занятие 3. Как увидеть правду в море лжи

Постправда. Фейковые новости. Советы по определению фейковых новостей. Борьба с распространением фейковых новостей на уровне российского законодательства. Ответственное отношение к репостам. Значимость критического мышления.

Занятие 4. Как соблюдать авторское право в Интернете

Авторское право. Виды лицензий авторского права. Копирайт. Проприетарная

лицензия. Копилефт. Лицензия Creative Commons. Пиратство, плагиат. Тест на отношение к сетевому пиратству. Статьи Гражданского кодекса Российской Федерации, связанные с вопросами авторского права.

Занятие 5. Всегда ли нужно оставаться на связи?

Социальные сети, мессенджеры. Общение в мессенджерах и социальных сетях. Чрезмерное увлечение общением в Интернете. Фабинг. FOMO. Прокрастинация. Способы самоконтроля и борьбы с прокрастинацией.

Занятие 6. Комфорт и безопасность в социальных сетях

Общение в Интернете и социальных сетях. Риски общения в социальных сетях. Помощь другим пользователям, столкнувшимся с трудностями. Создание комфортной и безопасной атмосферы при общении в Интернете. Нетикет. Службы поддержки в социальных сетях.

Занятие 7. Цифровая экономика: не только покупки

Цифровая экономика. Государственная программа «Цифровая экономика Российской Федерации». Цифровая экономика в повседневной жизни. Экономические отношения без посредников. Шеринг-экономика. Меры предосторожности при покупке товаров и услуг без посредников. Краудфандинг, краудсорсинг. Государственные и муниципальные услуги в Интернете.

Занятие 8. Что знают обо мне цифровые устройства

Виды персональных данных. Какая информация хранится на смартфонах. Примущества и недостатки хранения информации в смартфонах. «Умные» вещи. «Интернет вещей». Какие персональные данные собирают «умные» вещи. Правила безопасности при установке приложений. Шифрование в мессенджерах.

Занятие 9. Как управлять репутацией и удалять персональные данные в Интернете

Цифровые следы. Репутация в Сети. Праве на забвение. Рекомендации по удалению персональных данных из Сети. Статья 13.11 Кодекса РФ об административных нарушениях (Нарушение законодательства Российской Федерации в области персональных данных).

Занятие 10. «Умный» город

«Умные города. Цифровые технологии в городских инфраструктурах. Беспилотники. Технология Big Data. Фермы-небоскрёбы.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

5 КЛАСС

Занятия	Общее кол-во часов	Кол-во аудиторных часов	Кол-во часов практической работы
Модуль 1. Цифровой мир и интернет-зависимость (3 часа)			
Занятие 1. Зачем нам нужен Интернет	3	2	1
Модуль 2. Техносфера и технические риски (4 часа)			
Занятие 2. Как устроен Интернет	4	2	2
Модуль 3. Информация и контентные риски (8 часов)			
Занятие 3. Какая бывает информация	4	2	2
Занятие 4. Как работает поиск в Интернете	4	2	2
Модуль 4. Общение и коммуникационные риски (4 часа)			
Занятие 5. Как люди общаются в Интернете	4	2	2
Модуль 5. Цифровая экономика и потребительские риски (4 часа)			
Занятие 6. Как совершать покупки в Интернете	4	2	2
Модуль б. Персональные данные (8 часов)			
Занятие 7. Что такое персональные данные	4	2	2
Занятие 8. Какие следы мы оставляем в Интернете	4	2	2
Модуль 7. Цифровое будущее (3 часа)			
Занятие 9. Урок в школе будущего	3	1	2
Итого	34	17	17

6 КЛАСС

Занятия	Общее кол-во часов	Кол-во аудиторных часов	Кол-во часов практической работы
Модуль 1. Цифровой мир и интернет-зависимость (3 часа)			
Занятие 1. Мы в цифровом мире	3	1	2
Модуль 2. Техносфера и технические риски (4 часа)			
Занятие 2. Почему важны пароли в Интернете	4	2	2
Модуль 3. Информация и контентные риски (8 часов)			
Занятие 3. Полезные интернет- ресурсы	4	2	2
Занятие 4. Как искать и распознавать правдивую информацию	4	2	2
Модуль 4. Общение и коммуникационные риски (8 часов)			
Занятие 5. Как общаться в Интернете	3	2	1
Занятие б. Как избежать конфликтов в Интернете	3	2	1
Модуль 5. Цифровая экономика и потребительские риски *(4* часа)			
Занятие 7. Как избежать онлайн- мошенничества	*4*	2	2
Модуль 6. Персональные данные (8 часов)			
Занятие 8. Что такое персональные данные	*2*	1	1
Занятие 9. Что нужно знать о цифровых следах	*4*	2	2
Модуль 7. Цифровое будущее (3 часа)			
Занятие 10. Дома будущего	*3*	2	1
Итого	*34*	17	17

