ISSN 0869-4915

ОБЩЕРОССИЙСКИЙ МАССОВЫЙ ИЛЛЮСТРИРОВАННЫЙ ЖУРНАЛ

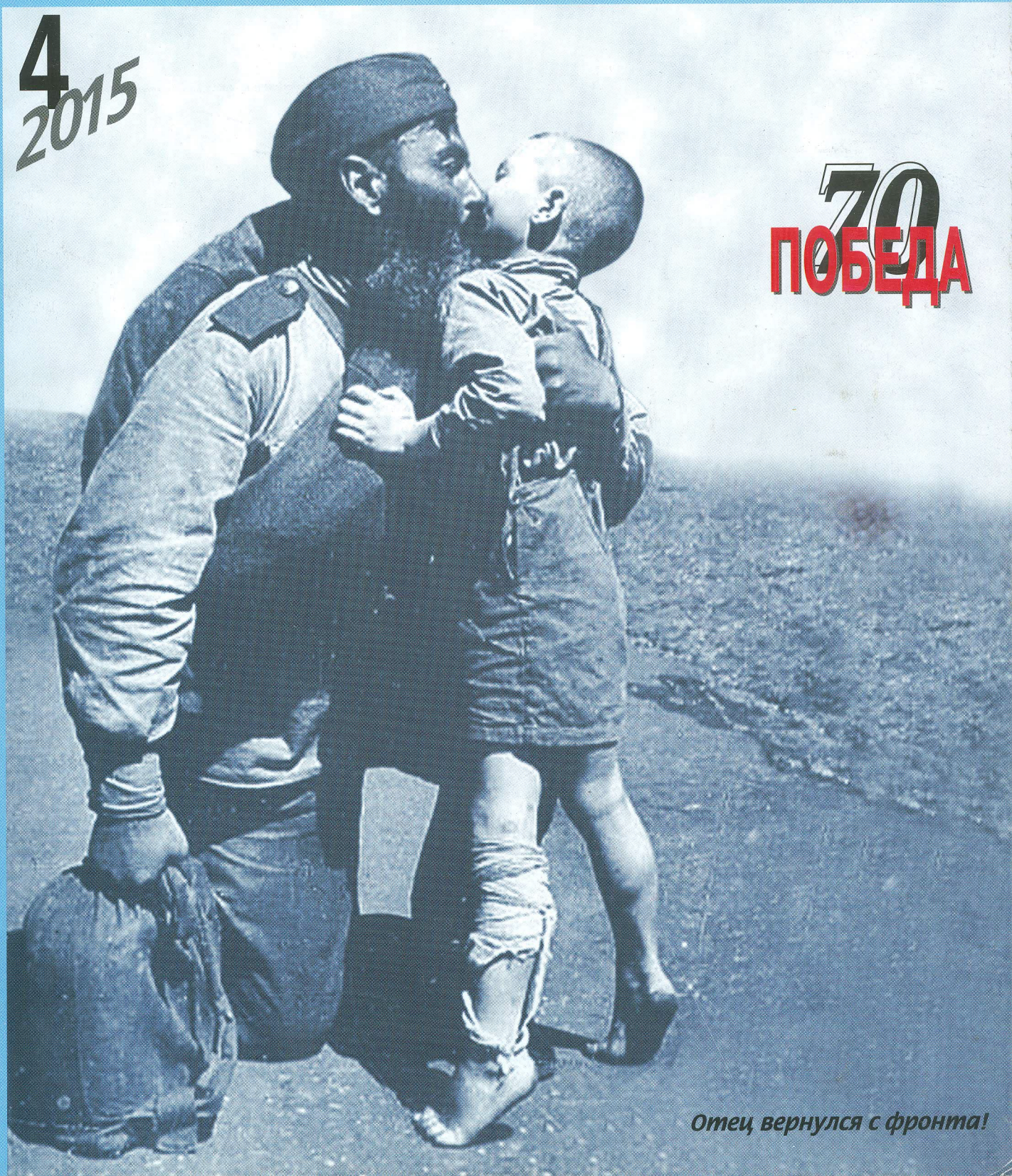
# БИБЛИОТЕКА

ИЗДАЁТСЯ С 1910 г.

