Планета Интернет – выбор взрослых, выбор детей

Выпуск 10

Введение

Реалии современного мира диктуют необходимость взаимодействия в Интернете. Мы учимся через Интернет, общаемся, работаем, делаем покупки и развлекаемся. Однако в Сети существуют различные риски: контентные, коммуникационные, потребительские, технические и один из самых главных – интернет-зависимость. Поэтому крайне важно сформировать здоровую позицию детей при взаимодействии с Интернетом, помочь им адаптироваться под новые, постоянно изменяющиеся условия.

Учёные изучают изменения психики под влиянием цифровых технологий. В отечественной психологии в настоящее время одно из основных мест занимают исследования тех изменений, которые возникают в психике под влиянием погружения в информационную среду.

Задача библиотечных специалистов состоит в том, чтобы помочь подросткам в социально-психологической адаптации, грамотном и безопасном использовании ресурсов Сети для интеллектуального развитии и расширения кругозора. Современные дети – довольно продвинутые пользователи, и важно, чтобы они сами сделали выводы о том, каким образом безопасно вести себя в Сети.

Дайджест составлен из текстовых фрагментов статей по теме использования Интернета и вопросов, возникающих, в связи с этим в России и в мире. Тексты были опубликованы в периодических изданиях, поступивших в Краснодарскую краевую детскую библиотеку имени братьев Игнатовых во второй половине 2021 и в первой половине 2022 года.

Содержание

1. Информационная безопасность в Сети. Защита цифровых платформ – минимизатор рисков в интернет-пространстве

Дмитриева О. Безопасность в Интернете / О. Дмитриева // Не будь зависим. – 2022. – № 1. – С. 36–41.

Изначально Интернет был создан для того, чтобы облегчить людям процесс поиска информации. Дальше Интернет взял на себя и многие другие функции.

Мы можем легко и быстро находить информацию, материал для написания рефератов, докладов, курсовых.

Можем общаться с людьми, которые находятся очень далеко.

Интернет даёт нам возможность получать образование, оканчивать курсы, посещать лекции знаменитых людей, педагогов.

Интернет позволяет «путешествовать» по миру, не выходя из дома, виртуально посещать музеи, достопримечательности разных стран.

По Интернету можно погружаться в разные профессии и выбрать себе дело по душе.

Интернет позволяет легально найти работу, зарабатывать.

Интернет даёт нам развлекательный контент.

Однако к многочисленным плюсам всё-таки прилагается некоторый ряд угроз, ряд опасностей: сетевое хулиганство, разглашение личных данных, нежелательная почта или спам, общение с опасными пользователями, фишинговые (мошеннические) сайты, формирование зависимости.

Вредоносные программы, компьютерные вирусы

Компьютерный вирус называется вирусом, потому что, во-первых, он ухудшает работу устройства, а во-вторых, может быть заразным. Компьютерный вирус создаёт человек. Это программа, которая специально написана программистом для получения доступа к чужим данным, получения контроля над чужим компьютером, создания помех в работе других программ.

Цели здесь могут быть самыми разными.

1. Программы-вымогатели.

Одни из самых распространенных вирусов – программы-вымогатели. Вирус блокирует доступ к каким-то данным на компьютере и угрожает порчей файлов, если вы не переведёте определённую сумму на конкретный номер.

2. Бэкдор[1].

Следующий тип вирусов – так называемый бэкдор, когда злоумышленник получает удалённый доступ к нашему компьютеру, к управлению им. И с нашего устройства он может совершать свою незаконную деятельность.

3. Майнер-программы.

Ещё бывают программы для майнинга, которые используют не само наше устройство, а его мощность в своих целях. Может быть, с помощью этой мощности генерируется что-то, криптовалюта, пароли, создаются ботнеты[2].

4. Вирус-червь.

Один из самых распространённых видов вирусов – черви. Эти программы не приносят прямой выгоды своему создателю, но вредят окружающим, портят данные на чужом компьютере.

Пути заражения вирусами

Как вирусы могут оказаться на нашем устройстве?

1. Такое происходит, если у нас уязвимо программное обеспечение. Допустим, мы установили антивирус лет 5 назад и с тех пор ни разу не обновляли. Важно регулярно обновлять программное обеспечение и антивирусные программы.
2. Физические носители. Достаточно частый источник заражения устройства вирусом – физические носители, то есть флешки, жёсткие диски.
3. Частый источник заражений – сообщения с приложенными к ним вредоносными файлами.

---

[1] **Бэкдор** (от англ. *back door* – «чёрный ход», буквально «задняя дверь») – дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом.

[2] **Ботнет** (англ. *botnet*, от слов *ro**bot*** – «робот» и ***net**work* – «сеть») – это компьютерная сеть, в которой каждое устройство с доступом в Интернет заражено вредоносной программой и управляется бот-мастером (бот-пастухом).

4. Ещё один источник проблем – мобильные приложения со скрытыми вредоносными функциями.

Никакие лишние приложения устанавливать не нужно, нельзя устанавливать приложения из сомнительных источников. Если эту технику безопасности мы будем соблюдать, то вирусов на нашем устройстве не окажется.

Сетевое хулиганство

Сетевое хулиганство – это когда кто-то в Интернете провоцирует нас на негативные эмоции, пишет нам что-то неприятное. Сетевой хулиган хочет обидеть, задеть. Он прибегает к запугиванию, унижению, распространению компрометирующей информации.

Есть два основных типа сетевого хулиганства – троллинг и кибербуллинг.

Троллинг

Троллинг всем знаком – когда нам пишут неприятный комментарий, вызывают нас на какие-то дискуссии, споры, вызывают у нас возмущение. Ничего опасного в троллинге нет, это просто неприятно, человек тратит наше время, наши нервы и таким образом развлекается. Поэтому отвечать на троллинг нельзя. Надо заблокировать тролля или игнорировать его послания.

Кибербуллинг

Второй тип сетевого хулиганства – кибербуллинг, более страшная и опасная вещь. Здесь речь может идти о постоянных оскорблениях, угрозах, может быть, даже о шантаже, когда человек в течение длительного времени получает такие сообщения с одного аккаунта или даже с разных. На самом деле, кибербуллинг, кибертравля – самое настоящее уголовно наказуемое правонарушение. Называется это «преследование», и оно запрещено.

Если вы с чем-то подобным столкнулись, в первую очередь стоит заблокировать такого отправителя, но, если он проявляет настойчивость, пишет с других аккаунтов, необходимо сообщить родителям, а в некоторых случаях – в полицию. Если о человеке кто-то распространяет сведения, порочащие его честь и достоинство, да ещё и лживые, это называется клеветой и карается штрафом от 500 тысяч рублей.

Утечка личных данных

Утечка личных данных – это проблема, с которой пользователи Интернета сталкиваются чаще по собственной неосторожности. Если вы хотите показать какой-то контент ограниченному кругу людей, показывайте со своего устройства, не выкладывая в Интернет.

Также доступ к нашей личной информации злоумышленники могут получать через открытый *Wi-Fi, Wi-FiFree*, который не требует пароля. Злоумышленники могут специально создать точку доступа к *Wi-Fi*, вы прошли мимо, и ваш телефон подсоединился – человек у вас похитил какие-нибудь ваши личные данные или вам вирус закинул. Участники сети могут видеть, какие сайты вы посещаете, и даже какие данные на них вводите. Вы пошли дальше, телефон отсоединился, и вы вообще об этом не узнаете. Чтобы такого не происходило, автоподключение нужно убрать. Нужно подсоединяться только к тем сетям, которым можно доверять.

Также важно не проводить никаких платежных операций, когда вы подключены к Интернету через открытую сеть.

Веб-камеры

Иногда угрозу для нашей личной информации представляет наша веб-камера. Есть такие модели ноутбуков, где вокруг веб-камеры есть специальные шторки, которые можно задвинуть. Эта деталь появилась не для красоты, а после серии случаев, когда злоумышленники взламывали веб-камеру у человека и следили за ним, записывали всё, что у него в жизни происходит. Признаком того, что наша веб-камера работает, является горящая на ней лампочка.

Как себя обезопасить

1. Необходимо выбирать себе надёжные пароли. Надёжный пароль – тот, который имеет минимум 8 символов. Символами должны быть буквы, заглавные и строчные, цифры, знаки.
2. Не записывайте пароль в очевидных местах, никому не сообщайте.
3. Если вы пользуетесь чужим устройством, школьным компьютером, то, выходя из своей почты, важно не просто её закрыть, но и нажать кнопку «выйти». Иначе потом компьютер может открыть вашу почту.

4. Также нельзя сохранять важные личные данные на компьютере, к которому имеет доступ кто-то, кроме нас, вводить персональные данные на сомнительных сайтах и ресурсах, оставлять свою личную информацию в открытом доступе.
5. Нужно завести отдельную [банковскую] карту специально для онлайн-операций.

Мошенничество в Интернете

Есть такой вид мошенничества, как фишинг, когда злоупотребляют нашим доверием, у нас выманивают пароли банковских карт, пароли от каких-то сайтов, чтобы в дальнейшем ими пользоваться.

А как понять, что сайт, где мы хотим сделать покупку, надежён?

У сайта должна быть хорошая репутация, может быть, вы им уже пользовались. Знак «замочек» в левом верхнем углу экрана свидетельствует о том, что у сайта есть сертификат безопасности, то есть его сложно взломать. Но стопроцентной гарантии нам ничего не даёт. Все равно могут быть разные случаи, поэтому, если есть возможность, лучше оплачивать покупку наличными курьеру при получении товара. Если вы всё-таки что-то оплачиваете в Интернете, желательно иметь для этого отдельную [банковскую] карточку, на которой лежит небольшая сумма.

Спам

Следующая проблема, связанная с использованием Интернета, – спам. Если получили спам, не открывайте его, а сразу удаляйте. Можно пожаловаться администрации почтового сервера, которому принадлежит адрес спамера. Не публикуйте свой адрес в открытых группах, открытых местах. Тогда спама будет гораздо меньше.

Опасное общение

Общаясь в Сети, можно познакомиться с кем угодно – с мошенником, преступником, сетевым хулиганом, неадекватным человеком. Знакомство через Интернет небезопасно. В таком общении нужно соблюдать определенные правила. Свою полную контактную информацию нельзя давать никому. Также важно по возможности проверять информацию, которую человек сообщает о себе.

