Введение

Для современного общества характерны бурное развитие компьютерной техники и информационных технологий, превращение информации в важнейший ресурс, непрерывное увеличение её объёма, осознание информации как средства управления личностью и обществом. Интернет-технологии играют в жизни детей и подростков важную роль – их используют в общении, обучении, самообучении, проведении досуга. В то же время существует большое количество онлайн-рисков, которые могут причинить вред здоровью – как физическому, так и психологическому, и важно научить детей безопасному взаимодействию с Интернетом, избеганию интернет-опасностей.

Проблеме информационной безопасности детей и подростков уделяется значительное внимание и на государственном уровне. В рамках Национальной стратегии действий в интересах детей и Десятилетия детства (2018–2027) разработан План мероприятий по реализации концепции информационной безопасности детей на 2018–2020 годы (Приказ Министерства связи и массовых коммуникаций РФ от 27.02.2018 № 88). Особое место в нём отведено работе по обеспечению информационной безопасности детства в библиотеках. Библиотеки как одни из старейших просветительских организаций наряду со школами и другими образовательными учреждениями должны брать на себя решение этих сложных проблем и становиться центрами приобщения своих юных пользователей к информационной культуре.

Сегодня необходимо задуматься, каков образ будущего России, какими будут последствия социально-гуманитарных и информационно-технологических изменений – и как всё это повлияет на развитие библиотек.

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 2018 и в 2019 году.

Содержание

1. Информационная безопасность детей. Защита персональных данных

Информационная безопасность детей // Не будь зависим. – 2018. – № 12. – С. 3–5.

Определение термина «информационная безопасность детей» содержится в Федеральном законе № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», регулирующем отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию.

Защиту информации от различных воздействий называют информационной безопасностью.

Согласно данному закону «информационная безопасность детей» – это состояние защищённости, при котором отсутствует риск, связанный с причинением информацией вреда здоровью ребёнка и (или) физическому, психическому, духовному, нравственному развитию.

По ФЗ № 436, информацией, причиняющей вред здоровью и (или) развитию детей, является:

1) информация, запрещённая для распространения среди детей;
2) информация, распространение которой ограничено среди детей определённых возрастных категорий.

Запрещено для распространения

К информации, запрещённой для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе причинению вреда своему здоровью, самоубийству;
2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
5) оправдывающая противоправное поведение;
6) содержащая нецензурную брань;
7) содержащая информацию порнографического характера.

Ограничено для распространения

К информации, распространение которой ограничено среди детей определенного возраста, относится информация:

1) представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
2) вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
3) представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
4) содержащая бранные слова и выражения, не относящиеся к нецензурной брани;

С учётом этого вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей

1. Независимо от возраста ребёнка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребёнку – главный метод защиты.
2. Если ваш ребёнок имеет аккаунт на одном из социальных сервисов (*LiveJournal, blogs.mail.ru, vkontakte.ru* и т. п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
3. Проверьте, с какими другими сайтами связан социальный сервис вашего ребёнка. Странички ребёнка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты.
4. Поощряйте своих детей сообщать обо всём странном или отталкивающим и не слишком остро реагируйте, когда они это делают.
5. Будьте в курсе сетевой жизни вашего ребёнка, интересуйтесь, кто его друзья в Интернете, так же, как интересуетесь реальными друзьями.

Возраст от 7 до 8 лет

В Интернете ребёнок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчёты, которые предоставляются программами по ограничению использования Интернета, то есть

«Родительским контролем», или то, что вы сможете увидеть во временных файлах.

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от вашего ребёнка соблюдения временных норм нахождения за компьютером.
3. Покажите ребёнку, что вы наблюдаете за ним не потому, что вам это хочется, а потому, что беспокоитесь о его безопасности и всегда готовы ему помочь.
4. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
5. Используйте специальные детские поисковые машины.
6. Используйте средства блокирования нежелательного контента как дополнение к стандартному «Родительскому контролю».
7. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
8. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
9. Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
10. Научите детей не загружать файлы, программы или музыку без вашего согласия.
11. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
12. В «белый» список сайтов, разрешённых для посещения, вносите только сайты с хорошей репутацией.
13. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
14. Не делайте табу из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».
15. Приучите вашего ребёнка сообщать вам о любых угрозах или тревогах, связанных с Интернетом.

Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств «Родительского контроля».

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от вашего ребёнка соблюдения норм нахождения за компьютером.
3. Наблюдайте за ребёнком при работе за компьютером, покажите ему, что вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.
4. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному «Родительскому контролю».
6. Не забывайте принимать непосредственное участие в жизни ребёнка беседовать с детьми об их друзьях в Интернете.
7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
8. Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
10. Создайте вашему ребёнку ограниченную учётную запись для работы на компьютере.
11. Приучите вашего ребёнка сообщать вам о любых угрозах или тревогах, связанных с Интернетом.
12. Расскажите детям о порнографии в Интернете.
13. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
14. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст детей от 13 до 17 лет

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей.

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребёнком список запрещённых сайтов («чёрный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.
3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты, таким образом, будто речь идёт о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному «Родительскому контролю».
5. Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
8. Приучите детей не загружать программы без вашего разрешения.
9. Приучите вашего ребёнка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти ещё раз в подобных случаях.
10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
11. Приучите себя знакомиться с сайтами, которые посещают подростки.
12. Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде, даже в виртуальном мире.
13. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Постоянно контролируйте использование Интернета вашим ребёнком!

Это не нарушение его личного пространства, а мера предосторожности и проявление вашей родительской ответственности и заботы.

Шляпников В. Коммуникативные риски: как защитить ребёнка / В. Шляпников // Не будь зависим. – 2018. – № 12 – С. 34–42.

Заведующий кафедрой психологии личности и дифференциальной психологии Московского института психоанализа, автор программ по повыше-

нию цифровой компетентности школьников, кандидат психологических наук Владимир Николаевич Шляпников провёл для педагогов и родителей семинар «Коммуникативные риски: как защитить от них ребёнка?».

Когда ребёнок выходит в Интернет, в его жизни появляются совершенно новые люди, значимые незнакомцы, значимые другие, которые начинают воздействовать на него и принимать активное участие в его социализации.

Здесь можно выделить три основных фактора уязвимости, которые делают ребёнка чувствительным к тем или иным проблемам, рискам.

Первый фактор – проблема открытости. Когда ребёнок выходит в Интернет, он утрачивает ощущение собственных границ, границ своей личной жизни.

Вторая серьёзная проблема, с которой сталкиваются не только дети, но и взрослые в Интернете, – информационная перегрузка. Средство противодействия – повышение медиаграмотности, формирование у ребёнка навыков потребления различных медийных продуктов.

Третья серьёзная проблема – проблема общения с незнакомцами.

Защита персональных данных

Самое главное, что нужно сделать при защите данных, – с самого начала жизни в Интернете детям нужно рассказать, что такое персональные данные. Невозможно защищать то, чего ты не понимаешь.

