**Пескова Ольга Викторовна**

**(ПГГПУ, ZM1313)**

**Безопасность детей в Интернете**

***Аннотация.*** *В статье рассмотрены вопросы детской и подростковой безопасности в интернете. Описаны правила поведения и технические средства для решения проблемы контроля действий ребенка в сети.*

***Ключевые слова:*** *интернет безопасность, кибербезопасность, правила безопасности в Интернете, вредоносный контент, Родительский контроль, буллинг, вирус, безопасный контент, детская безопасность, интернет-пространство.*

*O. Peskova*

***Safety of children on the Internet***

***Annotation.*** *The article deals with the issues of child and adolescent safety on the Internet. The rules of behavior and technical means for solving the problem of controlling the child's actions in the network are described.*

***Keywords:*** *internet security, cybersecurity, Internet security rules, malicious content, parental control, bullying, virus, secure content, child safety, Internet space.*

Каждый современный человек ежедневно проводит очень много времени в интернете. Российская аудитория интернет-пространства стремительно растет – дети, подростки и молодежь составляют его значительную часть. Сегодня каждый третий ребенок в нашей стране выходит в интернет, и чем старше подросток, тем больше среди них «интернетчиков».

«Детский» интернет отличается от «взрослого», в основном детская аудитория предпочитает играть в интернете, смотреть и снимать небольшие видеоролики, информацию дети ищут чаще всего исходя из учебной задачи, создают и управляют мультфильмами[[1]](#footnote-1). В виду того, что интернет дает пользователю огромные возможности как высокотехнологичный источник коммуникации, как инструмент поиска и получения информации-дети и подростки открывают и познают мир, формируют собственную личность.

С развитием интернет-технологий резко возросло число тех, кто пользуется его возможностями в неблаговидных целях. Как следствие немалая часть преступлений «перешедшая» или «родившаяся» в интернете[[2]](#footnote-2).

Ежедневно находясь в сети, пользователь должен понимать и отдавать отчет своим действиям по размещению информации на Интернет-ресурсах, о скачиваемых файлах, о способах и манере общения и т.п. В настоящее время, через возможные средства массовой информации, до пользователей, а в частности родителей, IT-специалисты и специалисты по Интернет-безопасности пытаются донести правила безопасного поведения в сети Интернет для детей. Государство на своем уровне так же регулирует этот вопрос: по средством введения элективных курсов или программ дополнительного образования в школах, колледжах, ВУЗах. Безусловно, обучить пользователя работать в интернете и делать это безопасно для себя и других – одна из важнейших задач.

Сейчас, когда информационные технологии общедоступны, со стороны правительства принимаются серьёзные меры по обеспечению безопасности всех граждан, обращающихся к ресурсам всемирной паутины – включая несовершеннолетних. Законодательство в сфере интернет-безопасности в разных странах мира может незначительно отличаться, но проблемы, с которыми оно борется, имеют сходное происхождение.

С 2000 года в США действует закон о защите конфиденциальности детей в Интернете (COPPA), призванный защитить лица младше 13 лет от раскрытия личной информации в сети. Закон направлен на регулирование работы вебсайтов – особенно таких социальных сетей, как Facebook и Instagram. После внедрения закона, регистрация на данных платформах возможна только пользователями старше 13 лет.

Одной из основных причин возникновения такого правового акта стала уязвимость детей дошкольного и младшего школьного возраста в сети интернет – ведь именно дети этих возрастных категорий становятся легкой добычей для интернет-хищников (лиц, которые посредством сети совершают противоправные действия по отношению к несовершеннолетним), а также подвергаются унижению (буллингу[[3]](#footnote-3)) и онлайн-груммингу[[4]](#footnote-4).

