Организация базового уровня кибербезопасности детей

Моторин Владислав Валерьевич¹

¹*Новосибирский государственный педагогический университет,
Куйбышевский филиал, Куйбышев, Россия*

Аннотация. Введение. Проблема кибербезопасности детей становится особенно важной в современном мире. Современные дети и подростки проводят значительное время в интернете. Дети активно используют социальные сети, играют в онлайн-игры и смотрят видеоконтент. Предпочтение развлекательного контента увеличивает риски вовлечения в деструктивные сообщества. Такой контент может быть использован злоумышленниками для привлечения внимания и вовлечения детей в деструктивные сообщества и призыва к противоправным действиям. Неконтролируемое потребление контента повышает риск киберугроз как для детей, так и для взрослых. Дети особенно уязвимы перед киберугрозами из-за их поведения в сети. *Методология.* При решении проблемы в первую очередь обращается внимание на статистику киберпреступлений, оцениваются масштабы миграции проблем реальной жизни в плоскость виртуального поля, изучается характер деструктивных сообществ через анализ содержания постов и сообщений. Выявляется рост безответственного поведения в сети и его негативное влияние на реальную жизнь. Проведение опросов среди детей и взрослых позволяет оценить уровень осведомленности о киберугрозах и знание правил кибергигиены. Это дополняет сравнительный анализ знаний между разными возрастными группами. Проводится оценка уровня противодействия деструктивному контенту со стороны государства и семьи. Выявляются недостатки в информационной культуре и осведомленности о киберугрозах. *Результаты исследования.* Киберугрозы являются реальной опасностью, несмотря на свой виртуальный характер. Усугубляет ситуацию недостаточная осведомленность родителей, что делает детей уязвимыми к киберугрозам и манипуляциям со стороны злоумышленников, таким как кибербуллинг, мошенники, фейки, деструктивные сообщества, шок- и трэш-контент, пропаганда анорексии, ЛГБТ и др. Организации, такие как «Лига безопасного интернета», играют важную роль в борьбе с киберугрозами, предлагая просвещение, защиту прав пользователей и противодействие запрещенному контенту. Однако только лишь усилий со стороны государства недостаточно. Обеспечение кибербезопасности детей требует объединения усилий как родителей, так педагогов и общества. Основной упор следует сделать на информирование и обучение родителей. Наиболее эффективным средством являются краткие рекомендации для них по контролю и организации кибербезопасности в семейном окружении. *Заключение.* Применение простых правил цифровой гигиены в повседневной жизни, а также в жизни ребенка позволяет обеспечить базовый уровень киберзащиты детей и подростков в интернете. Очень важно привлекать внимание общественности к вопросам кибербезопасности через публикации и образовательные мероприятия, поддерживать ширококомасштабное просвещение среди всех возрастных групп.

Ключевые слова: кибербезопасность детей; интернет; социальные сети; киберпреступления; кибербуллинг; фейки; рекомендации по кибербезопасности; контент-фильтрация; кибергигиена

Для цитирования: Моторин В. В. Организация базового уровня кибербезопасности детей // Конструктивные педагогические заметки. – 2024. – № 3 (23). – С. 118–125.