Можно ли с виртуальным знакомым встречаться лично? Лучше не рисковать. Но если идти на встречу, тут нужно неукоснительно соблюдать технику безопасности. Здесь бывали самые разные исходы.

1. Прежде чем идти на такую встречу, нужно кого-то об этом предупредить – родителей или друзей.
2. Встречу назначайте только в людном, общественном месте, в светлое время суток.
3. Не берите у него из рук еду и напитки.
4. Отказывайтесь входить с ним в квартиру.
5. Не заходите вместе с этим человеком в лифт, в подворотни.
6. Не позволяйте себя подвозить или провожать.
7. Если у вас возникнут сомнения, вам покажется, что намерения человека не чисты, поведение слишком навязчиво или подозрительно, не нужно бояться его обидеть, нужно тут же вставать и уходить.

Интернет-зависимость

И ещё одна угроза Интернета – интернет-зависимость. Интернет-зависимость – серьёзная болезнь, поведение со сниженным уровнем самоконтроля, грозящее вытеснить нормальную, реальную жизнь. Она может приводить к очень неприятным последствиям.

Признаки интернет-зависимости

1. Уныние и апатия при невозможности выхода в Интернет.
2. Постепенно теряется потребность в реальном общении, в прогулках. Зависимому иногда вовсе трудно выйти из дома.
3. Теряется ощущение времени. Если мы заходили в Интернет на пару минут проверить почту, а в итоге просидели там до глубокого вечера, весьма вероятно, что мы уже теряем контроль, и необходимо уделить этому внимание.
4. Во время пребывания в Сети человек забывает о своих профессиональных и домашних обязанностях, встречах и обещаниях.
5. Ресурсы в Интернете человек посещает автоматически, а не с конкретной целью.
6. Пользователь тратит деньги на развлечения в Сети, пытаясь скрыть это от семьи.

Последствия сидения за компьютером для здоровья – боль в глазах, проблемы со зрением, проблемы с опорно-двигательным аппаратом, эмоциональная нестабильность, нарушение умственных функций

– ухудшение памяти, внимания. Одно из самых частых последствий – так называемый синдром лучезапястного канала, когда человек всё время водит рукой мышкой. Ладонь всё время находится на углу стола, пережимается нерв, и теряется чувствительность некоторых пальцев.

Интернет – очень полезная вещь и замечательный инструмент. Главное, чтобы мы пользовались им умеренно и с пользой, чтобы контролировали время, которое проводим в Интернете. Можно попробовать устроить себе день без Интернета, вообще им не пользоваться, и посмотреть, что будет. Если всё хорошо, значит, зависимости нет. Важно, чтобы у вас были увлечения, не связанные с Интернетом: кружки, секции, личные встречи с друзьями. Если после попыток сократить время пребывания в Интернете ситуация не улучшилась, не стесняйтесь просить о помощи, в том числе специалистов.

Крайнева И. Информационная безопасность детей и подростков / И. Крайнева // Школьная библиотека. – № 5. – С. 9–10.

По результатам социологического онлайн-опроса учащихся 7–11-х классов Новгородской области, направленного на выявление причин агрессивного поведения среди подростков, которое проводил Институт управления образованием Российской академии образования, выявлено, что большинство подростков в свободное время предпочитают гулять, слушать музыку, общаться с друзьями и проводить время за компьютером.

Ведущий мотив высокой интернет-активности подростков – доминирование позитивного восприятия Интернета как источника информации и средства коммуникации. Более 90 % всех подростков воспринимают Интернет в первую очередь через спектр положительных эмоций. Позитивное эмоциональное подкрепление – одна из ключевых причин, которая побуждает подростка, несмотря на усталость, часами сидеть за компьютером или в телефоне. Большинство школьников указало, что Интернет вызывает у них интерес, любопытство и удивление.

Современные дети и подростки легко осваивают компьютер, мобильные устройства и умело пользуются ими. При этом у большинства детей не сформированы навыки безопасного поведения в Интернете.

Почему дети и подростки в интернет-пространстве нуждаются в защите?

1. У них имеется ряд возрастных особенностей переработки информации, особенности мышления, о которых родители могут забывать, воспринимая ребёнка как «маленькую версию взрослого», предоставляя ему возможности к самостоятельному поиску контента для проведения досуга.
2. Дети и подростки воспринимают поток информации из Интернета и других СМИ как реальность, не принимая во внимание субъективность суждений или возможную недостоверность информации. Может возникнуть риск вовлечения подростков в деструктивные группы в социальных сетях («группы смерти», экстремистские группы, которые могут внушать подросткам идеи о несправедливости мироустройства и их особом предназначении в «улучшении мира», группы, предлагающие подросткам «работу», заключающуюся в незаконной деятельности).
3. Как и любая проблема, кибербезопасность ребёнка отражается в семейном сценарии, а также нормах и правилах. Родители могут не придавать значения проявлениям кибербезопасности дома, и у детей формируется попустительская позиция через принятие родительских шаблонов.

Среди наиболее известных рисков виртуального пространства учащиеся называют:

- кражу личной информации;
- взлом страниц в социальных сетях;
- вирусы.

Многие учащиеся после долгого общения в Сети считают своих интернет-знакомых друзьями и могут предоставить им любую информацию о себе.

Рассмотрим подробнее ключевые направления, в которых подростки демонстрируют наименьшую компетентность.

- Безопасность личных данных

Фамилия, имя, отчество – допустимая к размещению информация. Дата рождения, номер телефона – предпочтительно размещать в режиме «Видно только друзьям / отдельному списку лиц». Место проживания – максимум, что может быть указано в профиле, это город

проживания. Данные документа, удостоверяющего личность, и иных документов размещать нельзя.

- Безопасность коммуникации

Обучая взаимодействию в Сети с незнакомцами, особое внимание следует уделить общению в личной переписке. Подростки должны понимать, что можно, а что нельзя сообщать человеку по ту сторону экрана.

- Защита от медианасилия

Поток информации, получаемый подростками, постоянно возрастает, что неизбежно приводит к получению нежелательной и небезопасной информации. В связи с этим возникает необходимость развития сознательности учащихся.

- Угроза кибербуллинга (интернет-травли)

Она заключается в использовании технологий для преследования, унижения, запугивания или высмеивания другого человека. Кибербуллинг может оказать разрушительное влияние на развитие детей и подростков, причём и в долгосрочной перспективе. Как и у других форм травли, у кибербуллинга есть вполне реальные последствия, ухудшающие качество жизни жертвы: дети могут столкнуться с депрессией, тревожностью и низкой самооценкой.

Как педагог может понять, стал ли ученик жертвой онлайн-травли

- Ребёнок/подросток кажется более одиноким или изолированным от окружающих.
- Неожиданные или внезапные проблемы с друзьями.
- Неожиданные изменения эмоционального фона.
- Ребёнок/подросток необычно часто расстраивается, в том числе по неожиданным поводам.
- Ухудшение успеваемости.
- Ученики начинают отвлекаться на занятиях или не обращать внимания на учителя.
- Частые пропуски занятий.
- Потеря интереса к внеклассным занятиям.
- Ученики начинают страдать от усиливающихся проблем с самооценкой.
- Ухудшение физического самочувствия.

Необходимо научить школьников, что делать в том случае, если они станут жертвами кибертравли

Обратиться ко взрослому, которому они доверяют.

Сохранить свидетельства и доказательства факта травли.

Не отвечать на угрозы.

Сообщить о факте онлайн-травли администраторам платформы или сервиса.

Подумать, как можно было бы защититься от кибербуллинга в будущем.

В случае возникновения кибербуллинга педагогам необходимо связаться с родителями участников травли, провести беседы с подростками по данной проблеме, обращаться за помощью к школьным психологам, специалистам центров психолого-педагогической, медицинской и социальной помощи.

Педагогам для обеспечения интернет-безопасности детей и подростков необходимо:

- проводить занятия с детьми по теме ответственного поведения в Интернете с привлечением других специалистов школы;
- убедить не сообщать в Интернете личную информацию;
- объяснить возможную опасность личных встреч с интернет-друзьями;
- обсуждать азартные сетевые игры и связанный с ними риск.

Результатами мероприятий по безопасному использованию Интернета могут стать как бумажные, так и электронные ресурсы, созданные подростками: рисунки, сочинения, буклеты, презентации, театрализованные выступления и видеофильмы.

Балабанова Е. Безопасность в Интернете глазами детей / Е. Балабанова // НаркоНет. – 2022. – № 6. – С. 31–34.

В гимназии «Эллада» у ребят есть возможности реализовывать свои задатки и способности в разных видах деятельности: на дополнительных занятиях и кружках. Интернет при этом выступает помощником. Постепенно дети учатся правильно и во благо использовать его потенциал.

В ходе классного часа «Интернет: за и против» учащиеся делятся на 4 группы.

В качестве разминки используется тематическая мотивирующая игра «Шпионы». Каждая команда получает скриншот, который содержит сведения из открытого аккаунта одного из случайных людей в какой-либо соцсети, например, в «Одноклассниках».

В роли «шпионов» – учащиеся, они за 2 минуты должны узнать как можно больше информации об этом человеке. Затем совместными усилиями они должны сделать вывод, что из социальных сетей можно почерпнуть очень много информации о человеке.

По итогам игры подростки сами делают вывод о том, что стоит и что не стоит публиковать в социальных сетях, и имеет ли вообще смысл в них регистрироваться. После этого проводится мозговой штурм.

Учащимся предлагают сформулировать мнение класса. Первая команда напишет плюсы Интернета, вторая команда – минусы. Третья выделяет риски Интернета, а четвёртая – его возможности.

По итогам представители от команд озвучивают результат работы.

К плюсам Интернета первая команда отнесла следующие его функции:

1. Заказ еды.
2. Покупка одежды.
3. Вызов такси.
4. Общение с родными на расстоянии и даже по видеосвязи.
5. Фильмы онлайн.
6. Книги онлайн.
7. Поиск информации.

К минусам Интернета вторая команда отнесла:

1. Вероятность встретиться в Сети с мошенниками.
2. Возможность нежелательного распространения личной информации.
3. Возможность выдачи своего местоположения через *IP*-адрес.
4. Наличие несмешных мемов.

К рискам Интернета, по мнению третьей команды, относятся:

1. Открытость личной информации.
2. Вероятность подсадить вирус на личный компьютер, смартфон или планшет.
3. Вероятность быть обманутым.

