**Понятие «сетевая грамотность», виды интернет угроз и рисков для младших школьников.**

Сетевая грамотность ещё одна важная часть цифровой грамотности. Кажется, даже важнее чем компьютерная грамотность, из-за количества угроз, которые хранит в себе Интернет.

**Сетевая грамотность** – это в свою очередь набор знаний, позволяющих безопасно и полезно использовать интернет. Это необходимый навык для успешной адаптации детей в сети.

**Защита персональных данных у детей**

Самым важным умением сетевой грамотности и основа нахождения в сети это защита персональных данных. В первую очередь, как пускать ребёнка в Интернет, нужно научить создавать и запоминать сложные пароли. Неважно пароль от аккаунта любимой игры или от социальной группы «Вконтакте». Конечно, если взрослым лень придумывать разные пароли и запоминать, вместо этого они хранят их на «стикерах» приклеенных на мониторе компьютера, что мы хотим от детей. Дети как губки, запоминают и повторяют за взрослыми, поэтому нам самим важно организовать свою безопасность и потом учить этому детей. Для этого есть всевозможные приложения для хранения ваших паролей, но рекомендуется хотя бы иметь текстовый документ, который будет храниться только на вашем персональном компьютере или на USB-носителе. Неважно, будь то «флешка» или внешний жёсткий диск он должен не выходить за пределы вашей жилплощади.

Практически любой доступ, к любым ресурсам, осуществляется по телефону или электронной почте. Следующим шагом, после того как создали почту, нужно научить пользоваться ей ребёнка. Помимо полезных уведомлений, магазинных чеках о покупках и сохранённых паролях, их ожидают странные, и даже опасные письма. Почтовые безопасные сервисы по блокировке нежелательной почты работают хорошо, но не идеально. Поэтому детям нужно подробно рассказать, что такое спам, фишинг и чем они отличаются.

**Спам** – это рассылка писем, зачастую вредоносная. Она распространяется массово «интернет-ботами» абсолютно случайно, вне зависимости от возраста, пола и места проживания. Стоит донести, что на первый взгляд безобидное письмо с названием «вы выиграли…» не несёт ничего хорошего. Не в коем случает не переходить по подозрительным ссылками и нужно сразу блокировать такие письма. Если же эти письма не введут никуда, а цель такого письма просто реклама какого-то продукта, они не опасны, но всё равно очень сильно докучают своим количеством.

**Фишинг**[[1]](#footnote-1) – это более изощрённый способ выудить персональные данные человека или заразить компьютер вирусом. Фишинг с английского языка «рыбалка». Название говорит само за себя, вас как бы «ловят» на удочку в сети Интернет. Фишинговые письма выглядят как письма от доверенных организаций. Это может быть, письмо от учителя, банка, директора и оно может вести на официальный адрес, но с одним отличием, одна или две буквы может отличаться от названия оригинального сайта. Когда идёт атака на конкретного человека, мошенники не поленятся даже сымитировать логотип и дизайн целого сайта. Поэтому нужно быть всегда внимательным и не вестись на «ложные» сайты.[[2]](#footnote-2)

Ещё в последнее время мошенники научились обходиться без ссылок, для этого вирусная программа может содержаться в рисунке или фотографии. Нужно сразу блокировать сообщения с текстом «Посмотри, это же ты на фотографии…» или «О, мы учились же вместе, нашёл твоё фото на сайте…».

Как только ребёнок усвоил информацию по этой теме и стал критически оценивать информацию можно пустить его в волшебный мир интернета.

**Интернет-ресурсы**[[3]](#footnote-3)– всё, что можно почитать, посмотреть и послушать. Всевозможные сайты, интернет-магазины, развлекательные площадки, форумы и чаты, это то из чего состоит Интернет.