Scientific article

Organizing a basic level of cybersecurity for children

Motorin Vladislav Valer'evich¹

¹*Novosibirsk State Pedagogical University, Kuibyshev branch, Kuibyshev, Russia*

Abstract. Introduction. The problem of cybersecurity of children is becoming especially important in the modern world. Modern children and teenagers spend a lot of time on the Internet. Children actively use social networks, online games and video content. The preference for entertainment content increases the risks of involvement in destructive communities. Entertainment content can be used by intruders to attract attention and involve children in destructive communities and illegal activities. Uncontrolled consumption of content increases the risk of cyber threats for both children and adults. Children are particularly vulnerable to cyber threats because of their online behavior. *Methodology.* When solving this problem, first of all, attention is paid to the statistics of cybercrimes, the scale of migration of real-life problems into the plane of the virtual field is estimated, the nature of destructive communities is studied through the analysis of the content of posts and messages. It reveals the growth of irresponsible behavior on the web and its negative impact on real life. Conducting surveys among children and adults allows you to assess the level of awareness about cyber threats and knowledge of the rules of cyber hygiene. This is complemented by a comparative analysis of knowledge between different age groups. The assessment of the level of counteraction to destructive content by the state and the family is carried out. Shortcomings in the information culture and awareness of cyber threats are revealed. *The results of the study.* Cyber threats are a real danger, despite their virtual nature. And this situation is aggravated by the lack of awareness of parents. This makes children vulnerable to cyber threats and manipulation by intruders, such as: cyberbullying, scammers, fakes, destructive communities, shock and trash content, propaganda of anorexia, LGBT, etc. Organizations such as the Safe Internet League play an important role in combating cyber threats by offering education, protecting user rights and countering prohibited content, but government efforts alone are not enough. At first, the most effective tool is brief recommendations for parents on how to control and organize cybersecurity in a family environment. *Conclusion.* The application of simple rules of digital hygiene in your daily life, as well as in the life of your child, allows you to organize a basic level of cyber protection for children and adolescents on the Internet. It is very important to draw public attention to cybersecurity issues through publications and educational events, and to support large-scale education among all age groups.

Keywords: cybersecurity of children; the Internet; social networks; cybercrimes; cyberbullying; fakes; cybersecurity recommendations; content filtering; cyber hygiene

For citation: Motorin V. V. Organizing a basic level of cybersecurity for children. *Constructive pedagogical notes*, 2024, no. 3 (23), pp. 118–125.

Введение. Проблема обеспечения кибербезопасности детей в наше время становится чрезвычайно актуальной по множеству причин. Начнем с того, что современ-

ные дети, подростки и молодежь проводят очень много времени в сети Интернет. Они активно общаются в соцсетях, проводят за играми в режиме онлайн, смотрят видеоролики и др. в виртуальном пространстве. При этом типичный интернет-серфер юного возраста предпочитает развлекательный контент, что значительно увеличивает риск вовлечения в какие-либо деструктивные сообщества через этот канал. Информация развлекательного характера чаще всего используется злоумышленниками как площадка для привлечения внимания и дальнейшей обработки пользователя с целью наживы, вовлечения в деструктивное сообщество, совершения противоправных действий. С нашей точки зрения, неконтролируемое потребление развлекательного контента в сети Интернет значительно повышает риск уязвимости даже взрослого пользователя перед киберугрозами, а ребенка тем более.

Методология. Убедитесь в серьезности рассматриваемой проблемы достаточно легко. Для этого следует проанализировать статистику киберпреступлений, которая увеличивается из года в год. Современное общество становится все более ориентированным на цифровой путь развития, соответственно, все проблемы реальной жизни мигрируют в виртуальную среду. Этот процесс ускоряется с каждым годом. Все чаще появляются публикации и новости о том или ином виде киберпреступлений. Простой анализ сообществ, имеющих деструктивную направленность, содержание постов и сообщений указывает, что рост безответственного поведения в сети Интернет растет, переходя в качественные изменения, которые проявляются уже в реальной жизни.

Статистические показатели по рассматриваемой проблеме подтверждают рост киберпреступлений, направленных на возрастной интервал «дети – молодежь». Разнообразии направлений деструктивных сообществ расширяется и модифицируется каждый год: терроризм, фейки, порнография, мошенники, скулшутинг, шок-контент, АУЕ, оффники, ЛГБТ и др. Чтобы убедиться в этом, достаточно задать ряд соответствующих запросов в поисковых системах популярных соцсетей.

В то же время наблюдения показывают, что уровень противодействия потоку деструктивного контента не имеет достаточно симметричного ответа. Информационная культура и осведомленность в области современных киберугроз у большинства взрослых, а тем более детей находится на низком уровне. В этом легко убедиться, проведя, например, опрос на знание элементарных правил кибергигиены среди детей. То же касается и взрослых. Их уровень в большинстве случаев несколько не выше, а, может быть, и ниже.