4. Вероятность получить убытки.

Среди возможностей Интернета четвёртая команда отметила:

1. Онлайн-обучение.
2. Удалённая работа.
3. Возможность скачивать программы, книги, музыку, возможность быть в курсе изменений погоды, общение, реклама, знакомство с иностранцами, развлечения и медийность.

Игра «Эксперты»

Ведущий раздаёт командам рабочие листы с разными темами, где изложены рекомендации по работе с минусами и рисками Интернета.

Группа 1: вредоносные программы.

Группа 2: сетевое хулиганство.

Группа 3: разглашение личных сведений.

Группа 4: опасное общение.

1-я группа. Вредоносные программы. Причины заражения вирусами:

1. Уязвимость операционной системы.
2. Отсутствие антивируса.
3. Социальные сети, мессенджеры, письма.
4. Приложения, которые просят разрешение на доступ к фотографиям, геопозиции, интернет-банкингу, счетам, переписке и т. д.

Рекомендации:

1. Обновлять операционную систему и стараться использовать новую версию.
2. Использовать антивирус.
3. Обновлять браузеры.

Рекомендации, добавленные детьми:

1. Устанавливайте лицензионные антивирусные программы.
2. Софт устанавливайте только из проверенных мест.
3. Не переходите по подозрительным ссылкам из писем.
4. Не кликайте по баннерам.

2-я группа. Сетевое хулиганство

Киберхулиган – человек, который запугивает или унижает другого человека с помощью мобильного телефона, электронной почты, текстовых сообщений в социальных сетях, на форумах или в чатах. Как правило, он действует анонимно. Жертва не знает агрессора!

Рекомендации:

1. Не молчи, сообщи об этом родителям, учителю.
2. Не отвечай на провокации!

Рекомендации, добавленные детьми:

1. Заблокируй хулигана, тролля!
2. Сделай на всякий случай скриншот переписки.

3-я группа. Разглашение личных сведений

Мошенники могут просить:

1. Номер телефона.
2. Пароль от почты.
3. Домашний адрес.
4. Пин-код карты.

Рекомендации:

1. Не доверяйте никому свою личную информацию.
2. Одним из признаков проверенных и надёжных сайтов является замок в верхнем левом углу адресной строки браузера.

Рекомендации, добавленные детьми:

1. Осуществляйте покупки на знакомых, проверенных сайтах.
2. Выбирайте вдумчиво, какую информацию стоит выкладывать в социальных сетях.
3. Не сообщайте пароли, номер телефона незнакомым людям.
4. Не сообщайте своё местожительство.
5. Не сохраняйте важные сведения на общедоступном компьютере.

4-я группа. Опасное общение

Общаясь в соцсети или мессенджере, вы можете познакомиться с человеком, который впоследствии оказывается мошенником, похитителем, аферистом, то есть выдает себя не за того, кем на самом деле является!

1. На аватарке может быть совершенно другой человек.
2. «Друг» может оказаться человеком из мест лишения свободы.
3. Он может быть намного старше, чем указал в сведениях о себе, или оказаться человеком другого пола.

Рекомендации:

1. С незнакомцами в Интернете нужно общаться так же, как с незнакомыми на улице.
2. Не давайте в переписке свою полную контактную информацию.

Рекомендации, добавленные детьми:

1. По возможности, проверяйте всю информацию о новом интернет-знакомом.
2. Просите выслать фото в реальном времени, например, в красном шарфе.
3. Никогда не верь виртуальному другу, если он обещает что-то купить или подарить тебе.

Зависимость от компьютерных игр и сетевых онлайн-игр приводит к тому, что:

1. Можно потратить немалые деньги на «прокачку» героя, покупку виртуальных денег или оборудования.
2. Может развиться агрессия.
3. От постоянного напряжения возможно ухудшение зрения.

Рекомендации:

1. Если после нескольких попыток сократить время игры у тебя ничего не получилось, обязательно проси помощи родителей.
2. Соблюдай семейные правила пользования гаджетами.

По итогам работы подростки сделали вывод, что Интернет в целом не плохой и не хороший. То или иное направление придают ему люди, которые им пользуются.

В конце классного часа каждая группа в течение 5–10 минут готовит свой проект памятки или буклета для более младших учеников.

Проект памятки по безопасности в Сети

Этикет в Интернете

В качестве основы можно использовать следующие рекомендации:

1. Говорите вежливо.
2. Отвечайте в хорошем настроении.
3. Пишите без ошибок.
4. Отвечайте на сообщения вовремя.
5. Шутки обозначайте при помощи смайликов (ваш собеседник должен понимать, что это шутка).
6. В тексте личных сообщений не принято выделять текст прописными буквами. Такое выделение рассматривается как крик.

Цифровая гигиена и кибербезопасность // Не будь зависим. – 2022. – № 1. – С. 24–29.

Занятие, посвящённое финансовой грамотности, Городской методический центр проводил совместно с Банком России по Центральному федеральному округу.

Ежедневно мы, наши дети, наши родители и вообще все, кто пользуется дистанционными банковскими услугами, сталкиваются с попытками мошенничества. У нас всё меньше становится денег в физическом выражении, наши средства находятся в банке, и мы управляем ими благодаря информации.

В первую очередь, это информация, расположенная на наших банковских картах, как внутри карты, так и на самой карте: номер карты, срок действия, полное имя владельца, трёхзначный код подтверждения, который находится на обороте. Также нужна информация, чтобы иметь доступ к своему личному кабинету в банке – логин и пароль. Кроме того, нужной информацией для управления деньгами в тех или иных случаях являются кодовое слово, которое указывается при заключении договора с банком, а также одноразовые коды.

Электронный банкинг

Дистанционное обслуживание, электронный банкинг – это оказание банковских услуг через Интернет и мобильную связь.

1. *PC*-банкинг.

Классический вид электронного банкинга, который появился первым, – удалённое управление своими счетами через доступ к личному кабинету в банке, с использованием персонального компьютера.

2. Мобильный банкинг.

Мобильный банкинг – удалённое управление своими финансами с помощью специальных приложений на мобильном телефоне, смартфоне.

3. *POS*-терминалы и банкоматы.

С их помощью мы оплачиваем покупки и услуги, тоже через Интернет. Любые операции, которые мы проводим через банкомат, осуществляются через Интернет.

И на все эти устройства нацелены мошенники, совершаются атаки. Цель мошенников – получение информации для доступа к чужим деньгам.

Методы мошенников

1. Социальная инженерия.

Технические атаки на устройства сложны, дорого стоят. Мошенники пользуются более дешёвыми средствами, а именно «взламывают человека» методами социальной инженерии. Мы сами являемся носителями той информации, которая нужна для управления нашими деньгами. Чем взламывать сложные приложения, над которыми трудятся высококвалифицированные программисты, гораздо проще уговорить человека совершить нужные мошеннику действия или передать ему информацию о себе, чтобы он сделал это от вашего имени.

2. Вирусы.

Также используется разнообразное вирусное программное обеспечение – не просто небольшие программы, а целые комплексы, которые эксплуатируются преступными группировками.

3. Сбор информации.

4. Утечка баз данных.

Кроме того, мошенники пользуются сбором информации и утечкой баз данных.

5. Поддельные сервисы и сайты.

Уроки пандемии по кибербезопасности

Во время пандемии проблема кибермошенничества усилилась, потому что больше людей начали пользоваться дистанционным интернет-банкингом – дистанционной оплатой, дистанционным заказом продуктов, дистанционной оплатой коммунальных услуг и так далее. Лучшим средством защиты от мошенничества для нас являются знание, понимание происходящего, осведомлённость, осмотрительность и холодный разум.

Статистика

По статистике видно, что за год значительно увеличилось количество денег, которые были похищены со счетов физических лиц. И можно увидеть, что доля возмещения крайне мала. Из-за чего это происходит?

Здесь играют роль два фактора. Первый: мошенники проводят операции таким образом, чтобы как можно быстрее спрятать похищенные деньги. Второй, самый важный: банки обязаны возвращать похищенные денежные средства только в том случае, если человек

сам не передал мошенникам свою конфиденциальную информацию, дал доступ к своим банковским счетам. Тогда, по федеральному закону «О национальной платёжной системе», банк не обязан возвращать эти денежные средства.

Поддельные сайты и сервисы

Поддельные сайты и сервисы – это наиболее общий механизм, которым пользуются мошенники, потому что он не таргетирован, направлен не на какого-то определённого человека, а сразу на всех. Во многом целевой аудиторией для подобных сайтов и сервисов как раз являются дети, поскольку у них мало жизненного опыта. Но не только на детей направлены подобные сайты. В основном, они тематические, создаются под информационную повестку, которая актуальна на данный момент. На сайте предлагается купить с доставкой этот товар. Всё выглядит как в обычном интернет-магазине. Человек выбирает товар, его переводят как бы на страницу оплаты, он вводит данные карты, подтверждает оплату, но вместо товара получает обнуление собственного счёта. Многое из того, что предлагается на подобных сайтах, просто нереально. Никто не будет продавать товар со скидкой в 90%. Нужно всё-таки совершать покупки в проверенных магазинах, по большей части, обращать внимание на детали самого сайта, то, как происходит общение с продавцом.

Признаки фишингового сайта

Как можно определить фишинговый сайт?

1. Правильность написания названия сайта.
2. Наличие или отсутствие безопасного соединения.
3. Способ попадания на сайт.
4. Открытые сети в *Wi-Fi*.
5. На сайте есть опечатки, ошибки, несоответствия, небрежности.
6. На странице оплаты отсутствуют логотипы программ *MasterCard SecureCode*.

Социальная инженерия

Один из самых популярных способов мошенничества – с помощью звонков. Мошенники могут представляться врачами, социальными работниками и т. д.

Основные этапы и принципы:

1. Первый этап – втереться в доверие.

2. Второй этап – психологическое давление.
3. Отсутствие времени на принятие решения.
4. Введение в заблуждение.
5. Целью могут быть не только деньги, но и ваши персональные данные.

Мошенничество на сайтах объявлений

Так, мошенники часто пользуются сайтами объявлений. Это удобный механизм, с помощью которого можно купить или продать ту или иную вещь.

1. Объявления о купле-продаже

Вам навязывают способ доставки товара и присылают поддельную ссылку на оплату. Покупатель делает вид, что оплатил товар, присылает поддельный чек, затем сообщает, что передумал, и просит вернуть деньги на карту.