Представьте себе ситуацию: вы сидите дома, и вдруг какой-то незнакомый, посторонний человек заходит к вам в квартиру, в комнату, начинает ковыряться в ваших вещах, заглядывать в шкаф, под стол, под кровать. Это вызывает сильное сопротивление, но здесь границы нашего личного пространства физически определены и эти границы легко защитить. В Интернете границы виртуальные, невидимые, незримые, поэтому, когда посторонний человек заходит в нашу виртуальную квартиру, мы не ощущаем его присутствия, тем не менее последствия для нас могут быть не менее плачевными.

Надо показать ребёнку прямые параллели между физическим пространством и виртуальным. Если ты выкладываешь свою фотографию, значит, готов выйти на всеобщее обозрение, на публику в 10–100 тысяч человек, а может быть, даже в несколько миллионов. Когда подростки начинают об этом задумываться, они понимают, что большое количество подписчиков, друзей не так хорошо, как кажется вначале.

Конечно, большую часть информации помещаем мы сами. Огромное количество информации о нас собирается, в общем-то, разными платформами, условно, без нашего согласия. И когда дети видят, какой колоссальный цифровой след они оставляют в Интернете, это заставляет их насторожиться.

Наконец, важно, чтобы они понимали, что эта информация не просто попадает в Интернет, а агрегируется, собирается воедино, и в результате там действительно хранится огромное цифровое досье на человека.

Есть подозрения, достаточно обоснованные, что эта информация остаётся там фактически навсегда, и при желании она может быть поднята и использована по-разному, совершенно непредсказуемым образом.

Последствия небрежного обращения с персональными данными

Здесь, как и всегда в процессе воспитания, важно избежать запугивания, каких-то страшных баек, легенд, в которые никто не верит, которые производят впечатление только до определённого возраста. Надо приводить конкретные примеры. Практически каждый день в новостях появляется какая-то история про неосторожное обращение с персональными данными. Эти примеры надо приводить и обсуждать с детьми.

Взлом аккаунта

Нужно донести до ребёнка, особенно подростка, мысль, что, если у тебя «угнали» аккаунт, это не значит, что ты перестал быть с ним связан. С него могут рассылать фишинговые[1] сообщения, с этим аккаунтом могут работать мошенники, террористы, те же экстремистские секты, которые часто используют украденные, чужие аккаунты.

Кибертравля

Бывает кибертравля, которая является продолжением травли в реальной жизни, и скорее это вопрос педагогический, чем технический. Бывает специальная травля, организованная в Интернете какими-то троллями. В любом случае, чем меньше я открыт, тем менее уязвим.

Шантаж

Шантаж, преследования – это ещё более серьёзная проблема. Когда мы выкладываем личную информацию, передаём её какому-то незнакомцу, мы никогда не знаем, как она может быть использована против нас.

Потеря денег

Потеря денежных средств из-за Интернета – очень серьёзная проблема. Подростки тоже часто сталкиваются с ситуацией, когда деньги списали с телефона, с игрового счёта.

[1] **Фишинг** (англ. *phishing* от *fishing* – «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным.

Надёжный пароль

Самое главное и простое правило – надёжный пароль, который должен защитить все наши учётные записи. Здесь можно поиграть в криптографов. И младшие, и старшие школьники с энтузиазмом воспринимают эту игру, это для них интересно.

Завести аккаунт для ребёнка

В любом случае, если ребёнок захотел завести аккаунт в соцсети, он это сделает – с вашей помощью или без вашей помощи. Лучше сделать вместе с вами, и чем правильней вы ему поможете, тем лучше он будет пользоваться тем или иным ресурсом.

Работа над контентом

Понятно, что, если ребёнок заводит страницу в социальной сети, он будет там что-то «постить», выкладывать. И нужно подсказать ребёнку, что всё подряд не следует постить, делать перепост, лайкать. По-хорошему – лучше начинать пользоваться соцсетями с 12 лет.

Интернет мешает учиться

То обилие информации, которая сегодня присутствует в Интернете, портит молодёжь, потому что информация обесценивается. Детей нужно учить правильно и грамотно к ней относиться, критически осмысливать её.

«Чёрные» и «белые» сайты

Существуют средства защиты, средства фильтрации, которые помогают в какой-то мере защитить ребёнка от негативного контента. Есть единый реестр запрещённых сайтов Роскомнадзора. Туда попадает вся информация, нарушающая федеральное законодательство: распространение наркотиков, суициды, экстремизм, детская порнография. Поэтому лучше учить подростка справляться с тем негативным контентом, с которым он может столкнуться, чем слепо его ограждать. Существуют программы родительского контроля. Они хорошо работают для дошкольников и младших школьников. Для подростков уже неэффективны, поскольку они умеют взламывать эти программы.

В диалоге с ребёнком

Часто родителям не нравятся те игры, в которые играет их ребёнок, те сайты, которые он посещает, те товарищи, с которыми он общается в социальных сетях. В принципе, конечно, можно на это всё реагировать исключительно однозначным запретом. А можно проявить интерес к этому увлечению ребёнка.

Ресурс ресурсу рознь

Важно формировать у ребёнка критическое отношение к онлайн-ресурсам. Онлайн-ресурсы бывают разные:

1) официальные сайты, на которых публикуется официальная информация, достоверная. Это та информация, которой можно доверять;
2) электронные СМИ. Они тоже в какой-то мере надёжные;
3) социальные СМИ, совместные среды, например, «Википедия»;
4) коммерческие сайты;
5) поддельные сайты. Тут, конечно, степень надёжности информации низкая.

Очень важно, чтобы школьник научился отличать одно от другого.

Очень важно ребёнка научить отличать факт от мнения.

Сегодня все социальные СМИ – это, конечно, мнения. Фактов очень мало. Надо уметь выделять факт. Есть определенные правила, когда, прочитав статью, вы должны разделить факты и мнения. Это первый шаг. Можно поискать первоисточники и перепроверить информацию. Часто можно увидеть расхождения. Есть правило трёх источников. Если информация подтверждается в трёх разных источниках, значит, она надёжная. Такая перепроверка и формирует в конечном счёте медиаграмотность.

Часто в Интернете встречаются объявления, призывы о помощи.

Надо скопировать сообщение в поисковик или сделать поиск по картинке, и можно увидеть первоисточник, и узнать, что на самом деле, человек, который предлагает пожертвовать на щенков, просит денег, обманывает. Несколько раз вдумчиво разобравшись с ресурсами, дети начинают понимать, что с Интернетом нужно обращаться аккуратно, и начинают возвращаться к первоисточникам, которые, в принципе, в Интернете тоже представлены. Ребёнок начинает критично относиться к информации в Интернете, понимает, что это пишут люди, а люди бывают разные.

Агрегаторы информации

Наконец, существуют новостные ленты, агрегаторы информации. Можно для себя настроить ленту таким образом, чтобы попадала только та информация, которая для вас интересна.

Общение с незнакомцами

Исследования показывают, что подростки склонны доверять незнакомцам в Интернете. Во-первых, поскольку им кажется, что это пространство относительно безопасно. Есть некая иллюзия: я общаюсь с человеком, неважно, кто он, но, если вдруг возникнет какая-то угроза, я всегда могу нажать кноп-

ку «выключить», «удалить», и он исчезнет из моего жизненного пространства.

Когда мы говорили о контентных рисках, о персональных данных, там есть технические средства, определённые правила, следуя которым, можно себя обезопасить. Когда мы говорим о проблемах общения с незнакомцами и вообще о проблеме общения, здесь технических средств нет. Здесь единственная надёжная защита – доверительные отношения с ребёнком с самого раннего возраста.