Несмотря на ряд законов и мероприятий, проводимых государством, острота проблемы не уменьшается, что можно проследить во многих публикациях [1; 2; 4–6]. Путь снижения остроты проблемы нам видится в широкомасштабном просвещении и взрослых, и детей в вопросах сетевой кибербезопасности. Для начала достаточно сформировать ряд простых правил цифровой гигиены, разработать ряд рекомендаций для сознательных родителей по контролю и организации элементов кибербезопасности, применимых в семейном окружении.

Результаты исследования. Причиной слабой осведомленности детей и молодежи о возможных киберугрозах является некомпетентности большинства родителей в этом вопросе. Многие взрослые даже не подозревают об угрозах виртуального мира, которые подстерегают их детей на просторах Интернета. Очень часто такие родители не заботятся даже о личной безопасности, не говоря уже о безопасности ребенка. Информационная культура таких взрослых как пользователей интернета находится на весьма низком уровне. Они часто становятся жертвами мошенников,

допускают утечку личной информации, раскрывают пароли злоумышленникам, а также страдают от сбоев программного обеспечения по собственной халатности.

Получается замкнутый круг: дети часто не хотят информировать родителей о своей онлайн-активности, а взрослые не проявляют интереса к тому, чем занимается ребенок на просторах Интернета. По сути, такие дети остаются безнадзорными перед лицом реальной опасности, исходящей от виртуального пространства. Они уязвимы перед виртуальными злоумышленниками. Существует большая вероятность, что такой ребенок может даже встретиться с опасным незнакомцем в реальной жизни после знакомства в интернете. Также дети могут случайно или же намеренно столкнуться с нежелательным контентом, включающим насилие, порнографию, шок-контент, фейковую информацию и т. д. Дети и подростки более уязвимы перед киберугрозами по сравнению со взрослыми, так как дети доверчивее, чем взрослые, поэтому методами социальной инженерии злоумышленнику через социальные сети и форумы проще выведать информацию личного характера, например, домашний адрес или номер телефона. Кибертравля, нападки, угрозы и оскорбления в сети с большей долей вероятности приводят к травмам и эмоциональному стрессу у детей, чем у взрослых. Опасному незнакомцу также проще войти в доверие к ребенку или подростку через виртуальный контакт, чем ко взрослому. Дети более подвержены манипуляциям.

Бесконтрольный характер интернет-общения детей породил новое явление – кибербуллинг. Это форма травли, осуществляемая с использованием цифровых технологий, представляющая серьезную проблему. В отличие от традиционного буллинга кибербуллинг может происходить круглосуточно, что делает его особенно опасным. Кибербуллинг включает в себя различные формы агрессии, такие как:

- оскорбление и унижение через публикацию негативных комментариев или изображений в социальных сетях;
- распространение слухов путем умышленно ложной информации о жертве;
- социальная изоляция и бойкот;
- исключение из онлайн-группы или чата;
- прямые угрозы физической расправы или другие формы запугивания с реализацией в реале.

Кибербуллинг может иметь серьезные психологические последствия для жертв, включая депрессию, тревожность, социальную изоляцию, резкое понижение самооценки и т. д. Эти последствия могут оказывать длительное влияние на эмоциональное и социальное развитие ребенка или подростка, что делает проблему кибербуллинга особенно актуальной для родителей и образовательных учреждений. Существуют различные методы и рекомендации для защиты детей от кибербуллинга.

1. Обучение и просвещение: важно обучать детей распознавать кибербуллинг и понимать, как реагировать на него. Это может включать обсуждение с родителями или учителями того, как безопасно использовать интернет.

2. Поддержка и открытость: родители должны создать атмосферу доверия, чтобы дети могли открыто говорить о своих переживаниях. Поддержка со стороны взрослых может помочь детям справиться с травлей.