2. Предложения работы

Людей заманивают на вакансии без опыта работы, без образования, но с гарантией стабильного, высокого дохода. Во многом такие предложения опасны именно для детей: здесь опять вступает в дело авантюризм характера.

Подобные предложения обычно выливается в:

1) сетевой маркетинг,
2) навязывание дополнительных платных услуг, например, надо сделать справку, которая стоит денег, или пройти платное обучение и так далее (а до самой работы или даже обучения дело чаще всего не доходит),
3) услуги по незаконному обналичиванию, отмыванию денег.

Обман на актуальных запросах

В условиях ограничений, закрытия стран люди всё равно хотели куда-то съездить отдохнуть и пытались найти способы. Мошенники это учитывают. Они делают сайты поддельных туроператоров и продают «эксклюзивные» рейсы, несуществующие отели, услуги, в том числе пользуясь уважаемыми площадками по аренде отелей и привлекая клиентов низкими ценами.

Важно помнить

Вариантов кибермошенничества множество. Как выйти из подобной ситуации с наименьшими потерями и вообще избежать этого?

Пока мы находимся в состоянии равновесия, можем размышлять, нужно понимать, какие данные мы не должны сообщать никому и никогда, ни при каких обстоятельствах.

1. Никогда не сообщайте данные своей карты, проверочные данные, логин и пароль для доступа в личный кабинет и кодовое слово.
2. Никогда не вводите эти данные на сайтах, на которые вы перешли по ссылке из письма или СМС, а ещё лучше – вообще не переходите никуда по ссылкам из подозрительных писем.
3. Не переводите деньги на счёт по просьбе неизвестного абонента, кем бы он ни представлялся.
4. Нужно помнить о бесплатном сыре в мышеловке.

Что делать, если уже совершены мошеннические действия?

1. Сразу позвоните в банк или, что быстрее, через приложение заблокируйте карту.
2. Сообщите в банк о мошеннической операции, о том, что эту операцию вы не совершали
3. Подобное действие – это преступление, а о любом преступлении нужно заявлять в полицию.

Как понять, что мобильный телефон заражен вирусом?

Вообще на телефонах операционные системы настроены так, что механизм защиты довольно сильный. Когда вы устанавливаете программы, нужно понимать, какие разрешения вы им даете. И надо насторожиться, если телефон ведёт себя не так, как обычно: греется, тормозит, быстро разряжается, необоснованно увеличивается трафик и так далее. Любое такое непонятное явление – это повод для того, чтобы провести проверку.

Надо ли менять пин-код карты в целях профилактики мошенничества?

Пин-код – это код, который нужен для того, чтобы взаимодействовать с банкоматом. Чтобы воспользоваться пин-кодом, нужно физически обладать картой. Поэтому есть смысл в том, чтобы менять пароли к доступу в онлайн-кабинет, менять пин-код для доступа в приложение на мобильном телефоне. Но менять пин-код для доступа к карте через банкомат не нужно.

Можно ли украсть деньги с карты с чипом, поднеся терминал в транспорте?

Это довольно сложно, и у получателя денег должен быть счёт юридического лица, и слишком очевидно, кто является преступником. Если карта лежит в кошельке, кошелек лежит в кармане или сумке, никто не будет пытаться подносить *POS*-терминал, чтобы украсть с неё деньги.

Наш цифровой портрет в Интернете // Не будь зависим. – 2022. – № 1. – С. 30–35.

То, что попало однажды в Интернет, остаётся там навсегда. Даже если вы удаляете, всё равно информация сохраняется на серверах. У наших гаджетов есть множество способов собирать и сохранять информацию о нас.

На основе этих данных и формируется цифровой портрет:

1. Умные голосовые помощники.
2. Учётная запись устройства.
3. Приложения.
4. Скрытые функции устройства.

Современные устройства на базе различных операционных систем имеют недокументированные возможности сбора и передачи данных в фоновом режиме. Они с определённой периодичностью могут незаметно для пользователя делать скриншоты экрана и имеют по умолчанию включённый микрофон. Всё это передаётся на серверы производителей.

Кто-то может думать, что ваша персональная информация никому не интересна. На самом деле, это не так. Возможно, вы сталкивались с таким явлением, как таргетированная реклама. Например, вы «гуглите» серёжки с бриллиантами, и на следующий день у вас вся лента в соцсети, весь Интернет полон серёжками с бриллиантами.

Как мошенники могут использовать историю ваших запросов?

Большинство сервисов в Интернете, которыми мы пользуемся даром, бесплатны лишь на первый взгляд. Именно информация о пользователях, которая может помочь составить их социальный портрет, является «валютой» в цифровом мире. На основе социальных портретов формируется выдача поисковых систем и социальных сетей, прогнозируется поведение людей и их предпочтения. Мошенники хитры

и предприимчивы. Нужно уметь отличать честных продавцов от мошенников.

Информацию о пользователях соцсетей интересно знать и работодателям.

Если вы что-то ищете в Интернете, это сразу попадает во все рекламы во всех ваших социальных сетях. Благодаря соцсетям можно обрисовать психологический портрет пользователя. Уже существуют программы, позволяющие создать психологический или лингвистический портрет пользователя.

Цифровой след бывает активным и пассивным. Активный след остается, когда мы заходим на сайт и вводим свои данные. Его пользователь оставляет сознательно, регистрируясь в различных онлайн-сервисах. Пассивный след оставляется непредумышленно: когда мы куда-то заходим, это сохраняется в нашей истории. А именно, сохраняются технические данные о гаджете, с которого осуществлялся выход в Сеть. И активный, и пассивный электронно-цифровой след дают много информации. С их помощью можно узнать более 40 видов данных о пользователе. Сотни и тысячи таких следов пользователя уже позволят составить виртуальный портрет его личности.

Как составить хороший цифровой портрет?

1. Первое, что нужно сделать, чтобы сформировать о себе хорошее мнение, чтобы у вас был нормальный цифровой портрет, – не публиковать в Интернете информацию, которая впоследствии сможет навредить вам, вас скомпрометировать, которую можно использовать против вас.
2. Ограничьте количество личной информации, размещаемой в соцсетях, сделайте её доступной только для близкого круга друзей.
3. Ознакомьтесь с политикой конфиденциальности ресурса, на котором вы собираетесь что-то о себе сообщать.
4. Используйте браузер без расширений и включайте в браузере режим приватного просмотра.
5. Настройте в браузере хранение *cookie*-файлов только в течение одного сеанса и их удаление при закрытии браузера.
6. Проверяйте наличие *http*-соединения у сайтов, где собираетесь вводить свои персональные данные.

7. Используйте антивирусные средства защиты и регулярно обновляйте их.
8. Критически оценивайте информацию, получаемую из социальных сетей и поисковых систем.

Рекомендации по предотвращению технических рисков

1. Установите на все домашние компьютеры антивирусные программы и специальные почтовые фильтры для предотвращения заражения компьютера и потери данных. Подобные программы наблюдают за трафиком и могут остановить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
2. Используйте только лицензионные программы и данные, полученные из надёжных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.
3. Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.
4. Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.
5. Регулярно делайте резервную копию важных данных, а также научите это делать ваших детей.
6. Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать.
7. Нельзя сообщать никакие пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.
8. Если вы пользуетесь Интернетом с помощью чужого устройства, не забывайте выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы. Никогда не следует сохранять на чужом компьютере свои пароли, личные файлы, историю переписки – по этой информации злоумышленники могут многое узнать о человеке.

Пожаловаться в «ВКонтакте»

1. Если вы увидели у кого-то другого в соцсети не очень хорошие записи, вы всегда можете пожаловаться, чтобы сделать Интернет лучше и безопасней.
2. Во «ВКонтакте» нажмите кнопку «Пожаловаться», в появившемся окне выберите подходящую категорию – оскорбление, материал для взрослых, пропаганда наркотиков, детская порнография, насилие/экстремизм, призыв к суициду.
3. Должно появиться сообщение: «Ваша жалоба будет рассмотрена модераторами».
4. Свяжитесь с администрацией напрямую и опишите суть подробно. Это можно сделать с помощью кнопки «Помощь». Там надо выбрать разделы «Общие вопросы» – «Как пожаловаться на группу?» – «Пожаловаться на сообщество». В появившемся диалоговом окне опишите подробно, почему данный контент противоправный, дайте на него ссылку.

2. Влияние интернет-среды на развитие детей и подростков

Пежемская Ю. Влияние интернет-среды на мышление подростков / Ю. Пежемская // НаркоНет. – 2022. – № 6. – С. 35–40.

Основными задачами представленного в работе исследования являлись:

1. Определение особенностей мышления подростков 12–16 лет.
2. Изучение степени и специфики погружённости подростков в интернет-среду.
3. Сравнительный анализ особенностей мышления групп подростков, глубоко и слабо погружённых в интернет-среду.

В ходе эмпирического исследования использовались тест Р. Атмаухера[3] и авторская методика «Индекс погружённости в интернет-среду»[4].

Результаты

Итоги решения первой задачи исследования показали изменение характеристик мышления подростков, произошедшие за последние 30 лет, в сторону улучшения вербальных и образных компонентов и снижения продуктивности практического математического мышления.

В процессе решения второй задачи выявили значительную степень погружённости подростков в интернет-среду при качественном разнообразии её использования. 46% пользуются возможностями Интернета ежедневно, а 51% указывают, что «живут в Интернете».

На первом этапе решения третьей задачи исследования была выдвинута гипотеза о непосредственном влиянии погружённости в интернет-среду на качественные характеристики мышления. Для этого было проведено сравнение особенностей мышления глубоко и слабо

[3] **Тест структуры интеллекта Амтхауэра** – тест, разработанный немецким психологом Рудольфом Амтхауэром для определения коэффициента интеллекта.

[4] **Методика «Индекс погружённости в интернет-среду»** даёт возможность экспресс-оценки разных сторон готовности подростков к использованию технических средств и информационных ресурсов Интернета для решения различных задач и осуществления интернет-коммуникации.

погружённых в интернет-среду подростков по «Индексу погружённости в интернет-среду».

В группу глубоко погружённых в Интернет вошли 117 подростков (средний возраст – 14,5 лет), которые показали индекс погружённости в цифровую среду больше 40 баллов.

В группу со слабым погружением в Интернет вошли 96 подростков (возраст – 14,1 лет), которые показали индекс погружённости в цифровую среду меньше 28 баллов.