Не нужно кривить душой, почти вся информация, которую многие используют для учёбы, она из Интернета. Дети, тем более, делая домашнее задание, особо не заморачиваются в выборе сайтов и проверки её подлинности из разных источников. Зашли на «Википедию», по первой ссылке и «так сойдет». Увы, далеко не все сайты гарантируют должную защиту личных данных или же психологическую защиту ребенка. Не всегда библиотекарь может заглянуть в монитор компьютера ребенка и посмотреть, что он там делает. Поэтому библиотеки в обязательном порядке должны иметь специальные системы фильтрации[[4]](#footnote-4) интернет-ресурсов, которые ограничивают доступ пользователей от вредной информации. В первую очередь должна стоять защита, которая запрещает скачивать или устанавливать ненужные программы и игры на общедоступные компьютеры.

Наличие антивирусных программ несёт в себе несколько полезных функций. Она защитит компьютеры от заражённых USB-носителей детей, на которые они переносят свои документы. Второе – они содержат «чёрные» и «белые» списки сайтов. «Чёрные» списки, постоянно пополняемые и обновляемые, они автоматически блокируют переходы по ссылкам на нежелательные источники. Это может быть информация порнографического характера, сайты экстремистского содержания или содержащая вредоносные действия: суицид или изготовление взрывчатого вещества. «Белые» в свою очередь, это настраиваемые списки сайтов, на которые конкретно Вы не ходите, чтобы ребёнок заходил. Как ещё наказать детей за прогулы в школе? Явно не запретом на прогулки с друзьями. Самый верный способ, который выбирают родители, блокируют сайты, игры или приложения своим детям.

**Общение в Интернете**

Ещё одна проблема, с которой чаще всего сталкиваются дети в Интернете, это негативное общение. Сейчас чаще всего от детей можно услышать термин «токсичный»,[[5]](#footnote-5) которое является англицизмом и обозначает «ядовитое», деструктивное поведение. Для Интернета, где границы между городами и странами полностью размыты, некоторые люди, необязательно дети, ведут себя неподобающим образом, отличающимся от реальной жизни. Ведь Интернет, это место своих законов. Зачастую многие проецируют свои проблемы и неудачи в комментариях под видеороликами, в чате или в других местах, где можно оставить своё мнение. Детям нужно рассказать, что стоит игнорировать такое общение, не нужно отвечать на агрессию. Порой такое «токсичное» общение от детей, не направлена на какого-то конкретного человека. Такое общение отражает их душевное состояние и они чувствуют свою безнаказанность в этот момент. Вот не понравился, кому-то в Интернете, выложенный, к примеру, рисунок на конкурсе талантов, и он оставляет свой гневный комментарий, выражая своё важное, как ему кажется, задевая этим автора. А есть дети, которые получают удовольствие «подкалывая» и принижая достоинство, даже там, где казалось бы невозможно. Таких людей называют «троллями»[[6]](#footnote-6).

**Троллинг** – это порой заведомо ложное высказывание, провокационное, сказанное для привлечения к себе внимания. Человеку, которому нечем заняться в радость поспорить с окружающими на тему, в которой они не разбираются. Но в споре, с таким человеком вы проиграете. Они всегда находят факты и доказательства, в которых вы не правы, даже если их ответы абсолютно иррациональны. Самое страшное для тролля это его полное игнорирование. Поэтому существует выражение «не кормите тролля», которое каждому ребенку нужно запомнить.

Но самое страшное явление, которое погубило много жизней это кибербуллинг.

**Кибербуллинг**[[7]](#footnote-7)– это травля, запугивание, унижение, направленное на конкретного человека. Отличие от буллинга классического, как не трудно догадаться, заключается в пространстве. Как ранее затрагивалось, на Интернет до недавних пор не распространялись законы реального мира. Сейчас же можно предоставить доказательства «скриншотами» переписки и аудиоголосовых сообщений, благодаря которым можно привлечь к ответственности виновника. Но даже это не пугает многих обидчиков и их привлекает возможность оставаться анонимным в Интернете. Цель кибербуллинга[[8]](#footnote-8) в унижении репутации человека путём распространения клеветы, порочащих фотографий, шантажа или распространения слухов, заведомо ложных.