3. Технологические решения: использование программ родительского контроля и фильтров может помочь ограничить доступ к нежелательному контенту и защитить детей от потенциальных угроз в интернете.

4. Сообщение о нарушениях: важно обучить детей, как сообщать о кибербуллинге, будь то через платформу, где происходит травля, или через правоохранительные органы, если ситуация выходит из-под контроля.

Кибербуллинг – это сложная и многогранная проблема. Исследования показывают, что явление стало распространенным среди детей и молодежи именно в связи с ростом использования сети Интернет. Больше всего от этого страдают школьники, которые легко становятся жертвами онлайн-насилия. Причем зачастую в роли агрессивной стороны чаще всего выступают ровесники, одноклассники, бывшие друзья и т. д., то есть участники своего же круга общения. Проблема усугубляется тем, что интернет-травля зачастую имеет латентный и лонгитюдный характер, протекая и нарастая годами, пока не выльется в реальное насилие или суицид в реальной жизни.

У современной молодежи системное и критическое мышление развито не в должной мере. Очень часто внимание детей и подростков захватывает недостоверная информация (фейк), нацеленная авторами на слабо контролируруемую сугубо эмоциональную реакцию пользователей без критического анализа. Было замечено уже давно [5], что основным полем для публикации сообщений выступают различные социальные сети. Основная цель создателей недостоверной информации – ввести как можно большее количество людей в заблуждение и вызвать общественный резонанс. Цели при этом могут быть различными, например, увеличение количества просмотров, месть, шутка, нанесение репутационного вреда конкретному лицу или организации и т. д.

Фейки – бич современного интернета. Для борьбы с ними применяются различные средства и технологии, например:

- федеральный закон «Об информации» №149-ФЗ, дающий определение фейка как недостоверной общественно важной информации, создающей угрозу жизни и здоровью граждан;
- автоматическое распознавание фейков (использование технологий управления данными для автоматического отделения фейков от реальных фактов; привлечение дополнительных информационных потоков для подтверждения проверяемого факта. Это может быть текст, фото, видео, голосовое сообщение);
- постоянный мониторинг сетевой активности (для осуществления данного процесса требуются специализированное ПО и серверные мощности);
- блокировка опасного контента (горячие линии для приема сообщений о противоправном контенте, что позволяет блокировать какую-то часть информации);
- быстрое оперативное опровержение фейков (необходимость публиковать ответ-опровержение на фейк на той же платформе в течение, например, двух часов);

В Российской Федерации существуют организации, которые занимаются вопросами кибербезопасности как для населения в целом, так и для детей в частности. Наиболее крупной из них является «Лига безопасного интернета» (ЛБИ) – организация, созданная в январе 2011 г. с целью формирования безопасного интернет-пространства России. Лига безопасного интернета занимается тремя основными направлениями.

1. Борьба с противоправным контентом. ЛБИ активно противодействует распространению опасного и запрещенного контента в интернете. Для этого в организации функционируют горячие линии, куда граждане могут сообщать о нарушениях. С момента своего создания Лига обработала более 340 тысяч обращений о детской

порнографии и более 41 тысячи о распространении наркотиков, что привело к блокировке более 146 тысяч ресурсов.

2. Просвещение и медиаграмотность. Лига занимается обучением детей и родителей навыкам медиаграмотности. С 2012 г. проводятся уроки по безопасности в сети Интернет, где обсуждаются темы распознавания опасного контента и защиты персональных данных. Каждый год проходит акция «Месяц безопасного Интернета».

3. Защита прав пользователей. ЛБИ принимает и обрабатывает сообщения о нарушении прав пользователей в интернете, стремясь обеспечить защиту граждан от мошенничества и других угроз.