Сравнение результатов выполнения теста Р. Амтхауэра глубоко и слабо погружёнными в Интернет подростками при помощи критерия Манна – Уитни[5] говорит о том, что глубоко погружённые в интернет-среду подростки имеют более высокие средние значения по всем субтестам теста Амтхауэра. Группа глубоко погружённых несколько более однородна по своим характеристикам – имеет меньшие стандартные отклонения.

Полученные нами данные полностью согласуются с признаками позитивного влияния использования компьютера на развитие интеллекта в целом и отдельных структурных компонентов – вербального, математического и пространственного.

На следующем этапе работы было выдвинуто предположение о различиях в мышлении глубоко и слабо погружённых подростков в зависимости от содержания их деятельности в интернет-среде. Значимых различий между теми, кто пользуется социальными сетями, мессенджерами, скайпом, чатами, скачивает аудио, видео и другой контент, смотрит новости в Интернете, не выявлено.

Больше всего статистически значимых различий по показателям интеллекта наблюдается среди тех, кто в разной мере пользуется электронной почтой, учится в Интернете, использует его для культурного развития и играет онлайн.

Учёба в Интернете полезна для некоторых функций мозга

Показатели внимания и памяти имеют наиболее низкие значения у тех подростков, которые редко обращаются к интернет-ресурсам для решения учебных задач, а у тех, кто делает это часто, они ниже, чем у

[5] **Критерий Манна – Уитни** – статистический критерий, используемый для оценки различий между двумя независимыми выборками по уровню какого-либо признака, измеренного количественно.

никогда не использующих Интернет для учёбы. Это может свидетельствовать о различиях в формировании механизмов памяти при оперировании материалом с онлайн-доступом и без него. Работа с учебной информацией – книги, учебники, образовательные сайты и сервисы – способствует повышению осведомлённости подростка.

Интернет содействует расширению житейских и научных знаний из различных областей, увеличению словарного запаса, развитию способности к логическому отбору информации и актуализации знаний, необходимых для решения задач. В учебной интернет-деятельности вероятно формирование установки на отсутствие необходимости запоминания и хранения в памяти информации, легко доступной и в любой момент восстановимой для дальнейшего использования.

Влияние игр в Интернете

Игры в Интернете в целом также дают негативный эффект в освоении целого ряда вербальных операций. Нечастое обращение к компьютерным играм не препятствует поиску аналогий и пониманию логических закономерностей. Задания на внимание и память также выполняются более успешно подростками, не увлечёнными играми в Интернете.

Как правило, сообразительность и подвижность мышления являются преимуществами любого игрока. В то же время чрезмерная игровая активность подростка, особенно в онлайн-играх, которые более динамичны и проще в логическом плане, не способствует развитию вербально-логического анализа, но предъявляет более высокие требования к коммуникации и побуждает к риску. Вероятно, до определённой степени игры могут стимулировать развитие индуктивного мышления, самостоятельности мышления, но при большой увлечённости ими освоение реальности отходит на второй план из-за виртуальности содержания деятельности.

Активные интернет-игроки проявили несколько более высокую способность к математическому обобщению и абстрагированию, индуктивному логическому мышлению и оперированию числами. Таким образом, игры в Интернете, по-видимому, дают возможность развивать теоретический и практический математический интеллект.

Электронная почта

Несмотря на то, что использование электронной почты оказалось связано с достаточно большим числом интеллектуальных показателей, его следует считать довольно слабым показателем интернет-активности современных подростков. Она не очень популярна, так как есть более удобные для них средства связи – чаты, мессенджеры, скайп, социальные сети.

Заключение

Можно констатировать, что вовлечённость в интернет-среду в целом выступает положительным фактором развития мыслительных функций и операций. С другой стороны, при анализе взаимосвязей содержания и степени погружённости в интернет-среду с мышлением можно обнаружить их неоднозначность как с точки зрения влияния различных сервисов, так и частоты пользования ими.

В тех случаях, когда интернет-среда является лишь одним из средств развития и не приобретает глобального значения как источник информации, коммуникации и развлечений, можно говорить о её локальном позитивном влиянии на интеллектуальное развитие подростков.

Больше всего статистически значимых различий по показателям интеллекта наблюдается среди тех, кто в разной мере пользуется электронной почтой, Инстаграмом, учится в Интернете, использует его для культурного развития и играет онлайн. Наиболее негативное влияние на развитие вербального, математического и пространственного компонентов интеллекта оказывает частое обращение к Инстаграму, вероятно, в силу преобладания в нём конкретно-визуального контента при отсутствии задач его вербализации и систематизации.

Использование Интернета для интеллектуального и культурного развития в целом способствует развитию интеллекта: чем чаще подростки используют Интернет для учёбы, тем выше показатели большинства вербальных и невербальных субтестов. Негативное влияние интенсивной интернет-активности в учебных целях может сказываться на функции внимания и памяти.

Как воспитать здорового подростка? // НаркоНет. – 2021. – № 11. – С. 18–36.

В подростковом возрасте огромную значимость имеют друзья, группа сверстников. Ребёнок утверждается в этом мире, познаёт себя. Жизнь в соцсетях, в виртуальном мире накладывает отпечаток на их мышление, чувства и поведение. В социальной психологии эффект принадлежности к группе заключается в том, что, когда мы ассоциируем себя с какой-то группой, то мы думаем с позиции этой группы, чувствуем, строим отношения и действуем по определённым моделям.

Педагог и учёный В. А. Плешаков ввёл термин «киберсоциализация». Он и многие другие учёные говорят о том, что институтом социализации становится Интернет. Оттуда дети берут ответы на вопросы, которые их волнуют. Во многом здесь ребёнок ищет ответы, чтобы понимать: кто я, к какой группе принадлежу, какие буду строить планы на жизнь, что для меня значимо, какие у меня ценности и так далее. Это надо понимать и обязательно учитывать. Он там сидит целыми днями. Он там развивается? Надо знать, что он там смотрит, в каких группах состоит, что на него может воздействовать.

Критериями интернет-зависимости можно считать критерии, свойственные любому виду аддикции[6].

1. Сверхценность этой деятельности.
2. Конфликт с окружающим миром и внутриличностный конфликт.
3. Симптом отмены.
4. Рост толерантности, терпимости к этому.
5. Эйфория.
6. Возможность рецидива.
7. Изменчивость настроения.
8. Включение в интернет-деятельность в ущерб реальной деятельности.

Зависимость от компьютерных игр

Зависимость от компьютерных игр – ещё один вид кибераддикции, и это настоящий бич нашего времени, потому что игры обладают

[6]**Адди́кция** (англ. *addiction* – зависимость, пагубная привычка, привыкание) – ощущаемая человеком навязчивая потребность в определённой деятельности.

большей аддиктогенностью, чем другие виды деятельности в Интернете.

Причины игровой зависимости

1. Эскапизм[7].
2. Неудовлетворённость своим социальным статусом.
3. Отыгрывание своей социальной роли.
4. Нереализованность потребностей в принципе.
5. Нереализованность потребностей в самостоятельности и свободе.
6. Получение необычных впечатлений.
7. Потребность в релаксации.
8. Привлекательность игр усиливается их красотой и реалистичностью изображения.

Далее указывалось на проблемы с цифровой этикой, то есть технологии развились, но как себя вести, общаться в Интернете? Этичность, следование нравственным нормам и правилам поведения в Сети отсутствуют. Мы видим это в таких проявлениях, как агрессия в Интернете, кибербуллинг, оскорбления, унижение. Такое поведение может даже подтолкнуть к суициду, особенно в подростковом, уязвимом возрасте, когда идентичность только развивается, и самооценка формируется.

Простого технического ноу-хау по управлению цифровыми системами связи уже недостаточно. По словам экспертов, необходимы более широкие социальные и даже межкультурные навыки общения и взаимодействия с людьми из отдалённых, возможно, различных культурных слоёв.

Эмпатия очень важна для поддержания межличностных отношений любого рода с помощью цифровых систем. Поскольку ожидается, что такая тенденция, как удалённая работа, будет развиваться, эксперты подчеркивают важность для молодёжи навыков общения и сотрудничества. Согласно исследованиям, современные дети лучше понимают язык смайликов, чем эмоции друг друга при общении онлайн, поскольку мало коммуницируют вживую, у них слабо развита эмпатия.

[7]**Эскапизм**, эскепизм, эскейпизм (англ. *escape* – «сбежать, спастись») – стремление уйти от реальности в мир удовольствий.

Общение в Интернете тоже должно строиться на эмпатии, на понимании другого человека. Глобализация позволяет общаться с любым человеком, и даже языки уже не преграда, так как в Интернете есть возможность перевода. Коммуникация становится всё доступней, поэтому у детей важно формировать понимание мира другого человека, уважение к разным культурам.

Критическое мышление

Также экспертами отмечалась важность развития навыков критического мышления. Цифровой мир требует, чтобы пользователи были более осведомлены о связях, отношениях и мотивах воздействия предоставленной информации. Цифровой мир, цифровая трудовая жизнь – это не столько технические вопросы, сколько вопрос, как мы действуем, насколько мы осведомлены об этих процессах.

Надо понимать, откуда берётся информация, на что она воздействует, каковы её задачи, как она может повлиять. Обязательно нужно учить детей различать фейковую, ложную информацию, понимать, где можно найти правдивые источники качественной информации, проверенные.

Дилемма

Конечно же, некая дилемма стоит перед нами, это основное противоречие на сегодняшний день в информационной безопасности. С одной стороны, мы должны обеспечить детей возможностью осваивать цифровой мир, иначе они не смогут адаптироваться к новым профессиональным вызовам, а с другой стороны, очень много интернет-рисков, которые приводят к негативным последствиям, в том числе кибераддикции, залипанию в Интернете в ущерб другим интересам.

Нам нужно думать о том, что детям придется работать в Интернете, не отвлекаясь, хотя, конечно, развлечения, релаксацию тоже никто не отменял. Но всё-таки основная функция человека – созидание, реализация в профессии, когда работа нравится, ты её любишь, она приносит удовлетворение. Найти здесь золотую середину – задача родителей.

Реан А. Буллинг: руководство для родителей / А. Реан // Не будь зависим. – 2021. – № 11. – С. 35–46.