В такие моменты дети не должны чувствовать свою беспомощность, нужно донести до них, что не стыдно и очень опасно скрывать такое от взрослых.[[9]](#footnote-9) Если по причине страха или стыда дети не могут поведать о своих проблемах родителям или другим взрослым, в рамках сетевой грамотности важно рассказать про телефон доверия. Это специальная психологическая служба всем нуждающимся. В ней работают профессионалы-психологи, с которыми анонимно можно поговорить или посоветоваться в непростой ситуации.[[10]](#footnote-10)

Также стоит родителям уделить внимание общению в интернете. Нужно знать с кем переписывается их ребёнок, чтобы избежать негативных последствий. Интернет это анонимная среда, где каждый может быть тем, кем захочет. Неизвестный собеседник или «друг из интернета»[[11]](#footnote-11) может вполне оказаться не тем, кем является.

**Интернет-зависимость**

Интернет зависимость, пожалуй, самая сильная зависимость на данный момент. Сейчас это уже стало считаться болезнью. Разделяют её на четыре вида. Первая и самая серьёзная «геймерская зависимость». Вторая зависимость это от социальных сетей, третья «интернет-сёрфинг», четвёртая бесконтрольное поглощение видеоконтента, пятая потребительская зависимость.

**«Геймерская зависимость»** –несложно догадаться зависимость от игр, в том числе от онлайн-игр. Онлайн-игры опасны тем, что они затягивают на очень долгий срок. В этих играх нельзя поставить на «стоп», разработчики постоянно выпускают обновления, что подпитывает интерес детей. Самые «засасываемые» это азиатские: китайские, корейские и японские. Здесь можно провести по несколько десятков лет, и для того, чтобы развить свой уровень многие готовы сидеть по 17 часов в день. Ещё одна проблема онлайн-игры это их условно-бесплатная система, так называемая free-to-play[[12]](#footnote-12), переводится как «играй бесплатно». Да игроков подкупает возможность бесплатно играть, без подписки с огромным количеством таких же человек. Но со временем они замечают, что кто-то сильно продвинулся вперёд в уровне, игровых доспехах и по сюжету. А всё потому, что основным доходом разработчиков в таких играх это внутриигровые покупки – улучшения, дополнительные рюкзаки для переноса предметов, возможность не терять «опыт» в случае, если ты не онлайн. И многие дети, которые хотят также, узнают, что всего лишь нужно пополнить счёт, скажем на 200 рублей. Но зависимость, на то и зависимость, что расходы растут, а возможность быть самым сильным в своей игре подкупает и вот уже ребёнок тратит не свои карманные деньги, предназначенные для обеда, а тянется к банковской карте родителя. Такая free-to-play система перекочевала в мобильные игры, где процветает, потому что мобильные игры идут практически на каждом смартфоне и разработка таких игр занимает меньше времени, чем хороший продукт для компьютера.

**Freemium** – ещё одна бизнес-модель онлайн-игр, когда ты играешь в игру бесплатно, но до определённого момента. И чтобы тебе продвинуться по сюжету или открыть дополнительные миссии, чтобы поиграть вместе с друзьями, тебе нужно заплатить какую-то сумму за дополнение к игре. Это тебя может коснуться через две недели игры или год, когда игра уже «засосала» полностью и у человека нет выбора.

Сейчас подавляющее большинство детей играет на игровых платформах Steam[[13]](#footnote-13) и Роблокс (Roblox)[[14]](#footnote-14) с огромным количеством бесплатных игр, в которых они могут столкнуться с всевозможными проблемами. Поэтому разговоры с детьми и родителями на эту тему сейчас более чем актуальны.

**Зависимость от социальных сетей** – трудно представить себя без социальных сетей, иногда вся работу построена на них. Для детей это свой мир, со своей самореализацией и одобрениями в виде «лайков». Реальное общение заменяется виртуальным, где всё ярко, интересно и просто. Важно детям показать прелесть реального мира, занимать их хобби и отграничивать время провождения в сети.[[15]](#footnote-15)

**«Интернет-сёрфинг»** это бессмысленное нахождение в Интернете. Так называемая форма провождения времени, когда человек «плывёт по течению», смотрит ненужные и бессмысленные новости. Это чаще происходит перед сном, когда можно не заметить, как за просмотром юмористических картинок или новостей из жизни «звёзд» пролетит вся ночь и не выспавшийся ребёнок идёт в школу.