«Лига безопасного интернета» включает в себя не только государственные структуры, но и коммерческие и общественные организации, а также индивидуальных участников, которые желают внести вклад в борьбу с опасным контентом. В ее состав входят десятки российских компаний, включая операторов связи и разработчиков программного обеспечения. «Лига безопасного интернета» играет важную роль в формировании безопасного пространства. Кроме Лиги существуют и другие интернет-порталы, которые предлагают пользователям различные учебные программы по кибербезопасности детей. Из них можно выделить, например: «Единый урок», «GeekBrains», «Лабораторию Касперского» [1], и «Российскую электронную школу» [2]. Предлагаемые этими организациями курсы позволяют осваивать основы кибербезопасности в режиме онлайн.

Если обратиться к вопросам обеспечения информационной безопасности детей в общеобразовательных учебных заведениях, то можно отметить, что ситуация здесь вполне удовлетворительная, так как соблюдаются некоторые административные и организационные правила, например, контакт учащихся с интернет-ресурсами осуществляется только под присмотром учителя или библиотекаря. В любом учебном заведении обязательным к использованию является специальное программное обеспечение для фильтрации контента. На сегодняшний день подавляющее большинство общеобразовательных учреждений со стороны интернет-провайдеров обеспечены средствами контент-фильтрации входящего трафика. Эти меры строго соблюдаются, поскольку они регулируются федеральными законодательными актами, такими как, например, Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию».

По поводу обеспечения кибербезопасности детей в учебных заведениях можно сказать, что ситуация в основном под контролем, но основное время ребенок проводит не в школе, а дома. Обеспечение кибербезопасности в этом случае целиком и полностью ложится на плечи родителей. К сожалению, здесь ситуация не так хороша, как этого хотелось бы. Целенаправленной концепции по обеспечению семейного подхода к решаемой проблеме на сегодняшний день не существует. Слабым звеном в системе обеспечения кибербезопасности детей, с нашей точки зрения, являются родители, а точнее их некомпетентность в этих вопросах. Именно проблему их информированности об основах кибербезопасности необходимо решать в первую очередь, на что указывают многие авторы [1; 3; 5; 6]. С нашей точки зрения, на первых порах помогут несложные и простые к выполнению рекомендации, соблюдение которых не составит особого труда, но при этом поможет обеспечить минимальный уровень информационной безопасности подрастающего поколения. Перечислим ряд конкретных мер, рассчитанных на сознательных родителей, по организации элементов домашней киберзащиты детей.

1. Располагайте компьютер или ноутбук ребенка в общедоступном месте, чтобы взрослые члены семьи могли легко контролировать его онлайн-активность.

2. Установите правила и ограничения по времени, проводимому ребенком в социальных сетях и за просмотром контента развлекательной направленности, с регулярным контролем настроек конфиденциальности.

3. Поощряйте открытое общение с ребенком по вопросам его сетевой активности, чтобы он рассказывал о своем опыте в интернете, включая подозрительные случаи общения и странные сомнительные знакомства.

4. Документируйте и оперативно информируйте соответствующие органы о фактах киберугроз в отношении ребенка.

5. Обучайтесь сами и обучайте детей основам кибергигиены, таким как навыки распознавания фишинговых атак, безопасное скачивание файлов, использование паролей и т. д.

6. Заключите договор с интернет-провайдером на предоставление услуг с контент-фильтрацией.

7. Обязательно используйте специальное программное обеспечение для фильтрации и блокировки нежелательного контента на мобильном телефоне ребенка.

Заключение. Эти несложные правила значительно усложняют задачи потенциальных злоумышленников и заметно повышают уровень безопасности детей. В соответствии с Конституцией РФ каждый ребенок имеет право на кибербезопасность. Основным закон нашего государства гарантирует возможность свободного поиска, получения, передачи информации, но при этом запрещает доступ к информации о частной жизни гражданина. Этот принцип действует в отношении не только взрослых, но и детей. Можно даже утверждать, что защита частной жизни детей должна обеспечиваться в большей степени, чем взрослых, которые, имея жизненный опыт, могут позаботиться о себе. Ограждением подрастающего поколения от киберугроз должны заниматься как государство, так и сами родители, повышая свой уровень информационной культуры и киберкомпетентности. Таким образом, обеспечение кибербезопасности детей является важной задачей, требующей комплексного подхода с использованием правовых, технических и организационных мер как со стороны государства, так и со стороны родителей. Только в этом случае эффективность мероприятий достигнет такого уровня, который будут соответствовать современным технологиям, создавая при этом надежную защиту подрастающего поколения от киберугроз.