Признаки нежелательного общения в Интернете

Что может послужить признаком того, что у ребёнка появились не очень хорошие друзья в Интернете?

Первое, что может насторожить, – ребёнок стал значительно больше времени проводить в Интернете.

Следует обратить внимание на перепады настроения.

Резкие изменения в поведении, в образе жизни.

Падение успеваемости. Это тоже может быть следствием нежелательного общения.

Любые перемены могут быть индикатором того, что с ребёнком что-то происходит.

Уважать границы

Вместе с тем, выстраивая доверительные отношения, важно уважать личное пространство ребёнка.

Нужно вводить определённые правила

Как только ребёнок начинает просить, чтобы ему купили компьютер или какой-то новый гаджет, сразу надо эти правила обсуждать. Ребёнок должен чувствовать, что ему доверяют.

Говорите с детьми

Надо рассказать ребёнку про онлайн-риски.

Выслушайте ребёнка

Важно дать возможность ребёнку высказаться. И, конечно, надо уважать ребёнка. Тогда ребёнок будет с огромным желанием делиться с вами и дальше.

Используйте ошибку для обучения

Нужно уважать право ребёнка на ошибку. Часто и дети допускают ошибки, и взрослые – попадаются на фишинговые ссылки, теряют деньги, сталкиваются с мошенниками. Если пару раз проработать с ребёнком ту или иную

проблему, у него сформируется эффективная стратегия совладания, которая в жизни пригодится.

Совместная деятельность

Нужно искать формы совместной деятельности в Интернете. Самый простой пример – поиграть вместе в онлайн-игру.

Дети смотрят на вас

Даже в подростковом возрасте всё равно мы неосознанно ориентируемся на своих родителей. Родитель и учитель – это всегда пример.

Вместе с коллегами мы разработали два пособия – «Уроки для подростков» по цифровой компетентности. Они расположены на информационном портале «Дети России онлайн». Он полезен и для родителей, и для учителей. Там есть тренинговые программы, которые вы сможете использовать в работе с детьми.

Гусев В. Кибербезопасность для всех / В. Гусев // НаркоНет. – 2019. – № 8. – С. 10–17.

Кибербезопасность – это безопасность вашего информационного поля, безопасность всего, что вы выкладываете в социальные сети, всего, чем можно воспользоваться против вас. Кибербезопасность вас защищает.

Техническая безопасность

Вначале поговорим про вирусы. Мы ошибочно привыкли полагать, что вирусы – такая вещь, которая может просто банально тормозить компьютер. На самом деле вредоносные программы – это любое программное обеспечение, предназначенное для получения несанкционированного доступа. Например, мы записываем какую-то программу на свой компьютер и забыли убрать одну галочку, в результате нам установили 10-15 приложений, которые потом будет трудно удалить. В принципе вирусы полностью могут заразить компьютер и зашифровать все данные. Прекрасный пример – когда переблокировали больше половины компьютеров Госслужбы США. Поэтому очень важно ставить на компьютеры антивирусные программы.

Вирусом можно заразить любой носитель информации, всё, что угодно, – обычный вордовский документ, файлы *PDF*, фотографии. Когда вы пытаетесь найти в Интернете такие файлы, как ГДЗ (готовые домашние задания) ответы на ЕГЭ и тому подобное, имейте в виду, злоумышленники тоже об этом отлично знают. Они заражают такие файлы, продвигают за деньги такие сайты, которые выводились бы в топ вашего поиска. Соответственно вы скачиваете какой-либо вордовский файл на компьютер, запускаете, у вас высвечивается оповещение, что данный файл, например, повреждён. Тем не менее вирус уже установился на ваш компьютер.

Чего не стоит нажимать в Интернете?

Если вы заходите на сайт и видите огромную кнопку «Скачать», пожалуйста, не нажимайте её. Такие кнопки были актуальны примерно в 2009 году. Сейчас нормальные форумы и сайты используют ссылки, которые ведут на Яндекс-диск, Гугл-диск. Им в большей степени можно доверять, поскольку корпорации заинтересованы в том, чтобы их файлы находились в безопасности, чтобы никто не смог скачать с их сервера какой-либо вирус.

Уязвимости, которые мы сами открываем на своём компьютере

Есть ошибочное мнение, что программа «Торрент» заблокирована, запрещена на территории России. Это не так. Эта программа лишь позволяет скачивать, передавать какие-либо данные. В России в 95% случаев она используется, чтобы скачать нелицензионный софт. Когда впервые вы запускаете на своём компьютере «Торрент», у вас обязательно высвечивается оповещение, что любой человек может начать раздачу абсолютно любого файла. То есть я, допустим, могу создать раздачу какого-нибудь популярного сериала, заразить вирусом аудиодорожку, и когда вы будете смотреть кино, ваш компьютер будет заражён вирусом.

VPN

VPN – это протокол Интернета. Во-первых, пользователей обманули, сказав, что он предоставляет анонимность, – это не так. Во-вторых, это достаточно опасная вещь. Популярность *VPN* и прокси-серверов возросла из-за того, что блокировали «Телеграмм» в России. Все *VPN* предоставлены частными компаниями. Значит, и я у себя дома могу поставить сервер *VPN* и настроить его таким образом, что, когда ко мне будут подключаться люди с мобильного телефона, я буду получать все их персональные данные.

Почему *VPN* не предоставляет анонимность? Потому что вы пользуетесь Интернетом через мой сервер, и я могу посмотреть всё, что вы в дальнейшем будете делать в Сети. И могу передать эту информацию кому угодно. Так что вам необходимо над этим задуматься.

Не доверяйте *Wi-Fi* без пароля

Не доверяйте незапароленным *Wi-Fi*-соединениям. В таких местах, как аэропорт, вокзал, вообще не подключайтесь к *Wi-Fi*. Почему? Потому что злоумышленники туда приходят как на работу, чтобы заражать роутеры. Для чего им это надо? Прилетает турист, или вы сами прилетели в другую страну. Ваша сим-карта не прошла авторизацию, у вас нет доступа к ней, и вы не можете ни звонить, ни подключиться к Интернету, ничего сделать не можете. Идёте по аэропорту и подключаетесь к первому же бесплатному *Wi-Fi* от *Duty Free*, например. Теперь злоумышленник может получить ваши личные персональные данные с помощью роутера. Он может сохранить ваш *MAC*-

адрес. *MAC*-адрес – это уникальный код вашей сетевой платы в телефоне. Она никогда ни с кем больше не повторится. После аэропорта вы едете в отель и там подключитесь к *Wi-Fi*. С данными вашего *MAC*-адреса человек будет знать, где вы остановились. Таким образом, он может без проблем отслеживать ваши передвижения, подключения через *Wi-Fi* к Интернету. Достаточно опасная вещь.