**«Поглощение видеоконтента»**,это тоже, что и «интернет-сёрфинг», только когда ребёнок проводит много времени на видео-площадках. TikTok, среди детей самая затягивающая платформа, в котором полезного контента наверно 10% и встретить его можно только тогда, когда им интересуешься и пользуешься внутренним поисковиком.

**«Потребительская зависимость»**[[16]](#footnote-16) – это зависимость от «шопинга», или же от покупки всевозможных товаров в интернет-магазинах. Знакома и взрослым и детям, когда спонтанно покупаешь какую-нибудь вещь по акции, и потом задаёшься вопросом, а зачем она мне?

Также если пользоваться не официальными интернет-магазинами, есть риск потери персональных данных, таких как паспортные данные или же привязанные банковские карты. Обязательно стоит донести до детей, что оплачивать нужно с официальных интернет-магазинах, не привязывать банковские карты и вообще делать покупки только с разрешения родителей.

Также риск того, что в Интернете очень много подделок[[17]](#footnote-17) крайне велик. Дети и в частности молодёжь, смотря на своих музыкальных кумиров или блогеров, хотя одеваться также в дорогие бренды. Так как в онлайн-магазинах мы не можем примерить или пощупать вещь, а довольствуемся только отзывами и фотографиями других покупателей, большой риск попасть на недобросовестного продавца. В Интернете сейчас много подделок, или по другому **replica.** (Качественная или часто некачественная подделка вещи дорогого бренда). Не так страшно, если вещь стоит изначально в несколько раз дешевле оригинала, поэтому тут очевидно, что продукт не является брендовым. Но если вещь стоит огромных денег и ребёнок в надежде купить оригинальные, например, кроссовки потратит свои накопленные деньги «в никуда», а вещь прослужит в лучшем случае сезон. Мошенники модной одежды, стали настолько изощрены, что создают вещи практически неотличимые от известного товара.

Таким образом, можем сделать вывод, что интернет является невероятно мощным инструментом, но вместе с его преимуществами идут и определенные риски. Если оставить детей без присмотра, они могут столкнуться с угрозами, такими как кибербуллинг, доступ к ненадлежащему контенту или даже связи с опасными людьми. Именно поэтому обучение сетевой грамотности младших школьников является второй важной задачей после компьютерной грамотности. Объединение компьютерной и сетевой грамотности создает основу для полноценного освоения цифровой среды. С раннего возраста они начнут понимать, как технологии могут влиять на их жизнь и как они могут использовать их для достижения своих целей, оставаясь при этом в безопасности.