Список источников

1. Кибербезопасность для детей – защита от угроз в интернете. Как научить детей кибербезопасности [Электронный ресурс] // Kaspersky: Лаборатория Касперского. – URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/cybersecurity-for-kids> (дата обращения: 17.06.2024).

2. Кибербезопасность для детей и взрослых [Электронный ресурс] // Российская электронная школа. – URL: <https://resh.edu.ru/page/cyber-project> (дата обращения: 17.06.2024).

3. *Смирнов В. М., Чернякова Е. М.* Право ребенка на кибербезопасность // Научно-образовательный журнал для студентов и преподавателей «StudNet». – 2022. – № 3. – С. 206–211.

4. *Степанова Н. А.* Обеспечение информационной безопасности детей в цифровом пространстве // Гуманитарные исследования Центральной России. – 2024. – № 1 (30). – С. 59–77.

5. Чельшьева И. В. Мир социальных сетей и семейное воспитание школьников: научно-популярное издание. – Таганрог: Изд-во Таганрог. ин-та имени А. П. Чехова, 2014. – 128 с.
6. Ченушкина С. В. Кибербезопасность детей в цифровом пространстве // Современные вызовы и пути решения проблем в сфере защиты прав детей: реализация принципов конвенции о правах ребенка: сборник материалов II Всерос. науч.-практ. конференции. – Екатеринбург, 2022. – С. 196–200.

References

1. *Cybersecurity for children – protection from threats on the Internet. How to teach children cybersecurity* [Electronic resource]. Kaspersky: Kaspersky Lab. URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/cybersecurity-for-kids> (accessed: 17.06.2024). (In Russian)
2. Cybersecurity for children and adults [Electronic resource]. *Russian electronic school*. URL: <https://resh.edu.ru/page/cyber-project> (accessed: 17.06.2024). (In Russian)
3. Smirnov V. M., Chernyakova E. M. The right of the child to cybersecurity. *Scientific and Educational Journal for Students and Teachers "Studnet"*, 2022, no. 3, pp. 206–211. (In Russian)
4. Stepanova N. A. Ensuring the information security of children in the digital space. *Humanitarian Studies of Central Russia*, 2024, no. 1 (30), pp. 59–77. (In Russian)
5. Chelysheva I. V. *The world of social networks and family education of schoolchildren: a popular scientific publication*. Taganrog: Taganrog Publishing House. Chekhov Institute, 2014, 128 p. (In Russian)
6. Chenushkina S. V. Cybersecurity of children in the digital space. *Modern challenges and solutions to problems in the field of protection of children's rights: implementation of the principles of the Convention on the Rights of the Child*: Collection of materials of the II All-Russian scientific and practical conference. Yekaterinburg, 2022, pp. 196–200. (In Russian)

Информация об авторе

В. В. Моторин, кандидат педагогических наук, доцент кафедры математики, информатики и методики преподавания, Новосибирский государственный педагогический университет, Куйбышевский филиал, Куйбышев, Россия.

Information about the author

V. V. Motorin, Candidate of Pedagogical Sciences, Associate Professor of the Department of Mathematics, Computer Science and Teaching Methods, Novosibirsk State Pedagogical University, Kuibyshev Branch, Kuibyshev, Russia.

Поступила: 28.07.2024

Одобрена после рецензирования: 19.08.2024

Принята к публикации: 30.08.2024

Received: 28.07.2024

Approved after review: 19.08.2024

Accepted for publication: 30.08.2024