В России не существует действительного закона, ограничивающего доступ детей к социальным сетям. В 2017 г. на обсуждение была выдвинута инициатива о запрете социальных сетей для детей младше 14 лет, которая, однако, в связи с недоработками, была отклонена. В конце 2020 года Государственная Дума снова вернулась к обсуждению данного вопроса и законопроекта, предлагающего регулирование деятельности лиц, не достигших 14-летнего возраста, в соответствии с которых предлагается ввести обязательную регистрацию в социальных сетях с использованием паспортных данных. Однако, после мартовских заседаний законопроект так и не был принят, и направлен на доработку, ввиду того, что подразумевает редакцию многих нормативно-правовых актов. Но данный факт не означает, что сфера киберпространства на территории Российской Федерации никак не регулируется. В России действует федеральный закон N 436-ФЗ от 29 декабря 2010 (ред. от 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью и развитию», согласно которому производится разделение информационной продукции на пять категорий и запрещается распространение информации среди детей в зависимости от их возраста.[[5]](#footnote-5) На территории Российской Федерации, при поддержке комитета по информационной политике и информационным технологиям, были внесены изменения в Кодекс об административных правонарушениях, в частности наложения санкций за оскорбление и унижение чести и достоинства человека высказанные онлайн[[6]](#footnote-6). Действие данного закона вступило в силу с 1 февраля 2021 года. В соответствии с содержанием санкции ответственность за ее исполнение ложиться полностью на владельцев социальных сетей, в виду того, что пользователь – это «арендатор» канала.

Дети и подростки – это отдельная и очень уязвимая категория пользователей интернет-пространства. Существует множество способов и средств, для того, чтобы оградить их от нежелательного контента и необдуманных действий. Рассмотрим наиболее значимые из них.

1. **Блокировка сайтов с ненадлежащим контентом.**

Не секрет, что далеко не все сайты предназначены для просмотра детьми. Ребенок может случайно наткнуться на сайт с ненадлежащим контентом просто через запрос в поисковой системе или пройдя по ссылке, которую отправил приятель (или любой пользователь, имеющий на то возможность).

Провайдер рекомендует использовать функцию Родительского контроля. Так вы будете уверены, что сайты с «запрещенным» контентом не просматриваются вашим ребенком. Она доступна и как отдельное защитное решение, и в составе комплексных.

Функция «безопасный поиск» в Родительском контроле блокирует неприемлемый контент, а большинство решений предоставляют родителям подробные отчеты, о том, что делает их ребенок в Интернете.

## Не вступайте в разговоры с незнакомыми людьми.

Ребенок с удовольствием играет в новейшую онлайн-игру с друзьями, общаясь с ними через чаты? Но в этих чатах также есть киберпреступники, которые прячутся за аватарами, стараясь обманом вынудить ваших детей раскрыть личную информацию. Эта информация затем может использоваться для кражи ваших идентификационных данных и денег.

Игра в известные игры или игры на проверенных сайтах может помочь защитить вашего ребенка. Но даже в этом случае вам будет сложно защитить своего ребенка в Интернете, просто отслеживая, с кем и о чем он разговаривает онлайн.

В таком случае помогут различные защитные продукты, которые не позволяют ребенку отправлять через чаты и мессенджеры личную информацию, например, номер банковского счета, имена и адреса.

И в этих чатах «обитают» не только киберпреступники. К сожалению, как и в реальной жизни, в Интернете ребенок может стать жертвой онлайн-издевательств[[7]](#footnote-7).

## Не поддавайтесь онлайн-буллингу.

На игровых сайтах некоторые участники играют, просто чтобы провоцировать и издеваться над другими игроками. Таких называют «[кибербулли](https://www.kaspersky.ru/about/press-releases/2015_ugroza-detjam-o-kotoroj-ne-znajut-vzroslye)».

Контролировать и предотвращать интернет-травлю в видеоиграх сложно. Как правило, модераторы пытаются блокировать хулиганов, но при большом количестве игроков невозможно уследить за каждым.

И здесь опять на помощь придут функции родительского контроля. Они отслеживают, с кем ваш ребенок общается онлайн, и позволяют вам блокировать любые нежелательные контакты.

Вы также можете получать предупреждения, когда какое-либо из обозначенных вами слов используется в онлайн-коммуникации.

Обратите внимание: даже при такой защите все равно невозможно полностью контролировать действия своего ребенка в Интернете.

Безобидные на первый взгляд сайты могут содержать вредоносные ссылки, поставят под угрозу безопасность всей вашей сети.

## Не скачивайте вирус.

Киберпреступники знают, что дети часто ищут в Сети бесплатное ПО, музыку и игры. Они также знают, что дети часто доверяют ссылкам и вложениям электронной почты[[8]](#footnote-8).

Если ваш ребенок пройдет по одной из этих ссылок, он может загрузить вирус, который не поставит под угрозу безопасность не только его компьютера, но всей вашей сети. Ребенок может сделать это непреднамеренно: он всего лишь кликнул на рекламный баннер, а вредоносное ПО уже незаметно загружается на его компьютер и угрожает его безопасности.