1. Кибербезопасность подростков в сети интернет. Противодействие киберугрозам : учебно-методическое пособие. – Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2022. – 65 с. Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/283286 (дата обращения: 21.03.2024). Режим доступа: для авториз. пользователей. [↑](#footnote-ref-1)
2. Хоффман Э. Безопасность веб-приложений : разведка, защита, нападение. – Санкт-Петербург [и др.] : Питер, 2021. – 327, [3] с. : ил. – (Бестселлеры O'Reilly). – 978-5-4461-1786-4. [↑](#footnote-ref-2)
3. Гущина, О. М. Цифровая культура : учебно-методическое пособие. – Тольятти : ТГУ, 2023. Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/396050 (дата обращения: 20.03.2024). – Режим доступа: для авториз. пользователей. [↑](#footnote-ref-3)
4. Цифровая школа: специализированное программное обеспечение в предметной учебной деятельности : учебно-методическое пособие. – Ставрополь : СГПИ, 2020. Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/193076 (дата обращения: 20.03.2024). – Режим доступа: для авториз. пользователей. [↑](#footnote-ref-4)
5. Квазинаучный термин «токсичный» в современной блогосфере (на материале русского, английского и французского языков) // Известия Волгоградского государственного педагогического университета. – 2022. – № 5 (168). – С. 132-139. – ISSN 1815-9044. Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/journal/issue/338315 (дата обращения: 14.11.2024). – Режим доступа: для авториз. пользователей. [↑](#footnote-ref-5)
6. Гайнуллина, Л. Ф. Троллинг как форма проявления иронии в интернет-пространстве: философский и культурно-антропологический аспекты // Известия Уральского федерального университета. Серия 3: Общественные науки. – 2019. – № 2(188). – С. 153-163. – ISSN 2227-2291. Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/journal/issue/311758 (дата обращения: 14.11.2024). – Режим доступа: для авториз. пользователей. [↑](#footnote-ref-6)
7. Гендина, Н. И. Информационная культура личности: технология продуктивной интеллектуальной работы с информацией в условиях интернет-среды : учебное пособие : в 2 томах. – Кемерово : КемГИК, 2020. Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/174716 (дата обращения: 20.03.2024). – Режим доступа: для авториз. пользователей. [↑](#footnote-ref-7)
8. Бенедетти Т. Кибербуллер в нокауте. Соцсети: инструкция по применению. – Москва : Эксмо, 2021. – 95 с. : цв. ил. – (Non-fiction. Подростки (11-14 лет)). – 978-5-04-154280-1. [↑](#footnote-ref-8)
9. Форназари Э. Что такое буллинг? : разбираемся вместе с героями любимых книжек!. – Москва : Росмэн, 2021. – 60, [3] с. : цв. ил. – 978-5-353-09859-1. [↑](#footnote-ref-9)
10. Шапкина А. Н. Антибуллинг : дополнительная общеразвивающая программа по профилактике буллинга : методические рекомендации : для учащихся 11-13 лет. – Москва : Национальное образование, 2022. – 127 с. : ил., табл. – (Психолог в школе). – 978-5-4454-1523-7. [↑](#footnote-ref-10)
11. Айкен М. Дядя из интернета любит меня больше, чем ты : как защитить ребенка от опасностей интернета. – Москва : Бомбора™ : Эксмо, 2020. – 398 с. – (Digital trends) (Top Business Awards). – 978-5-04-102310-2. [↑](#footnote-ref-11)
12. Сивоплясова, С. Ю. Цифровизация социально-экономических процессов. Цифровые технологии в повседневных практиках населения : учебное пособие. – Москва : МАИ, 2022. Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/256340 (дата обращения: 26.03.2024). – Режим доступа: для авториз. пользователей. [↑](#footnote-ref-12)
13. Баланов, А. Н. Комплексное руководство по разработке: от мобильных приложений до веб-технологий : учебное пособие для вузов. – Санкт-Петербург : Лань, 2024. Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/394577 (дата обращения: 31.03.2024). Режим доступа: для авториз. пользователей. [↑](#footnote-ref-13)
14. Плахотная, Ю. И. Ассоциация как механизм когнитивной деятельности в формировании концептуальной картины мира // Вестник Кемеровского государственного университета. – 2021. – № 2. – С. 541-550. Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/journal/issue/323180 (дата обращения: 31.03.2024). – Режим доступа: для авториз. пользователей. [↑](#footnote-ref-14)
15. Афанасьев А. А. Основы выживания в сети : краткий курс для детей и родителей : методическое пособие. – Москва : Наше завтра, 2023. – 122 с. : ил. – 978-5-907729-28-5. [↑](#footnote-ref-15)
16. Сивоплясова, С. Ю. Цифровизация социально-экономических процессов. Цифровые технологии в общественной жизни : учебное пособие. – Москва : МАИ, 2022. Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/256337 (дата обращения: 26.03.2024). – Режим доступа: для авториз. пользователей. [↑](#footnote-ref-16)
17. Грунт, Е. В. Потребительское поведение молодежи при выборе модной одежды // Известия Уральского федерального университета. Серия 3: Общественные науки. – 2017. № 1(161). – С. 26-38. Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/journal/issue/311811 (дата обращения: 26.03.2024). Режим доступа : для авториз. пользователей. [↑](#footnote-ref-17)