С распространением интернет-технологий и массовой мобильной связи увеличилась виртуальная активность детей в социальных сетях. Так появился новый вид буллинга с использованием современных технологий общения – кибербуллинг. Это совокупность агрессивных действий в адрес конкретного человека через унижение с помощью мобильных телефонов, сети Интернет и иных электронных устройств.

Проявления кибербуллинга

1. Отправка оскорбительных сообщений.
2. Передразнивание в режиме онлайн.
3. Размещение в публичном доступе личной информации, направленной на причинение вреда или унижение другого человека.
4. Ведение блогов или форумов в социальных сетях, целью которых является оскорбление и унижение человека, принесение ему психологических переживаний и страданий.

В последнее время именно этот вид буллинга становится доминирующей формой агрессии. Часто он сопровождается другими формами насилия.

Кибербуллинг – скрытый для окружающих процесс, но дети, которые подверглись травле в виртуальном пространстве, получают не менее серьёзную психологическую травму различной степени тяжести, поэтому от родителей требуется особое чуткое внимание к фактам его проявления.

Как родители могут помочь своим детям противостоять кибербуллингу

1) Быть в курсе того, какую активность ребёнок проявляет онлайн, какие сайты посещает.
2) Можно поставить «Родительский контроль». Но это не панацея, не стоит на него полностью полагаться.
3) Если вам удастся проявить искренний интерес к самым любимым сайтам ребёнка и узнать о них побольше, и от него и самостоятельно, это будет хорошим фактором повышения кибербезопасности ребёнка.

4) Хорошо, если ребёнок согласиться «дружить» с вами в соцсетях. Если отказывается дружить с вами – это его право, но, может быть, он согласится дружить с каким-то другим взрослым, с которым у вас есть контакт.
5) Попросить у ребёнка пароли от его аккаунтов и пообещать, что воспользуетесь ими только в случае крайней необходимости. Обязательно сдержите слово. Попытки «шпионить» за детьми приводят зачастую к быстрому разоблачению родителей и полному исчезновению у ребёнка доверия. После этого у родителя остается очень мало шансов узнать о происходящем, если ребёнок действительно окажется в опасной ситуации.
6) Договориться с ребёнком о том, что он сразу расскажет вам, если окажется в ситуации кибербуллинга. Заверить его, что при этом вы не отберёте у него телефон или компьютер, и сдержать слово.

Обучите ребёнка некоторым правилам безопасности в Сети
1) Научите ребёнка хорошенько думать с том, что он публикует в Сети. Научите его никогда не делиться тем, что потом может поставить его в неловкое положение: будучи однажды помещённой в Сеть, информация перестает принадлежать человеку. Это очень важно усвоить.
2) Предложите ребёнку задуматься над тем, кому он может доверить доступ к своей личной информации: будет ли его страница открыта для всех или только для друзей.
3) Научите его ни с кем, кроме вас, не делиться своими паролями.

Если есть факты кибербуллинга, надо:
1) Не отвечать на оскорбительные сообщения и не пересылать их.
2) Сделать скриншоты, оставить доказательства того, что были нападки.
3) Заблокировать пользователя, от которого исходят оскорбительные сообщения.
4) Сообщить провайдеру или руководству соцсети или сайта о том, что правила их сервиса нарушаются (в случае с кибербуллингом это почти всегда так).

Краткие методические рекомендации для родителей

Если вы узнали, что ваш ребёнок подвергается травле

1. Не забывайте, что ничто не оправдывает издевательств!
2. Ребёнок, ставший жертвой издевательств, может быть не готов обсуждать это.
3. Не пытайтесь сделать события менее значимыми или использовать иронию. Не предлагайте быстрые решения и не обвиняйте никого.
4. Только сам ребёнок может оценить, чувствует он себя хорошо и безопасно или чувствует угрозу от чьего-то поведения.
5. Не только школа и учителя несут ответственность за случаи издевательства.
6. Поймите страх вашего ребёнка перед издевательствами.
7. Каждый человек имеет право и даже обязан немедленно пресечь травлю.
8. Рассмотрите вероятность того, что ваш ребёнок не сказал учителю, что его травят, что он не может рассказать вам всё или что он может исказить некоторые детали.
9. Как родитель вы не можете потребовать, чтобы ваш ребёнок был популярен в классе, но вы вправе рассчитывать на то, что, если он относится к другим с уважением, то к нему тоже будут относиться с уважением.

Если вы замечаете признаки травли своего рёбенка

1. Сохраняйте спокойствие и подумайте, как бы вы могли обсудить этот вопрос с ребёнком.
2. Поговорите с ребёнком и скажите, что вы заметили, что у него проблемы.
3. Пообещайте ребёнку, что не будете сердиться на него, если он расскажет всё.
4. Обсудите с ребёнком шаги, которые необходимо предпринять, чтобы остановить травлю.
5. Свяжитесь со школой и спросите, что вы могли бы сделать вместе, чтобы остановить буллинг.
6. Оцените свои знания и навыки, необходимые для того, чтобы справиться с ситуацией.

Если вы узнали, что ваш ребёнок – зачинщик травли, помните:

1. Агрессор не плохой ребёнок, и вы не плохой родитель.

2. Чтобы изменить поведение агрессора, он должен чётко понять, что оно неприемлемо.
3. Быть источником издевательств или их объектом не является естественной частью взросления.
4. Агрессором часто движет опасение, что его положение в классе или группе нестабильно.
5. Поведение агрессора не изменится, пока его поддерживают свидетели или люди, чьё мнение для него важно.

Грибов Д. Дети в соцсети / Д. Грибов // Не будь зависим. – 2022. – № 2. – С. 2–16.

Одной из первых социальных сетей в стране стала сеть «ВКонтакте». Эта площадка позволяет пользователям отправлять сообщения, создавать собственные страницы и сообщества, обмениваться изображениями, тегами, аудио- видеозаписями, играть в браузерные игры. «ВКонтакте» занимает первое место по длительности пребывания российской мобильной аудитории и первое место по обмену сообщениями и количеству публикаций в России.

Рунет несёт в себе огромное количество нежелательного для детской психики контента. И существует множество способов оградить ребёнка от этого, например, регламентировать время за компьютером или в Интернете, контролировать все сферы интересов вашего ребёнка в рамках Сети.

Интернет нельзя воспринимать как однозначно плохое место, где можно встретить только угрозы. Интернет дает нам очень многое. В то же время надо знать о подводных камнях и уметь их обходить.

Во-первых, надо обращать внимание на сохранность приватных данных, право человека на сохранение в цифровом мире информации, которая принадлежит ему. Интернет развивается очень быстро, все цифровые сервисы тоже очень быстро развиваются. Пользователь оставляет огромное количество информации – фотографии, геометки, посты и комментарии, в том числе к различным видео. Важно объяснить ребёнку с самого начала, как только он начинает использовать Интернет, чтобы он не публиковал личную информацию, в частности, персональные данные, данные паспорта.

Во-вторых, отметим проблему кибербуллинга, когда травля происходит 24 часа в сутки 7 дней в неделю, и ребёнок не знает, как с

этим бороться, как поступить. Задача родителей – создать такие условия, чтобы ребёнок в случае возникновения каких-то вопросов, негативных ситуаций всегда мог к ним обратиться. Есть такие вещи, которыми дети не готовы делиться, поскольку не знают, как отреагируют родители. Поэтому с ребёнком стоит поговорить о том, что, если он столкнулся с кибербулингом, он должен заблокировать обидчика, добавить в чёрный список и ни в коем случае не отвечать на комментарии.

Одна из проблем Интернета – это онлайн-мошенничество, различные способы обмана с целью похитить данные пользователя. Ими могут быть логин и пароль от социальной сети, от игрового сервиса, данные банковской карты и любые персональные данные. Дети зачастую не знают, какие методы могут использовать злоумышленники, чтобы эту информацию выудить.

Например, существует спам. Спам – способ обмана, когда мошенники прикрываются известным брендом или именем, чтобы получить деньги от пользователя. Они используют рекламу в соцсетях, предлагая пройти опрос или принять участие в розыгрыше лотереи. Вы участвуете в бесплатной лотерее, отвечаете на лёгкий вопрос, например, что вы любите больше всего есть на ужин, и даётся 4 варианта ответа. Якобы любой ответ приведёт вас к большому выигрышу. Дети могут поверить, а в дальнейшем им нужно будет оплатить, скажем, 200 или 300 рублей, чтобы получить свой выигрыш. Естественно, они ничего не получат.

Мы каждый год проводим исследования, и сами дети говорят о том, с какими угрозами они могут столкнуться. На первом месте у них – материалы для взрослых. Дети воспринимают эту ситуацию как угрозу для себя, потому что могут случайно найти такой контент, перейдя по баннеру на какой-то сайт. И под материалами для взрослых имеется в виду не только порнография, материалы, связанные с сексом, переписка, фото и видео, но и ненормативная лексика, и контент, связанный с алкоголем, наркотиками и насилием. Конечно, родители должны использовать технические решения, чтобы ограничить ребёнка от таких случайных переходов.

Конечно, желательно, чтобы родители понимали, что цифровая безопасность – это не только антивирусные программы, а именно родительский контроль. Многие родители продолжают по истории по-

иска или проверке браузера пытаться понять, что же ребёнок искал в Интернете. Но это не очень эффективно и выглядит как прошлый век. При этом сильно портит отношения между родителями и детьми, потому что дети уже в младшем возрасте воспринимают это как вмешательство в их частную жизнь. Хотя, казалось бы, любой родитель скажет: «Так, подожди, у нас не должно быть секретов, я посмотрю».

Есть намного более эффективные способы, позволяющие узнать, чем интересуются ребёнок. Возможно, он случайно перешёл по ссылке и нашёл какую-то информацию, которая ему по возрасту ещё не подходит. Он может даже это пропустить. А вот если он периодически, например, интересуется темой, связанной с насилием или с нецензурной лексикой, здесь уже повод поговорить. Может быть, его что-то беспокоит, может быть, он эту информацию узнаёт из каких-то других источников.

На сайте *VK* есть очень подробная инструкция в поддержку пользователей. Если что-то не получается, предоставляется техническая поддержка. Кроме того, родители должны знать новые способы мошенничества, с которыми можно встретиться в Интернете, и рассказывать об этом своему ребёнку.

3. Формирование информационной культуры и медийной грамотности читателей в деятельности современных библиотек

Маслова О. Безопасный Интернет для всех / О. Маслова // Современная библиотека. – № 5. – С. 30–33.