В любом случае, лучшая защита - это надежное защитное решение, которое блокирует небезопасные ссылки и проверяет каждую скачиваемую программу на наличие признаков вредоносного ПО. Вы будете иметь возможность контролировать всю домашнюю сеть с вашего компьютера и настраивать параметры безопасности для каждого устройства по отдельности[[9]](#footnote-9).

Это общие правила безопасности, соблюдая и применяя которые вы сможете обезопасить своего ребенка при работе в интернет-пространстве. Но следует помнить, что техническое решение проблемы никак не влияет на внутренние и возрастные особенности развития и поведения ребенка. В первую очередь важно помнить, что взрослые не должны забывать о детях и о «живом» общении. Главной проблемой современного общества является то, что у людей не хватает на него времени, мы слишком много и часто заняты: работой, решением повседневных задач и проблем, бытом. Зачастую происходит так, что родители предоставляют ребенку полную свободу действий в раннем, психологически незрелом возрасте. Что в таком случае происходит? Ребенок понимает, что родителям некогда, что им не до него и пытается найти «свое» общество в интернете. Иногда с ребенком нужно просто разговаривать, слышать и слушать его, несмотря на возраст, принимать участие в решении его «детских» проблем. Как следствие, ребенок будет вдумчив на просторах интернета, не станет автоматически нажимать кнопку «да» при появлении запроса на странице и не поддастся на провокации кибер-хулиганов или потенциальных киберпреступников. Очень важным является выстраивание доверительных детско-родительских отношений, тогда вы всегда будете знать, чем занят ваш ребенок, с кем он общается и какие проблемы у него возникают. И за их решением он пойдет к вам, а не к виртуальным «друзьям». Важно помнить, что защитные решения и внутренние убеждения дополняют эту комплексную работу, контролируя поведение ребенка в Интернете, что обеспечивает его и вашу безопасность.

**Библиографический список**

1. Безопасность детей в сети Интернет. Электронный ресурс. Режим доступа: - https://liceum46.edusite.ru/p31aa1.html
2. Детская безопасность в Интернете – руководство для родителей. Электронный ресурс. Режим доступа: - https://findmykids.org/blog/ru/detskaya-bezopasnost-v-internete
3. Что меняется в законодательстве о социальных сетях? Электронный ресурс. Режим доступа: - http://duma.gov.ru/news/50660/
4. Защите детей в Интернете. Электронный ресурс. Режим доступа: - https://www.kaspersky.ru/resource-center/preemptive-safety/kids-online-safety
5. Босова Л.Л. УМК по информатике 7-9 класс: учебник. –М.: БИНОМ. Лаборатория знаний, 2019. -248с. (с.185)
6. Угринович Н.Д. Информатика и ИКТ. Базовый уровень: учебник для 10 класса. – М.: БИНОМ. Лаборатория знаний, 2009. -212с.

1. Угринович Н.Д. Информатика и ИКТ. Базовый уровень: учебник для 10 класса. – М.: БИНОМ. Лаборатория знаний, 2009. -212с. [↑](#footnote-ref-1)
2. Безопасность детей в сети Интернет. Электронный ресурс. Режим доступа: - https://liceum46.edusite.ru/p31aa1.html [↑](#footnote-ref-2)
3. намеренные оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени. Часть киберкультуры. [↑](#footnote-ref-3)
4. процесс общения в сети, во время которого в доверие к ребёнку втирается незнакомый человек для использования его в своих целях. [↑](#footnote-ref-4)
5. Детская безопасность в Интернете – руководство для родителей. Электронный ресурс. Режим доступа: - https://findmykids.org/blog/ru/detskaya-bezopasnost-v-internete [↑](#footnote-ref-5)
6. Что меняется в законодательстве о социальных сетях? Электронный ресурс. Режим доступа: - http://duma.gov.ru/news/50660/ [↑](#footnote-ref-6)
7. Защите детей в Интернете. Электронный ресурс. Режим доступа: - https://www.kaspersky.ru/resource-center/preemptive-safety/kids-online-safety [↑](#footnote-ref-7)
8. Босова Л.Л. УМК по информатике 7-9 класс: учебник. –М.: БИНОМ. Лаборатория знаний, 2019. -248с. (с.185) [↑](#footnote-ref-8)
9. Защите детей в Интернете. Электронный ресурс. Режим доступа: - https://www.kaspersky.ru/resource-center/preemptive-safety/kids-online-safety [↑](#footnote-ref-9)