Представим себе следующую ситуацию. Вы зашли в кафе выпить чашечку кофе, переждать какое-то время. Напротив сижу я со своим ноутбуком. Вы подключаетесь к *Wi-Fi*, и я подключён к *Wi-Fi*. Это значит, что мы подключились к одному роутеру. То есть мы находимся с вами в одной локальной сети. Значит, между устройствами можно передавать какие-либо данные. Например, я со своего ноутбука могу перекинуть какой-либо носитель информации на ваш телефон. Если у вас телефон на платформе *Android*, я без проблем загружу вам вирус. Если от компании *Apple*, я смогу получить достаточно большое количество ваших персональных данных: имя, фамилию, номер телефона и так далее, данные сим-карты.

Каким сетям в большей степени можно доверять?

Хороший пример – государственная *MT-free*, которая находится сейчас в метро, автобусах, очень защищённая, хорошая сеть. Также школам предоставляется защищённый, мощный *Wi-Fi*. Для чего везде в вашей школе стоят роутеры, белые и синие? Это как раз роутеры компании *Cisco*. Очень защищённое и очень дорогое оборудование. Те роутеры, которые стоят у вас дома, белые с антенной, за 1,5 тыс. рублей, – это незащищённые системы.

Bluetooth

Bluetooth-гарнитура – очень важная вещь. Сейчас практически у всех есть или *Bluetooth*-наушники, или *Bluetooth*-колонки. Радиотехника – это такая вещь, которую вообще без проблем можно взламывать, перехватывать, можно делать с ней всё, что угодно. Особенно с учётом того, что человечество придумало всего два *pin*-кода, чтобы защитить абсолютно всю *Bluetooth*-гарнитуру: 0000 или 1234, в зависимости от того, где она была произведена – в Китае или Европе.

Как сейчас это происходит в России? Человек садится с ноутбуком с антенной в рюкзаке в электричку. Пока он едет, к нему подсаживаются люди, которые слушают музыку, например, в *Bluetooth*-наушниках. И пока он слушает, происходит взлом его *Bluetooth*-гарнитуры, и за счёт этого человека делаются звонки на платные номера. С его счёта будут списываться деньги. Более опытные программисты могут подключаться к микрофону, динамикам, к самому телефону.

Как достичь безопасности?

Во-первых, когда вы покупали вашу *Bluetooth*-гарнитуру, вы обязательно получили руководство, где было написано, как изменить *pin*-код и как быть в безопасности. Второе: вам просто нужно зайти в Интернет, вбить название вашей *Bluetooth*-гарнитуры и написать запрос: как изменить пин-код? Вы найдёте инструкцию, поменяете пин-код, и это займёт буквально 5-10 минут. Тогда вы будете в безопасности!

Социальные сети

Вы должны понимать, что такое социальные сети, а что мессенджеры. Социальные сети всегда работают методом сервера. Там есть сервер, который сохраняет все данные – когда вы вошли в соцсеть, что делали, куда перешли, что написали и так далее. Мессенджер работает по-другому. Если с телефона удалено сообщение отправителя и получателя, значит, этого сообщения больше не существует. Отследить его никак нельзя, получить доступ невозможно. В социальных сетях всё иначе. Что бы вы ни удалили – свои фотографии, посты, сообщения, – имея определённые знания, можно восстановить доступ ко всему в любой момент времени. Человечество дошло до того момента, когда удалять за каждым человеком информацию стало дороже, чем хранить её. *Microsoft* начинает развивать механизм, который позволяет хранить информацию в ДНК.

Осторожно – фотобанк!

Основная угроза соцсети «ВКонтакте» – фотобанк. Фотобанк – сервер, сохраняющий все изображения, которые вы когда-либо добавляли в социальные сети. Все эти фотографии находятся в общем доступе на одном сервере. И любой человек имеет к этому серверу абсолютный доступ. Любой может зайти и посмотреть любую вашу фотографию, которую вы когда-либо скидывали через соцсеть.

Ни в коем случае через социальные сети не передавайте такие вещи, как банковская карта, ваш паспорт, личные фотографии. Имейте в виду, что любой информацией можно воспользоваться в любой момент времени против вас. Хотя бы один раз слитый в социальных сетях паспорт – навсегда бомба замедленного действия. Когда ей воспользуются – завтра, через неделю или через 10 лет – уже вопрос вероятности.

Для передачи личной информации пользуйтесь месенджерами. Месенджеры тоже можно взломать, но для этого нужен дубликат сим-карты. Это уже намного сложнее, чем если какой-нибудь человек ради интереса будет пытаться взломать, например, вашу электронную почту.

Не общайтесь с незнакомцами

В Интернете действует такой же принцип, как и на улице: не стоит общаться с незнакомыми людьми. Какие сейчас есть виды хакинга? «Взламывают» одного ребёнка из класса и с помощью него начинают производить разнообразные рассылки: «Слушай, забыл твой номер телефона, напиши мне его, пожалуйста». Человек может не задуматься и написать телефон, вероятность этого очень высокая.

Для детей до 4–5-х классов используют даже такие механизмы. Злоумышленник пишет: «Давай я приду к тебе в гости, поиграем в компьютер, напиши, пожалуйста, свой адрес». И ребёнок пишет.

Что с этой информацией может произойти в дальнейшем? Так вот, эта информация попадает в Даркнет[2]. И что с ней происходит? В Интернете можно купить такие файлы, где будет написано: «Дети 10–18 лет». С именами, фамилиями, номерами телефонов, фотографиями, взятыми из соцсетей, чтобы биометрической камерой можно было найти человека по уникальным точкам на лице и список всех социальных сетей человека.

В лучшем случае такие файлы продают каким-либо рекламным компаниям, которые в дальнейшем рассылают спам. В худшем – запрещённым на территории России организациям. Это достаточно опасные вещи, надо это понимать и внимательно ко всему относиться.

Геометки

Геометка, или геотаргетинг[3]. *Instagram* была первой соцсетью в мире, которая агрессивно выдвинула на рынок такую вещь, как геопозиция. То есть она стала добавлять в социальные сети точные координаты, где человек делает фотографию. Фотография – это не только изображение, это достаточно большой программный код.

У многих есть современные телефоны, смартфоны. Уже давно, когда мы открываем галерею в телефоне, видно, что каждая фотография классифицируется не по дате, а по точному адресу. Можно по фотографии посмотреть: город Москва, такая-то улица и так далее. Из-за чего это происходит? В телефоне есть маленькая плата – называется *GPS*-трекер. Он соединяется со спутником и точно понимает, в каких координатах широты и долготы по земному шару мы сейчас находимся.

---

[2] **Даркнет** (англ. *DarkNet*, также известен как «Скрытая сеть», «Тёмная сеть», «Теневая сеть», «Тёмный веб») – скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов

[3] **Геотаргетинг** (англ. *geo targeting*, от *target* – цель) – в веб-разработке и интернет-маркетинге метод выдачи посетителю содержимого, соответствующего его географическому положению.

Чем это чревато? Например, достану сейчас свой телефон, сфотографирую вас и выложу эту фотографию в «Инстаграм», добавив геометку другого города. Человек зайдёт на эту геометку и подумает: странно, что она здесь оказалась. Но если по специальной программе подключиться к этой фотографии можно понять, что я её сделал здесь с разбросом в 2-3 метра.