В рамках Недели безопасного Рунета Рязанская областная детская библиотека провела круглый стол «Безопасный Интернет для всех!». В 2021 и 2022 гг. он проходил как видеоконференция в *Zoom*. Большинство докладов посвящены реальным опасностям Сети. Темы докладов нередко связаны с повесткой информационных агентств, такими ситуациями, как скулшутинг[8], челенджи[9] на «выбывание», рост экстремистских тенденций в стране. Все эти тенденции уходят корнями в Интернет. И школьников виртуозно вовлекают в тематические паблики, влияют на их мировоззрение и поступки.

Эта повестка венчает и без того неутешительную, сложившуюся за годы «дикого Рунета» картинку: дети массово имеют доступ к девиантным страницам в соцсетях, где сформированы чёткие схемы вовлечения школьников в группы смерти, в распространении запрещенных веществ селфхарма[10] и суицида. Эксперты, выступившие на нашем круглом столе, анализируют так называемый деструктивный контент соцсетей – в примерах, скриншотах, цитатах из пабликов. Политолог и глава информационно-аналитического центра «Граница настоящего» Яна Амелина (г. Москва) ведёт мониторинг пабликов, посвящённых колумбайнингу[11]. Калейдоскоп тем, фактов и острых

[8] **Скулшутинг** (от англ. *school shooting* – «школьная стрельба») – это вооружённое нападение в учебных учреждениях, применение вооружённого насилия на территории образовательных учреждений.

[9] **Челендж** (англ. *Challenge* – варианты перевода: «вызов», «преодоление препятствий», «совершение определённого действия на спор») – жанр интернет-роликов, в которых блогер выполняет задание на видеокамеру и размещает запись в Сети, а затем предлагает повторить это задание своему знакомому или неограниченному кругу пользователей.

[10] **Селфхарм** (от англ. *self-harm* – «самоповреждение», «членовредительство» (по отношению к себе)) – это агрессия, направленная на себя, которая проявляется в разных формах причинения самому себе вреда.

[11] **Колумбайнинг** (от «Колумбайн» (англ. *Columbine High School*) – это название старшей школы в США, в которой в 1999 году произошло самое громкое вооружён-

вопросов в ситуации, когда правовое поле Рунета всё ещё не получило окончательных механизмов регулирования, ярко отражён в разнообразии выступлений 2021–2022 гг.

Юрий Афанасьев (г. Череповец), директор АНО[12] «Центр информационной безопасности в сети Интернет "«Защита"», раскрыл последние тенденции распространения «психоактивных и новых психоактивных веществ» через Интернет.

Среди других тенденций последних двух лет:

- информационный разрыв между поколениями, когда взрослый человек даже и не понимает толком, от чего именно обезопасить ребёнка. Так, мы твердим детям о вреде сигарет, а их подсаживают на совсем другие вещества. И с каждым годом это новый класс веществ;
- «эклектика» деструктивного контента (разнообразные сочетания деструктивных тем);
- риски в информационной безопасности: от подростковых иллюзий в Рунете (безнаказанность и вседозволенность) до плохой зашиты цифровых платформ, обслуживающих нужды школы;
- омоложение деструктивных сообществ в социальных сетях;
- особая необходимость профилактики рисков среди дошколят, которые массово становятся пользователями гаджетов и соцсетей.

Предупредить и просветить

Педагоги, библиотекари, родители, наставники детства знакомили с суровой реальностью Рунета, учили бдительности. Но в противовес тревожной информации в программе круглого стола есть «якоря» добрых начинаний, идеи просвещения и профилактики опасностей. Наши встречи, обсуждения помогают узнать о программах обучения, медиаграмотности, об АНО, которые разрабатывают информационные буклеты, видеоматериалы. Библиотекари, педагоги получили эти материалы в доступ, чтобы присоединиться к образовательному проекту.

ное нападение учеников на своих одноклассников) – это вооружённое нападение обучающегося или стороннего человека на учащихся внутри образовательного заведения.

[12] **АНО** – Автономная некоммерческая организация.

Так, профилактическую работу с родителями, мониторинг и официальную экспертизу социальных страниц проводят специалисты АНО «ЦЗДИУ»[13] – давние участники из Рязани. Александр Дубинин, руководитель Школы безопасности «Свет» (г. Смоленск) придумал проект «Медиагигиена в каждый дом», он стал победителем в номинации «Просветительский *IT*-проект года – 2021».

Римма Желтоухова – глава рязанского филиала Национального мониторингового центра помощи пропавшим и пострадавшим детям – представляла собственную программу, обучающие пособия, буклеты, где в доступной форме описаны риски, раскрыты пути верификации[14] фактов и собеседников «из Сети».

Педагоги городских школ не просто были слушателями, но и не раз выступали с докладами, делились собственными инициативами просвещения, профилактики в школе. Наталья Ашеулова, социальный педагог школы № 10, подготовила доклад «Школьник и Интернет: как избежать ловушек и получить пользу?». Ольга Еременко (школа № 60) рассказала коллегам, как пробует сделать Интернет безопасным для младшеклассников, Галина Морозова (школа № 23) – как формируют представление о безопасном поведении у обучающихся с особенностями здоровья, интеллекта. Естественно, подобные тенденции, за годы взращённые усилиями общественников и педагогов, теперь подкреплены «запросами» к государству, прогосударственным корпорациям на консолидированные усилия. А в 2022-м на круглом столе с приветственным словом выступила детский омбудсмен Рязанской области Анжелика Евдокимова. Упомянув, что в 2021 г. был создан «Альянс по защите детей в цифровой среде» (объединение девяти крупных технологических, цифровых и медиакомпаний России для разработки в Рунете позитивного контента), омбудсмен призвала регион присоединиться к всероссийской хартии «Цифровая этика детства».

В программу Недели безопасного Рунета были включены не только дискуссии для взрослых, но и творческие мероприятия для детей, когда они учились опознавать риски в Рунете. Так, в 2020 г. в пред-

[13] **ЦЗДИУ** – Центр защиты детей от интернет-угроз.

[14] **Верификация** в различных сферах деятельности человека может подразумевать: подтверждение того, что заданные требования выполнены, через предоставление объективных свидетельств.

дверии круглого стола прошёл областной конкурс детских творческих работ «Сказка о безопасности в Интернете». В необычном соревновании приняли участие более 30 юных авторов не только из Рязанской, но и из Нижегородской области. Победительница отличилась «Сказкой про трёх беспечных поросят». В жанре инфографики[15] участники 9–16 лет обозначали опасности Интернета, «умное» использование гаджетов, правила сохранения личных данных. В творческом конкурсе к XI круглому столу – областном конкурсе социальных видеороликов «Я в контенте» участники снимали видеосюжеты на тему безопасного поведения в Рунете.

Данильчук Т. Формирование информационной культуры – одно из ключевых направлений в деятельности школьной библиотеки / Т. Данильчук // Школьная библиотека. – 2022. – № 5. – С. 28-29.

В информационно-библиотечном центре нашей школы мы постарались создать современное комфортное пространство. В настоящее время ИБЦ (информационный библиотечный центр) школы состоит из двух библиотек: для 1–4-х классов и для 5–11-х классов.

Библиотека для 5–11-х классов разделена на зоны, которые напрямую связаны с процессом обучения и являются помощниками в формировании информационной культуры школьников и в учебно-воспитательном процессе. Зона коворкинга представляет собой идеальную площадку для проведения семинаров, конференций, открытых уроков, интерактивных викторин. Здесь находится интерактивная панель с хорошей акустической системой. В компьютерной зоне расположены 30 посадочных мест для пользователей библиотеки с доступом к Интернету. Мультимедийно-выставочная зона позволяет оформить интерактивные выставки, которые наполняют пространство новыми смыслами и с помощью современных технологий рассказывают о мире автора на актуальном времени языке.

Особое внимание мы уделили созданию разных читательских зон и особой комфортной среды для общения. Зона тихого чтения, зона

[15] **Инфографика** (от лат. *informatio* – преподношение, разъяснение, изложение; и др.-греч. *γραφικός* – письменный, от *γράφω* – пишу) – это графический способ подачи информации и данных с целью быстрого и чёткого преподнесения сложной информации.

группового обсуждения предназначены для чтения, отдыха и общения, проведения мастер-классов. В зоне абонемента стеллажи открытого доступа дают возможность читателям самостоятельно выбрать научно-познавательную, справочную, художественную литературу. Фонд русской и зарубежной классики, современной художественной литературы, научно-познавательной, справочной и учебной литературы составляет 37 738 единиц хранения.

Библиотека располагает современной базой, техническими средствами доступа к информации на любых носителях. Подписание соглашения с Президентской библиотекой позволило открыть удалённый электронный читальный зал и получить доступ к качественным источникам информации. Читатели из начальной школы и 5–8-х классов имеют возможность получать знания на образовательных платформах «Учи.ру», «Я-Класс» и др.

С первых дней открытия школы (2017 г.) приоритетной в работе библиотеки стала программа по формированию информационной культуры учащихся. Программа «Информационная культура школьника» разработана, адаптирована и реализуется на основе учебно-методического комплекса для учащихся 5–7-х классов Занятия проходят в информационно-библиотечном центре. Цифровизация, оснащение техникой, выигранные школой гранты помогли нам сделать программу метапредметной дисциплиной. Содержание курса позволяет использовать различные типы уроков. Учащимся нравятся зачётные уроки, которые проходят в конце каждого изучаемого раздела в программе в виде теста и в виде игры. Анализируя результаты зачётных уроков, мы отметили проблемы с формированием метапредметного результата: копирайт-мышления, интернет-мышления, выделения общего и частного, систематизации информации по признакам. Формированию информационной культуры учащихся способствуют образовательные интенсивы, которые проходят в информационно-библиотечном центре на базе современной музейно-образовательной площадки. Экспозиция музейно-образовательной площадки «Держава, Державин и я» включает в себя изобразительный, книжный, документальный, предметный ряды и аудиовизуальное сопровождение. Образовательные интенсивы включают в себя информационный блок, интерактивный блок, блок рефлексии. Реализация проекта стала возможной благодаря тому, что коллектив единомышленников школы в

2021 году выиграл грант на сумму 5 млн рублей в рамках национального проекта «Образование».

Иванченко А. Как создать цифровую библиотеку в школе? / А. Иванченко // Школьная библиотека. – 2022. – № 5. – С. 30–38.