НАГРАЖДЁН ОРДЕНОМ «ЗНАК ПОЧЁТА»

4
2015

70 ПОБЕДА



*Отец вернулся с фронта!*

Светлана ГАСПАРЯН,
юрисконсульт Библиотеки
имени И.М. Лаврова

# ЦИФРОВАЯ ЗОНА ОПАСНОСТИ

## • ПЯТЬ СОВЕТОВ ТЕМ, КТО РАБОТАЕТ С ЮНЫМИ ПОЛЬЗОВАТЕЛЯМИ СЕТИ ИНТЕРНЕТ

**Несмотря на безусловно положительную роль, которую коммуникационные средства и Интернет играют в жизни человека, существуют определённые риски при их использовании. Особой опасности в незащищённом информационном пространстве подвергаются дети. Публикуемая статья поможет библиотекарям, работающим с юными пользователями, родителям и педагогам лучше сориентироваться в этой всё более обостряющейся и тревожащей общество проблемной ситуации.**

Совершенствование технологий создаёт условия для эффективного развития современного общества. Коммуникационные средства, став неотъемлемой частью жизни людей, проникли во все сферы их деятельности. Мобильные телефоны, коммуникаторы, компьютеры, Интернет открыли новые возможности для общения, образования, работы, отдыха и творческой самореализации личности. Число пользователей мобильных телефонов и Глобальной сети с каждым днём неуклонно увеличивается. Большую их часть составляют молодёжь, дети.

Важно понимать, что наряду с успешным решением образовательных задач в Интернете можно натолкнуться на источники, несущие негативную, лживую и неэтичную информацию. Присутствует и информация агрессивного и социально опасного содержания. А предпочтение виртуального мира реальности способно оказать негативное влияние на психику и здоровье ребёнка, вызвать ухудшение зрения, повышенную тревожность, раздражительность, социальную дезадаптацию и зависимое поведение.

Обеспечение государством информационной безопасности детей, защита физического, умственного и нравственного развития несовершеннолетних, а также человеческого достоинства во всех аудиовизуальных медиауслугах и электронных СМИ — требование международного права.

Стандарты в области информационной безопасности детей нашли отражение и в российском законодательстве. Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» устанавливает правила медиабезопасности при обороте на территории России печатной, аудиовизуальной продукции на любых видах носителей, программ для компьютеров и баз данных СМИ, а также информации, размещаемой в телекоммуникационных сетях и сетях подвижной радиотелефонной связи. Закон определяет информационную безопасность детей как состояние защищённости, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

### *Совет первый:* *Защитите детей от нежелательного контента*

Контентные риски — это материалы (тексты, картинки, аудио-, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию,

эротику и порнографию, нецензурную лексику, разжигающие расовую ненависть, содержащие пропаганду анорексии и булимии, суицида, азартных игр, употребления наркотических веществ и т. д.

Как же помочь ребёнку избежать столкновения с нежелательным контентом?

- Приучите советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации подобного рода.
- Объясните детям, что далеко не всё, что они могут прочесть или увидеть в Интернете, — правда. Приучите их спрашивать о том, в чём они не уверены.

Старайтесь спрашивать ребёнка об увиденном в сети, поскольку зачастую, открыв один сайт, он хочет познакомиться и с другими подобными ресурсами.

### *Совет второй:*
### *Научите ребёнка быть осторожным при знакомстве с новыми людьми в сетях*

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты, киберпреследования, кибербуллинг и др.

Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут оказаться злоумышленники. В некоторых случаях они стремятся обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам. Бывает, что преступники заняты поисками жертвы. Специалисты используют термин «груминг», обозначающий установление дружеских отношений с ребёнком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребёнка. Общаясь лично («в привате»), злоумышленник входит в доверие, пытается узнать личную информацию и договориться о встрече.

Как предупредить груминг?

- Будьте в курсе того, с кем контактирует в Интернете ваш ребёнок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем общаются.
- Объясните ребёнку, что нельзя разглашать в сетях информацию личного характера (номер телефона, домашний адрес, номер школы и т. д.), а также пересылать интернет-знакомым свои фотографии.
- Если ребёнок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу.
- Не позволяйте ребёнку встречаться с онлайн-знакомыми без вашего разрешения или в отсутствие взрослого человека. Если ребёнок желает встретиться с новым интернет-другом, следует настоять на сопровождении его взрослым на эту встречу.
- Интересуйтесь, куда и с кем ходит ваш ребёнок.

**Как избежать кибербуллинга?**

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребёнку опасность и не всегда знают, как её предотвратить.

Вот на что следует обращать внимание, чтобы вовремя заметить, что ребёнок стал жертвой кибербуллинга.