Предположим, я сейчас выступаю в роли социального инженера – злоумышленника. В современных телефонах присутствует такая вещь, как высота над уровнем моря, то есть координаты в пространстве, можно понять, на каком этаже сделана фотография. Все данные о вашей квартире есть. Что с этим можно сделать? Есть 2 варианта. Первый: если я опытный программист, я могу написать программу, которая будет отслеживать все ваши дальнейшие геометки. Если я неопытный, я буду ежедневно заходить на вашу страничку, чтобы получать дополнительную информацию. Скорее всего, вы со своими родителями поедете на отдых. В другой город, деревню, другую страну. Вы будете выкладывать фотографии свои и родителей, а в комментариях можете написать: «Осталось всего две недели отдыха». Всё, понятно, что вас нет дома, и родителей тоже. В Интернете я выставляю запрос профессиональным ворам, и если они обчистят вашу квартиру, то мне за это заплатят деньги. Вот так на данный момент работает киберпреступность.

Береги электронную почту

Основа основ безопасности – электронная почта. Бывший агент ФБР Эдвард Сноуден, достаточно мощный программист в сфере безопасности данных, сказал: «Дайте мне доступ к личной электронной почте человека, и я получу доступ к его жизни». К нашей электронной почте подвязано вообще всё – наши социальные сети, приложения, электронные банковские чеки приходят на почту. Иной раз хватит всего лишь одного авиабилета и одного банковского чека – и можно позвонить в Сбербанк, представиться вами и затребовать восстановление доступа к вашей банковской карте. Вот такими механизмами сейчас оперируют. И опять же знайте, что через электронную почту можно восстановить доступ с паролем во все ваши социальные сети.

Те, у кого телефон или аппаратура от компании *Apple*, точно знают: для того чтобы зарегистрироваться в *iCloud*[4], в пароле обязательно должны быть одна заглавная буква, одна маленькая и одна цифра. Это называется стандарт безопасного пароля. Если в вашем пароле будут 3 большие буквы, 3 маленькие буквы, 3 цифры, при учёте, что этот пароль уникален, потребуется 100–150 лет, чтобы его подобрать.

Самая распространённая ошибка любого пользователя – на всех сервисах использовать один и тот же пароль. Не так давно взломали компанию

[4] ***iCloud*** – интернет-сервис с поддержкой *push*-технологий (англ. *push* букв. «проталкивание»), созданный компанией *Apple*.

Facebook, социальную сеть. Как это произошло? Взломали почтовый сервис *Yahoo*, это как наш «Яндекс» примерно. Вытащили оттуда пару миллионов аккаунтов. 2 млн аккаунтов были выложены в Сеть. Программисты прикрепили всего лишь один текстовый файл: «Люди, отнеситесь серьёзней к своей личной информации!».

Для взрослых я обычно привожу пример, что если взломают, например, их аккаунт от игры «Ферма», то смогут получить доступ к их рабочей почте. Таким образом происходят все взломы. Тогда возникает вопрос: как создать уникальный пароль для каждого сервиса, и его ещё и запомнить? Всё очень просто. Этот пароль будет константой, неизменной величиной. Вы его создадите, придумаете один раз и больше менять не будете. А потом добавьте в пароль всего один символ. Например, 1 – учёба, 2 – работа, 3 – игровой профиль. И вы будете в безопасности.

Что изменилось в Рунете?

Соцсеть «ВКонтакте» принадлежит российской технологической компании *Mail.ru Group*. Все её серверы находятся в России. Также по Федеральному закону «О противодействии терроризму» на территории России расположились сервера мессенджеров *Whatsapp* и *Viber*. Это, кстати, была первая причина блокировки «Телеграмм». Что делают данные серверы? Они могут подтвердить какие-либо ваши сообщения. Как это происходит? При административных делах серверы обычно используются так. Они могут подтвердить, с какого телефона вы вышли на связь, какой роутер был ближайшим, какая была вышка связи, какая была сим-карта и так далее. При уголовных делах используются механизмы, которые могут понять, с какой скоростью вы нажимаете на такую-то кнопку на своей клавиатуре или на телефоне, как часто автозамена делает здесь изменения. Фактически благодаря этому алгоритму можно добиться подтверждения вашей личности на 95–98%.

Думай, что выкладываешь в Сеть

Приведу вам яркий пример неправильного поведения в Интернете. Две девушки поссорились в школе. Одна решила другой отомстить и разместила её фотографию в раздевалке спортзала в неподобающем виде. Взяла эту фотографию и выложила в соцсети «ВКонтакте», в группе, где были школьники. Эта фотография провисела недолго, примерно 1,5-2 часа. Разразился огромный скандал. Девушка удалила фотографию, но всё-таки прецедент был. Девушку, конечно, наказали, но на тот момент она отделалась лёгким испугом. После этого прошло ещё 2-3 недели, и эта фотография снова оказалась в сети «ВКонтакте» и начала распространяться в геометрической прогрессии. Репостами, перепостами она оказалась уже в тысячах разнообразных групп, то есть удалить её стало невозможно.

Когда полиция вначале проверяла, думали, что, пока фотография висела в Сети, кто-то её сохранил и выложил в другие группы. Но к этому подключились соответствующие серверы, и выяснилось, что фотографию выложила снова та же самая девушка. В итоге её арестовали в школе по очень серьёзному обвинению. Ей грозило до 25 лет лишения свободы. Её отчислили из школы. И её родителей оштрафовали на 1 480 000 рублей в счёт возмещения морального ущерба.

О кибертравле

Травля может привести к самым печальным последствиям. Вас поставят на учёт, ваших родителей финансово накажут. А при условии буллинга[5] и травли, если участвовали такие слова «Мы побьём тебя за школой», хотя бы намёк на физическую расправу, то может быть заведено уголовное дело.

Относитесь к технологиям ответственно

Предположим, у вас дома стоит ноутбук. В нём есть встроенный микрофон. Отключим ноутбук от Интернета, *Wi-Fi,* локальной сети. И на протяжении 5–10 минут вы возле него говорите: «Покупка машины, хочу купить машину, покупка иномарки». Включаете Интернет – и видите, что вся ваша дальнейшая реклама связана только с покупкой машины. Кто нарушает в этом плане ваши права, ваше личное пространство? Никто. Мы устанавливаем себе какой-либо браузер на компьютер – *Google Chrom, Opera* и др. Там есть лицензионное сообщение, в котором прописано, что эта компания имеет полный доступ к нашим микрофонам, личным данным, поисковым запросам, для того чтобы показывать нам таргетированную[6] рекламу.

Будьте аккуратными с современными технологиями, а точнее, с искусственным интеллектом, помощниками Алиса, Кортана и Сири. Это слишком опасные технологии, которые очень рано дали людям.

---

[5] **Бу́ллинг** (жарг. Бу́ллинг – англ. *bullying*) – травля, агрессивное преследование одного из членов коллектива (особенно коллектива школьников и студентов, но также и коллег) со стороны другого, но также часто группы лиц, не обязательно из одного формального или признаваемого другими коллектива.

[6] **Таргетированная реклама** (от англ. *Target* – цель) – это форма онлайн-рекламы, в которой используются сложные методы и настройки поиска целевой аудитории в соответствии с заданными параметрами, характеристиками и интересами пользователей, релевантными для определенных товаров или услуг, которые рекламирует рекламодатель.

Безопасность превыше всего // Не будь зависим. – 2019. – № 8. – С. 10–14.