7 КЛАСС

Занятие	Общее кол-во часов	Кол-во аудиторных часов	Кол-во часов практической работы
Модуль 1. Цифровой мир и интернет-зависимость (3 часа)			
Занятие 1. Как не заблудиться в Интернете	3	1	2
Модуль 2. Техносфера и технические риски (3 часа)			
Занятие 2. Как безопасно подключаться к Интернету	3	2	1
Модуль 3. Информация и контентные риски (8 часов)			
Занятие 3. Как искать полезную информацию в Интернете	4	2	2
Занятие 4. Почему нужно проверять информацию в Интернете	4	2	2
Модуль 4. Общение и коммуникационные риски (8 часов)			
Занятие 5. Человек в Интернете: реальный или виртуальный?	4	2	2
Занятие 6. Как противостоять агрессии в Интернете	4	2	2
Модуль 5. Цифровая экономика и потребительские риски (3 часа)			
Занятие 7. Как безопасно совершать покупки в Интернете	3	1	2
Модуль б. Персональные данные (6 часов)			
Занятие 8. Как персональные данные оказываются в Сети	3	1	2
Занятие 9. Для чего нужно управлять персональными данными	3	1	2
Модуль 7. Цифровое будущее (3 часа)			
Занятие 10. Цифровой мир будущего	3	2	1
Итого	34	17	17

8 КЛАСС

Занятие	Общее кол-во часов	Кол-во аудиторных часов	Кол-во часов практической работы
Модуль 1. Цифровой мир и интернет-зависимость (3 часа)			
Занятие 1. Новая реальность — дополненная и виртуальная	3	1	2
Модуль 2. Техносфера и технические риски (4 часа)			
Занятие 2. Защита от вредоносных программ	4	2	2
Модуль 3. Информация и контентные риски (7 часов)			
Занятие 3. Как стать мастером поиска в Интернете	3	1	2
Занятие 4. Как распознать фейки в Интернете	3	1	2
Модуль 4. Общение и коммуникационные риски (8 часов)			
Занятие 5. Репутация в Интернете: как её сохранить	4	2	2
Занятие 6. Агрессия в Сети: способы предотвращения	4	2	2
Модуль 5. Цифровая экономика и потребительские риски (4 часа)			
Занятие 7. Электронные платежи: правила безопасности	4	2	2
Модуль 6. Персональные данные (6 часов)			
Занятие 8. Персональные данные в Сети: как их защитить	3	1	2
Занятие 9. Оберегаем личное пространство в Интернете	3	1	2
Модуль 7. Цифровое будущее (3 часа)			
Занятие 10. Профессии будущего	3	2	1
Итого	34	17	17

9 КЛАСС

Занятие	Общее кол-во часов	Кол-во аудиторных часов	Кол-во часов практической работы
Модуль 1. Цифровой мир и интернет-зависимость (3 часа)			
Занятие 1. Искусственный интеллект: что нас ждёт в будущем?	3	1	2
Модуль 2. Техносфера и технические риски (3 часа)			
Занятие 2. Как безопасно искать и хранить информацию в Интернете	3	2	1
Модуль 3. Информация и контентные риски (7 часов)			
Занятие 3. Как увидеть правду в море лжи	3	1	2
Занятие 4. Как соблюдать авторское право в Интернете	4	2	2
Модуль 4. Общение и коммуникационные риски (8 часов)			
Занятие 5. Всегда ли нужно оставаться на связи?	4	2	2
Занятие б. Комфорт и безопасность в социальных сетях	4	2	2
Модуль 5. Цифровая экономика и потребительские риски (4 часа)			
Занятие 7. Цифровая экономика: не только покупки	4	2	2
Модуль 6. Персональные данные (б часов)			
Занятие 8. Что знают обо мне цифровые устройства	3	1	2
Занятие 9. Как управлять репутацией и удалять персональные данные в Интернете	3	1	1
Модуль 7. Цифровое будущее (3 часа)			
Занятие 10. «Умный город»	3	2	1
Итого	34	17	17