Как организовать работу цифровой библиотеки в школе?

На наш взгляд, цифровая (электронная) библиотека в широком смысле – это комплекс организационных, программных и технологических инструментов, предназначенных для обеспечения образовательной деятельности различными видами цифрового контента, автоматизации основных процессов библиотечно-информационного обслуживания и интегрированных на уровне пользовательских данных с библиотечно-информационными сервисами, электронными и публичными библиотеками, цифровыми образовательными ресурсами и платформами.

Такая библиотека может быть построена как набор самостоятельных сервисов, которые будут предоставляться пользователям библиотеки как услуги по сбору, обработке, хранению, представлению и передаче информации. Определим их примерный набор и функциональность.

Базовый набор сервисов:

- автоматизированная библиотечно-информационная система (АБИС), обеспечивающая создание и ведение электронного каталога путём создания собственных или заимствования готовых библиографических записей из внешних ресурсов;
- система хранения собственного контента образовательной организации в различных форматах, обеспечивающая полнотекстовый поиск и регламентированный онлайн-доступ;
- доступ к внешним ресурсам и электронным библиотечным системам, образовательными просветительским ресурсам и платформам;
- сайт библиотеки или раздел на сайте образовательной организации для информирования пользователей, организации виртуальных выставок, публикации дайджестов и пр.

Основной набор сервисов:

- система автоматизации процессов книгообеспеченности и комплектования, интегрированная с федеральными региональными

перечнями учебников и каталогами ведущих поставщиков контента;
- доступ к верифицированному контенту «Библиотеки цифрового образовательного контента» и сервису «Цифровой помощник ученика», разрабатываемых в рамках Стратегии цифровой трансформации образования РФ;
- дискавери-сервис, позволяющий через единую точку входа (поисковую строку) объединять в поисковой выдаче ресурсы различных поставщиков контента, включая вопросы образовательных онлайн-платформ;
- сервис избирательного распространения информации (ИРИ), позволяющий рассылать уведомления об окончании срока выдачи литературы, новых поступлениях в библиотеку, проводимых мероприятиях и пр.;
- сервис аналитики и подготовки отчётов, позволяющий вести текущий учёт деятельности библиотеки и собирать статистическую отчётность в автоматическом режиме;
- личный кабинет, в котором в зависимости от прав пользователя отображается информация о фондах библиотеки, читателях, выданных изданиях, сроках сдачи, обеспечена возможность рассылать сообщения, готовить отчёты и т. д.).

Дополнительный набор сервисов:
- автоматизированная книговыдача на основе технологии штрихкодирования;
- электронный читательский билет, интегрированный с пропуском, социальной или банковской картой, мобильным приложением и др.

Какие электронные ресурсы и цифровые сервисы можно использовать в работе?

Рассмотрим подробнее базовый набор прикладных сервисов для цифровой (электронной) библиотеки и имеющиеся сегодня решения.

Автоматизированная библиотечно-информационная система (АБИС)

Сегодня среди отечественных АБИС существует немало решений, поддерживающих основные процессы автоматизации библиотечно-информационной деятельности, но далеко не все из них отвечают по-

требностям школьных библиотек в силу избыточности своего функционала, сложности администрирования, необходимости существенных расходов на поддержание работоспособности, оплату работы специалистов и т. д.

АБИС семейства «МАРК» предназначены для комплексной автоматизации процессов библиотечной работы в организациях различных категорий, в том числе в учреждениях общего и среднего профессионального образования.

Возможности АБИС семейства «МАРК» позволяют библиотеке с использованием различных источников заимствования готовых записей сформировать электронный каталог литературы и предоставить широкий доступ к нему и личному кабинету читателя через Интернет, наладить автоматизированные учёт литературы, комплектование и книговыдачу, на лету формировать множество статистических отчётов и выходных форм (от каталожной карточки до инвентарной книги), автоматически рассчитывать книгообеспеченность учебного процесса и др. Поддерживается интеграция с различными видами современного библиотечного оборудования, с внешними поставщиками цифрового контента (ЭБС) и информационными системами.

Доступ к электронным библиотечным системам

Электронно-библиотечная система образовательной организации может быть создана как с помощью отдельного программного комплекса, эксплуатируемого непосредственно в образовательной организации, так и с помощью совокупности подобных комплексов, агрегаторов контента, ряд из которых эксплуатируется внешними операторами, если они образуют единую информационную систему, используемую в образовательной организации.

Для организации доступа к внешним электронным библиотечным ресурсам мы рекомендуем обратить внимание на следующие ресурсы.

1) Мобильное приложение НЭБ «Свет»

Бесплатная платформа для чтения на персональных устройствах пользователей, на которой собрана коллекция из более чем 1 800 произведений мировой классики, современных бестселлеров и научно-популярных книг, представлены известные экранизации, увлекательные тесты, таймер чтения и счётчик персональных рекордов. Приложение поможет расширить кругозор, подготовиться к урокам или восполнить пробелы в школьном образовании. Книги созданы на плат-

форме Национальной электронной библиотеки с соблюдением всех авторских прав.

В приложении можно:

- искать книги по названию или автору, по тегам и рекомендованному возрасту, а также по объёму;
- изучать литературу и науку с помощью статей и подборок от литературоведов, преподавателей, учёных и популяризаторов знания;
- искать в сторис интересные факты, рекомендации и разборы произведений;
- смотреть фильмы и спектакли из коллекции сервиса Культура.рф *(www.culture.ru)*;
- проверить полученные знания с помощью интерактивных тестов;
- поставить цель по количеству прочитанных книг на год и спланировать свой комфортный темп чтения.

Подробная информация на сайте проекта: *https://svetapp.rusneb.ru*.

2) «Литрес: Школа»

Электронная библиотека в удобном формате от крупнейшего сервиса электронных и аудиокниг. Благодаря сервису преподаватели и читатели получают доступ к каталогу, разработанному специально для школьной среды. Каталог включает в себя более 9 000 произведений художественной, научно-популярной и учебной литературы, в т. ч. на иностранных языках. Здесь также можно найти словари и актуальные справочники ОГЭ/ЕГЭ. Бесплатная коллекция насчитывает более 2 500 электронных произведений.

Чтобы выдавать книги читателям, библиотекарю не нужно тратить время на формирование книжного фонда – весь каталог уже таковым является, библиотекарь просто предоставляет читателю доступ к произведению посредством книговыдач. При этом стоимость такой книговыдачи фиксированная, что позволяет оптимизировать бюджет на комплектование школьной библиотеки. Кроме того, библиотекарю доступен широкий интуитивно понятный функционал: создание читательских билетов индивидуальное и массовое – посредством *Exel*-таблиц, формирование групп читателей, создание книжных подборок, которые можно выдавать читателям посредством пары кликов, а также выгрузка статистики, прикрепляемой к внутренним отчётам орга-

низации. Возрастные ограничения в системе соблюдаются автоматически. Читатель получает доступ к библиотеке через бесплатное мобильное приложение. Отдельно хочется отметить возможность работы с текстом, которую предоставляет приложение.

«ЛитРес: Школа» решает вопрос комплектования, и цифровизации образовательного пространства. На базе такой электронной библиотеки школа сможет реализовать интерактивные мероприятия для учащихся, направленные на популяризацию чтения.

3) Электронная библиотека *ELiSKiosk.*

Программа автоматически скачивает 4 100 интерактивных электронных образовательных ресурса из «Медиатеки Москвы», бесплатных для использования в школе, и 600 произведений русской классики в формате *epub* и создаёт всего в несколько кликов электронную библиотеку с навигацией по скачанным ресурсам.

4) Национальная электронная детская библиотека (НЭДБ)

Это бесплатная еженедельно пополняемая коллекция оцифрованных материалов из фондов РГДБ, библиотек-партнёров, частных коллекций. Особенностью библиотеки являются старинные редкие издания, дореволюционная и советская периодика, диафильмы, современная литература для детей и о детях. Интерфейс НЭДБ снабжён разветвлённым, но интуитивно понятным аппаратом выбора и поиска и удобными средствами просмотра, адаптированными под разные виды материалов.

Содержимое электронной библиотеки для удобства навигации сгруппировано по видам материалов – это книги, журналы, газеты, диафильмы. Все материалы распознаны, поэтому поиск ведётся не только по метаданным, описывающим материал, но и по его содержимому. Для просмотра выбранного материала используется специальный элемент, который адаптируется для просмотра разных видов материалов. Для книг и журналов наиболее подходящим является виртуальная книга, которую можно развернуть на полный экран и листать стрелками на клавиатуре или кликами мыши на страницах.

Подробная информация на сайте библиотеки: *https://arch.rgdb.ru/xmlui.*

Спроектируем будущее цифровой (электронной) библиотеки. Итак, цифровая библиотека школы интегрируется с другими смежными системами и начинает использовать данные:

- об учениках;
- о читательских активностях в других библиотеках, электронных и общедоступных.

Используя эти данные, во-первых, рутинные процессы можно заменить на автоматизированные, во-вторых, смоделировать новые сервисы:

- рейтинг читателя с учётом всех практик чтения, а не только в школьной библиотеке;
- мониторинг востребованности контента библиотеки с учётом образовательных программ и воспитательных практик;
- прогноз успеваемости ученика с учётом его активности при работе с образовательным контентом;
- персонализированная рекомендательная библиография с учётом интересов и способностей учеников;
- конструктор читательского портфолио с учётом разнообразных читательских активностей на протяжении учёбы в школе.

Применение предложенных сервисов и данных позволяет построить персональный профиль (портфолио) читателя, который будет актуализироваться на протяжении всего его обучения и позволит в автоматическом режиме отслеживать читательскую активность, вести дневник читателя, выстраивать персональные траектории учащегося в зависимости от его интересов, предлагать дополнительные источники информации в соответствии с результатами освоения учебной программы. Данный сервис, по нашему мнению, будет востребован всеми участниками образовательных отношений: ученик может использовать его в качестве сервиса; родители – отслеживать читательскую активность ребёнка, его интересы; педагоги видят взаимосвязь между освоением учебной программы и прочитанными книгами.

Составитель: Т. И. Чикунова, главный библиограф информационно-библиографического отдела

Редактор: А. В. Осыкина

Ответственный за выпуск: Т. И. Хачатурова, директор Краснодарской краевой детской библиотеки имени братьев Игнатовых