Чтобы избежать проблем со здоровьем ребёнка, необходимо строго соблюдать рекомендации специалистов: психологов, врачей, педагогов.

Отбор проверенных сайтов

Дошкольники не могут самостоятельно искать полезные для себя ресурсы, поэтому родители должны осуществлять отбор и поиск таких материалов для ребёнка. Полезен мультсериал «Учиться вместе с кисой Алисой», сайт «Солнышко» https://solnet.ee, «Почемучка» (http://pochemu4ka.ru), «Чудесенка» (http://chudesenka.ru), «Теремок» (http://www.teremoc.ru). На портале «Чудо-юдо» находятся развивающие игры, мультфильмы, пазлы, кроссворды, ребусы.

Образовательные материалы

В качестве образовательных материалов рассматриваются демонстрационные картинки, сказки, сюжетно-ролевые игры, обучающие мультфильмы и обучающие компьютерные игры.

Используем картинки

Пока ребёнок не умеет читать, необходимо использовать картинки. Они имеются в многочисленных книжках, буклетах для детей на тему «Безопасность жизнедеятельности», в Интернете на соответствующих сайтах для детей и родителей.

Изучаем правила по сказкам

Использование примеров из сказок – это метод обучения ребёнка знаниям безопасного поведения на основе сюжетно направленного художественного текста, оказывающего на него сильное эмоциональное воздействие.

Сюжетно-ролевые игры

Сюжетно-ролевые игры помогают детям овладевать первоначальными знаниями правил безопасного поведения в Интернете, эффективно учат распознавать ситуации потенциально опасных интернет-рисков и выбирать оптимальные способы их недопущения или минимизации.

Обучающие мультфильмы

В Интернете также можно найти огромное количество мультипликационных фильмов на тему «Интернет-безопасность для детей младшего возраста». Возьмите на вооружение серию мультфильмов Спас-экстрим «Аркадий Паровозов» – «Почему нельзя заходить на сомнительные сайты в Интернете», «Остерегайся мошенничества в Интернете», «Безопасность в Интерне-

те» и другие. Эти мультфильмы можно найти, набрав в поисковой строке «Мультфильмы по теме интернет-безопасность». Выйдут ссылки на ресурсы, размещённые в Интернете.

Обучающие компьютерные игры

Обучающие, дидактические компьютерные игры имеют два основных блока – содержание, которое включает в себя познавательные задания для ребёнка, дидактически ценные. И блок средств, то есть интерфейс игры, который обеспечивает способ деятельности, реализацию конкретных действий, ведущих к усвоению знаний и формированию заложенных в эту игру определенных навыков и умений. По теме интернет-безопасности также можно найти немало компьютерных обучающих игр в Интернете.

Игра «Дикий интернет-лес»

Одна из них – обучающая игра «Дикий интернет-лес». Она создана в рамках программы Совета Европы «Строим Европу для детей и вместе с детьми». Программа имеет целью продвижение прав детей и их защиту от любых форм насилия. Имеет русскоязычный интерфейс.

Не только Интернет

Родители должны объяснять, что Интернет не должен быть главным и тем более единственным увлечением в жизни. Пусть родители как можно чаще говорят ребёнку, что, кроме Интернета, у него должны быть любимые книги, дополнительные занятия в клубах, кружках, секциях, а также игры с друзьями на свежем воздухе.

Подводя итоги, скажем, что в условиях семейного воспитания необходимо:

1) применять современные программно-технологические средства обеспечения интернет-безопасности;
2) использовать проверенные ресурсы, интересные и полезные детям;
3) с учётом возрастных интересов и возможностей ребёнка использовать соответствующие образовательные материалы, нацеленные на формирование и развитие личностных знаний и навыков безопасного поведения в Интернете;
4) постоянно контролировать соблюдение ребёнком здоровьесберегающих правил и времени пребывания за компьютером.

Желательно составить и вывесить на видном месте памятку безопасного поведения в Интернете. Иногда её называют Семейным соглашением.

Памятка безопасного поведения в Интернете

Не нажимай в электронных письмах на неизвестные ссылки от неизвестных отправителей.

Не открывай присланные незнакомцами файлы из Интернета, ведь таким путём распространяется большинство компьютерных вирусов.

Не указывай в Интернете личные данные – своё настоящее имя, возраст домашний адрес, номер телефона.

Общаясь в Сети, играя в компьютерные онлайн-игры, используй не своё настоящее имя, а ник.

Прежде чем начать общаться с кем-то в Сети, следует попросить у родителей разрешения. Соблюдай осторожность. Человек, с которым ты собираешься общаться в Интернете, может быть совсем не тем, за кого себя выдаёт.

В Интернете нужно вести себя так вежливо, как в общении с другими людьми, не писать грубости, не распространять сплетни и не унижать достоинство людей.

Если тебе приходят письма с неприятным или оскорбляющим тебя содержанием, обязательно сообщи об этом родителям.

В заключение ещё раз подчеркну, обучение детей безопасному поведению в Интернете является не одноразовой акцией, а систематической практикой семейного воспитания.

Управление персональными данными // Нарконет. – 2018. – № 11 – С. 18–25.

(Описание предыдущих уроков см. в дайджесте «Планета "Интернет" – выбор взрослых, выбор детей», выпуск 6.)

Урок № 10

«Как удалить персональные данные из Интернета?»

В начале урока ведущий озвучивает тему занятия в формате минилекции. Далее участники переходят к обсуждению этого случая в формате беседы с ведущим.

Упражнение «Право на забвение»

Задача: знакомство учащихся с категориями данных, подлежащих удалению из Интернета, и возможными способами их удаления.

Ведущий предлагает группе выполнить следующее упражнение. Оно состоит из трёх этапов.

Первый этап

Ведущий делит класс на три равные подгруппы. Каждая получает карточку с историей запроса на удаление данных и памятку «Как удалить персональные данные из Сети?». Задача – внимательно изучив историю, пред-

ставить себя на месте героя и принять решение: удаления какой информации они вправе требовать от администрации ресурса, на котором эти данные были размещены.

Второй этап

Подгруппы обмениваются письмами, прилагая к ним карточки с историями. Участники подгруппы должны написать письмо пользователю – герою истории – с аргументированным ответом: отказом или согласием на удаление данных.

Третий этап

Представители подгрупп по очереди зачитывают письмо, полученное от другой группы, историю, связанную с этим письмом, и затем озвучивают свой ответ. Авторы запроса должны ответить, согласны ли они с решением администрации сайта.

После того как все подгруппы выступят, можно переходить к обсуждению и подводить итоги упражнения.

Как удалить персональные данные из Интернета?

В первую очередь необходимо удалить личную информацию с ресурса-первоисточника, на котором она впервые была размещена.

Для этого:

1. Внимательно изучите условия и правила использования ресурса, уделив особое внимание разделам «Конфиденциальность» и «Безопасность».
2. Воспользуйтесь подобной системой, если она есть.
3. Письмо в администрацию ресурса должно быть написано в форме вежливой и хорошо аргументированной просьбы об удалении персональных данных.
4. Письмо должно содержать: данные о заявителе.
5. Администрация ресурса должна рассмотреть вашу жалобу в течение десяти рабочих дней.
6. Если вы получили от администрации ресурса мотивированный отказ в удалении информации, внимательно изучите его и попробуйте понять, что вы сделали неправильно.
7. Если вы не получили ответа от администрации ресурса или на вашу просьбу ответили немотивированным отказом, не отчаивайтесь. Обращайтесь за помощью к взрослым, например, к операторам линии помощи «Дети онлайн» (8-800-25-000-15).