- Беспокойное поведение. Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя поведением. Депрессия и нежелание идти в школу — явные признаки того, что ребёнок подвергается агрессии.
- Неприязнь к Интернету. Если ребёнок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно это надоедает. Но, как правило, внезапное нежелание пользоваться Интернетом связано с проблемами, возникшими в виртуальном мире.
- Нервозность при получении новых сообщений. Негативная реакция ребёнка на звук письма, поступившего по электронной почте, должна насторожить родителя. Если ребёнок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Каковы меры предупреждения кибербуллинга?

- Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов: читать грубости так же неприятно, как и слышать.
- Научите детей правильно реагировать на обидные слова или действия других пользователей (то есть не отвечать тем же).
- Объясните, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.
- Старайтесь следить за тем, что ваш ребёнок делает в Интернете, а также за его настроением после пользования сетью.

### *Совет третий:*
### *Предостерегите от интернет-мошенников*

Кибермошенничество — один из видов преступлений, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских

счетов, паспортные данные, коды, пароли и др.) с целью причинить материальный или иной ущерб.

Если дети имеют доступ к вашим банковским данным или номеру кредитной карты, они могут приобрести практически что угодно через Интернет — от постера до роскошной машины, а также оплатить услуги — от онлайновых игр до путешествия вокруг света.

Меры предупреждения кибермошенничества:

- Проинформируйте ребёнка о распространённых методах мошенничества и научите его советоваться со взрослыми, перед тем как воспользоваться теми или иными услугами в Интернете.
- Установите на компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут использоваться для предупреждения множества действий на заражённых системах, наиболее частым из которых является кража конфиденциальных данных.
- Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надёжности и, если ваш ребёнок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности. При обращении в такой магазин:

— ознакомьтесь с отзывами покупателей;
— проверьте реквизиты и название юридического лица — владельца магазина;
— уточните, как долго существует магазин;
— поинтересуйтесь, выдаёт ли он кассовый чек;
— сравните цены в разных интернет-магазинах;
— позвоните в справочную магазина;
— обратите внимание на правила интернет-магазина;
— выясните, сколько точно вам придётся заплатить.

### *Совет четвёртый:*
### *Покажите вред здоровью от игровой и интернет-зависимости*

В России всё более актуальны проблемы так называемой интернет-зависимости (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, если у сотрудников появляется влечение к пребыванию онлайн. Компьютерная зависимость — патологическое пристрастие к проведению времени за компьютером. Это навязчивое желание включить компьютер и неспособность его выключить. Человек может проводить в виртуальной реальности от 5 до 20 часов в сутки.

Согласно исследованиям К. Янг, предвестниками интернет-зависимости являются:

- навязчивое стремление постоянно проверять электронную почту;
- предвкушение следующего сеанса онлайн;
- увеличение времени, проводимого онлайн;
- увеличение количества денег, расходуемых онлайн.

Если считаете, что ваши близкие, в том числе дети, страдают от чрезмерной увлечённости компьютером и это наносит вред их здоровью, учёбе, отношениям в обществе, приводит к конфликтам в семье, можете обратиться к специалистам. Они помогут построить диалог и убедить зависимого признать существование проблемы, согласиться получить помощь, оказываемую как в терапевтических группах, так и стационарно, с использованием специальных медицинских процедур.

### *Совет пятый:*
### *Убедите ребёнка не загружать на компьютер вредоносные программы*

Такие программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) наносят вред компьютеру и хранящейся в нём информации. Они также могут снижать скорость обмена данными и даже использовать компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Меры предупреждения появления вредоносных программ:

- Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить атаки злоумышленников.
- Используйте только лицензионные программы и данные, полученные из надёжных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.
- Объясните ребёнку, как важно использовать проверенные информационные ресурсы и не скачивать нелицензионный контент.
- Делайте резервную копию важных данных.
- Старайтесь периодически менять пароли (например, электронной почты) и не используйте слишком простые.
- Регулярно полностью проверяйте свои домашние компьютеры.

Не стоит думать, что Интернет — это безопасное место, в котором дети могут чувствовать себя защищёнными. Как известно, использование средств воспитательной работы без организации действенного контроля — практически бесполезное занятие: точно так же, как и осуществление репрессивного контроля без воспитательной работы. Только в их единстве удастся помочь детям чувствовать себя в безопасности, оградить их от влияния злоумышленников. Пусть компьютер и Интернет будут вам и вашим детям во благо!