Какая информация может быть удалена из Интернета?

Принимая решение об удалении информации, администрация ресурса руководствуется целым рядом соображений:

1) информация, размещённая на сайте, не должна нарушать законодательство РФ, а значит, удалить противозаконный контент будет достаточно легко. Ознакомиться с законодательными актами, регулирующими обращение информации в Интернете, можно на сайте Роскомнадзора http:// eais.rkn.gov.ru;
2) информация, размещённая на сайте, не должна нарушать правила использования ресурса и пользовательское соглашение;
3) ещё одна категория данных, подлежащих удалению, – недостоверные данные, порочащие честь, достоинство или деловую репутацию пользователя (ГК РФ, ч. 4, разд. I, гл. 8, ст. 152);
4) администрация ресурса также обязана по вашему требованию удалить персональные данные, размещённые на сайте без вашего согласия.

Итоги занятия

Даже если нам удастся удалить первоисточник информации, она все равно сохранится в ресурсах, занимающихся сбором и индексацией данных в Сети. Некоторые из этих ресурсов хранят информацию в кэше[7] из технических соображений, например, чтобы ускорить работу поисковиков. Другие собирают персональные данные с коммерческими целями.

Образовательные результаты

В результате освоения программы у учащихся должны быть сформированы 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.

Методы защиты конфиденциальных персональных данных от несанкционированного доступа

Специальные безопасные режимы работы в браузерах.

Приёмы, позволяющие контролировать распространение персональных данных в Интернете, а также удалять следы онлайн-активности с различных устройств и онлайн-ресурсов.

Настройки приватности в социальных сетях и на других онлайн-ресурсах.

[7] **Кэш**, или кеш (англ. *cache*, от фр. *Cacher* – «прятать»), – промежуточный буфер с быстрым доступом к нему, содержащий информацию, которая может быть запрошена с наибольшей вероятностью.

Обращение в службу технической поддержки разработчиков устройств, приложений, онлайн-ресурсов; в общественные и государственные организации.

Оценка уровня цифровой грамотности по управлению персональными данными в Интернете.

Методика представляет собой набор из 20 тестовых заданий с одним верным вариантом ответа. На выполнение теста отводится 30-40 минут.

Управление персональными данными // Нарконет. – 2018. – № 12. – С. 26–31.

Автосинхронизация

Автосинхронизация – автоматический процесс приведения данных, которые содержатся на нескольких устройствах, к одинаковому состоянию. Такой процесс может быть как односторонним, так и двусторонним.

Аккаунт

Аккаунт, учётная запись (англ. *account*) – хранимая в компьютерной системе совокупность данных о пользователе, необходимых для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

Аутентификация

Аутентификация – процедура проверки подлинности.

Браузер

Браузер, или веб-обозреватель (англ. *webbrowser*, устар. броузер), – прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов, управления веб-приложениями, а также для решения других задач.

Вотсапп

Ватсап, вотсап, вотсапп (англ. *WhatsApp*, игра слов от *What's Up* – «Что происходит?») – бесплатный частный коммерческий мессенджер[8] для смартфонов.

Видеохостинг

Видеохостинг – сайт, позволяющий загружать и просматривать видео в браузере, например, через специальный проигрыватель.

[8]**Мессенджер** (англ. *Instant messaging, IM* – службы мгновенных сообщений *(Instant Messaging Service, IMS)*) – это программа (приложение) для смартфона или персонального компьютера, позволяющая мгновенно обмениваться с друзьями текстовыми сообщениями, телефонными звонками и даже разговаривать с использованием видеосвязи

Википедия

Википедия (англ. *Wikipedia*) – свободная, общедоступная, мультиязычная, универсальная интернет-энциклопедия, реализованная на принципах вики[9]. Википедия расположена по адресу http://www.wikipedia.org.

Вики-проект

Вики-проект – веб-сайт, работающий на технологии вики, который развивается за счёт коллективного труда сообщества авторов, как правило, неоплачиваемого и добровольного.

Вики-среда

Вики-среда (соединение слов *wiki* и «среда») – совокупность вики-проектов, их содержания, участников и технической основы.

Виртуальная реальность

Виртуальная реальность, искусственная реальность, электронная реальность, компьютерная модель реальности (англ. *virtual reality, VR*) – мир (объекты и субъекты), созданный техническими средствами, передаваемый человеку через его ощущения: зрение, слух, обоняние, осязание и др.

Геолокация

Геолокация (англ. *geolocation*) – определение реального географического местоположения электронного устройства, например, радиопередатчика, сотового телефона или компьютера, подключённого к Интернету.

Единый реестр доменных имён

Единый реестр доменных имён, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты, содержащие информацию, распространение которой в Российской Федерации запрещено – автоматизированная информационная система ведения и использования базы данных о сайтах, содержащих запрещённую к распространению в России информацию.

Идентификатор

Идентификатор – имя, под которым зарегистрирован пользователь в проверяющей его компьютерной системе.

Инстаграм

Инстаграм (англ. *Instagram*) – бесплатное приложение для обмена фотографиями и видеозаписями с элементами социальной сети, позволяющее снимать фотографии и видео, применять к ним фильтры, а также распространять их через свой сервис и ряд других социальных сетей.

Информер

Информер (англ. *Informer* – «осведомитель, доносчик») – автоматически обновляющийся специальный блок, который устанавливается на сайте поль-

[9] **Ви́ки** (англ. *wiki*) – веб-сайт, содержимое которого пользователи могут самостоятельно изменять с помощью инструментов, предоставляемых самим сайтом.

зователя для предоставления посетителям дополнительной оперативной информации в какой-либо области.

Кейлогеры

Кейлогеры (англ. *keyloggers*) – специальные программы и устройства, позволяющие регистрировать нажатие клавиш на клавиатуре компьютера.

Кибербуллинг

Кибербуллинг (англ. *cyberbulling*) – намеренное и регулярное причинение вреда (запугивание, унижение, травля, физический или психологический террор) одним человеком или группой людей другому человеку с использованием электронных форм контакта.

Комментарии

Комментарии (см. также «пост») не существуют отдельно от записей. Главная задача комментария – дать возможность развернуто оценить запись, уточнить непонятные моменты или выразить несогласие с автором.

Конфиденциальность

Конфиденциальность (англ. *confidence* – «доверие»):

1. Необходимость предотвращения утечки (разглашения) какой-либо информации.
2. Обязательное для выполнения лицом, получившим доступ к определенным сведениям (сообщениям, данным) независимо от формы их представления, требование не передавать их третьим лицам без согласия лица, самостоятельно создавшего информацию либо получившего на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Кэш

Кэш (англ. *cache*; фр. *Cacher* – «прятать»):

1. Промежуточный буфер с быстрым доступом, содержащий ту информацию, которая будет запрошена с наибольшей долей вероятности.
2. Кэширование интернет-страниц – процесс сохранения часто запрашиваемых документов на (промежуточных) прокси-серверах или электронном устройстве пользователя с целью предотвращения их постоянной загрузки с сервера-источника и уменьшения трафика.

Логин

Логин (англ. *login*; *name*; *username*; *user* – «пользователь») – имя (идентификатор) учётной записи пользователя в компьютерной системе.

Мессенджер

Мессенджер, система обмена мгновенными сообщениями (англ. *instant messaging, IM*) – службы мгновенных сообщений, программы-онлайн-

консультанты (*Online Saler*) и программы-клиенты для обмена сообщениями в реальном времени через Интернет.

Настройки приватности

Настройки приватности – система специальных параметров, позволяющих пользователю онлайн-ресурса настраивать уровень внешнего доступа к различным видам персональной информации.

Неприкосновенность частной жизни

Неприкосновенность частной жизни (в юридической науке) – ценность, обеспечиваемая правом на неприкосновенность частной жизни.

В России неприкосновенность частной жизни провозглашается ст. 23, 24 Конституции РФ.

Оператор персональных данных

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и/или осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Паблик

Паблик, публичная страница (англ. *public*) – сообщество в социальной сети, в которое могут вступить зарегистрированные в ней пользователи.

Пароль

Пароль (фр. *parole* – «слово») – условное слово или набор знаков, предназначенный для подтверждения личности или полномочий.

Персональные данные

Персональные данные (согласно Федеральному закону РФ № 152) – любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу – субъекту персональных данных (ст. 3 Федерального закона РФ от 27.07.2006 № 152).

Пин-код

Пин-код (англ. *Personal Identification Number* – «личный опознавательный номер») – аналог пароля (см. «Пароль»).

Поисковый запрос

Поисковый запрос – последовательность символов, которую пользователь вводит в поисковую строку, чтобы найти интересующую его информацию.

Существует несколько категорий запросов:

- Информационные – когда пользователь хочет найти информацию;
- Навигационные – когда пользователь хочет найти определённый сайт или компанию;
- транзакционные – когда пользователь хочет совершить определённое действие.

Пост

Пост (англ. *post*) – запись, отдельное сообщение на веб-форуме.

Право на забвение

Право на забвение (англ. *right to be forgotten* – «право быть забытым») – право ограничивать доступ к неприятной или устаревшей информации о себе в глобальной сети.

Приватность

Приватность (англ. *privacy* – «уединение», «уединённость»):

1. Право человека на личное пространство, свободное от вмешательства других людей и организаций. Выделяется 4 типа: физическая; личности, или поведенческая; персональной коммуникации, или коммуникационная; персональной информации, или информационная.
2. Регуляторный динамический процесс, детерминирующий и непрерывно корректирующий границы личности с точки зрения её взаимоотношений с окружающим миром.
3. Право индивида решать, насколько быть открытым или закрытым по отношению к внешнему миру, какая информация и при каких условиях может быть сохранена как тайна или, наоборот, передана другим людям.

Сет

Сет (англ. *Set* – «комплект») – комплект предметов экипировки игрового персонажа.

Скайп

Скайп (англ. *Skype*) – бесплатное программное обеспечение с закрытым кодом, обеспечивающее текстовую, голосовую и видеосвязь через Интернет между компьютерами (*IP*-телефония) и опционально использующее платные услуги для звонков на мобильные и стационарные телефоны.

Смартфон

Смартфон (англ. *smartphone* – «умный телефон») – мобильный телефон, дополненный функциональностью карманного персонального компьютера.

Скриншот

Снимок экрана, скриншот, скрин (англ. *screenshot*) – изображение, полученное устройством и показывающее в точности то, что видит пользователь на экране монитора или другого визуального устройства вывода.

Спам

Спам (англ. *spam*):

1. Рассылка коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать.
2. Название распространяемых материалов. Распространителей спама называют спамерами.

Тамблер

Тамблер (англ. *Tumblr*) – сервис микроблогов, включающий в себя множество картинок, статей, видео- и *gif*-изображений по разным тематикам и

позволяющий пользователям публиковать посты в их тамблелоге[10] (англ. *tumblelog*). Сервис характеризует себя как «простейший способ вести блог» (англ. *The easiest way to blog*).

Твиттер

Твиттер (англ. *to twit* – «чирикать, щебетать, болтать») – социальная сеть для публикации коротких сообщений при помощи веб-интерфейса.

Трансграничная передача данных

Трансграничная передача персональных данных – передача персональных данных оператором через государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Трекеры (англ. *track* – «след, отслеживание») – общее название устройств и программ, с помощью которых можно отследить разные показатели организма, например, пульс, правильность осанки, качество питания, ритмы сна и т. д.

Фитнес-трекер (см. Трекеры) – браслет или клипса со встроенным датчиком, способные отслеживать множество факторов, касающихся здоровья и тренировок: продолжительность и качество сна (функция «умный будильник»), количество пройденных шагов, качество питания, показатели пульса, сожжённые калории, настроение, уровень насыщения крови кислородом, калорийность поступающей в организм пищи.

Фишинг

Фишинг (англ. *phishing*, от *fishing* – «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.

Форсквэр

Форсквэр (англ. *foursquare* – «квадрат, квадратный») – социальная сеть с функцией геопозиционирования, предназначенная, в основном, для работы с мобильными устройствами.

Цифровая компетентность

Цифровая компетентность – основанная на непрерывном овладении системой соответствующих знаний, умений, мотивации и ответственности способность индивида уверенно, эффективно, критично и безопасно выбирать и применять инфокоммуникационные технологии в разных сферах жизнедеятельности.

Цифровой след

Цифровой след, цифровой отпечаток – вся совокупность персональной информации о пользователе, которая хранится в Интернете.

---

[10] Тамблелог (от. англ. *tumblelog*), он же Тамбллог или Тлог, – это разновидность блога, с тем отличием, что запись в блоге может быть только определённого формата

Черный список

Чёрный список:

1. Функция, предусматривающая возможность блокировки активности пользователя на онлайн-ресурсе в целях пресечения поведения, запрещённого правилами сервиса, публикации запрещённого контента, спама и вирусов.
2. Функция в социальной сети, позволяющая заблокировать недоброжелателям доступ к профилю пользователя в целях его защиты от нежелательного общения, рекламных рассылок и спама.

Электронная подпись

Электронная подпись (ЭП), электронная цифровая подпись (ЭЦП) – реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки – подтвердить факт подписания электронного документа (неотказуемость).

Изучи Интернет и управляй им!

Координационным центром национального домена сети Интернет при поддержке Ростелекома создан социально-образовательный проект, направленный на повышение цифровой грамотности детей и подростков – «Изучи Интернет и управляй им!».

Ежегодно в рамках проекта «Изучи Интернет и управляй им!» проходит Всероссийский онлайн-чемпионат под одноимённым названием, в котором школьники могут продемонстрировать своё знание устройства Интернета.

В 2016 году все вопросы и задания чемпионата были посвящены теме безопасности в Интернете – защите от сетевых угроз и борьбе с киберпреступниками, конфиденциальности данных, безопасности в социальных сетях.

Тема чемпионата 2018 года – технологии будущего.